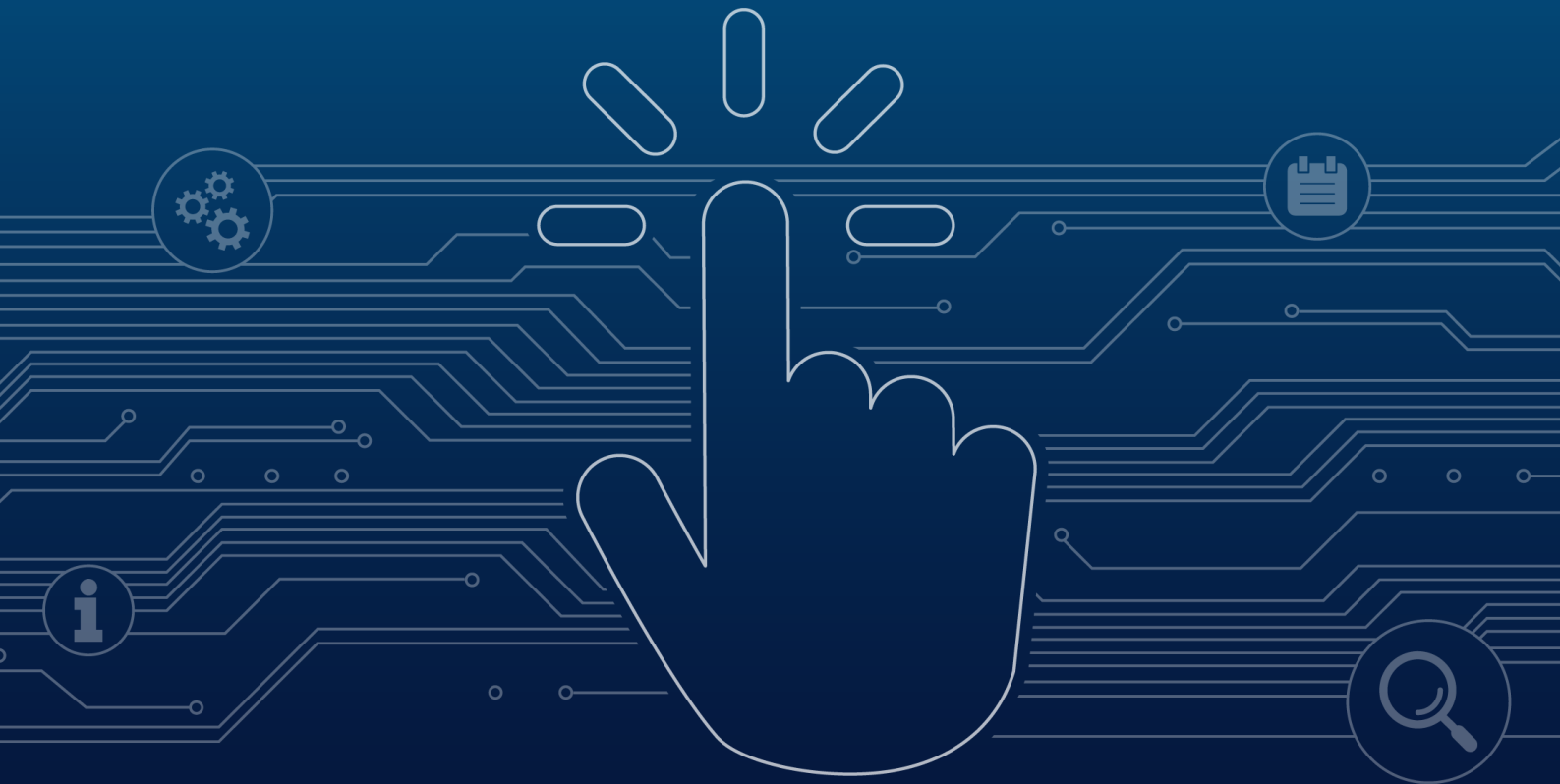


# PRTG Manual

Comprehensive IT monitoring



## [PRTG Manual](#)

© 2024 Paessler GmbH

All rights reserved. No parts of this work may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems—without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: July 2024 in Nuremberg



# Contents

<b>Part 1 Welcome to PRTG</b>	<b>13</b>
1.1 About this Document	15
1.2 Key Features	16
1.3 New in this Version	19
1.4 Available Licenses	20
1.5 System Requirements	22
1.6 Introduction: Monitoring with PRTG	33
<b>Part 2 Quick Start Guide</b>	<b>37</b>
2.1 Step 1: Download, Installation, and First Login	39
2.2 Step 2: Smart Setup	41
<b>Part 3 Using PRTG Hosted Monitor</b>	<b>48</b>
3.1 Create a PRTG Hosted Monitor Instance	50
3.2 Manage a PRTG Hosted Monitor Subscription	61
3.3 Use Multi-Factor Authentication with PRTG Hosted Monitor	79
<b>Part 4 Installing the Software</b>	<b>89</b>
4.1 Download PRTG	91
4.2 Update From Previous Versions	92
4.3 Install a PRTG Core Server	94
4.4 Install a Cluster	101
4.5 Enter a License Key	102
4.6 Activate the Product	104
4.7 Install a Remote Probe	106
4.8 Uninstall PRTG Products	119
<b>Part 5 Understanding Basic Concepts</b>	<b>122</b>
5.1 Architecture and User Interfaces	124
5.2 Failover Cluster	128
5.3 Object Hierarchy	132
5.4 Inheritance of Settings	136
5.5 Tags	138
5.6 Dependencies	140
5.7 Scheduling	141
5.8 Notifying	142
5.9 Access Rights Management	145
5.10 Data Reporting	149
5.11 IPv6 Support	150
<b>Part 6 Basic Procedures</b>	<b>151</b>
6.1 Login	153
6.2 Welcome Page	157
6.2.1 Customer Service	161

6.3	General Layout .....	164
6.4	Sensor States .....	181
6.5	Historic Data Reports .....	185
6.6	Similar Sensors .....	192
6.7	Recommended Sensors .....	197
6.8	Object Settings .....	201
6.9	Alarms .....	202
6.10	System Information .....	205
6.11	Logs .....	210
6.12	Tickets .....	213
6.13	Working with Table Lists .....	218
6.14	Object Selector .....	222
6.15	Priority and Favorites .....	224
6.16	Pause .....	227
6.17	Context Menus .....	229
6.18	Hover Popup .....	235
6.19	Main Menu Structure .....	237
<b>Part 7 Device and Sensor Setup .....</b>		<b>252</b>
7.1	Auto-Discovery .....	254
7.2	Create Objects Manually .....	257
7.2.1	Add an Auto-Discovery Group .....	258
7.2.2	Add a Group .....	313
7.2.3	Add a Device .....	363
7.2.4	Add a Sensor .....	414
7.3	Manage Device Tree .....	418
7.4	Root Group Settings .....	420
7.5	Probe Settings .....	458
7.6	Group Settings .....	526
7.7	Device Settings .....	597
7.8	Sensor Settings .....	667
7.8.1	Active Directory Replication Errors Sensor .....	669
7.8.2	ADO SQL v2 Sensor .....	675
7.8.3	Application Server Health (Autonomous) Sensor .....	688
7.8.4	AWS Alarm v2 Sensor .....	693
7.8.5	AWS Cost Sensor .....	699
7.8.6	AWS EBS v2 Sensor .....	707
7.8.7	AWS EC2 v2 Sensor .....	714
7.8.8	AWS ELB v2 Sensor .....	721
7.8.9	AWS RDS v2 Sensor .....	728
7.8.10	Beckhoff IPC System Health Sensor .....	735
7.8.11	Business Process Sensor .....	740
7.8.12	Cisco IP SLA Sensor .....	748
7.8.13	Cisco Meraki License Sensor .....	754
7.8.14	Cisco Meraki Network Health Sensor .....	759
7.8.15	Cisco WLC Access Point Overview Sensor (BETA) .....	765
7.8.16	Citrix XenServer Host Sensor .....	771
7.8.17	Citrix XenServer Virtual Machine Sensor .....	777
7.8.18	Cloud HTTP v2 Sensor .....	783
7.8.19	Cloud Ping v2 Sensor .....	792
7.8.20	Cluster Health Sensor .....	800
7.8.21	Common SaaS Sensor .....	804

7.8.22	Core Health Sensor .....	809
7.8.23	Core Health (Autonomous) Sensor .....	814
7.8.24	Dell EMC Unity Enclosure Health v2 Sensor .....	820
7.8.25	Dell EMC Unity File System v2 Sensor .....	826
7.8.26	Dell EMC Unity Storage Capacity v2 Sensor .....	831
7.8.27	Dell EMC Unity Storage LUN v2 Sensor .....	836
7.8.28	Dell EMC Unity Storage Pool v2 Sensor .....	841
7.8.29	Dell EMC Unity VMware Datastore v2 Sensor .....	847
7.8.30	Dell PowerVault MDi Logical Disk Sensor .....	852
7.8.31	Dell PowerVault MDi Physical Disk Sensor .....	857
7.8.32	DHCP Sensor .....	862
7.8.33	DICOM Bandwidth Sensor .....	869
7.8.34	DICOM C-ECHO Sensor .....	875
7.8.35	DICOM Query/Retrieve Sensor .....	881
7.8.36	DNS v2 Sensor .....	888
7.8.37	Docker Container Status Sensor .....	894
7.8.38	Enterprise Virtual Array Sensor .....	900
7.8.39	Event Log (Windows API) Sensor .....	905
7.8.40	Exchange Backup (PowerShell) Sensor .....	914
7.8.41	Exchange Database (PowerShell) Sensor .....	920
7.8.42	Exchange Database DAG (PowerShell) Sensor .....	926
7.8.43	Exchange Mail Queue (PowerShell) Sensor .....	933
7.8.44	Exchange Mailbox (PowerShell) Sensor .....	939
7.8.45	Exchange Public Folder (PowerShell) Sensor .....	945
7.8.46	EXE/Script Sensor .....	951
7.8.47	EXE/Script Advanced Sensor .....	961
7.8.48	File Sensor .....	970
7.8.49	File Content Sensor .....	976
7.8.50	Folder Sensor .....	983
7.8.51	FortiGate System Statistics Sensor .....	990
7.8.52	FortiGate VPN Overview Sensor .....	995
7.8.53	FTP Sensor .....	1000
7.8.54	FTP Server File Count Sensor .....	1006
7.8.55	HL7 Sensor .....	1013
7.8.56	HPE 3PAR Common Provisioning Group Sensor .....	1019
7.8.57	HPE 3PAR Drive Enclosure Sensor .....	1025
7.8.58	HPE 3PAR Virtual Volume Sensor .....	1031
7.8.59	HTTP Sensor .....	1037
7.8.60	HTTP v2 Sensor .....	1044
7.8.61	HTTP Advanced Sensor .....	1051
7.8.62	HTTP Apache ModStatus PerfStats Sensor .....	1064
7.8.63	HTTP Apache ModStatus Totals Sensor .....	1070
7.8.64	HTTP Content Sensor .....	1076
7.8.65	HTTP Data Advanced Sensor .....	1084
7.8.66	HTTP Full Web Page Sensor .....	1093
7.8.67	HTTP IoT Push Data Advanced Sensor .....	1101
7.8.68	HTTP Push Count Sensor .....	1108
7.8.69	HTTP Push Data Sensor .....	1114
7.8.70	HTTP Push Data Advanced Sensor .....	1122
7.8.71	HTTP Transaction Sensor .....	1130
7.8.72	HTTP XML/REST Value Sensor .....	1141
7.8.73	Hyper-V Cluster Shared Volume Disk Free Sensor .....	1152
7.8.74	Hyper-V Host Server Sensor .....	1158
7.8.75	Hyper-V Virtual Machine Sensor .....	1163
7.8.76	Hyper-V Virtual Network Adapter Sensor .....	1169

7.8.77	Hyper-V Virtual Storage Device Sensor .....	1175
7.8.78	IMAP Sensor .....	1181
7.8.79	IP on DNS Blacklist Sensor .....	1194
7.8.80	IPFIX Sensor .....	1199
7.8.81	IPFIX (Custom) Sensor .....	1208
7.8.82	IPMI System Health Sensor .....	1216
7.8.83	jFlow v5 Sensor .....	1221
7.8.84	jFlow v5 (Custom) Sensor .....	1231
7.8.85	LDAP Sensor .....	1240
7.8.86	Local Folder Sensor .....	1245
7.8.87	Microsoft 365 Mailbox Sensor .....	1252
7.8.88	Microsoft 365 Service Status Sensor .....	1262
7.8.89	Microsoft 365 Service Status Advanced Sensor .....	1267
7.8.90	Microsoft Azure SQL Database Sensor .....	1272
7.8.91	Microsoft Azure Storage Account Sensor .....	1279
7.8.92	Microsoft Azure Subscription Cost Sensor .....	1284
7.8.93	Microsoft Azure Virtual Machine Sensor .....	1290
7.8.94	Microsoft SQL v2 Sensor .....	1296
7.8.95	Modbus RTU Custom Sensor .....	1309
7.8.96	Modbus TCP Custom Sensor .....	1318
7.8.97	MQTT Round Trip Sensor .....	1326
7.8.98	MQTT Statistics Sensor .....	1331
7.8.99	MQTT Subscribe Custom Sensor .....	1336
7.8.100	Multi-Platform Probe Connection Health (Autonomous) Sensor .....	1343
7.8.101	Multi-Platform Probe Health Sensor .....	1347
7.8.102	MySQL v2 Sensor .....	1352
7.8.103	NetApp Aggregate Sensor .....	1365
7.8.104	NetApp Aggregate v2 Sensor .....	1372
7.8.105	NetApp I/O Sensor .....	1378
7.8.106	NetApp I/O v2 Sensor .....	1386
7.8.107	NetApp LIF Sensor .....	1392
7.8.108	NetApp LIF v2 Sensor .....	1399
7.8.109	NetApp LUN Sensor .....	1405
7.8.110	NetApp LUN v2 Sensor .....	1412
7.8.111	NetApp NIC Sensor .....	1418
7.8.112	NetApp NIC v2 Sensor .....	1425
7.8.113	NetApp Physical Disk Sensor .....	1431
7.8.114	NetApp Physical Disk v2 Sensor .....	1438
7.8.115	NetApp SnapMirror Sensor .....	1444
7.8.116	NetApp SnapMirror v2 Sensor .....	1451
7.8.117	NetApp System Health Sensor .....	1457
7.8.118	NetApp System Health v2 Sensor .....	1465
7.8.119	NetApp Volume Sensor .....	1472
7.8.120	NetApp Volume v2 Sensor .....	1479
7.8.121	NetFlow v5 Sensor .....	1486
7.8.122	NetFlow v5 (Custom) Sensor .....	1496
7.8.123	NetFlow v9 Sensor .....	1505
7.8.124	NetFlow v9 (Custom) Sensor .....	1515
7.8.125	Network Share Sensor .....	1524
7.8.126	OPC UA Certificate Sensor .....	1531
7.8.127	OPC UA Custom Sensor .....	1536
7.8.128	OPC UA Server Status Sensor .....	1542
7.8.129	Oracle SQL v2 Sensor .....	1547
7.8.130	Oracle Tablespace Sensor .....	1560
7.8.131	Packet Sniffer Sensor .....	1567

7.8.132	Packet Sniffer (Custom) Sensor .....	1575
7.8.133	PerfCounter Custom Sensor .....	1583
7.8.134	PerfCounter IIS Application Pool Sensor .....	1589
7.8.135	Ping Sensor .....	1594
7.8.136	Ping v2 Sensor .....	1600
7.8.137	Ping Jitter Sensor .....	1606
7.8.138	POP3 Sensor .....	1611
7.8.139	Port Sensor .....	1618
7.8.140	Port v2 Sensor (BETA) .....	1626
7.8.141	Port Range Sensor .....	1632
7.8.142	PostgreSQL Sensor .....	1637
7.8.143	Probe Health Sensor .....	1649
7.8.144	Python Script Advanced Sensor .....	1655
7.8.145	QoS (Quality of Service) One Way Sensor .....	1664
7.8.146	QoS (Quality of Service) Round Trip Sensor .....	1671
7.8.147	RADIUS v2 Sensor .....	1679
7.8.148	RDP (Remote Desktop) Sensor .....	1685
7.8.149	Redfish Power Supply Sensor .....	1689
7.8.150	Redfish System Health Sensor .....	1695
7.8.151	Redfish Virtual Disk Sensor .....	1702
7.8.152	REST Custom Sensor .....	1708
7.8.153	REST Custom v2 Sensor (BETA) .....	1728
7.8.154	Script v2 Sensor .....	1750
7.8.155	Sensor Factory Sensor .....	1757
7.8.156	sFlow Sensor .....	1770
7.8.157	sFlow (Custom) Sensor .....	1780
7.8.158	SFTP Secure File Transfer Protocol Sensor .....	1788
7.8.159	Share Disk Free Sensor .....	1794
7.8.160	SIP Options Ping Sensor .....	1798
7.8.161	SMTP Sensor .....	1803
7.8.162	SMTP&IMAP Round Trip Sensor .....	1810
7.8.163	SMTP&POP3 Round Trip Sensor .....	1820
7.8.164	SNMP APC Hardware Sensor .....	1829
7.8.165	SNMP Buffalo TS System Health Sensor .....	1834
7.8.166	SNMP Cisco ADSL Sensor .....	1839
7.8.167	SNMP Cisco ASA VPN Connections Sensor .....	1843
7.8.168	SNMP Cisco ASA VPN Traffic Sensor .....	1847
7.8.169	SNMP Cisco ASA VPN Users Sensor .....	1852
7.8.170	SNMP Cisco CBQoS Sensor .....	1856
7.8.171	SNMP Cisco System Health Sensor .....	1861
7.8.172	SNMP Cisco UCS Blade Sensor .....	1866
7.8.173	SNMP Cisco UCS Chassis Sensor .....	1871
7.8.174	SNMP Cisco UCS Physical Disk Sensor .....	1876
7.8.175	SNMP Cisco UCS System Health Sensor .....	1880
7.8.176	SNMP CPU Load Sensor .....	1886
7.8.177	SNMP Custom Sensor .....	1890
7.8.178	SNMP Custom Advanced Sensor .....	1896
7.8.179	SNMP Custom String Sensor .....	1902
7.8.180	SNMP Custom String Lookup Sensor .....	1911
7.8.181	SNMP Custom Table Sensor .....	1917
7.8.182	SNMP Custom v2 Sensor (BETA) .....	1924
7.8.183	SNMP Dell EqualLogic Logical Disk Sensor .....	1930
7.8.184	SNMP Dell EqualLogic Member Health Sensor .....	1935
7.8.185	SNMP Dell EqualLogic Physical Disk Sensor .....	1941
7.8.186	SNMP Dell Hardware Sensor .....	1946

7.8.187	SNMP Dell PowerEdge Physical Disk Sensor .....	1951
7.8.188	SNMP Dell PowerEdge System Health Sensor .....	1956
7.8.189	SNMP Disk Free Sensor .....	1963
7.8.190	SNMP Disk Free v2 Sensor (BETA) .....	1967
7.8.191	SNMP Fujitsu System Health v2 Sensor .....	1972
7.8.192	SNMP Hardware Status Sensor .....	1978
7.8.193	SNMP HP LaserJet Hardware Sensor .....	1982
7.8.194	SNMP HPE BladeSystem Blade Sensor .....	1987
7.8.195	SNMP HPE BladeSystem Enclosure System Health Sensor .....	1991
7.8.196	SNMP HPE ProLiant Logical Disk Sensor .....	1995
7.8.197	SNMP HPE ProLiant Memory Controller Sensor .....	2000
7.8.198	SNMP HPE ProLiant Network Interface Sensor .....	2006
7.8.199	SNMP HPE ProLiant Physical Disk Sensor .....	2011
7.8.200	SNMP HPE ProLiant System Health Sensor .....	2017
7.8.201	SNMP IBM System X Logical Disk Sensor .....	2024
7.8.202	SNMP IBM System X Physical Disk Sensor .....	2028
7.8.203	SNMP IBM System X Physical Memory Sensor .....	2032
7.8.204	SNMP IBM System X System Health Sensor .....	2037
7.8.205	SNMP interSeptor Pro Environment Sensor .....	2042
7.8.206	SNMP Juniper NS System Health Sensor .....	2046
7.8.207	SNMP LenovoEMC Physical Disk Sensor .....	2050
7.8.208	SNMP LenovoEMC System Health Sensor .....	2054
7.8.209	SNMP Library Sensor .....	2058
7.8.210	SNMP Linux Disk Free Sensor .....	2066
7.8.211	SNMP Linux Load Average Sensor .....	2074
7.8.212	SNMP Linux Meminfo Sensor .....	2078
7.8.213	SNMP Linux Physical Disk Sensor .....	2083
7.8.214	SNMP Memory Sensor .....	2087
7.8.215	SNMP NetApp Disk Free Sensor .....	2091
7.8.216	SNMP NetApp Enclosure Sensor .....	2096
7.8.217	SNMP NetApp I/O Sensor .....	2101
7.8.218	SNMP NetApp License Sensor .....	2105
7.8.219	SNMP NetApp Logical Unit Sensor .....	2109
7.8.220	SNMP NetApp Network Interface Sensor .....	2114
7.8.221	SNMP NetApp System Health Sensor .....	2118
7.8.222	SNMP Nutanix Cluster Health Sensor .....	2123
7.8.223	SNMP Nutanix Hypervisor Sensor .....	2128
7.8.224	SNMP Poseidon Environment Sensor .....	2134
7.8.225	SNMP Printer Sensor .....	2138
7.8.226	SNMP QNAP Logical Disk Sensor .....	2143
7.8.227	SNMP QNAP Physical Disk Sensor .....	2147
7.8.228	SNMP QNAP System Health Sensor .....	2152
7.8.229	SNMP Rittal CMC III Hardware Status Sensor .....	2156
7.8.230	SNMP RMON Sensor .....	2160
7.8.231	SNMP SonicWall System Health Sensor .....	2165
7.8.232	SNMP SonicWall VPN Traffic Sensor .....	2169
7.8.233	SNMP Synology Logical Disk Sensor .....	2174
7.8.234	SNMP Synology Physical Disk Sensor .....	2178
7.8.235	SNMP Synology System Health Sensor .....	2182
7.8.236	SNMP System Uptime Sensor .....	2187
7.8.237	SNMP Traffic Sensor .....	2191
7.8.238	SNMP Traffic v2 Sensor (BETA) .....	2198
7.8.239	SNMP Trap Receiver Sensor .....	2207
7.8.240	SNMP Uptime v2 Sensor .....	2217
7.8.241	SNMP Windows Service Sensor .....	2222

7.8.242	SNTP Sensor .....	2226
7.8.243	Soffico Orchestra Channel Health Sensor .....	2230
7.8.244	Soffico Orchestra Scenario Sensor .....	2235
7.8.245	SSH Disk Free Sensor .....	2240
7.8.246	SSH INodes Free Sensor .....	2250
7.8.247	SSH Load Average Sensor .....	2256
7.8.248	SSH Meminfo Sensor .....	2262
7.8.249	SSH Remote Ping Sensor .....	2268
7.8.250	SSH SAN Enclosure Sensor .....	2275
7.8.251	SSH SAN Logical Disk Sensor .....	2282
7.8.252	SSH SAN Physical Disk Sensor .....	2289
7.8.253	SSH SAN System Health Sensor .....	2296
7.8.254	SSH Script Sensor .....	2304
7.8.255	SSH Script Advanced Sensor .....	2314
7.8.256	SSL Certificate Sensor .....	2323
7.8.257	SSL Security Check Sensor .....	2331
7.8.258	Syslog Receiver Sensor .....	2337
7.8.259	System Health Sensor .....	2346
7.8.260	System Health v2 Sensor .....	2350
7.8.261	TFTP Sensor .....	2355
7.8.262	Traceroute Hop Count Sensor .....	2359
7.8.263	Veeam Backup Job Status Sensor .....	2364
7.8.264	Veeam Backup Job Status Advanced Sensor .....	2369
7.8.265	VMware Datastore (SOAP) Sensor .....	2375
7.8.266	VMware Host Hardware (WBEM) Sensor .....	2381
7.8.267	VMware Host Hardware Status (SOAP) Sensor .....	2386
7.8.268	VMware Host Performance (SOAP) Sensor .....	2392
7.8.269	VMware Virtual Machine (SOAP) Sensor .....	2398
7.8.270	Windows CPU Load Sensor .....	2404
7.8.271	Windows IIS Application Sensor .....	2409
7.8.272	Windows MSMQ Queue Length Sensor .....	2414
7.8.273	Windows Network Card Sensor .....	2420
7.8.274	Windows Pagefile Sensor .....	2427
7.8.275	Windows Physical Disk I/O Sensor .....	2432
7.8.276	Windows Print Queue Sensor .....	2439
7.8.277	Windows Process Sensor .....	2448
7.8.278	Windows SMTP Service Received Sensor .....	2454
7.8.279	Windows SMTP Service Sent Sensor .....	2459
7.8.280	Windows System Uptime Sensor .....	2464
7.8.281	Windows Updates Status (PowerShell) Sensor .....	2469
7.8.282	WMI Battery Sensor .....	2477
7.8.283	WMI Custom Sensor .....	2482
7.8.284	WMI Custom String Sensor .....	2488
7.8.285	WMI Disk Health Sensor .....	2496
7.8.286	WMI Event Log Sensor .....	2501
7.8.287	WMI Exchange Server Sensor .....	2510
7.8.288	WMI Exchange Transport Queue Sensor .....	2515
7.8.289	WMI File Sensor .....	2522
7.8.290	WMI Free Disk Space (Multi Disk) Sensor .....	2527
7.8.291	WMI HDD Health Sensor .....	2535
7.8.292	WMI Logical Disk I/O Sensor .....	2542
7.8.293	WMI Memory Sensor .....	2548
7.8.294	WMI Microsoft SQL Server 2005 Sensor (Deprecated) .....	2553
7.8.295	WMI Microsoft SQL Server 2008 Sensor .....	2561
7.8.296	WMI Microsoft SQL Server 2012 Sensor .....	2568

7.8.297	WMI Microsoft SQL Server 2014 Sensor .....	2575
7.8.298	WMI Microsoft SQL Server 2016 Sensor .....	2582
7.8.299	WMI Microsoft SQL Server 2017 Sensor .....	2589
7.8.300	WMI Microsoft SQL Server 2019 Sensor .....	2596
7.8.301	WMI Remote Ping Sensor .....	2603
7.8.302	WMI Security Center Sensor .....	2608
7.8.303	WMI Service Sensor .....	2613
7.8.304	WMI Share Sensor .....	2619
7.8.305	WMI SharePoint Process Sensor .....	2626
7.8.306	WMI Storage Pool Sensor .....	2631
7.8.307	WMI Terminal Services (Windows 2008+) Sensor .....	2636
7.8.308	WMI Terminal Services (Windows XP/Vista/2003) Sensor .....	2641
7.8.309	WMI UTC Time Sensor .....	2646
7.8.310	WMI Vital System Data v2 Sensor .....	2650
7.8.311	WMI Volume Sensor .....	2656
7.8.312	WSUS Statistics Sensor .....	2661
7.8.313	Zoom Service Status Sensor .....	2668
7.9	Additional Sensor Types (Custom Sensors) .....	2676
7.10	Channel Settings .....	2681
7.11	Notification Triggers Settings .....	2693
<b>Part 8 Advanced Procedures .....</b>		<b>2705</b>
8.1	Toplists .....	2707
8.2	Move Objects .....	2712
8.3	Clone Object .....	2714
8.4	Multi-Edit .....	2718
8.5	Create Device Template .....	2725
8.6	Show Dependencies .....	2728
8.7	Geo Maps .....	2731
8.8	Notifications .....	2735
8.9	Libraries .....	2738
8.9.1	Library Management .....	2741
8.9.2	Libraries and Node Settings .....	2744
8.9.3	Library Context Menus .....	2751
8.10	Reports .....	2754
8.10.1	Run Reports .....	2759
8.10.2	Report Settings .....	2764
8.11	Maps .....	2776
8.11.1	Map Designer .....	2780
8.11.2	Maps Settings .....	2792
8.11.3	Map Rotation .....	2797
8.12	Setup .....	2799
8.12.1	Account Settings .....	2801
8.12.1.1	My Account .....	2801
8.12.1.2	Notification Templates .....	2808
8.12.1.3	Notification Contacts .....	2842
8.12.1.4	Schedules .....	2846
8.12.1.5	API Keys .....	2851
8.12.2	System Administration .....	2855
8.12.2.1	User Interface .....	2855
8.12.2.2	Monitoring .....	2869
8.12.2.3	Notification Delivery .....	2877
8.12.2.4	Core & Probes .....	2887
8.12.2.5	User Accounts .....	2901



8.12.2.6	User Groups .....	2912
8.12.2.7	Administrative Tools .....	2918
8.12.2.8	Cluster .....	2923
8.12.2.9	Single Sign-On .....	2925
8.12.2.10	Maintainer Mode .....	2931
8.12.3	PRTG Status .....	2935
8.12.3.1	System Status .....	2935
8.12.3.2	Cluster Status .....	2960
8.12.4	License Information .....	2962
8.12.5	Auto-Update .....	2969
8.12.6	Optional Downloads .....	2974
8.12.7	Help and Support Center .....	2976
8.12.8	Contact Support .....	2977
<b>Part 9 PRTG MultiBoard .....</b>		<b>2983</b>
<b>Part 10 PRTG Apps for Mobile Network Monitoring .....</b>		<b>2987</b>
<b>Part 11 Desktop Notifications .....</b>		<b>2992</b>
<b>Part 12 Sensor Technologies .....</b>		<b>2995</b>
12.1	Monitoring via SNMP .....	2997
12.2	Monitoring via WMI .....	3004
12.3	Monitoring via SSH .....	3007
12.4	Monitoring Bandwidth via Packet Sniffing .....	3009
12.5	Monitoring Bandwidth via Flows .....	3011
12.6	Bandwidth Monitoring Comparison .....	3014
12.7	Monitoring Quality of Service .....	3016
12.8	Monitoring Backups .....	3021
12.9	Monitoring Virtual Environments .....	3022
12.10	Monitoring Databases .....	3028
12.11	Monitoring via HTTP .....	3032
<b>Part 13 PRTG Administration Tool .....</b>		<b>3039</b>
13.1	PRTG Administration Tool on PRTG Core Server Systems .....	3041
13.2	PRTG Administration Tool on Remote Probe Systems .....	3067
<b>Part 14 Advanced Topics .....</b>		<b>3079</b>
14.1	Active Directory Integration .....	3081
14.2	Application Programming Interface (API) Definition .....	3084
14.2.1	HTTP API .....	3085
14.2.2	Live Data .....	3088
14.2.2.1	Single Object Property .....	3089
14.2.2.2	Single Object Status .....	3092
14.2.2.3	Multiple Object Property or Status .....	3099
14.2.2.4	System Information .....	3120
14.2.3	Live Graphs .....	3124
14.2.4	Historic Data .....	3127
14.2.5	Object Manipulation .....	3130
14.2.6	Custom Sensors .....	3137
14.2.7	Custom Notifications .....	3151
14.2.8	Mini Probe API .....	3153
14.3	Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors .....	3173

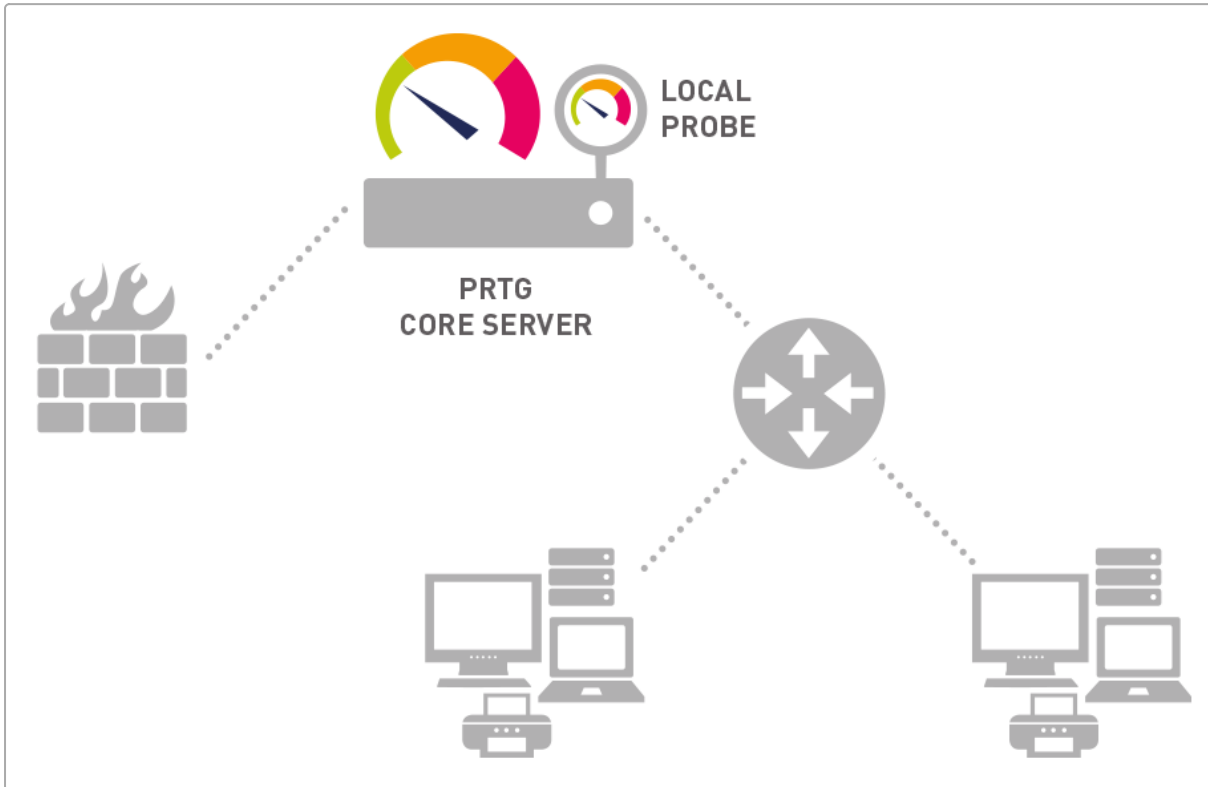
14.4	Channel Definitions for Flow, IPFIX, and Packet Sniffer Sensors .....	3178
14.5	Define IP Address Ranges .....	3180
14.6	Define Lookups .....	3181
14.7	Regular Expressions .....	3193
14.8	Calculating Percentiles .....	3195
14.9	Add Remote Probe .....	3196
14.9.1	Remote Probes and Multiple Probes .....	3198
14.9.2	Classic Remote Probe Setup via Device Tools .....	3202
14.10	Failover Cluster Configuration .....	3208
14.11	Data Storage .....	3213
<b>Part 15</b>	<b>Appendix .....</b>	<b>3219</b>
15.1	Abbreviations .....	3221
15.2	Available Sensor Types .....	3232
15.3	Default Ports .....	3288
15.4	Differences between PRTG Network Monitor and PRTG Hosted Monitor .....	3293
15.5	Escape Special Characters and Whitespaces in Parameters .....	3312
15.6	Glossary .....	3313
15.7	Icons .....	3322
15.8	Legal Notices .....	3323
15.9	Placeholders for Notifications .....	3325
15.10	Standard Lookup Files .....	3335
15.11	Supported AWS Regions and Their Codes .....	3350

# Part 1

# Welcome to PRTG

# 1 Welcome to PRTG

Welcome to PRTG. You have chosen a software product that comes with a comprehensive set of features to monitor your entire network.



A Standard Installation of PRTG

## Monitoring Networks with PRTG

PRTG is a comprehensive network monitoring application for Windows-based systems. It is suitable for networks of all sizes and capable of LAN, WAN, WLAN, and VPN monitoring. You can also monitor physical or virtual web, mail, and file servers, Linux systems, Windows clients, routers, and much more.

PRTG monitors network availability and bandwidth usage, as well as various other network parameters such as quality of service, memory load, and CPU usage, even on remote machines. PRTG provides system administrators with live readings and periodical usage trends to optimize the efficiency, layout, and setup of leased lines, routers, firewalls, servers, and other network components.

The software monitors a network that uses Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), packet sniffer, Cisco NetFlow, IPFIX, sFlow, jFlow, and many other industry standard protocols. It runs on a Windows-based machine in your network for 24 hours a day. PRTG constantly records the network usage parameters and the availability of network systems. The recorded data is stored in an internal database for later analysis.

## 1.1 About this Document

This document introduces you to PRTG Network Monitor and Paessler PRTG Enterprise Monitor, both from now on referred to as **PRTG**. Everything you need to know to use PRTG or PRTG Hosted Monitor is in this document:

- Plan monitoring results
- Achieve the best monitoring results
- Use a cluster for fail-safe monitoring
- Set up devices, sensors, dependencies, and much more

This document is also a reference for all settings in PRTG. While there is short contextual help in the PRTG web interface, this document provides more comprehensive information about available options. Whenever possible, links to more detailed resources are provided, such as articles in our [Knowledge Base](#).

This document does not give an in-depth explanation of monitoring protocols and file formats. It also only briefly addresses the use of the application programming interface (API) built into PRTG.

- To use PRTG right away, see section [Quick Start Guide](#) <sup>38</sup>.
  - To learn more about monitoring with PRTG, see section [Introduction: Monitoring with PRTG](#) <sup>33</sup>.
  - For more information, browse the manual content or use the manual search with keywords and choose the section that you want to read.
- For an overview of the icons and abbreviations that are used in this document, see section [Appendix](#) <sup>3220</sup>.

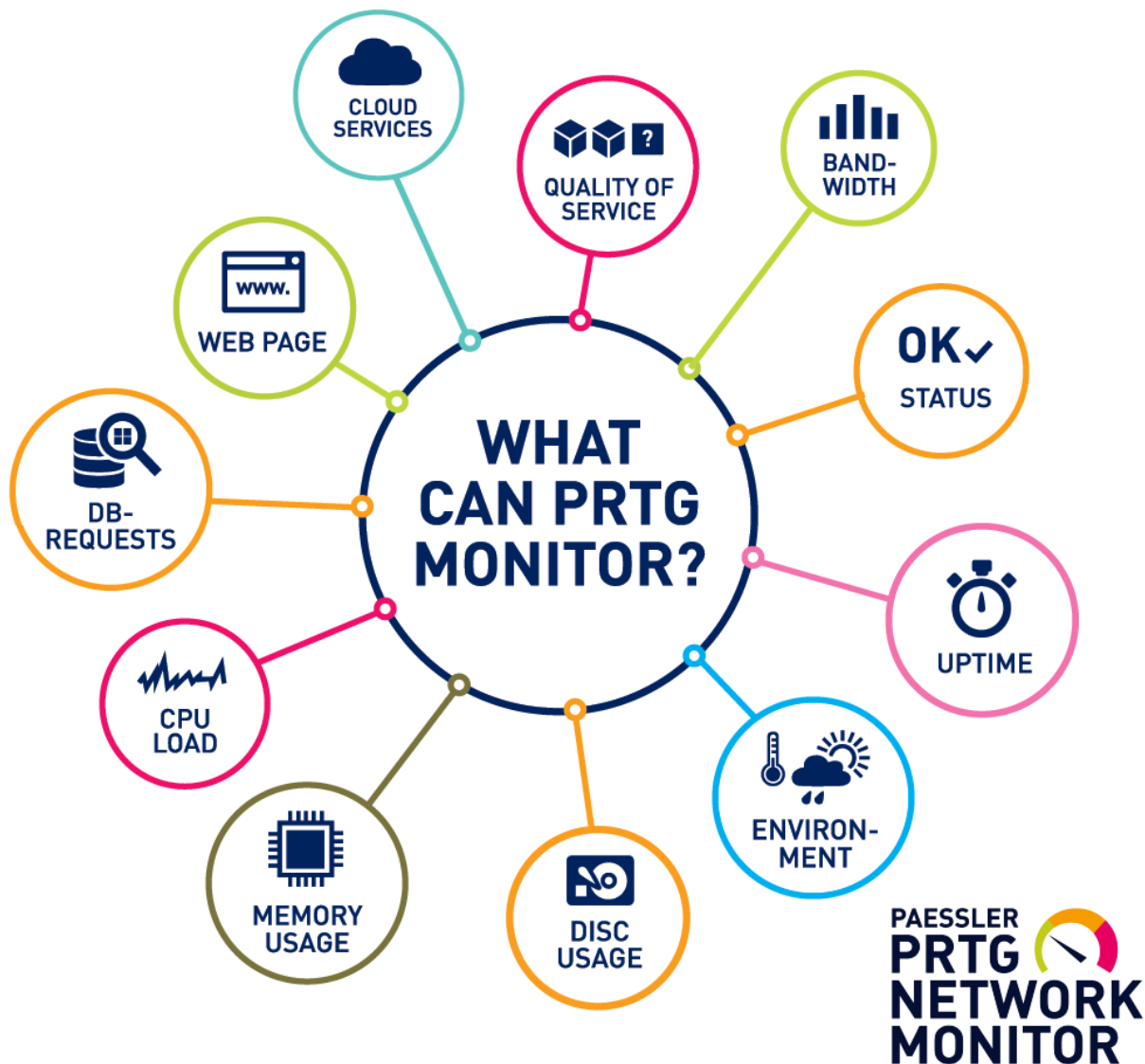
## 1.2 Key Features

PRTG offers two options to monitor your network: PRTG Network Monitor and PRTG Hosted Monitor.

- PRTG Network Monitor: The PRTG core server and local probe run in your network.
- PRTG Hosted Monitor: Paessler runs the PRTG core server and hosted probe for you in the cloud.

**i** The PRTG web interface is the same for both PRTG Hosted Monitor and PRTG Network Monitor.

### Areas of Application



PRTG can monitor:

- Uptimes, downtimes, and slow servers
- System health of hardware devices
- Network devices and bandwidth

- Applications
- Virtual servers
- Service level agreements (SLA)
- System usage (for example CPU load, free memory, and free disk space)
- Database performance and table values
- Email servers
- Physical network environments
- Cloud services


It can also:

- Classify network traffic and content by source or destination
- Measure Quality of Service (QoS) and Voice over IP (VoIP) parameters
- Collect system information for hardware
- Detect unusual activity between network components and warns about potential security issues
- Detect unusual behavior by devices or users
- Assess the real usage of network and hardware
- Fail-safe monitor a cluster

## Key Features

- High performance: The database system stores raw monitoring results as well as logs, Toplists, and tickets. This outperforms Structured Query Language (SQL) servers for monitoring data. You can distribute high loads among several probes and also access the database through the PRTG API.
- Low [system requirements](#)<sup>[22]</sup>: To run PRTG Network Monitor, an average PC that is not older than 2 years is enough. Even a netbook can monitor more than a thousand sensors.

 PRTG Hosted Monitor requires no hardware for the PRTG core server.

- High security standards: Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connections and web servers, secure ciphers, personalized user rights management, and much more.  For more information, see the Knowledge Base: [What security features does PRTG include?](#)
- SSL/TLS-secured web server with HTTP and HTTPS support for the PRTG web interface. This acts as a Single Page Application (SPA) to avoid time-intensive page reloading.
- Email relay server for automatic email delivery.
- Customizable alerts for specific needs:
  - Various notification methods: email, push, SMS text messages, Syslog messages and Simple Network Management Protocol (SNMP) traps, HTTP requests, event logs, Amazon Simple Notification Service (SNS), executing scripts.
  - Multiple ways to trigger notifications: status alerts, limit alerts, threshold alerts, multiple condition alerts, escalation alerts.
  - Gradual dependencies to avoid alarm floods, acknowledging certain alarms to avoid further notifications, and alert scheduling.

- In-depth report generator to create reports on demand or scheduled reports in HTML, as .pdf, .csv, or .xml. Several report templates are available by default.
- Graphics engine for user-friendly live graphs and historic data graphs.
- Network analysis modules to automatically find network devices and sensors.
- Distributed monitoring to monitor several networks in different locations.
- Special features for managed service providers (MSP) to monitor customer networks and increase the quality of service.
- Data publishing with real-time [dashboards](#), including live performance and status information. Design these dashboards with many different objects and integrate external objects as well.
- Multiple languages: English, German, Spanish, French, Portuguese, Dutch, Japanese, Russian, and Simplified Chinese.
- Customization: The PRTG API lets you develop your own features. Additionally, you can create custom sensors, notifications, and device templates according to your specific needs.

PRTG supports monitoring for up to several thousand sensors per installation, depending on various parameters. It can also work with remote probes to distribute high monitoring loads, to monitor multiple sites or network segments from one central core installation, and to monitor non-Windows systems. It is also possible to configure fail-safe monitoring with a cluster to perform automatic failovers.

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>




## 1.3 New in this Version

The continuous development and rollout of PRTG constantly expands its functionalities. Instead of delivering only a few versions with massive changes in every update each year, PRTG is automatically and consistently improved with new features and fixes.

PRTG Network Monitor has three release channels:

- **Stable:** Best tested version for live systems. It is updated about once every 8 weeks. Use it on live systems.
- **Preview:** Offers the latest features and fixes and is updated twice between stable releases. Consider this version a "beta", so do not use this version on live systems that you depend on.
- **Canary:** Provides nightly builds and is updated very often. It is not extensively tested. Never use it on live systems that you depend on.

With the release channels, you can choose from maximum stability, early access to new features, or a mix of both.

 PRTG Hosted Monitor does not have release channels. Instead, we roll out the latest Stable version to PRTG Hosted Monitor instances in stages.

 For an overview of all changes in the different versions, see the Paessler website: [Release notes for the "stable" release channel](#)

### More

 PAESSLER WEBSITE

Release notes for the "stable" release channel

- <https://www.paessler.com/prtg/history/stable>



PRTG version history

- <https://www.paessler.com/prtg/history>

## 1.4 Available Licenses

PRTG licenses count by [sensors](#)<sup>[134]</sup>. Three different license editions are available.

Edition	Description
Trial edition	<p>The trial edition is intended for evaluation purposes:</p> <ul style="list-style-type: none"> <li>▪ Allows you to use an unlimited number of sensors.</li> <li>▪ Supports all available sensors.</li> <li>▪ For PRTG Network Monitor, you must request a trial license key. Click the Free Trial button on the <a href="#">Paessler website</a> to see the license details and the key.</li> <li>▪ The trial edition of PRTG Network Monitor is limited to 30 days and automatically turns into a freeware edition afterward.</li> </ul> <p>☁ PRTG Hosted Monitor provides a 10-day trial. Afterward, your instance is deleted. Upgrade to a commercial edition to keep your instance.</p> <p>ⓘ Each PRTG Network Monitor license includes one single failover <a href="#">cluster</a><sup>[128]</sup> that consists of two cluster nodes. A cluster with two or three failover nodes requires an additional license key. A cluster with four failover nodes requires two additional license keys.</p> <p>ⓘ After the trial period, the PRTG Network Monitor trial edition automatically turns into a freeware edition that lets you use up to 100 sensors for free.</p>
Freeware edition	<p>The freeware edition is a good solution for starters or for private use:</p> <ul style="list-style-type: none"> <li>▪ Free for personal and commercial use.</li> <li>▪ Allows you to use up to 100 sensors.</li> <li>▪ Supports all available sensors.</li> </ul> <p>ⓘ If you want to use the freeware edition, install the trial edition first and get a trial license key. After the trial period, the trial edition automatically turns into a freeware edition that lets you use up to 100 sensors for free.</p> <p>☁ The freeware edition is not available in PRTG Hosted Monitor.</p>
Commercial edition	<p>There are several types of commercial edition available that suit the demands of smaller as well as larger customers and organizations:</p> <ul style="list-style-type: none"> <li>▪ Allows you to use a maximum number of sensors (consider our <a href="#">recommendations</a><sup>[27]</sup>).</li> <li>▪ Supports all available sensors.</li> </ul>

Edition	Description
	<p> Each PRTG Network Monitor license includes one single failover <a href="#">cluster</a><sup>128</sup> that consists of two cluster nodes. A cluster with two or three failover nodes requires an additional license key. A cluster with four failover nodes requires two additional license keys.</p> <p> For more information about available commercial edition subscription licenses, see the Paessler Portal: <a href="#">PRTG Network Monitor licenses &amp; pricing</a>.</p>

## More

 **PAESSLER WEBSITE**

Download PRTG and get a trial license key

- <https://www.paessler.com/prtg/download>

 **PAESSLER PORTAL**



















PRTG Network Monitor licenses & pricing

- <https://shop.paessler.com/>

## 1.5 System Requirements


There are different aspects that you need to consider regarding the system requirements for PRTG. Meet these requirements to avoid issues while you monitor your network.



In this section:

- [Basic System Requirements](#) 
  - [Requirements for the PRTG Core Server](#) 
  - [Requirements for Remote Probes](#) 
  - [General Performance Impact Considerations](#) 
  - [Running PRTG in Virtual Environments](#) 
  - [Running PRTG in a Cluster](#) 
  - [Large PRTG Installations](#) 
- [Detailed System Requirements](#) 
  - [Supported Operating Systems for the PRTG Core Server and Remote Probes](#) 
  - [Hardware and Network Size Requirements for the PRTG Core Server](#) 
  - [Hardware and Network Size Requirements for Classic Remote Probes](#) 
  - [Hardware and Network Size Requirements for Multi-Platform Probes](#) 
  - [Performance Impact Considerations Based on Sensor Types](#) 
  - [Supported Web Browsers](#) 
- [Further System Requirements](#) 
  - [Screen Resolution](#) 
  - [Requirements for Monitored Devices](#) 
  - [Requirements for Smartphones and Tablets](#) 

### Basic System Requirements

PRTG consists of two main [system parts](#) : PRTG core server and probes.

- If you want to use PRTG Network Monitor, you need to install PRTG on a system that meets the [basic system requirements for the PRTG core server](#) .

 If you want to use PRTG Hosted Monitor, you need to install at least one remote probe on a system that meets the [basic system requirements for remote probes](#) .

### Requirements for the PRTG Core Server

 For more information, see the [hardware and network size requirements](#)  for the PRTG core server.

For installations of the [PRTG core server](#) , you need to meet the following requirements.

Category	Requirements
Hardware	We recommend that you use x64 server hardware or a properly configured <a href="#">virtual environment</a> <sup>[25]</sup> .
Operating system	We recommend that you use Microsoft Windows Server 2022, Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows 11, or Microsoft Windows 10.
Microsoft .NET Framework	It is required that <a href="#">.NET 4.7.2 or later</a> of the Microsoft .NET Framework is installed on the PRTG core server system or the remote probe system. For new installations of the PRTG core server or classic remote probes, we recommend .NET Framework <a href="#">4.8</a> .  ■ For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a>
Web browser	The following browsers are officially supported by the PRTG web interface: <ul style="list-style-type: none"> <li>▪ Google Chrome 75</li> <li>▪ Mozilla Firefox 67</li> <li>▪ Microsoft Edge 79</li> <li>▪ Safari 11 or iOS (Safari) 11</li> </ul> <p>ⓘ For security and performance reasons, we strongly recommend that you always use the latest version of Google Chrome to access the PRTG web interface.</p>



☁ PRTG Hosted Monitor does not require any hardware for the PRTG core server, but it needs at least one remote probe installation to monitor your local network.

## Requirements for Remote Probes

■ For more information, see the [hardware and network size requirements](#)<sup>[28]</sup> for remote probes.




For installations of [classic remote probes](#)<sup>[3198]</sup>, you need to meet the following requirements:

Category	Requirement
Hardware	We recommend that you use compatible x86 hardware or a properly configured <a href="#">virtual environment</a> <sup>[25]</sup> .
Operating system	We recommend that you use Microsoft Windows Server 2022, Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows 11, or Microsoft Windows 10.

Category	Requirement
Microsoft .NET Framework	<p>It is required that <a href="#">.NET 4.7.2 or later</a> of the Microsoft .NET Framework is installed on the PRTG core server system or the remote probe system. For new installations of the PRTG core server or classic remote probes, we recommend .NET Framework <a href="#">4.8</a>.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Stable network connection	<p>Remote probes require a stable network connection between the PRTG core server and the remote probe.</p> <p> Remote probes that connect to a PRTG Hosted Monitor instance need a reliable internet connection. Unstable connections, for example via 3G, might work but you might lose monitoring data if the connection is unreliable.</p>

 For more information on system requirements for the multi-platform probe, see the see the [Multi-Platform Probe for PRTG](#) manual.

### General Performance Impact Considerations

Category	Performance Impact Considerations
Hardware resources	<p>For a PRTG core server to work properly, it is crucial to have a certain amount of hardware resources available. If the server runs out of resources, PRTG sends warning and emergency messages to the primary email address of the <a href="#">PRTG System Administrator</a> user.</p> <p> You receive warning messages if the available disk space falls below <a href="#">1 GB</a> or if the available memory falls below <a href="#">500 MB</a>, and emergency messages if the available disk space or memory fall below <a href="#">50 MB</a>. In this case, react immediately and free up system resources.</p>
Sensors	<p>Ping and SNMP sensors create much less load than complex sensors like flow sensors, VMware sensors, Sensor Factory sensors, WMI sensors. or Syslog Receiver or SNMP Trap Receiver sensors, for example.</p> <p> There are also limitations for some sensors that do not depend on hardware resources, for example, WMI and SNMP v3 sensors. You can overcome these limitations if you distribute the sensors between remote probes.</p> <p> For clusters, we recommend that you stay below 2,500 sensors per cluster.</p>

Category	Performance Impact Considerations
Channels	We recommend that you use sensors with less than <b>50</b> channels. Note that sensors with more than 50 channels are not officially supported. PRTG will try to display all channels but it will limit usability and have a high impact on system performance.
Scanning interval	For a single PRTG core server setup without a cluster, we recommend that you mainly use 1-minute scanning intervals for up to 2,000 sensors and 5-minute intervals if you have more sensors.  <b>i</b> To give you an impression: To monitor 5,000 sensors with a 1-minute scanning interval, PRTG takes 7.2 million measurements and evaluates, notifies, and stores them. This adds 700 MB of additional data to the database every single day.
CPU-intensive features	Try to limit the use of the following features: <ul style="list-style-type: none"> <li>▪ Many quickly refreshed <a href="#">maps</a> <sup>[2776]</sup></li> <li>▪ Frequent generation of huge <a href="#">reports</a> <sup>[2754]</sup></li> <li>▪ Heavy usage of <a href="#">packet sniffing</a> <sup>[3009]</sup>, Sensor Factory sensors, and <a href="#">Toplists</a> <sup>[2707]</sup></li> <li>▪ Frequent automatically scheduled <a href="#">auto-discoveries</a> <sup>[254]</sup> for large network segments</li> <li>▪ Constant queries of monitoring data via the <a href="#">PRTG API</a> <sup>[3084]</sup></li> </ul>
Network connection quality	The quality of your network also plays an important role. When you monitor via User Datagram Protocol (UDP), for example, a high packet loss rate can lead to frequent timeouts. Remote probes that connect via unstable (WAN) connections can lead to delays as well.

## Running PRTG in Virtual Environments

You can run the PRTG core server and remote probes on virtualized platforms. However, PRTG consists of a lot of different components that all rely on the performance and the stability of the probe system where virtual environments add even more layers of complexity. This needs to be considered when you want to set up your PRTG installation in a way that you can achieve the same level of performance as on a physical server.

Most PRTG installations from 500 to 5,000 sensors do not need any specific optimization regarding your virtual infrastructure.

If you run larger installations of PRTG with more than 5,000 sensors, we strongly recommend that you follow the instructions in our [Best Practice Guide: Running large installations of PRTG in a virtual environment](#).

**i** Particularly for virtual systems, make sure that you have a unique Windows security identifier [per system](#).

## Running PRTG in a Cluster

We recommend a single [failover cluster](#)<sup>128</sup> for fail-safe monitoring. This consists of two PRTG core servers that each work as a cluster node.

In a cluster, the monitoring load doubles with each cluster node, so the performance of each additional cluster node is halved. Therefore, in a single failover cluster, divide our recommended numbers from earlier in the section in half.

☁ This feature is not available in PRTG Hosted Monitor.

## Large PRTG Installations

The maximum number of sensors you can monitor with one PRTG Network Monitor installation mainly depends on the monitoring technology and the scanning intervals you use. In general, we recommend that you use a dedicated physical machine to run both the PRTG core server and remote probes. [Running large installations of PRTG in a virtual environment](#) is possible if you follow some specific rules and guidelines to achieve the required level of performance.

■ For more information, see section [Detailed System Requirements](#)<sup>26</sup>.

■ For more information, see the Knowledge Base: [How can I speed up PRTG—especially for large installations?](#)

☁ PRTG Hosted Monitor is restricted to a maximum of 10,000 sensors. More sensors are not possible.

## Detailed System Requirements

### Supported Operating Systems for the PRTG Core Server and Remote Probes

Category	Requirements
Supported operating systems	<p>The 32-bit and 64-bit versions of the following operating systems are officially supported for the PRTG core server service and PRTG probe service:</p> <ul style="list-style-type: none"> <li>▪ Microsoft Windows Server 2022*</li> <li>▪ Microsoft Windows Server 2019*</li> <li>▪ Microsoft Windows Server 2016*</li> <li>▪ Microsoft Windows 11</li> <li>▪ Microsoft Windows 10</li> </ul> <p>* Windows servers in <a href="#">Core</a> mode or <a href="#">Minimal Server Interface</a> are not officially supported.</p>



Category	Requirements
Operating system version	The version (32-bit or 64-bit) of the PRTG core server depends on the version of your operating system.
Microsoft .NET Framework	<p>It is required that <a href="#">.NET 4.7.2 or later</a> of the Microsoft .NET Framework is installed on the PRTG core server system or the remote probe system. For new installations of the PRTG core server or classic remote probes, we recommend .NET Framework <a href="#">4.8</a>.</p> <ul style="list-style-type: none"> <li><span style="color: #0070C0;">■</span> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></li> <li><span style="color: #0070C0;">ⓘ</span> The .NET framework is imperative if you want to monitor VMware and XenServer virtual environments. Many other sensors also need an installed Microsoft .NET Framework.</li> </ul>
Disabled FIPS mode	<p>Make sure that the Federal Information Processing Standards (FIPS) mode (Windows security option "System Cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing.") is disabled on Windows systems that run the PRTG core server service or PRTG probe service. FIPS-compliant encryption can cause issues with sensors that use the .NET framework.</p> <ul style="list-style-type: none"> <li><span style="color: #0070C0;">■</span> For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></li> </ul>

☁ PRTG Hosted Monitor is restricted to a maximum of 10,000 sensors. More sensors are not possible.

## Hardware and Network Size Requirements for the PRTG Core Server

Hardware requirements for the PRTG core server service mainly depend on the sensors and scanning intervals that you use. Your network size can also influence the performance of your monitoring.

Sensors per PRTG core server	CPU cores	RAM	Disk space	Concurrently active administrator sessions	Number of remote probes
Up to 500	4	4 GB	100 GB	< 30	< 30
Up to 1,000	6	6 GB	500 GB	< 30	< 30
Up to 2,500	8	8 GB	750 GB	< 20	< 60
Up to 5,000	8	12 GB	1,000 GB	< 20	< 60

Sensors per PRTG core server	CPU cores	RAM	Disk space	Concurrently active administrator sessions	Number of remote probes
Up to 10,000	10 - 12	16 GB	1,500 GB	< 15	< 80
> 10,000	We recommend that you set up additional PRTG core servers. For more information on scaling, you can also contact the <a href="#">Paessler Presales team</a> .				

### Hardware and Network Size Requirements for Classic Remote Probes

Hardware requirements for the PRTG probe service mainly depend on the sensors and scanning intervals that you use. Your network size can also influence performance of your monitoring.

Sensors per classic remote probe	CPU cores	RAM	Disk space
Up to 200	2	2 GB	40 GB
200 - 2,000	4	4 GB	40 GB
2,000 - 5,000	6	6 GB	40 GB
> 5,000	We recommend that you set up additional remote probes. For more information on scaling, you can also contact the <a href="#">Paessler Presales team</a> .		

**i** A remote probe system does not have any special disk requirements (< 1 GB). In general, we recommend at least 40 GB.

### Hardware and Network Size Requirements for Multi-Platform Probes

Hardware requirements for the multi-platform probe mainly depend on the operating system, sensors, and scanning intervals that you use. Your network size can also influence performance of your monitoring.

**i** Multi-platform probes currently support the following non-Windows systems: Ubuntu Linux, Debian Linux, RHEL/CentOS, and Raspberry PI OS.

Sensors per multi-platform probe	CPU cores	RAM	Disk space
Up to 200	2	1 GB	8 GB
200 - 2,000	4	2 GB	8 GB
2,000 - 5,000	6	2 GB	8 GB
> 5,000	We recommend that you set up additional multi-platform probes. For more information on scaling, you can also contact the <a href="#">Paessler Presales team</a> .		

**i** For more information about concrete hardware examples you can use with the multi-platform probe, see the [Multi-Platform Probe for PRTG](#) manual.

### Performance Impact Considerations Based on Sensor Types

You can find the [performance impact](#)<sup>[2952]</sup> of a specific sensor on the Overview tab of the sensor or in the [Add Sensor](#)<sup>[414]</sup> dialog.

**■** For an overview list of all sensors, including their performance impact, see section [Available Sensor Types](#)<sup>[3232]</sup>.

In general, consider the following rules for the different sensor types:

Sensor Type	Performance Impact Considerations
SNMP v1 and v2, Ping, Port, and HTTP	We recommend that you use these sensor types for scenarios with thousands of sensors.
SNMP v3	SNMP v3 has performance limitations because of the use of encryption. Furthermore, keep in mind that SNMP v3, unlike SNMP v1 and v2c, does not scale with more CPU power. Because of this limitation, PRTG can only handle a limited number of requests per second so that you can use only a limited number of sensors using SNMP v3.
WMI	Try to keep the number of WMI sensors per probe below 120 sensors (with a 60-second scanning interval), or below 600 sensors (with a 300-second scanning interval).
Flow	The maximum number of flow sensors depends on the traffic pattern, the number of flow packets per second that the probe receives, as well as the performance of the probe system.

Sensor Type	Performance Impact Considerations
Packet Sniffer	This sensor type creates the highest CPU load on the probe system. We only recommend this technology for monitoring low traffic connections (< 50 Mbit/s steady stream). If the traffic often exceeds 10 Mbit/s, use a dedicated remote probe.
VMware monitoring	Monitoring VMware is limited to about 30 sensors at a 60-second scanning interval, or 100 sensors at a 5-minute scanning interval. On probes that run on at least Windows Server 2016, you can use more VMware sensors. These limitations come from the VMware platform.  ■ For more information, see the Knowledge Base: <a href="#">How can I increase the connection limit on VMware systems? PE121</a>

❗ You can overcome these limitations if you distribute the sensors between remote probes.

### Supported Web Browsers

❗ Microsoft Internet Explorer 11, older versions of Microsoft Edge 79, as well as other browsers that are not officially supported, have issues with some functionalities of the PRTG web interface. However, you can access the PRTG web interface with any browser.

❗ Deprecated Internet Explorer versions as well as some mobile browsers might not be able to display all features of the PRTG web interface.

Category	Requirements
Mozilla Firefox	❗ Mozilla Firefox is potentially vulnerable to cross-site scripting (XSS) attacks. These XSS exploits are possible if you click, for example, phishing links in emails that contain malicious code, and you are logged in to PRTG with Mozilla Firefox.  ■ For more information, see the Knowledge Base: <a href="#">How secure is it to access the PRTG web interface with Firefox?</a>
Plugins	Plugins can also have an effect when you view the PRTG web interface. Make sure that you add exceptions for PRTG in the plugins' settings, particularly if you use ad blockers.  ■ For more information, see the Knowledge Base: <a href="#">The logs page in the PRTG web interface does not load. What can I do?</a>

### Further System Requirements

#### Screen Resolution

A screen resolution of at least 1024x768 pixels is sufficient for most functions of PRTG. However, we recommend a screen resolution of 1200x800 pixels or higher.

## Requirements for Monitored Devices

Category	Requirement
SNMP monitoring	<p>The target devices must support SNMP v1, v2c, or v3. An SNMP-compatible software must be installed on the device. You must enable SNMP on the device and you must grant the PRTG core server system access to the SNMP interface.</p> <p>■ For more information, see section <a href="#">Monitoring via SNMP</a><sup>[2997]</sup>.</p>
Windows/WMI monitoring	<p>To monitor via WMI, you need a Windows network. Use only the officially <a href="#">supported operating systems</a><sup>[26]</sup> when you monitor via WMI.</p> <p>■ For more information, see section <a href="#">Monitoring via WMI</a><sup>[3004]</sup>.</p>
Flow monitoring	<p>The target devices must be able to send NetFlow (NetFlow v5, NetFlow v9, or IPFIX) data packets or sFlow v5 packets to the probe system.</p> <p>■ For more information, see section <a href="#">Monitoring Bandwidth via Flows</a><sup>[3011]</sup>.</p>
Packet sniffer monitoring	<p>PRTG can only analyze data packets that pass the network card of the local machine. Switches with monitoring ports are necessary for network-wide monitoring in switched networks.</p> <p>■ For more information, see section <a href="#">Monitoring Bandwidth via Packet Sniffing</a><sup>[3009]</sup>.</p>
Other sensor types	<p>You can find specific sensor and device requirements (for example, modules, components, device configurations) in the corresponding sensor section and in the Add Sensor dialog.</p>

## Requirements for Smartphones and Tablets

You can optionally use the PRTG apps for iOS and Android.

- For more information and system requirements, see section [PRTG Apps for Mobile Network Monitoring](#)<sup>[2988]</sup>.

## More

### ■ KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/71305>

How can I increase the connection limit on VMware systems? PE121

- <https://kb.paessler.com/en/topic/30643>

How secure is it to access the PRTG web interface with Firefox?

- <https://kb.paessler.com/en/topic/70192>

The logs page in the PRTG web interface does not load. What can I do?

- <https://kb.paessler.com/en/topic/77329>

How can I speed up PRTG—especially for large installations?

- <https://kb.paessler.com/en/topic/2733>

How do I run PRTG under a different Windows user account than the local system account?

- <https://kb.paessler.com/en/topic/89016>

What do I have to consider when I want to do a regular cleanup of my PRTG environment?

- <https://kb.paessler.com/en/topic/89999>

## PAESSLER WEBSITE

System requirements for PRTG Network Monitor

- <https://www.paessler.com/prtg/system-requirements>

## 1.6 Introduction: Monitoring with PRTG

This section shows you how to prepare your IT infrastructure so that you can monitor it with PRTG.

In this section:

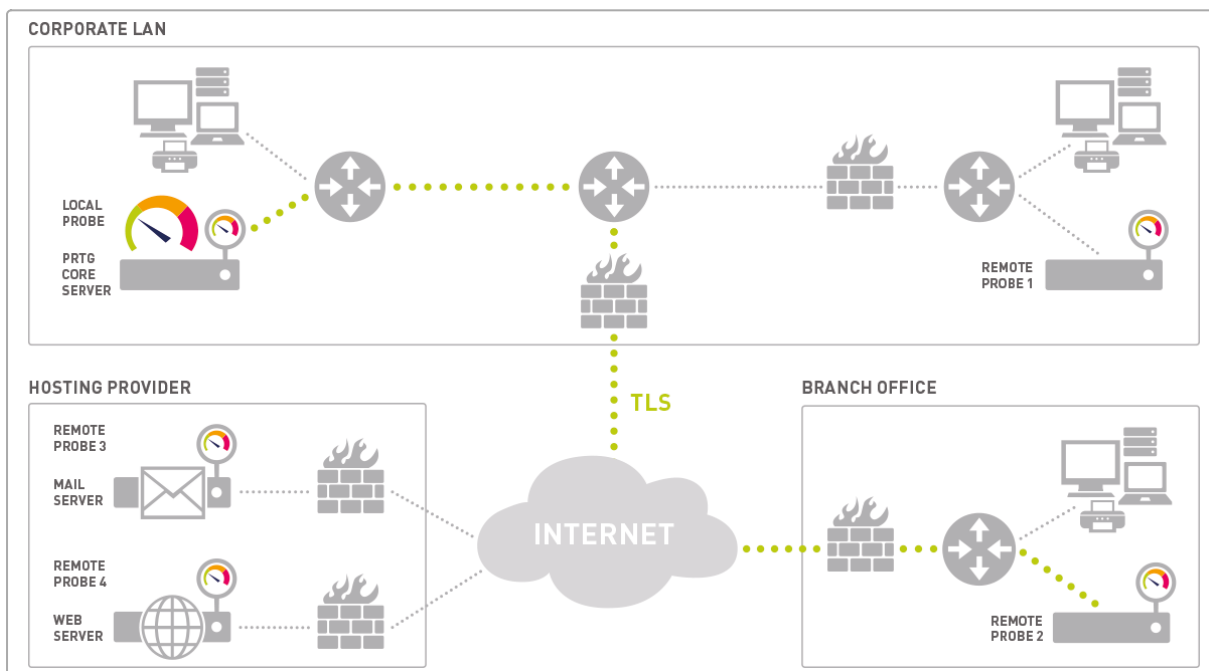
- [What PRTG Does](#)<sup>[33]</sup>
- [How to Monitor with PRTG](#)<sup>[34]</sup>
- [What PRTG Monitors](#)<sup>[34]</sup>
- [How to Prepare Monitoring](#)<sup>[35]</sup>
- [Which Hardware Do I Want to Monitor](#)<sup>[35]</sup>

■ To immediately start monitoring with PRTG, go to section [Quick Start Guide](#)<sup>[38]</sup>.

### What PRTG Does

PRTG is a unified monitoring tool that can monitor almost any object that has an IP address. It consists of the [PRTG core server](#)<sup>[125]</sup> and one or more [probes](#)<sup>[125]</sup>:

- The PRTG core server is responsible for configuration, data management, PRTG web server, and more.
- Probes collect data and monitor processes on [devices](#)<sup>[134]</sup> via [sensors](#)<sup>[134]</sup>.



Sensors are the building blocks of PRTG. A sensor can tell you about one or more aspects of a device:

- Uptime
- Load
- Interface throughput

- Bandwidth usage
- Loading times
- Speed
- Hardware status
- Temperature
- Quality
- Resource consumption
- User counts
- Record counts
- Log events
- Database requests

## How to Monitor with PRTG

PRTG obtains monitoring data from target devices in the following ways:

- Polls or queries sensor data: PRTG actively gathers data from a device in regular intervals. This includes, for example, device status, resource usage, and performance metrics. Most sensors use this method. PRTG can also consume and collect sensor data based on interfaces with, for example, HTTP or HTTPS requests, port checks, email checks, File Transfer Protocol (FTP) downloads, and database requests.
- Listens for or receives sensor data: PRTG passively receives data from a device or application. This includes, for example, unexpected events, Syslogs and Simple Network Management Protocol (SNMP) traps, [detailed data flow](#)<sup>[3014]</sup>, and event log messages.

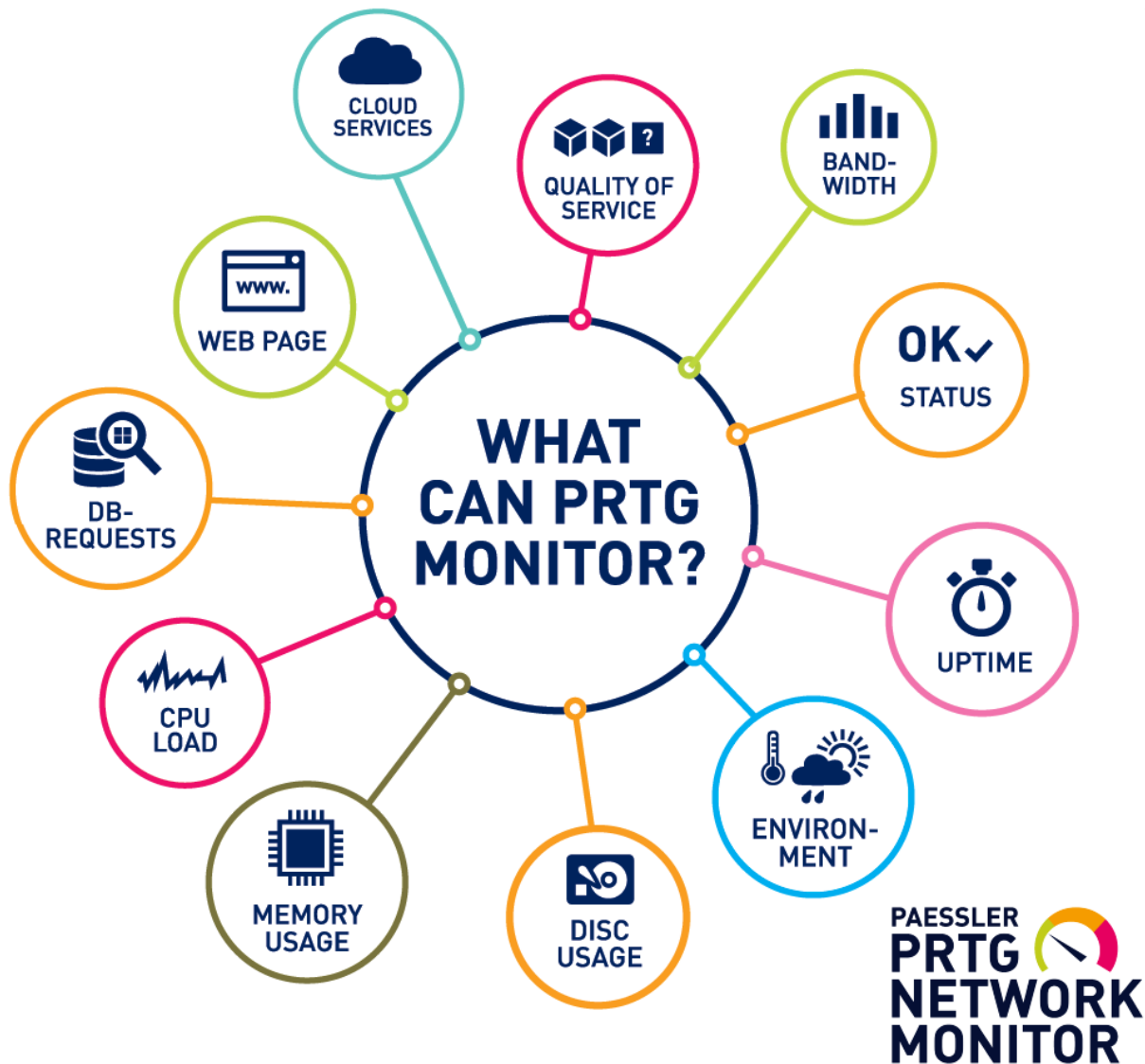
Most of the monitoring data that PRTG collects is actively queried. It is the basis for statistical sampling to see how a device or application performs over time.

■ For more information, see section [Sensor Technologies](#)<sup>[2996]</sup>.

## What PRTG Monitors

PRTG comes with [hundreds of sensors](#)<sup>[3232]</sup>. They range from platform-specific sensors to generic hardware and bandwidth sensors. Some of them are preconfigured to immediately gather monitoring data from their target devices. You can also create custom sensors or write custom scripts that return data from applications. Visit the [PRTG Sensor Hub](#)<sup>[3263]</sup> to learn more about ready-to-use custom sensors.





■ For more information, see section [Available Sensor Types](#) <sup>3232</sup>.

## How to Prepare Monitoring

The first step in comprehensive monitoring is to make a plan. Think about the following questions:

- What do I need to monitor in my IT infrastructure?
- How can I retrieve the needed information? Which technologies and credentials are required?
- Which notification methods do I want to use to receive alerts if something is wrong?

## Which Hardware Do I Want to Monitor?

We recommend that you start with your [Business Critical Tier-1](#). This usually includes the core network and other infrastructure that all network devices depend upon:

- Key infrastructure, such as core routers, switches, VPN and firewalls

- Basic network services, such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS)
- Authentication, like Lightweight Directory Access Protocol (LDAP)

Use the following list to help you plan the monitoring of your IT infrastructure with PRTG:

1. Core infrastructure
  - a. Routers, switches, firewalls
  - b. Core network services: DNS, Active Directory (AD), LDAP servers
2. For your hardware devices, you need statistics on availability, usage, and performance.
3. PRTG retrieves data via standard protocols:
  - a. Ping, SNMP; web queries via HTTP and HTTPS; email via Post Office Protocol version 3 (POP3), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP)
  - b. Hardware parameters via SNMP, Secure Shell (SSH), Simple Object Access Protocol (SOAP)
  - c. Bandwidth usage via Flow (NetFlow, jFlow, sFlow, IPFIX), packet sniffing, SNMP
  - d. Windows systems via Windows Management Instrumentation (WMI)
  - e. Other interfaces via SSH and scripts (for example, PowerShell and Python)

## More

### KNOWLEDGE BASE

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

My HTTP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/85284>

How can I send SMS text message notifications via a modem or a mobile phone with PRTG?

- <https://kb.paessler.com/en/topic/393>

How can I use push notifications with PRTG?

- <https://kb.paessler.com/en/topic/60892>

### VIDEO TUTORIAL

SNMP Trap receiver and syslog receiver sensors

- <https://www.paessler.com/support/videos-and-webinars/videos/syslog-receiver>

Notifications

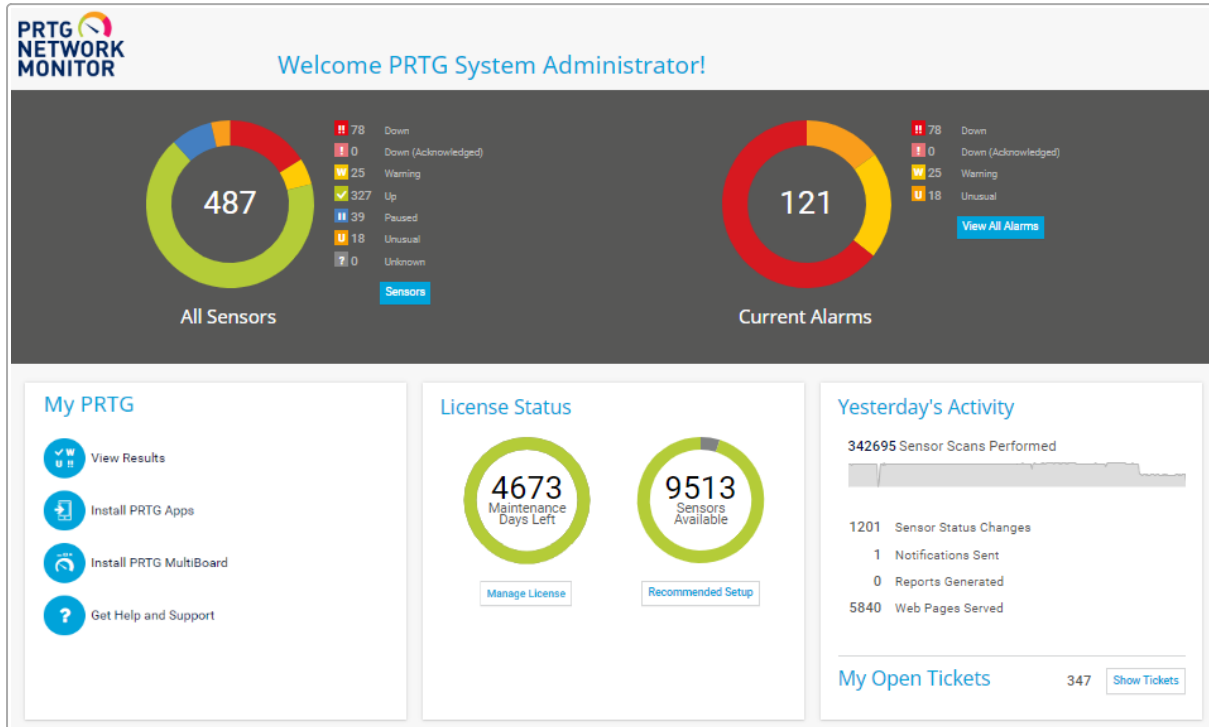
- <https://www.paessler.com/support/videos-and-webinars/videos/notifications>

# Part 2

# Quick Start Guide

## 2 Quick Start Guide

Welcome to PRTG. This section gives you a quick start into monitoring with PRTG.



Welcome Page

To set up your network monitoring, download the PRTG installer from the [Paessler website](#) and follow the steps in the installation wizard, or set up a PRTG Hosted Monitor instance on <https://www.paessler.com/prtg/prtg-hosted-monitor> and install a remote probe in your LAN. Provide some information about your network in the [smart setup](#)<sup>39</sup> and PRTG immediately starts to monitor your network. You can adjust the setup to your needs later on.

In this section:

- [Step 1: Download, Installation, and First Login](#)<sup>39</sup>
- [Step 2: Smart Setup](#)<sup>41</sup>

## 2.1 Step 1: Download, Installation, and First Login

To use PRTG Network Monitor, download it from the [Paessler website](#) and install it on a Windows system.

☁ For information on how to set up a PRTG Hosted Monitor instance, see section [Create a PRTG Hosted Monitor Instance](#).

### Download PRTG

Download the latest stable version of PRTG from the [Paessler website](#) as a [trial version](#)<sup>[20]</sup>. Buy and manage your license at the [Paessler Portal](#).

### Install PRTG

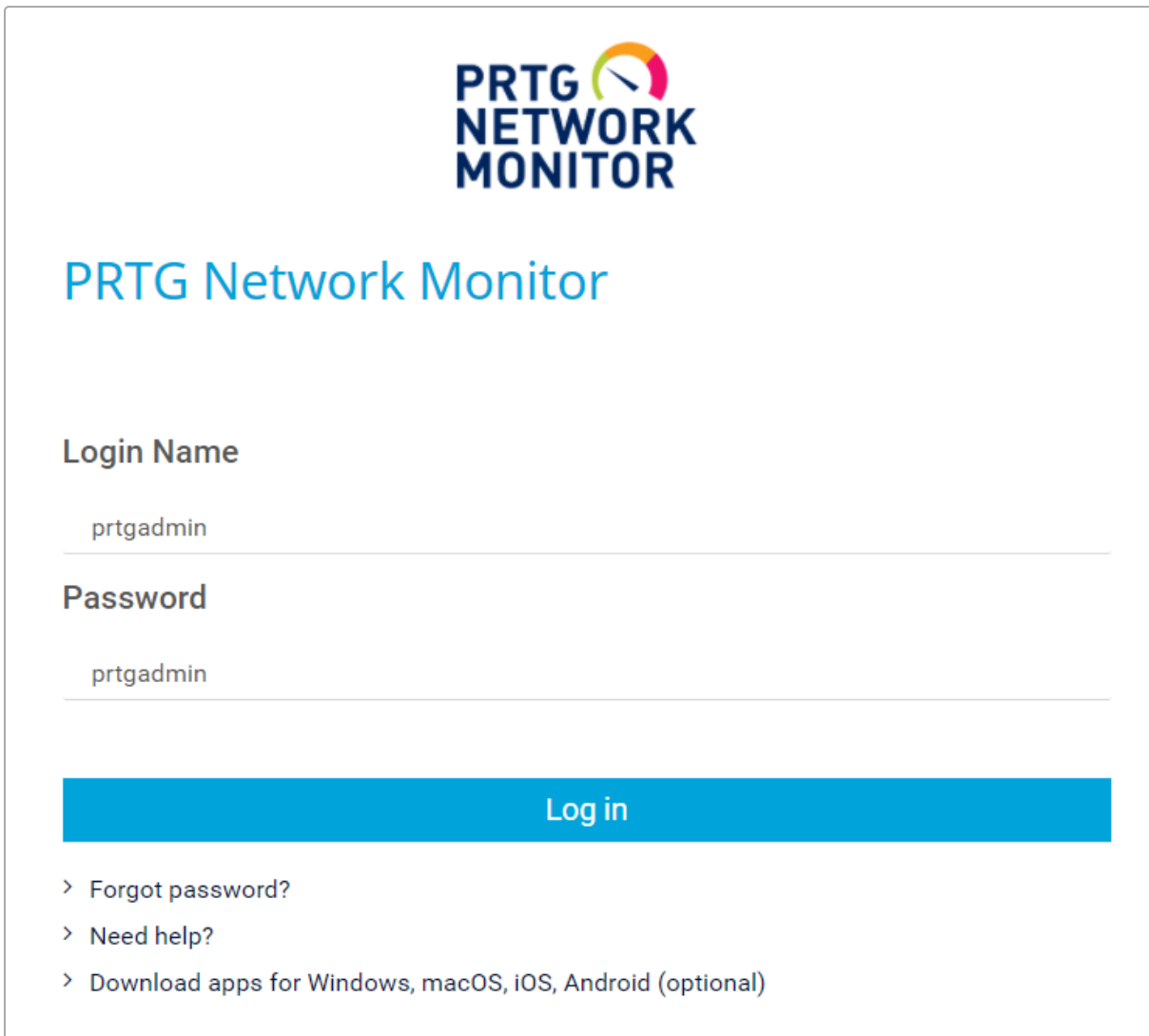
Double-click the setup file on the system that you want to use as the PRTG core server. Follow the [installation wizard](#)<sup>[94]</sup> and install the software.

At the end of the installation, open the PRTG web interface with one of the officially [supported browsers](#)<sup>[22]</sup>.

ⓘ Because of scripting incompatibilities, you might not be able to use all functionalities of the PRTG web interface with Internet Explorer 10 or earlier and other older browsers. If you cannot access the PRTG web interface, open the URL of PRTG in a different supported browser.

### Login

After you installed PRTG Network Monitor, open the PRTG web interface with a supported browser. You see the login screen.



**PRTG NETWORK MONITOR**

## PRTG Network Monitor

**Login Name**

prtgadmin

**Password**

prtgadmin

**Log in**

- > [Forgot password?](#)
- > [Need help?](#)
- > [Download apps for Windows, macOS, iOS, Android \(optional\)](#)

Login Screen

PRTG automatically fills in the credentials of the predefined [PRTG System Administrator](#) user. The login name and the initial password is [prtgadmin](#). Click Log in to proceed.

■ See the [next step](#) <sup>41</sup> for more information about the initial configuration of PRTG. <sup>41</sup>

### More

 VIDEO TUTORIAL

All video tutorials

- <https://www.paessler.com/support/videos-and-webinars/videos>

## 2.2 Step 2: Smart Setup

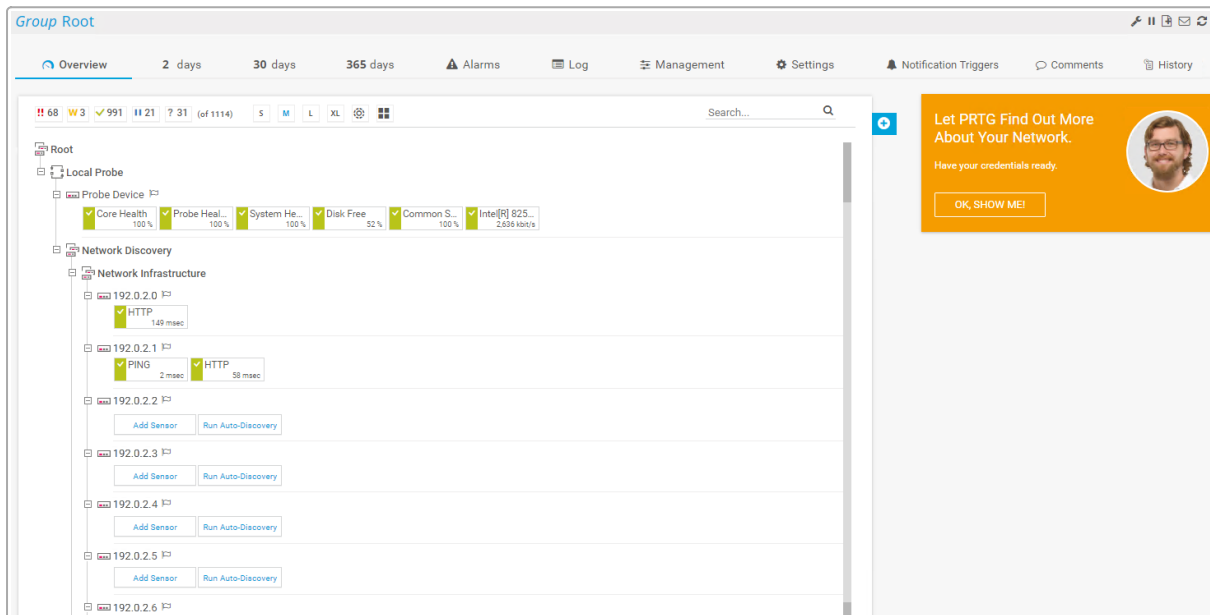
PRTG automatically starts the smart setup on a new PRTG installation. This setup assistant guides you through the initial setup of your network monitoring system. The smart setup reappears until you have completed all steps. You can skip the introduction altogether right at the beginning.

### First Start

When you log in for the first time, you see the [device tree](#)<sup>164</sup>. PRTG Network Monitor already includes several [devices](#)<sup>134</sup> with [sensors](#)<sup>134</sup> that monitor your network, sorted into different [groups](#)<sup>133</sup>. PRTG automatically creates the device tree during the installation process via the [auto-discovery](#)<sup>254</sup> feature.

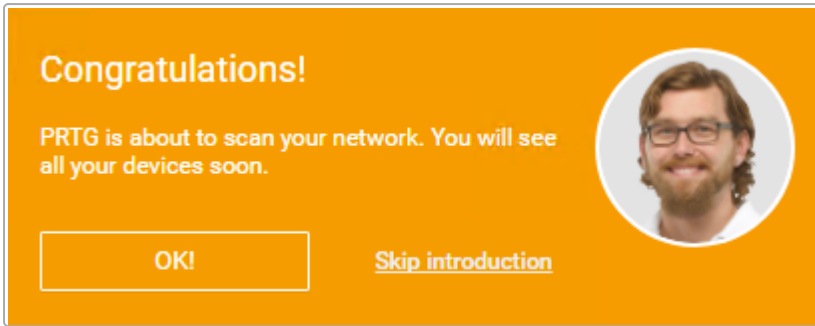
PRTG scans your network by pinging IP addresses in the subnet of your PRTG core server and adds all reachable devices to your specific network monitoring structure.

- ❶ The smart setup scans only for devices with IP addresses in private network ranges. You can manually start an auto-discovery for other subnets later.



Device Tree after Initial Auto-Discovery

In the upper-right corner of the PRTG web interface, you can see the smart setup assistant. They guide you through 5 setup steps during which you can enter more information about your network. PRTG runs another auto-discovery with this information to add additional devices and sensors to your monitoring. You can still edit the settings that you provided during the smart setup later on to adjust the monitoring to your needs.



Start Your Introduction to PRTG

Click OK! to start a guided tour.

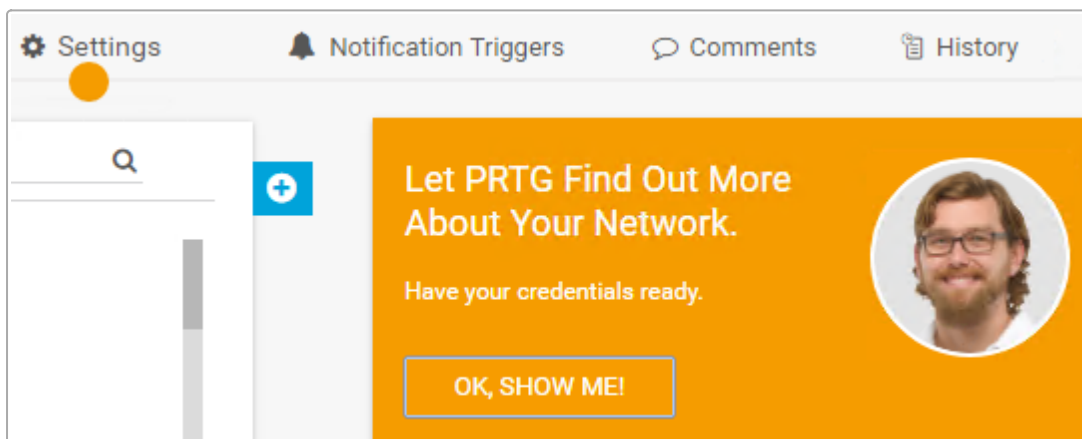
**i** If you click Skip introduction, the smart setup assistant never appears again. We strongly recommend that you take the guided tour if you are new to PRTG.

The steps to take are:

- [Step 1: Provide Credentials](#)<sup>42</sup>
- [Step 2: Enter Location Information](#)<sup>44</sup>
- [Step 3: Change Your PRTG Login Password](#)<sup>44</sup>
- [Step 4: Confirm Your Email Address](#)<sup>45</sup>
- [Step 5: Switch to SSL/TLS](#)<sup>46</sup> (if you access PRTG from a different system)

## Step 1: Provide Credentials

Your smart setup assistant asks you to provide credentials for devices in your network. Click OK, Show Me!, follow the animated mouse pointer, and open the Settings tab of the root group.



Have Your Credentials Ready

On the Settings tab, enter various administrator credentials for your network environment. With these credentials, PRTG can automatically add a large number of additional devices and sensors to your device tree. This way, you do not need to manually add every single device.



### Credentials for Windows Systems

Domain or Computer Name <sup>?</sup>

User Name <sup>?</sup>

Password <sup>?</sup>

---

### Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

User Name <sup>?</sup>

Authentication Method <sup>?</sup>  Password (default)  
 Private key

Password <sup>?</sup>

WBEM Protocol <sup>?</sup>  HTTP  
 HTTPS (default)


WBEM Port <sup>?</sup>  Default  
 Custom

SSH Port <sup>?</sup>

SSH Rights Elevation <sup>?</sup>  Run the command as the connecting user (default)  
 Run the command as a different user using 'sudo' (with password)  
 Run the command as a different user using 'sudo' (without password)  
 Run the command as a different user using 'su'

SSH Connection Mode <sup>?</sup>  Default  
 Compatibility mode (deprecated)

**How Can PRTG Access Your Systems?**



Please enter administrator credentials so PRTG can discover more sensors for your devices.

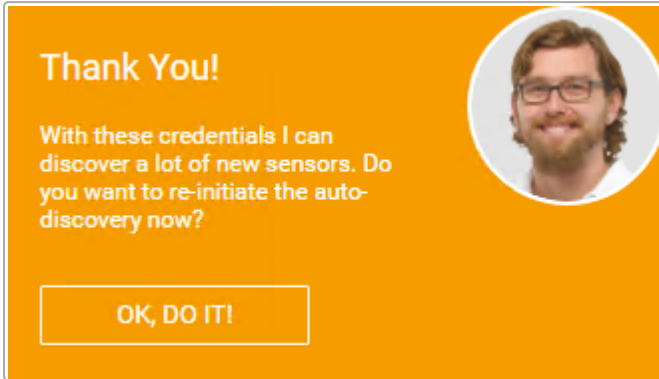
Provide Your Credentials

- To monitor your Windows clients and servers via Windows Management Instrumentation (WMI), enter Windows administrator credentials for your network. We recommend that you use domain administrator credentials if you use an Active Directory. For a general introduction to the technology behind WMI, see section [Monitoring via WMI](#)<sup>[3004]</sup>.
- If you have systems that run on Linux, Solaris, or macOS, enter root access credentials for these systems. For a general introduction to Secure Shell (SSH) monitoring, see section [Monitoring via SSH](#)<sup>[3007]</sup>.
- If you use the virtual environments VMware or Citrix XenServer, enter root access credentials for these systems. For a general introduction to the monitoring of virtual environments, see section [Monitoring Virtual Environments](#)<sup>[3022]</sup>.
- To monitor hardware like routers or switches, the Simple Network Management Protocol (SNMP) is the most commonly used protocol. Usually, all SNMP-enabled devices use the same settings by default: SNMP  $v2c$ , the community string `public`, and SNMP port `161`. For a general introduction to the technology behind SNMP, see section [Monitoring via SNMP](#)<sup>[2997]</sup>.
- You can also enter credentials for database management systems or credentials for Amazon Web Services (AWS) monitoring.

PRTG stores these credentials in the root group of your device tree. All dependent devices automatically inherit these credentials and use them for monitoring. You can disable the [inheritance of settings](#)<sup>[136]</sup> at any level if you want to enter other credentials instead.

■ For more information about the available options, see section [Root Group Settings](#)<sup>[422]</sup>.

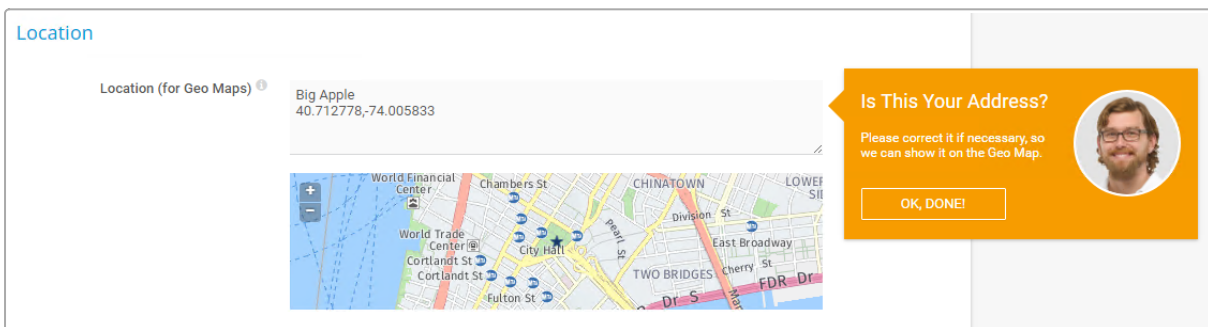
Click OK, Done! to finish this setup step. Click OK, Do It! to start a detailed auto-discovery.



Start a Detailed Auto-Discovery

### Step 2: Enter Location Information

While PRTG runs a new auto-discovery in your network with the provided credentials, the setup assistant asks you to provide the location of your PRTG core server. This information is displayed in [geographical maps](#)<sup>[2731]</sup>. Enter your location and confirm with OK, Done!. Click OK, Show Me! to get back to the device tree.

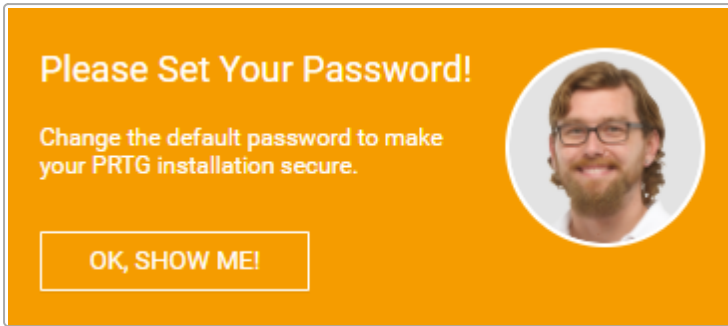


Enter Your Location

■ For more information about the available options, see section [Root Group Settings](#)<sup>[422]</sup>.

### Step 3: Change Your PRTG Login Password

Back in the device tree, the setup assistant in PRTG Network Monitor asks you to change your password. Click OK, Show Me! and follow the assistant to your account settings. By default, PRTG uses the **PRTG System Administrator** user account with the login name **prtgadmin** and the password **prtgadmin**. So we strongly recommend that you change the password to protect PRTG from unauthorized access.



Start the Password Change

Enter your New Password and confirm it under Confirm Password. The password must meet the following requirements:

- At least eight characters long
- At least one numeral
- At least one capitalized letter

Click OK, Done! to save your new password.

Change the Default Password

■ For more information about the available options, see section [My Account](#) <sup>2802</sup>.

### Step 4: Confirm Your Email Address

To complete the smart setup, check whether the email address that you entered during the installation is correct.

**i** A correct email address is mandatory for PRTG to reach you via email notifications when there are alarms and for other important messages.

Click OK, Done! and follow the assistant back to the device tree.

Verify Your Email Address

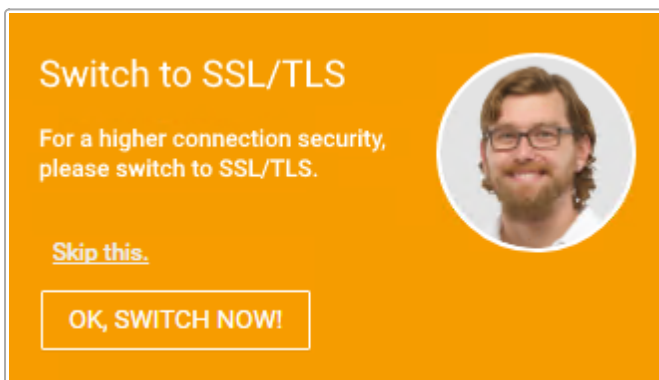
■ For more information about the available options, see section [My Account](#)<sup>2801</sup>.

## Step 5: Switch to SSL/TLS

For PRTG Network Monitor, if you access the PRTG web interface from a system other than the system where you installed PRTG, the setup assistant asks you to switch to a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. We strongly recommend that you run the PRTG web interface secured with SSL/TLS, especially if you make your PRTG web interface available from the internet. Otherwise, your passwords are sent over your network without encryption.

- Click OK, Switch Now! to get more information about using SSL/TLS for the PRTG web server.
- In the new window, click Yes, switch to SSL/TLS to switch to an SSL/TLS-secured connection.
- PRTG must restart its services to apply the changes. The PRTG web interface is reachable under an HTTPS URL afterward.
- When the PRTG web interface reloads, it most likely shows a certificate warning. Confirm the certificate warning to proceed to the login screen.

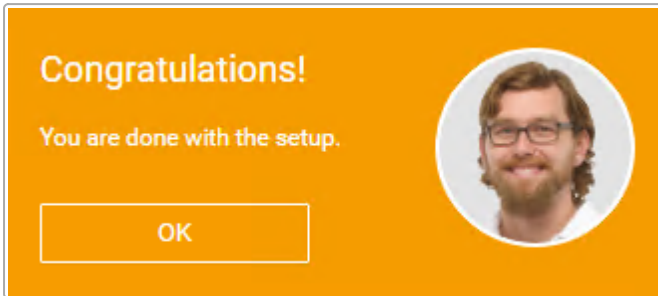
■ For more information, see the Knowledge Base: [Why does my browser show an SSL certificate warning when I open the PRTG web interface?](#)



Switch to a Secure Connection

■ For more information, see section [User Interface](#)<sup>2855</sup>.

## You Are Done



Finish the Smart Setup

While you went through the smart setup, PRTG created additional devices and sensors for you. The first monitoring values are also available.

- To become familiar with the PRTG web interface, we recommend that you read on in section [General Layout](#)<sup>[164]</sup>.

## More

### ■ KNOWLEDGE BASE

Why does my browser show an SSL certificate warning when I open the PRTG web interface?

- <https://kb.paessler.com/en/topic/89984>

### ▶ VIDEO TUTORIAL

Smart setup

- [https://www.paessler.com/support/videos-and-webinars/videos/installation\\_of\\_prtg\\_network\\_monitor](https://www.paessler.com/support/videos-and-webinars/videos/installation_of_prtg_network_monitor)




## Part 3

# Using PRTG Hosted Monitor

## 3 Using PRTG Hosted Monitor

The following sections show you how to create a PRTG Hosted Monitor instance, how to manage a PRTG Hosted Monitor subscription, and how to use multi-factor authentication.

In this section:

- [Create a PRTG Hosted Monitor Instance](#) 
- [Manage a PRTG Hosted Monitor Subscription](#) 
- [Use Multi-Factor Authentication with PRTG Hosted Monitor](#) 

■ See the Paessler website for [PRTG Hosted Monitor – Service description](#) and [FAQ – PRTG Hosted Monitor](#).

### More

■ PAESSLER WEBSITE

PRTG Hosted Monitor – Service description


- <https://www.paessler.com/prtg/prtg-hosted-monitor>

FAQ – PRTG Hosted Monitor

- <https://www.paessler.com/prtg/prtg-hosted-monitor/faq>

### 3.1 Create a PRTG Hosted Monitor Instance

To create a PRTG Hosted Monitor instance, open a web browser and go to the [PRTG Hosted Monitor Customer Portal](#).



 We recommend that you use Google Chrome 75.



The banner features the Paessler PRTG Hosted Monitor logo in the top left corner. The main text reads "Hosted monitoring software for cloud and hybrid IT infrastructures". Below this, there are three bullet points: "✓ Monitor your systems, devices, applications, traffic & more", "✓ Suited for small to large environments", and "✓ Start monitoring with our cloud-based monitoring solution". At the bottom left, there is a prominent orange button labeled "FREE TRIAL".

Free Trial

In this section:

- [Create a PRTG Hosted Monitor Instance](#)  51
- [Smart Setup for PRTG Hosted Monitor](#)  60



## Create a PRTG Hosted Monitor Instance

1. On the [PRTG Hosted Monitor Customer Portal](#), click Free Trial to create your PRTG Hosted Monitor instance. PRTG Hosted Monitor automatically assigns a domain name to your instance. You can change the domain name at any time.

PAESSLER  
PRTG  
HOSTED  
MONITOR

Sign Up

Log In Sign Up

Sign up with Google

Sign up with Amazon

Sign up with Microsoft Account

OR

yours@example.com

your password

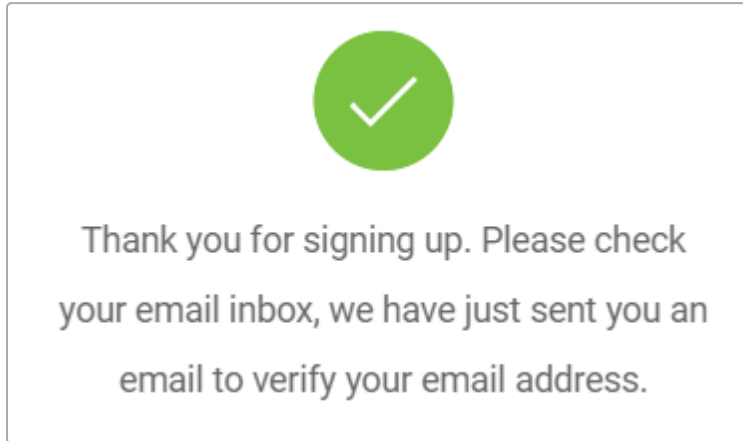
By signing up I agree to the [terms and conditions](#) and [privacy policy](#).

SIGN UP >

Sign Up to PRTG Hosted Monitor

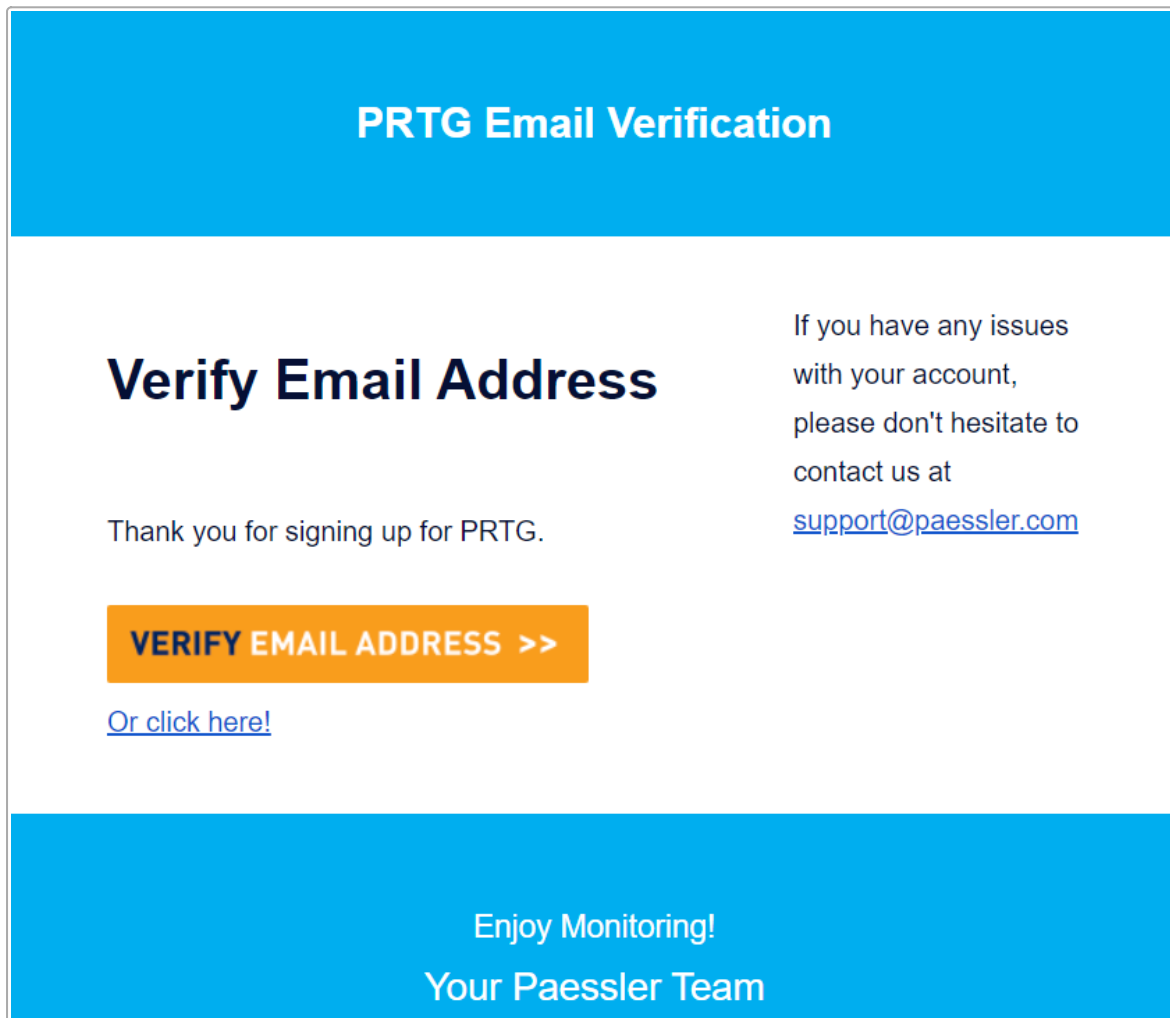
2. You can sign up with your Google, Amazon, or Windows account via single sign-on (SSO) (Auth0). PRTG Hosted Monitor connects to and then automatically uses this account for the login. Click the respective button and follow the instructions. Alternatively, you can sign up via email. Enter a valid Email address and a Password. The password must meet the following requirements:
  - At least 8 characters long
  - At least one uppercase letter
  - At least one lowercase letter

- At least **one** numeral
3. Make sure that you agree to the terms and conditions and privacy policy. Click Sign Up to register for your PRTG Hosted Monitor instance. You then see that a verification email has been sent to your inbox.



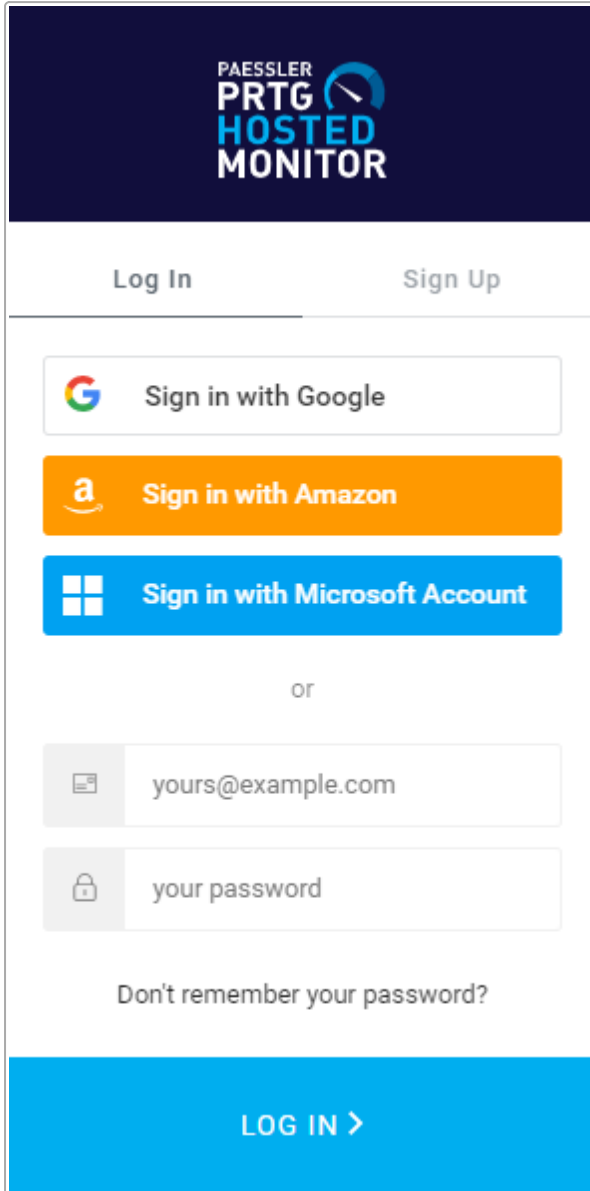
Verify Email Address Notification

4. Go to your inbox and open the email.



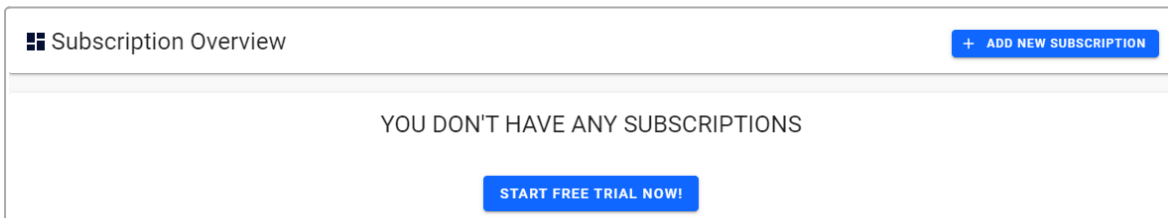
Verify Email Address

- 5. Click Verify Email Address to verify your email address and to go to the login screen.



Login Screen

- 6. Enter your credentials and click Log In to log in to PRTG Hosted Monitor.



Add New Subscription

7. Click Add New Subscription.

### Optional - Select Domain

Choose your subdomain

You can provide your own unique subdomain name here, e. g. your-name or leave it empty and we will generate one for you.

### Select Region

This defines the location where your PRTG will be hosted, which can be changed later if necessary.

Region  
Frankfurt

### Try Free Trial

**TRIAL PLAN**

**Free For 10 Days**  
You can only have one active trial at a time.

SELECT PLAN

Monitor up to 500 aspects of your devices in your network, which usually means about 50 devices.

### Paid Plans

MONTHLY ANNUAL / MULTI-ANNUAL

HOSTED 500	HOSTED 1000	HOSTED 2500	HOSTED 5000	HOSTED 10000
<b>129€ / Month</b>	<b>229€ / Month</b>	<b>499€ / Month</b>	<b>899€ / Month</b>	<b>1299€ / Month</b>
SELECT PLAN	SELECT PLAN	SELECT PLAN	SELECT PLAN	SELECT PLAN
Monitor up to 500 aspects of your devices in your network, which usually means about 50 devices.	Monitor up to 1000 aspects of your devices in your network, which usually means about 100 devices.	Monitor up to 2500 aspects of your devices in your network, which usually means about 250 devices.	Monitor up to 5000 aspects of your devices in your network, which usually means about 500 devices.	Monitor up to 10000 aspects of your devices in your network, which usually means about 1000 devices.

### Summary

Selected domain: **not selected (will be assigned randomly)**  
Selected region: **Frankfurt - Europe**  
Selected plan: **not selected**

### Payment \*


Credit Card  
 Request purchase on account

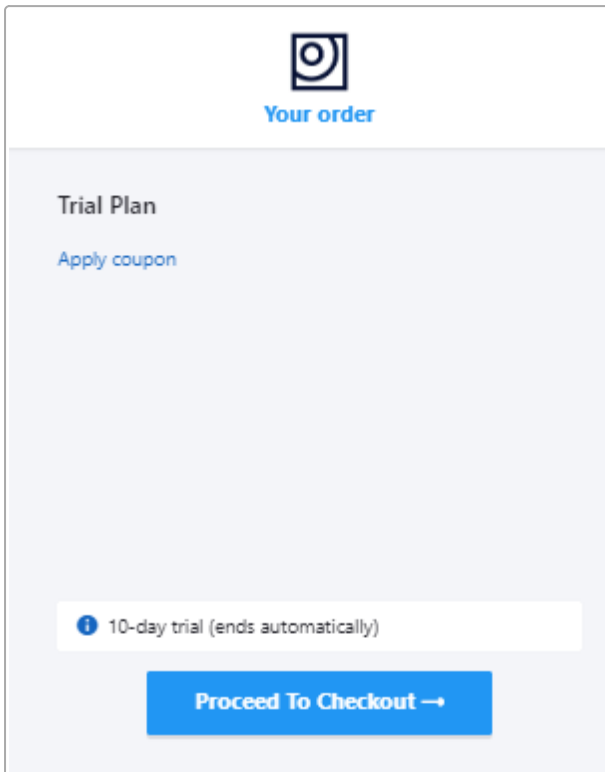
By subscribing to a PRTG Hosted Monitor plan, I accept the transfer of my data for the purpose of payment processing to [Stripe Inc.](#) and [Chargebee Inc.](#)  
I also accept the periodic payment withdrawal for my PRTG Hosted Monitor subscription based on the billing period I selected above. See our [terms & conditions](#) and [privacy policy](#) for details.

CHECKOUT

Subscription Setup

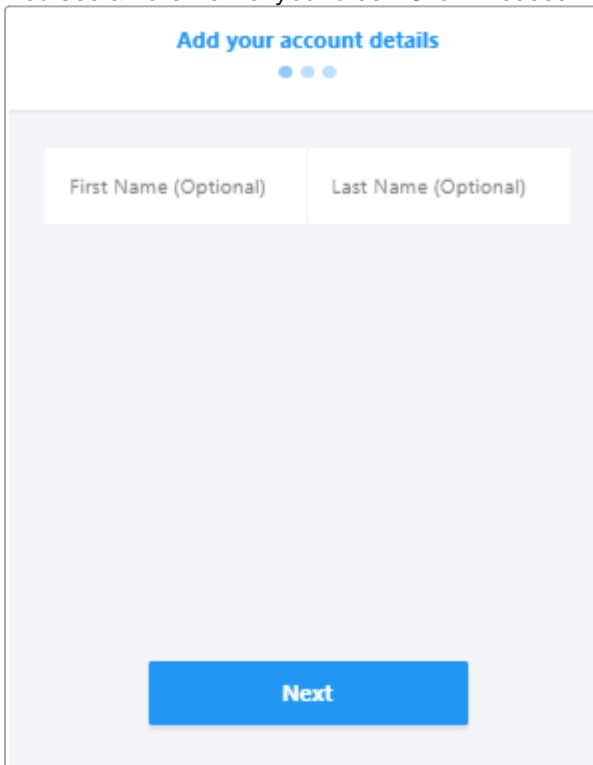
8. Select the region in which PRTG Hosted Monitor hosts your instance.

9. Select a subscription plan that fits your requirements and click Checkout.  
 The billing account will be charged after the free 10-day trial period.



Order Overview

10. You see an overview of your order. Click Proceed To Checkout.



Account Details

11. Optionally enter your first name and last name and click Next.

**Add your billing address**

● ● ●

First Name	Last Name
Company (Optional)	
Address Line1	
Address Line2 (Optional)	
City	Zip
State	Country Pick an option ▼

**Next**

Billing Address

12. Enter your billing information. Then click Next

13. To enable data sharing, click .

### Data Sharing

Share unanonymized data (Optional)

**i** Allow personal data, such as object names, IP addresses, email addresses and user account ID to be visible in shared data. For more information, see the [Knowledge Base](#).

**Next**

Data Sharing

14. Enter your billing information. Then click Next.

**Complete your order**

**Trial Plan** €0.00 >  
10-day trial (ends automatically)

[Apply coupon](#)

**Account** [Edit →](#)

**Subscription Details** [Edit →](#)

**Billing**  
John Q. Public  
12345 Example Street  
City 12345 WA United States [Edit →](#)

**Subscribe**

Secure Checkout

Account and Billing Details Overview

15. You see an overview of your account and billing details. Click Subscribe to finish.

**Subscription Overview** [+ ADD NEW SUBSCRIPTION](#)

**PREPARING INSTANCE**

ⓘ It may take a while until your PRTG is ready.

**PRTG DOMAIN**  
my-instance.my-prtg.com

**PRTG TIMEZONE**  
(UTC+01:00) Sarajevo, Skopje, Warsaw, Zagreb

**PRTG SERVER REGION**  
Zurich - Europe

**PRICING PLAN**  
Trial Plan

**SUBSCRIPTION STATUS**  
Trial Active

**FREE TRIAL DAYS LEFT**  
10

[OPEN PRTG](#) [MANAGE](#) [UPGRADE SUBSCRIPTION](#)

Subscription Progress



14. The Subscription Overview page opens and shows the progress of the PRTG Hosted Monitor installation.

PRTG Hosted Monitor Instance Ready

15. Your PRTG Hosted Monitor instance is now ready. Click Open PRTG to open your PRTG Hosted Monitor instance in the PRTG web interface.

16. Enter your credentials on the [login screen](#) <sup>53</sup>.

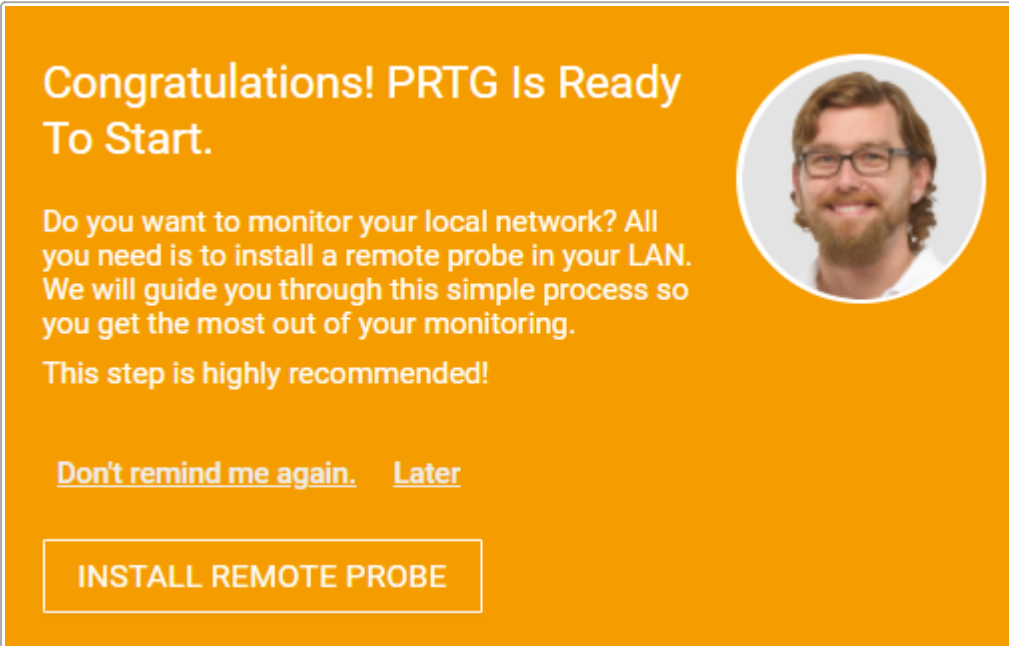
Welcome

Your PRTG Hosted Monitor instance is now up and running. To open the [device tree](#), click View Results, or click Devices in the [main menu bar](#).

PRTG Hosted Monitor automatically creates a [hosted probe](#) that runs on the hosted instance. It shows several health values of the instance and you can instantly monitor all servers, services, and devices that are publicly available via the internet with the hosted probe.

## Smart Setup for PRTG Hosted Monitor




A Paessler employee guides you through the smart setup. In particular, you must install a [remote probe](#), which is required for monitoring your LAN. We strongly recommend that you do so.



The image shows a notification box with an orange background. On the left, the text reads: "Congratulations! PRTG Is Ready To Start." followed by "Do you want to monitor your local network? All you need is to install a remote probe in your LAN. We will guide you through this simple process so you get the most out of your monitoring." and "This step is highly recommended!". At the bottom left are two links: "Don't remind me again." and "Later". At the bottom center is a button labeled "INSTALL REMOTE PROBE". On the right side of the notification is a circular profile picture of a man with glasses and a beard.

Smart Setup: Install a Remote Probe

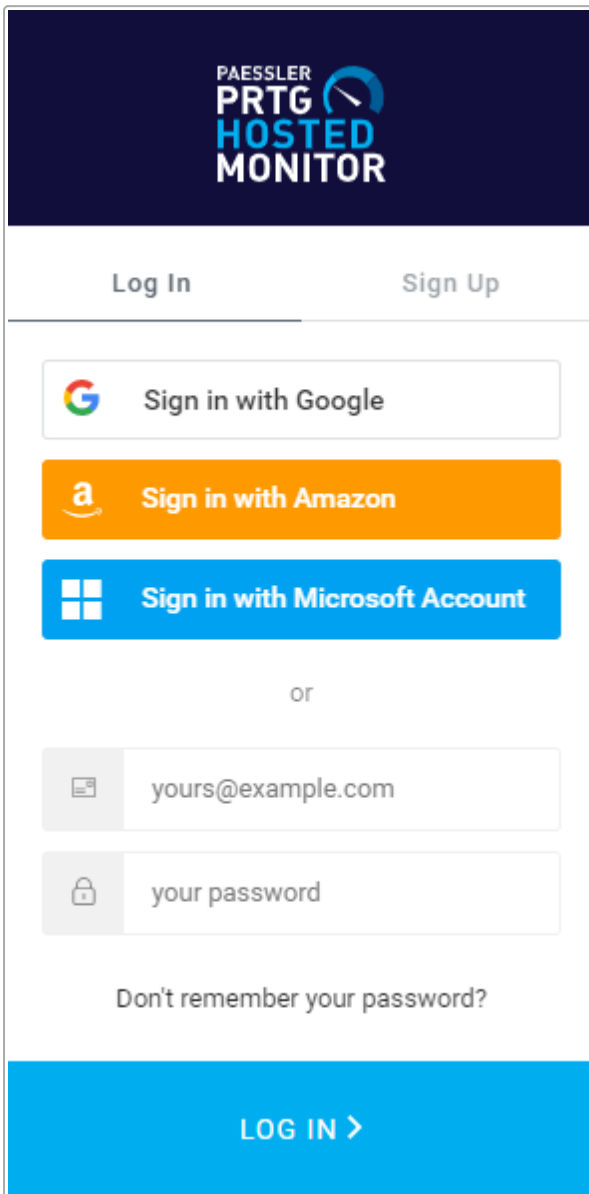
Click Install Remote Probe to start the installation.

-  The multi-platform probe is currently not compatible with PRTG Hosted Monitor.
-  For more information, see section [Install a Remote Probe](#).
-  For more information about other steps of the smart setup, see section [Step 2: Smart Setup](#) for PRTG Network Monitor.

### 3.2 Manage a PRTG Hosted Monitor Subscription

PRTG Hosted Monitor offers subscription plans that you can tailor to your needs and that you can manage via the PRTG Hosted Monitor Customer Portal. To manage your subscription, open a web browser, go to the [PRTG Hosted Monitor Customer Portal](#), and log in.

**i** We recommend that you use Google Chrome 75.






















Login Screen

Provide the credentials that you entered when you signed up, the code that is shown, and click Log In, or use single sign-on (SSO) and continue with your Google, Amazon, or Microsoft account via the respective button.

In this section:

- [Subscription Overview](#) 

- [Manage Subscription](#)  <sup>64</sup>
  - [Change PRTG Subdomain](#)  <sup>66</sup>
  - [Change PRTG Timezone](#)  <sup>66</sup>
  - [Change Multi Factor Authentication in PRTG](#)  <sup>67</sup>
  - [Microsoft Entra ID Integration](#)  <sup>68</sup>
  - [Data Sharing Options](#)  <sup>68</sup>
  - [Request Hosting Transfer](#)  <sup>68</sup>
  - [Restart Instance](#)  <sup>68</sup>
  - [Cancel Subscription](#)  <sup>69</sup>
  - [Change Subscription](#)  <sup>69</sup>
- [Account Settings](#)  <sup>70</sup>
  - [Reset Password](#)  <sup>71</sup>
  - [Billing Details](#)  <sup>72</sup>
  - [Payment Details](#)  <sup>73</sup>
- [Invoices](#)  <sup>74</sup>
- [Upload](#)  <sup>75</sup>
  - [Upload Device Templates](#)  <sup>76</sup>
  - [Upload Custom Files](#)  <sup>76</sup>
- [Logout](#)  <sup>77</sup>

## Subscription Overview

Subscription Overview
+ ADD NEW SUBSCRIPTION

✓
INSTANCE READY

PRTG DOMAIN	my-instance.my-prtg.com
PRTG TIMEZONE	(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
PRTG SERVER REGION	Frankfurt - Europe
PRICING PLAN	Trial Plan
SUBSCRIPTION STATUS	Trial Active
FREE TRIAL DAYS LEFT	10

OPEN PRTG
MANAGE
UPGRADE SUBSCRIPTION

Subscription Overview

Here you see an overview of your PRTG Hosted Monitor subscription. Click [Add New Subscription](#) to upgrade to a commercial subscription, for example. Click [Open PRTG](#) to open your PRTG Hosted Monitor instance in the PRTG web interface. Or click [Manage](#) to manage your subscription.

Manage Subscription

< Manage Subscription

INSTANCE READY

Change PRTG Subdomain

IMPARTIAL-YAKIMYPRTG.COM  
my-instance.myprtg.com

Change PRTG Timezone

PRTG TIMEZONE  
(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Change Multi-Factor Authentication In PRTG

When you enable this option, the accounts of all invited users will be forced to use multi-factor authentication. Next time they log in, they have to set MFA up accordingly (if not done already). Also, it will not be possible to disable MFA for already and newly invited users.

Only users with activated multi factor authentication can access this PRTG instance

Data Sharing Options

You can define the depth of Information about your PRTG Hosted Monitor Instance that you want to share with Paessler for product Improvement and optimization purposes. Your data will neither be used for advertising purposes nor be sold to nor be shared with third parties.

For more information, see the Knowledge Base: <https://kb.paessler.com/en/topic/91492>

You share anonymized information about objects and their properties, log messages and history, raw channel values, and more with Paessler.

- Share telemetry data
- Share anonymized data (default)
- Share comprehensive data

Request Hosting Region Transfer

Request your Instance to be transferred to either the closest hosting region or a preferred one.

REQUEST TRANSFER

Restart Instance

Initiate a restart of your Instance. This operation stops PRTG services momentarily while your Instance is rebooting.

RESTART INSTANCE

Change Subscription

ACTIVE - TRIAL PLAN

Free For 10 Days

You can only have one active trial at a time.

CANCEL SUBSCRIPTION

10 Days Left

Monitor up to 500 aspects of your devices in your network, which usually means about 50 devices.

MONTHLY ANNUAL / MULTI-ANNUAL

HOSTED 500

HOSTED 1000

HOSTED 2500

HOSTED 5000

HOSTED 10000

### Change PRTG Subdomain

Here you can change your subdomain. The domain name can be anywhere from 4 to 60 characters long.

1. Enter a new domain name such as [myfirstdomain](#). If you enter [myfirstdomain](#) as the domain name, for example, your PRTG Hosted Monitor instance is reachable under [myfirstdomain.my-prtg.com](#).  
**i** If you have remote probes, you must manually change the domain name for the PRTG core server. This corresponds to the Server (IPv4 Address or DNS Name) setting in the [PRTG Administration Tool](#).

#### CHANGE YOUR SUBDOMAIN

**ⓘ** IF YOU HAVE REMOTE PROBES, YOU MUST CHANGE THE DOMAIN FOR THE CORE AS WELL. [READ MORE ABOUT HERE.](#)

**ⓘ** PLEASE BE PATIENT, IT CAN TAKE UP TO 24 HOURS UNTIL YOUR PRTG INSTANCE IS AVAILABLE UNDER YOUR NEW DOMAIN.

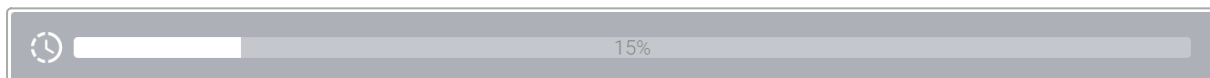
Do you really want to change your subdomain to **myfirstdomain.my-prtg.com**?

[CANCEL](#) [GOT IT](#)

Domain Change

2. Click Got It to continue. You can see the progress in the status bar.

**i** This can take a few minutes.



Domain Change Progress

When the change is complete, the PRTG Hosted Monitor instance is ready.

**✓** INSTANCE READY

Instance Ready

### Change PRTG Timezone

Here you can change the time zone.



## Change PRTG Timezone

PRTG TIMEZONE

(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

(UTC-12:00) International Date Line West

(UTC-11:00) Coordinated Universal Time-11

(UTC-10:00) Aleutian Islands

(UTC-10:00) Hawaii

(UTC-09:30) Marquesas Islands

(UTC-09:00) Alaska

Time Zone Options

Select a time zone from the dropdown list. You see the following message.

Successfully changed Timezone to (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

CLOSE

Time Zone Changed

## Change Multi Factor Authentication in PRTG

To enable multi-factor authentication for all users of your PRTG Hosted Monitor instance, click .

### Change Multi-Factor Authentication In PRTG

**i** When you enable this option, the accounts of all invited users will be forced to use multi-factor authentication. Next time they log in, they have to set MFA up accordingly (if not done already). Also, it will not be possible to disable MFA for already and newly invited users.

Only users with activated multi factor authentication can access this PRTG instance

Change Multi Factor Authentication in PRTG

**i** After you enable this option, multi-factor authentication is activated for all users of your PRTG Hosted Monitor instance and they are asked to scan a QR code with a Time-based One-time Password algorithm (TOTP) application and to enter the current one-time password (OTP) to finish the setup. For more information, see the Knowledge Base: [Can I enable multi-factor authentication for my PRTG Hosted Monitor instance?](#)

### Microsoft Entra ID Integration

To use Microsoft Entra ID as a single sign-on (SSO) provider for PRTG Hosted Monitor, log in to the Azure Portal under <https://portal.azure.com>. After Microsoft Entra ID is integrated into PRTG Hosted Monitor, you can also invite other users from your Active Directory (AD) into PRTG Hosted Monitor. For detailed instructions on how to integrate Microsoft Entra ID into PRTG Hosted Monitor, see the Knowledge Base: [How to integrate Microsoft Entra ID into PRTG Hosted Monitor?](#).

### Data Sharing Options

To define the depth of information that you want to share with Paessler for product improvement and optimization purposes, you can choose among the given options.

**Data Sharing Options**

You can define the depth of information about your PRTG Hosted Monitor instance that you want to share with Paessler for product improvement and optimization purposes. Your data will neither be used for advertising purposes nor be sold to nor be shared with third parties.

For more information, see the Knowledge Base: <https://kb.paessler.com/en/topic/91492>

**i** You share anonymized information about objects and their properties, log messages and history, raw channel values, and more with Paessler.

Share telemetry data

Share anonymized data (default)

Share comprehensive data

Data Sharing Options

### Request Hosting Transfer

To request a transfer of your hosting region on your PRTG Hosted Monitor instance, click Request Transfer.

**Request Hosting Region Transfer**

Request your instance to be transferred to either the closest hosting region or a preferred one.

**REQUEST TRANSFER**

### Restart Instance

To restart your PRTG Hosted Monitor instance, click Restart.

**Restart Instance**

**RESTART**

**i** Please, note that PRTG won't be available until the instance is fully restarted. The operation can take up to 10 minutes.

Restart Instance

### Cancel Subscription

1. Click Cancel Subscription to cancel your PRTG Hosted Monitor subscription.

**CANCEL SUBSCRIPTION**

**ARE YOU SURE YOU WANT TO CANCEL YOUR TRIAL PLAN SUBSCRIPTION?**

Warning: Trial subscriptions cannot be restored!

Before leaving, please select the reason:

- Accidentally subscribed
- Too expensive
- Too complicated
- Bad support
- Features missing
- Company restructure
- Other tool will be used for that in the future
- Project cancelled / finished
- Prefer on-premise
- Other reasons

**CANCEL** **GOT IT**

Cancel Subscription

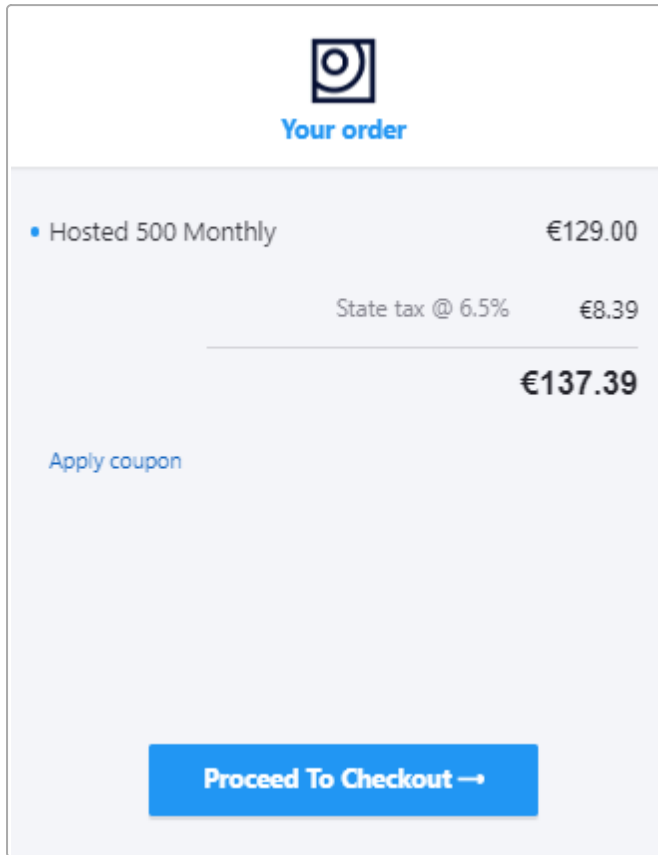
2. Click Got It to finalize the cancellation. You see the following message.

**Subscription cancelled** **CLOSE**

Subscription Cancelled

### Change Subscription

1. Click Change Subscription to select a new PRTG Hosted Monitor subscription and to open the payment checkout dialog. You see an overview of your order.



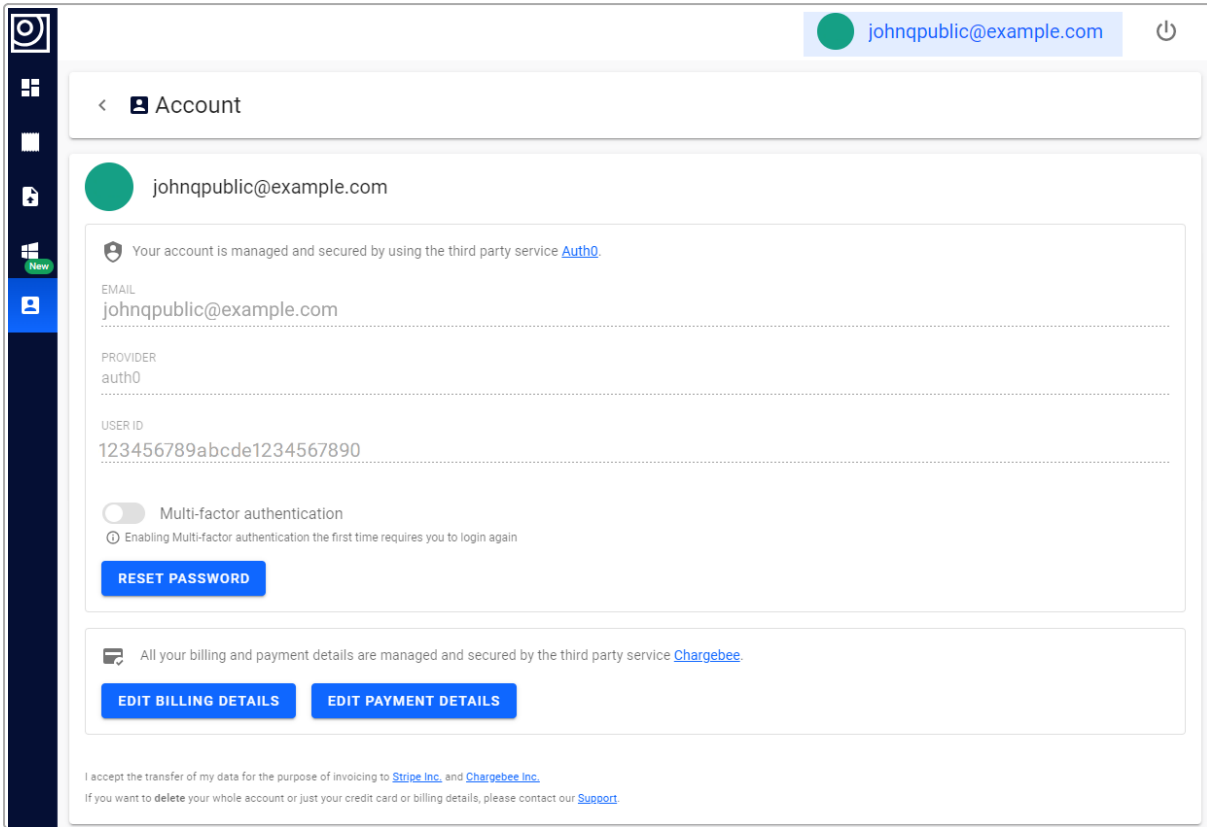
Change Subscription

2. Click Proceed To Checkout and follow the steps to enter your name, billing address, and credit card information if you did not do so during the creation of your PRTG Hosted Monitor instance.

## Account Settings

Click your account in the upper-right corner of the [PRTG Hosted Monitor Customer Portal](#) to open your account settings. Here you can view your profile, change your password, or enable or disable multi-factor authentication.

■ For more information, see section [Use Multi-Factor Authentication with PRTG Hosted Monitor](#) <sup>79</sup>.



Account Overview

### Reset Password

1. Click Reset Password to change the password for your PRTG Hosted Monitor account. PRTG then notifies you that an email has been sent to your inbox.

2. Go to your inbox and open the email. Click Change Password to go to the change password screen.

PAESSLER  
**PRTG**  
**HOSTED**  
**MONITOR**

## Change Password

Enter a new password for  
johnqpublic@example.com

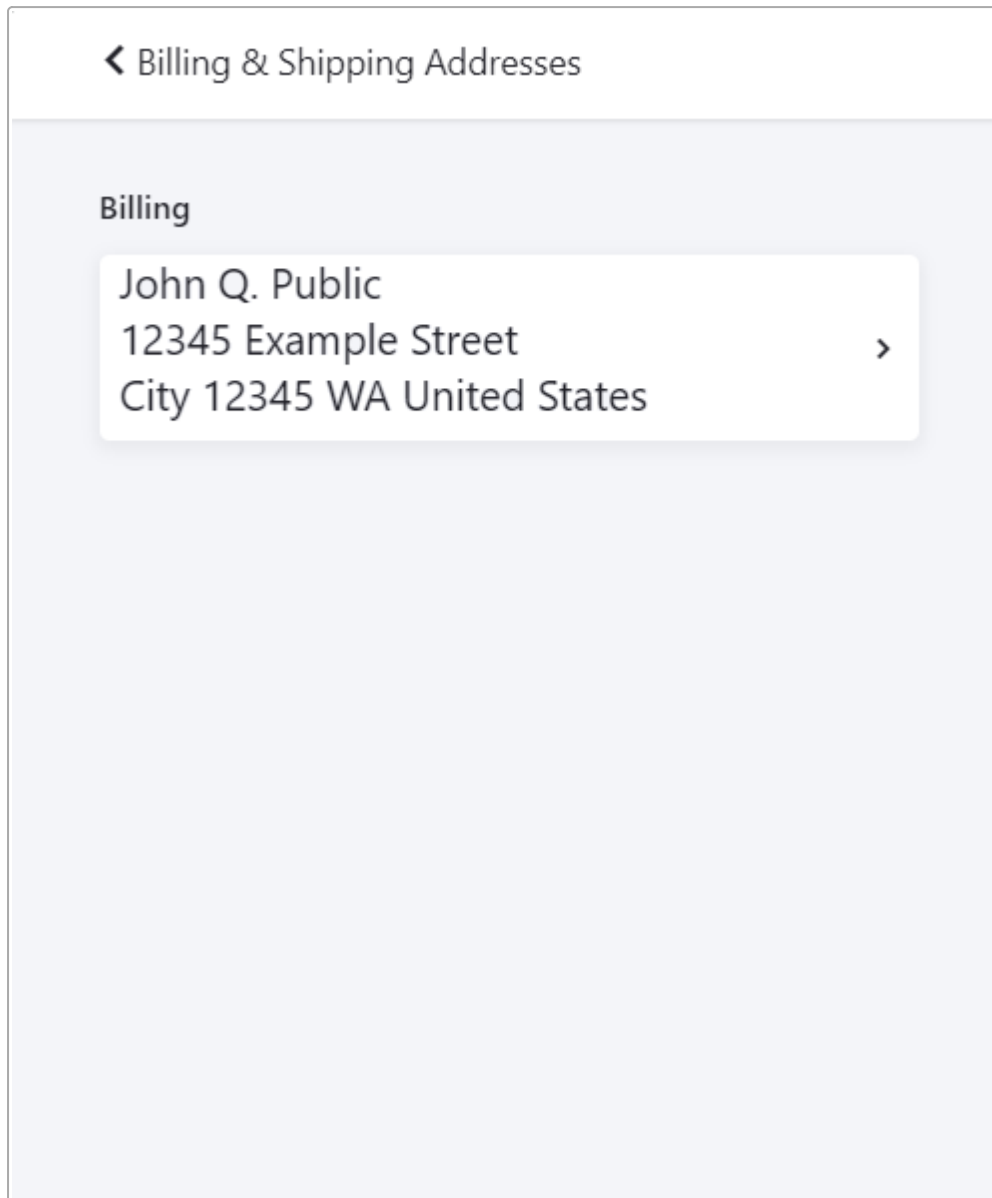
>

Change Password

3. Enter your new password, then enter it again to confirm it.

Billing Details

1. Click Edit Billing Details to change your billing address.



Billing and Shipping Addresses



2. Select the billing address that you want to change.
3. Enter the new information and select Update to change it.

#### Payment Details

When you purchase a PRTG Hosted Monitor subscription, you need your payment information.


1. Enter your payment details and billing details here to save them for later use or edit details you already entered.

← Add a payment method

Card Number	
Expiry	CVV 
Address Line1	
Address Line2 (Optional)	
City	Zip
State	Country Pick an option 

I authorize Paessler AG to save this payment method and automatically charge this payment method whenever a subscription is associated with it.

**Add**

 You may be redirected to your bank page for 3D secure verification.

Add a Payment Method

2. Click Add to add the new payment details.

## Invoices

Here you can view and download all of your invoices.



Invoices

Invoice	Date ↓	Price	Download
^ Invoices from 2023			
Trial Plan	8/4/2023	\$0.00	
Trial Plan	3/5/2023	\$0.00	

Invoices

## Upload

Here you can upload custom [device templates](#) and [custom files](#).

File Upload

Select your PRTG subscription  
my-instance.my-prtg.com

**INSTANCE READY**

**Custom Device Templates**

You can [create your custom device templates](#) in an existing PRTG installation, save it and upload it to your PRTG Hosted Monitor instance. Alternatively, you can use predefined community-made custom device templates that are available at the [PRTG Sensor Hub](#) and [Gitlab](#).

**Note:** Paessler carefully checked and selected the custom device templates. However, they are not officially supported. Do not expect all templates to work properly.

Select the device templates that you want to upload

UPLOAD

**My Custom Files**

Upload your custom files. Upload your own [created custom device templates](#) here if the predefined custom templates you need are not available in the list above.

**You cannot upload files that are larger than 1MB.**

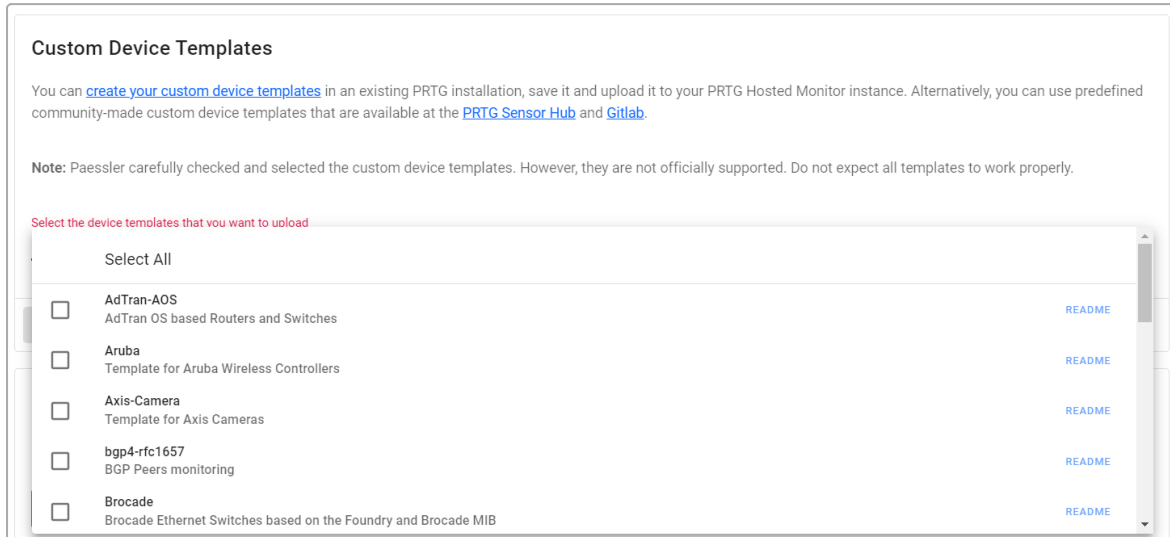
- MIB/ .MIB, .mib, .my
- devicetemplates/ .odt
- lookups/custom/ .ovl
- snmplibs/ .oidlib
- webroot/icons/devices/ .svg, .png

UPLOAD

Upload

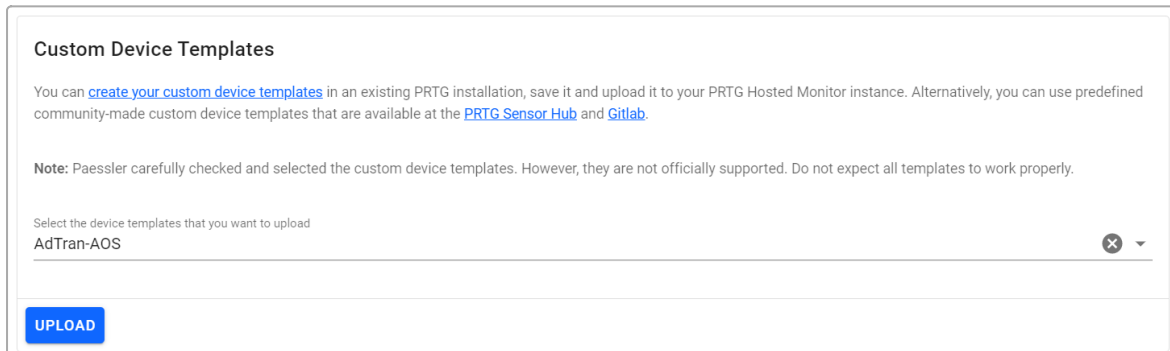
### Upload Device Templates

1. Click Select your PRTG subscription to select the subscription for which you want to upload files.
2. Click Select the device templates that you want to upload to select one or more device templates.



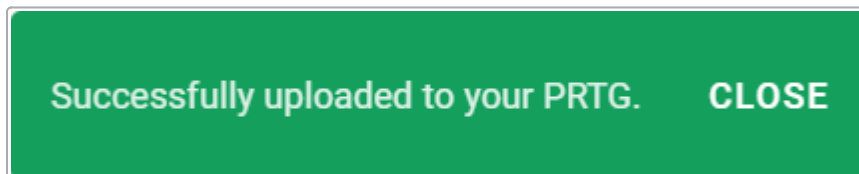
Device Templates

3. Enable the check box next to one or more device template names to select them.  
**i** You can also click Readme to open the README.md file of the device template in [GitLab](#).
4. Click outside of the dropdown list to continue.



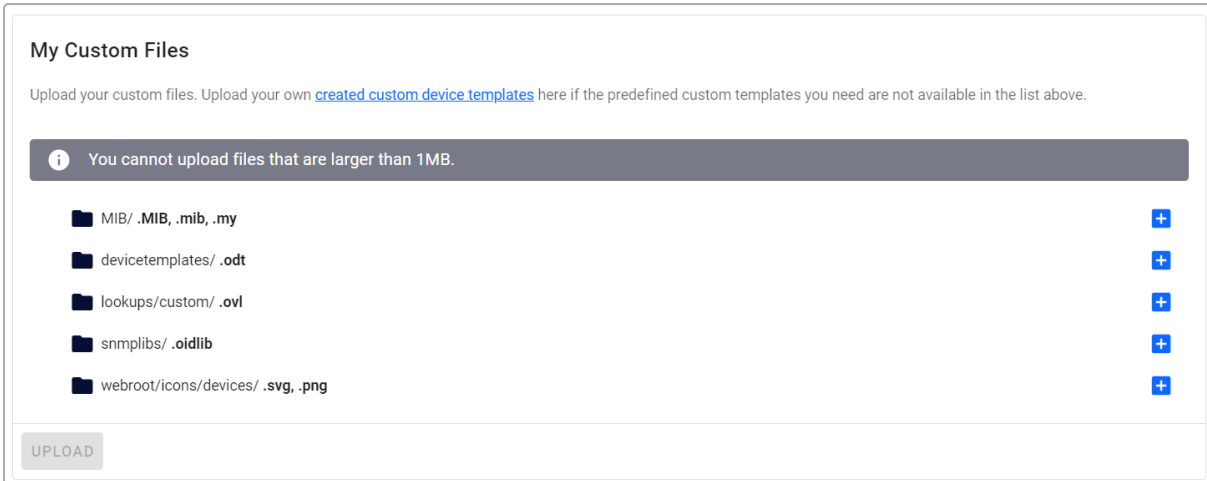
Upload File

5. Click Upload to upload the device templates.




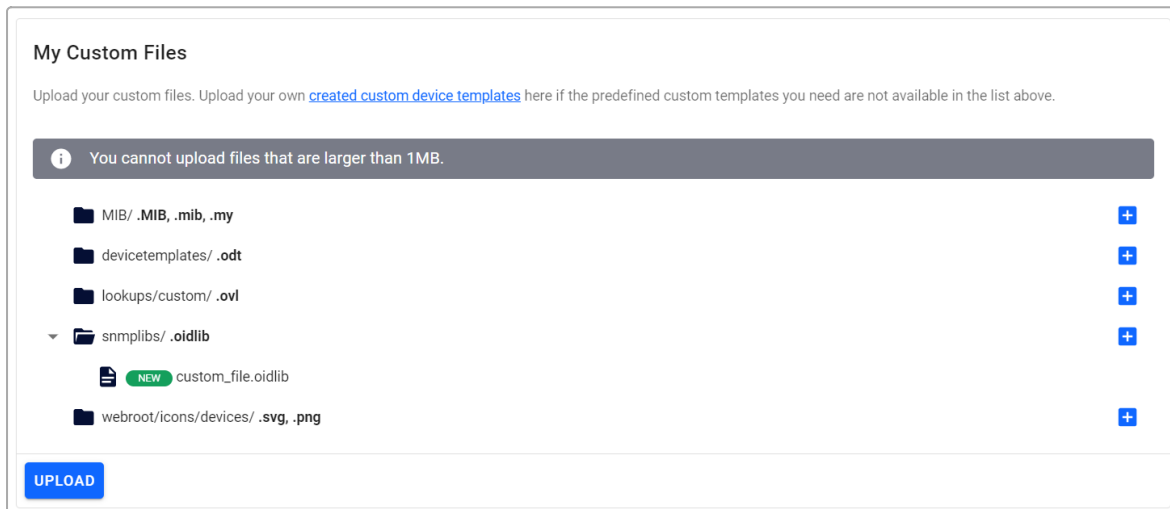
Device Template Upload Successful

### Upload Custom Files



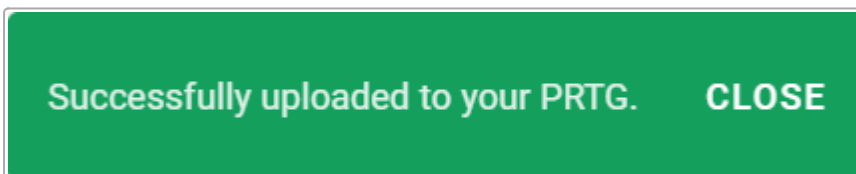
Custom Files

1. Click  next to the type of file that you want to upload and browse for the path to the file in the File Explorer.
2. Select the file and click Open.



Custom File

3. Click Upload to upload the custom device template files.



Custom File Upload Successful

## Logout

Click Logout in the upper-right corner to log out of your PRTG Hosted Monitor account.

## More

### ■ KNOWLEDGE BASE

Can I enable multi-factor authentication for my PRTG Hosted Monitor instance?

- <https://kb.paessler.com/en/topic/88234>

How to integrate Microsoft Entra ID into PRTG Hosted Monitor?

- <https://kb.paessler.com/en/topic/91634>

### 3.3 Use Multi-Factor Authentication with PRTG Hosted Monitor

You can use multi-factor authentication with PRTG Hosted Monitor. In combination with an authenticator app that supports the Time-based One-time Password algorithm (TOTP), such as Google Authenticator, you can make your PRTG Hosted Monitor instance even more secure.

☁ Multi-factor authentication is only available in PRTG Hosted Monitor. For more information, see the Knowledge Base: [Can I enable multi-factor authentication for my PRTG Hosted Monitor instance?](#)

In this section:

- [Initial Setup](#) <sup>79</sup>
- [Manually Enter the QR Code](#) <sup>84</sup>
- [Log In With Multi-Factor Authentication](#) <sup>84</sup>
- [Disable Multi-Factor Authentication](#) <sup>85</sup>
- [Use The Recovery Code](#) <sup>86</sup>

#### Initial Setup

To set up multi-factor authentication for your PRTG Hosted Monitor instance, open a web browser, go to the [PRTG Hosted Monitor Customer Portal](#), and log in. Then click your account in the upper-right corner.

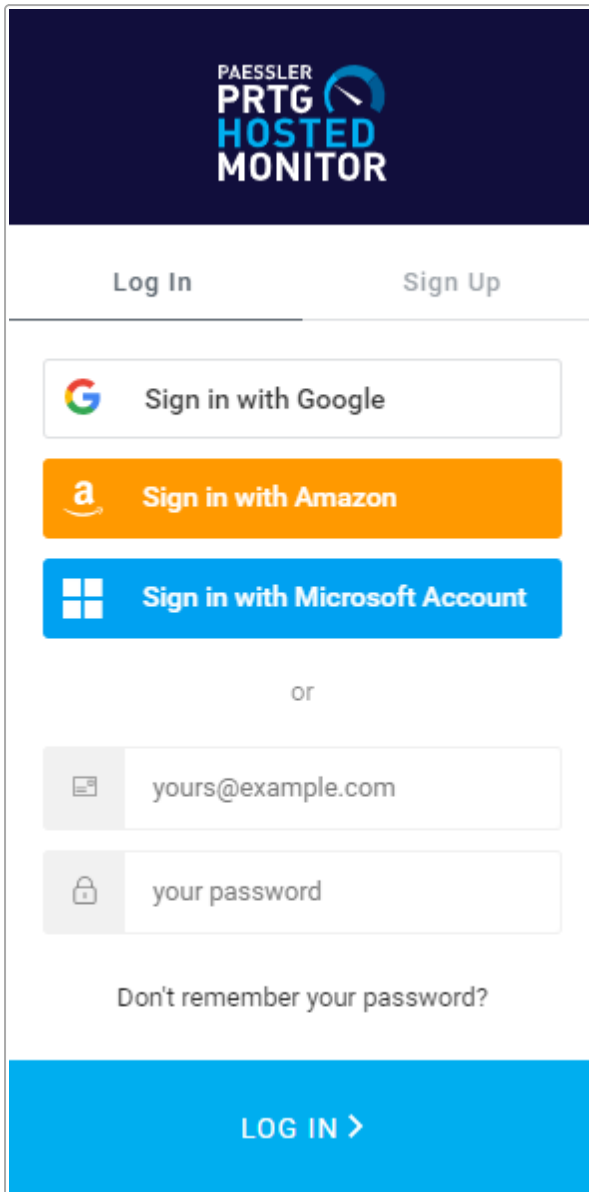
ⓘ We recommend that you use Google Chrome 75.

ⓘ You can only enable multi-factor authentication for your own user account here. To enable or disable multi-factor authentication for all users of your PRTG Hosted Monitor instance, go to [Manage Subscription](#). For more information, see section [Manage a PRTG Hosted Monitor Subscription](#) <sup>67</sup>.

The screenshot shows the 'Account Overview' page for a user with the email 'johnqpublic@example.com'. The page is titled 'Account' and features a navigation sidebar on the left with icons for home, settings, and user profile. The main content area is divided into two sections. The first section, titled 'Auth0', states that the account is managed and secured by the third-party service Auth0. It displays the user's email, provider (auth0), and user ID (123456789abcde1234567890). A toggle switch for 'Multi-factor authentication' is currently off, with a note that enabling it requires a login. A 'RESET PASSWORD' button is located below this section. The second section, titled 'Chargebee', states that all billing and payment details are managed and secured by the third-party service Chargebee. It includes 'EDIT BILLING DETAILS' and 'EDIT PAYMENT DETAILS' buttons. At the bottom, there is a privacy notice: 'I accept the transfer of my data for the purpose of invoicing to Stripe Inc. and Chargebee Inc. If you want to delete your whole account or just your credit card or billing details, please contact our Support.'

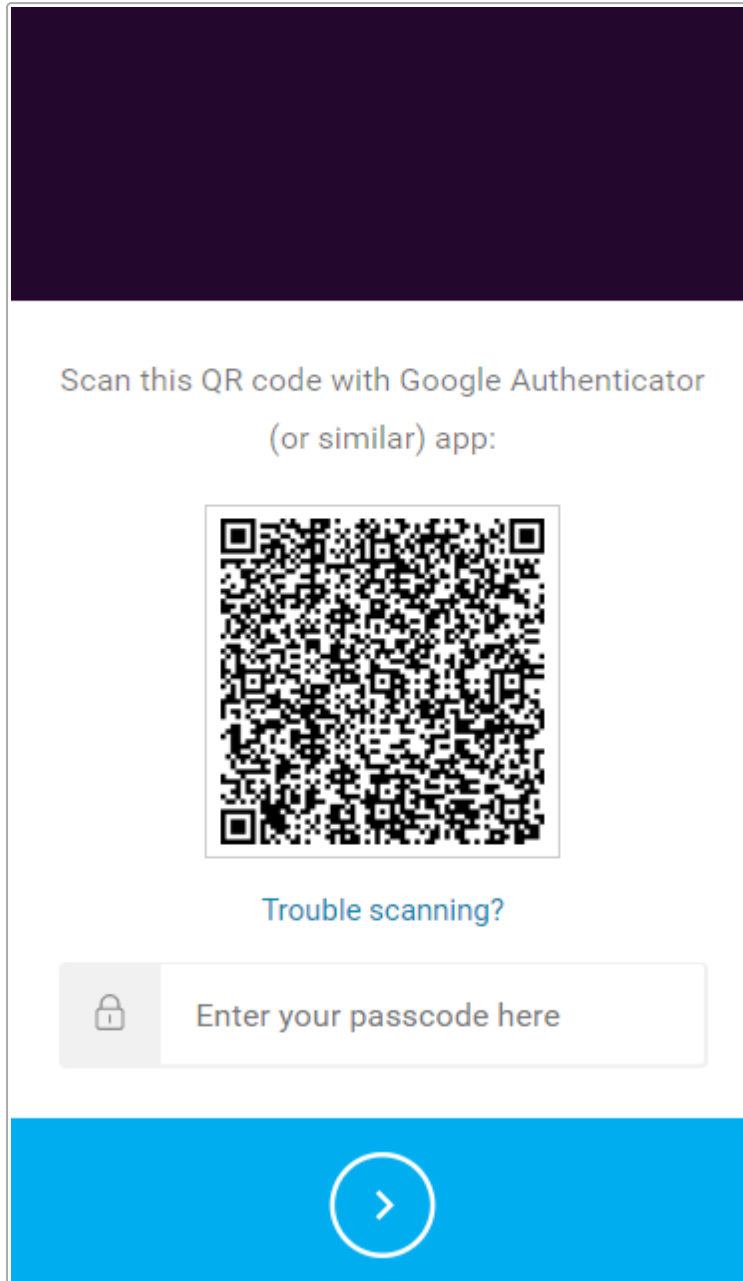
Account Overview

1. To enable multi-factor authentication, click .  
 If you enable multi-factor authentication for the first time, you must log in again.




Login Screen

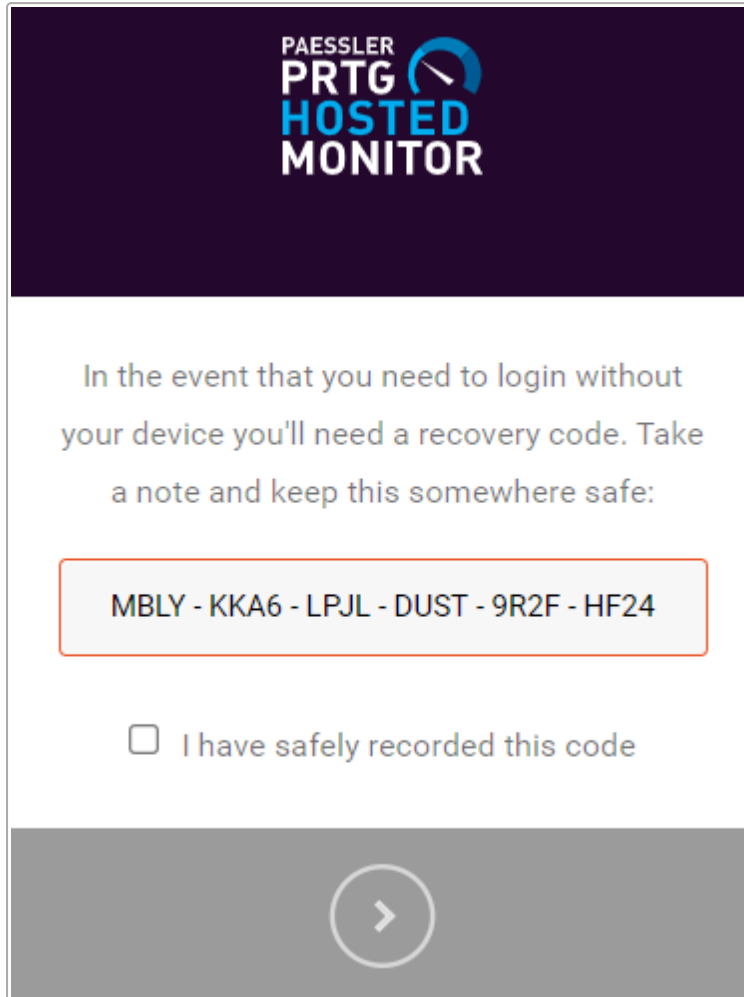
2. Provide the credentials you entered when you signed up and click Log In, or use single sign-on (SSO) and continue with your Google, Amazon, or Windows account via the respective button. For more information on this, see the Knowledge Base: [How to integrate Microsoft Entra ID into PRTG Hosted Monitor?](#)





Scan QR Code



3. Scan the QR code with your authenticator app and enter the passcode from the authenticator app in the field below the QR code.  
■ If your authenticator app is unable to scan the code, see [Manually Enter the QR Code](#)  for more information.

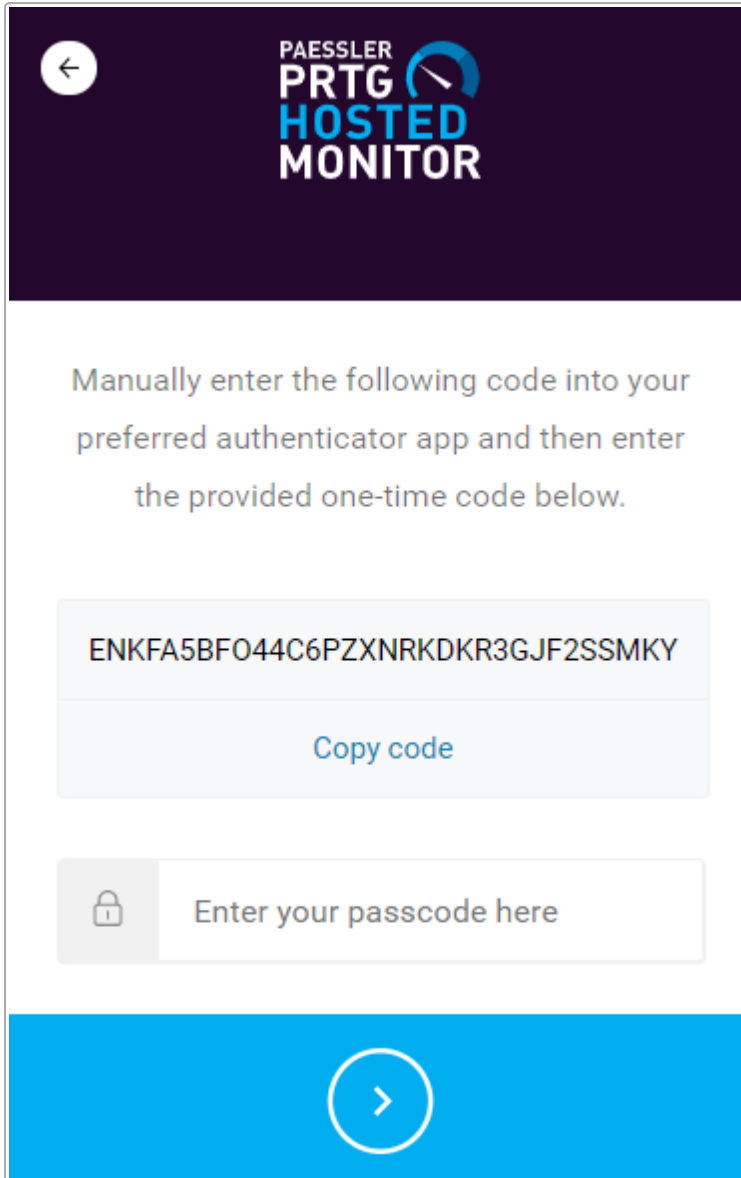


Recovery Code


4. You receive a recovery code. Make sure to save it somewhere safe. Click the check box to confirm that you have safely recorded the code.
5. Click  to log in to the [PRTG Hosted Monitor Customer Portal](#).
-  If you lose your recovery code, [contact the Paessler support team](#).

## Manually Enter the QR Code

1. If your authenticator app is unable to scan the QR code, click [Trouble scanning?](#)

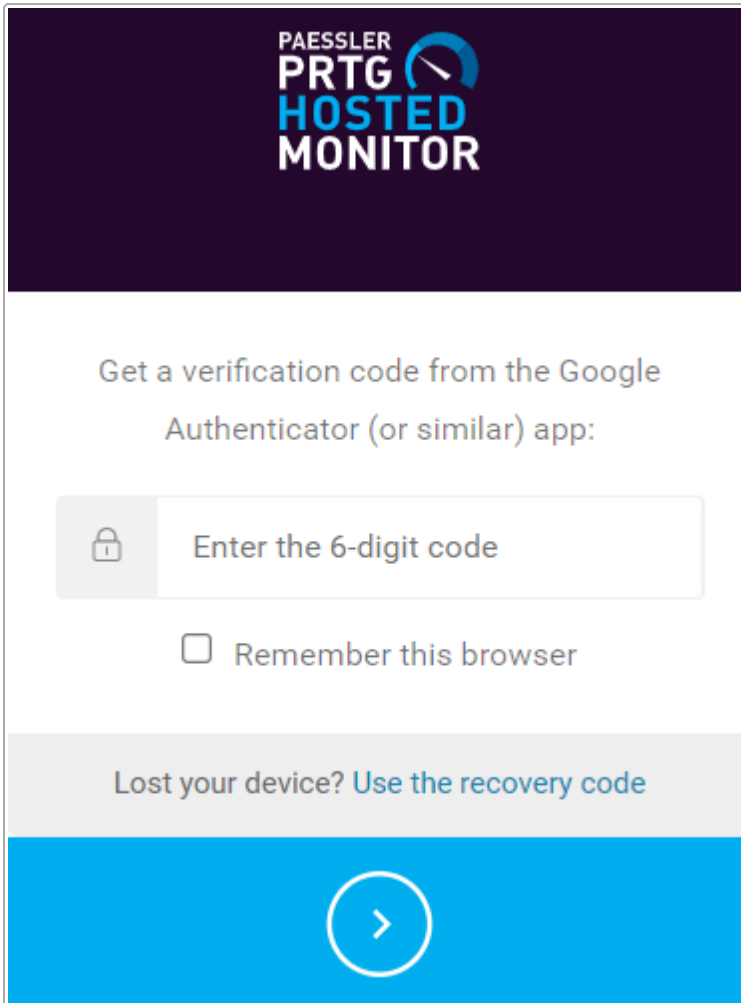


Manually Enter the QR Code



2. Follow the instructions in your authenticator app to manually enter the code.
3. Enter the one-time passcode that your authenticator app generates in the [Enter your passcode here](#) field.
4. Click  to continue.

## Log In With Multi-Factor Authentication

After you set up multi-factor authentication, the next time you log in to the [PRTG Hosted Monitor Customer Portal](#), you see an additional login screen.




Log In With Multi-Factor Authentication

1. Enter the 6-digit code from your authenticator app.
  2. Select the check box next to Remember this browser if you do not want to enter the code in this browser every time you log in.
    - ⓘ This applies for 30 days. If you clear your browsing data such as cookies during this time, it no longer applies.
  3. Click  to continue.
- ⓘ If you lose your device, see [Use The Recovery Code](#)  for more information.

## Disable Multi-Factor Authentication

To disable multi-factor authentication, follow these steps:

1. Log in to the [PRTG Hosted Monitor Customer Portal](#).
2. Click your account in the upper-right corner.
3. Click  under Multi-Factor Authentication.

You see the following message.

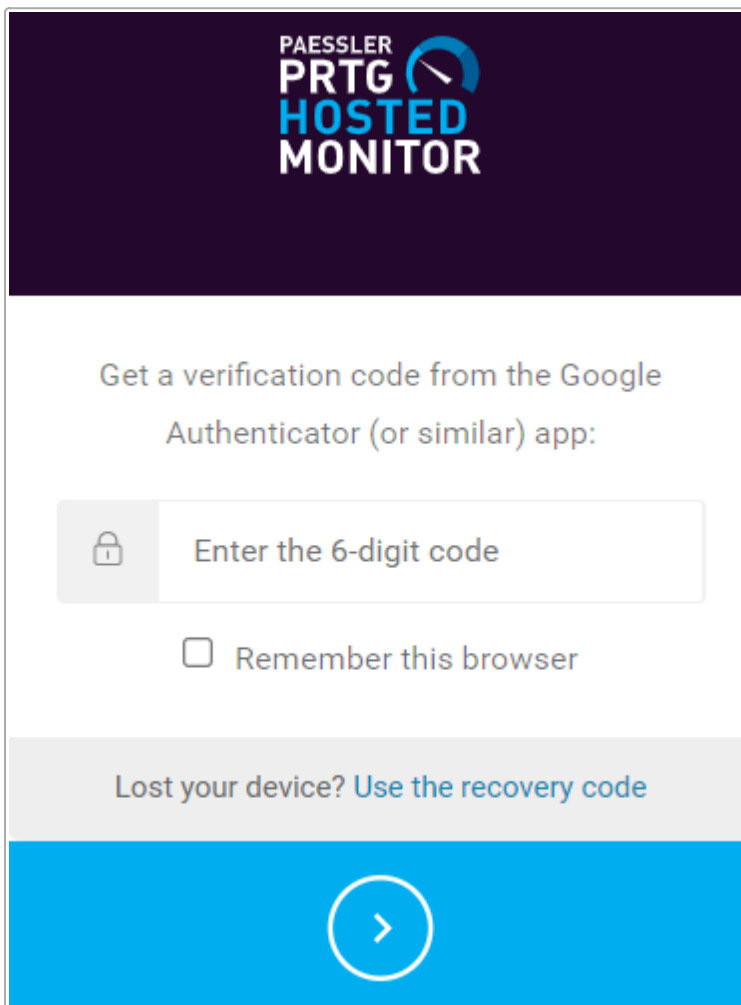
Multi-factor authentication is now disabled. **CLOSE**

Multi-Factor Authentication Now Disabled

The next time you log in to the PRTG Hosted Monitor Customer Portal, multi-factor authentication is no longer enabled.

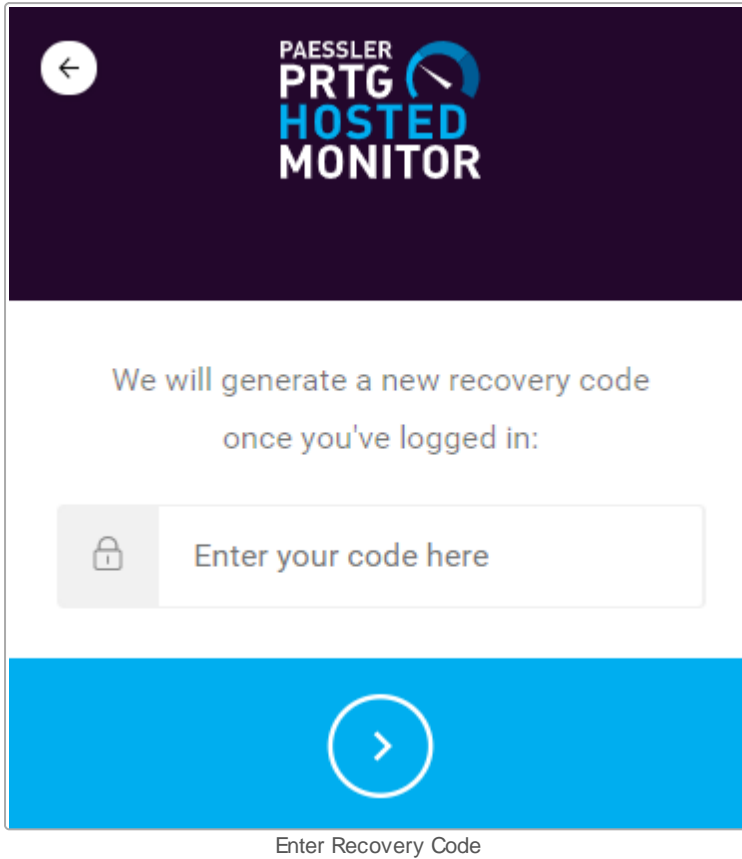
### Use The Recovery Code



1. If you lose your device, click Use the recovery code on the login screen.



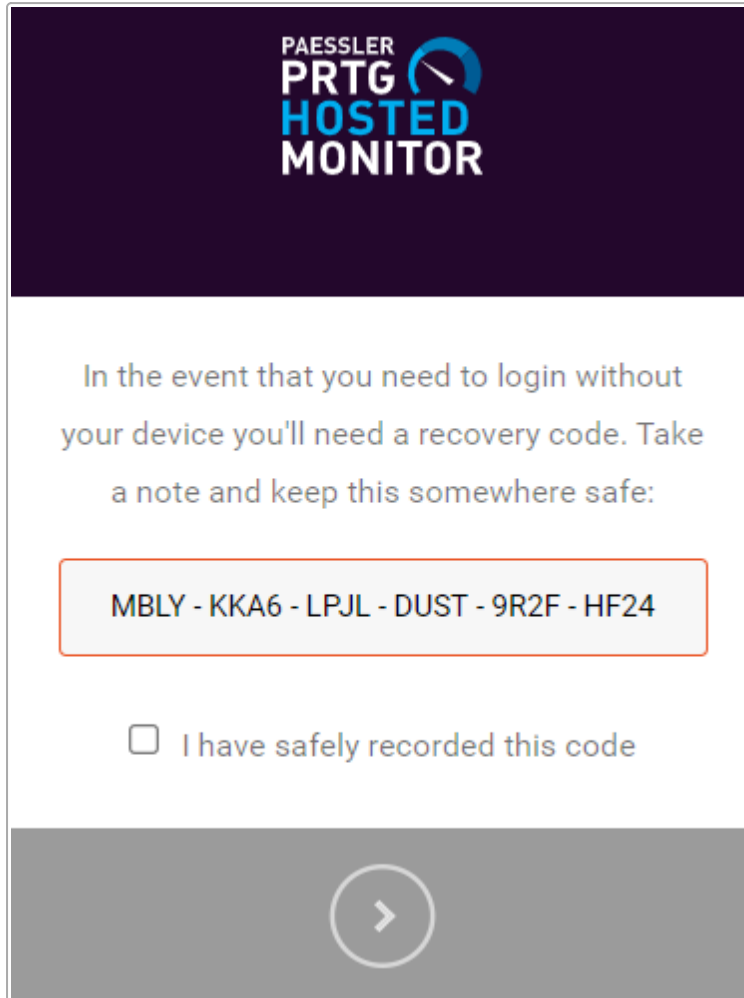
Log In With Multi-Factor Authentication

You see the following screen.




2. Enter your recovery code and click  to continue.  
 The recovery code must contain 24 alphanumeric characters.

3. You receive a new recovery code.



Recovery Code

4. Make sure to save the recovery code somewhere safe. Click the check box to confirm that you have safely recorded the code.
5. Click  to log in to the [PRTG Hosted Monitor Customer Portal](#).
- ① If you lose your recovery code, [contact the Paessler support team](#).

## More

### ■ KNOWLEDGE BASE

Can I enable multi-factor authentication for my PRTG Hosted Monitor instance?

- <https://kb.paessler.com/en/topic/88234>

How to integrate Microsoft Entra ID into PRTG Hosted Monitor?

- <https://kb.paessler.com/en/topic/91634>

# Part 4









## Installing the Software

## 4 Installing the Software

The following sections show you how to download and install PRTG Network Monitor.

☁ If you want to use PRTG Hosted Monitor, go straight to section [Create a PRTG Hosted Monitor Instance](#) to get started.

In this section:

- [Download PRTG](#)  <sup>91</sup>
- [Update from Previous Versions](#)  <sup>92</sup>
- [Install a PRTG Core Server](#)  <sup>94</sup>
- [Install a Cluster](#)  <sup>101</sup>
- [Enter a License Key](#)  <sup>102</sup>
- [Activate the Product](#)  <sup>104</sup>
- [Install a Remote Probe](#)  <sup>106</sup>
- [Uninstall PRTG Products](#)  <sup>119</sup>



## 4.1 Download PRTG

Download the latest stable version of PRTG from the [Paessler website](#) as a [trial version](#)<sup>[20]</sup>. Buy and manage your license at the [Paessler Portal](#).



The banner features the Paessler PRTG Network Monitor logo at the top left. The main text reads 'PRTG Download' in a large, white, sans-serif font, followed by 'One solution to monitor everything' in a slightly smaller font. Below this, it states 'Unlimited use of PRTG for 30 days free of charge.' A prominent orange button with the text 'FREE DOWNLOAD' is centered. At the bottom, it clarifies: 'Unlimited use of PRTG for 30 days. After 30 days PRTG reverts to the freeware edition. You can upgrade to a paid license at any time.'

Download PRTG

 Once you have installed PRTG, the [auto-update](#)<sup>[20]</sup> automatically downloads and installs new software versions.

## 4.2 Update From Previous Versions

If you have a previous PRTG version installed, there are several things you need to consider before you update to the newest PRTG version. See also the [system requirements](#)<sup>[22]</sup> for all requirements.

**i** While in most cases, your monitoring data and configuration are maintained when you update PRTG, we still recommend that you have a backup of both. For more information, see the Knowledge Base: [How do I back up all data and configuration of my PRTG installation?](#)

**i** In certain cases, antivirus software like Windows Defender interferes with the PRTG installer. This might cause high CPU load on the PRTG core server, which might prevent an update. Temporarily disable Windows Defender and other antivirus software if you have issues when you install PRTG updates.

**☁** On PRTG Hosted Monitor instances, updates are managed automatically, so you do not need to do them manually.

In this section:

- [Update to PRTG 22.2.77](#)<sup>[92]</sup>
- [Update from PRTG 16.1.22 or later](#)<sup>[92]</sup>
- [Update from Older PRTG Products](#)<sup>[93]</sup>

### Update to PRTG 22.2.77

As of PRTG 22.2.77, PRTG is signed with renewed certificates. To seamlessly update to any version as of PRTG 22.2.77, an [intermediate update](#) is required for the PRTG core server and all probes if you run a version previous to PRTG 22.1.75. If you auto-update from previous versions which are lower than PRTG 22.1.75, PRTG automatically installs an intermediate version first. The intermediate version you receive via auto-update or from the Paessler support team is PRTG 22.1.75.1594. You must perform an additional auto-update to install the newest version. PRTG notifies you with a [ticket](#)<sup>[213]</sup> about this. Your configuration is kept.

**i** We recommend that you use the auto-update to install the newest PRTG version.

### Update from PRTG 16.1.22 or later

If you run any version as of PRTG 16.1.22 or later, [install](#)<sup>[94]</sup> the newest version on top of the previous version. Your configuration is kept. PRTG automatically updates [classic remote probes](#)<sup>[3198]</sup> as well. If you have configured PRTG as a [failover cluster](#)<sup>[128]</sup>, you only need to install an update on any cluster node (master node or failover node). PRTG automatically deploys the new version to the cluster.

We recommend that you use the [auto-update](#)<sup>[2969]</sup> to install the newest version. Always make sure that you have a proper backup of your monitoring data.

**i** Important notes:

- PRTG 19.3.52: PRTG does not run on Windows XP anymore. Make sure that you install PRTG on an [officially supported operating system](#)<sup>[26]</sup>.
- PRTG 19.1.48: Sensors that require the .NET framework need .NET 4.7.2 or later. For more information, see the Knowledge Base: [Which .NET version does PRTG require?](#)

- PRTG 18.3.43: PRTG does not run on Windows Server 2003 R2 anymore. Make sure that you install PRTG on an officially supported operating system.
- PRTG 17.3.34: This version comes with a completely rewritten PRTG web interface. If you have customized the PRTG web interface with one of the dedicated files in a previous version, all your customizations are lost as soon as you install PRTG 17.3.34. You must redo your changes to keep the customizations.
- PRTG 16.3.26: The Mobile Web GUI was removed from PRTG.
- PRTG 16.2.25: Several sensors were removed from PRTG.

## Update from Older PRTG Products

For more information on updating from older PRTG versions, see the Knowledge Base: [How do I update from older versions?](#)

## More

### KNOWLEDGE BASE

How do I back up all data and configuration of my PRTG installation?

- <https://kb.paessler.com/en/topic/523>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Why do I get an error message when trying to restart Windows Server 2019 after a PRTG update?

- <https://kb.paessler.com/en/topic/86854>

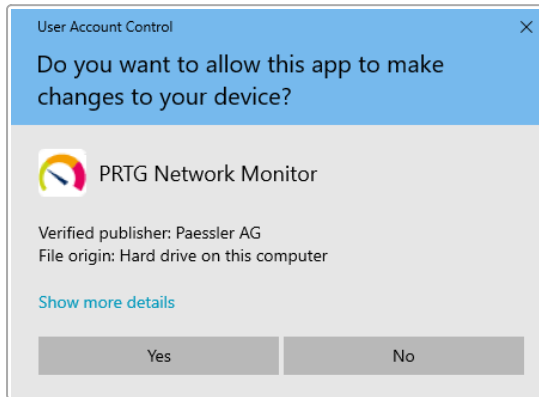
How do I update from older versions?

- <https://kb.paessler.com/en/topic/91395>

## 4.3 Install a PRTG Core Server

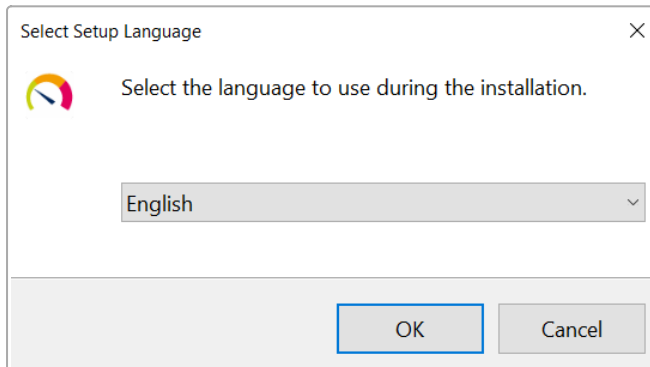
Installing PRTG Network Monitor works like other Windows-based applications. To install PRTG, run the installation setup program from the .zip file that you downloaded.

1. Confirm the question of the [Windows User Account Control](#) with Yes to allow PRTG to install. The installation dialog guides you through the installation process.



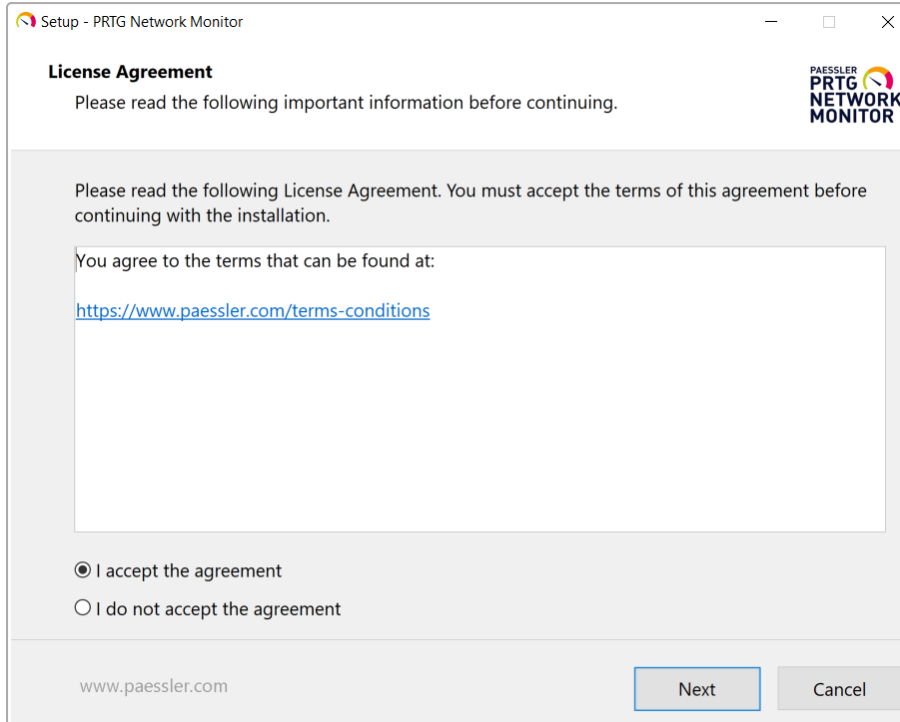
Windows User Account Control Confirmation Request

2. Select a language for the installation and click OK. The available language options depend on both your Windows version and the setup file.

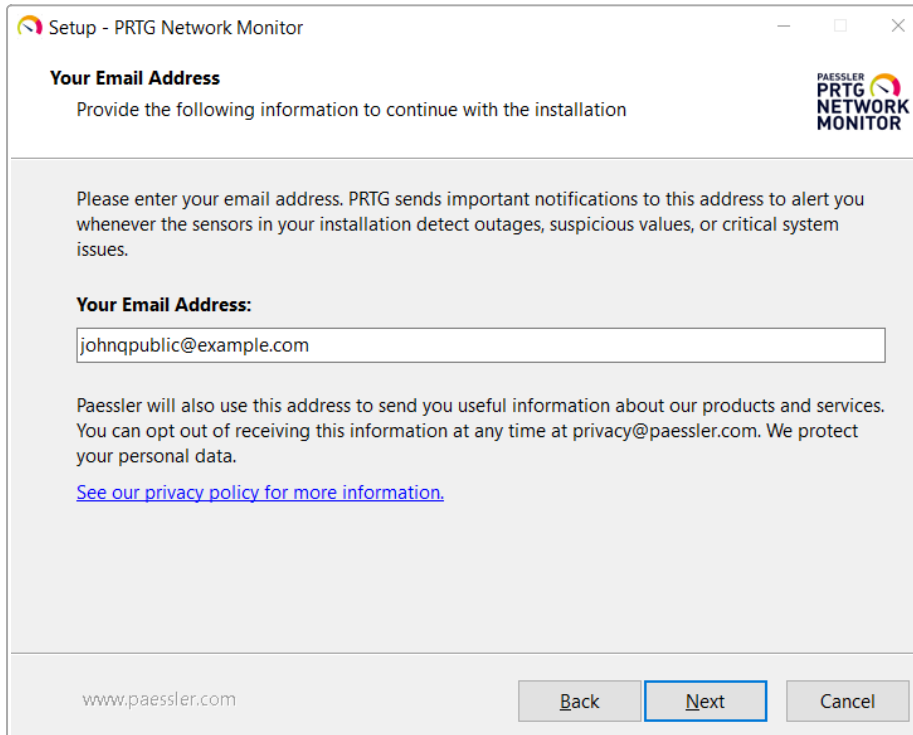


Setup Language Selection

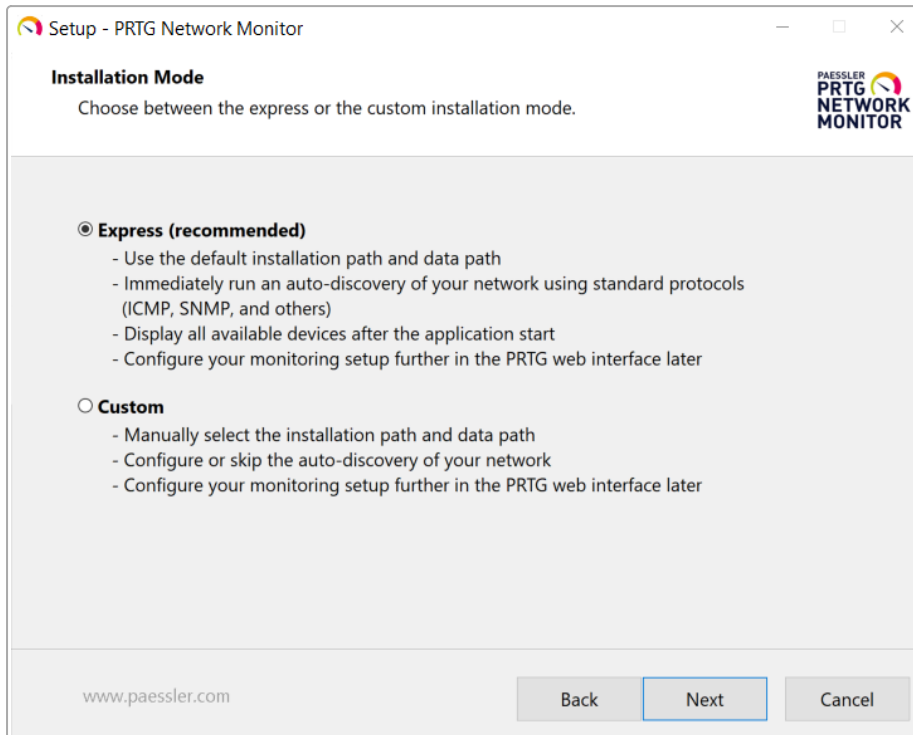
3. Accept the [license agreement](#) and click Next.



4. Enter your email address to make sure you receive important system alerts and click Next.

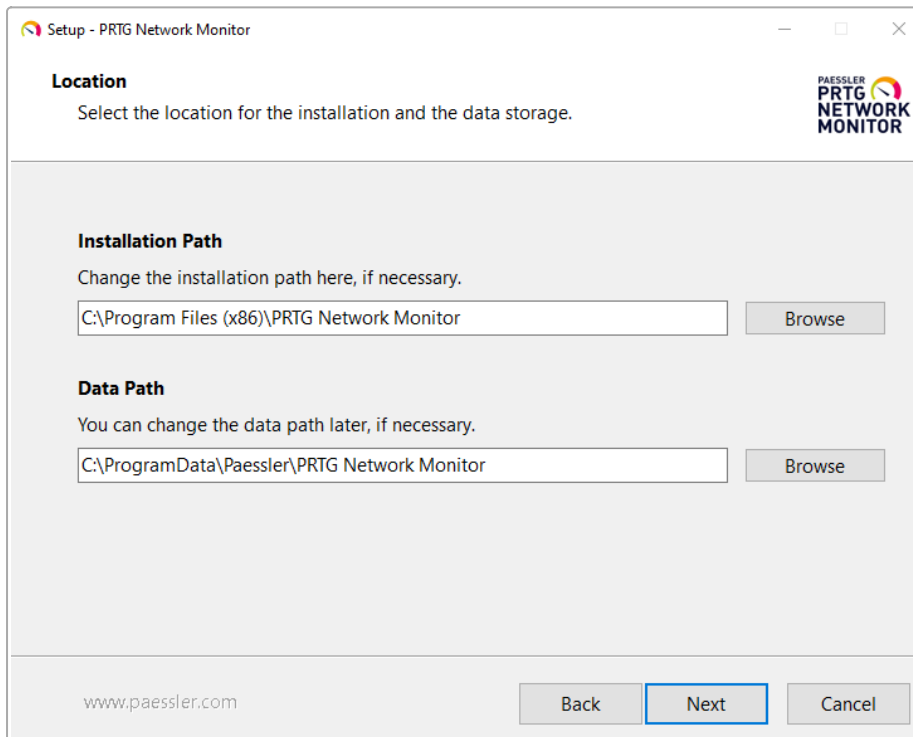


5. Select if you want to use the Express or the Custom installation mode and click Next. If you select the Express installation mode, you can directly proceed with step 9.



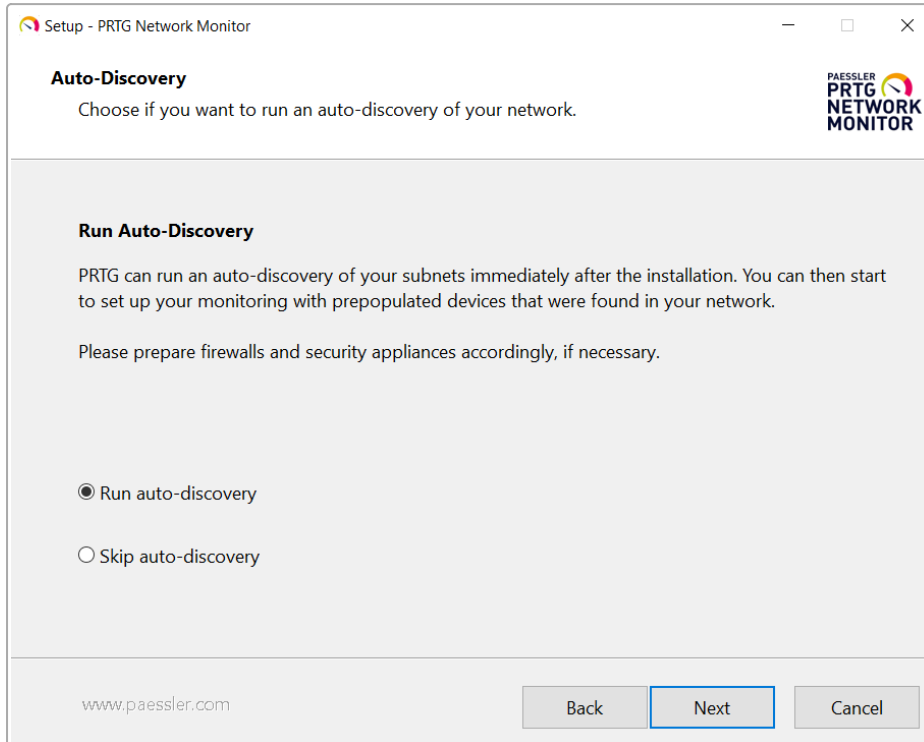
Setup Dialog: Installation Mode

6. This page is only visible if you use the Custom installation mode. You can change the paths to the [PRTG program directory and PRTG data directory](#), if necessary. Click Next.



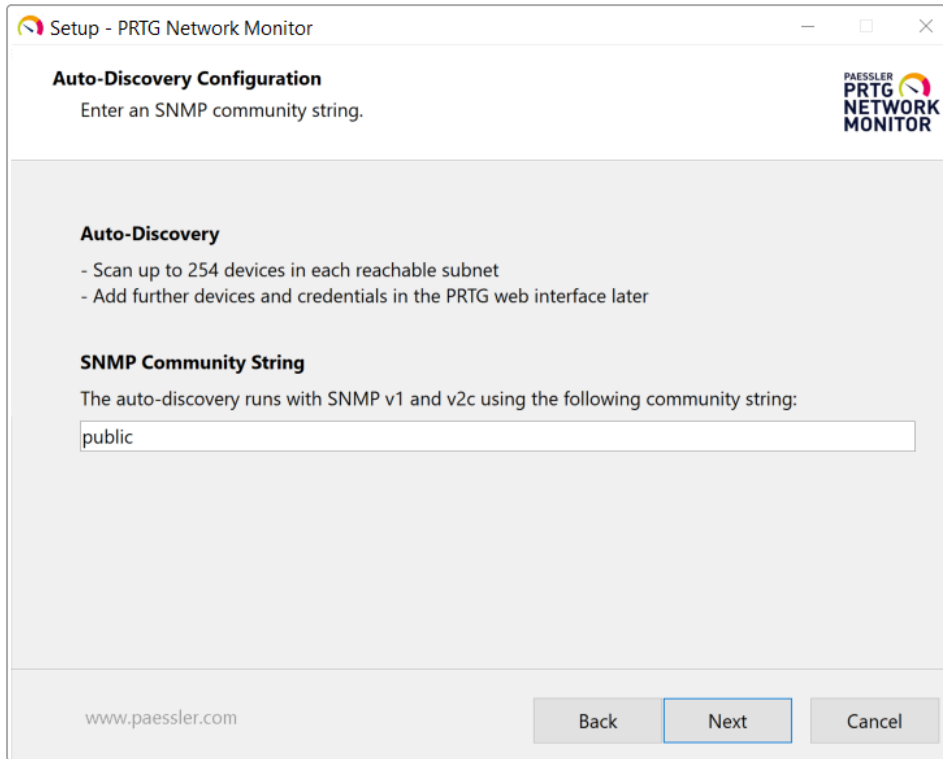
Setup Dialog: Location for Installation and Data Storage

7. This page is only visible if you use the Custom installation mode. Select if you want to run an [auto-discovery](#) of your network or if you want to skip the auto-discovery. Click Next.



Setup Dialog: Run or Skip Auto-Discovery

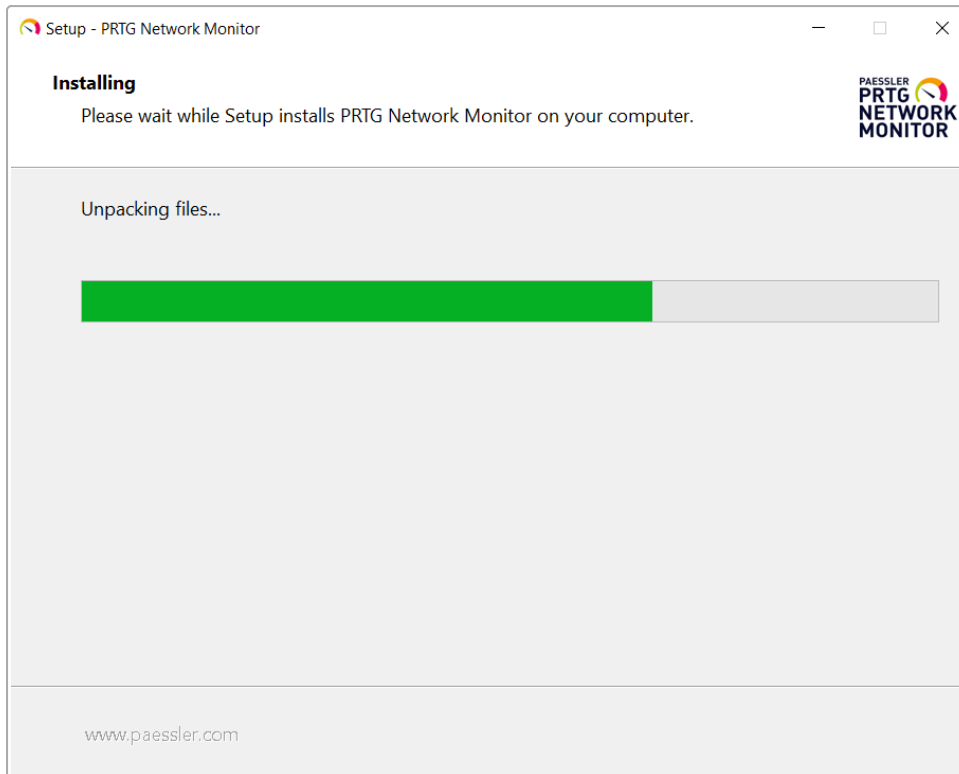
- This page is only visible if you select Run auto-discovery. You can enter a Simple Network Management Protocol (SNMP) community string. The default SNMP community string is **public**. Click Next.



Setup Dialog: Auto-Discovery Configuration



9. PRTG is installed on your system.



Setup: Installing PRTG

10. Click Finish to complete the setup of PRTG.

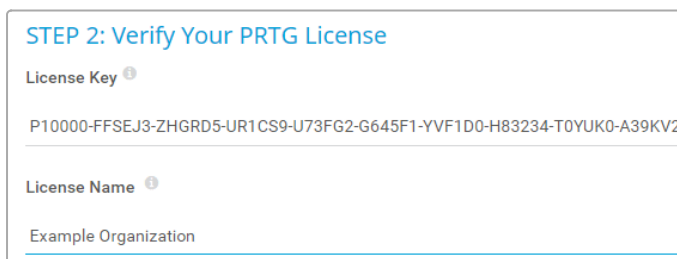
After installation, you can open the [PRTG web interface](#)<sup>[152]</sup> in your system's default browser. Make sure that a [supported browser](#)<sup>[22]</sup> is available on the system.

**i** In some cases, antivirus software like Windows Defender interferes with the PRTG installer. This might cause high CPU load on the PRTG core server, which might prevent a successful installation. Temporarily disable Windows Defender and other antivirus software in these cases.

## Enter License Information

PRTG validates your license information during the installation process by connecting to the activation server. If there are issues with the license information, PRTG asks you to verify your License Key and License Name on the first login.

Enter the License Key and, if prompted, the License Name exactly as received from Paessler.



Setup Dialog: Enter License Information

■ For more information, see section [Enter a License Key](#)<sup>[102]</sup>.

If you think that you have correctly entered your license information but get a [License Invalid](#) message, contact [sales@paessler.com](mailto:sales@paessler.com).

❶ You can find the label License Owner in some documents from the Paessler Portal. License Owner is the same as License Name. PRTG might ask you for this information during installation or when you [change your license key](#)<sup>[102]</sup>.

❶ When you update a commercial version with a new trial installer, PRTG ignores the new trial license key.

## More

### ■ KNOWLEDGE BASE

I cannot open the PRTG web interface via the desktop shortcut anymore. What can I do?

- <https://kb.paessler.com/en/topic/89024>

How can I establish a secure web interface connection to PRTG?

- <https://kb.paessler.com/en/topic/273>

PRTG blocks port 80 although I'm using SSL on port 443. How to free port 80?

- <https://kb.paessler.com/en/topic/5373>

### ■ PAESSLER WEBSITE

Terms and conditions of Paessler GmbH

- <https://www.paessler.com/terms-conditions>

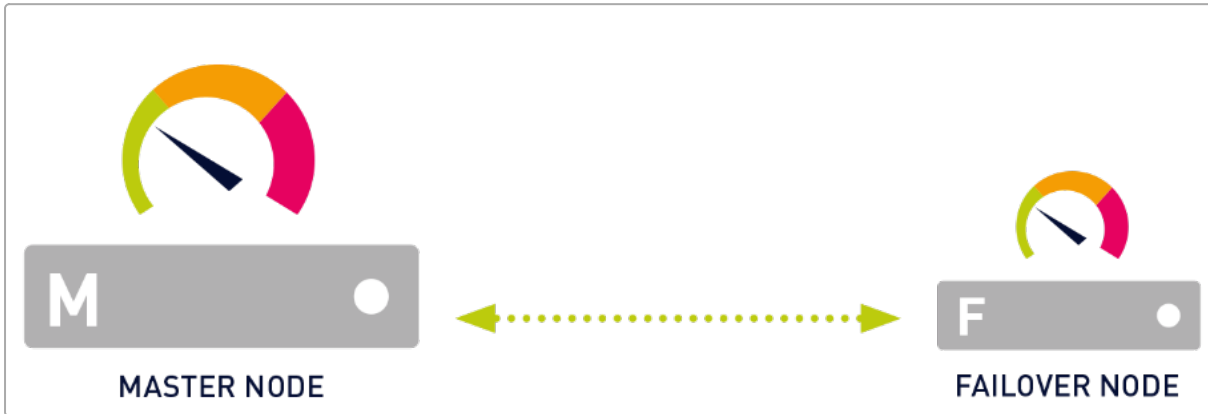
Privacy policy

- <https://www.paessler.com/privacy-policy>

## 4.4 Install a Cluster

PRTG offers one single failover cluster in all licenses, including the freeware edition. A single failover cluster consists of two machines, **master node** and **failover node**. Each machine runs one installation of PRTG. They are connected to each other and exchange configuration and monitoring data. You can run a cluster with up to five cluster nodes.

☁ This feature is not available in PRTG Hosted Monitor.



■ For more information, see section [Failover Cluster Configuration](#) 3208.

### More

#### ■ KNOWLEDGE BASE

What is the clustering feature in PRTG?

- <https://kb.paessler.com/en/topic/6403>

## 4.5 Enter a License Key

The license information consists of a License Key and the License Name. The License Key is a string that consists of 10 blocks with six characters each.

License Information	Example
License Key	P10000-FFSEJ3-ZHGRD5-UR1CS9-U73FG2-G645F1-YVF1D0-H83234-T0YUK0-A39KV2
License Name	Example Organization

### Your License Information

For the trial edition and freeware edition, you receive the required license information on the Paessler web page when you download the trial edition of PRTG. When you install the trial edition, you usually do not need to manually enter your license key, as the installation setup program extracts all the necessary information from the file name. If the installer cannot extract the information from the file name or if other issues occur, you might need to enter your license information manually.

For the commercial edition, you receive your license information from Paessler via email or in a license document in the [Paessler Portal](#). When you install the commercial edition, PRTG asks you to enter your license information during the setup process. We recommend that you copy and paste the information.

**i** If there are issues with the license information, PRTG asks you to verify your license information on the first login.

**i** You can find the label License Owner in some documents from the Paessler Portal. License Owner is the same as License Name. PRTG might ask you for this information during installation or when you [change your license key](#)<sup>[102]</sup>.

**■** For more information about the different licenses, see section [Available Licenses](#)<sup>[20]</sup>.

### Change License Key

Because PRTG already asks for a license key during installation, you usually do not need to manually enter one afterward. However, there are still scenarios where you need to change your license key and activate the respective license. For example, you must provide the subscription license key of your commercial edition if you upgrade from a freeware edition or trial edition, or if you want to upgrade your subscription license to one with a higher sensor count.

To enter a new license key, follow these steps:

1. Log in to the [PRTG web interface](#)<sup>[124]</sup>.
2. Select Setup | License Information from the [main menu bar](#)<sup>[250]</sup>.
3. Click Change License Key. The Update Your License page appears where you can activate your new license.

4. Select the activation type Automatic (online activation with optional HTTP proxy) if your PRTG core server can connect to the internet.

**i** Without internet access, you must select Manual (offline activation). The activation process works a bit differently in this case and requires manual interaction. See section [License Information](#) for more information.

5. Enter your license information and click Update License.

6. PRTG connects to the Paessler activation server on port 443 and validates your license.


If everything works fine, you see the message Activation was successful as License Status at the top of the page.

**i** The PRTG core server needs an internet connection on port 443 to activate. If a proxy connection is needed, see [step 3](#) on the Update Your License page. If the activation fails, you can also try an offline activation.

For more information, see section [License Information](#).

### License Information

License Status	Activation was successful
License Name	Example Organization
License Key	P10000-FFSEJ3-ZHGRD5-UR1CS9-U73FG2-G645F1-YVF1D0-H83234
System ID	SYSTEMID-AAAA1111-BBBB2222-3333CCCC-4444DDDD-5555EEEE
Customer ID	012345678
Licensed Edition	PRTG Network Monitor (next validation on 15/3/2024 at the latest)
Last Update	02/02/2024 13:21:54
Subscription until	07/05/2027 (1059 days left)
Number of Sensors	Unlimited



Manage License
Change License Key
Refresh Information
Deactivate this License

Update Your License: Click Change License Key

## More

### KNOWLEDGE BASE

How do I upgrade to a later edition of PRTG?


- <https://kb.paessler.com/en/topic/4193>

The automatic license activation of my PRTG Enterprise Monitor license does not work. What can I do?

- <https://kb.paessler.com/en/topic/89281>

## 4.6 Activate the Product

PRTG Network Monitor automatically activates your license via the internet during the installation process. If PRTG cannot access the activation server, you must manually activate your license.


 You must complete the product activation process once to use PRTG, otherwise it does not run. Do not forget to activate your subscription license when you want to upgrade your installation from a trial edition or freeware edition.

### Online Activation

Because PRTG already asks for a license key during installation, you usually do not need to manually enter one afterward. However, there are still scenarios where you need to change your license key and activate the respective license. For example, you must provide the subscription license key of your commercial edition if you upgrade from a freeware edition or trial edition, or if you want to upgrade your subscription license to one with a higher sensor count.

To enter a new license key, follow these steps:

1. Log in to the [PRTG web interface](#)<sup>[124]</sup>.
2. Select Setup | License Information from the [main menu bar](#)<sup>[250]</sup>.
3. Click Change License Key. The Update Your License page appears where you can activate your new license.
4. Select the activation type Automatic (online activation with optional HTTP proxy) if your PRTG core server can connect to the internet.

 Without internet access, you must select Manual (offline activation). The activation process works a bit differently in this case and requires manual interaction. See section [License Information](#)<sup>[296]</sup> for more information.

5. Enter your license information and click Update License.
6. PRTG connects to the Paessler activation server on port 443 and validates your license.

If everything works fine, you see the message Activation was successful as License Status at the top of the page.

 The PRTG core server needs an internet connection on port 443 to activate. If a proxy connection is needed, see [step 3](#)<sup>[296]</sup> on the Update Your License page. If the activation fails, you can also try an offline activation.

 For more information, see section [License Information](#)<sup>[296]</sup>.

### Offline Activation

 The following process only applies to PRTG Network Monitor. If you use PRTG Enterprise Monitor, see the Paessler website: [How to use PRTG Enterprise Monitor in an offline environment in 5 steps](#).


If no internet connection is available, you must activate PRTG manually:

1. In the PRTG web interface, select Setup | License Information from the main menu bar.

2. Click Change License Key. The Update Your License page appears where you can activate your license.
3. Select the activation type Manual (offline activation).
4. Enter your license information and follow the instructions of [step 3b](#)<sup>[2967]</sup> and [step 4](#)<sup>[2967]</sup> on the Update Your License page.
5. Click Update License.

If the activation was successful, you see the message Activation was successful as License Status at the top of the page.

 For more information, see section [License Information](#)<sup>[2965]</sup>.

 If your PRTG core server is offline, you must manually activate your license each time. This makes sure that you can install updates, for example.

## More

### KNOWLEDGE BASE

Which servers does PRTG connect to for software auto-update, activation, etc.?

- <https://kb.paessler.com/en/topic/32513>

### PAESSLER WEBSITE

How to use PRTG Enterprise Monitor in an offline environment in 5 steps

- <https://www.paessler.com/support/how-to/prtg-enterprise-monitor-offline>

## 4.7 Install a Remote Probe

Remote probes can extend your monitoring with PRTG:

- Monitor different subnetworks that are separated from your PRTG core server by a firewall, and keep an eye on remote locations. You can install [one or more remote probes](#)<sup>[319]</sup>.
- Distribute monitoring load by taking it from the PRTG core server system and putting it on one or more remote probe systems.

☁ You need a classic remote probe if you want to monitor your local network with a PRTG Hosted Monitor instance.

There are three types of remote probes:

1. [Classic remote probe](#)<sup>[3313]</sup>
2. [Multi-platform probe](#)<sup>[3316]</sup>
3. [Mini probe](#)<sup>[3316]</sup>

ⓘ You can use multi-platform probes to extend your monitoring to non-Windows systems. For more information about multi-platform probes, see the [Multi-Platform Probe for PRTG](#) manual.

ⓘ If you run PRTG in a cluster, see [Cluster and Remote Probes Outside the LAN](#)<sup>[109]</sup> in this section.

■ If you have issues after the installation, see section [Debugging Classic Remote Probe Connection Issues](#)<sup>[115]</sup>.

■ For a partially automatic installation of a classic remote probe directly from the device tree in the PRTG web interface, see section [Classic Remote Probe Setup via Device Tools](#)<sup>[3202]</sup>. For a quick installation guide, see the Paessler website: [How to install a PRTG remote probe in 4 steps](#).

### Steps to Take

To install a classic remote probe with the Classic Remote Probe Installer, follow these steps:

- [Step 1: Meet the Requirements](#)<sup>[106]</sup>
- [Step 2: Prepare the PRTG Core Server](#)<sup>[107]</sup>
- [Step 3: Download the Classic Remote Probe Installer from the PRTG Web Interface](#)<sup>[109]</sup>
- [Step 4: Install a New Classic Remote Probe](#)<sup>[110]</sup>
- [Step 5: Approve the New Remote Probe](#)<sup>[113]</sup>

### Step 1: Meet the Requirements

To install a classic remote probe on a target system, make sure that you meet the following requirements:

- The target system runs on at least Windows 7.
- The target system is accessible via remote procedure call (RPC). This is usually the case when your PRTG core server and the target system are located in the same LAN segment. Otherwise, open Windows [services.msc](#) on the target system and start the RPC service.



- Programs are allowed to communicate through your Windows Firewall. Open the settings of your firewall and select Allow an app through firewall. Mark the check box for Remote Service Management, and the check box Public in the corresponding line.
- Because the remote probe initiates the connection, you must make sure that a connection to your PRTG core server from the outside can be established. The process is the same as if you wanted to allow access to the PRTG web server provided by the PRTG core server via port 80 or 443. In most cases, this means that you will require an [allow](#) or [allow-nat](#) network address translation (NAT) rule that enables a remote probe to reach the PRTG core server via the Transmission Control Protocol (TCP) port [23560](#). Then, the remote probe uses a dynamic port from the high port range ([49152 - 65535](#)) for outgoing connections.


 If you need to set a different port, which we do not recommend, see the Knowledge Base: [How can I customize ports for core-probe connections used by PRTG?](#)

 You cannot install a remote probe on a system that already has a probe installed.

 For more information on the requirements for remote probes, see section [System Requirements](#)<sup>[23]</sup>.

 If you are using PRTG Hosted Monitor, start from [Step 3: Download the Classic Remote Probe Installer from the PRTG Web Interface](#)<sup>[109]</sup>.

## Step 2: Prepare the PRTG Core Server.

 Because remote probes need to connect to your PRTG core server, PRTG needs to accept incoming remote probe connections. So, with PRTG Network Monitor, first prepare your PRTG core server before you install a remote probe.

Edit the relevant settings in section [Core & Probes](#)<sup>[2887]</sup>. From the main menu in the [PRTG web interface](#)<sup>[124]</sup>, select Setup | System Administration | Core & Probes to access the probe settings and go to the Probe Connection Settings.

### Probe Connection Settings

**Probe Connection IP Addresses** ⓘ

Local probe only, 127.0.0.1

All IP addresses available on this computer

Specify IP addresses

**Access Keys** ⓘ

**Allow IP Addresses** ⓘ

**Deny IP Addresses** ⓘ

**Deny GIDs** ⓘ

**Connection Security** ⓘ

High security (TLS 1.3, TLS 1.2)

Default security (TLS 1.3, TLS 1.2) (recommended)

Weakened security (TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0)

**Mini Probes** ⓘ

Do not allow mini probes (default)

Allow mini probes to connect to the PRTG web server

Allow mini probes to connect to an extra port

**PRTG MultiBoard File Transfer** ⓘ

Disable (default)

Enable

Probe Connection Settings in System Administration

#### Step 2.1: Probe Connection IP Addresses

By default, a PRTG core server accepts connections from the local probe only (IP address [127.0.0.1](#)). This setting is the most secure setting, but it does not allow any remote probes to connect to your PRTG core server.

To accept remote probes, select one of the following settings:

- All IP addresses available on this computer: Any IP address on your PRTG core server system accepts incoming probe connections.
- Specify IP addresses: Specify IP addresses that accept incoming connections.

#### Step 2.2: Allow IP Addresses

In the Allow IP Addresses field, you can enter the IP address of the target system on which you want to install a remote probe. You can also enter the word [any](#). This sets the PRTG core server to accept remote probe connections from any IP address.

ⓘ If you use [any](#), make sure that you only write the word in lower case. Other variations are not valid.

Other settings are not required. For more information about the fields for Access Keys, Deny IP Addresses, and Deny GIDs, see section [Core & Probes](#)<sup>[2890]</sup>.

When you are done, click Save to save your settings.

**i** If you change this setting, PRTG needs to restart the PRTG core server to apply your changes. After you click Save, a dialog box appears that asks you to confirm the restart. Click OK to trigger the restart. During the restart, all users of the PRTG web interface, the [PRTG app for desktop](#)<sup>[2984]</sup>, or the [PRTG Apps for Mobile Network Monitoring](#)<sup>[2988]</sup> are disconnected and reconnected.

**i** To edit the core-probe connection settings, you can also use the [PRTG Administration Tool](#)<sup>[3041]</sup> on your PRTG core server.

### Cluster and Remote Probes Outside the LAN

**i** If you run PRTG as a cluster and you want to run remote probes outside your local network, you must make sure that your cluster nodes and the addresses that they use are reachable from the outside. Check your cluster node settings under [Cluster](#)<sup>[2923]</sup> before you install a remote probe outside your local network. Enter valid Domain Name System (DNS) names or IP addresses for both cluster nodes to reach each other and for remote probes to individually reach all cluster nodes. Remote probes outside your LAN cannot connect to your cluster nodes if they use local addresses.

If you already have a remote probe installed outside your LAN and the remote probe is disconnected because of this, follow these steps:

1. Uninstall the remote probe.
2. Update the [cluster node settings](#)<sup>[2923]</sup> with addresses that are reachable from outside your LAN.
3. Restart the PRTG core servers.
4. Install the remote probe again. It then obtains the IP address or DNS name entries that it can reach.

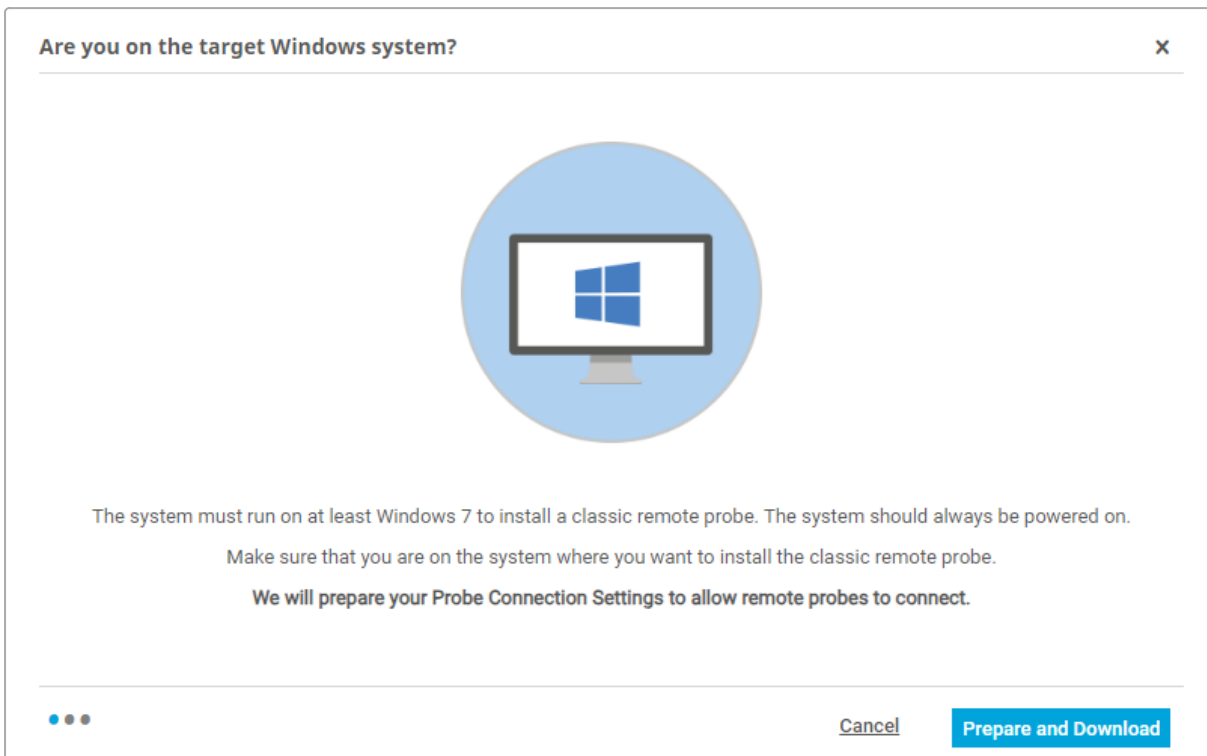
 See also section [Failover Cluster Configuration](#)<sup>[3210]</sup>, section Remote Probes in a Cluster.

### Step 3: Download the Classic Remote Probe Installer from the PRTG Web Interface

1. On the Windows system on which you want to install a classic remote probe, log in to the PRTG web interface.
2. From the main menu bar, select Setup | Optional Downloads | Classic Remote Probe Installer.
3. Click Add Remote Probe to start the installation assistant.  
**i** The Add Remote Probe button is also available in the device tree.
4. Wait until the installation is completed. The classic remote probe then automatically connects to your PRTG core server.
5. In the appearing dialog window, click Prepare and Download to start the download.
6. Save the setup program to your local disk.

In the installation approach with the assistant, PRTG guides you through the installation process. If you Download the Classic Remote Probe Installer directly, you must install the classic remote probe without the assistant.

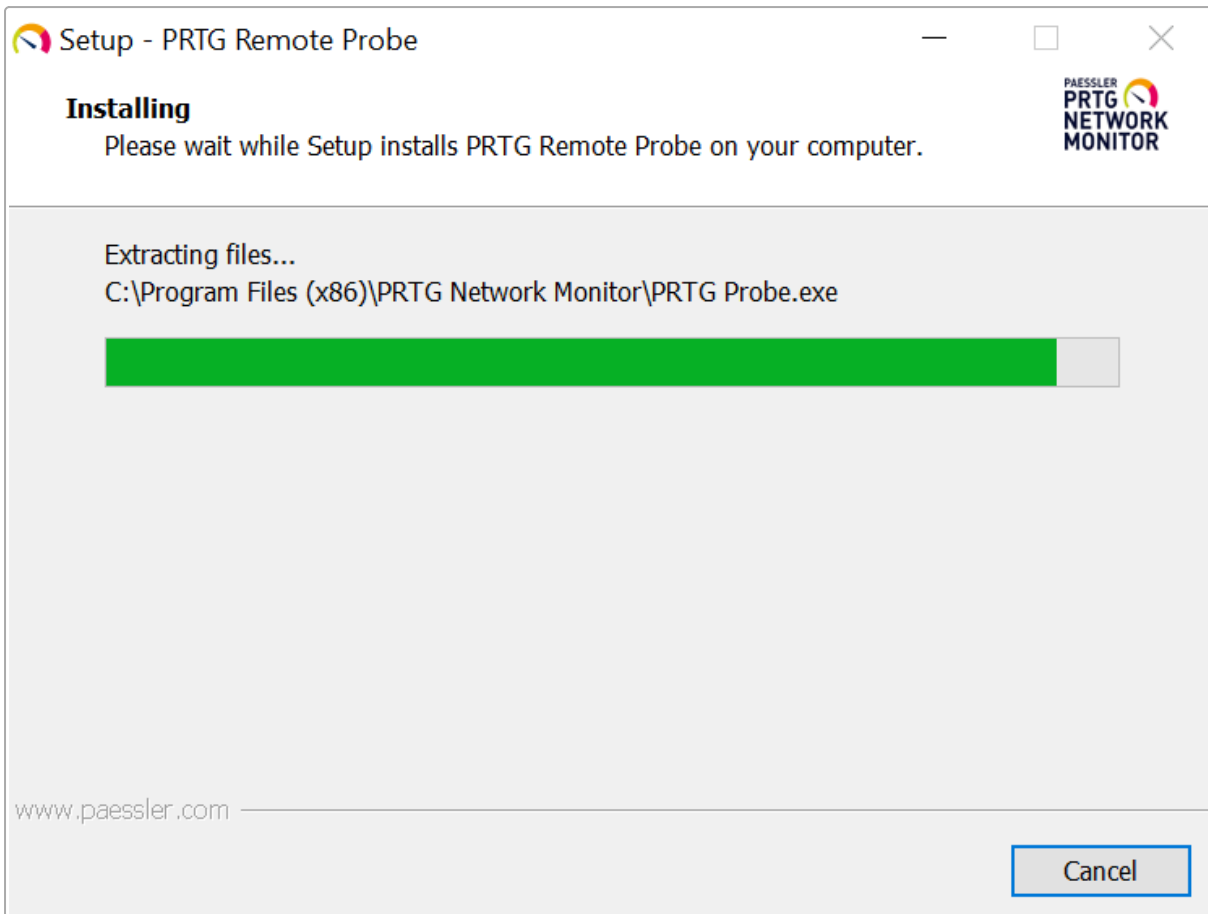
- ☰ If you connect remote probes to PRTG Network Monitor, [prepare](#)<sup>107</sup> your Probe Connection Settings first.



- ❗ The PRTG version numbers of the PRTG core server service and PRTG probe service must match. PRTG automatically updates classic remote probes when you install a new version on the PRTG core server. If PRTG advises you to manually update your classic remote probe, open a web browser on the remote system and download the classic remote probe installer as described in this section.

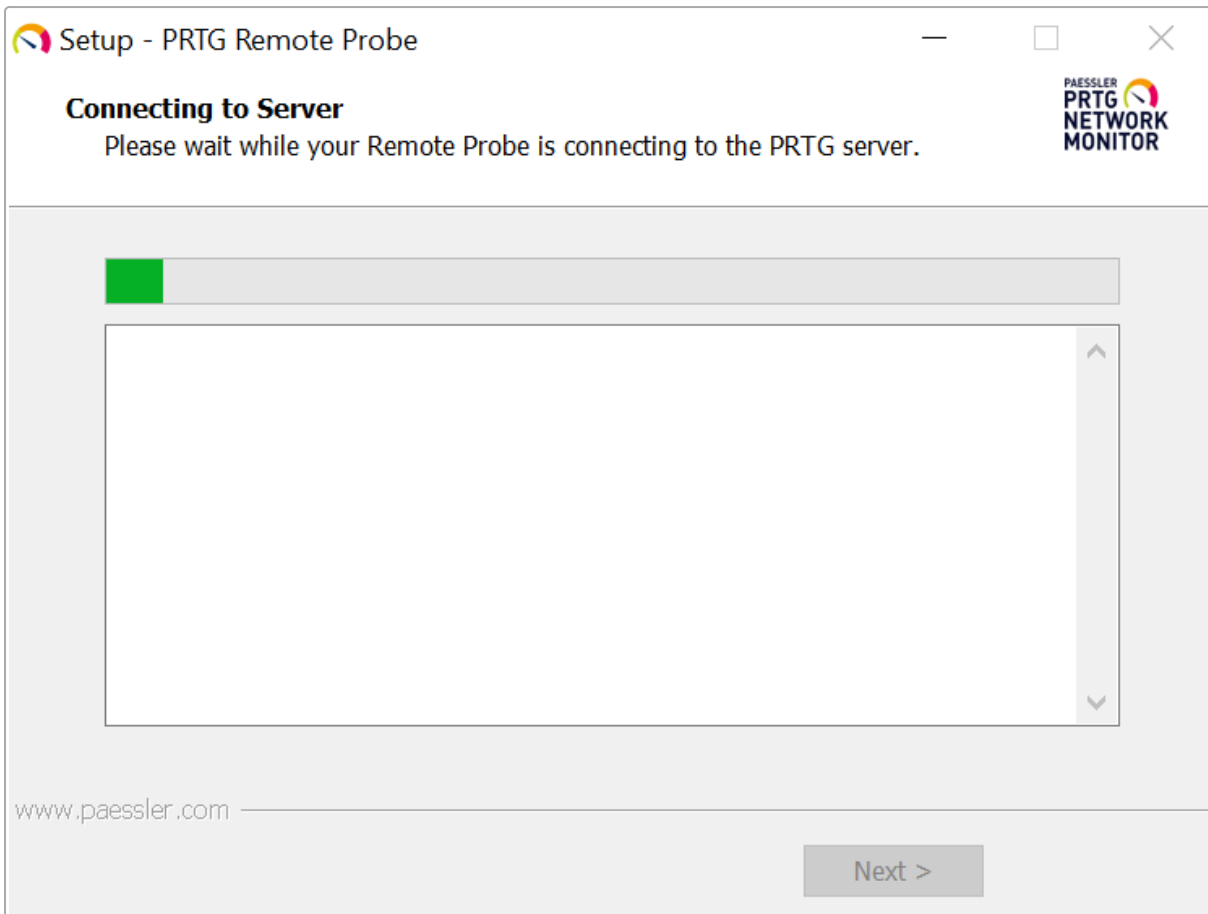
#### Step 4: Install a New Classic Remote Probe

1. Execute the setup program that you downloaded.
2. Confirm the [Windows User Account Control](#) dialog with Yes to allow the installation. The usual software installation wizard guides you through the installation process.
3. Click Install to start the installation process.



Remote Probe Setup Installing

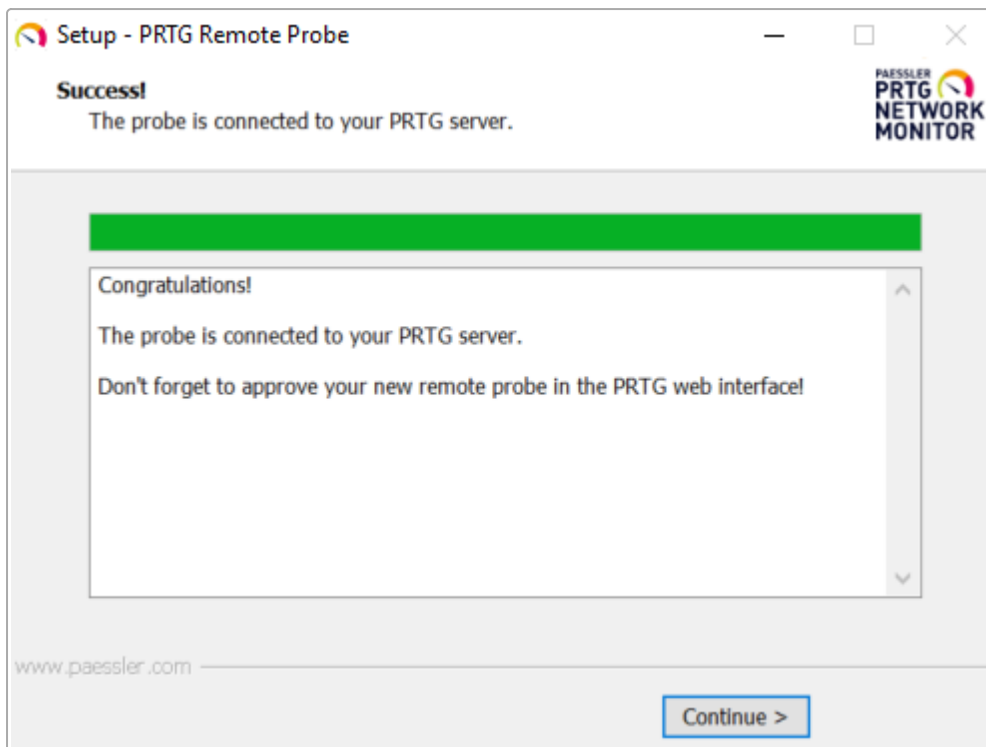
Wait until the installation is complete. The remote probe then automatically connects to your PRTG core server.



Remote Probe Setup Connecting to the PRTG Core Server

If the remote probe successfully connects to your PRTG core server, you can complete the setup of your new remote probe.

**i** To allow your new remote probe to connect to a PRTG Hosted Monitor instance, PRTG automatically sets the Allow IP Addresses field in [Core & Probes](#) to [any](#). You can also use [any](#) for PRTG Network Monitor, but we recommend that you use this setting in intranets only. If [any](#) is not an option for you, cancel it in the Allow IP Addresses field and enter the IP address of your remote probe instead.



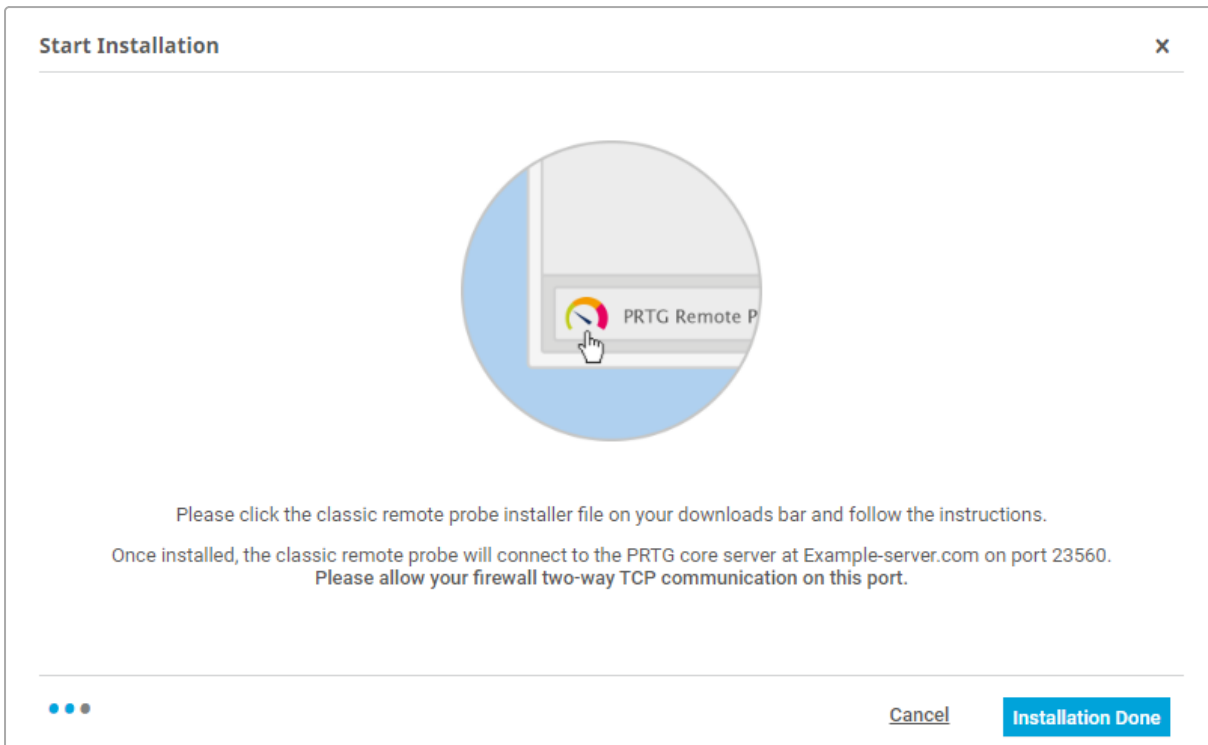
Remote Probe Setup Successful

4. Click Continue to finish the remote probe installation.
5. Click Finish to exit the installation wizard.

The remote probe is now installed on your computer as a Windows service.

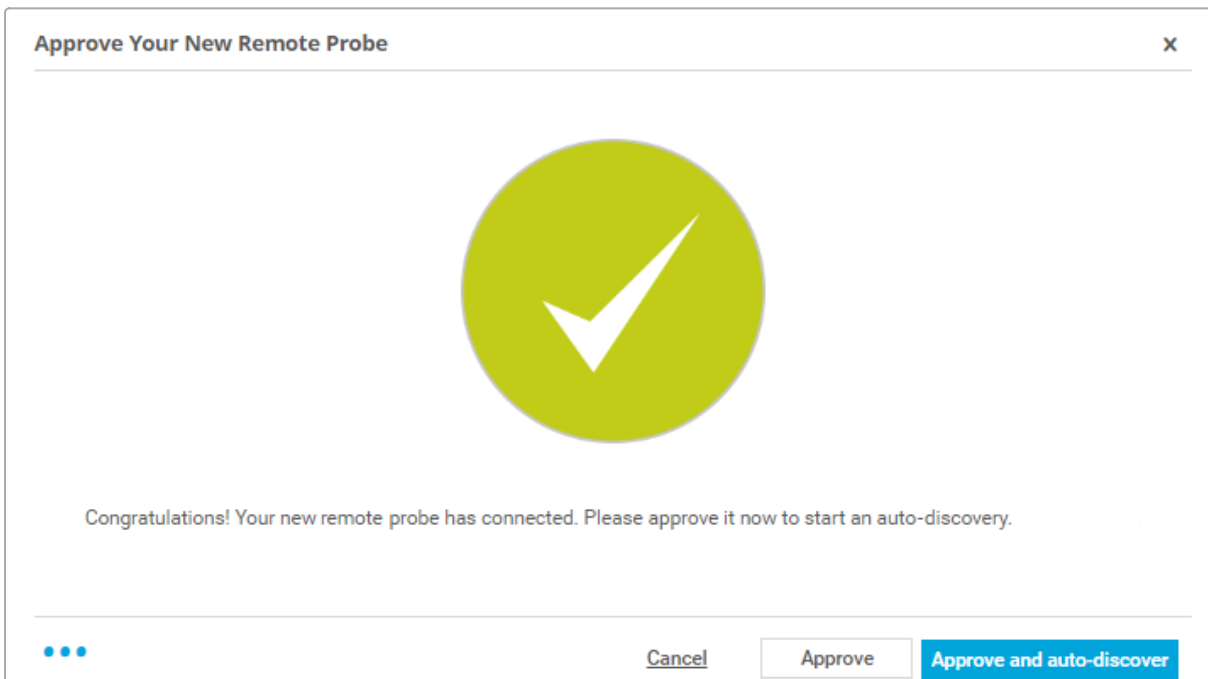
### Step 5: Approve the New Remote Probe

In the installation assistant, click Installation Done.



Confirm that Installation is Done

☁ If you successfully installed the remote probe from a PRTG Hosted Monitor installation, you see the following dialog box.

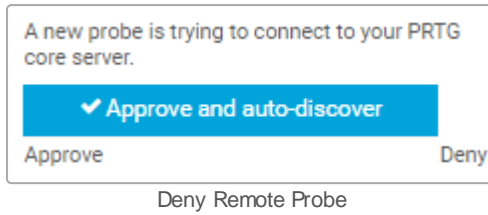


Approve Remote Probe for PRTG Hosted Monitor

Click **Approve and auto-discover** to include the new remote probe and network in your device tree and to start the [auto-discovery](#)<sup>[254]</sup>. It discovers devices and automatically creates suitable sensors. Optionally, click **Approve** to only approve the remote probe without the auto-discovery. The remote probe appears in your device tree.



For unwanted remote probe connections, click Cancel. A new window appears in the lower-right corner.



Click **Deny** to deny the new remote probe.

**i** If you deny or remove a remote probe, PRTG automatically adds the global ID (GID) of this device to the Deny GIDs list in [Core & Probes](#)<sup>[2888]</sup>. PRTG automatically denies future remote probe connections from this device.

**i** If you deny the remote probe in the device tree, it does **not** uninstall the remote probe, but only denies access to the PRTG core server. The remote probe continues to run on the target system until you uninstall it manually.

Once approved, PRTG automatically opens the new remote probe in the device tree and creates a set of sensors for the remote probe to make sure you can immediately detect bottlenecks on the remote probe system. We recommend that you keep these sensors. You can now create groups, devices, and sensors for monitoring via the new remote probe.

**i** You do not need to approve classic remote probes after updates.

When a new remote probe connects to the PRTG core server for the first time, you receive a new ToDo ticket.

**i** PRTG automatically updates classic remote probes but, in rare cases, you must manually update classic remote probes. You receive a [ToDo ticket](#)<sup>[213]</sup> in this case. Follow the steps [above](#)<sup>[109]</sup> to manually update classic remote probes.

## Debugging Classic Remote Probe Connection Issues

If you have issues with the connection between the PRTG core server and classic remote probe, make sure that you meet the following requirements:

- Recheck if you fulfilled all the requirements as described in [step 1](#)<sup>[106]</sup> of this section like the Windows Firewall settings.
- The IP address of the computer on which you want to install a remote probe is not listed in the Deny IP Addresses field in [Core & Probes](#)<sup>[2888]</sup>.
- You can also take a look at the log files of the classic remote probe. The probe process writes log files with a file name in the format PRTG Probe Log (x).log. Open the one with the most recent date.

For a correct connection, the log should look similar to this:

```

11/6/2023 1:21:58 PM PRTG Probe V23.4.90.1235
11/6/2023 1:21:58 PM System time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome,
Stockholm, Vienna
11/6/2023 1:21:58 PM libeay32.dll=1.0.2.11
11/6/2023 1:21:58 PM ssleay32.dll=1.0.2.11
11/6/2023 1:21:58 PM PRTG Probe "example-DNS" starting on "example-
DNS" (GID={AAAA1111-22BB-33CC-DD44-EEEEEE555555})
11/6/2023 1:21:58 PM Memory Manager: NexusMM4
11/6/2023 1:21:58 PM OS: Microsoft Windows 10 Enterprise (10.0 Build 15063), 4 CPUs
(Quad x64 Model 78 Step 3), code page "Windows-1252", on "NVME SAMSUNG MZFLV256"
11/6/2023 1:21:58 PM Data Path: C:\ProgramData\Paessler\PRTG Network Monitor\
11/6/2023 1:21:58 PM System Path: C:\Program Files (x86)\PRTG Network Monitor\
11/6/2023 1:21:58 PM Local IP: 0.0.0.0
11/6/2023 1:21:58 PM Core Server IP: example-DNS.exempldomain.com
11/6/2023 1:21:58 PM Core Server Port: 23560
11/6/2023 1:21:58 PM SSL Enabled
11/6/2023 1:21:58 PM Probe GID: {AAAA1111-22BB-33CC-DD44-EEEEEE555555}
[...]
11/6/2023 1:21:58 PM Start Connection
11/6/2023 1:21:58 PM Start Done
11/6/2023 1:21:58 PM (14608):Initializing WMIConnectionPool
11/6/2023 1:21:58 PM (14608):WMIConnectionPool maximum number of concurrent
establishings is set to: 20
11/6/2023 1:22:03 PM Connect from to example-DNS.exempldomain.com:23560
11/6/2023 1:22:03 PM TCP connected from 10.49.12.51:55199 to example-
DNS.exempldomain.com:23560
11/6/2023 1:22:03 PM State changed to connected (example-DNS.exempldomain.com:23560)
11/6/2023 1:22:03 PM Reconnect
11/6/2023 1:22:04 PM Connected
11/6/2023 1:22:10 PM Send Login
11/6/2023 1:22:10 PM Local: 11/6/2023 1:22:10 PM UTC: 11/6/2023 12:22:10 PM
11/6/2023 1:22:10 PM MarkUnused
11/6/2023 1:22:10 PM Login OK: Welcome to PRTG

```

If the connection fails, for example because of an incorrect Access Key, or because of incorrect IP address settings (see [step 2](#)<sup>[107]</sup>), you see:

```

11/6/2023 1:42:02 PM Try to connect...
11/6/2023 1:42:02 PM Connected to 10.0.2.167:23560
11/6/2023 1:42:07 PM Login NOT OK: Access key not correct!

```

If you need to adjust any settings for the connection to the PRTG core server, use the [PRTG Administration Tool](#)<sup>[3067]</sup> on the remote probe system.

Remote Probe Settings in PRTG Administration Tool

Under Connection to PRTG Core Server, you can then edit the following settings:

- **Server (IPv4 Address or DNS Name):** Enter the IP address or Domain Name System (DNS) name of the PRTG core server that the remote probe is to connect to. If you use network address translation (NAT) rules, you must enter the IP address that is externally visible, because the remote probe connects from outside your network.
- **Access Key and Confirm Access Key:** Enter the access key that the remote probe is to send to the PRTG core server. You must define this access key on the PRTG core server in [Core & Probes](#)<sup>[2888]</sup>. Make sure that the access keys match.

Click Save & Close to confirm your settings and to (re)start the PRTG probe service.

For more information about these settings, see section [PRTG Administration Tool](#)<sup>[3067]</sup>.

## More

### ■ KNOWLEDGE BASE

How can I customize ports for core-probe connections used by PRTG?

- <https://kb.paessler.com/en/topic/65084>

I cannot open the PRTG web interface via the desktop shortcut anymore. What can I do?

- <https://kb.paessler.com/en/topic/89024>

What is the multi-platform probe and how can I use it?

- <https://kb.paessler.com/en/topic/90140>

### ■ PAESSLER WEBSITE

How to connect PRTG through a firewall in 4 steps

- <https://www.paessler.com/support/how-to/firewall>

How to install a PRTG remote probe in 4 steps

- <https://www.paessler.com/support/how-to/remote-probe-installation>

## 4.8 Uninstall PRTG Products

Whether you uninstall an entire PRTG installation or a remote probe installation, take the following steps. Use the Windows uninstall routines to remove the software from your system.

■ For more information on how to uninstall a multi-platform probe, see the [Multi-Platform Probe for PRTG](#) manual.

### Step 1

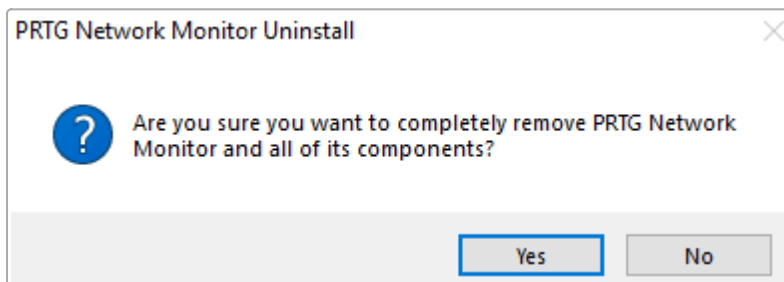
From the Windows Start menu, run Uninstall PRTG Network Monitor or open your Windows Control Panel and select the desired entry in the Programs and Features section. To uninstall a remote probe, only the second option applies. Depending on the installed products, not all uninstall programs are available.

### Step 2

If asked, confirm the question of the Windows User Account Control with Yes to allow the program to uninstall. The software uninstall dialog guides you through the uninstall process.

### Step 3

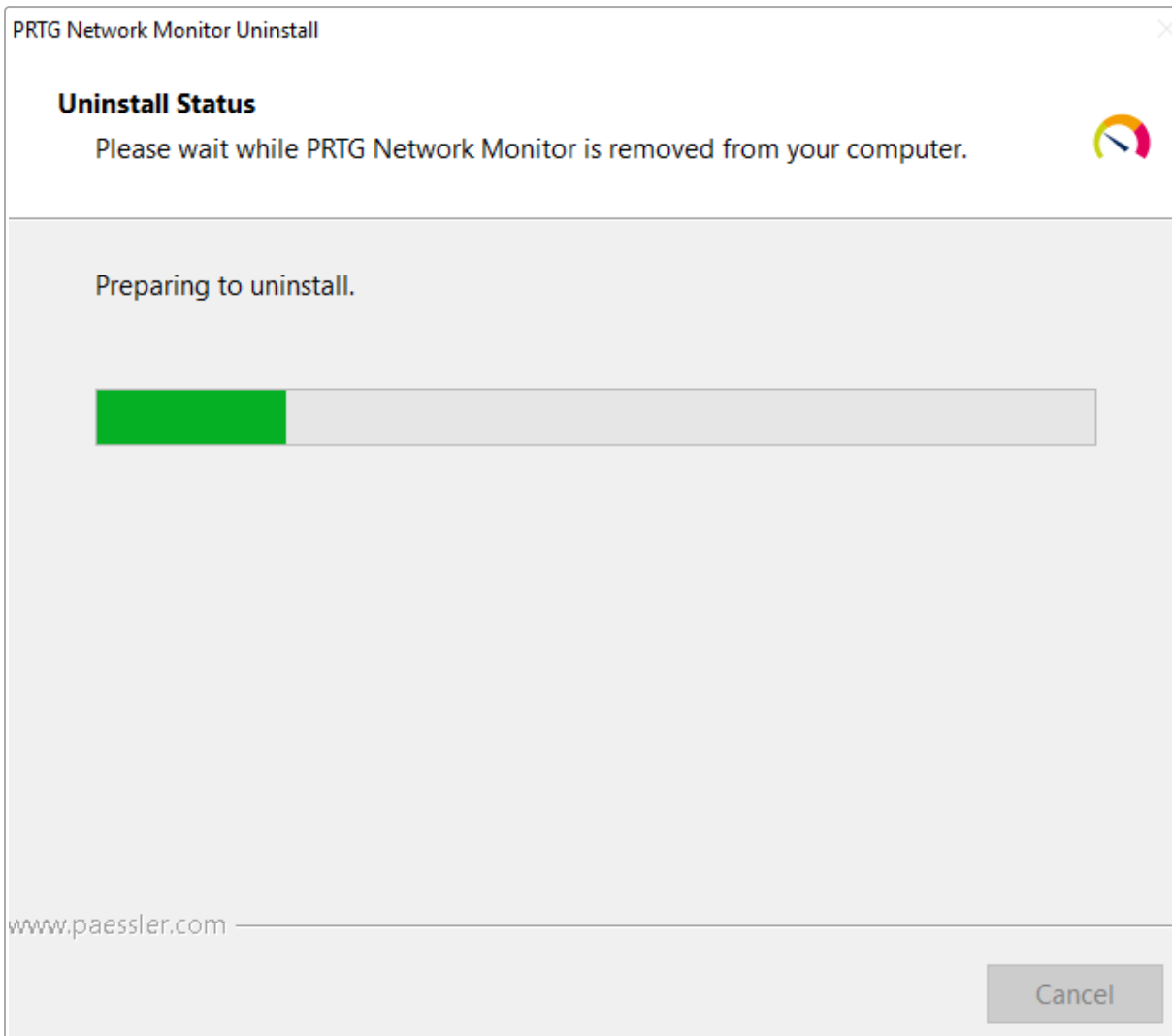
Confirm the removal of the software with Yes.



Uninstall PRTG Network Monitor Step 1

### Step 4

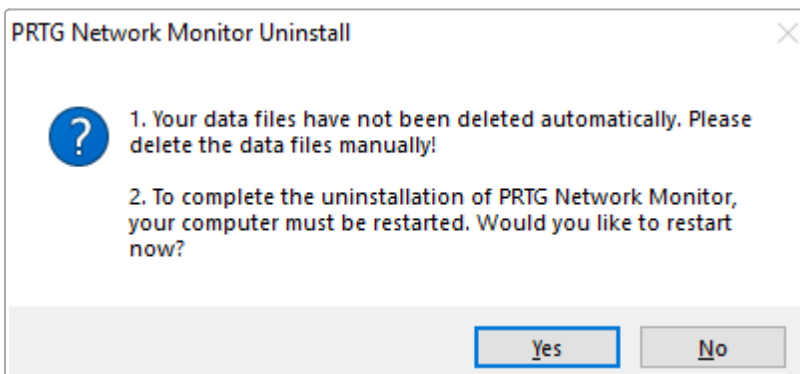
Wait while the software is removed.



Uninstall PRTG Network Monitor Step 2

## Step 5

Confirm a system restart with Yes.



Uninstall PRTG Network Monitor Step 3


## Step 6

After the system restart, the software is removed, but there is still some custom data in the PRTG program directory. If you have uninstalled an entire PRTG installation or a remote probe installation, your monitoring data is still stored on the system. To completely remove all PRTG data, delete the PRTG Network Monitor folder as well as the Paessler\PRTG Network Monitor folder in the PRTG data directory.

■ For more information, see section [Data Storage](#) .

## Step 7

During the installation of PRTG, a component called Npcap is also installed on your system. After you uninstall PRTG, you need to manually uninstall this feature. To do so, open your Windows Control Panel and select Npcap 0.9983 in the Programs and Features section. Click Uninstall to remove this feature from your Windows system.

 If you updated to PRTG 19.2.50, you also need to manually uninstall the Npcap loopback adapter. For more information, see the Knowledge Base: [I have issues with additional services after updating to PRTG 19.2.50. What can I do?](#)

## More

### ■ KNOWLEDGE BASE

I have issues with additional services after updating to PRTG 19.2.50. What can I do?

- <https://kb.paessler.com/en/topic/86103>

Can we remotely and silently uninstall a classic remote probe?

- <https://kb.paessler.com/en/topic/27383>

### ■ Multi-Platform Probe for PRTG

- [Multi-Platform Probe for PRTG](#) (PDF)

# Part 5












# Understanding Basic Concepts



## 5 Understanding Basic Concepts

There are a number of basic concepts that are essential for understanding the functionality of PRTG. This includes, for example, the underlying architecture of the monitoring system, the hierarchy of objects, the inheritance of settings, the access rights management, and notifications.

In this section:



- [Architecture and User Interfaces](#)  124
- [Failover Cluster](#)  128
- [Object Hierarchy](#)  132
- [Inheritance of Settings](#)  136
- [Tags](#)  138
- [Dependencies](#)  140
- [Scheduling](#)  141
- [Notifying](#)  142
- [Access Rights Management](#)  145
- [Data Reporting](#)  149
- [IPv6 Support](#)  150

## 5.1 Architecture and User Interfaces

In this section, you can find an overview of the components of PRTG and how it works.

### Overview

You can classify the components of PRTG into three main categories: system parts, user interfaces, and basic system administration tools.

Category	Components
System Parts	<p><a href="#">PRTG core server</a><sup>[125]</sup> This is the central part of a PRTG installation. The PRTG core server includes the data storage, the web server, the report engine, the notification system, and more. The PRTG core server is configured as a Windows service that permanently runs.</p> <p><a href="#">Probes</a><sup>[125]</sup> This is the part of PRTG that performs the actual monitoring. There are local probes, remote probes, and cluster probes in PRTG Network Monitor, and there are hosted probes and remote probes in PRTG Hosted Monitor. Probes forward all monitoring data to the central PRTG core server. Probes are configured as services that permanently run.</p> <p> We assume that all systems on which the PRTG core server with the local probe or any remote probes run are secure. It is every system administrator's responsibility to make sure that only authorized persons can access these systems. For this reason, we highly recommend that you use dedicated machines for your PRTG system parts.</p>
User Interfaces	<p><a href="#">PRTG web interface</a> With the Asynchronous JavaScript and XML (AJAX) based PRTG web interface, you can configure devices and sensors, review monitoring results, and configure the system administration and user management.</p> <p><a href="#">PRTG app for desktop</a><sup>[2984]</sup> The PRTG app for desktop is a cross-platform application that you can use as an alternative interface for fast access to data and monitoring management. With the PRTG app for desktop, you can connect to several independent PRTG core servers or PRTG Hosted Monitor instances to display their data and centrally manage your monitoring.</p> <p><a href="#">PRTG apps for mobile network monitoring</a><sup>[2988]</sup> With the PRTG apps for iOS and Android, you can monitor your network on the go and receive push notifications in case of alerts.</p>
System Administration Tools	<p><a href="#">PRTG Administration Tool on PRTG Core Server Systems</a><sup>[3041]</sup>  With the PRTG Administration Tool on the PRTG core server system, you can configure basic PRTG core server settings in PRTG Network Monitor such as the <a href="#">PRTG System Administrator</a> user login, web server IP addresses and the web server port, probe connection settings, the cluster mode, the system language, and more.</p>

Category	Components
	<p><a href="#">PRTG Administration Tool on Remote Probe Systems</a><sup>130671</sup></p> <p>With the PRTG Administration Tool on the remote probe system, you can configure basic remote probe settings such as the name of the remote probe, IP address and server connection settings, and more.</p>

## PRTG Core Server

The PRTG core server is the heart of PRTG. It performs the following tasks:

- Configuration management for target devices (for example, servers, workstations, printers, switches, routers, or virtual machines (VM))
- Management and configuration of connected probes
- Cluster management
- Database for monitoring results
- Notification management including a mail server for email delivery
- Report generation and scheduling
- User account management
- Data purging (for example, deleting data that is older than 365 days)
- Web server and application programming interface (API) server

**i** In a [cluster](#)<sup>128</sup>, the master node is responsible for all of these tasks.

The built-in and secure web server, for which you require no additional Microsoft Internet Information Services (IIS) or Apache, supports HTTP as well as HTTPS (secured with Secure Sockets Layer (SSL)/Transport Layer Security (TLS)). It serves the PRTG web interface when you access it via a browser and also answers PRTG API calls.

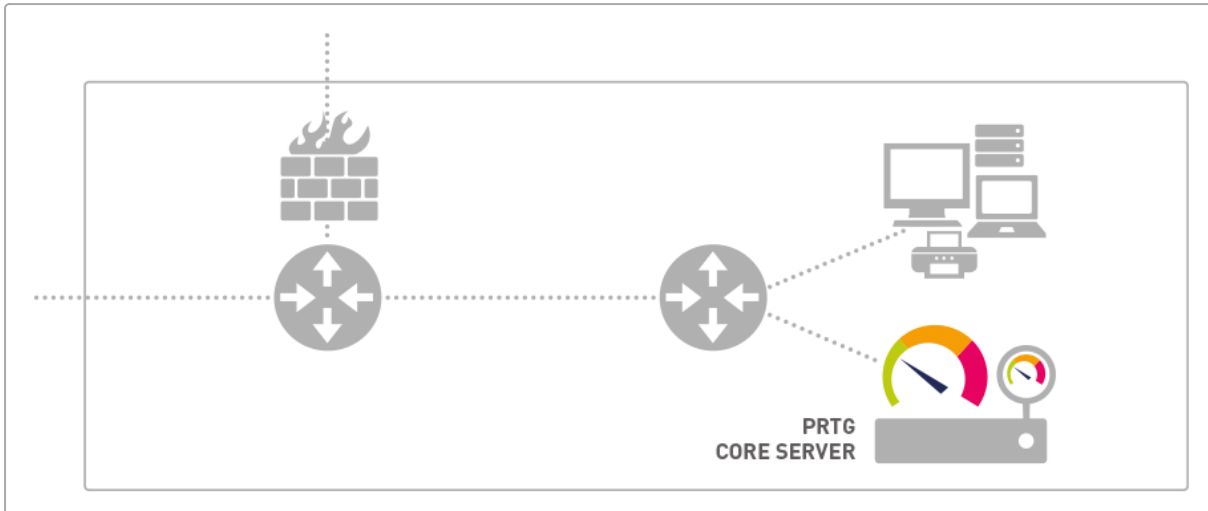
**i** The PRTG core server is configured as a Windows service that permanently runs. A logged-in user is not required.

## Probes

On the probe, PRTG performs the actual monitoring via the sensors that you created on a device (for example, a computer, a router, a server, a firewall, and more). The probe receives its configuration from the PRTG core server, runs the monitoring processes, and delivers monitoring results back to the PRTG core server.

**☰** For PRTG Network Monitor, there is always a local probe that runs on the PRTG core server system.

**☁** For PRTG Hosted Monitor instances, there is always a hosted probe that runs on the PRTG core server system that Paessler hosts for you.





PRTG Core Server and Local Probe That Monitors a LAN

The actual monitoring is performed by probe processes that run on one or more systems.

- ❶ The probes are configured as a Windows service that permanently runs. A logged-in user is not required.

Probe Type	Description
Local probe	<p>During the installation, PRTG automatically creates the <a href="#">local probe</a>. In a single-probe installation, which is the default setup, the local probe performs all monitoring.</p> <p>For PRTG Network Monitor, the PRTG core server with the local probe inside the corporate LAN can monitor services and servers in the entire LAN.</p>
Hosted probe	<p>When you create a PRTG Hosted Monitor instance, the system automatically creates the <a href="#">hosted probe</a>. The hosted probe shows monitoring values of the hosted instance and can monitor devices, servers, and services that are publicly available in the internet like websites.</p>
Cluster probes	<p>In a cluster, a <a href="#">cluster probe</a> runs on all cluster nodes. All devices that you create on the cluster probe are monitored by all cluster nodes, so data from different perspectives is available and monitoring continues even if one of the cluster nodes fails.</p>
Remote probes	<p>You can create additional <a href="#">remote probes</a> to monitor multiple locations, to monitor a LAN with PRTG Hosted Monitor, or for several other scenarios. Remote probes use SSL/TLS-secured connections to the PRTG core server. With remote probes, you can securely monitor services and systems inside remote networks that are not publicly available or that are secured by firewalls.</p>

Probe Type	Description
	<p>There are three types of remote probes: classic remote probes, multi-platform probes, and mini probes.</p> <ul style="list-style-type: none"> <li>■ For more information, see section <a href="#">Add Remote Probe</a><sup>[3196]</sup>.</li> <li>▶ For more information, see the video tutorial: <a href="#">Distributed monitoring with PRTG</a>.</li> </ul>
Classic remote probes	<p>Classic remote probes extend your monitoring to other Windows systems in your local or remote network.</p> <ul style="list-style-type: none"> <li>■ For more information, see section <a href="#">Install a Remote Probe</a><sup>[106]</sup>.</li> </ul>
Multi-platform probes 	<p>You can install <a href="#">multi-platform probes</a> on Linux systems in your local or remote network. The multi-platform probe scans the network and sends monitoring results to the <a href="#">PRTG core server</a><sup>[125]</sup> via a NATS server.</p> <ul style="list-style-type: none"> <li>■ For more information, see the <a href="#">Multi-Platform Probe for PRTG</a> manual.</li> </ul>
Mini probes 	<p>Mini probes let you create small probes on any device, not only on Windows systems.</p> <ul style="list-style-type: none"> <li>■ For more information, see section <a href="#">Mini Probe API</a><sup>[3153]</sup>.</li> </ul>

## More

### PAESSLER WEBSITE

#### Getting started with PRTG

- <https://www.paessler.com/support/getting-started>

#### How to connect PRTG through a firewall in 4 steps

- <https://www.paessler.com/support/how-to/firewall>

### VIDEO TUTORIAL

#### Distributed monitoring with PRTG

- [https://www.paessler.com/support/videos-and-webinars/videos/distributed\\_monitoring](https://www.paessler.com/support/videos-and-webinars/videos/distributed_monitoring)

#### What is a sensor?

- <https://www.paessler.com/support/videos-and-webinars/videos/what-is-a-sensor>

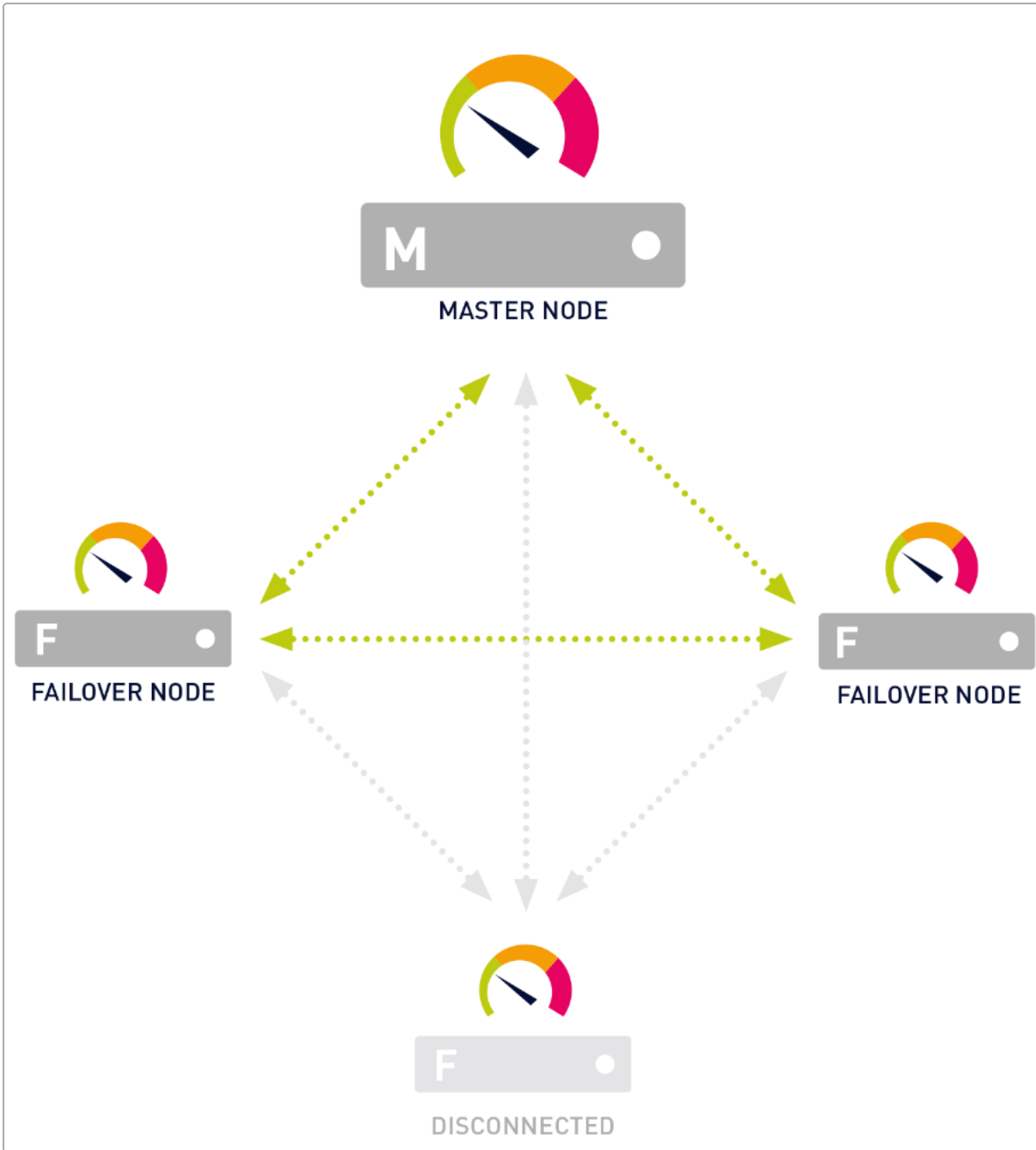
## 5.2 Failover Cluster

A [cluster](#) consists of two or more PRTG core servers that work together to form a high-availability monitoring system.

 This feature is not available in PRTG Hosted Monitor.

### Cluster Concept



A cluster consists of at least two cluster nodes: one [master node](#) and one or more [failover nodes](#), where up to four failover nodes are possible. Each cluster node is a full PRTG core server installation that can perform all of the monitoring and alerting on its own.



Cluster with Two Cluster Nodes

See the following table for more information on how a cluster works:

Feature	Description
Connection and communication	Cluster nodes are connected to each other with two TCP/IP connections. They communicate in both directions and a single cluster node only needs to connect to one other cluster node to integrate itself into the cluster.


Feature	Description
Object configuration	During normal operation, you configure devices, sensors, and all other monitoring objects on the master node. The master node automatically distributes the configuration among all other cluster nodes in real time.
Fail-safe monitoring	<p>All devices that you create on the cluster probe are monitored by all cluster nodes, so data from different perspectives is available and monitoring continues even if one of the cluster nodes fails.</p> <p>If the master node fails, one of the failover nodes takes over and controls the cluster until the master node is back. This ensures continuous data collection.</p>
Active-active mode	A cluster works in <a href="#">active-active</a> mode. This means that all cluster nodes permanently monitor the network according to the common configuration that they receive from the master node. Each cluster node stores the results in its own database. PRTG also distributes the storage of monitoring results among the cluster.
PRTG updates	You only need to install PRTG updates on one cluster node. This cluster node automatically deploys the new version to all other cluster nodes.
Notification handling	If one or more cluster nodes discover downtime or threshold breaches, only one installation, either the primary master node or the failover master node, sends out notifications, for example, via email, SMS text message, or push message. Because of this, there is no notification flood from all cluster nodes in case of failures.
Data gaps	<p>During the outage of a cluster node, it cannot collect monitoring data. The data of this single cluster node shows gaps. However, monitoring data for the time of the outage is still available on the other cluster nodes.</p> <p> There is no functionality to fill these gaps with the data of other cluster nodes.</p>
Monitoring results review	Because the monitoring configuration is centrally managed, you can only change it on the primary master node. However, you can review the monitoring results of any of the failover nodes in read-only mode if you log in to the PRTG web interface.
Remote probes	<p>If you use <a href="#">classic remote probes in a cluster</a><sup>[5210]</sup>, each remote probe connects to each cluster node and sends the data to all cluster nodes. You can define the Cluster Connectivity of each remote probe in its <a href="#">settings</a><sup>[521]</sup>.</p> <p> You cannot add multi-platform probes to a cluster. For more information about the multi-platform probe, see the <a href="#">Multi-Platform Probe for PRTG</a> manual.</p>



## Performance Considerations for Clusters

Monitoring traffic and load on the network is multiplied by the number of used cluster nodes. Furthermore, the devices on the cluster probe are monitored by all cluster nodes, so the monitoring load increases on these devices as well.

For most usage scenarios, this does not pose a problem, but always keep in mind the [system requirements](#). As a rule of thumb, each additional cluster node means that you need to divide the number of sensors that you can use by two.

 PRTG does not officially support more than 5,000 sensors per cluster. Contact the [Paessler Presales team](#) if you exceed this limit. For possible alternatives to a cluster, see the Knowledge Base: [Are there alternatives to the cluster when running a large installation?](#)

## Cluster Setup

 For more information, see section [Failover Cluster Configuration](#).

## More

### KNOWLEDGE BASE

What is the clustering feature in PRTG?

- <https://kb.paessler.com/en/topic/6403>

In which web interface do I log in to if the master node fails?

- <https://kb.paessler.com/en/topic/7113>

What are the bandwidth requirements for running a cluster?

- <https://kb.paessler.com/en/topic/8223>

Are there alternatives to the cluster when running a large installation?

- <https://kb.paessler.com/en/topic/75474>

What is the multi-platform probe and how can I use it?

- <https://kb.paessler.com/en/topic/90140>

### PAESSLER WEBSITE

How to connect PRTG through a firewall in 4 steps

- <https://www.paessler.com/support/how-to/firewall>

### VIDEO TUTORIAL

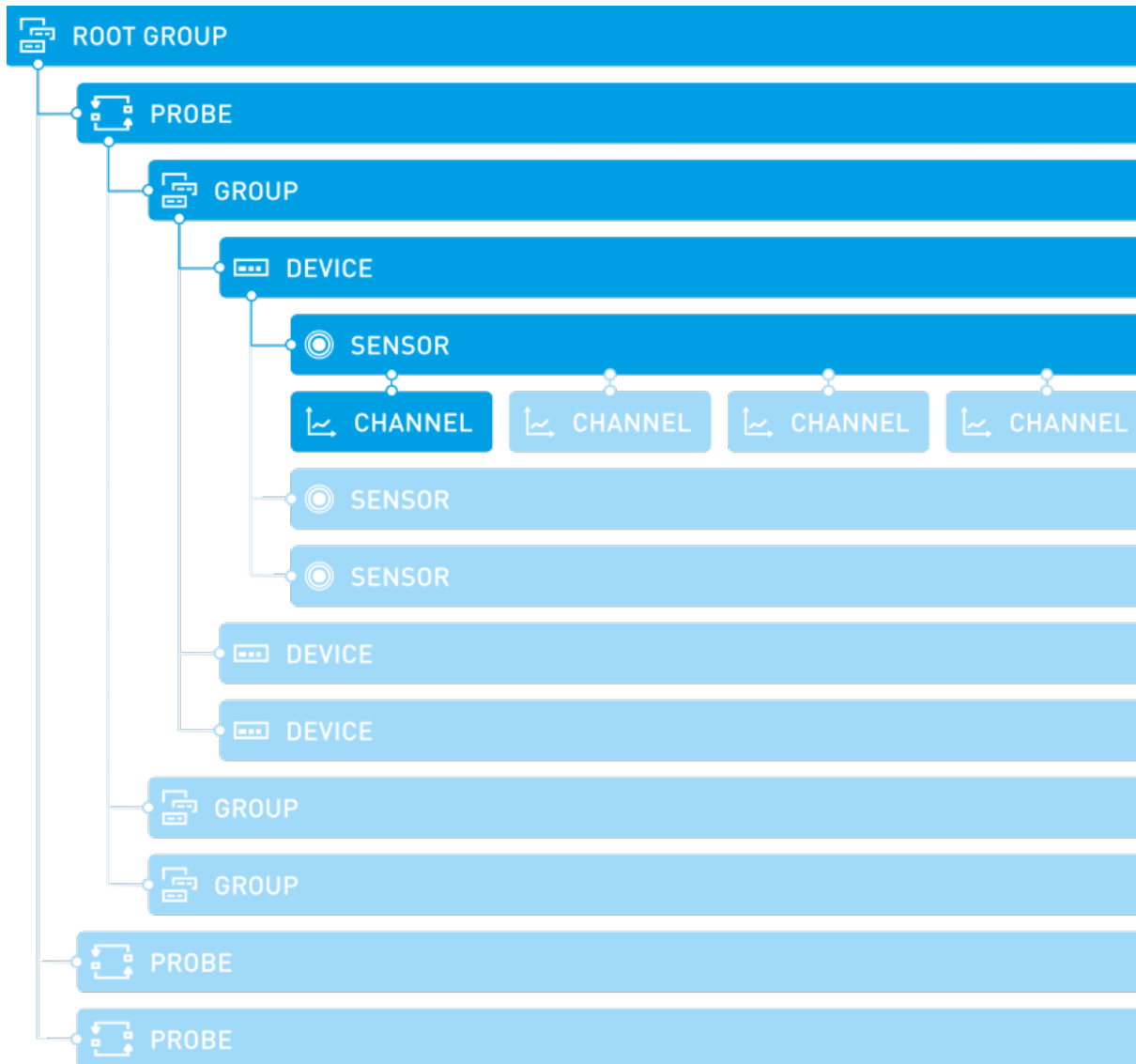
How to set up a PRTG cluster

- <https://www.paessler.com/support/videos-and-webinars/videos/how-to-set-up-a-cluster>

## 5.3 Object Hierarchy

PRTG arranges all objects in the monitoring configuration in a tree-like hierarchy. You can arrange the objects in groups that monitor similar devices, services, or particular locations. You can also use this hierarchical order to define common settings for larger groups of objects. The settings of the root group, for example, apply to all other objects underneath in the object hierarchy by default.

For more information, see section [Inheritance of Settings](#)<sup>[136]</sup>.



Object Hierarchy in PRTG

### Root Group

The [root group](#) is the topmost instance in PRTG. It contains all other objects in your setup. We recommend that you [adjust all default settings for the root group](#)<sup>[420]</sup>. This is because all other objects in the device tree [inherit](#)<sup>[136]</sup> these standard settings by default so that you do not need to set up the same configuration for each object anew.

## Probe

Each group is part of a **probe** (this excludes root group). This is where the actual monitoring takes place. All objects that you add to a probe are monitored via that probe. In PRTG Network Monitor, every PRTG core server installation automatically installs the **local probe**.

☁ In PRTG Hosted Monitor, every instance has the **hosted probe**.

In a **failover cluster**<sup>[128]</sup>, there is an additional **cluster probe** that runs on all cluster nodes. All devices that you create on the cluster probe are monitored by all cluster nodes, so data from different perspectives is available and monitoring continues even if one of the cluster nodes fails.

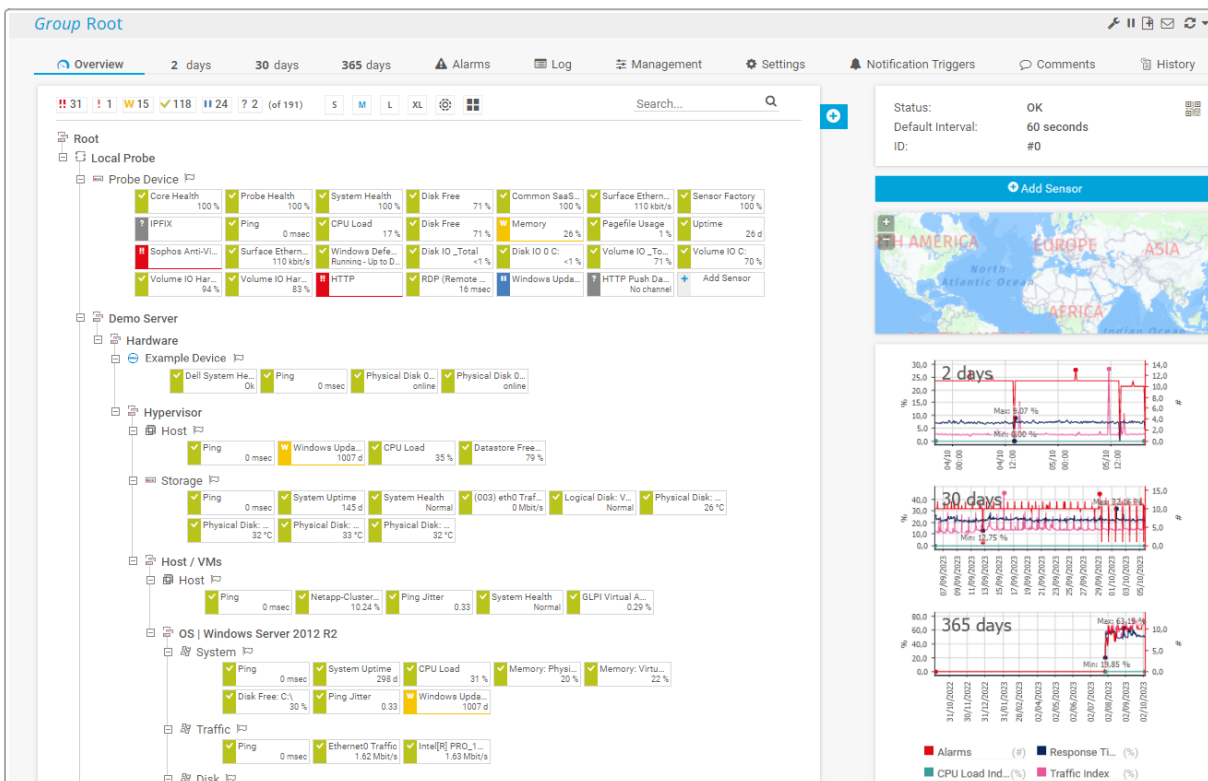
You can add additional probes and remote probes to your configuration to also monitor remote devices from outside your network.

■ For more information, see section **Add Remote Probe**<sup>[3196]</sup>.

## Group

On each probe, there are one or more **groups** that have structural purposes. Use groups to arrange similar objects so that they inherit the same settings. To a group, you add devices. You can arrange your devices in different nested groups to reflect the structure of your network.

Here you can see a sample configuration of a device tree with the local probe, several groups, devices, and their sensors:




Object Hierarchy in the Device Tree

## Device


You can add [devices](#) that you want to monitor to each probe or group. Each device in your configuration represents real hardware or a virtual device in your network, for example:

- Web or file servers
- Client computers (Windows, Linux, or macOS)
- Routers or network switches
- Almost every device in your network that has its own IP address

 You can add devices with the same IP address or Domain Name System (DNS) name multiple times. This way, you can get a more detailed overview when you use a large number of sensors or you can use different device settings for different groups of sensors. The sensors on all of these devices then query the same real hardware device in your network.

PRTG additionally adds the [probe device](#) to the local probe. This is an internal system device with several sensors. It has access to the probe system and monitors the system's health parameters.

PRTG automatically analyzes the devices that you add and recommends appropriate sensors on the Overview tab of the device. To create recommended sensors, click Add These Sensors in the Recommended Sensors table.

 For more information about the Overview tab, see the Knowledge Base: [What options do I have to review my monitoring data in detail?](#)

 You can turn off the sensor recommendation in the system administration settings under [Monitoring](#)<sup>2874</sup>.

## Sensor

On each device, you can create a number of [sensors](#). Every sensor monitors one single aspect of a device, for example:

- A network service like Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), or HTTP
- The traffic on a network switch
- The CPU load of a device
- The memory usage of a device
- The traffic on one network card
- A NetFlow device
- The system health of a device
- And much more

 For more information, see the video tutorial: [What is a sensor?](#)

## Channel

Every sensor has a number of [channels](#) through which it receives the different data streams. The available channels depend on the type of sensor. One channel can contain, for example:

- Downtime and uptime of a device
- Traffic in, Traffic out, or Traffic sum of a bandwidth device (for example, a router)
- Mail traffic of a NetFlow device
- CPU load of a device
- Loading time, Download bandwidth, or Time to first byte of a web page
- Response time of a ping request to a device
- And much more

## More

 VIDEO TUTORIAL

What is a sensor?

- <https://www.paessler.com/support/videos-and-webinars/videos/what-is-a-sensor>

## 5.4 Inheritance of Settings

The [hierarchically structured](#)<sup>[132]</sup> device tree organizes the devices in your network. This object hierarchy is the basis for the [inheritance of settings](#). Objects in the device tree can inherit their settings from a higher level. For example, you can change the scanning interval of all sensors by editing the interval setting of the root group (if you define no other setting underneath in the object hierarchy).

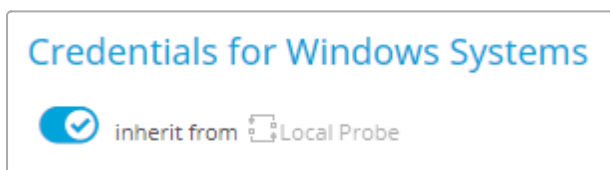
### Inheritance to Child Objects

You can override the inheritance of settings to child objects at any level of the object hierarchy if you set a different value for a specific probe, group, device, or sensor. All objects underneath inherit these new settings. Object settings from higher levels do not inherit the new settings.


Settings that are inherited to all objects include:

- Scanning intervals
  - [Notification triggers](#)<sup>[2693]</sup>
  - Credentials for different systems
  - Compatibility settings for specific sensor types
  - Channel and unit configurations
  - [Access rights](#)<sup>[145]</sup>
  - [Tags](#)<sup>[138]</sup>
  - Paused [status](#)<sup>[181]</sup>: If an object is paused by the user or by a schedule, PRTG sets all sensors on this object to the Paused status as well
- i** There is one exception for devices and sensors. Sensors [always](#) inherit the IP Address/DNS Name of a device and the compatibility settings. You cannot change these settings at sensor level.

Here you can see the Credentials for Windows Systems setting that the object inherits from the parent:



Inherited Credentials for Windows Systems

Click  next to inherit from [\[parent object\]](#) to override the parent object's settings and enter new settings for this object and all objects underneath in the object hierarchy.

Credentials for Windows Systems

**i** Click Save for your settings to take effect. If you click  after you enter your settings, the object inherits the parent object's settings again and your object-specific settings do not take effect.

## Default Settings in Root Group

For all settings except passwords, PRTG already includes a set of default values. The following settings, for example, are inherited by all sensors from the root group:

- A default scanning interval of one minute
- SNMP v1 with the community string set to public (this is the default setting for most devices)
- The dependency type Use parent (default)
- And more

Before you set up your monitoring, we recommend that you review the root group settings and set the default values to suit your setup. This includes the credentials for the different systems in your network that you want to monitor (Windows, Linux, virtual servers, different vendors, and more).

■ For more information, see section [Root Group Settings](#) <sup>420</sup>.

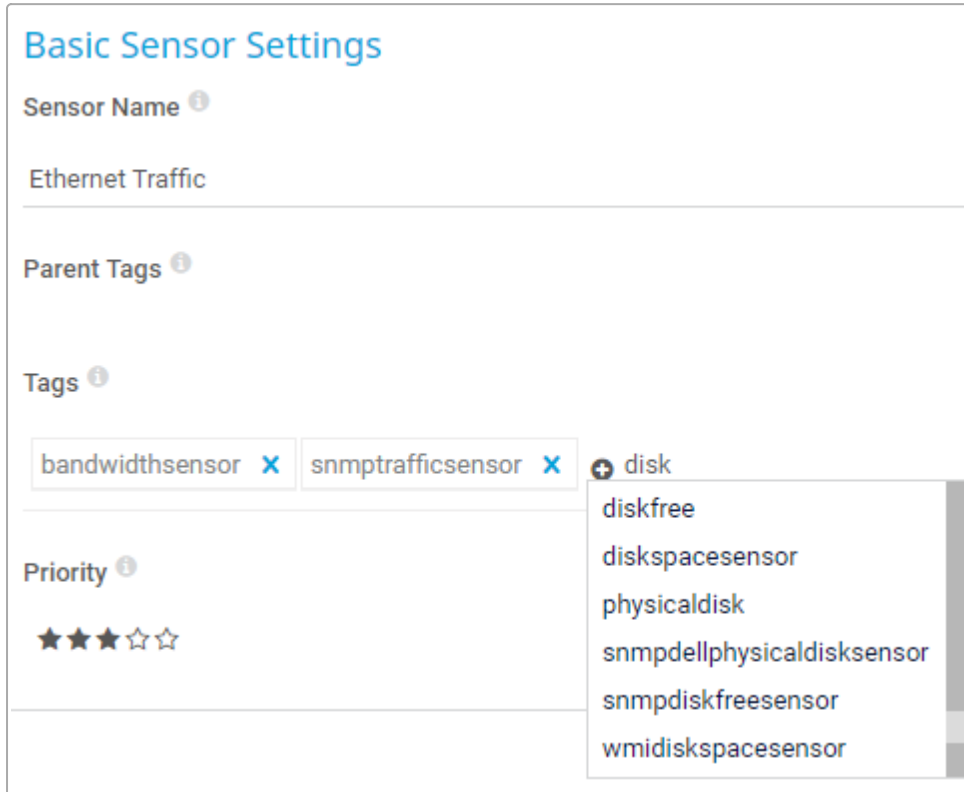
## Inheritance of Notification Triggers

If you add notification triggers at probe, group, or device level, these are also inherited to all sensors underneath in the object hierarchy unless you manually disable the inheritance.

■ For more information, see section [Notification Triggers Settings](#) <sup>2693</sup>.

## 5.5 Tags

For every object in your setup, you can define tags in the [object settings](#)<sup>[201]</sup> to additionally categorize these objects. Although some tags are predefined when you [add objects](#)<sup>[257]</sup>, you can add further tags. For example, you can mark all bandwidth sensors that are especially important for you with the tag [bandwidthimportant](#).



View and Edit Tags in Basic Sensor Settings

To confirm a tag, use the Enter key, the Spacebar key, or a comma.


- ❶ If you multi-edit tags, PRTG overwrites existing tags.
- ❷ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (<>).
- ❸ For performance reasons, it can take some minutes until you can filter for new tags that you added.

### Inheritance of Tags

Tags in object settings are automatically [inherited](#)<sup>[136]</sup> by all other objects underneath in the [object hierarchy](#)<sup>[132]</sup>. You can view inherited tags in section Parent Tags in the settings of a sensor, device, or group.

For example, a device with the tag [netflow](#) automatically passes on this tag to all sensors that you add to the device. This is useful, for example, if you include sensors by tag in [reports settings](#)<sup>[276]</sup>. PRTG adds all sensors with the tag [netflow](#) to the report so that you do not need to manually tag every single sensor.



 You cannot disable the inheritance of tags.

## Filter by Tags

You can use one or more tags to filter [table lists](#)<sup>[218]</sup> for specific objects, or to add sensors to [libraries](#)<sup>[2738]</sup> and [reports](#)<sup>[2754]</sup>.

When you filter by tags, you can also use the plus sign (+) or the minus sign (-) to categorize tags as [must have](#) or [must not have](#).

- Use a tag with a leading + to specify that objects with this tag must be included.
- Use a tag with a leading – to specify that objects with this tag must not be included.
- Use tags without a leading plus or minus sign to specify that objects need to have at least one of these tags to be included.

The filter only shows an object if all three conditions are met. The order of the tags in a tag field does not matter.

### Examples

Here are some examples that show how to filter by tags:

- If you enter [-netflow](#), the table list, library, or report includes all objects that do not have this tag. With the tags [+netflow](#) or [netflow](#), you filter for objects that have this tag.
- If you enter [+netflow -bandwidthimportant](#), the table list, library, or report includes all objects that have the tag 'netflow', but excludes all objects that have the tag 'bandwidthimportant'.
- If you enter [netflow bandwidthimportant](#), the table list, library, or report includes all objects that have either the tag 'netflow' or the tag 'bandwidthimportant' or both tags.

## Tag Display Limits

For performance reasons, PRTG has a display limit of 1,000 tags when you select Sensors | By Tag in the [main menu bar](#)<sup>[241]</sup>. If you have more than 1,000 tags, PRTG shows no tags here. You can, however, still use tags for filters and searches, for example.

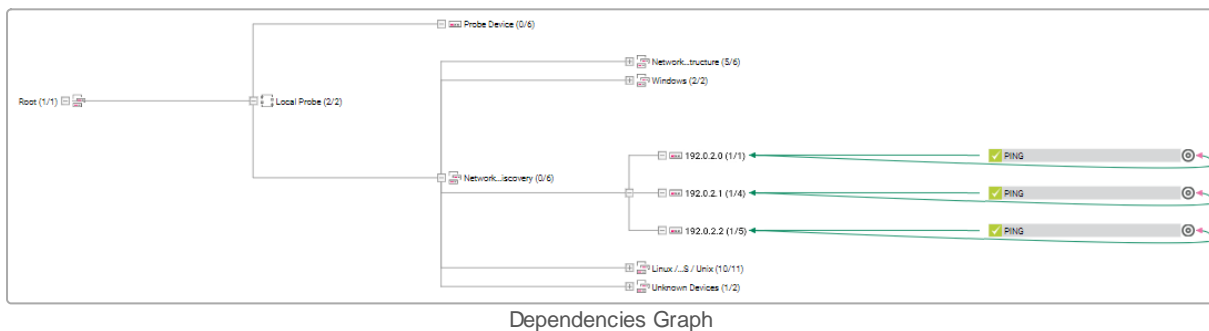
## 5.6 Dependencies

You can use dependencies to pause sensors based on the [status](#) of a different (master) sensor to avoid false alarms and incorrect downtime recording. A dependency stops the monitoring of one sensor or a set of sensors as soon as the parent sensor shows the Down status or if the parent sensor shows the Paused status because of another dependency. This means, for example, that you can stop monitoring remote network services when the corresponding firewall is down because of connection problems.

When you use the [auto-discovery](#) feature, PRTG sets the [Ping](#) sensor of a device as the [master](#) object for the device by default. This means that monitoring for the entire device is paused if the Ping sensor shows the Down status or if it shows the Paused status because of a dependency. Usually, it makes little sense to monitor any other parameters while the Ping sensor indicates that the device is unavailable.

- i** You do not trigger a status change by [dependency](#) if you manually pause a master object or if you pause it by [schedule](#). For more information, see the Knowledge Base: [Why will dependent objects not automatically pause when I pause the master object?](#)
- i** If a sensor shows the Paused status because of a dependency, the objects that use the sensor as parent also show the Paused status.

To view the list of dependencies, select Devices | Dependencies and the corresponding dependencies path from the [main menu bar](#). From there you can also access the [dependencies graph](#) that visualizes all dependencies in your network.



- For more information about the dependency settings, see the [settings of the object](#) for which you want to set a dependency, section Schedules, Dependencies, and Maintenance Window.

### More

#### ■ KNOWLEDGE BASE

Why will dependent objects not automatically pause when I pause the master object?



- <https://kb.paessler.com/en/topic/76351>

## 5.7 Scheduling

With schedules, you can specify active and inactive time spans for monitoring. For example, you can choose to monitor only on Sundays between 16:00 and 20:00. If you use scheduling, PRTG automatically [pauses](#)<sup>[227]</sup> specific objects outside of the scheduled active times. A sensor in the Paused [status](#)<sup>[181]</sup> does not collect monitoring data, does not change its status, and does not trigger any [notifications](#)<sup>[142]</sup>. You can also pause monitoring for planned system maintenance windows to avoid false alarms. You can apply different schedules to every object. PRTG also uses schedules for reports and notifications.

**i** You do not trigger a status change by [dependency](#)<sup>[140]</sup> if you manually pause a master object or if you pause it by [schedule](#)<sup>[141]</sup>. For more information, see the Knowledge Base: [Why will dependent objects not automatically pause when I pause the master object?](#)

### Schedules, Dependencies, and Maintenance Window

 inherit from  Internet

*Schedules, dependencies, and maintenance windows always pause all sensors inside a group or device. This pausing is always inherited to all child objects and the inheritance cannot be disabled. Below you can set additional schedules, dependencies, or maintenance windows that will be used in parallel to any inherited setting.*

**Schedule** **i** None ▼

**Maintenance Window** **i**

**Dependency Type** **i**

None

Saturdays [GMT+0200]

Sundays [GMT+0200]

Weekdays [GMT+0200]

**Weekdays Eight-To-Eight (8:00 - 20:00) [GMT+0200]**

Weekdays Nights (17:00 - 9:00) [GMT+0200]



Weekdays Nights (20:00 - 8:00) [GMT+0200]

Weekdays Nine-To-Five (9:00 - 17:00) [GMT+0200]

Weekends [GMT+0200]

---

**Access Rights**

 inherit from  Internet

Available Default Schedules in Device Settings

Schedules are user account specific. To change the predefined schedules or to add your own schedules, see section [Schedules](#)<sup>[2846]</sup>.

**i** If you use a cluster with cluster nodes in different time zones, the schedule applies at the local time of each cluster node. For more information, see section [Failover Cluster Configuration](#)<sup>[3208]</sup>.

### More

#### KNOWLEDGE BASE

Why will dependent objects not automatically pause when I pause the master object?

- <https://kb.paessler.com/en/topic/76351>

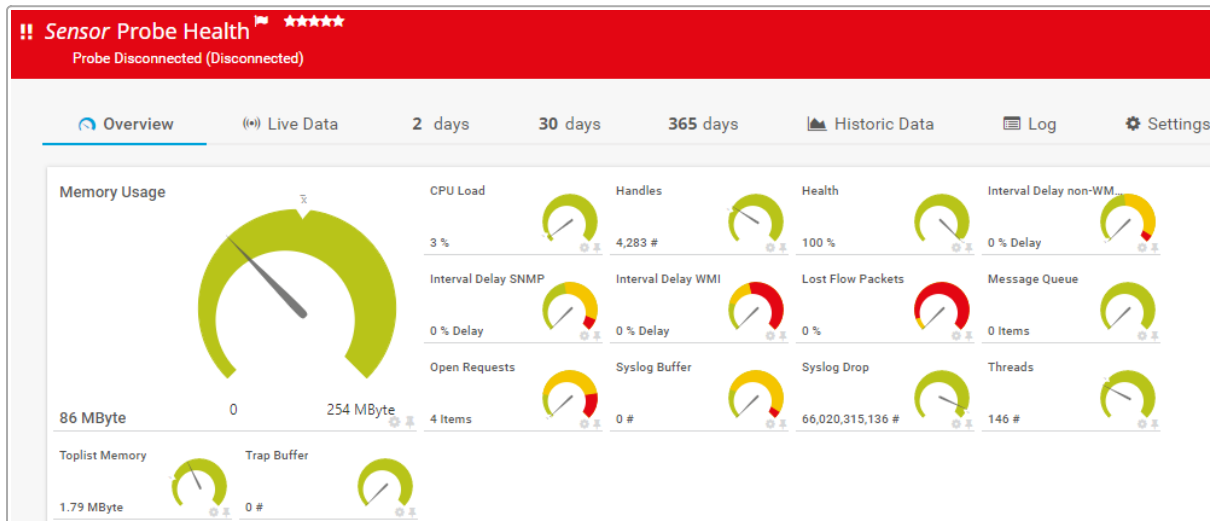
## 5.8 Notifying

PRTG keeps you or other responsible people informed about the status of the network. There are several methods that you can use to stay up to date.

### Internal Sensor Alerts

Alerts are an important part of monitoring that informs you when there are issues, when values exceed limits, or when a sensor status changes, for example. Some sensors display internal alerts in case of errors, for example, disconnected probes or socket and timeout errors. There are also sensors whose internal sensor alerts you can modify. To see if you can modify an alert, check the sensor's settings for customizable options.

Here is an example of a sensor that is in the Down [status](#)<sup>[181]</sup> because of an internal sensor alert.



Probe Health Sensor with Disconnected Probe Alert

HTTP sensors, for example, show preconfigured internal alerts based on specific HTTP status codes.

For more information, see the Knowledge Base: [Which HTTP status code leads to which HTTP sensor status?](#)

### Channel Limits

There are also alerts that are triggered by limits that you can set in the [channel settings](#)<sup>[2681]</sup> of a sensor. PRTG triggers a [sensor status](#)<sup>[181]</sup> change when a sensor measures values that exceed or fall below a defined limit. For example, you can set an [SNMP CPU Load](#) sensor to the Down status when it measures values that you consider critical. This sensor then appears in the [alarms](#)<sup>[202]</sup> list as well.

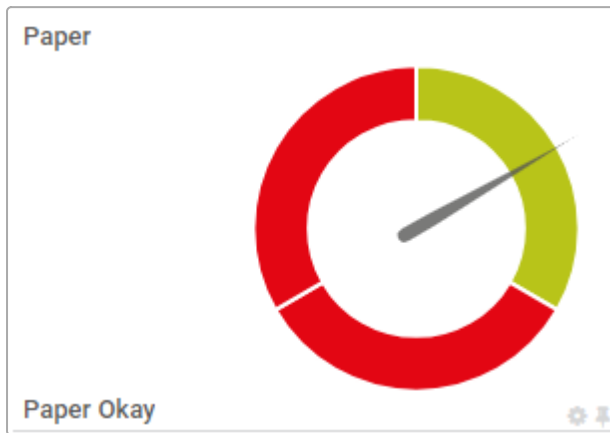
**i** This type of alert only applies when a value breaches the configured limits. If the value is normal again in the next sensor scan, the sensor shows the Up status again.

**i** The value type that you need to configure for limits depends on the type of data that the channel returns. You can set [absolute values or delta values](#)<sup>[2690]</sup>.

**▶** For more information, see the video tutorial: [How to set channel limits.](#)

## Lookups for Channels

PRTG also uses lookups for some sensors. In general, lookups make data more human friendly because they map status values that a device returns, usually integers, to more informative expressions in words that show you the status of a target device in plain text.



SNMP HP LaserJet Hardware Gauge

Additionally, lookups can define the sensor status in combination with specific status codes. For example, a sensor can show the Unknown status if a channel value, provided by lookups, indicates that the device is **inactive**, instead of displaying a numeric value like **-1**.

You can also modify preconfigured lookups or create your own custom lookups.

■ For more information, see section [Define Lookups](#) <sup>[3181]</sup>.

## Notifications

PRTG can send a [notification](#) <sup>[2735]</sup> when it discovers, for example, downtime, an overloaded system, threshold breaches, or similar situations. Notifications use various [methods](#) <sup>[2815]</sup> to notify you of issues. After you create [notification templates](#) <sup>[2808]</sup> in the system settings, you can select the templates on the Notification Triggers tab of probes, groups, devices, and sensors, as well as the root group.

The status or the data of a sensor can also trigger notifications. With this mechanism, you can configure custom external alerts. Which [notification triggers](#) <sup>[2693]</sup> are available depends on the kind of object you edit. You can define notification triggers that are activated by an 'on change' event. Some sensors offer the option to trigger a notification whenever sensor values change.

■ For more information, see section [Notifications](#) <sup>[2735]</sup>.

## Alarms

The alarms list shows all sensors that are in the Down, Down (Partial), Down (Acknowledged), Warning, or Unusual status. Sensors in the Up, Paused, or Unknown states do not appear here.

■ For more information, see section [Alarms](#) <sup>[202]</sup>.


## Logs

The logs list shows the log file that includes all monitoring events. PRTG documents the activity of every single object, so you can use this data to check if your setup works as expected.

■ For more information, see section [Logs](#) .

## Tickets

The tickets list shows tickets with important system information or actions that you need to take. We recommend that you view every ticket and take appropriate action. By default, PRTG sends an email to the [PRTG System Administrator](#) user for every new ticket that the system or a user creates. If a ticket is assigned to a specific user, this user also receives an email by default.

■ For more information, see section [Tickets](#) .

## More

### ■ KNOWLEDGE BASE

Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

### VIDEO TUTORIAL

How to set channel limits

- <https://www.paessler.com/support/videos-and-webinars/videos/how-to-set-channel-limits>

## 5.9 Access Rights Management

With the access rights management, you can define which user in which user group can access which objects in your PRTG installation, and you can manage all user access rights and group access rights.

You can create a nearly unlimited number of other users, which you can organize in a nearly unlimited number of user groups. Each user group can have separate [access rights](#)<sup>[145]</sup> for each object in the device tree except channels, as well as for libraries, maps, and reports. Objects can also [inherit](#)<sup>[136]</sup> access rights according to the [object hierarchy](#)<sup>[132]</sup>.

### User Access Rights Overview

Each user also has specific access rights. There are [administrators](#) who are user group members with administrative rights, [read/write users](#), and [read-only users](#). You can define the user type in the user account settings (read-only user or read/write user).

■ For more information, see section [User Accounts](#)<sup>[2901]</sup>.

**Account Settings**

<b>User Type</b> ⓘ	<input type="radio"/> Read/write user <input checked="" type="radio"/> Read-only user
<b>Acknowledge Alarms</b> ⓘ	<input type="radio"/> Allow user to acknowledge alarms <input checked="" type="radio"/> Do not allow user to acknowledge alarms (default)
<b>Password Change</b> ⓘ	<input type="radio"/> Allow user to change the account password <input checked="" type="radio"/> Do not allow user to change the account password (default)
<b>Primary Group</b> ⓘ	PRTG Users Group
<b>Status</b> ⓘ	<input checked="" type="radio"/> Active <input type="radio"/> Paused
<b>Last Login</b> ⓘ	(has not logged in yet)

User Access Rights in User Accounts Settings

Individual user access rights, combined with the access rights of the groups that the user is a member of, determine the access rights for device tree objects, libraries, maps, and reports. In general, group access rights override user access rights unless a user is a read-only user. Read-only users always have only read access.

You can define the group access rights for each object in the device tree via the corresponding [context menus](#)<sup>[229]</sup> or in the [object settings](#)<sup>[201]</sup>.

### Group Access Rights Overview

The following classes of group access rights are available, in hierarchical order (from the lowest group access right to the highest group access right).

ⓘ The access rights apply to device tree objects and to libraries, maps, and reports.

Group Access Rights	Description
No access	The members of the user group <b>cannot</b> see or access the object. They also cannot see or access logs, tickets, or alarms for the object.
Read access	The members of the user group can <b>only</b> view the object and its settings. <b>i</b> <b>Read-only users</b> who have been explicitly allowed to acknowledge alarms and <b>read/write users</b> in a user group that has <b>read access</b> can still acknowledge alarms. For more information, see section <a href="#">User Accounts</a> [2906].
Write access	The members of the user group can view the object and edit its settings. They can also add and delete objects, acknowledge alarms, edit notification templates, notification contacts, and schedules.
Full access	The members of the user group can view the object and edit its settings. They can also add and delete objects, acknowledge alarms, edit notification templates, notification contacts, and schedules. In addition, they can edit group access rights for objects.

If a user group has **administrative rights**, all user group members always have **full access** to every object in the device tree, library, map, and report, and all other functionalities and features of PRTG.

**i** Group access rights that you define directly on an object, for example a device, override inherited rights. If you do not define group access rights directly on an object, PRTG checks the next object that is higher up in the object hierarchy for group access rights until there is no higher-level object available.

Access Rights		
Object ▼	Access ↕	Comments ↕
PRTG Administrators	Full access	Administrator
PRTG Users Group	Write access	Defined in current object
UserGroup Admin	Full access	Administrator
UserGroup No Ticket	Read access	Defined in current object

Different Access Rights Depending on User Groups

**i** Users are either members of **PRTG user groups** or of **Active Directory groups**. They cannot be members of both types of user group. We recommend that you use only one type of user group to minimize administration.



## Group Access Rights in Combination with User Access Rights

The following table shows the correlation between group access rights and user access rights. The table applies to both PRTG user groups and Active Directory groups, as well as to both PRTG users and Active Directory users. The column headings show the group access rights to an object. The row headings show the type of user.

Group Access Rights and User Access Rights Combined				
	User group has read access to an object	User group has write access to an object	User group has full access to an object	Administrator group
Read-only user	Read access	Read access	Read access	n/a
Read/write user	Read access	Write access	Full access	Full access
Administrator	Full access	Full access	Full access	Full access

The following rules apply:

- Read-only users
  - always have only read access, no matter what access rights you define for the user groups they are members of.
  - can never see or use the ticket system.
  - can acknowledge alarms and change their own password in their user account settings, if an administrator allows them to.
  - can never be members of user groups with administrative rights.
- Read/write users
  - can use the ticket system if the user group they are members of has access to the ticket system.
  - can acknowledge alarms.
  - can change their own password.
  - can have full access to device tree objects, libraries, maps, and reports, if the user group they are members of has full access to the respective object.
  - always have administrative rights if they are members of a group with administrative rights.
- Administrators
  - are members of groups with administrative rights.
  - have no access restrictions at all.

- can also manage user accounts, user groups, and cluster setups.
  - can change the monitoring configuration of PRTG.
- ⓘ If a user is a member of more than one user group, the group access rights of the user group with the highest access rights apply.

## 5.10 Data Reporting

With PRTG, you can view, analyze, and review monitoring data for specific time spans. There are several ways to create customized data reporting.

### View Historic Sensor Data

To get an overview of a single sensor's historic data, you can generate historic data reports via the sensor's Historic Data tab.

■ For more information, see section [Historic Data Reports](#) <sup>[185]</sup>.

### Generate Reports

In addition to reports about a single sensor's historic data, you can also create comprehensive and detailed reports for all monitoring data.

■ For more information, see section [Reports](#) <sup>[2754]</sup>.

### Export Data with the PRTG API

You can also export all raw monitoring data to .xml or .csv files and generate your own reports with any third-party software.

■ For more information, see section [Application Programming Interface \(API\) Definition](#) <sup>[3084]</sup>.

### Make Data Available


You can make monitoring data available to others via a specific read-only user, or you can create public HTML pages to display your monitoring data via the [Maps](#) feature.


■ For more information, see section [Access Rights Management](#) <sup>[145]</sup> and section [Maps](#) <sup>[2776]</sup>.

## 5.11 IPv6 Support

PRTG supports the IPv6 protocol for most sensors. You can choose whether you want to query data from your network devices via an IPv4 or IPv6 connection. Specify your preference in the [device settings](#)<sup>[597]</sup>. The sensors you add to the device use the protocol that you select.

In the IPv6: Outgoing IP for Monitoring Requests setting of the [PRTG Administration Tool](#)<sup>[8058]</sup>, you can additionally select the IPv6 address that PRTG uses for outgoing monitoring requests. The same option is also available for IPv4.

 Not all sensors are IPv6 compatible. Incompatible sensors are not selectable on IPv6 devices. For an overview list of all sensors, including the IP version that they support, see section [Available Sensor Types](#)<sup>[3232]</sup>.





















 The hosted probe of a PRTG Hosted Monitor instance does not support the IPv6 protocol. If you want to use sensors that support IPv6, add them to a remote probe device.

# Part 6

## Basic Procedures

## 6 Basic Procedures

The following sections introduce the basic features and concepts of PRTG:

- [Login](#)  153
- [Welcome Page](#)  157
  - [Customer Service](#)  161
- [General Layout](#)  164
- [Sensor States](#)  181
- [Historic Data Reports](#)  185
- [Similar Sensors](#)  192
- [Recommended Sensors](#)  197
- [Object Settings](#)  201
- [Alarms](#)  202
- [System Information](#)  205
- [Logs](#)  210
- [Tickets](#)  213
- [Working with Table Lists](#)  218
- [Object Selector](#)  222
- [Priority and Favorites](#)  224
- [Pause](#)  227
- [Context Menus](#)  229
- [Hover Popup](#)  235
- [Main Menu Structure](#)  237


## 6.1 Login

For PRTG Network Monitor, you can log in to the PRTG web interface once the PRTG core server is installed. In your browser, open the IP address or Domain Name System (DNS) name of the PRTG core server system and click Log in.


You can look up and change the web server settings of PRTG Network Monitor at any time in the [PRTG Administration Tool](#)<sup>[3041]</sup> on the PRTG core server system. In particular, when you access PRTG from the internet, you should use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. To secure your connection, click Switch to SSL/TLS under Enable SSL/TLS for the PRTG web interface on the welcome screen.

### Load the PRTG Web Interface

In a web browser, enter the IP address or URL of the PRTG core server system. If you use a cluster, connect to the master node. You can also double-click the PRTG Network Monitor desktop icon on the PRTG core server system.

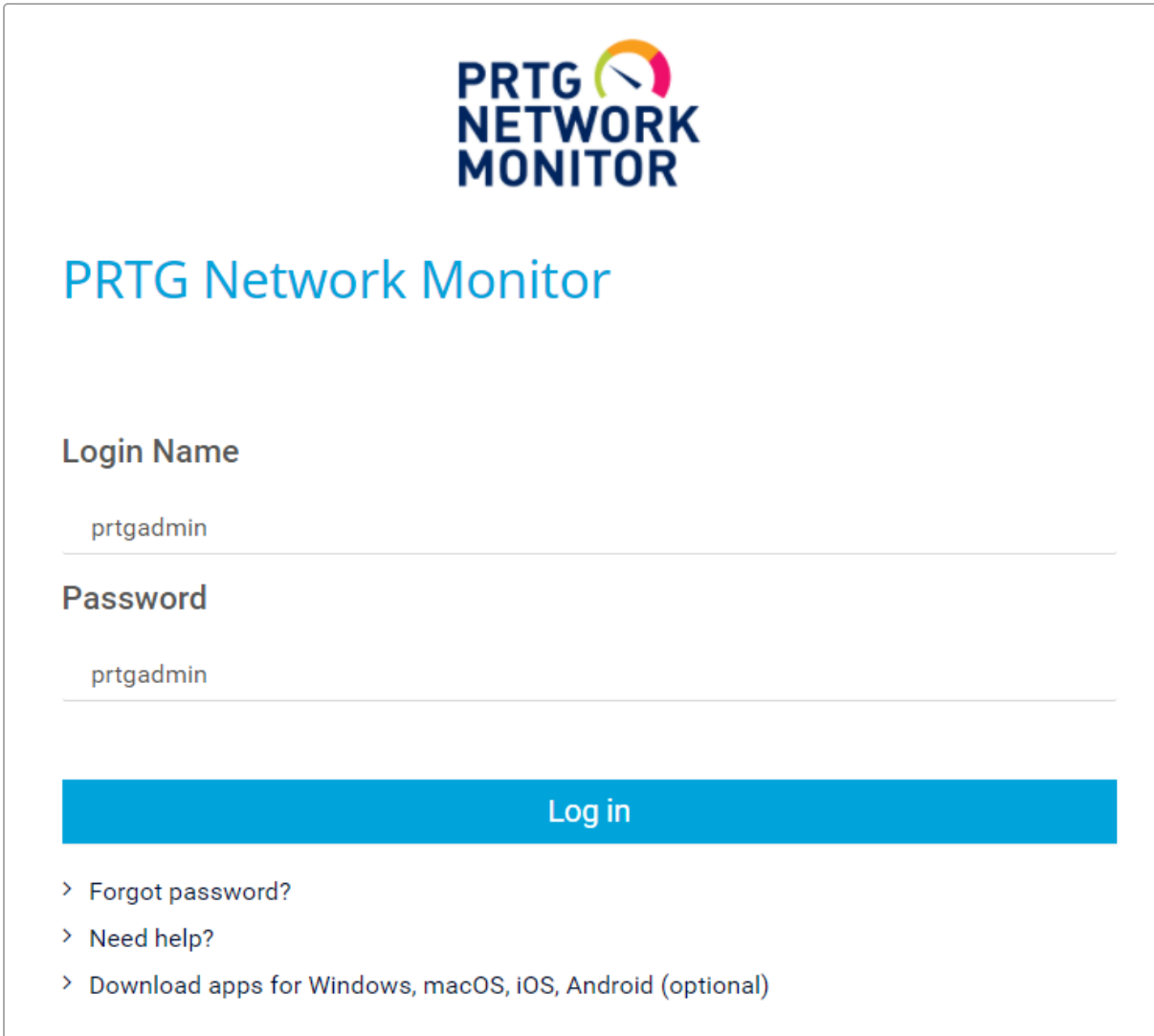
 If you run PRTG on localhost, do not use the DNS name <http://localhost> to log in to the PRTG web server, as this might considerably slow down the PRTG web interface. Use your local IP address or <http://127.0.0.1> instead.

If you see an SSL certificate warning in your browser, you can usually confirm it.

 For more information, see the Knowledge Base: [Why does my browser show an SSL certificate warning when I open the PRTG web interface?](#)

### Login Screen

After loading the PRTG web interface, the login screen is visible. You can either log in as the predefined [PRTG System Administrator](#) user or as any other user. As an administrator, you can use all functionalities of the PRTG web interface. Administrators can [create additional users](#)<sup>[2901]</sup> with administrative rights or users with more restricted user access rights (for example, read-only users).



**PRTG NETWORK MONITOR**

## PRTG Network Monitor

**Login Name**

prtgadmin

**Password**

prtgadmin

**Log in**




- > [Forgot password?](#)
- > [Need help?](#)
- > [Download apps for Windows, macOS, iOS, Android \(optional\)](#)

Login Screen

### Log In as Predefined Administrator (First Time Login)

 This option is not available in PRTG Hosted Monitor.

When you log in for the first time, the login name and password for the predefined [PRTG System Administrator](#) user account are both `prtgadmin`. PRTG automatically fills in the default credentials and shows the password in plain text.

-  After login, you should change the default password. To do so, go to [Setup | Account Settings | My Account](#) and specify a new password in section [User Account Settings](#).
-  If you are not logged in to the PRTG web interface, you can change the credentials for the predefined user account at any time in the [PRTG Administration Tool](#).
-  If you enter a different login name or change your password, the password is no longer shown in plain text.



## Log In as User

If you received user credentials from your system administrator, enter them in the login screen to log in to the PRTG web interface. This also applies if you use other administrator credentials.

## Login Options

- Log in: Log in to the fully featured PRTG web interface. We recommend that you use this option for PRTG whenever possible. It offers the full functionality of PRTG. Use Google Chrome 75 or Mozilla Firefox 67 for best performance.
  - ❗ Make sure that a [supported browser](#)<sup>[22]</sup> is available on the system.
    - Download apps for Windows, macOS, iOS, Android (optional): Opens Setup | Optional Downloads in the PRTG web interface. You can optionally [download](#)<sup>[2974]</sup> the [PRTG apps](#)<sup>[2988]</sup> for iOS or Android or the [PRTG app for desktop](#)<sup>[2984]</sup>.
  - ❗ If you use this download option, you require your login name and password for the login (or the default credentials).
- ❗ Only Google Chrome 75 and Mozilla Firefox 67 are fully compatible with the PRTG web interface.

Enter specific credentials or use the default credentials that PRTG fills in automatically. Click Log in to proceed to the PRTG web interface.

## Recover Password

If you cannot remember your PRTG Network Monitor password, click the Forgot password? link. The Password Recovery page opens. Enter your Login Name, click Request a New Password, and PRTG sends an email to the primary email address of your user account. Click the link in the email to set a new password. The link is valid for 60 minutes. Enter a New Password, then enter it again under Confirm Password. Click Set New Password to change your password.

- ❗ The password must be at least 8 characters long and must contain a capital letter and a number.
- ❗ When the password is successfully reset, all active user sessions of this user account are logged out. Log in again with the new password.

## Login Screen with Single Sign-On (SSO)

After you [configure SSO](#)<sup>[2925]</sup>, you see a new button on the login screen of the PRTG web interface.



## PRTG Network Monitor

Login Name

prtgadmin

Password

prtgadmin

Log in

> [Forgot password?](#)

Log in with single sign-on

> [Need help?](#)

> [Download apps for Windows, macOS, iOS, Android \(optional\)](#)

Log in with SSO

Click Log in with single sign-on to continue with the login procedure of the single sign-on provider. After finishing the login procedure, you will be transferred back to PRTG.

### More

#### KNOWLEDGE BASE

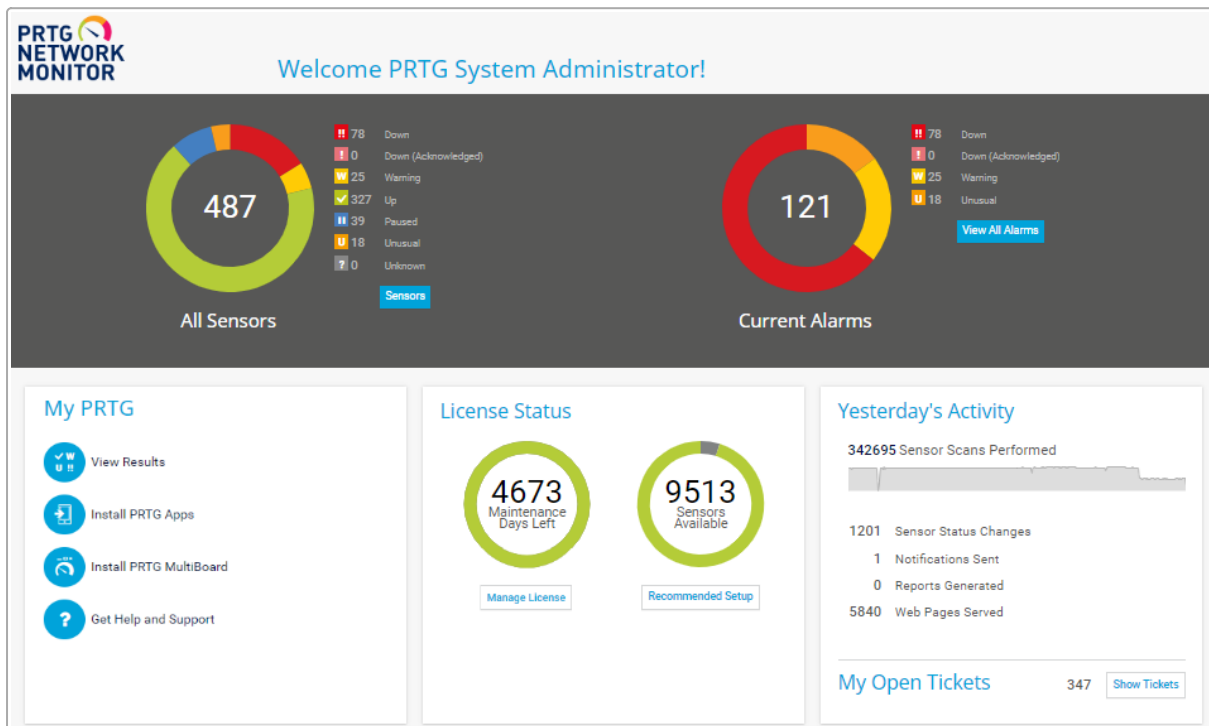
Why does my browser show an SSL certificate warning when I open the PRTG web interface?

- <https://kb.paessler.com/en/topic/89984>

## 6.2 Welcome Page

After you completed the [smart setup](#) [41], you see the Welcome page by default when you log in to the PRTG web interface. The collected information about your PRTG installation makes the page a good starting point for your daily monitoring activities. You can set a different home page in your [account settings](#) [200]. Of course, you can also use the [Maps](#) [277] feature to create customized dashboards that you can use as your home page.

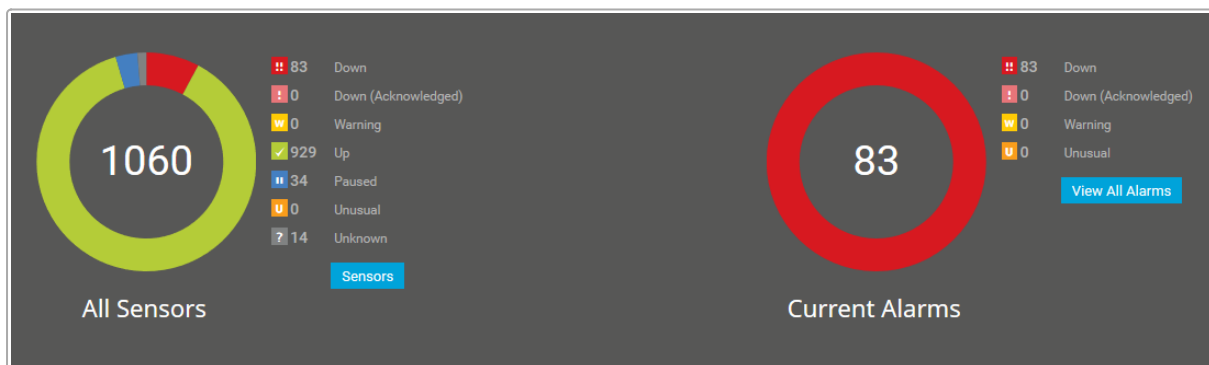
**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.



Welcome to PRTG

### Sensor Overview

The Welcome page displays various information about your PRTG installation and is similar to a dashboard. It keeps you informed about all sensors and alarms:

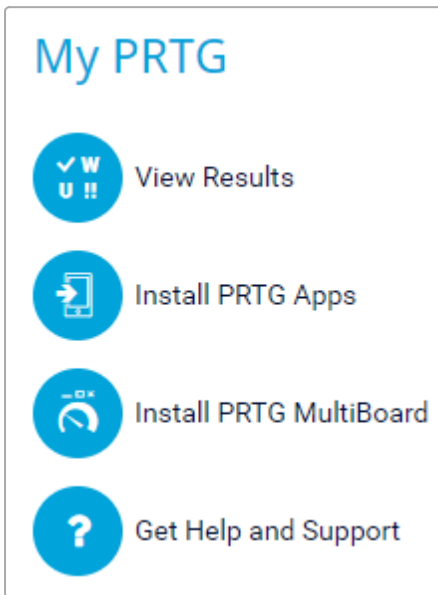


Sensor Overview on the Welcome Page


- Click Sensors to open the [top 10 lists](#) for sensors.
- Click View All Alarms to open a [list of alarms](#) in your installation.
- Click a sensor [status](#) to open a list of all sensors with the corresponding status.

## My PRTG Section

In the My PRTG section, you can directly access different pages in the PRTG web interface.



My PRTG Section on the Welcome Page

Option	Description
View Results	Open the <a href="#">device tree</a> that shows your monitoring results.
Install PRTG Apps	Open the download page for the <a href="#">PRTG apps for iOS or Android</a> .
Install PRTG MultiBoard	Open the download page for <a href="#">PRTG MultiBoard</a> .
Get Help and Support	Open the <a href="#">Help and Support Center</a> from where you can access the PRTG Manual, the Knowledge Base, and video tutorials. You can also open <a href="#">support tickets</a> and contact <a href="#">our customer service</a> from this page.
Manage Subscription	<p> This option is only visible if you use PRTG Hosted Monitor.</p> <p>Open your PRTG Hosted Monitor dashboard and manage your subscriptions.</p>

## Other Sections

Other sections are, for example, the License Status section, the Yesterday's Activity section, the Paessler Blog section, and the Update Available section.

The screenshot displays two main sections on the Welcome Page. The 'License Status' section features two circular progress indicators: one for 'Maintenance Days Left' at 4697 and another for 'Sensors Available' at 9550. Below these are buttons for 'Manage License' and 'Recommended Setup'. The 'Yesterday's Activity' section shows a total of 173326 sensor scans performed, accompanied by a mini bar chart. Below the chart, it lists: 350 Sensor Status Changes, 3 Notifications Sent, 0 Reports Generated, and 11788 Web Pages Served. At the bottom of this section, it says 'My Open Tickets' with a count of 12 and a 'Show Tickets' button.

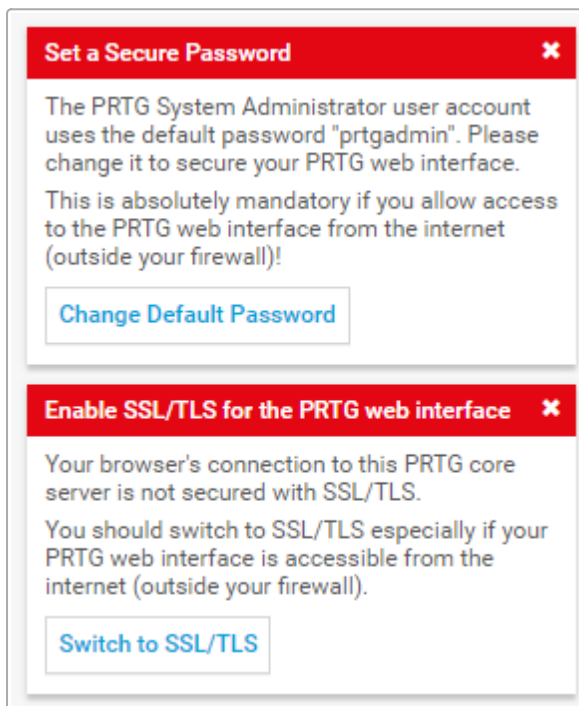
License Status Section and Yesterday's Activity Section on the Welcome Page

Section	Description
License Status	<p>Shows the remaining number of days your PRTG Network Monitor the maintenance or subscription is active and the number of sensors that you can still add with your license. Click <a href="#">Manage License</a> to open the Paessler Portal and manage your license. Click <a href="#">Get More Sensors</a> to open the Paessler Portal and upgrade your license. See also section <a href="#">License Information</a><sup>[2962]</sup>.</p> <p><b>i</b> For technical reasons, the number of available sensors that is displayed here includes sensors in the Paused status although they do not count towards the maximum number of sensors that your license allows. Add the number of <a href="#">indefinitely paused</a><sup>[227]</sup> sensors to the displayed number to know exactly how many sensors are still available on your installation.</p> <p><b>i</b> If your license has an unlimited number of sensors, PRTG takes 10,000 sensors as the starting point to calculate the number of available sensors that is displayed here. Consider the <a href="#">system requirements</a><sup>[22]</sup> for a recommended PRTG core server setup and click <a href="#">Recommended Setup</a> for more information.</p>
Yesterday's Activity	<p>Shows what your PRTG core server or PRTG Hosted Monitor instance did for you on the day before. Hover over the mini graph to show the number of sensor scans on a specific day. See also the Activity History in section <a href="#">System Status</a><sup>[2948]</sup>. Click <a href="#">Show Tickets</a> under My Open Tickets to display all open tickets that are assigned to you.</p>

Section	Description
Paessler Blog	Shows recent information about PRTG and Paessler. Click the heading of an article to open it on the Paessler website.
Update Available	This section is only visible if an update is available. It shows the version number of your PRTG Network Monitor installation and the version number of the latest available PRTG version. You see the label <b>NEW</b> if a newer version is available. Click Install Update to open the <a href="#">Auto-Update</a> page.

## Further options

There are some further options on the Welcome page, for example, you can set a secure password or enable SSL/TLS for the PRTG web interface.



Further Options on the Welcome Page

- If your PRTG Network Monitor installation is not Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured, PRTG asks you to enable SSL/TLS for the PRTG web interface. Click [Switch to SSL/TLS](#) and in the Do you want to switch to SSL/TLS? dialog, click Yes, switch to SSL/TLS to enable SSL/TLS. See also section [User Interface](#). Click to remove this note.
- If you still use the default password of the [PRTG System Administrator](#) user ([prtgadmin](#)) for PRTG Network Monitor, PRTG asks you to set a secure password if your PRTG web interface is publicly available. Click [Change Default Password](#) to define a new password. See also section [User Accounts](#). Click to remove this note.
- In the video section, you find informative videos about monitoring with PRTG. Click a video to open it and play it on the Paessler website.

## 6.2.1 Customer Service

If you have any questions about license purchases or upgrades, you can directly contact the Paessler Customer Service from the [Help and Support Center](#)<sup>[2976]</sup> in the PRTG web interface. We readily assist you with quotes or information about licenses, and guide you through the purchasing process. Our Customer Service team is also happy to send you the contact information of a knowledgeable PRTG partner in your region or research any technical specifications you might need beforehand.

① PRTG securely transmits your feedback or questions to Paessler via the PRTG Cloud. Make sure that your PRTG core server has access to the internet and can reach the URL <https://api.prtgcloud.com:443> for successful transmission.

Contact Paessler Customer Service / Send Your Feedback to Paessler ✕

---

Ask a Question or Give Us Your Feedback

Your Name

John Q. Public

---

Your Email Address

johnqpublic@example.com

---

Your Country

Deutschland (Germany) ▾

---

Your Phone Number

+49

---

How Can We Help?

Information on licensing

Need a quote

Need contact to a Technical Presales Engineer

Need contact to a partner/reseller in my country

Other

Emotional State

OK ▾

---

Describe Your Question in One Sentence <sup>?</sup>

---

**This field is required.**

Do You Have Any Further Comments?

---

Cancel OK

Contact Paessler Customer Service Form





## Ask a Question or Give Us Your Feedback

Provide the following information in this section of the Contact Paessler Customer Service form.

Field	Description
Your Name	Enter your full name for contact information.
Your Email Address	Enter an email address with which we can reach you.
Your Country	Select the country in which you run PRTG so that we can provide you with contact information for a partner nearby.
Your Phone Number	Enter a phone number with which we can reach you.
How Can We Help?	Select the scope of your question.
Emotional State	If you want to, you can indicate your feelings about PRTG and your purchase process.
Describe Your Question in One Sentence	Provide a short description that indicates the topic of your request.
Do You Have Any Further Comments?	Enter your comments here. This can be feedback or any questions for our customer service.

Click OK to send your question or feedback to our customer service. Click Cancel to close the customer service contact form without sending it.

 If you have technical questions about your setup, [contact the Paessler support team](#) .

## 6.3 General Layout

This section provides a general overview of the structure of the PRTG web interface. The central focus is the Devices view, which you can select via the [main menu bar](#)<sup>[238]</sup>. The Devices view presents the device tree and your monitoring results.

In this section:

- [Welcome Page](#)<sup>[164]</sup>
- [Device Tree View Layout](#)<sup>[164]</sup>
- [Navigation](#)<sup>[167]</sup>
- [Global Header Area](#)<sup>[168]</sup>
- [Page Header Bar](#)<sup>[170]</sup>
- [Page Content](#)<sup>[171]</sup>
- [Switch Device Tree View](#)<sup>[174]</sup>
- [Classic Device Tree View](#)<sup>[174]</sup>
- [Extended Device Tree Views](#)<sup>[175]</sup>
- [Add Button](#)<sup>[178]</sup>
- [Default Objects in the Device Tree](#)<sup>[178]</sup>
- [Priority and Favorites](#)<sup>[179]</sup>

### Welcome Page

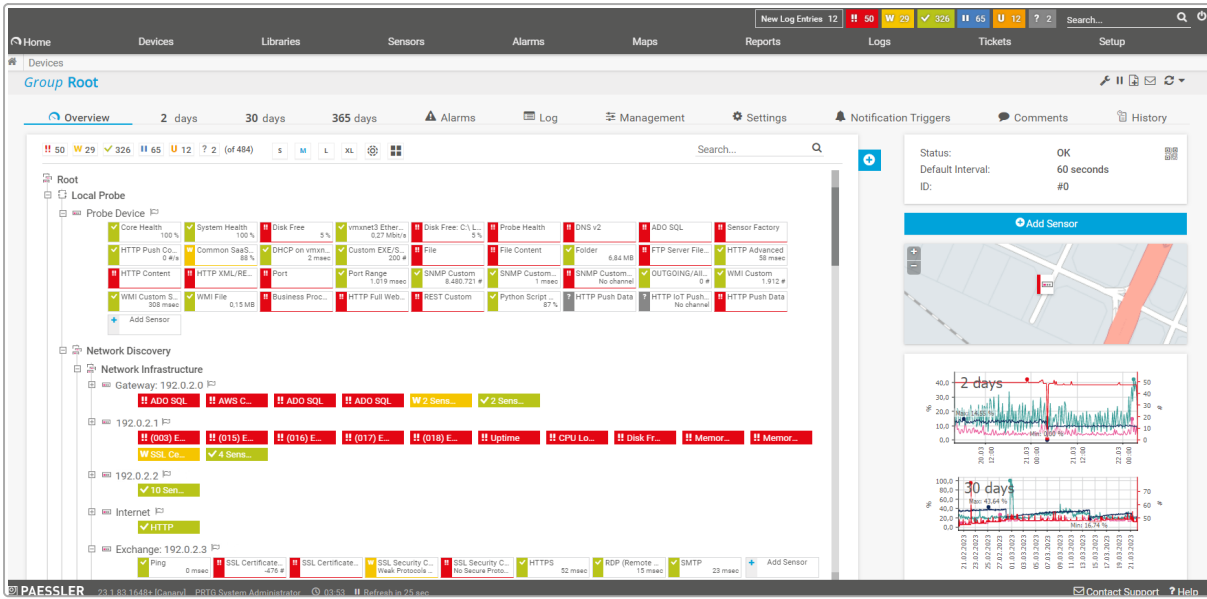
When you log in to the PRTG web interface, you see the Welcome [page](#)<sup>[157]</sup> by default. You can set a different home page in your [account settings](#)<sup>[280]</sup>.

Click View Results to open the device tree.

### Device Tree View Layout

Click View Results on the Welcome page or select Devices from the main menu bar to display the device tree.

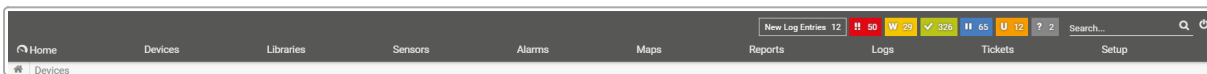
### Device Tree



Device Tree

From top to bottom, the device tree page has several areas that are covered in further detail in this section. For a general overview of the device tree page, see the table below.

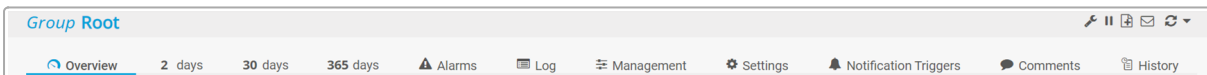
### Global Header Area



Global Header Area

Item	Description
<a href="#">Global header area</a> <sup>[168]</sup>	This area contains the main menu bar at the very top, the global status bar, breadcrumbs that show the path to the selected object, a quick search box, and the logout button.

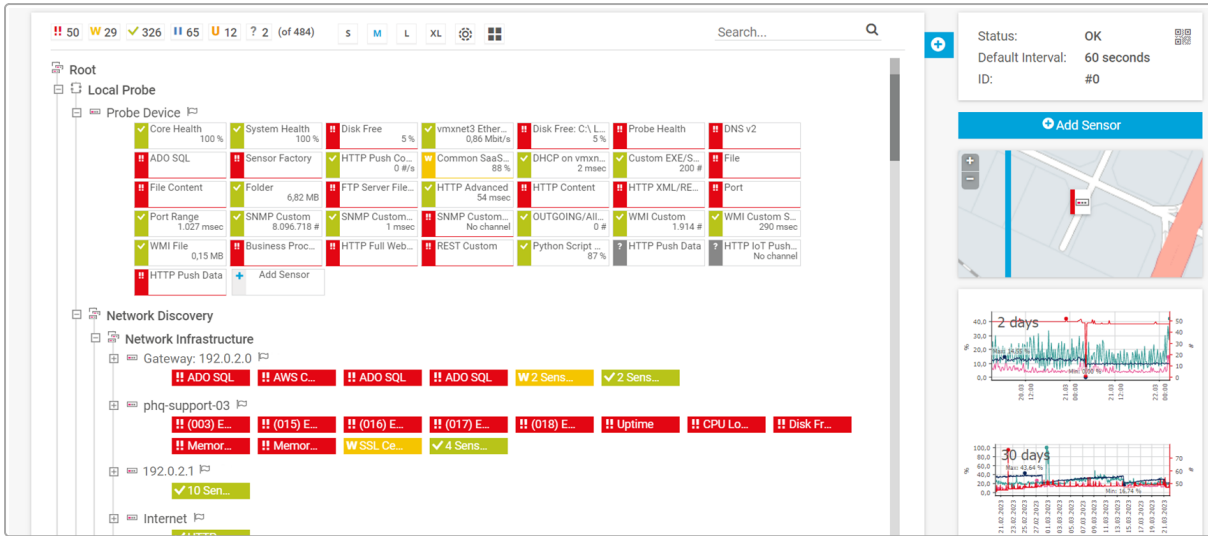
### Page Header Bar



Page Header Bar

Item	Description
<a href="#">Page header bar</a> <sup>[170]</sup>	This area contains the page heading with the name of the selected object, several tabs with settings, and quick action buttons.

### Page Content



Page Content

Item	Description
<a href="#">Page content</a> <sup>171</sup>	This area contains information about the selected object and all other objects underneath in the device tree hierarchy, the object's status bar, a quick search box, the QR code that links to the URL of the selected page, and graphs for different time spans.

View Options



View Options

Item	Description
<a href="#">Viewing options</a> <sup>174</sup>	These are part of the page content. Here you can adjust how your device tree is displayed.

Footer Section



Footer Section

Item	Description
Page footer	This area shows information about the version of PRTG, the logged in user account, and the time (depending on the <a href="#">time zone settings</a> for the logged in user).
Pause (⏸) Resume (▶) Auto-Update (🔄) Contact support (✉) Help (?)	<p>A timer counts down how much time remains until the next automatic page refresh. Click Pause to pause the refresh timer and click Resume to resume. If you open a different page while the refresh timer is paused, the timer resumes automatically and starts with the defined Refresh Interval (Sec.) that you can configure in your account settings.</p> <p><b>i</b> Long <a href="#">table lists</a> that are set to display 1000 items at a time are excluded from the automatic refresh to ensure system performance.</p> <p>Click Auto-Update for quick access to the <a href="#">auto-update</a> settings if a new version is available. To open the <a href="#">Contact Support form</a>, click Contact support. For context-sensitive help, click Help.</p> <p>If you run PRTG in a cluster, you also see a cluster-related element. It shows the name of the cluster node that you are logged in to and displays whether this is a master node or a failover node. Click the bar to show the <a href="#">cluster status</a>. On a failover node, you can review all data, but PRTG does not save changes in the settings. To change the settings, log in to the master node.</p>

## Navigation

To navigate the PRTG web interface, the following options are available:

- The main menu bar provides access to all important aspects of the software.
- The quick search is often the fastest way to find a specific object (for example, a sensor or a device).
- The clickable breadcrumbs show the path to a selected object in the object hierarchy.
- Click an object to see its details. In the page heading of the page header bar, you always see the name of the object that you have selected.
- Use the page tabs to switch between various subpages.
- Right-click objects to open their [context menu](#).
- Hover over objects to display tool tips. Hover longer to open a quick-access window ([hover popup](#)).
- Drill down into the object hierarchy of probes, groups, devices, and sensors in the device tree. To do so, click a subobject of the displayed object (for example, click a sensor on the Overview tab of a device).

These navigation options offer complete access to the functionality of PRTG.

In the following sections, we describe the different areas of the PRTG web interface.

## Global Header Area

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

## Global Header Area



Global Header Area

The global header area of the PRTG web interface provides important, very condensed information about your installation and offers access to all content and settings. The following table lists the elements that make up the global header area.

## Main Menu Bar



Main Menu Bar

Item	Description
Main menu bar	To navigate the PRTG web interface, the main menu bar is the best starting point. We recommend that you take a few minutes to familiarize yourself with the main menu bar and its submenus.  ■ For more information, see section <a href="#">Main Menu Structure</a> <sup>[237]</sup> .

## New Alarms




Item	Description
New alarms, New log entries, Updated tickets	The information boxes show how many new alarms, new log entries, and updated tickets have occurred. Click the respective box to view the lists of <a href="#">alarms</a> <sup>[202]</sup> , <a href="#">logs</a> <sup>[210]</sup> , or <a href="#">tickets</a> <sup>[213]</sup> .

## Global Sensor Status Symbols





Global Sensor Status Symbols

Item	Description
Global sensor status symbols	<p>This area shows the accumulated states of all configured sensors, grouped into the different sensor states. You see boxes with numbers that show the amount of sensors that are in the respective status. For example, you can see how many sensors are in the Up, Down, or Warning status. Click a box to view a list of all sensors that are in the respective status.</p> <p> For more information, see section <a href="#">Sensor States</a> <sup>181</sup>.</p>

### Search Box




Search Box

Item	Description
<p>Search ()</p> <p>Log out ()</p>	<p>You can start a Search or Log out in the top-right corner.</p> <p>To search for an object, enter a name, parts of a name, an IP address, a Domain Name System (DNS) name, or a tag in the search box and confirm with the Enter key. PRTG performs a string search in your entire monitoring setup, including groups, devices, sensors, libraries, maps, reports, tickets, and object comments.</p> <p>A page with items and online help articles that are related to the search term opens.</p>

### Breadcrumbs

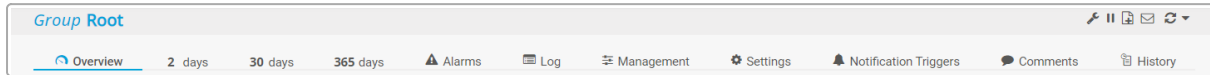


3 breadcrumbs

Item	Description
Breadcrumbs	<p>Below the main menu bar, PRTG shows a path that retraces the steps back to the Welcome page (or your defined starting page). Use these breadcrumbs to navigate back to where you came from.</p> <p>If you click  on a breadcrumb item, a dropdown list opens that shows all objects on the same level. You can either search for an object or select one directly. For example, you can directly access all other sensors on a device, other devices within a group, and other groups on the same probe. Other probes in your root group are also available.</p>

## Page Header Bar

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.



Page Header Bar

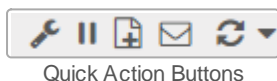
The page header bar below the global header area consists of the following elements.

### Page Heading



Item	Description
Page heading Priority star ( ★★☆☆☆ )	The page heading displays the selected object's type and name. In the screenshot, this is the group that is called <b>Root</b> . Here you can define the object's priority as well. To do so, click one of the five stars on Priority star next to the object's name (this setting is not available for the root group).  ■ For more information, see section <a href="#">Priority and Favorites</a> <sup>224</sup> .

### Quick Action Buttons

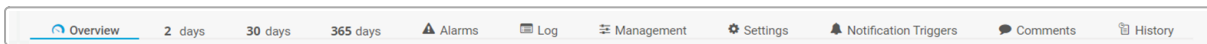


Quick Action Buttons



Item	Description
<p>Quick action buttons</p> <p>Pause (  )</p> <p>Resume (▶)</p> <p>Settings of the object (🔧)</p> <p>Add a ticket (🎫)</p> <p>Send a link to the selected page per email (✉)</p> <p>Perform an immediate scan (🔄)</p> <p>Context menu (▼)</p>	<p>On the right-hand side, there is a row of icons for several actions. Depending on the selected page, you can Pause and Resume the object. You can also open the Settings of the object, Add a ticket, Send a link to the selected page per email, or Perform an immediate scan.</p> <p>Click on Context menu to open the context menu of the selected object for further options.</p> <p>■ For more information, see section <a href="#">Context Menus</a> <sup>229</sup>.</p>

### Tabs General Layout

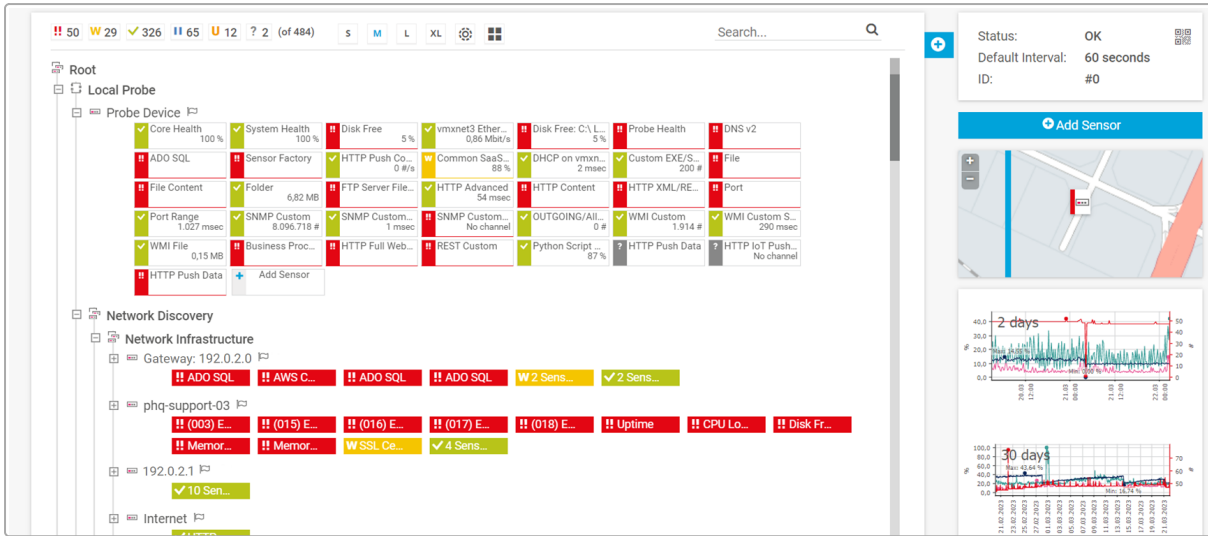


Tabs General Layout

Item	Description
<p>Tabs</p>	<p>Via tabs, you can navigate to the various subpages of an object, for example, to its monitoring data or settings.</p> <p>■ For more information, see section <a href="#">Object Settings</a> <sup>201</sup> and the Knowledge Base: <a href="#">What options do I have to review my monitoring data in detail?</a></p>

### Page Content

The page content of the general layout varies depending on the selected object. It shows information about the object and all other objects underneath in the object hierarchy. The deeper down in the hierarchy you can find a selected object, the more detailed is the displayed information.



Page Content

### Sensor Status Bar



Sensor Status Bar

Item	Description
Sensor status bar	<p>This element is visible when you view a probe, a group (including the root group), or a device. It is not available on the Overview tab of a sensor. The sensor status bar shows the accumulated states of all sensors for the selected object, grouped into different sensor states. They show the number of sensors that are in the respective status.</p> <p>For example, you can see how many sensors are in the Up, Down, or Warning status. You can hide sensors that are in a certain status by clicking the respective status icon. To show the sensors again, click the status icon again.</p> <p>For more information on sensor states, see section <a href="#">Sensor States</a> <sup>181</sup></p>

### View Options



View Options

Item	Description
Viewing options	This element is only visible when you view a probe or a group. It is not available when you view device or sensor details. For a detailed description, see <a href="#">Switch Device Tree View</a> <sup>[174]</sup> below.

Device Tree Search


Device Tree Search

Item	Description
Device tree search	In the search box to the right of the viewing options, enter a keyword to search the device tree for matching items. The device tree highlights matching devices and sensors by graying out all others. This gives you a quick overview of sensors that monitor a specific part of your network. For example, you can enter the keyword <b>firewall</b> to highlight devices and sensors that match this string.

Add Button

Item	Description
Add (+)	Click Add to add new objects to your monitoring setup. For a detailed description, see <a href="#">Add Button</a> <sup>[178]</sup> below.

Object Status

Status:	OK	
Default Interval:	60 seconds	
ID:	#0	

Object Status

Item	Description
Object status, Scanning interval, Object ID, QR code	<p>This element displays the status of the selected object, the interval in which PRTG scans the object, the ID of the object, and the QR code for the selected page. If you use a <a href="#">PRTG app for iOS or Android</a>, you can scan the code to directly view the object on your mobile device. Click the QR code to enlarge it for scanning.</p> <p>Depending on the object type, this element shows additional information:</p> <ul style="list-style-type: none"> <li>▪ All objects underneath the root group show their <a href="#">dependency</a>.</li> <li>▪ Groups and devices display the time that has elapsed since the last execution of the <a href="#">auto-discovery</a> on the selected object.</li> <li>▪ Devices show their DNS name or IP address as defined in the <a href="#">device settings</a> and the time that has elapsed since the last execution of the <a href="#">sensor recommendation</a> on this device.</li> <li>▪ Sensors show additional monitoring statistics as well as their <a href="#">performance impact</a>.</li> </ul>

## Switch Device Tree View

Wherever a probe or group is displayed, you can choose between a number of viewing options.

### Device Tree Viewing Options





## Classic Device Tree View



Via the Switch Device Tree View in the page header bar, you can adjust how much information is included next to each object. Use it to switch from a very condensed view ( **S** ) to a very spacious view ( **L** ). Use **XL** to switch the device tree to a list view.

In the classic device tree view, you can collapse devices, groups, and probes. Click  left of the object name to summarize the sensors according to their respective status. By default, sensors in the Down, Down (Partial), or Down (Acknowledged) status are summarized if there are more than ten sensors with the same status, otherwise they are displayed individually.

## Extended Device Tree Views

There are two additional options to the classic device tree view with which you can display the status of all sensors of your entire installation in a single overview. Click  to change to the sunburst view. To change to the tree map view, click .

### Sunburst View

The sunburst view displays your entire installation as a circle diagram. The groups are represented as inner circles, and all devices that belong to a group are shown as 'cake slices' that are attached to the outside of a circle element.

The sunburst is interactive:

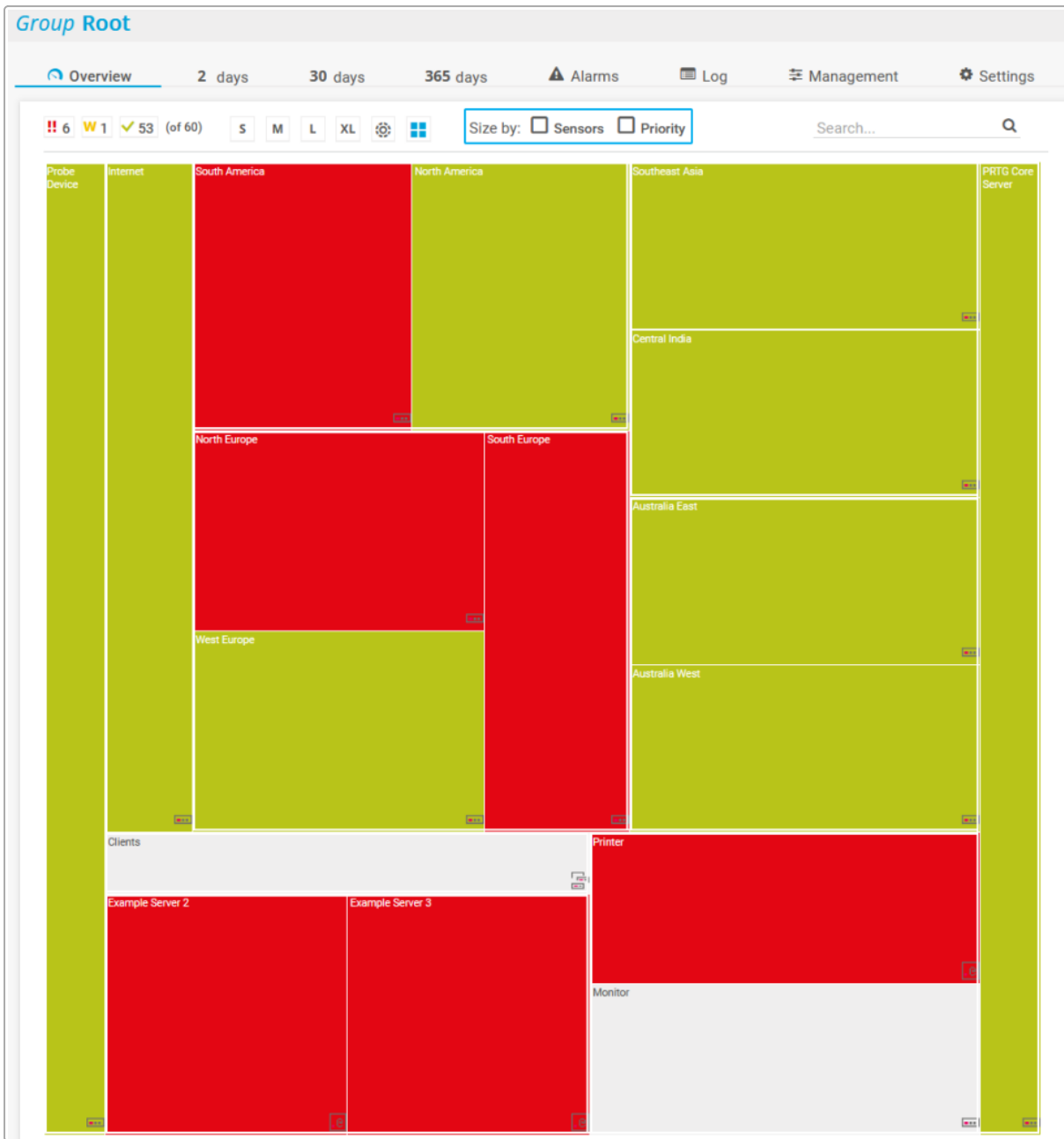
- You can click elements to open the Overview tab of your monitoring objects.
- You can zoom in and out with your mouse wheel while pressing the Ctrl key.



Sunburst View

### Tree Map View

The tree map view displays all devices of your entire installation as tiles that are sorted into a square and that are arranged according to the groups they belong to. Each device dynamically changes color to reflect the overall status of the sensors on the device.



Tree Map View

The following aspects apply to both the sunburst view and the tree map view:

### Colors

A device or group can have different colors, depending on the states of the sensors that are on the device or in the group. The sensor states are ranked according to their priority, for example, the Down status has a higher priority than the Warning status, which has a higher priority than the Up status.

■ For an overview of the colors and their states, see section [Sensor States](#)<sup>181</sup>.

Size by: Sensors / Size by: Priority

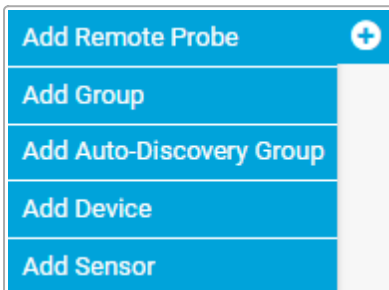
You can adjust the size of the different squares according to the number of sensors that run on a device or in a group, or the sensors' [priority](#)<sup>[224]</sup>, or both. Select the check boxes in the page header bar to change the square size.



## Add Button

Hover over  to add new objects to your monitoring setup. An assistant appears and guides you through the necessary steps.

 The content of the menu varies depending on the selected object.



Add Button Menu

See the following sections for more information:

- [Add Remote Probe](#)<sup>[3196]</sup>
- [Add an Auto-Discovery Group](#)<sup>[258]</sup>
- [Add a Group](#)<sup>[313]</sup>
- [Add a Device](#)<sup>[363]</sup>
- [Add a Sensor](#)<sup>[414]</sup>

## Default Objects in the Device Tree

By default, PRTG Network Monitor creates a [probe device](#) on the local probe or on the hosted probe (PRTG Hosted Monitor). The probe device represents the probe system. PRTG automatically monitors the system health of the PRTG core server and each probe to discover overload that might distort monitoring results. To monitor the status of the probe system, PRTG automatically creates the following sensors:



- [Core Health](#)
- [Core Health \(Autonomous\)](#)
- [Probe Health](#)
- [System Health](#)
- Some device-specific sensors for disk usage and bandwidth.

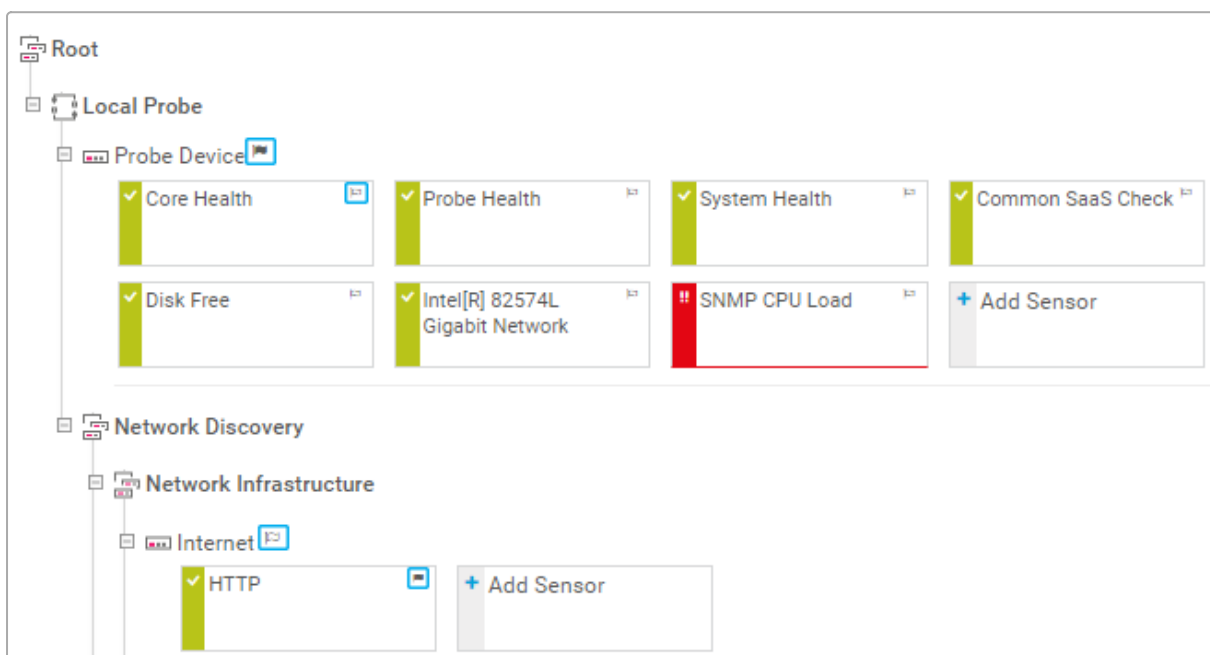


In a cluster, PRTG also creates a [cluster probe device](#) with a [Cluster Health](#) sensor that monitors the system health of the cluster.

With multi-platform probes, PRTG also creates a [Multi-Platform Probe Health](#) sensor and a [Multi-Platform Probe Connection Health \(Autonomous\)](#) sensor that monitor the health of the multi-platform probes.

## Priority and Favorites

You can mark a device or sensor as a favorite. To do so, click  to the right of the respective object in the device tree. The flag turns dark gray. To remove an object from your favorites, click . The flag turns transparent again.






One-Click Favorites in the Device Tree

 The favorite flag for sensors is available for the [L](#) or [XL](#) viewing options.

A quick way to set the priority of an object is via the five stars in the [page header bar](#)<sup>170</sup> next to the object name. Click the stars to adjust the priority. ★★★★★ means top priority, ★☆☆☆☆ means lowest priority.



One-Click Favorite and Priority in the Page Header Bar

You can also add any device or sensor to your favorites in the page header bar of the respective object. To do so, click  for a device or  for a sensor. Click  for a device or  for a sensor to remove the respective object from your favorites.

 For more information, see section [Priority and Favorites](#)<sup>224</sup>.

## More

### ■ KNOWLEDGE BASE




What options do I have to review my monitoring data in detail?






- <https://kb.paessler.com/en/topic/90007>


## 6.4 Sensor States

The color of a sensor or object indicates its status. In the table below, you find a list of states that a sensor or object can show. This list also reflects the priority of the sensor states whenever PRTG shows summarized sensor states, for example, in the [device tree](#)<sup>[164]</sup> or in [geographical maps](#)<sup>[2731]</sup>. For example, if all sensors on a device show the Up status and one of the sensors changes to the Down status, the device shows the Down status as well because this status has a higher priority. The device is then displayed accordingly in the [extended device tree views](#)<sup>[175]</sup>.

- ❗ The Down and Down (Partial) states are considered to be equal regarding status priority.
- ❗ In the device tree, hover over an object's name to view the total number of alarms for the object. In geographical maps, hover over the location marker to view the total number of alarms at this location.

Status Icon	Status Name	Meaning
	Down	<p>At least one sensor on this object (or at this location) shows the Down status.</p> <ul style="list-style-type: none"> <li>▪ PRTG is unable to reach the device or the sensor has detected an error. For more information, see section <a href="#">Sensor Behavior for the Warning and Down States</a><sup>[183]</sup>. <ul style="list-style-type: none"> <li>❗ In this case, the sensor does not record any data in its channels while it shows the Down status.</li> </ul> </li> <li>▪ There is an error limit in the <a href="#">channel settings</a><sup>[2681]</sup> or the sensor shows the Down status because of a <a href="#">lookup</a><sup>[3181]</sup>. <ul style="list-style-type: none"> <li>❗ In this case, the sensor continues to record data in all channels although it shows the Down status.</li> </ul> </li> </ul>
	Down (Partial)	<p>In a cluster, at least one cluster node reports that this sensor shows the Down status, while at least one other cluster node reports that the same sensor shows the Up status.</p> <ul style="list-style-type: none"> <li>❗ This status is not available for sensors on remote probes in a <a href="#">failover cluster</a><sup>[128]</sup>.</li> </ul>
	Down (Acknowledged)	<p>At least one sensor on this object (or at this location) showed the Down status and a user acknowledged this status via Acknowledge Alarm in the <a href="#">context menu</a><sup>[229]</sup>.</p> <ul style="list-style-type: none"> <li>▪ There is no sensor in the Down status.</li> <li>❗ For acknowledged alarms, PRTG does not send further <a href="#">notifications</a><sup>[2735]</sup>.</li> </ul>

Status Icon	Status Name	Meaning
		<p> If you pause and resume a sensor in the Down (Acknowledged) status, it shows the Down status again.</p>
	Warning	<p>At least one sensor on this object (or at this location) shows the Warning status.</p> <ul style="list-style-type: none"> <li>▪ The sensor detected an error and shows the Warning status but the sensor is trying to reach the target device again. The sensor might soon change to the Down status. For more information, see <a href="#">Sensor Behavior for the Warning and Down States</a><sup>[183]</sup>.</li> <li>▪ There is a warning limit in the channel settings or the sensor shows the Warning status because of a lookup.</li> <li>▪ There is no sensor in the Down or Down (Acknowledged) status.</li> </ul>
	Unusual	<p>At least one sensor on this object (or at this location) shows the Unusual status.</p> <ul style="list-style-type: none"> <li>▪ The sensor reports unusual values for this weekday and this time of the day. The unusual detection is based on the sensor's historic average data. You can configure or disable the unusual detection in the system administration settings under <a href="#">Monitoring</a><sup>[2871]</sup>.</li> <li>▪ You can also disable the unusual detection for specific groups. <ul style="list-style-type: none"> <li>■ For more information, see section <a href="#">Group Settings</a><sup>[593]</sup>.</li> </ul> </li> <li>▪ There is no sensor in the Down, Down (Acknowledged), or Warning status.</li> </ul>
	Up	<p>All sensors on this object (or at this location) show the Up status.</p> <ul style="list-style-type: none"> <li>▪ The last scan was okay and the sensors receive data.</li> <li>▪ There is no sensor in the Down, Down (Acknowledged), Warning, Paused, or Unusual status.</li> </ul>
	Paused	<p>All sensors on this object (or at this location) show the Paused status.</p>

Status Icon	Status Name	Meaning
		<ul style="list-style-type: none"> <li>The sensor is paused for a specific time span, indefinitely, or because of a <a href="#">dependency</a><sup>[140]</sup>.</li> <li>There is no sensor in the Down, Down (Acknowledged), Warning, Unusual, or Up status.</li> </ul> <p><b>i</b> A sensor in the Paused status does not count towards the maximum number of sensors that your license allows.</p>
	Unknown	<p>All sensors on this object (or at this location) show the Unknown status.</p> <ul style="list-style-type: none"> <li>The sensor has not received any data yet or there is an error in (network) communication, likely on the probe system. If sensors continuously show this status, you might need to restart PRTG. <ul style="list-style-type: none"> <li>For more information about extended troubleshooting, see the Knowledge Base: <a href="#">What to check if sensors are gray?</a> and <a href="#">My sensors show the Unknown status after a PRTG core server restart. What can I do?</a></li> </ul> </li> <li>There is no sensor in the Down, Down (Acknowledged), Warning, Unusual, Paused, or Up status.</li> </ul>

## Sensor Behavior for the Warning and Down States

The Down status indicates that there is an issue with an object, for example, a device. There are various reasons for the Down status, for example, an interruption in the physical connection to the device or an internet connection outage.

After a failed request, PRTG tries to contact the device again before it sets a sensor to the Down status (this is true for almost all sensors):

- If a request to a device fails for the first time, the sensor changes to the Warning status. PRTG repeats the request and immediately attempts to rescan the device.
- If the second request also fails, the sensor changes to the Down status by default until the device is reachable again. You can change this behavior in the [scanning interval](#)<sup>[450]</sup> settings of any object in the device tree. PRTG tries to reach the device with every scanning interval.

This procedure gives devices and services the chance to recover from a momentary overload and prevents false alarms. Still, you are immediately informed about any network issues.

- i** This behavior does not apply to the Warning or Down states that result from warning limits or error limits in the channel settings. This behavior also does not apply to channels that use lookups.

## More

### KNOWLEDGE BASE

What to check if sensors are gray?

- <https://kb.paessler.com/en/topic/25643>

My sensors show the Unknown status after a PRTG core server restart. What can I do?

- <https://kb.paessler.com/en/topic/87266>

### VIDEO TUTORIAL

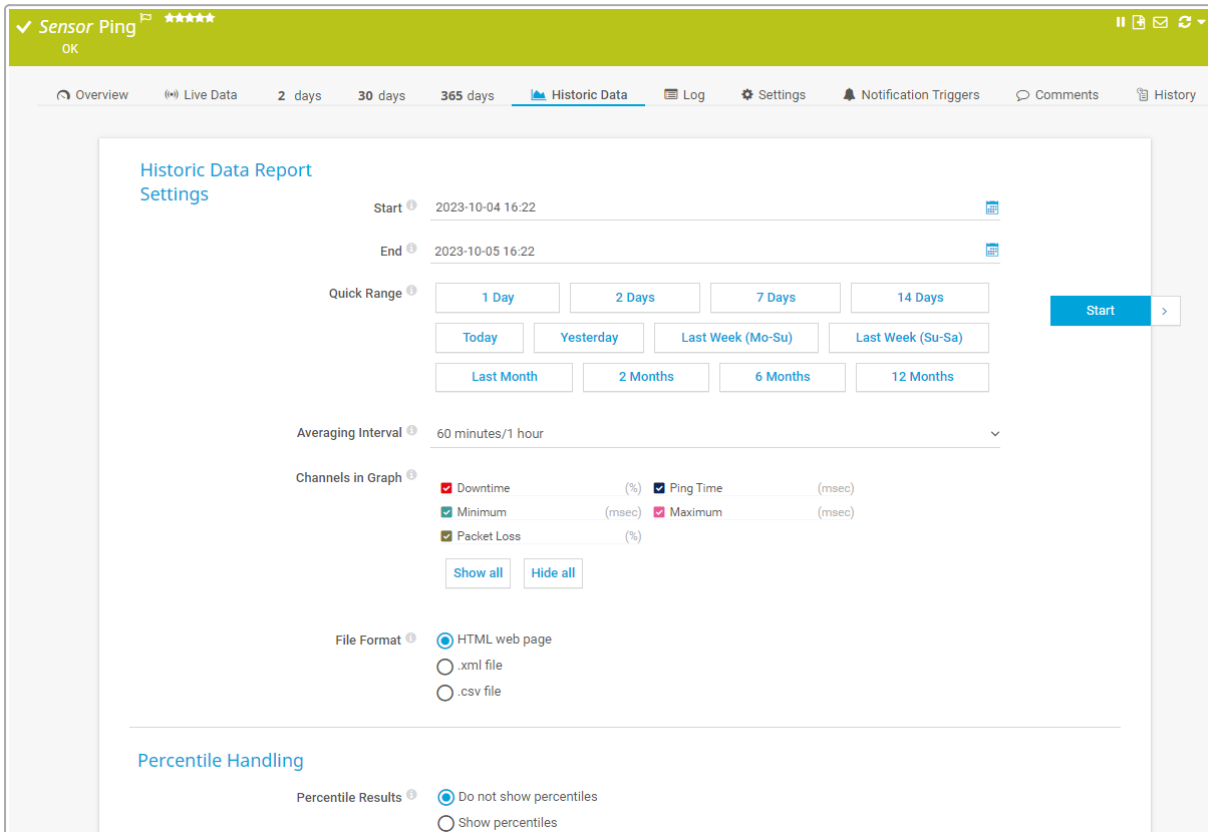
Sensor states

- <https://www.paessler.com/support/videos-and-webinars/videos/sensor-states>

## 6.5 Historic Data Reports

For quick reviews of a sensor's monitoring data, use historic data reports as an alternative to the comprehensive [reports](#) feature. You can run and view a historic data report for each sensor on demand. Additionally, you can export a sensor's historic data as an .xml file or a .csv file to your computer to further process the data with third-party applications.

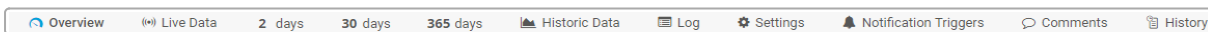
There are two ways to open historic data reports: Either click the Historic Data tab of a sensor or select Sensors | View Historic Data from the [main menu bar](#).



Historic Data Tab of a Ping Sensor

### Historic Data (Sensor Tab)

Probe, group, device, and sensor pages have tabs that you can use to navigate between different options. For example, you can view your network's status, view monitoring results, or change settings.



Tabs Bar for Sensors

The Historic Data tab is only available for sensors, not for probes, groups, or devices. When you open the Historic Data tab of a sensor, no sensor selection is available. If you want to select a different sensor for the report, select Sensors | View Historic Data from the main menu bar.

## Historic Monitoring Data (Sensors Main Menu)

When you open historic data reports via Sensors | View Historic Data from the main menu bar, PRTG asks you to select the sensor for which you want to create a report with the [object selector](#)<sup>[222]</sup>.

## Historic Data Report Settings

### Historic Data Report Settings

Start ⓘ 2023-10-04 16:22 📅

End ⓘ 2023-10-05 16:22 📅

Quick Range ⓘ

1 Day
2 Days
7 Days
14 Days

Today
Yesterday
Last Week (Mo-Su)
Last Week (Su-Sa)

Last Month
2 Months
6 Months
12 Months

Averaging Interval ⓘ 60 minutes/1 hour ▼

Channels in Graph ⓘ

Downtime (%)
  Ping Time (msec)

Minimum (msec)
  Maximum (msec)

Packet Loss (%)

Show all
Hide all

File Format ⓘ

HTML web page

.xml file

.csv file

Historic Data Report Settings

Setting	Description
Sensor	<p>This setting is only visible if you open View Historic Data from the main menu bar.</p> <p>To select the sensor for which you want to create the report, click  to open the object selector.</p> <p> For more information, see section <a href="#">Object Selector</a><sup>[222]</sup>.</p>
Start	<p>Specify the start date and time for the data that you want to review. Use the date time picker to enter the date and time.</p> <p> You cannot generate the historic data report if monitoring data was <a href="#">deleted</a><sup>[289]</sup> after the specified start date. Set the start of the report to a date for which data is available.</p>



Setting	Description
End	Specify the end date and time for the data that you want to review. Use the date time picker to enter the date and time.
Quick Range	<p>You can use several buttons to select start and end dates more quickly. Click any of these buttons to change the Start and End values:</p> <ul style="list-style-type: none"> <li>▪ 1 Day, 2 Days, 7 Days, or 14 Days: Set the <a href="#">date range</a><sup>[220]</sup> to the respective day or days. The current time of the current day is the end date.</li> <li>▪ Today, Yesterday, Last Week (Mo-Su), Last Week (Su-Sa), Last Month, 2 Months, 6 Months, 12 Months: Set the date range to the last matching period. It starts at 00:00 and ends at 00:00 of the following day.</li> </ul>
Averaging Interval	<p>With this option, you can activate and configure averaging. Select an interval for which PRTG calculates the average value:</p> <ul style="list-style-type: none"> <li>▪ No interval (display raw data): PRTG performs no averaging and displays only raw data. <ul style="list-style-type: none"> <li>ⓘ PRTG stores raw data for up to 40 days. After this time, PRTG calculates averages again.</li> </ul> </li> <li>▪ 15 seconds, 30 seconds, or 60 seconds/1 minute</li> <li>▪ 2 minutes, 5 minutes, 10 minutes, 15 minutes, 20 minutes, or 60 minutes/1 hour</li> <li>▪ 2 hours, 4 hours, 6 hours, 12 hours, or 24 hours/1 day</li> </ul> <p>ⓘ A shorter interval results in a more detailed historic data report for the sensor.</p> <p>The best settings for you depend on the scanning interval of the sensor, the selected time period, and the intended use for the historic data report. Try different settings and compare the results. See also <a href="#">Automatic Averaging</a><sup>[190]</sup> in this section.</p>
Channels in Graph	<p><a href="#">This setting is only visible if you view historic data via the Historic Data tab of a sensor.</a></p> <p>Select the channels that you want to include in the graph of the historic data report. You can select individual channels via the respective check boxes, and show or hide all channels via the Show all or Hide all buttons. In the graph, PRTG then only shows the data of selected channels.</p> <p>ⓘ The historic data report table always shows the data of all channels.</p>
Cluster Node	<p><a href="#">This setting is only visible if the sensor runs on a cluster probe.</a></p>

Setting	Description
	<p>Select the cluster node's data that PRTG includes in the historic data report:</p> <ul style="list-style-type: none"> <li>▪ All nodes: Include the data of all cluster nodes in the report.</li> <li>▪ [Several specific nodes]: Use a specific cluster node's data for the report. The cluster nodes you see are specific to your setup.</li> </ul>
File Format	<p>Select the output format for the report:</p> <ul style="list-style-type: none"> <li>▪ HTML web page: Display the result directly as an HTML web page. This is also a good option if you want to check the results before you export them to a different file format.</li> <li>▪ .xml file: Export the data as an .xml file. Your browser usually shows a download dialog when you use this option.</li> <li>▪ .csv file: Export the data as a .csv file, for example, to import it into Microsoft Excel. Your browser usually shows a download dialog when you use this option.</li> </ul>

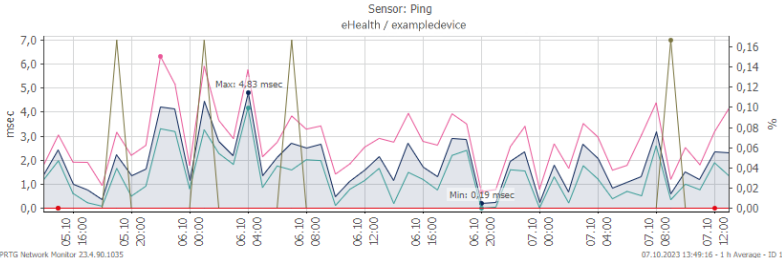
## Percentile Handling

### Percentile Handling

Percentile Results ⓘ  Do not show percentiles  
 Show percentiles

Percentile Handling

Setting	Description
Percentile Results	<p>Define if you want to include an additional <a href="#">percentile calculation</a> ⓘ of your data in the historic report:</p> <ul style="list-style-type: none"> <li>▪ Do not show percentiles: PRTG does not use a percentile formula to calculate your monitoring results. It only shows the standard values.</li> </ul>

Setting	Description																																								
	<ul style="list-style-type: none"> <li>Show percentiles: PRTG displays an additional percentile calculation for the <b>primary</b> channel in the value table for each scanning interval.</li> </ul> <div data-bbox="512 472 1342 1232" style="border: 1px solid #ccc; padding: 10px;"> <p><b>Report for Ping</b></p> <p>Report Time Span: 05.10.2023 13:47:00 - 07.10.2023 13:47:00</p> <p>Sensor Type: Ping (30 s interval)</p> <p>Probe, Group, Device: Local Probe &gt; eHealth &gt; exampledevice</p> <p>Uptime Stats: Up: 100 % [01d 23h 59m 30s] Down: 0 % [00s]</p> <p>Request Stats: Good: 100 % [5761] Failed: 0 % [0]</p> <p>Average (Ping Time): 2 msec</p> <p>Percentile: 11 msec</p>  <p>Legend: Downtime (%), Ping Time (msec), Minimum (msec), Maximum (msec), Packet Loss (%)</p> <table border="1" data-bbox="526 1064 1340 1232"> <thead> <tr> <th>Date Time</th> <th>Ping Time (msec)</th> <th>Minimum (msec)</th> <th>Maximum (msec)</th> <th>Packet Loss (%)</th> <th>Downtime (%)</th> <th>Percentile (Ping Time)</th> <th>Coverage (%)</th> </tr> </thead> <tbody> <tr> <td>Averages (of 48 values)</td> <td>2 msec</td> <td>1 msec</td> <td>3 msec</td> <td>&lt;1 %</td> <td>0 %</td> <td></td> <td>99 %</td> </tr> <tr> <td>05.10.2023 13:00:00 - 14:00:00</td> <td>1 msec</td> <td>1 msec</td> <td>2 msec</td> <td>0 %</td> <td>0 %</td> <td>1 msec</td> <td>43 %</td> </tr> <tr> <td>05.10.2023 14:00:00 - 15:00:00</td> <td>2 msec</td> <td>2 msec</td> <td>3 msec</td> <td>0 %</td> <td>0 %</td> <td>11 msec</td> <td>100 %</td> </tr> <tr> <td>05.10.2023 15:00:00 - 16:00:00</td> <td>1 msec</td> <td>1 msec</td> <td>2 msec</td> <td>0 %</td> <td>0 %</td> <td>1 msec</td> <td>100 %</td> </tr> </tbody> </table> <p>Example of a Historic Data Report with Percentile Calculation for the Primary Channel</p> </div>	Date Time	Ping Time (msec)	Minimum (msec)	Maximum (msec)	Packet Loss (%)	Downtime (%)	Percentile (Ping Time)	Coverage (%)	Averages (of 48 values)	2 msec	1 msec	3 msec	<1 %	0 %		99 %	05.10.2023 13:00:00 - 14:00:00	1 msec	1 msec	2 msec	0 %	0 %	1 msec	43 %	05.10.2023 14:00:00 - 15:00:00	2 msec	2 msec	3 msec	0 %	0 %	11 msec	100 %	05.10.2023 15:00:00 - 16:00:00	1 msec	1 msec	2 msec	0 %	0 %	1 msec	100 %
Date Time	Ping Time (msec)	Minimum (msec)	Maximum (msec)	Packet Loss (%)	Downtime (%)	Percentile (Ping Time)	Coverage (%)																																		
Averages (of 48 values)	2 msec	1 msec	3 msec	<1 %	0 %		99 %																																		
05.10.2023 13:00:00 - 14:00:00	1 msec	1 msec	2 msec	0 %	0 %	1 msec	43 %																																		
05.10.2023 14:00:00 - 15:00:00	2 msec	2 msec	3 msec	0 %	0 %	11 msec	100 %																																		
05.10.2023 15:00:00 - 16:00:00	1 msec	1 msec	2 msec	0 %	0 %	1 msec	100 %																																		
<p>Percentile Type</p>	<p>This setting is only visible if you select Show percentiles above.</p> <p>Enter the percentile type that you want PRTG to use for the calculation. If you choose, for example, to calculate the 95th percentile, enter <b>95</b> here and 5% of peak values are discarded. Enter an integer.</p>																																								
<p>Percentile Averaging Interval</p>	<p>This setting is only visible if you select Show percentiles above.</p> <p>Enter a value to define the averaging interval on which PRTG bases the percentile calculation. The default value is <b>300</b> seconds (5 minutes). This means that PRTG takes 5-minute averages as basic values for the percentile calculation. Enter an integer.</p>																																								
<p>Percentile Mode</p>	<p>This setting is only visible if you select Show percentiles above.</p> <p>Select the mode for percentile calculation:</p> <ul style="list-style-type: none"> <li>Discrete: PRTG takes discrete values to calculate percentile results.</li> <li>Continuous: PRTG interpolates between discrete values and bases the calculation on interpolated values.</li> </ul>																																								

Click Start to generate a historic data report.

**i** You cannot generate the historic data report if monitoring data was [deleted](#) after the specified start date. Set the start of the report to a date for which data is available.

## Remarks for Reports

- Any sensor graph in your report only shows channels that you select via the Show in graphs option in the [channel settings](#).
- Reports show statistics for the uptime (the Up and Down [states](#) in percent) and for requests ([Good](#) and [Failed](#) in percent). PRTG rounds values between 5% and 95%, as well as 100% and 0%, to whole numbers without decimal places. Other values are shown with 3 decimal places.
- Because PRTG rounds values, the statistics in the report section Sensor Status History can differ from the values in the report section Uptime Stats by a few seconds.
- PRTG limits data reporting to 5 requests per minute.
- Reports cannot show uptime or downtime data for the [Sensor Factory](#) sensor.
- Create reports that include an appropriate amount of data. Reports might not work as expected if PRTG has to process too many sensors with short scanning intervals. Adjust your report size and the time span that the report covers, if necessary.

## Automatic Averaging

For performance reasons, PRTG automatically averages monitoring data when it calculates data for large periods of time.

Period of Time in Report	Minimum Level of Detail (Averaging Interval)
Up to 40 days	Any
40 to 500 days	60 minutes/1 hour or longer

**i** Reports for periods that are longer than 500 days are not possible. If you enter a longer period, PRTG automatically shortens it to 365 days.

**i** In some cases, the generated report might contain a period of time that differs from the defined start and end date for the report because of internal averaging processes. When averaging intervals are longer than 1 hour and do not equal 24 hours, and when they are combined with specific periods of time, the resulting data points might be asynchronous to the periods of time. Consider this behavior particularly if you use [application programming interface \(API\) calls](#) to generate reports.

## More

### ■ KNOWLEDGE BASE

Why is there missing data in historic data reports?

- <https://kb.paessler.com/en/topic/61382>

How does PRTG compute CPU Index, Traffic Index and Response Time Index?

- <https://kb.paessler.com/en/topic/313>

## 6.6 Similar Sensors

With PRTG, you can detect relationships between different components in your network. For example, you can detect extraordinarily high CPU load that correlates with extraordinarily high traffic at a specific time of a day or week. This can give you a hint to further investigate that part of your network.

### What Is Similarity?

The similarity calculation is based on the values that are saved in the sensor history. If measured values change in the same way, the [Similar Sensors Detection](#) feature detects it and shows you the sensors for which it found similar data relations. PRTG shows all sensors that reach 85% to 100% similarity.

The analysis of similar sensors is a heuristic calculation that shows interconnections and correlations in your network. The analysis is completely automated. It is based on mathematics and fuzzy logic and optimizes your sensor usage by tracking redundant monitoring of some aspects of your system.

### Similar Sensors Detection

You can adjust the depth of the similar sensors detection or turn it off under Setup | System Administration | Monitoring.

### Similar Sensors Detection

**Analysis Depth** ⓘ

- Manage automatically based on sensor count (default)
- Analyze only primary channels
- Analyze all channels (higher CPU load)
- Disable detection of similar sensors

Similar Sensors Detection Settings

You can also enable or disable the similar sensors detection for specific probes, groups, and devices, and specify [inheritance](#)<sup>[136]</sup> in the [object's settings](#)<sup>[201]</sup>, section Advanced Network Analysis.

### Advanced Network Analysis

	<b>Unusual Detection</b> ⓘ	<input checked="" type="radio"/> Enable (default) <input type="radio"/> Disable
	<b>Similar Sensors Detection</b> ⓘ	<input checked="" type="radio"/> Enable (default) <input type="radio"/> Disable
	<b>System Information</b> ⓘ	<input checked="" type="radio"/> Enable (default) <input type="radio"/> Disable

Activation of the Similar Sensors Detection

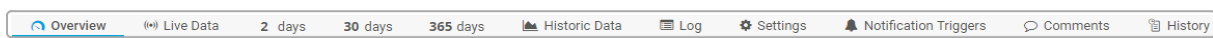
There are two options to view similar sensors:

- Via the Overview tab of sensors that includes a [Similar Sensors section](#)<sup>193</sup> where PRTG lists channels that show similarities to channels of the selected sensor.
- Via Sensors | Simulate Error Status in the main menu bar where you get an [overview](#)<sup>195</sup> of all similar sensors.

To edit the list of similar sensors results, use the [available filters](#)<sup>196</sup>.

## Similar Sensors (Sensor Overview Tab)

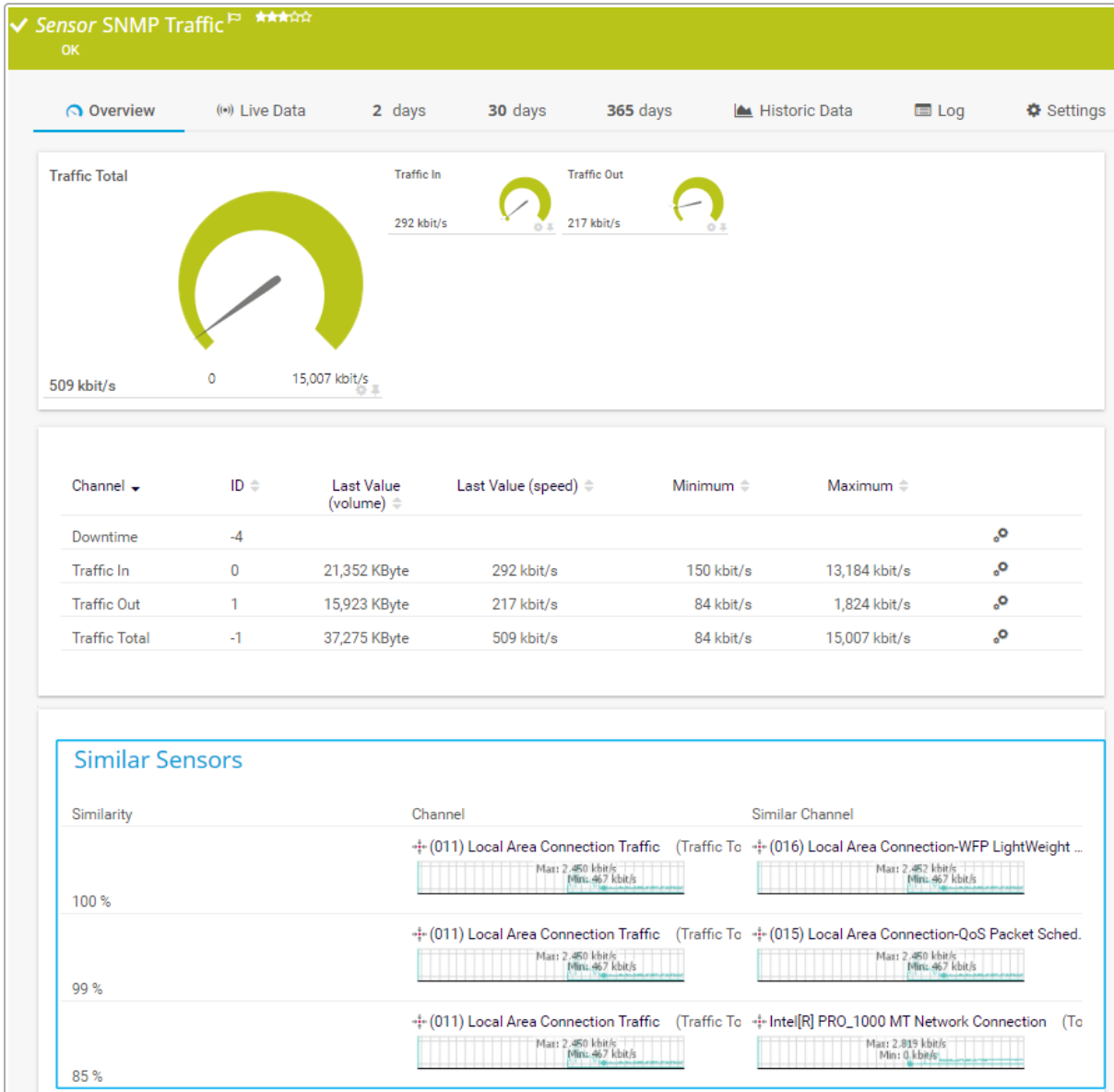
Probe, group, device, and sensor pages have tabs that you can use to navigate between different options. For example, you can view your network's status, view monitoring results, or change settings.



Tabs Bar for Sensors

On the Overview tab of a sensor, PRTG lists channels that show similarities to channels of the selected sensor. The table is empty if PRTG detects no similarities to the selected sensor.

- ⓘ PRTG shows similar sensors here when channels have 85% similarity or more. The similar sensors detection saves up to 15 entries per sensor.



Similar Sensors Section on a Sensor's Overview Tab

The Similar Sensors section provides the following information.

Column Header	Description
Similarity	Shows the similarity between two channels in percent.
Channel	Shows a channel of the selected sensor.
Similar Channel	Shows a channel of a sensor that is similar to the channel of the selected sensor that you can see in the Channel column in the same row.



**i** PRTG does not show the Similar Sensors section when the analysis is disabled or when you exceed 1,000 sensors and select the Manage automatically based on sensor count (default) option as Analysis Depth in the [Monitoring](#) settings. In this case, you see the following notice:

The similar sensors detection is a heuristic calculation that analyzes similar values in the sensor data of your entire PRTG installation. This way, PRTG can detect unexpected correlations between different components in your network and help optimize your sensor usage.

Why can't I see any sensor similarities here?

- The Similar Sensors Detection feature is currently turned off. To enable the detection and analysis of similar sensors, open **Setup | System Administration | Monitoring** and set your preferred analysis depth in the **Similar Sensors Detection** section.
- For more information about the similar sensors detection in PRTG, see the [PRTG Manual: Similar Sensors](#).

Similar Sensors Detection Notice

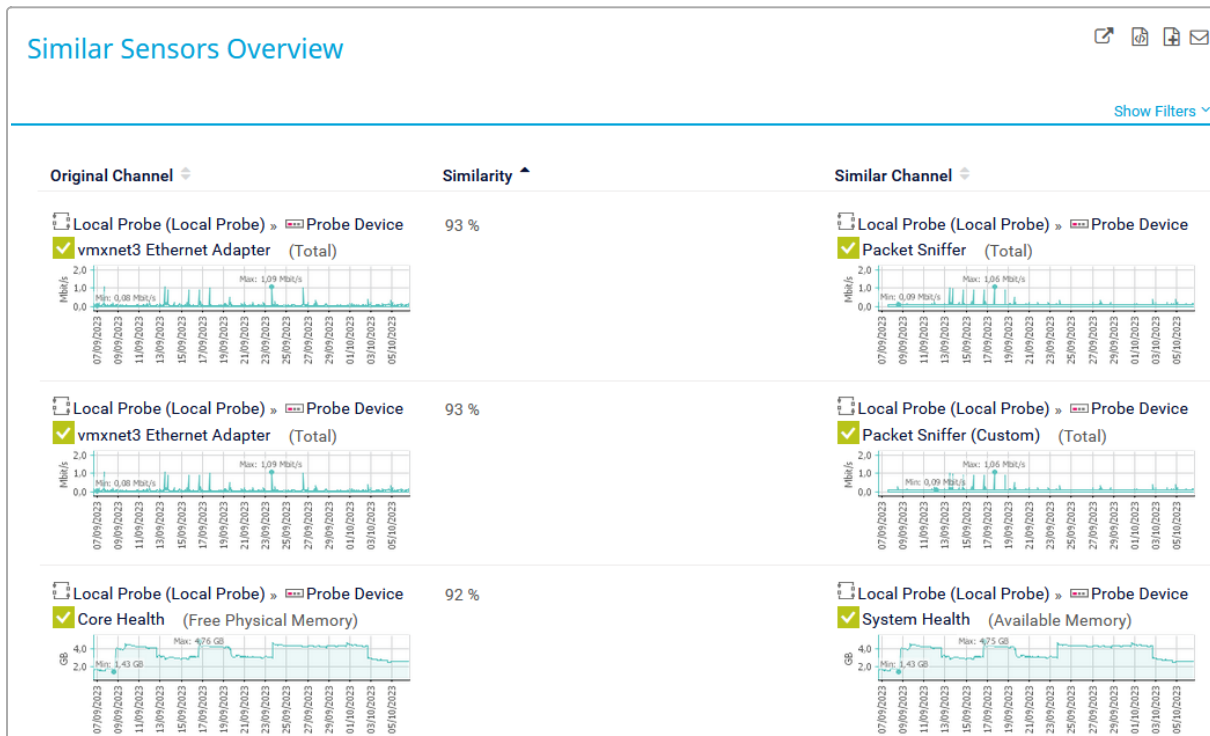
## Similar Sensors Overview (Sensors Menu)

This page shows the results of the similar sensors detection from the entire monitoring database. PRTG lists all channels with similarities here. Above the table, there are several filter options to display similar sensors as required. Select the object of interest, the degree of similarity, and display back references.

For more information, see section [Working with Table Lists](#).

**i** The analysis of similar sensors requires sensor data from at least seven days to have enough data for comparison. If not enough data is available, no data is shown on the Similar Sensors Overview or in the Similar Sensors section on a sensor's Overview tab.

**i** PRTG shows similar sensors here when channels have at least 85% similarity. Furthermore, the analysis saves up to 15 entries per sensor.



Similar Sensors Overview

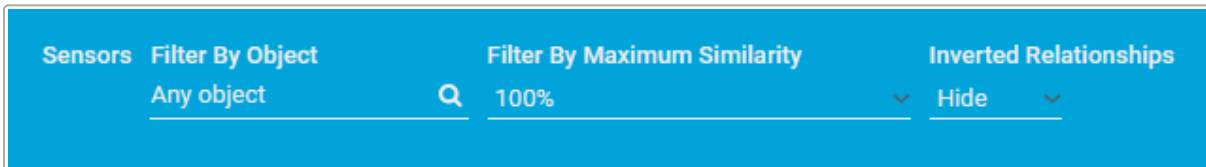
You can click the column headers to sort the list. The Similar Sensors Overview provides the following information.

Column Header	Description
Original Channel	Shows channels that other channels are compared to. Click the column header to sort the list according to the order in the device tree in ascending or descending order.
Similarity	Shows the similarity between two channels in percent. Click the column header to sort the list according to the similarities in ascending or descending order.
Similar Channel	Shows a channel that is similar compared to the original channel. Click the column header to sort the list according to the order in the device tree in ascending or descending order.

**i** PRTG does not show the Similar Sensors Overview item in the main menu bar if you disable the analysis or if you exceed 1,000 sensors and select the Manage automatically based on sensor count (default) option as Analysis Depth in the [Monitoring](#) settings.

### Adjust the Similar Sensors Overview to Your Needs

You can use various filters to adjust the results in the Similar Sensors Overview. Click Show Filters and edit the filters that appear.



Filters for the Similar Sensors Analysis

Filter	Description
Filter By Object	Select the device, probe, or group that you want the Similar Sensors Detection to cover. This way, you can apply the analysis to the parts of your network that you are interested in.
Filter By Maximum Similarity	Select a degree of similarity from 85% to 100%.
Inverted Relationships	If you select Show, PRTG shows all similarity relationships, that is, <b>A matches B</b> and <b>B matches A</b> .  If you select Hide, PRTG only shows <b>A matches B</b> relationships. This reduces the number of displayed similar sensors.

## 6.7 Recommended Sensors

With the [Recommended Sensors Detection](#) feature, PRTG can explore any device and check which sensors you have already created. If it finds useful sensors that you have not created yet, you see a list of recommended sensors for your device.

☁ You cannot use this feature on the hosted probe of a PRTG Hosted Monitor instance. You can use this feature on remote probes.

ⓘ The recommended sensors detection does not apply to the [user group setting](#) <sup>[2914]</sup> Allowed Sensors. Therefore, read/write users can also add all recommended sensors.

The screenshot shows the 'Device Internet' overview page. At the top, there are navigation tabs for 'Overview', '2 days', '30 days', '365 days', 'Alarms', 'System Information', 'Log', and 'Settings'. A message box states: 'To see sensor gauges here, please change the priority of one or more sensors to ★★★★★ / ★★★★★.' Below this is a table of existing sensors:

Pos	Sensor	Status	Message	Graph	Priority	
1.	HTTP	Up	OK	Loading time 110 μsec	★★★★☆	<input type="checkbox"/>

Below the table is a 'Recommended Sensors' section with the following data:

Priority	Sensors	Total Sensors	Links
★★★★★	1xPing	1	<a href="#">Add These Sensors</a>
★★★★☆	1xSSL Security Check (Port 4...)	2	<a href="#">Add These Sensors</a>

At the bottom left of the recommended sensors section is a 'Recommend Now' button.

Recommended Sensors on Device Overview Tab

### Get Sensor Recommendations

By default, PRTG recommends sensors for any device that you add and shows the suggested sensors for the device on its Overview tab, as long as your installation includes less than 5,000 sensors in total. To add the recommended sensors, click [Add These Sensors](#).

You can see the time that has passed since the last sensor recommendation in the [page header bar](#) <sup>[170]</sup> on the Overview tab of a device.

If you want to manually start the recommended sensors detection on any device, follow the steps below.

## Step 1: Select the Device

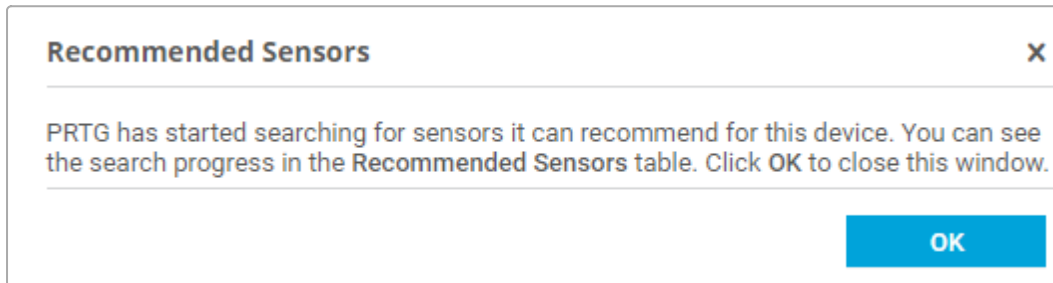
Open the Overview tab of the device that you want to analyze.

## Step 2: Recommend Now

To start the analysis of your device, click Recommend Now or right-click the device and select Recommend Now from the [context menu](#)<sup>[229]</sup>.

- ⓘ If you do not see the Recommend Now option, make sure that the Recommended Sensors Detection in the [Monitoring](#)<sup>[2874]</sup> settings. Probe devices do not support this option.

Depending on the complexity of your device, it can take some time until you see the results of the analysis.



Recommended Sensors Investigation

PRTG runs the recommended sensors detection with low priority in the background to prevent potential performance issues. Because of this, the recommended sensors detection can take more time than expected if PRTG needs resources to ensure the gapless monitoring of your network. By default, the recommended sensors detection starts automatically when you add a new device, when you do not have more than 5,000 sensors, or when the last analysis was executed more than 30 days ago. You can change these settings under Setup | System Administration | Monitoring, section Recommended Sensors Detection.

- ⓘ To recommend [Simple Network Management Protocol \(SNMP\) sensors](#)<sup>[3232]</sup> for a device, the detection engine uses the SNMP version that you defined in the Credentials for SNMP Devices section of the [device settings](#)<sup>[615]</sup>.

## Step 3: Get the Results

After PRTG analyzed your device, it suggests a list of sensors that are useful for a more comprehensive monitoring.

### Recommended Sensors

Priority	Sensors	Total Sensors	Links
★★★★★	1xPING	1	<a href="#">Add These Sensors</a>
★★★★☆	1xSSL Security Check (Port 443), 1xSSL Certificate Sensor (Port ...	2	<a href="#">Add These Sensors</a>

[Recommend Now](#)

**What is this?**  
PRTG can inspect your devices to recommend useful sensors.

List of Recommended Sensors

The list of recommended sensors provides the following information.

Column Header	Description
Priority	Shows which <a href="#">priority</a> <sup>[224]</sup> the suggested sensors have when you add them. The recommended sensors table is sorted by priority, beginning with the top priority (★★★★★) in the first row.  ⓘ You can manually change the priority of a sensor after you add it.
Sensors	Shows the suggested sensors and the number of sensors of one type that PRTG recommends for this device. For example, you might want to add an <a href="#">SNMP Traffic</a> sensor multiple times for several network interfaces.
Total Sensors	Shows the total number of suggested sensors per table row. These sensors have the same priority.
Links	Displays an Add These Sensors button for every table row. Click to automatically add the sensors in this table row to the device.

ⓘ The recommended sensors detection checks if a certain sensor exists on your device and recommends that you add this sensor if it does not exist. If this sensor existed previously on the device, but you deleted it, PRTG suggests this sensor again. In this case, ignore the recommendation of this sensor or follow [step 4](#)<sup>[199]</sup>.

## Step 4: Add Recommended Sensors

Click Add These Sensors in a table row to add all sensors in this row to the analyzed device.

ⓘ If you want to add **all** suggested sensors regardless of their priority, click every Add These Sensors button in the Recommended Sensors table. If you want to add only **some** of the sensors of a certain priority, click Add These Sensors, then [delete](#)<sup>[229]</sup> or [pause](#)<sup>[227]</sup> the sensors you do not need afterward.

## Settings for the Recommended Sensors Detection

You can also adjust the settings for the recommended sensors detection or disable it under Setup | System Administration | Monitoring.

**Recommended Sensors Detection**

Detection Handling ⓘ  Manage automatically based on sensor count (default)  
 Always show recommended sensors  
 Disable sensor recommendation

Recommended Sensors Detection Settings

If you use the Manage automatically based on sensor count (default) setting, PRTG uses an intelligent assistant to count the number of sensors you have and decides whether to start the detection of recommended sensors or not. The detection does not start if your PRTG installation includes 5,000 sensors or more to prevent performance issues. We recommend that you use this option so that you do not miss any important monitoring data about your network and so that you do not risk performance issues.

- ⓘ Disable the recommended sensors detection if you encounter performance issues or if you do not want to display this information on device Overview tabs.

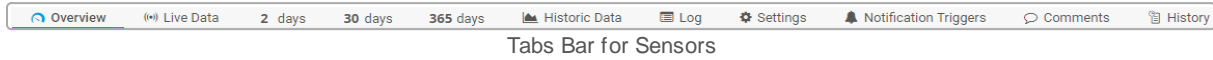
## Auto-discovery

You can also use the auto-discovery to find suitable sensors. You can start the auto-discovery when you [add a new device](#)<sup>[369]</sup>, you can [manually start](#)<sup>[255]</sup> it at any time, or you can choose if you want PRTG to [analyze a whole section](#)<sup>[602]</sup> of your network, for example, devices that are covered by a certain IP address range.

- ⓘ The auto-discovery has a higher priority than the detection of recommended sensors. If both are active, PRTG queues the sensor recommendation and executes the auto-discovery first.

## 6.8 Object Settings





Probe, group, device, and sensor pages have tabs that you can use to navigate between different options. For example, you can view your network's status, view monitoring results, or change settings.




Tabs Bar for Sensors

### General Settings

On the Settings tab, you can define all settings for the selected object. The available options vary depending on the kind of object that you select. See the following sections for information about the object types:

- [Root Group Settings](#) 
- [Probe Settings](#) 
- [Group Settings](#) 
- [Device Settings](#) 
- [Sensor Settings](#)

 You cannot open [channel settings](#)  via tabs. Go to a sensor's Overview tab to edit the channel settings.

### Notification Triggers Settings

On the Notification Triggers tab, you can set notification triggers for every object. If you use these settings for a probe, group, or device, they are inherited to all sensors on these objects. The available notification trigger options are the same for all objects.










 For more information, see section [Notification Triggers Settings](#) .

### Comments

On the Comments tab, you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

### History

On the History tab, all changes in the settings of an object are logged with a time stamp, the name of the user who made the change, and a message. The history log retains the last 100 entries.

 On some pages, you can click  in the [page header bar](#)  to access the history of subordinate objects. This includes [system administration](#)  settings and [account settings](#) , [reports](#) , [libraries](#) , and [maps](#) . For more information, see section [Logs](#) .

## 6.9 Alarms

You can see all sensors that are in the Down, Down (Partial), Down (Acknowledged), Warning, or the Unusual [status](#). Sensors in other states, for example, Up, Paused, or Unknown, do not appear here. This is useful for keeping track of all irregularities in your network.

**i** By default, [table lists](#)<sup>[218]</sup> that show alarms are sorted by [priority](#)<sup>[224]</sup>. Click a column header to sort the list items by a different category.

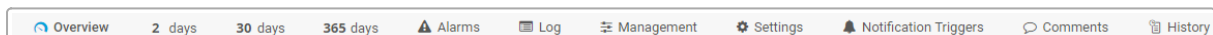
Sensor	Probe Group Device	Status	Down for	Last Value	Message	Graph	Priority	
!! Ping	Local Probe (Local Probe) » Linux / macOS / Unix » 192.0.2.0	Down	14 h 22 m		Request timed out (ICMP error...	Ping Time No data	★★★★★	<input type="checkbox"/>
!! Ping	Local Probe (Local Probe) » Linux / macOS / Unix » 192.0.2.1	Down	2 d 14 h 22 m		Request timed out (ICMP error...	Ping Time No data	★★★★★	<input type="checkbox"/>
!! Ping	Local Probe (Local Probe) » Linux / macOS / Unix » 192.0.2.2	Down	14 h 23 m		Request timed out (ICMP error...	Ping Time No data	★★★★★	<input type="checkbox"/>
!! Ping	Local Probe (Local Probe) » Linux / macOS / Unix » 192.0.2.3	Down	14 d		Request timed out (ICMP error...	Ping Time No data	★★★★★	<input type="checkbox"/>
!! Ping	Local Probe (Local Probe) » Linux / macOS / Unix » 192.0.2.4	Down	5 d 21 h 23 m		Request timed out (ICMP error...	Ping Time No data	★★★★★	<input type="checkbox"/>

Alarms List

There are two ways to display the alarms list. Either click the Alarms tab of a probe, group, or device, or click Alarms in the [main menu bar](#)<sup>[237]</sup>.

### Alarms (Object Tab)

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



Tabs Bar for Groups and Probes

Click the Alarms tab of a probe, group, or device to show a table list of all sensors on the selected object that show the Down, Down (Partial), Down (Acknowledged), Warning, or Unusual [status](#)<sup>[181]</sup>. This list is a subset of the entries that are available via the Alarms | All option in the main menu bar.

**i** The Alarms tab is not available for sensors.

### Alarms (Main Menu Bar)

Click Alarms in the main menu bar to show a table list of all sensors in your installation that show the Down, Down (Partial), Down (Acknowledged), Warning, or Unusual status. You can also show these sensors as gauges or only show a subset of sensors in specific states. Hover over Alarms to show further options:



Option	Description
All	Open a list of all sensors that are in the Down, Down (Partial), Down (Acknowledged), Warning, or Unusual status.
Show as Gauges	Open a page with the gauges of all sensors that are in the Down, Down (Partial), Down (Acknowledged), Warning, or Unusual status. The size of the gauges corresponds to the sensor's priority.
Errors Only	Open a list of all sensors that are in the Down, Down (Partial), or Down (Acknowledged) status.
Warnings Only	Open a list of all sensors that are in the Warning status.
Unusuals Only	Open a list of all sensors that are in the Unusual status.

## Acknowledge Alarm

An acknowledged alarm shows the Down (Acknowledged) status. It does not [trigger](#)<sup>[2693]</sup> any more [notifications](#)<sup>[2735]</sup>.

- i** If the alarm condition clears, the sensor usually returns to the Up status with the next sensor scan.
- i** If a sensor in the Down (Acknowledged) status was paused and resumed, it shows the Down status again.

To acknowledge an alarm, right-click a sensor that shows the Down status. From the [context menu](#)<sup>[229]</sup>, select Acknowledge Alarm, then select a time span, optionally enter a message, and click OK. The message appears in the last message value of the sensor.

The time spans that you can select are: Acknowledge Indefinitely, acknowledge For 5 Minutes, For 15 Minutes, For 1 Hour, For 3 Hours, For 1 Day, or Until. If you select Until, provide the following information:

Field	Description
Selected Objects	Shows the sensors for which you want to acknowledge the alarm. You can acknowledge alarms for more than one sensor using <a href="#">multi-edit</a> <sup>[2718]</sup> .
Message	Enter a text, for example, the reason why you acknowledge the alarm. Enter a string or leave the field empty.
Until	Select the date when the Down (Acknowledged) status ends. Use the date time picker to enter the date and time.

Field	Description
	<p>ⓘ If the alarm condition still exists after the specified date, the sensor shows the Down status again.</p> <p>ⓘ To return the sensor to the Down status before the specified date, you can Pause and then Resume the sensor via the <a href="#">context menu</a>.</p>

ⓘ By default, only read/write [users](#) or administrators can acknowledge alarms. However, you can give read-only users the right to acknowledge alarms, too. See the system administration settings, section [User Accounts](#).

## More

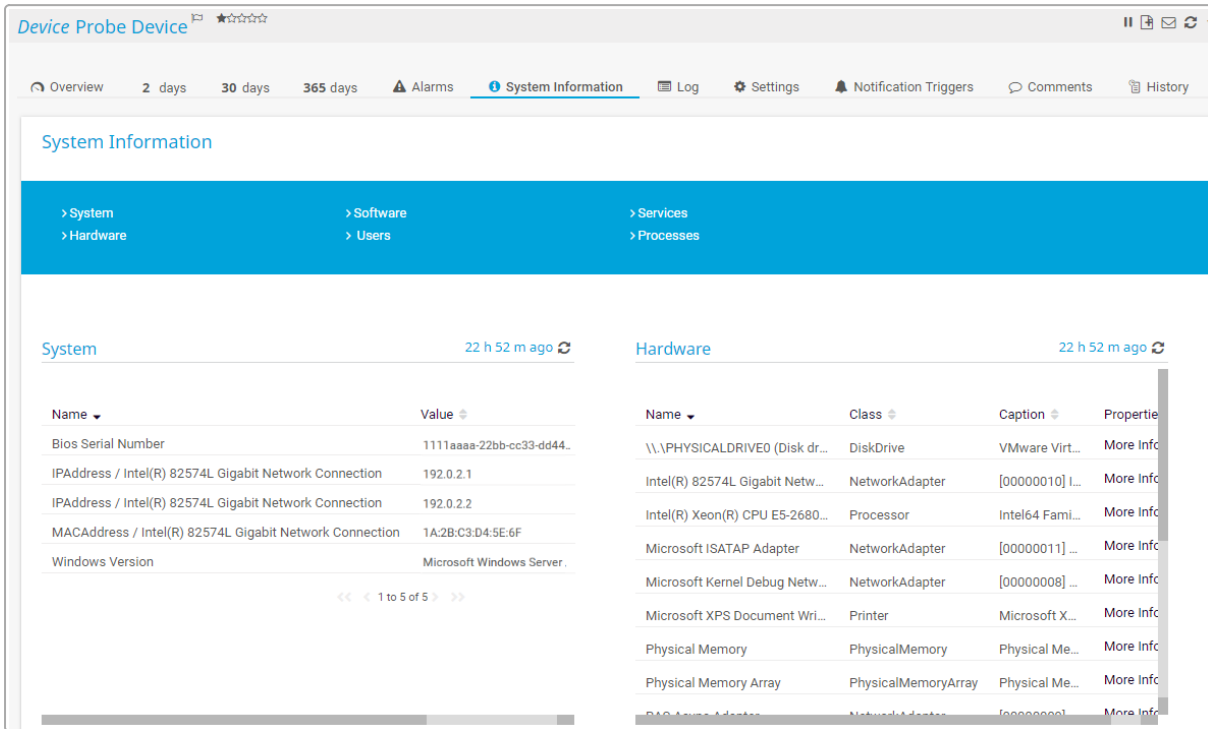
### ■ KNOWLEDGE BASE

Which audible notifications are available in the PRTG web interface and in the PRTG app for desktop?

- <https://kb.paessler.com/en/topic/26303>

## 6.10 System Information

With the [System Information](#) feature, you can see what is going on in the systems that you have in your network. To see the system information for a device, click the device's System Information tab.



System Information Tab on a Windows Device

The system information shows

- basic system data of your device like the BIOS serial number or MAC and IP addresses,
- all connected hardware types and their properties,
- the software you have installed, including version and vendor information,
- the users that are connected to your system and their domains,
- a list of all active or stopped Windows system services including their properties, and
- a list of all processes that are running on your system, including their ID and start time.

System information is available for all devices that run with an [officially supported Windows operating system](#). You can also retrieve system information from devices that run with Linux or Unix, and from all other devices that have the Simple Network Management Protocol (SNMP) enabled.

☁ You cannot use this feature on the hosted probe of a PRTG Hosted Monitor instance. You can use this feature on remote probes.

### Prerequisites

You already meet the main prerequisites for retrieving system information if you already monitor a device with sensors that use Windows Management Instrumentation (WMI) or the Simple Network Management Protocol (SNMP). PRTG automatically displays the data on the respective device's System Information tab. To retrieve all available system information, enable both WMI and SNMP on the device.

**i** The System Information feature is enabled by default. To retrieve the data, PRTG automatically uses the [credentials for Windows systems](#)<sup>[606]</sup> and the [credentials for SNMP devices](#)<sup>[615]</sup> that you entered in the device settings or that the device [inherits](#)<sup>[132]</sup> from a parent object like the root group. Consider this when you monitor devices that are outside of your local network, especially when you use [SNMP v1](#) or [SNMP v2c](#), which do not provide encryption.

Meet the following prerequisites if you do not yet use WMI or SNMP sensors:

Option	Description
Valid credentials	Specify valid credentials for Windows systems and for SNMP devices in the <a href="#">device settings</a> <sup>[597]</sup> .
Remote Registry Windows service	Enable the Remote Registry service on the target computer, for example, via <a href="#">services.msc</a> , and set the Startup Type to Automatic.
Remote Procedure Call (RPC) Windows service	Enable the RPC Windows service on the target computer, for example, via <a href="#">services.msc</a> , and set the Startup Type to Automatic.
WMI	<p>Enable WMI on both the probe system and the target system. In particular, configure the firewall of the target system to allow WMI.</p> <p>■ For more information, see section <a href="#">Monitoring via WMI</a><sup>[3004]</sup> and the Knowledge Base: <a href="#">My WMI sensors don't work. What can I do?</a></p>
SNMP	<p>Enable SNMP on the target system. PRTG automatically uses the SNMP Compatibility Options as defined in the <a href="#">device settings</a><sup>[597]</sup> or as inherited from a parent object like the root group.</p> <p>■ For more information, see section <a href="#">Monitoring via SNMP</a><sup>[2997]</sup> and the Knowledge Base: <a href="#">My SNMP sensors don't work. What can I do?</a></p>

**i** It is not necessary to meet every single prerequisite but then some tables do not show all data or they can even remain empty. For example, if you do not enable SNMP on the target device, you get less information for the System table.

The first data usually comes in after a few minutes. If PRTG cannot retrieve some data, for example, because of a misconfiguration, the respective System Information table shows an error message.

■ For more information, see the Knowledge Base: [How can PRTG get data for System Information tables?](#)

**i** System information for your devices is only for informational purposes. We cannot guarantee that the data displayed in PRTG fully corresponds to the device parameters.

Software
31 S Ago

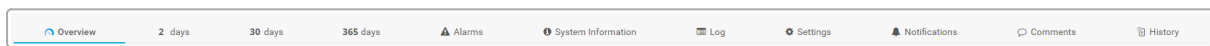
No Data Available

- *Error: The sensor could not connect to the Remote Registry Windows service of the target system. To resolve this issue, make sure that the service is running. Also make sure that you entered correct Credentials for Windows Systems in the device settings. For more information, see <https://kb.paessler.com/en/topic/67824>. (code: PE255)*
- *Error: SNMP No Response*

Error Messages: No Data Available

### System Information (Device Tab)

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



Tabs Bar for Devices

Select a device and click the System Information tab.

**i** The System Information feature is enabled by default. If you do not see the System Information tab, you need to enable System Information in the device settings under Advanced Network Analysis. You can also inherit the setting from an object that is higher in the [object hierarchy](#) <sup>[132]</sup>.

### Advanced Network Analysis

<b>Unusual Detection</b> <small>i</small>	<input checked="" type="radio"/> Enable (default)
	<input type="radio"/> Disable
<b>Similar Sensors Detection</b> <small>i</small>	<input checked="" type="radio"/> Enable (default)
	<input type="radio"/> Disable
<b>System Information</b> <small>i</small>	<input checked="" type="radio"/> Enable (default)
	<input type="radio"/> Disable


Advanced Network Analysis

### Analyze Your Systems

On the System Information tab, PRTG displays a table for each system information category for the device.

Category	System Information	Request Method (WMI or SNMP)
System	Shows system data of the device like the BIOS serial number, IP addresses, MAC addresses, and the Windows version.	WMI and SNMP
Hardware	Shows hardware that is connected to the device like disk drives, CD/DVD, video controllers, processors, network adapters, sound devices, printers, and memory. You can see the Class and the Caption of a hardware device. In the Properties column, you get more information about the hardware, for example, the description.	WMI and SNMP
Software	Shows the installed software and the Version number of the device. In the Properties column, you get more information about the software, for example, the size.  ⓘ PRTG uses <a href="#">Uninstall</a> registry keys to retrieve the list of installed software, so the displayed software might differ from the software that the target Windows system shows under Programs and Features.  ⓘ The System Information scan for software on the probe device uses the credentials of the probe system and ignores credentials that you specified on the Settings tab.	WMI and SNMP
Users	Shows the user accounts that are connected to the device and their Domain.	WMI
Services	Shows the available Windows services on the device. You can see the State of the service (running, stopped) and the start type (Startup Type automatic, manual, or disabled). In the Properties column, you can get more information about a service, for example, the description.	WMI
Processes	Shows the processes that are running on the device as listed on the <a href="#">Processes</a> tab of the Windows Task Manager. You can also see the Start Time (only WMI) and Process ID of a process.	WMI and SNMP

You can sort each [table list](#)<sup>[218]</sup> via the column headers.

Click  in the upper-right corner of a table to retrieve new information for this System Information category. The time stamp shows the time that has passed since the last table refresh.

31 S Ago   
Table Refresh

PRTG automatically retrieves data for the tables System, Hardware, and Software once every 24 hours. The tables Users, Services, and Processes refresh each time you open the System Information tab. PRTG also updates all system information tables when the PRTG core server is restarted, for example, after an update.

- ⓘ PRTG can perform up to 24 system information scans at the same time, so it can take some time until you see data in the tables after a server restart.

## Data Storage

PRTG stores data files with the retrieved system information in the corresponding \System Information Database subfolders of the [PRTG data directory](#)<sup>[3214]</sup>.

- ⓘ If you delete a device, the system information files of this device remain in these subfolders unless you manually delete them.

PRTG uses the following subfolders for System Information data.

Subfolder	Description
hardware	Data for the Hardware table
loggedonusers	Data for the Users table
processes	Data for the Processes table
services	Data for the Services table
software	Data for the Software table
system	Data for the System table

## More

### ■ KNOWLEDGE BASE

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

How can PRTG get data for System Information tables?

- <https://kb.paessler.com/en/topic/67824>

My HTTP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/85284>

## 6.11 Logs

Logs show all past activities and events in your monitoring setup. With the logs, you can, for example, review past user activities, system events, or check whether messages were sent. In a typical setup, a huge amount of log data is produced. Because PRTG records the activity of every single object, you can use this information to check if your setup works as required.

You can choose from several filters to navigate the log entries.

For more information, see section [Working with Table Lists](#) <sup>218</sup>.

**Log Entries** Items: 50  
Show Filters

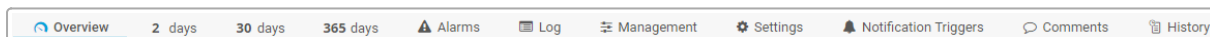
Date Time	Parent	Type	Object	Status	Message
05/10/2023 14:08:58	Probe Device	Local Folder (BETA)	Local Folder	Up	0 #
05/10/2023 14:08:53	Probe Device	FortiGate VPN Overview (...)	FortiGate VPN Overview	Down	The sensor could not authenticate again
05/10/2023 14:07:21	Example Device 1	SNMP Traffic 32bit	(019) Ethernet0-WFP 802.3 MAC Layer ...	Up	0,04 Mbit/s
05/10/2023 14:07:19	192.0.2.0	SNMP Traffic 32bit	(019) Ethernet0-WFP 802.3 MAC Layer ...	Up	0,34 Mbit/s
05/10/2023 14:07:18	Probe Device	System Health	System Health	Up	100 %
05/10/2023 14:07:16	Example Device 2	SNMP Traffic 32bit	(018) Ethernet0-QoS Packet Scheduler...	Up	0,34 Mbit/s
05/10/2023 14:07:15	Example Device 3	SNMP Traffic 32bit	(018) Ethernet0-QoS Packet Scheduler...	Up	0,04 Mbit/s
05/10/2023 14:07:13	Probe Device	Windows Network Card	vmxnet3 Ethernet Adapter	Up	0,08 Mbit/s
05/10/2023 14:07:03	192.0.2.0	SSL Certificate	SSL Certificate Sensor (Port 443)	Down	-92 # (Days to Expiration) is below the t...
05/10/2023 14:07:00	Example Device 1	SNMP Traffic 32bit	(016) Ethernet0-WFP Native MAC Layer...	Up	0,04 Mbit/s

List with Log Entries

There are two ways to open the logs list. Either click the Log tab of a probe, group, device, or sensor, or click Logs in the [main menu bar](#) <sup>246</sup>.

### Log (Object Tab)

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



Tabs Bar for Groups and Probes



Click the Log tab to show a table list with all log information for the selected object. This is a more detailed log than the system log that is available via the Logs | All option in the main menu bar.

### Logs (Main Menu Bar)

Click Logs in the main menu bar to show a table list of all system log entries in your installation. Hover over Logs for further options:



Option	Description
All	Open a list with log information about all objects in your installation. The list begins with the most recent log entry.
Status Changes	<p>Open a list with log information about specific status changes. Hover over Status Changes to choose from the following sensor states:</p> <ul style="list-style-type: none"> <li>▪ Up &amp; Down</li> <li>▪ Down</li> <li>▪ Warning</li> <li>▪ Unusual</li> <li>▪ Up</li> <li>▪ Paused/Resumed</li> <li>▪ Acknowledged Alarms</li> </ul>
System Events	<p>Open a list with log information about specific system event types. Hover over System Events to choose from the following event types:</p> <ul style="list-style-type: none"> <li>▪ Report Related</li> <li>▪ Cluster Related  <span style="color: #00AEEF;"> ⓘ This event type only appears if you have a cluster.</span></li> <li>▪ Auto-Discovery Related</li> <li>▪ Notifications Related</li> <li>▪ Status Message Related</li> </ul>
Object History	<p>Open a list with log information about changes to the PRTG setup and deletions of subordinate system objects. The Object History has several tabs. To view the changes to all related settings and deletions of objects, use the following tabs:</p> <ul style="list-style-type: none"> <li>▪ My Account</li> <li>▪ System Administration</li> <li>▪ Notification Templates</li> <li>▪ Schedules</li> <li>▪ User Accounts</li> <li>▪ User Groups</li> <li>▪ Reports</li> <li>▪ Libraries</li> <li>▪ Maps</li> </ul>

Option	Description
	<p> You can also navigate to a corresponding page, for example, you can select Setup   Account Settings   My Account from the main menu bar, and click  in the <a href="#">page header bar</a><sup>[170]</sup> to directly go to the related object history tab.</p>

## More

### KNOWLEDGE BASE

The logs page in the PRTG web interface does not load. What can I do?

- <https://kb.paessler.com/en/topic/77329>

## 6.12 Tickets

PRTG has its own ticket system. A ticket includes information about recent events in your PRTG installation that need a closer look. Each ticket is a task for a particular user or user group.

Tickets							
							Items: <span>▼</span> 50
							Show Filters <span>▼</span>
Last modified <span>▼</span>	Priority <span>↕</span>	Ticket ID <span>↕</span>	Subject	Assigned to <span>↕</span>	Status <span>↕</span>	Object <span>↕</span>	<input type="checkbox"/>
14/08/2023 15:16:57	★★★★☆	#5	🔔 Automatic update successful	PRTG Administrators	○	System	<input type="checkbox"/>
14/08/2023 15:11:31	★★★☆☆	#4	🔔 Software update is available	PRTG Administrators	○	System	<input type="checkbox"/>
31/07/2023 16:29:40	★★★★☆	#3	🔔 We recommend at least Win...	PRTG Administrators	○	System	<input type="checkbox"/>
27/07/2023 16:36:09	★★★☆☆	#2	🔔 Auto-Discovery finished for '1...	PRTG Administrators	○	Local Probe	<input type="checkbox"/>
27/07/2023 16:26:36	★★★★☆	#1	🔔 Welcome to PRTG!	PRTG Administrators	○	Root	<input type="checkbox"/>

List of Tickets

Each task has a life cycle in the ticket system. The task's life cycle starts when a ticket is created. The users who are responsible then take care of this issue. Once the issue has been resolved, the ticket can be closed and the life cycle of the task ends. PRTG automatically creates tickets, for example, when the [auto-discovery](#) [254] has finished, and you can create tickets for every kind of issue as well. In addition, you can set up [notifications](#) [2735] that open a ticket when an issue occurs.

Every ticket has a unique ID, a priority, and a status. You can open, resolve, or close a ticket.

PRTG can also [send an email](#) [217] to you whenever a ticket is assigned to you or if one of your tickets has been changed.

❗ Except for administrator groups, you can disable the ticket system for particular user groups under Setup | System Administration | User Groups. You can also [disable ticket emails](#) [217] for every user account.

### Ticket Types




There are three types of tickets:

Type	Description
User Tickets	User tickets are created by users, for example, to assign monitoring-related tasks to a particular <a href="#">user account</a> [2901] or <a href="#">user group</a> [2912].
ToDo Tickets	<p>ToDo tickets are created by PRTG to show important system information and to inform you about specific system events. ToDo tickets are assigned to the predefined <a href="#">PRTG Administrators</a> group. You cannot change the user group to which PRTG assigns ToDo tickets and you cannot disable ToDo tickets.</p> <p>❗ Users that belong to an administrator group do not receive new ToDo tickets and notifications about changes by default, only the predefined <a href="#">PRTG System Administrator</a> user does. You cannot change this behavior.</p>

Type	Description
	<p>See the following examples for cases in which PRTG creates a ToDo ticket:</p> <ul style="list-style-type: none"> <li>▪ The auto-discovery created new devices or sensors. <ul style="list-style-type: none"> <li>ⓘ In the ticket, PRTG only lists the device templates that it used to create the sensors.</li> </ul> </li> <li>▪ A new probe has connected to the PRTG core server and you must acknowledge it.</li> <li>▪ A new cluster node has connected to the cluster and you must acknowledge it.</li> <li>▪ A new version of the software is available.</li> <li>▪ A new report is ready for review.</li> <li>▪ In a few other situations, for example, the system is running out of disk space, there are license issues, or an error occurs.</li> </ul> <p>ⓘ The related object of ToDo tickets is System.</p>
Notification Tickets	Notification tickets are created via notifications that you set in the <a href="#">notification template settings</a> <sup>[2808]</sup> .

## Ticket States

Tickets can have three different states:

Sym bol	State	Description
	Open	New tickets are open as long as the issue that is described in the ticket exists.
	Resolved	The issue that is described in the ticket does not persist any longer because a user resolved it.
	Closed	A user resolved the ticket, the solution to the issue was reviewed for correctness, and the ticket does not require any other action.


## Tickets (Main Menu)

ⓘ This option is only available in the main menu bar if the user group to which the logged in user belongs is allowed to use the ticket system. You can disable a user group's access to the ticket system in the user group settings under Setup | System Administration | User Groups. **Read-only** users never have access to the ticket system and cannot see the Tickets option in the main menu bar.

You have several options to display a list of tickets that is filtered to your needs. In the main menu bar, click Tickets to show all open tickets that are assigned to you. Hover over Tickets to show other available filter options:

Option	Description
My Tickets	Click to show all open tickets that are assigned to you. Hover over My Tickets to show other options to filter these tickets according to their status: Open, Resolved, Closed, or All.
All Tickets	Click to show all open tickets of all users. Hover over All Tickets to show other options to filter these tickets according to their status: Open, Resolved, Closed, or All.
ToDo Tickets	<p>Click to show all open tickets of the ToDo <a href="#">type</a><sup>[213]</sup>. Hover over ToDo Tickets to show other options to filter these tickets according to their status: Open, Resolved, Closed, or All.</p> <p>Click Open to show all open ToDo tickets. Hover over Open to show other options to filter these tickets according to their event type: All, Report Related, Auto-Discovery Related, Probe Related, Cluster Related, System Errors, or New Software Version.</p>

## Add a User Ticket

From the main menu bar, select Tickets | Add Ticket, or hover over  and click Add Ticket. This opens the Add Ticket dialog.

Step 1: Select the object to which the new ticket is related via the [object selector](#)<sup>[222]</sup>. Click OK.

**i** You can skip step 1 if you use an object's [context menu](#)<sup>[229]</sup> in the device tree to open the ticket.

Step 2: Provide the following information and click OK to create a user ticket:

- Subject: Enter a subject for the ticket that indicates the topic of the issue.
- Assigned to: From the dropdown list, select a user or a user group that is responsible for this issue.
- Priority: Define a [priority](#)<sup>[224]</sup> from the lowest priority (☆☆☆☆) to the top priority (★★★★★).
- Comments: Enter a message. This message should describe the issue in detail.

After you open a new user ticket, a corresponding list of tickets appears. In this [table list](#)<sup>[218]</sup>, you can sort the items by clicking the column headers. Additionally, several search options are available in the filter directly above the table:

Option	Description
Status	all, open, resolved, closed

Option	Description
Type	Tickets, User Tickets, ToDo Tickets, Notification Tickets
Assigned To	<p>Show only tickets that are assigned to a specific user or user group:</p> <ul style="list-style-type: none"> <li>▪ anyone: Apply no user filter and show all tickets.</li> <li>▪ me: Show tickets that are assigned to you (the user who is logged in).</li> <li>▪ Groups: Show tickets that are assigned to a specific user group. The displayed user groups are specific to your setup.</li> <li>▪ Users: Show tickets that are assigned to a specific user. The displayed users are specific to your setup.</li> <li>▪ Disallowed: Display users or user groups that do not have access rights to the selected object. This is for your information only. You cannot select disallowed users or user groups.</li> </ul>
Related To	<p>Specify the relationship to a monitoring object. Select groups, probes, devices, or sensors with the object selector.</p> <p><b>i</b> ToDo tickets are related to System.</p>
Changed Between	Define a time span to view tickets that changed during this time. Use the date time picker to enter the date and time.

Click the subject of a ticket to open the ticket.

ToDo Ticket #4 ★★☆☆☆ ✉

[Software update is available](#)

---

Status: open Assigned to: **PRTG Administrators** Related Object: System Type: ToDo (New Software Version) ID: #4 
[Edit](#) [Assign](#) [Resolve](#) [Close](#)

---

[Last Update](#)

Opened by **PRTG System Administrator** + Assigned to **PRTG Administrators** 14/08/2023 15:11:31

---

[14/08/2023 15:11:31] The new PRTG version 23.3.88.1122 has been downloaded and will be installed right now. We will stop and restart the PRTG services.

An Open ToDo Ticket with Instructions

## Actions

The following actions are available for a specific ticket:

Action	Description
Edit (✎)	Open a dialog where you can change the subject and the priority of the ticket, as well as assign the ticket to a different user. You can optionally add a message to this ticket. Click OK to apply your changes.
Assign (👤)	Open a dialog where you can give the ticket to a different user or user group. Select a user or a user group via the dropdown list. You can optionally add a message to this ticket. Click OK to apply your changes.
Resolve (✔)	Open a dialog where you can resolve the ticket. The status <b>resolved</b> indicates that the issue that is described in this ticket does not persist anymore. You can optionally add a message to this ticket that indicates, for example, what was done to resolve the issue. Click OK to apply your changes.
Close (🔒)	Open a dialog where you can close the ticket after the issue was resolved and reviewed. You can optionally add a message to this ticket. Click OK to apply your changes.
Reopen (🔄)	Open a dialog where you can reopen a ticket after it was resolved or closed. Do so, for example, if the solution to the issue was not correct. You can optionally add a message to this ticket that indicates, for example, why you have opened the ticket again. Click OK to apply your changes.

ⓘ Only user group members that have the respective [access rights](#)<sup>[145]</sup> can view and edit tickets that are related to a certain monitoring object.

## Tickets as Emails

You can receive all tickets that are assigned to you or to your user group as emails. PRTG also notifies you via email each time a ticket that is assigned to you or to your user group is edited. This way, you are always informed about new notifications (if you enabled this setting), important system information (if you are an administrator), or the communication between other users.

You can disable the setting Email Notifications in the user account settings under Setup | System Administration | User Accounts. If you select Do not receive any emails from the ticket system for a specific user account, this particular user does not receive ticket emails anymore.

ⓘ If you defined to receive tickets as emails and you are the predefined [PRTG System Administrator](#) user, you receive emails for ToDo tickets as well, although ToDo tickets are usually opened by the [PRTG System Administrator](#) user.

## 6.13 Working with Table Lists

In the PRTG web interface, you often see table lists, for example, sensor or device lists. Table lists are also available in [libraries](#) [2738], [maps](#) [2776], [reports](#) [2754], [notifications](#) [2735], and [schedules](#) [2846], as well as in [logs](#) [210] and [tickets](#) [213]. All of these table lists are similar in layout and functionality.

Sensor	Probe Group Device	Status	Last Value	Message	Graph	Priority	Fav.	Perf. Impact	
✓ Ping	Local Probe (Local Probe) » Linux / macOS / Unix » 192.0.2.0	Up	0 msec	OK	Ping Time 0 msec	★★★★★	🔖	📊	<input type="checkbox"/>
✓ Ping	Local Probe (Local Probe) » Linux / macOS / Unix » 192.0.2.1	Up	1 msec	OK	Ping Time 1 msec	★★★★★	🔖	📊	<input type="checkbox"/>
✓ Ping	Local Probe (Local Probe) » Linux / macOS / Unix » 192.0.2.2	Up	0 msec	OK	Ping Time 0 msec	★★★★★	🔖	📊	<input type="checkbox"/>
✓ Ping	Local Probe (Local Probe) » Sensors » 192.0.2.3	Up	0 msec	OK	Ping Time 0 msec	★★★★★	🔖	📊	<input type="checkbox"/>
✓ Ping	Local Probe (Local Probe) » Linux / macOS / Unix » 192.0.2.4	Up	0 msec	OK	Ping Time 0 msec	★★★★★	🔖	📊	<input type="checkbox"/>


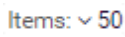


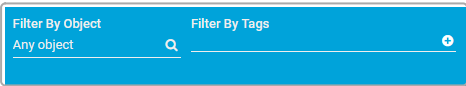
Example of a Table List

### Table List Options

See the following table for ways to work with table lists:

Feature	Display	Description
Paging		The content of a table list is displayed on several pages. Click the respective paging button at the end of a list to view other pages or to go to the beginning or the end of the list.
New Window		Click the respective button to open the table list in a new window.
Date Range		Use the date and time picker to show table list entries within a specific time period. Click the first field to select a start date and the second field to select an end date. Click Done to apply the selected date and time.



Feature	Display	Description
Select Range		<p>When you view <a href="#">log</a> lists, click <b>Select Range</b> in the upper-left corner of the table list to select the time period for which you want to show log entries. Choose from Today, Yesterday, and several other time periods. Select Unlimited to disable this filter again.</p> <p><b>■</b> For more information, see section <a href="#">Date Ranges</a> <sup>[220]</sup>.</p>
Items		<p>Click <b>Items</b> in the upper-right corner of a table list to select how many rows are shown on each page. You can choose between 50, 100, 500, and 1000.</p>
Sorting		<p>Click a column header to sort the list items by the respective category. You can click all column headers that include arrow icons to sort the list, for example, by Status, Last Value, Priority, and more. The sorting options vary depending on the content of the table list.</p>
Show XML		<p>Click the respective button to download the selected page in XML format. Your browser usually shows a download dialog.</p>
Filtering		<p>You can filter table lists via the <b>Show Filters</b> option directly above a list. The filter options vary depending on the content of the table list.</p> <p>Use the filter options, for example, to show specific objects in the list. Click <b>Any object</b> in the <b>Filter By Object</b> section to select an object from the device tree with the <a href="#">object selector</a> <sup>[221]</sup>.</p>

Feature	Display	Description
		<p>Enter one or more <a href="#">tags</a> <sup>138</sup> into the field Filter By Tags to filter the list for corresponding objects. You can use the plus sign (+) and the minus sign (-) to categorize tags as <a href="#">must have this tag</a> or <a href="#">does not need this tag</a>.</p> <p><b>i</b> For performance reasons, it can take some minutes until you can filter for new tags that you added.</p>

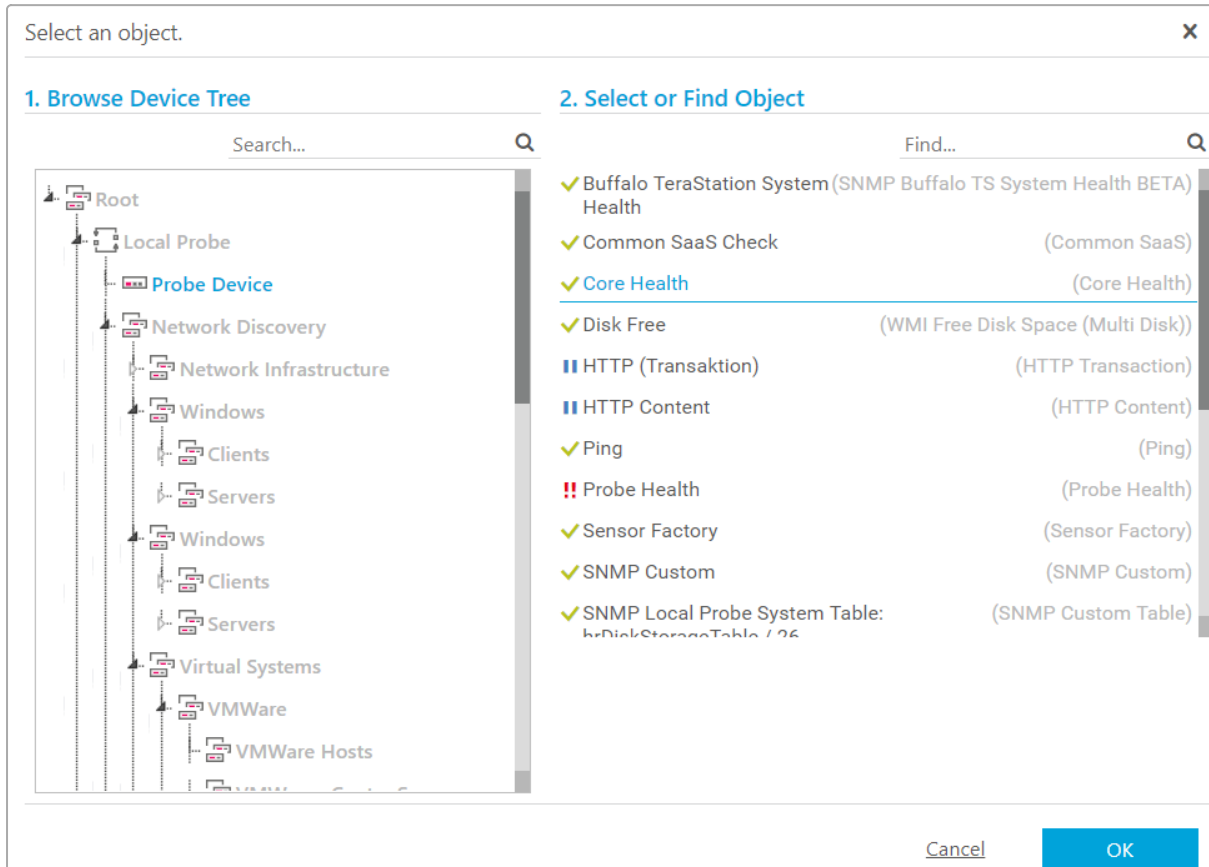
### Date Ranges

Range	Description	Example (Based on 14.01.2023)
Today	Start: 00:00 of today End: 00:00 of tomorrow	2023-01-14 (00:00) - 2023-01-15 (00:00)
Yesterday	Start: 00:00 of yesterday End: 00:00 of today	2023-01-13 (00:00) - 2023-01-14 (00:00)
7 days	Start: 00:00 of 7 days ago End: 00:00 of tomorrow	2023-01-07 (00:00) - 2023-01-15 (00:00)
30 days	Start: 00:00 of the same day last month End: 00:00 of tomorrow	2022-12-14 (00:00) - 2023-01-15 (00:00)
6 months	Start: 00:00 of the same day 6 months ago End: 00:00 of tomorrow	2022-07-14 (00:00) - 2023-01-15 (00:00)
12 months	Start: 00:00 of the same day 12 months ago End: 00:00 of tomorrow	2022-01-14 (00:00) - 2023-01-15 (00:00)

Range	Description	Example (Based on 14.01.2023)
Unlimited	Start: 00:00 of the same day 7 years ago ( <a href="#">historic data</a> <sup>1851</sup> for logs is limited to 750 days)  End: 00:00 of tomorrow	2016-01-14 (00:00) - 2023-01-15 (00:00)



## 6.14 Object Selector

For some features, you need to select an object, for example, when you want to create historic data reports. In this case, PRTG uses the object selector with which you can browse all objects in your installation to select an object in two steps.



Object Selector

### Step 1: Browse Device Tree

On the left-hand side, you see your specific device tree setup with all probes, groups, and devices. Click  to collapse an object. Click  to expand the object again and show its subobjects.

Click a device to view its sensors on the right-hand side.

You can also directly search for an object in the device tree. To do so, enter a probe name, group name, or device name into the Search box on the left-hand side. You can also use a substring for the search.

### Step 2: Select or Find Object

Select a device on the left-hand side to see the sensors on this device on the right-hand side. PRTG displays the name of the sensor as well as the sensor type. Hover over a sensor to view its parent objects.

You can also directly search for a sensor in the sensor list. To do so, enter the sensor name, group name, device name, or tag into the Find box on the right-hand side.

Select a sensor and click OK.

## 6.15 Priority and Favorites

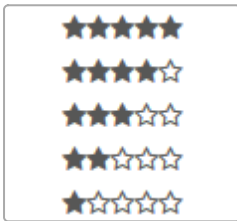
You can set priorities for all your monitoring objects and also mark devices or sensors as favorites. Both settings affect how PRTG displays your objects.

- ① PRTG stores priority and favorites settings for the entire installation. The settings are not user specific.

### Priority for All Objects

The priority setting affects the order by which PRTG lists your objects in [table lists](#)<sup>[218]</sup>. PRTG lists objects with a higher priority first. Furthermore, a device displays gauges for sensors with a high priority on its Overview tab.

To change the priority settings, right-click an object to open its [context menu](#)<sup>[229]</sup> and select Priority/Favorite. You can choose from the top priority with 5 stars (★★★★★) to the lowest priority with one star (★☆☆☆☆). By default, PRTG sets all objects to the medium priority with 3 stars (★★★☆☆). In the [page header bar](#)<sup>[170]</sup> and in table lists, you can directly set a priority via the star icons.



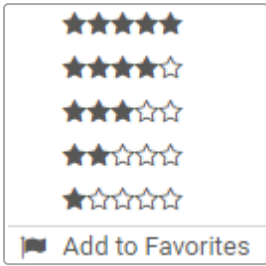
Context Menu: Priority

- ① For a sensor, select a priority of 4 or 5 stars to display its the gauge of its primary channel on the Overview tab of its parent device.
- ① For a map, select a priority of 5 stars to display it as a menu item under Home in the [main menu bar](#)<sup>[237]</sup>.


### Favorites for Devices and Sensors

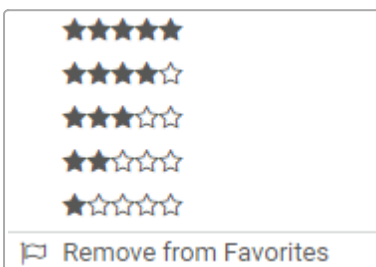
To open a list of all your favorite devices or sensors, select Devices | Favorite Devices or Sensors | Favorite Sensors from the main menu bar. These lists are sorted by priority as well.

You can mark any device or sensor as a favorite to add it to the favorites list. Right-click an object to open its context menu. Select Priority/Favorite | Add to Favorites. PRTG adds a dark gray flag icon (🚩) next to the object's name in the device tree to mark the object as a favorite.





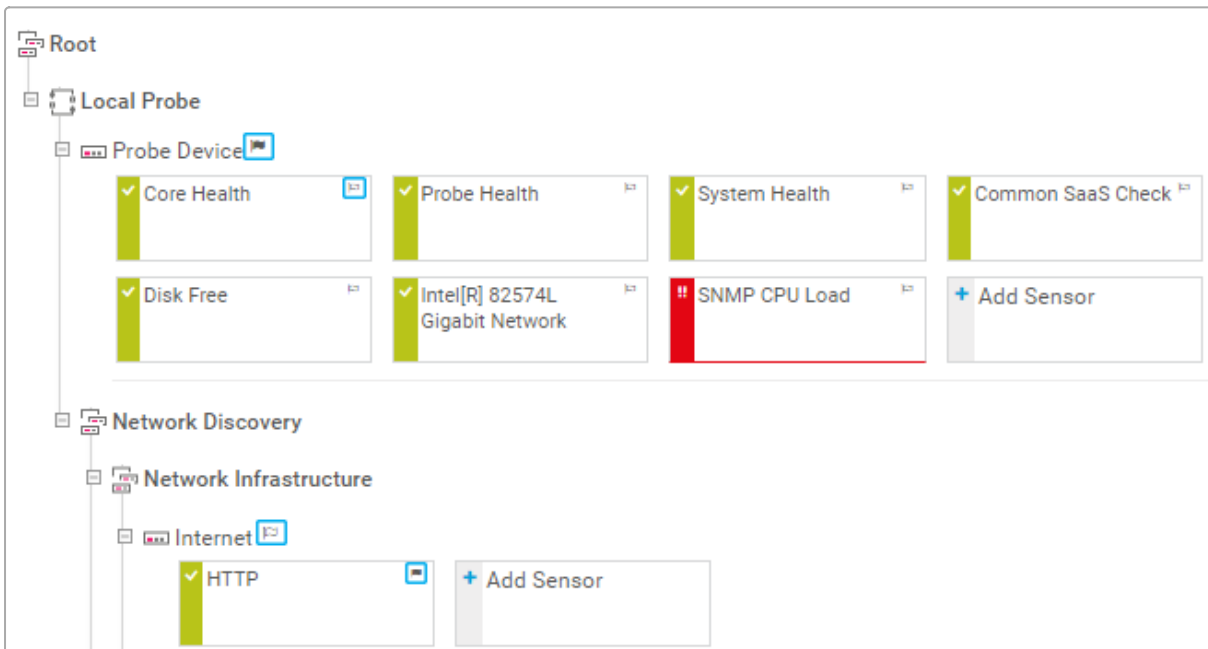
Context Menu:  
Priority/Favorites (Add)

To remove an object from the favorites list, select Priority/Favorite | Remove from Favorites from the context menu. The flag icon turns transparent (  ).







Context Menu: Priority/Favorites  
(Remove)

There is also the option to add a device or sensor to your favorites with one click in the device tree. Click the flag icon to the right of the respective object name. To make an object a favorite, click  . The flag turns dark gray. To remove an object from your favorites, click  . The flag turns transparent.



One-Click Adding to Favorites in the Device Tree

## Priority and Favorites in the Page Header Bar

You can also add any device or sensor to your favorites on the respective object's Overview tab. To do so, click  in the page header bar of a device or  in the page header bar of a sensor. Click  for a device or  for a sensor to remove the respective object from your favorites.



One-Click Favorite and Priority in the Page Header Bar

It is also possible to set the priority of an object via the five stars in the page header bar. ★★★★★ means top priority, ★☆☆☆☆ means lowest priority.



## 6.16 Pause


Several options are available to pause monitoring. You can pause monitoring for a single sensor or for an entire device, group, or probe.

### Pause by Intention (Manually or by Schedule)

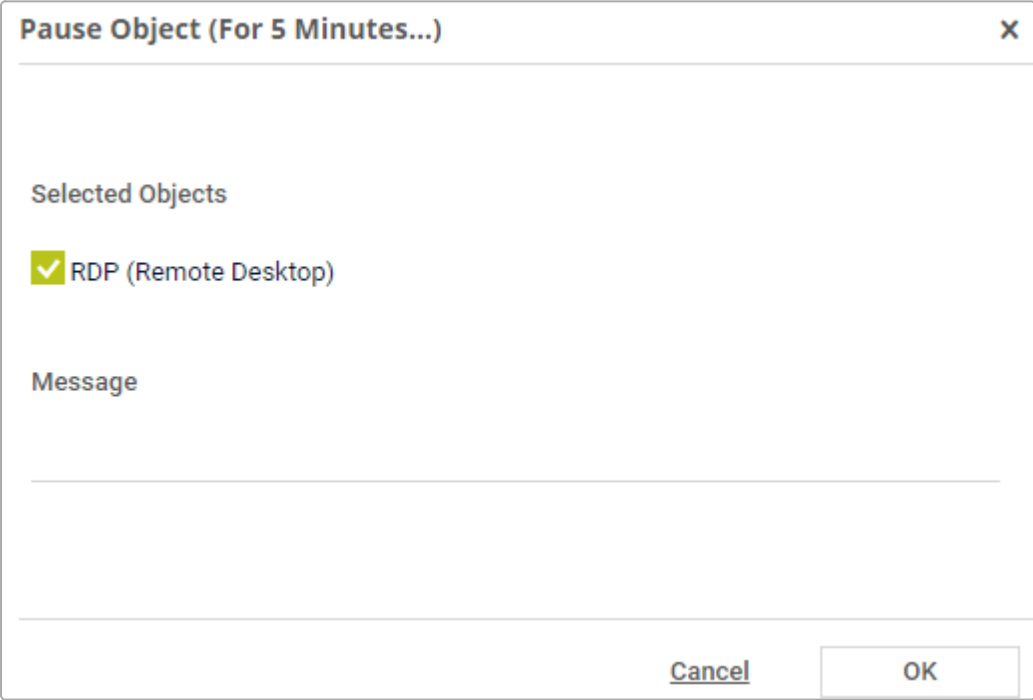
Navigate to an object in the [device tree](#)<sup>164</sup> and select Pause from the [context menu](#)<sup>229</sup>.

You can select Pause Indefinitely, or you can pause the object For 5 Minutes, For 15 Minutes, For 1 Hour, For 3 Hours, For 1 Day, or Until a specific date. If you select Until, you can additionally define a time period. Use the date time picker to enter the date and time. The object automatically resumes monitoring after this time period.

You can also set up a One-time Maintenance Window to automatically pause an object at a specified time. In the dialog that appears, define the start and end date of the maintenance window. Use the date time picker to enter the date and time.

- ❶ To cancel an active maintenance window before the defined end date, change the time entry under Maintenance Ends to a date in the past.
- ❷ If you select  from an object's [hover popup](#)<sup>235</sup>, the object is paused indefinitely until you resume monitoring again.

When you select a pause option, a dialog appears in which you can optionally enter a message. PRTG shows the message in the object's status message as long as the object is in the Paused status. Confirm with OK to pause the object.



**Pause Object (For 5 Minutes...)** X

Selected Objects

RDP (Remote Desktop)

Message

Cancel OK

Pause Message Prompt

You can also pause monitoring via [schedules](#)<sup>[2846]</sup>. If you pause a master sensor by schedule or manually, you do not trigger a status change by [dependency](#)<sup>[228]</sup>.

■ For more information, see the Knowledge Base: [Why will dependent objects not automatically pause when I pause the master object?](#)

ⓘ While a sensor is in the Paused [status](#)<sup>[181]</sup>, it does not collect any monitoring data, it does not change its status, and it does not trigger any [notifications](#)<sup>[142]</sup>. An object also keeps the Paused status after a restart of PRTG.

## Pause by Hierarchy

If you pause monitoring for an object in the device tree, PRTG pauses all objects underneath in the [object hierarchy](#)<sup>[132]</sup> as well. For example, if you pause a group, PRTG also pauses all sensors on all devices in this group. After you pause an object, you can resume monitoring at any time by selecting Resume from the context menu.

ⓘ You cannot resume monitoring for single child objects that are paused by a parent object. You can only resume the object that you originally set to the Paused status.

## Pause by Dependency

There is a way to automatically pause objects by dependency. If you have a master sensor, for example, a master [Ping](#) sensor for a device, PRTG can automatically pause all dependent sensors on the device if the master sensor shows the Down status.

■ For more information, see section [Dependencies](#)<sup>[140]</sup>.

## More

### ■ KNOWLEDGE BASE

Why will dependent objects not automatically pause when I pause the master object?

- <https://kb.paessler.com/en/topic/76351>

## 6.17 Context Menus

Right-click an object to view a context menu with many options for direct access to monitoring data and functions.

**i** To view your browser's context menu, press the Ctrl key (Google Chrome) or the Shift key (Mozilla Firefox) while right-clicking. You then see the context menu of your browser instead of the context menu of PRTG. This is not possible with Internet Explorer.





### Context Menus








**i** Which options are available depends on the type of object that you select.




Action	Description
Scan Now	Perform an immediate scan of the object. This queries data for all objects underneath in the <a href="#">object hierarchy</a> <sup>[132]</sup> .
Details	Show the Overview tab of the object.  ■ For more information about the Overview tab, see the Knowledge Base: <a href="#">What options do I have to review my monitoring data in detail?</a>
Edit	<b>i</b> Which options are available depends on the type of object that you select.  Hover over Edit to show the Edit menu. The following actions are available: <ul style="list-style-type: none"> <li>▪ Settings: Open a dialog to edit the <a href="#">object settings</a><sup>[201]</sup>.</li> <li>▪ Notification Triggers: Open the <a href="#">Notification Triggers</a><sup>[229]</sup> tab of the object.</li> <li>▪ Access Rights: Open a dialog to edit the <a href="#">access rights</a><sup>[145]</sup> for the object.</li> <li>▪ Rename: Open a dialog to edit the name of the object.</li> <li>▪ Management: Open the Management <a href="#">tab</a><sup>[418]</sup> of the object.</li> </ul>
Acknowledge Alarm	<b>This option is only available in the sensor context menu when you select a sensor in the Down or Down (Partial) status.</b>  You can acknowledge an alarm for the sensor. A sensor with an acknowledged alarm shows the Down (Acknowledged) status and does not <a href="#">trigger</a> <sup>[2693]</sup> any more <a href="#">notifications</a> <sup>[2735]</sup> . The following actions are available: <ul style="list-style-type: none"> <li>▪ Acknowledge Indefinitely</li> <li>▪ Acknowledge the alarm for a certain period of time:</li> </ul>

Action	Description
	<ul style="list-style-type: none"> <li>▫ For 5 Minutes</li> <li>▫ For 15 Minutes</li> <li>▫ For 1 Hour</li> <li>▫ For 3 Hours</li> <li>▫ For 1 Day</li> <li>▫ Until: Define a custom time period to acknowledge the alarm. Use the date time picker to enter the date and time.</li> </ul> <p><b>i</b> If the alarm condition still exists after this time period, the sensor shows the Down status again.</p> <p><b>i</b> When the alarm condition clears, the sensor usually returns to the Up status immediately with the next sensor scan.</p> <p><b>■</b> For more information about acknowledging an alarm, see section <a href="#">Alarms</a><sup>[203]</sup>.</p>
Add Sensor	<p>Open a dialog that guides you through the process of adding a new sensor to the device.</p> <p><b>■</b> For more information, see section <a href="#">Add a Sensor</a><sup>[414]</sup>.</p>
Auto-Discovery	<p>This option is only available for auto-discovery groups or devices that have the auto-discovery feature <a href="#">enabled</a><sup>[529]</sup>.</p> <p>Hover over Auto-Discovery to show the Auto-Discovery menu. The following actions are available:</p> <ul style="list-style-type: none"> <li>▫ Run Auto-Discovery: Immediately start a search to automatically add new sensors to the device. The search runs in the background and uses the options you set for the Auto-Discovery Level in the device settings under Auto-Discovery Settings. If there are new sensors, you see them after a few minutes. <ul style="list-style-type: none"> <li><b>■</b> For more information, see section <a href="#">Auto-Discovery</a><sup>[255]</sup>.</li> </ul> </li> <li><b>i</b> If you set the option No auto-discovery for the Auto-Discovery Level in the device settings and start the auto-discovery from the context menu, PRTG runs it with the standard device identification and changes the device setting to Standard auto-discovery (default).</li> <li>▫ Run Auto-Discovery with Template: Open a dialog to start an automatic search with a standard, detailed, or custom device template. <ul style="list-style-type: none"> <li><b>i</b> If you select this option from the context menu, the options you set for the Auto-Discovery Level in the object settings do not apply.</li> </ul> </li> </ul> <p><b>☁</b> This option is not available on the hosted probe of a PRTG Hosted Monitor instance.</p>

Action	Description
Create Device Template	<p>This option is only available for devices.</p> <p>Open a dialog that guides you through the process of creating a new device template. The template is then available for the auto-discovery.</p> <p>■ For more information, see section <a href="#">Create Device Template</a><sup>[2725]</sup>.</p>
Recommend Now	<p>This option is only available if the <a href="#">Recommended Sensors Detection</a><sup>[2874]</sup> is enabled.</p> <p>Start an analysis to get sensor recommendations for the device. When PRTG finishes the analysis of the device, you see the recommended sensors in a table list on the device's Overview tab where you can directly add the respective sensors.</p>
Add Group	<p>This option is only available for probes and groups.</p> <p>Open a dialog that guides you through the process of adding a new group.</p> <p>■ For more information, see section <a href="#">Add a Group</a><sup>[313]</sup>.</p>
Add Auto-Discovery Group	<p>This option is only available for probes and groups.</p> <p>Open a dialog that guides you through the process of adding a new auto-discovery group. PRTG creates a new group and runs an auto-discovery in your network to automatically add devices and sensors.</p> <p>■ For more information, see section <a href="#">Add an Auto-Discovery Group</a><sup>[258]</sup>.</p> <p>☁ This option is not available on the hosted probe of a PRTG Hosted Monitor instance.</p>
Add Device	<p>This option is only available for probes and groups.</p> <p>Open a dialog that guides you through the process of adding a new device.</p> <p>■ For more information, see section <a href="#">Add a Device</a><sup>[363]</sup>.</p>
Sort Alphabetically	<p>Sort direct child objects in alphabetical order.</p> <p>ⓘ PRTG stores the sorting order in the monitoring configuration. You cannot undo it.</p>
Delete	<p>Delete the object. PRTG asks for confirmation before it actually deletes an object.</p>

Action	Description
	<p> You cannot delete local probes or hosted probes.</p>
Clone	<p>Open a dialog that guides you through the process of cloning the object.</p> <p> For more information, see section <a href="#">Clone Object</a><sup>[2714]</sup>.</p>
Move	<p> Which options are available depends on the type of object that you select.</p> <p>Hover over Move to open the Move menu. The following actions are available:</p> <ul style="list-style-type: none"> <li>▪ Top: Move the object to the top of the parent object.</li> <li>▪ Up: Move the object one entry up.</li> <li>▪ Down: Move the object one entry down.</li> <li>▪ Bottom: Move the object to the bottom of the parent object.</li> <li>▪ Rename: Open a dialog to edit the name of the object.</li> <li>▪ Management: Open the Management <a href="#">tab</a><sup>[418]</sup> of the object.</li> <li>▪ To Other Group: Move the object to a different group.</li> </ul>
Pause or Resume	<p>Hover over Pause to open the Pause menu. The following actions are available:</p> <ul style="list-style-type: none"> <li>▪ If the object already shows the Paused <a href="#">status</a><sup>[181]</sup> or if it shows the Down status because of a <a href="#">simulated error</a>, the Resume option appears. Click Resume to restart monitoring on the object. Use the date time picker to enter the date and time. The object automatically resumes monitoring after this time period.</li> <li>▪ You can also set up a One-time Maintenance Window to automatically pause the object at a specified time. In the dialog that appears, define the start and end date of the maintenance window. Use the date time picker to enter the date and time.</li> </ul> <p> To cancel an active maintenance window before the defined end date, change the time entry under Maintenance Ends to a date in the past.</p> <ul style="list-style-type: none"> <li>▪ If the object already shows the Paused <a href="#">status</a><sup>[181]</sup> or if it shows the Down status because of a <a href="#">simulated error</a>, the Resume option appears. Click Resume to restart monitoring on the object.</li> </ul>
Simulate Error Status	<p><a href="#">This option is only available for sensors.</a></p> <p>Manually set the sensor to the Down status. If the sensor already shows the Down status because of a <a href="#">simulated error</a>, the Resume option appears. Click Resume to restart monitoring.</p>

Action	Description
	<p> The Simulate Error Status option does not work for sensors that run on mini probes.</p>
Priority	<p>Hover over Priority to open the Priority menu. Define the priority of the object.</p> <p> For more information, see section <a href="#">Priority and Favorites</a> <sup>224</sup>.</p>
Historic Data	<p>Hover over Historic Data to open the Historic Data menu. The following actions are available:</p> <ul style="list-style-type: none"> <li>▪ Open the historic data tabs for the specified time interval: Last 2 days, Last 30 days, or Last 365 days. <ul style="list-style-type: none"> <li> For more information, see the Knowledge Base: <a href="#">What options do I have to review my monitoring data in detail?</a></li> </ul> </li> <li>▪ Create Report: Open a dialog to add a new report. <ul style="list-style-type: none"> <li> When you create a report via the context menu, PRTG automatically includes the selected probe in the report.</li> </ul> </li> </ul> <p> For more information, see the Paessler website: <a href="#">How to set up reports in PRTG in 5 easy steps</a>.</p>
Device Tools	<p><a href="#">This option is only available for devices.</a></p> <p>Hover over Device Tools to open the Device Tools menu. The following actions are available:</p> <p> This option is not available on the hosted probe of a PRTG Hosted Monitor instance.</p> <ul style="list-style-type: none"> <li>▪ Go to Service URL: Open the service page that you defined in the <a href="#">device settings</a> <sup>597</sup>. If no service URL is available for the device, you can enter an address in the dialog that appears.</li> <li>▪ New Window with HTTP: Open a new browser window with HTTP and the IP address or Domain Name System (DNS) name of the device.</li> <li>▪ New Window with HTTPS: Open a new browser window with HTTPS and the IP address or DNS name of the device.</li> <li>▪ New Window with FTP: Open a new browser window with the File Transfer Protocol (FTP) and the IP address or DNS name of the device.</li> <li>▪ Remote Desktop: Download an .rdp file. When you execute this file, a remote desktop starts with the IP address or DNS name of the device. <ul style="list-style-type: none"> <li> In Firefox, you must use <a href="#">mstsc.exe (Microsoft Terminal Service)</a> to open the file.</li> </ul> </li> <li>▪ Traceroute: Start a traceroute on the device. PRTG displays the route and measures transit delays of packets across the IP network.</li> </ul>

Action	Description
	<ul style="list-style-type: none"> <li>Install Remote Probe: Open a dialog to install a classic remote probe on the device. For more information, see section <a href="#">Classic Remote Probe Setup via Device Tools</a> <sup>3202</sup>.</li> <li> This option is only available on devices on local probes.</li> <li> This option is not available in PRTG Hosted Monitor.</li> </ul>
Find Duplicates	<p>This option is only available for devices.</p> <p>In your configuration, search for devices with the same IP address or DNS name as the selected device.</p>
Send Link by Email	<p>Send a link to the object by email. Click to create a new email with your system's standard email client. The email contains a direct link to the Overview tab of the object.</p>
Add Ticket	<p>Open the Add Ticket dialog.</p> <ul style="list-style-type: none"> <li> For more information, see section <a href="#">Tickets</a> <sup>215</sup>.</li> </ul>

## More

### KNOWLEDGE BASE

What options do I have to review my monitoring data in detail?

- <https://kb.paessler.com/en/topic/90007>

### PAESSLER WEBSITE

How to set up reports in PRTG in 5 easy steps

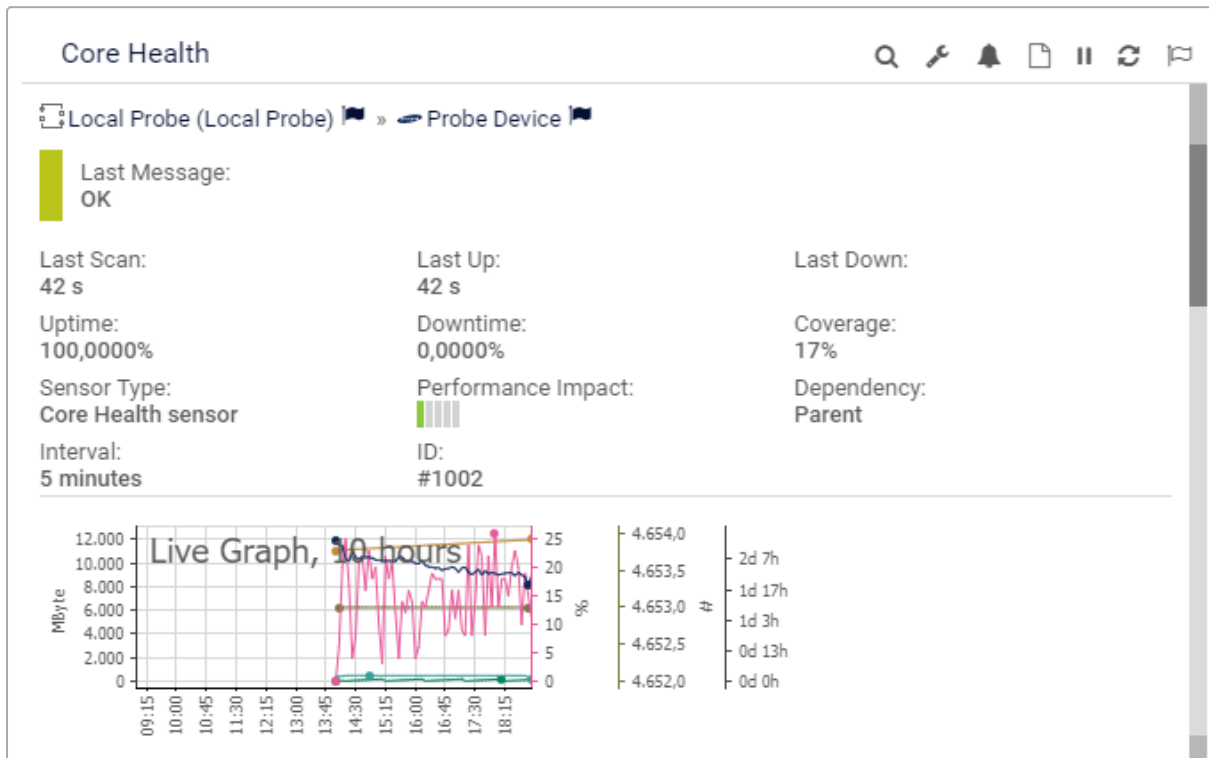
- <https://www.paessler.com/support/how-to/reports>



## 6.18 Hover Popup

When you rest the mouse pointer over an object's icon in the [device tree](#)<sup>[164]</sup> or in [table lists](#)<sup>[218]</sup>, for example, a hover popup window appears and shows details about this object. The hover popup contains information from the object's Overview tab as well as several graphs. The exact information that PRTG provides depends on the type of object.

For more information about the Overview tab, see the Knowledge Base: [What options do I have to review my monitoring data in detail?](#)



Hover Popup Example: Core Health Sensor

**i** The hover popup only appears if your browser window that shows the PRTG web interface is the active window on your desktop. The hover popup disappears with every (automatic) page refresh.

### Quick Action Buttons

In the top-right corner of the hover popup window, you can see several quick action buttons with which you can view or edit the object. These are the most important options from the object's [context menu](#)<sup>[229]</sup>.

**i** The available buttons depend on the type of object that you hover over.

Action	Description
Details (🔍)	Show the Overview tab of the object.

Action	Description
Settings (🔧)	Open the object's settings.
Notification Triggers (🔔)	Show the Notification Triggers tab of the object.
Rename (📄)	Open a dialog to edit the name of the object.
Pause Indefinitely (⏸)	Indefinitely pause the object and all objects underneath in the <a href="#">object hierarchy</a> <sup>[132]</sup> . If you want to resume monitoring, you must manually resume the paused object.
Resume (▶)	Resume monitoring for the object and all objects underneath in the object hierarchy.
Delete (🗑)	Delete the object. PRTG asks for confirmation before it actually deletes an object.
Scan Now (🔄)	Perform an immediate scan of the object. This queries data for all objects underneath in the object hierarchy.
Add to Favorites (🚩)	Make the object a <a href="#">favorite</a> <sup>[224]</sup> and add it to your favorites list.
Remove from Favorites (🚩)	Remove the object from your favorites list.

## More

### ■ KNOWLEDGE BASE

What options do I have to review my monitoring data in detail?

- <https://kb.paessler.com/en/topic/90007>

## 6.19 Main Menu Structure

You can access all functions via the main menu bar. In this section, you find information about the most important menu items. You can either directly click a menu item or you can hover over it to show more options.



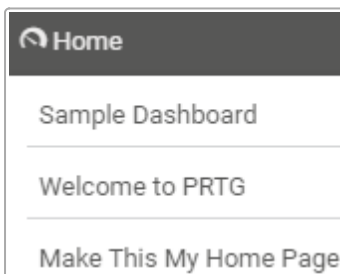
**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

In this section:

- [Home](#) <sup>237</sup>
- [Devices](#) <sup>238</sup>
- [Libraries](#) <sup>240</sup>
- [Sensors](#) <sup>241</sup>
- [Alarms](#) <sup>244</sup>
- [Maps](#) <sup>244</sup>
- [Reports](#) <sup>245</sup>
- [Logs](#) <sup>246</sup>
- [Tickets](#) <sup>247</sup>
- [Setup](#) <sup>249</sup>
- [Search Box](#) <sup>251</sup>
- [Logout](#) <sup>251</sup>

### Home

Click to open your home page. The default home page is the Welcome [page](#) <sup>164</sup>. Hover over Home to show other options.



Main Menu: Home





Option	Description
Sample Dashboard	<p>Open a preconfigured dashboard to view monitoring data in a different layout. This dashboard is one of the default <a href="#">maps</a> [2776] that PRTG automatically creates with a new installation.</p> <p><b>i</b> The Home menu shows maps that have a 5-star <a href="#">priority</a> [224] (★★★★★) To show a map here, give it 5 stars on the Maps overview via the <a href="#">main menu bar</a> [244]. You can include up to 10 map entries in the menu. For more information, see section <a href="#">Home Menu</a> [2778].</p> <p><b>i</b> You can change the appearance of the default dashboard with the <a href="#">Map Designer</a> [2780]. To not show the sample dashboard in the menu, define a priority that is lower than 5 stars for this map.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
Switch Cluster Node	<p><b>This option is only available if PRTG runs in a failover cluster</b> [128].</p> <p>Show available cluster nodes. Hover over Switch Cluster Node to show other options. Follow the menu path that is specific to your setup to select a different cluster node. The current master node is shown in bold letters. Click a cluster node's name to leave the current cluster node, to connect to the other cluster node, and to show the same page there.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
Welcome to PRTG	<p>Open the Welcome page that shows the Paessler news feed and various information about your PRTG installation. It also provides links to major sections of the PRTG web interface.</p> <p><b>i</b> This is the default home page of the PRTG web interface.</p>
Make This My Home Page	<p>Change the page that is loaded when you click Home in the main menu bar. Select this option on any page to set its URL as your home page. This setting is user sensitive. The default home page is <a href="#">/welcome.htm</a>.</p> <p><b>i</b> You can also change the home page under Home Page URL in the <a href="#">My Account</a> [2801] settings.</p>

## Devices

Click to show the device tree. Hover over Devices to show other options.

Devices
All
Favorite Devices
Device List
Dependencies
Add Group
Add Auto-Discovery Group
Add Device

Main Menu: Devices

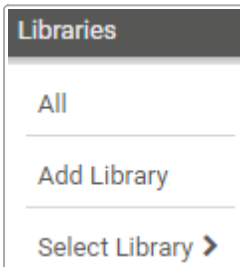
Option	Description
All	Open the Overview tab of the <a href="#">root group</a> [132] that shows the <a href="#">device tree</a> [164].
Favorite Devices	Open a <a href="#">table list</a> [218] of all devices that you marked as <a href="#">favorites</a> [224]. Click  to show a printable list of the QR codes of all your favorite devices.  <i>i</i> To mark any device as a favorite device, select Priority/Favorite   Add to Favorites from its context menu, or click  on a device's Overview tab.
Device List	Open a list of all devices in your setup.
Dependencies	Open an overview list of the <a href="#">dependencies</a> [140] configured for the objects in your setup. You can select dependencies and define master dependencies in the Schedules, Dependencies, and Maintenance Window <a href="#">object settings</a> [201] (not available for the root group).
Add Group	Start a dialog that guides you through the process of adding a new group to your setup.   For more information, see section <a href="#">Create Objects Manually</a> [257].  <i>i</i> You can also create new groups by selecting Add Group from a probe's or group's context menu.
Add Auto-Discovery Group	Start a dialog that guides you through the process of adding a new auto-discovery group to your setup. PRTG creates a new group and runs an auto-discovery in your network to automatically add devices and sensors to this group.   For more information, see section <a href="#">Add an Auto-Discovery Group</a> [258].

Option	Description
	<p><b>i</b> You can also create new auto-discovery groups by selecting Add Auto-Discovery Group from a probe's or group's context menu.</p> <p><b>☁</b> This option is not available on the hosted probe of a PRTG Hosted Monitor instance.</p>
Add Device	<p>Start a dialog that guides you through the process of adding a new device to a group. During the process, you can choose if PRTG runs an auto-discovery for the new device to automatically add sensors.</p> <p><b>■</b> For more information, see section <a href="#">Create Objects Manually</a> <sup>257</sup>.</p> <p><b>i</b> You can also create new devices by selecting Add Device from a group's context menu.</p>

## Libraries

Click to open the Libraries list where you can view or add custom device tree views of your network status and monitoring data. Hover over Libraries to show other options.

**■** For more information, see section [Libraries](#) <sup>2738</sup>.

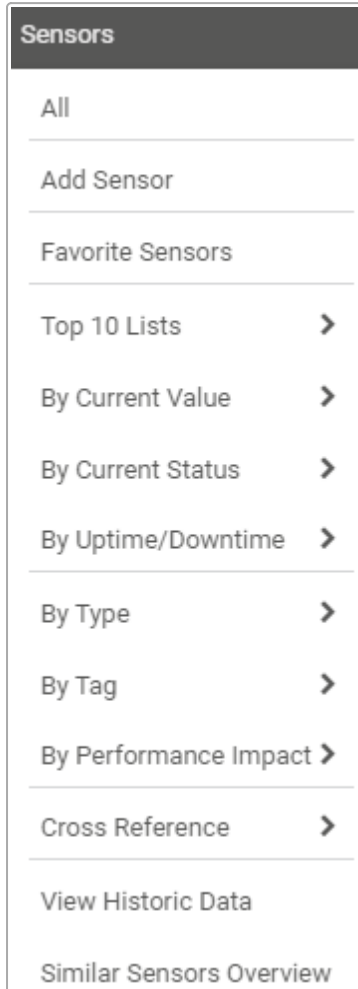


Main Menu: Libraries

Option	Description
All	Open the Libraries list where you can view or add custom device tree views of your network status and monitoring data.
Add Library	Open a dialog to create a new library.
Select Library	Open a library. Hover over Select Library to show more options. Follow the alphabetical menu path that is specific to your setup to view your libraries. Click a library to open it.







## Sensors

Click to open a list of all [sensors](#)<sup>[134]</sup>. Hover over Sensors in the main menu bar to show other options.








Main Menu: Sensors

Option	Description
All	<p>Open a table list of all <a href="#">sensors</a><sup>[134]</sup>. In list, you can sort the items via the column headers.</p> <p><b>i</b> The column Last Value shows only the last value of the sensor's <a href="#">primary channel</a>.</p>
Add Sensor	<p>Start a dialog that guides you through the process of adding a new sensor to a device. For more information, see section <a href="#">Add a Sensor</a><sup>[414]</sup>. During the process, you can also choose to create a new device via the <a href="#">Add a Device</a><sup>[363]</sup> dialog, which you can also open directly from the <a href="#">Devices menu</a><sup>[238]</sup>.</p>

Option	Description
Favorite Sensors	<p>Open a list of all sensors that you marked as favorites.</p> <p> To mark any sensor as a favorite sensor, select Priority/Favorite   Add to Favorites from its context menu or click  on a sensor's Overview tab.</p>
Top 10 Lists	<p>Open a dashboard view with different top 10 lists that show the highest uptime or downtime, ping response times, the bandwidth usage, website response times, the CPU usage, the disk usage, the memory usage, and the system uptime. Click to show top 10 lists for all sensors. Hover over Top 10 Lists to show other options. Follow the menu path that is specific to your setup to only view top 10 lists for a specific probe or group.</p> <p> The shown sensors are selected by default tags.</p>
By Current Value	<p>Open a list of sensors filtered by value. Hover over By Current Value to show other options. Follow the menu path to view lists of sensors with the Fastest Value or the Slowest Value for</p> <ul style="list-style-type: none"> <li>▪ Ping</li> <li>▪ Port</li> <li>▪ Web Pages</li> <li>▪ IMAP/POP3/SMTP</li> <li>▪ FTP</li> </ul> <p>as well as a list of sensors with the Highest Value or the Lowest Value regarding</p> <ul style="list-style-type: none"> <li>▪ Bandwidth</li> <li>▪ CPU</li> <li>▪ Disk</li> <li>▪ Memory</li> </ul> <p> The shown sensors are selected by default tags.</p>
By Current Status	<p>Open a list of sensors filtered by status. Hover over By Current Status to show other options. Follow the menu path to view lists of all sensors in a specific status.</p> <p> For more information, see section <a href="#">Sensor States</a>  181.</p>
By Uptime/Downtime	<p>Open a list of sensors filtered by different parameters. Hover over By Uptime/Downtime to show other options. Follow the menu path to view lists of all sensors sorted by</p>



Option	Description
	<ul style="list-style-type: none"> <li>▪ Best Uptime (%)</li> <li>▪ Highest Uptime (Time)</li> <li>▪ Worst Downtime (%)</li> <li>▪ Highest Downtime (Time)</li> </ul>
By Type	<p>Open a list of sensors filtered by <a href="#">sensor type</a><sup>[3232]</sup>. Hover over By Type to show other options. Follow the alphabetical menu path that is specific to your setup to view a sensor list that contains only sensors of one specific sensor type.</p>
By Tag	<p>Open a list of sensors filtered by <a href="#">tag</a><sup>[138]</sup>. Hover over By Tag to show other options. Follow the alphabetical menu path that is specific to your setup to see available tags. Select a tag to view a list that contains only sensors marked with this tag.</p> <p> If you have more than 1,000 tags, no tags are shown here. For more information, see section <a href="#">Tags</a><sup>[139]</sup>.</p>
By Performance Impact	<p>Open a list of sensors filtered by <a href="#">performance impact</a><sup>[2952]</sup>. Follow the menu path to view a sensor list that contains only sensors with a specific level of impact on the performance of the probe:</p> <ul style="list-style-type: none"> <li>▪ Very High</li> <li>▪ High</li> <li>▪ Medium</li> <li>▪ Low</li> <li>▪ Very Low</li> </ul> <p> For an overview list of all sensors, including their performance impact, see section <a href="#">Available Sensor Types</a><sup>[3232]</sup>.</p>
Cross Reference	<p>Open the sensor cross reference to show information about all sensors including <a href="#">priority and favorite</a><sup>[224]</sup> status, <a href="#">scanning interval</a><sup>[450]</sup>, <a href="#">access rights</a><sup>[145]</sup>, <a href="#">notification trigger settings</a><sup>[201]</sup>, <a href="#">schedules</a><sup>[141]</sup>, and <a href="#">dependencies</a><sup>[140]</sup>. Click to show a sensor cross reference for all sensors. Hover over Cross Reference to show other options. Follow the menu path that is specific to your setup to view cross reference information for sensors by type or tag.</p>
View Historic Data	<p>Open a dialog to generate historic sensor data reports.</p> <p> For more information, see section <a href="#">Historic Data Reports</a><sup>[185]</sup>.</p>
Similar Sensors Overview	<p>Open an overview with a list of similar sensors.</p>

Option	Description
	 For more information, see section <a href="#">Similar Sensors</a>  192

## Alarms

Click to open a list of all sensors that show the Down, Down (Partial), Down (Acknowledged), Warning, or Unusual status. Hover over Alarms to show other options.

**Alarms**

---

All

---

Show as Gauges

---

Errors Only

---

Warnings Only

---

Unusuals Only

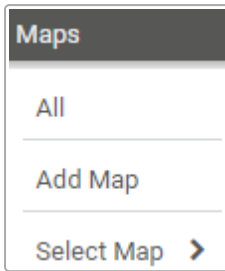
Main Menu: Alarms

Option	Description
All	Open a list of all sensors that are in the Down, Down (Partial), Down (Acknowledged), Warning, or Unusual status.
Show as Gauges	Open a page with the gauges of all sensors that are in the Down, Down (Partial), Down (Acknowledged), Warning, or Unusual status. The size of the gauges corresponds to the sensor's priority.
Errors Only	Open a list of all sensors that are in the Down, Down (Partial), or Down (Acknowledged) status.
Warnings Only	Open a list of all sensors that are in the Warning status.
Unusuals Only	Open a list of all sensors that are in the Unusual status.

## Maps

Click to open the Maps overview where you can view or add custom views of your network status and monitoring data. Hover over Maps to show other options.

For more information, see section [Maps](#)<sup>[2776]</sup>.



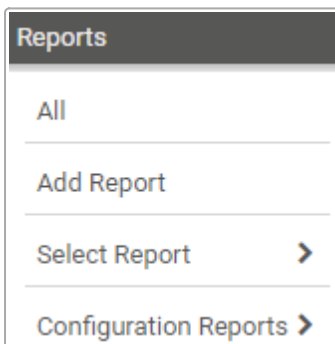
Main Menu: Maps

Option	Description
All	Open the Maps list where you can view or add custom views of your network status and monitoring data.
Add Map	Open a dialog to create a new map.
Select Map	Hover over Select Map to show a list of your maps. Click a map to open it.

## Reports

Click to open the Reports overview where you can view or add reports about your monitoring data. Hover over Reports to show other options.

For more information, see section [Reports](#)<sup>[2754]</sup>.



Main Menu: Reports

Option	Description
All	Open the Reports list where you can view or add reports about your monitoring data.

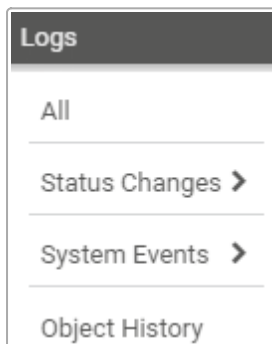
Option	Description
Add Report	Open a dialog to create a new report.
Select Report	Hover over Select Report to show a list of your reports about monitoring data. Click a report to open it.
Configuration Reports	Hover over Configuration Reports to see the available <a href="#">configuration reports</a> <sup>[2757]</sup> . Select an item to create reports for maps, reports, users and user groups, and system configuration to document changes to the configuration.

## Logs

Click to show log information for all objects in your configuration. Hover over Logs to show other options.

■ For more information, see section [Logs](#)<sup>[210]</sup>.

ⓘ Logs for monitoring objects, such as sensors, are available as long as you define Log File Records in the Historic Data Purging settings under Setup | System Administration | Core & Probes.



Main Menu: Logs

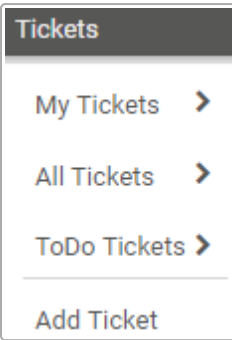
Option	Description
All	Open a list with log information about all objects in your installation. The list begins with the most recent log entry.
Status Changes	Open a list with log information about specific status changes. Hover over Status Changes to choose from the following sensor states: <ul style="list-style-type: none"> <li>▪ Up &amp; Down</li> <li>▪ Down</li> <li>▪ Warning</li> <li>▪ Unusual</li> </ul>

Option	Description
	<ul style="list-style-type: none"> <li>▪ Up</li> <li>▪ Paused/Resumed</li> <li>▪ Acknowledged Alarms</li> </ul>
System Events	<p>Open a list with log information about specific system event types. Hover over System Events to choose from the following event types:</p> <ul style="list-style-type: none"> <li>▪ Report Related</li> <li>▪ Cluster Related               <ul style="list-style-type: none"> <li> ⓘ This event type only appears if you have a cluster.</li> </ul> </li> <li>▪ Auto-Discovery Related</li> <li>▪ Notifications Related</li> <li>▪ Status Message Related</li> </ul>
Object History	<p>Open a list with log information about changes to the PRTG setup and deletions of subordinate system objects. The Object History has several tabs. To view the changes to all related settings and deletions of objects, use the following tabs:</p> <ul style="list-style-type: none"> <li>▪ My Account</li> <li>▪ System Administration</li> <li>▪ Notification Templates</li> <li>▪ Schedules</li> <li>▪ User Accounts</li> <li>▪ User Groups</li> <li>▪ Reports</li> <li>▪ Libraries</li> <li>▪ Maps</li> </ul> <p> ⓘ You can also navigate to a corresponding page, for example, you can select Setup   Account Settings   My Account from the main menu bar, and click ⓘ in the <a href="#">page header bar</a><sup>[170]</sup> to directly go to the related object history tab.</p>

## Tickets

Click to show all open tickets that are assigned to you. Hover over Tickets to show other options.

■ For more information, see section [Tickets](#)<sup>[213]</sup>.



Main Menu: Tickets

Option	Description
My Tickets	Open a list of all open tickets that are assigned to you. Hover over My Tickets to show other options to filter these tickets according to their status.
All Tickets	Open a list of all open tickets of all users. Hover over All Tickets to show other options to filter these tickets according to their status.
All Tickets	Open a list of open tickets of the type <b>ToDo</b> . Hover over All Tickets to show other options to filter these tickets according to their status.
Add Ticket	Open the Add Ticket dialog to create a <b>user ticket</b> . <span style="color: blue;">■</span> For more information about available options, see section <a href="#">Tickets</a> <sup>213</sup> .

## Setup

























Click to show the setup page. Hover over Setup to show other options.

■ For more information, see section [Setup](#) <sup>2799</sup>.

Setup
Overview
Account Settings >
System Administration >
PRTG Status
License Information
Auto-Update >
Optional Downloads >
PRTG API
Help and Support Center
Contact Support

Main Menu: Setup

Option	Description
Overview	Open the <a href="#">setup page</a> <sup>[2799]</sup> .
Account Settings	Open the <a href="#">My Account</a> <sup>[2801]</sup> settings. Hover over Account Settings to directly show and open the account settings tabs: <ul style="list-style-type: none"> <li>▪ <a href="#">My Account</a><sup>[2801]</sup></li> <li>▪ <a href="#">Notification Templates</a><sup>[2808]</sup></li> <li>▪ <a href="#">Notification Contacts</a><sup>[2842]</sup></li> <li>▪ <a href="#">Schedules</a><sup>[2846]</sup></li> </ul>
System Administration	Open the <a href="#">System Administration</a> <sup>[2855]</sup> settings. Hover over System Administration to directly show and open the system administration tabs: <ul style="list-style-type: none"> <li>▪ <a href="#">Manage Subscription</a><sup>[2855]</sup></li> <li>▪ <a href="#">User Interface</a><sup>[2855]</sup></li> <li>▪ <a href="#">Monitoring</a><sup>[2869]</sup></li> <li>▪ <a href="#">Notification Delivery</a><sup>[2877]</sup></li> </ul>

Option	Description
	<ul style="list-style-type: none"> <li>▪ <a href="#">Core &amp; Probes</a> </li> <li>▪ <a href="#">Cluster</a>  </li> <li>▪ <a href="#">User Accounts</a> </li> <li>▪ <a href="#">User Groups</a> </li> <li>▪ <a href="#">Administrative Tools</a> </li> <li>▪ <a href="#">Single Sign-On</a> </li> </ul>
PRTG Status	<p>Open the <a href="#">System Status</a>  page. If you run PRTG in a cluster, hover over PRTG Status to show other options:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">System Status</a> </li> <li>▪ <a href="#">Cluster Status</a> </li> </ul>
License Information	<p>Open the <a href="#">license information</a>  page.</p> <p> This option is not available in PRTG Hosted Monitor.</p>
Auto-Update	<p>Open information about the <a href="#">Software Auto-Update</a>  status of your PRTG installation. On this page, you can also download and install available updates. Hover over Auto-Update to show other options:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Status</a> : View the update status and manually check for the latest update.</li> <li>▪ <a href="#">Settings</a> : Define your update settings.</li> </ul> <p> This option is not available in PRTG Hosted Monitor.</p>
Optional Downloads	<p>Open the <a href="#">download page</a>  for additional downloads. Hover over Optional Downloads to show other options:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">PRTG Apps</a> </li> <li>▪ <a href="#">PRTG app for desktop</a> </li> <li>▪ <a href="#">Classic Remote Probe Installer</a> </li> </ul>
PRTG API	<p>Open the <a href="#">Application Programming Interface (API) Definition</a> .</p>
Help and Support Center	<p>Open the <a href="#">Help and Support Center</a>  from where you can access the PRTG Manual, the Knowledge Base, and video tutorials. You can also open <a href="#">support tickets</a>  and contact our <a href="#">customer service</a>  from this page.</p>



Option	Description
Contact Support	Open the <a href="#">Contact Paessler Support / Send Your Feedback to Paessler</a> form.

## Search Box



Main Menu: Search Box

Click the Search box to find objects in your monitoring setup. Enter your search term and press the Enter key. PRTG performs a string search in your entire monitoring setup, including groups, devices, sensors, libraries, maps, reports, tickets, and object comments, as well as in the PRTG Manual. You see all search results on a new page.

- ① You can only search for names that are actually displayed. To search for a specific user, for example, use their display name. You cannot search for the user's login name or email address.
- ① PRTG uses different logical operators for the search in tickets and for the search in other objects. For the ticket search, PRTG uses the logical operator **OR**. If you search for a string like 'operating system', for example, you receive results for all tickets that contain either 'operating' **or** 'system' or both. For all other objects, PRTG uses the logical operator **AND**. So you receive results for all other objects that contain both 'operating' **and** 'system'.

## Logout















Click  to log out of PRTG and return to the [login screen](#).

# Part 7

## Device and Sensor Setup

# 7 Device and Sensor Setup

In this section:

- [Auto-Discovery](#)  254
- [Create Objects Manually](#) 
  - [Add an Auto-Discovery Group](#)  258
  - [Add a Group](#)  313
  - [Add a Device](#)  363
  - [Add a Sensor](#)  414
- [Manage Device Tree](#)  418
- [Root Group Settings](#)  420
- [Probe Settings](#)  458
- [Group Settings](#)  526
- [Device Settings](#)  597
- [Sensor Settings](#)
- [Additional Sensor Types \(Custom Sensors\)](#)  2676
- [Channel Settings](#)  2681
- [Notification Triggers Settings](#)  2693

## 7.1 Auto-Discovery

The auto-discovery automatically creates a set of sensors for all of the devices that are in your network. The auto-discovery is primarily intended for devices that are in the same network as your probes.

**i** Unless you skip the auto-discovery during the installation process, PRTG runs an initial auto-discovery as soon as you finish the installation of PRTG. It automatically shows you the devices that are available in your network as well as suitable sensors for monitoring.

### How the Auto-Discovery Works

The auto-discovery has three steps:

1. Scan a network segment for devices via ping (at the group level only).
2. Assess the device type for all of the devices that it discovered in step 1 (via the Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), and other protocols).
3. Create sensor sets that match the discovered device types from step 2. It does this based on built-in device templates that have recommended sensors for many device types. Optionally, it can also create sensor sets via device templates that users [created](#)<sup>[2725]</sup>.

You can use [auto-discovery groups](#)<sup>[258]</sup> to use the auto-discovery for a range of IP addresses or for individual devices that you manually created. You can run the auto-discovery one time, on demand via the context menu, or via schedule at every hour, day, or week. If you run the auto-discovery at group level daily or weekly, it automatically creates new devices when they connect to the network and it adds suitable sensors.

**i** PRTG creates a notifying [ticket](#)<sup>[213]</sup> when it discovers at least one new device or sensor. You also receive a ticket if an error occurs. By default, PRTG also sends tickets via email. You can change this in the [My Account](#)<sup>[2807]</sup> settings.

**i** HTTP sensors' names indicate the protocol that they use to access the target device ([HTTP](#), [HTTP \(8080\)](#), and [HTTPS](#)). This distinguishes HTTP sensors from each other if the auto-discovery adds more than one HTTP sensor to a device.

### Restrictions

Note the following restrictions of the auto-discovery:

- PRTG cannot discover devices that are not reachable via ping. This is because step 1 scans for devices via ping. If, for example, a firewall blocks echo requests, PRTG cannot discover a device behind the firewall.
- Define credentials for objects that are higher in the [object hierarchy](#)<sup>[132]</sup>, for example, in the settings of the parent device. If possible, we recommend that you define these settings in the [root group](#)<sup>[420]</sup>.
- If a device has more than one IP address, it might show up more than once in the auto-discovery results, even though PRTG tries to identify these situations.
- Auto-discovery on group level does not create new sensors on devices that already exist, but only on newly discovered devices. If you want to automatically add sensors to a device, run the auto-discovery on the device via its [context menu](#)<sup>[229]</sup>.

- Frequent auto-discoveries of large network segments can lead to performance issues. Because of this we recommend that you only schedule regular auto-discoveries where necessary.
  - For more information, see the Knowledge Base: [Why can automatic auto-discoveries evoke performance issues?](#)
- PRTG automatically adds suitable device icons to discovered devices. PRTG uses a device's MAC address for this purpose, which it determines via the Address Resolution Protocol (ARP). This only works via IPv4 and not via IPv6. Usually, ARP works only in the local network unless your router supports ARP and you configure it accordingly.
- The auto-discovery does not apply the [user group setting](#)<sup>[2914]</sup> Allowed Sensors. Therefore, the auto-discovery adds all sensors that are defined in the used device templates.

## Run the Auto-Discovery Now

You can run an auto-discovery at any time on a specific device. To do so, right-click the device and select Auto-Discovery | Run Auto-Discovery from the context menu. PRTG immediately starts to search for new sensors to add to the device. If you use the auto-discovery for an auto-discovery group, PRTG adds devices with suitable sensors, if it finds any. If you use it for a device, PRTG adds new sensors, if found. In the corresponding [page header bar](#)<sup>[170]</sup>, you can always see when PRTG ran the last auto-discovery on a selected group or device.

☁ Auto-discovery for groups is not available on hosted probes.

❗ The auto-discovery also adds manually deleted devices or sensors again. If you do not want this to happen, you must always create objects [manually](#)<sup>[257]</sup>.

## Auto-Discovery in Progress

While the auto-discovery is in progress, you might experience a lower system performance than usual, because PRTG is working in the background to discover your network. Depending on the IP address ranges defined (up to 65,536 addresses), the discovery might run for up to several days before it is complete. You can review the status of the discovery process as follows:

- In the device tree, next to the group or device name, you can see a percentage value that shows the progress of the auto-discovery.
- During the auto-discovery, the PRTG web interface displays a box in the lower-right corner that shows the number of active auto-discovery tasks.
- To stop an auto-discovery, right-click the group or device, and select Pause | For 5 Minutes from the context menu. PRTG [pauses](#)<sup>[227]</sup> monitoring for 5 minutes and stops the auto-discovery tasks.

## Disable Initial Auto-Discovery

To disable the initial auto-discovery for a fresh PRTG installation, run the installer in a command prompt and add `/NoInitialAutoDisco=1` as a parameter. This might be useful for performance reasons or if you prefer to manually add devices and sensors to your installation.

## More

### ■ KNOWLEDGE BASE

Why can automatic auto-discoveries evoke performance issues?

- <https://kb.paessler.com/en/topic/14423>

How can I turn off auto-discovery?

- <https://kb.paessler.com/en/topic/10403>

How does auto-discovery with SNMP Traffic sensors work?

- <https://kb.paessler.com/en/topic/85407>

## 7.2 Create Objects Manually

We recommend that you use the [auto-discovery](#)<sup>[254]</sup> feature to create a basic monitoring setup for your network. Afterward, you can manually add devices that were not discovered, or [arrange](#)<sup>[2712]</sup> detected devices in groups.

In this section


- [Add an Auto-Discovery Group](#)<sup>[258]</sup>
- [Add a Group](#)<sup>[313]</sup>
- [Add a Device](#)<sup>[363]</sup>
- [Add a Sensor](#)<sup>[414]</sup>


### Add a Remote Probe


■ For more information, see section [Add Remote Probe](#)<sup>[3196]</sup>.

## 7.2.1 Add an Auto-Discovery Group

There are several ways to manually add an auto-discovery group:

- Select Devices | Add Auto-Discovery Group from the [main menu bar](#)<sup>[238]</sup>. A dialog appears that guides you through the process of starting an automatic detection of devices and sensors in your network.
- Hover over  and select Add Auto-Discovery Group from the menu.
- Select Add Auto-Discovery Group from the [context menu](#)<sup>[229]</sup> of the probe or group to which you want to add the new auto-discovery group. This skips step 1 and leads you directly to [step 2](#)<sup>[261]</sup>.






 This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

 You cannot use this feature on the hosted probe of a PRTG Hosted Monitor instance. You can use this feature on remote probes.

In this section:

- [Add an Auto-Discovery Group](#)<sup>[259]</sup>
- [Step 1: Select a Parent](#)<sup>[260]</sup>
- [Step 2: Define Auto-Discovery Group Settings](#)<sup>[261]</sup>
- [Basic Group Settings](#)<sup>[262]</sup>
- [Auto-Discovery Settings](#)<sup>[263]</sup>
- [Inherited Settings](#)<sup>[270]</sup>
- [Credentials for Windows Systems](#)<sup>[270]</sup>
- [Credentials for Linux/Solaris/macOS \(SSH/WBEM\) Systems](#)<sup>[273]</sup>
- [Credentials for VMware/XenServer](#)<sup>[277]</sup>
- [Credentials for SNMP Devices](#)<sup>[279]</sup>
- [Credentials for Database Management Systems](#)<sup>[284]</sup>
- [Credentials for AWS](#)<sup>[285]</sup>
- [Credentials for Script Sensors](#)<sup>[286]</sup>
- [Credentials for Cisco Meraki](#)<sup>[288]</sup>
- [Credentials for Dell EMC](#)<sup>[289]</sup>
- [Credentials for FortiGate](#)<sup>[290]</sup>
- [Credentials for HPE 3PAR](#)<sup>[290]</sup>
- [Credentials for HTTP](#)<sup>[292]</sup>
- [Credentials for Microsoft Azure](#)<sup>[294]</sup>
- [Credentials for MQTT](#)<sup>[296]</sup>
- [Credentials for NetApp](#)<sup>[299]</sup>
- [Credentials for OPC UA](#)<sup>[301]</sup>



- [Credentials for Soffico Orchestra](#)  304
- [Credentials for Redfish](#)  306
- [Credentials for REST API](#)  308
- [Credentials for Veeam](#)  309
- [Access Rights](#)  310

## Add an Auto-Discovery Group

The Add an Auto-Discovery Group dialog appears when you add a new auto-discovery group to a parent group. It only shows the settings that are required to create the auto-discovery group. Therefore, you do not see all settings in this dialog.

- ① You can change all settings on the Settings tab of the auto-discovery group later. For more information, see section [Group Settings](#)  526.

## Step 1: Select a Parent

### Add an Auto-Discovery Group (Step 1 of 2)

**Select a Parent**  
Select a parent object for the auto-discovery group.

[PRTG Manual: Add an Auto-Discovery Group](#)

**Add a New Auto-Discovery Group**  
To automate the monitoring setup, define an auto-discovery level and a list of device IP addresses/DNS names. PRTG will automatically create devices and add suitable sensors.

**Select a Probe or Group to Add the New Auto-Discovery Group to**

Select a probe or group from the list. You can add a new auto-discovery group faster by right-clicking a probe or group in the device tree and selecting **Add Auto-Discovery Group** from the context menu.

Search...

- Root
  - Local Probe
    - 1st group
      - MAIL
        - Group
      - ROUTER/SWITCHES
      - VMWARE
      - SNMP
        - Servers
      - DATABASES
      - MISC
        - CLOUD
      - Services
      - WINDOWS
      - eHealth

Add Auto-Discovery Group Assistant Step 1

Select the probe or group that you want to add the new auto-discovery group to. Click OK.

## Step 2: Define Auto-Discovery Group Settings

### Add an Auto-Discovery Group to Local Probe ✕

Enter the group settings followed by the auto-discovery preferences. PRTG then automatically creates devices within the group and adds suitable sensors. Specify credentials and access rights for the group, if necessary. All devices in this group inherit these settings.

**PRTG Manual: Auto-Discovery**

#### Basic Group Settings

Group Name ⓘ

Group

---

Tags ⓘ

+

---

#### Auto-Discovery Settings

Auto-Discovery Level ⓘ

Default auto-discovery (recommended)

Detailed auto-discovery

Auto-discovery with specific device templates

Auto-Discovery Schedule ⓘ

Once (default) ▾

---

Auto-Discovery Scanning Method ⓘ

Class C base IP address with start/end (IPv4) (default)

List of individual IP addresses and DNS names (IPv4)

IP address and subnet (IPv4)

IP address with octet range (IPv4)

List of individual IP addresses and DNS names (IPv6)

---

[Cancel](#)

Add Auto-Discovery Group Assistant Step 2

## Basic Group Settings

### Basic Group Settings

**Group Name** ⓘ

Group

---

**Tags** ⓘ

+

Basic Group Settings

Setting	Description
Group Name	<p>Enter a name to identify the group. By default, PRTG shows this name in the <a href="#">device tree</a><sup>[164]</sup>, as well as in <a href="#">alarms</a><sup>[202]</sup>, <a href="#">logs</a><sup>[210]</sup>, <a href="#">notifications</a><sup>[2735]</sup>, <a href="#">reports</a><sup>[2754]</sup>, <a href="#">maps</a><sup>[2776]</sup>, <a href="#">libraries</a><sup>[2738]</sup>, and <a href="#">tickets</a><sup>[213]</sup>.</p> <p>ⓘ If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Tags	<p>Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically <a href="#">inherited</a><sup>[138]</sup>.</p> <p>ⓘ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (&lt;&gt;).</p> <p>ⓘ For performance reasons, it can take some minutes until you can filter for new tags that you added.</p>

## Auto-Discovery Settings

## Auto-Discovery Settings

### Auto-Discovery Level ⓘ

- Default auto-discovery (recommended)
- Detailed auto-discovery
- Auto-discovery with specific device templates

### Auto-Discovery Schedule ⓘ

Once (default)

### Auto-Discovery Scanning Method ⓘ

- Class C base IP address with start/end (IPv4) (default)
- List of individual IP addresses and DNS names (IPv4)
- IP address and subnet (IPv4)
- IP address with octet range (IPv4)
- List of individual IP addresses and DNS names (IPv6)
- Use computers from the Active Directory (maximum 1000 computers)

### IPv4 Base ⓘ

### IPv4 Range Start ⓘ

1

### IPv4 Range End ⓘ

254


### Name Resolution ⓘ

- Use DNS names (default)
- Use IP addresses

### Handling of Already Known Devices ⓘ

- Skip auto-discovery for devices/IP addresses already known within PRTG (default)
- Perform auto-discovery for devices/IP addresses already known within PRTG

Auto-Discovery Settings

Setting	Description
Auto-Discovery Level	<p>Select the level of detail for the <a href="#">auto-discovery</a> <sup>[254]</sup>:</p> <ul style="list-style-type: none"> <li>▪ No auto-discovery: Select this option if you only want to manually create devices and sensors.</li> <li>▪ Standard auto-discovery (default): Create a set of standard sensors for standard monitoring. This option works fine for most installations.</li> <li>▪ Detailed auto-discovery: Create all standard sensors and additional sensors from detailed variants of device templates. As a result, you might get many sensors. This option is suitable for small network segments and whenever you want to monitor the maximum number of sensors available.</li> <li>▪ Auto-discovery with specific device templates: Customize the auto-discovery and select or combine standard, detailed, and custom device templates. Select one or more templates from the Device Templates list.</li> </ul> <p> Auto-discoveries can be resource intensive. They are primarily intended for devices on the same network as your probes.</p>
Device Templates	<p><b>This setting is only visible if you select Auto-discovery with specific device templates <a href="#">above</a>.</b></p> <p>Select one or more device templates by enabling a check box in front of the template name. PRTG uses the device templates that you select for the auto-discovery on the device:</p> <ul style="list-style-type: none"> <li>▪ ADSL</li> <li>▪ Buffalo TeraStation NAS</li> <li>▪ Cisco ASA VPN</li> <li>▪ Cisco Device (Generic)</li> <li>▪ Dell EqualLogic</li> <li>▪ Dell MDi Disk</li> <li>▪ DNS Server</li> <li>▪ Environment Jakarta</li> <li>▪ Environment Poseidon</li> <li>▪ FTP Server</li> <li>▪ Generic Device (Ping Only)</li> <li>▪ Generic Device (SNMP Enabled)</li> <li>▪ Generic Device (SNMP Enabled, Detailed)</li> <li>▪ HTTP Web Server</li> <li>▪ Hyper-V Host Server</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ IPMI-enabled Device</li> <li>▪ Juniper NS Device</li> <li>▪ Linux/UNIX Device (SNMP or SSH Enabled)</li> <li>▪ Mail Server (Generic)</li> <li>▪ Mail Server (MS Exchange)</li> <li>▪ Microsoft SharePoint 2010</li> <li>▪ MQTT Round Trip</li> <li>▪ NAS LenovoEMC</li> <li>▪ NAS QNAP</li> <li>▪ NAS Synology</li> <li>▪ NetApp</li> <li>▪ NTP Server</li> <li>▪ OPC UA</li> <li>▪ Printer (Generic)</li> <li>▪ Printer (HP)</li> <li>▪ RDP Server</li> <li>▪ RMON-compatible Device</li> <li>▪ Server (Cisco UCS)</li> <li>▪ Server (Compaq/HP Agents)</li> <li>▪ Server (Dell)</li> <li>▪ Server (Fujitsu)</li> <li>▪ Server (IBM)</li> <li>▪ SNMP Rittal CMC III Hardware Status</li> <li>▪ SonicWall</li> <li>▪ SSL Security Check</li> <li>▪ Switch (Cisco Catalyst)</li> <li>▪ Switch (Cisco IOS Based)</li> <li>▪ Switch (HP Procurve)</li> <li>▪ UNIX/Linux Device</li> <li>▪ UPS Health (APC)</li> <li>▪ UPS Health (Generic)</li> <li>▪ UPS Health (Liebert)</li> </ul>




Setting	Description
	<ul style="list-style-type: none"> <li>▪ VMware ESXi / vCenter Server</li> <li>▪ Web Server</li> <li>▪ Windows (Detailed via WMI)</li> <li>▪ Windows (via Remote PowerShell)</li> <li>▪ Windows (via WMI)</li> <li>▪ Windows IIS (via SNMP)</li> <li>▪ XenServer Hosts</li> <li>▪ XenServer Virtual Machines</li> </ul> <p>Once the auto-discovery is finished, PRTG creates a new <a href="#">ticket</a><sup>[213]</sup> and lists the device templates that it used to create new sensors.</p>
Schedule	<p>Select when PRTG runs the auto-discovery:</p> <ul style="list-style-type: none"> <li>▪ Once (default): Run the auto-discovery only once. PRTG adds new devices and sensors once. If you select this option, you must manually <a href="#">start the auto-discovery</a><sup>[255]</sup>.</li> <li>▪ Hourly: Run the auto-discovery for new devices and sensors every 60 minutes. <ul style="list-style-type: none"> <li>ⓘ Use this option with caution. Frequent auto-discoveries might cause performance issues, in particular when PRTG scans large network segments every hour.</li> </ul> </li> <li>▪ Daily: Run the auto-discovery for new devices and sensors every 24 hours. The first auto-discovery runs immediately. All other discoveries start at the time that you define in the <a href="#">Monitoring</a><sup>[2875]</sup> settings, section Auto-Discovery.</li> <li>▪ Weekly: Run the auto-discovery for new devices and sensors every 7 days. The first auto-discovery runs immediately. All other discoveries start at the time that you define in the Monitoring settings, section Auto-Discovery.</li> </ul> <p>ⓘ For performance reasons, PRTG sets Schedule to Once (default) on all devices that the scheduled auto-discovery creates.</p>
Auto-Discovery Scanning Method	<p>Select how you want to define the IP address range for the auto-discovery:</p> <ul style="list-style-type: none"> <li>▪ Class C base IP address with start/end (IPv4) (default): Enter an IPv4 class C address range.</li> <li>▪ List of individual IP addresses and DNS names (IPv4): Enter a list of individual IPv4 addresses or Domain Name System (DNS) names.</li> <li>▪ IP address and subnet (IPv4): Enter an IPv4 address and subnet mask.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ IP address with octet range (IPv4): Enter an IPv4 address range for every IP octet individually. With this, you can define very customizable IP address ranges.</li> <li>▪ List of individual IP addresses and DNS names (IPv6): Enter a list of individual IPv6 addresses or DNS names.</li> <li>▪ Use computers from the Active Directory (maximum 1000 computers): Search in the Active Directory for computers to perform the auto-discovery.               <ul style="list-style-type: none"> <li>ⓘ Make sure that you specify your Active Directory domain in the <a href="#">Core &amp; Probes</a> settings.</li> </ul> </li> </ul> <p>ⓘ PRTG can only discover subnets with up to 65,536 IP addresses. If you define a range with a higher number of addresses, the discovery stops before it is completed.</p>
IPv4 Base	<p><i>This setting is only visible if you select Class C base IP address with start/end (IPv4) (default) <a href="#">above</a>.</i></p> <p>Enter a class C network as the IP base for the auto-discovery. Enter the first three octets of an IPv4 address, for example, <a href="#">192.168.0</a>.</p>
IPv4 Range Start	<p><i>This setting is only visible if you select Class C base IP address with start/end (IPv4) (default) <a href="#">above</a>.</i></p> <p>Enter the IP octet of the class C network (specified above) from which PRTG starts the auto-discovery. This completes the IP base to an IPv4 address. For example, enter <a href="#">1</a> to discover from <a href="#">192.168.0.1</a> onwards.</p>
IPv4 Range End	<p><i>This setting is only visible if you select Class C base IP address with start/end (IPv4) (default) <a href="#">above</a>.</i></p> <p>Enter the IP octet of the class C network (specified above) at which PRTG stops the auto-discovery. This completes the IP base to an IPv4 address. For example, enter <a href="#">254</a> to discover up to <a href="#">192.168.0.254</a>.</p>
IPv4/DNS Name List IPv6/DNS Name List	<p><i>This setting is only visible if you select List of individual IP addresses and DNS names (IPv4) or List of individual IP addresses and DNS names (IPv6) <a href="#">above</a>.</i></p> <p>Enter a list of IP addresses or DNS names that the auto-discovery scans. Enter each address on a separate line.</p>
IPv4 and Subnet (IPv4)	<p><i>This setting is only visible if you select IP address and subnet (IPv4) <a href="#">above</a>.</i></p>

Setting	Description
	<p>Enter an expression in the format address/subnet, for example, <a href="#">192.168.3.0/255.255.255.0</a>. You can also use the short form like <a href="#">192.168.3.0/24</a>. If you want to include multiple addresses and subnets, enter them as a list separated by a comma, for example, <a href="#">192.168.3.0/255.255.255.0, 192.169.0.0/255.255.255.0</a>. PRTG scans the complete host range (without network and broadcast address) that is defined by the IP address and the subnet mask.</p>
<p>IP Address with Octet Range</p>	<p><a href="#">This setting is only visible if you select IP address with octet range (IPv4) above.</a></p> <p>Enter an expression in the format a1.a2.a3.a4, where <a href="#">a1</a>, <a href="#">a2</a>, <a href="#">a3</a>, and <a href="#">a4</a> are each a number between 0-255, or a range with two numbers and a hyphen like <a href="#">1-127</a>. PRTG calculates all permutations of all ranges. For example, <a href="#">10.0.1-10.1-100</a> results in 1,000 IP addresses that PRTG scans during the auto-discovery.</p>
<p>Organizational Unit</p>	<p><a href="#">This setting is only visible if you select Use computers from the Active Directory (maximum 1000 computers) above.</a></p> <p>Enter an <a href="#">organizational unit (OU)</a> to restrict the Active Directory search to computers that are part of this OU. For top-level OUs, use the distinguished name (DN) format without <a href="#">OU=</a> and without the domain components (DCS). If you leave this field empty, there are not any restrictions.</p> <p>Example:</p> <ul style="list-style-type: none"> <li>▪ For the DN <a href="#">OU=Domain Controllers,DC=example,DC=com</a>, enter only <a href="#">Domain Controllers</a>.</li> </ul> <p>If you have sub-OUs, use the DN format without the leading <a href="#">OU=</a> and without the DCS.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>▪ For the DN <a href="#">OU=webserver,OU=production,DC=example,DC=com</a>, enter only <a href="#">webserver,OU=production</a>.</li> <li>▪ For the DN <a href="#">OU=intranet,OU=webserver,OU=production,DC=example,DC=com</a>, enter only <a href="#">intranet,OU=webserver,OU=production</a>.</li> </ul> <p><b>i</b> Make sure that the OU contains computer accounts. If the OU is empty, you receive an error message.</p> <p><b>i</b> Do not enter the domain components. PRTG automatically uses the domain components from the domain name you enter in the <a href="#">Core &amp; Probes</a> <small>[2897]</small> settings.</p>

Setting	Description
Name Resolution	<p>Select how to monitor newly discovered devices. This only affects <a href="#">new</a> devices. This does not change the setting for other devices. Depending on your selection, the IP Address/DNS Name field of an <a href="#">added device</a><sup>599</sup> shows the DNS name or IP address that PRTG uses to access the target device:</p> <ul style="list-style-type: none"> <li>▪ Use DNS names (default): Monitor newly discovered devices via their DNS names (if available) We recommend that you use this option.</li> <li>▪ Use IP addresses: Monitor newly discovered devices via their IP addresses.</li> </ul> <p><b>i</b> This setting does not affect how PRTG shows the devices in the device tree.</p>
Handling of Already Known Devices	<p>Select how to handle known devices:</p> <ul style="list-style-type: none"> <li>▪ Skip auto-discovery for existing devices/IP addresses (default): Do not rescan existing devices or IP addresses. PRTG only adds devices with new IP addresses or DNS names. PRTG does not add devices that already exist in your configuration for example, in other groups. We recommend that you use this option.</li> <li>▪ Perform auto-discovery for existing devices/IP addresses: Rescan devices that have existing IP addresses with every auto-discovery. PRTG adds devices that already exist in other groups to this group and runs the auto-discovery on the newly added devices. <ul style="list-style-type: none"> <li><b>i</b> The auto-discovery does not run on devices that already exist in the group. If you want to run the auto-discovery for these devices, you must manually start the auto-discovery on them.</li> </ul> </li> </ul> <p><b>i</b> In certain cases, the IP resolution might not work and might result in PRTG not adding a device if it has the same local IP address as it does in a different LAN.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#)<sup>420</sup> if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#)<sup>136</sup>.


## Credentials for Windows Systems

Click  to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">Active Directory Replication Errors</a></li> <li>▪ <a href="#">Event Log (Windows API)</a></li> <li>▪ <a href="#">Exchange Backup (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database DAG (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mail Queue (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mailbox (PowerShell)</a></li> <li>▪ <a href="#">Exchange Public Folder (PowerShell)</a></li> <li>▪ <a href="#">File</a></li> <li>▪ <a href="#">File Content</a></li> <li>▪ <a href="#">Folder</a></li> <li>▪ <a href="#">Hyper-V Cluster Shared Volume Disk Free</a></li> <li>▪ <a href="#">Hyper-V Host Server</a></li> <li>▪ <a href="#">Hyper-V Virtual Machine</a></li> <li>▪ <a href="#">Hyper-V Virtual Network Adapter</a></li> <li>▪ <a href="#">Hyper-V Virtual Storage Device</a></li> <li>▪ <a href="#">PerfCounter Custom</a></li> <li>▪ <a href="#">PerfCounter IIS Application Pool</a></li> <li>▪ <a href="#">Share Disk Free</a></li> <li>▪ <a href="#">Windows CPU Load</a></li> <li>▪ <a href="#">Windows IIS Application</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Windows MSMQ Queue Length</a></li> <li>▪ <a href="#">Windows Network Card</a></li> <li>▪ <a href="#">Windows Pagefile</a></li> <li>▪ <a href="#">Windows Physical Disk I/O</a></li> <li>▪ <a href="#">Windows Print Queue</a></li> <li>▪ <a href="#">Windows Process</a></li> <li>▪ <a href="#">Windows SMTP Service Received</a></li> <li>▪ <a href="#">Windows SMTP Service Sent</a></li> <li>▪ <a href="#">Windows System Uptime</a></li> <li>▪ <a href="#">Windows Updates Status (PowerShell)</a></li> <li>▪ <a href="#">WMI Battery</a></li> <li>▪ <a href="#">WMI Custom</a></li> <li>▪ <a href="#">WMI Custom String</a></li> <li>▪ <a href="#">WMI Disk Health</a></li> <li>▪ <a href="#">WMI Event Log</a></li> <li>▪ <a href="#">WMI Exchange Server</a></li> <li>▪ <a href="#">WMI Exchange Transport Queue</a></li> <li>▪ <a href="#">WMI File</a></li> <li>▪ <a href="#">WMI Free Disk Space (Multi Disk)</a></li> <li>▪ <a href="#">WMI HDD Health</a></li> <li>▪ <a href="#">WMI Logical Disk I/O</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">WMI Memory</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2005 (Deprecated)</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2008</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2012</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2014</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2016</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2017</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2019</a></li> <li>▪ <a href="#">WMI Remote Ping</a></li> <li>▪ <a href="#">WMI Security Center</a></li> <li>▪ <a href="#">WMI Service</a></li> <li>▪ <a href="#">WMI Share</a></li> <li>▪ <a href="#">WMI SharePoint Process</a></li> <li>▪ <a href="#">WMI Storage Pool</a></li> <li>▪ <a href="#">WMI Terminal Services (Windows 2008+)</a></li> <li>▪ <a href="#">WMI Terminal Services (Windows XP/Vista/2003)</a></li> <li>▪ <a href="#">WMI UTC Time</a></li> <li>▪ <a href="#">WMI Vital System Data v2</a></li> <li>▪ <a href="#">WMI Volume</a></li> <li>▪ <a href="#">WSUS Statistics</a></li> </ul>
--	---	---

## Credentials for Windows Systems

 inherit from

**Domain or Computer Name** 

www.example.com

**User Name** 

johnqpublic

**Password** 

.....

Credentials for Windows Systems

Setting	Description
Domain or Computer Name	<p>Enter the domain or computer name of the user account with which you want to access the Windows system. PRTG uses this account for Windows Management Instrumentation (WMI) sensors and other Windows sensors.</p> <p>If you want to use a Windows local user account on the target device, enter the computer name. If you want to use a Windows domain user account (recommended), enter the domain name. PRTG automatically adds a prefix to use the NT LAN Manager (NTLM) protocol if you do not explicitly define it. Do not leave this field empty.</p>
User Name	<p>Enter the user name for access to the Windows system. Usually, you use credentials with administrator rights.</p>
Password	<p>Enter the password for access to the Windows system. Usually, you use credentials with administrator rights.</p>

## Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [SFTP Secure File Transfer Protocol](#)
- [SSH Disk Free](#)
- [SSH INodes Free](#)
- [SSH Load Average](#)
- [SSH Meminfo](#)
- [SSH Remote Ping](#)
- [SSH SAN Enclosure](#)
- [SSH SAN Logical Disk](#)
- [SSH SAN Physical Disk](#)
- [SSH SAN System Health](#)
- [SSH Script](#)
- [SSH Script Advanced](#)
- [VMware Host Hardware \(WBEM\)](#)

## Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

inherit from

**User Name** ⓘ

johnqpublic

**Authentication Method** ⓘ

Password (default)

Private key

**Password** ⓘ

.....

**WBEM Protocol** ⓘ

HTTP

HTTPS (default)

**WBEM Port** ⓘ

Default

Custom

**SSH Port** ⓘ

22

**SSH Rights Elevation** ⓘ

Run the command as the connecting user (default)

Run the command as a different user using 'sudo' (with password)

Run the command as a different user using 'sudo' (without password)









Run the command as a different user using 'su'



**SSH Connection Mode** ⓘ

Default

Compatibility mode (deprecated)



Setting	Description
User Name	Enter the user name for access to the Linux/Solaris/macOS system via Secure Shell (SSH) and Web-based Enterprise Management (WBEM). Usually, you use credentials with administrator rights.
Authentication Method	<p>Select the authentication method for the login:</p> <ul style="list-style-type: none"> <li>▪ Password (default): Provide the password for the login.</li> <li>▪ Private key: Provide an RSA private key for authentication.</li> </ul> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For more information, see section <a href="#">Monitoring via SSH</a><sup>[8007]</sup>.</p>
Password	<p><b>This setting is only visible if you select Password (default) above.</b></p> <p>Enter a password for access to the Linux/Solaris/macOS system via SSH and WBEM. Usually, you use credentials with administrator rights.</p>
Private Key	<p><b>This setting is only visible if you select Private key above.</b></p> <p>Paste the entire RSA private key, including the <b>BEGIN</b> and <b>END</b> lines. Make sure that a corresponding public key exists on the target device.</p> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For more information, see section <a href="#">Monitoring via SSH</a><sup>[8007]</sup>.</p> <p> If you do not insert a private key for the first time but if you want to <b>change</b> the private key, you need to <a href="#">restart the PRTG core server service</a><sup>[2919]</sup> for the private key change to take effect.</p>
WBEM Protocol	<p>Select the protocol that you want to use for the connection to the system via WBEM:</p> <ul style="list-style-type: none"> <li>▪ HTTP: Use an unsecure connection for WBEM.</li> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection for WBEM.</li> </ul> <p> This setting is only relevant if you use WBEM sensors.</p>
WBEM Port	Select if you want to use one of the default ports for the connection to the system via WBEM or if you want to set a custom port:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Default: Use one of the default ports. The default port for unsecure connections is <a href="#">5988</a> and the default port for secure connections is <a href="#">5989</a>.</li> <li>▪ Custom: Use a custom port.</li> </ul> <p> This setting is only relevant if you use WBEM sensors.</p>
Custom WBEM Port	<p>This setting is only visible if you select Custom above.</p> <p>Enter a custom WBEM port. Enter an integer.</p>
SSH Port	<p>Enter the port for SSH connections. Enter an integer. The default port is <a href="#">22</a>.</p> <p> By default, PRTG automatically uses this setting for all <a href="#">SSH sensors</a> <small>(3232)</small> unless you define a different port number in the sensor settings.</p>
SSH Rights Elevation	<p>Select the rights that you want to use to run the command on the target system:</p> <ul style="list-style-type: none"> <li>▪ Run the command as the connecting user (default): Use the rights of the user who establishes the SSH connection.</li> <li>▪ Run the command as a different user using 'sudo' (with password): Use the rights of a different user with a password required for <a href="#">sudo</a> to run commands on the target system, for example, as a root user.</li> <li>▪ Run the command as a different user using 'sudo' (without password): Use the rights of a different user without a password required for <a href="#">sudo</a> to run commands on the target system, for example, as a root user.</li> <li>▪ Run the command as a different user using 'su': Use the rights of a different user with <a href="#">su</a> to run commands on the target system.</li> </ul>
Target System User Name	<p>This setting is only visible if you select an option that includes <a href="#">sudo</a> or <a href="#">su</a> above.</p> <p>Enter a user name to run the specified command on the target system as a different user than the root user. If you leave this field empty, you run the command as a root user. Make sure that you set the Linux password even if you use a public key or a private key for authentication. This is not necessary if the user is allowed to run the command without a password.</p>
Password	<p>This setting is only visible if you select an option that includes <a href="#">sudo</a> or <a href="#">su</a> with password above.</p> <p>Enter the password to run the <a href="#">sudo</a> command or the <a href="#">su</a> command.</p>

Setting	Description
SSH Connection Mode	<p>Select the connection mode that you want to use to <a href="#">access data with SSH sensors</a> <sup>3007</sup>:</p> <ul style="list-style-type: none"> <li>▪ Default: This is the default connection mode for SSH sensors. It provides the best performance and security.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default connection mode does not work on the target system. The compatibility mode is the connection mode that PRTG used in previous versions and it is deprecated.</li> </ul> <p><b>i</b> We strongly recommend that you use the default connection mode.</p> <p><b>i</b> You can also individually select the connection mode for each SSH sensor in the sensor settings.</p>

## Credentials for VMware/XenServer

Click  to interrupt the [inheritance](#) <sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

- [Citrix XenServer Host](#)
- [Citrix XenServer Virtual Machine](#)
- [VMware Datastore \(SOAP\)](#)
- [VMware Host Hardware \(WBEM\)](#)
- [VMware Host Hardware Status \(SOAP\)](#)
- [VMware Host Performance \(SOAP\)](#)
- [VMware Virtual Machine \(SOAP\)](#)

## Credentials for VMware/XenServer

inherit from

User Name i

johnqpublic

Password i

.....

VMware Protocol i

HTTPS (default)

HTTP

Credentials for VMw are/XenServer

Setting	Description
User Name	Enter the user name for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.
Password	Enter the password for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.  <span>i</span> Single sign-on (SSO) passwords for vSphere do not support special characters. For more information, see the VMware sensors sections.
VMware Protocol	Select the protocol for the connection to VMware ESXi, vCenter Server, or Citrix XenServer: <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
Session Handling	Select if you want to reuse a session for VMware sensors:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Reuse a session for multiple scans (default): Select this option if you want a VMware sensor to reuse a single session for multiple sensor scans to query data. With this option, the sensor does not need to log in and out for each sensor scan. We recommend that you use this option because it reduces network load and log entries on the target device. This can increase performance.</li> <li>▪ Create a new session for each scan: If you select this option, PRTG does not reuse a session and a VMware sensor has to log in and out for each sensor scan. This can decrease performance.</li> </ul>

## Credentials for SNMP Devices

Click  to interrupt the [inheritance](#) 136.

 The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">Cisco IP SLA</a></li> <li>▪ <a href="#">SNMP APC Hardware</a></li> <li>▪ <a href="#">SNMP Buffalo TS System Health</a></li> <li>▪ <a href="#">SNMP Cisco ADSL</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Connections</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Traffic</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Users</a></li> <li>▪ <a href="#">SNMP Cisco CBQoS</a></li> <li>▪ <a href="#">SNMP Cisco System Health</a></li> <li>▪ <a href="#">SNMP Cisco UCS Blade</a></li> <li>▪ <a href="#">SNMP Cisco UCS Chassis</a></li> <li>▪ <a href="#">SNMP Cisco UCS Physical Disk</a></li> <li>▪ <a href="#">SNMP Cisco UCS System Health</a></li> <li>▪ <a href="#">SNMP CPU Load</a></li> <li>▪ <a href="#">SNMP Custom</a></li> <li>▪ <a href="#">SNMP Custom Advanced</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">SNMP Fujitsu System Health v2</a></li> <li>▪ <a href="#">SNMP Hardware Status</a></li> <li>▪ <a href="#">SNMP HP LaserJet Hardware</a></li> <li>▪ <a href="#">SNMP HPE BladeSystem Blade</a></li> <li>▪ <a href="#">SNMP HPE BladeSystem Enclosure Health</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Logical Disk</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Memory Controller</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Network Interface</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Physical Disk</a></li> <li>▪ <a href="#">SNMP HPE ProLiant System Health</a></li> <li>▪ <a href="#">SNMP IBM System X Logical Disk</a></li> <li>▪ <a href="#">SNMP IBM System X Physical Disk</a></li> <li>▪ <a href="#">SNMP IBM System X Physical Memory</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">SNMP NetApp Enclosure</a></li> <li>▪ <a href="#">SNMP NetApp I/O</a></li> <li>▪ <a href="#">SNMP NetApp License</a></li> <li>▪ <a href="#">SNMP NetApp Logical Unit</a></li> <li>▪ <a href="#">SNMP NetApp Network Interface</a></li> <li>▪ <a href="#">SNMP NetApp System Health</a></li> <li>▪ <a href="#">SNMP Nutanix Cluster Health</a></li> <li>▪ <a href="#">SNMP Nutanix Hypervisor</a></li> <li>▪ <a href="#">SNMP Poseidon Environment</a></li> <li>▪ <a href="#">SNMP Printer</a></li> <li>▪ <a href="#">SNMP QNAP Logical Disk</a></li> <li>▪ <a href="#">SNMP QNAP Physical Disk</a></li> <li>▪ <a href="#">SNMP QNAP System Health</a></li> <li>▪ <a href="#">SNMP Rittal CMC III Hardware Status</a></li> <li>▪ <a href="#">SNMP RMON</a></li> <li>▪ <a href="#">SNMP SonicWall System Health</a></li> <li>▪ <a href="#">SNMP SonicWall VPN Traffic</a></li> </ul>
---	---	--

<ul style="list-style-type: none"><li>▪ <a href="#">SNMP Custom String</a></li><li>▪ <a href="#">SNMP Custom String Lookup</a></li><li>▪ <a href="#">SNMP Custom Table</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Logical Disk</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Member Health</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Physical Disk</a></li><li>▪ <a href="#">SNMP Dell Hardware</a></li><li>▪ <a href="#">SNMP Dell PowerEdge Physical Disk</a></li><li>▪ <a href="#">SNMP Dell PowerEdge System Health</a></li><li>▪ <a href="#">SNMP Disk Free</a></li></ul>	<ul style="list-style-type: none"><li>▪ <a href="#">SNMP IBM System X System Health</a></li><li>▪ <a href="#">SNMP interSeptor Pro Environment</a></li><li>▪ <a href="#">SNMP Juniper NS System Health</a></li><li>▪ <a href="#">SNMP LenovoEMC Physical Disk</a></li><li>▪ <a href="#">SNMP LenovoEMC System Health</a></li><li>▪ <a href="#">SNMP Library</a></li><li>▪ <a href="#">SNMP Linux Disk Free</a></li><li>▪ <a href="#">SNMP Linux Load Average</a></li><li>▪ <a href="#">SNMP Linux Meminfo</a></li><li>▪ <a href="#">SNMP Linux Physical Disk</a></li><li>▪ <a href="#">SNMP Memory</a></li><li>▪ <a href="#">SNMP NetApp Disk Free</a></li></ul>	<ul style="list-style-type: none"><li>▪ <a href="#">SNMP Synology Logical Disk</a></li><li>▪ <a href="#">SNMP Synology Physical Disk</a></li><li>▪ <a href="#">SNMP Synology System Health</a></li><li>▪ <a href="#">SNMP System Uptime</a></li><li>▪ <a href="#">SNMP Traffic</a></li><li>▪ <a href="#">SNMP Trap Receiver</a></li><li>▪ <a href="#">SNMP Windows Service</a></li></ul>
--	--	--

## Credentials for SNMP Devices

inherit from

**SNMP Version** ⓘ

SNMP v1

SNMP v2c (default)

SNMP v3

**Community String** ⓘ

public

**SNMP Port** ⓘ

161

**Timeout (Sec.)** ⓘ




5

Credentials for SNMP Devices

Setting	Description
SNMP Version	<p>Select the Simple Network Management Protocol (SNMP) version for the connection to the target SNMP device:</p> <ul style="list-style-type: none"> <li>▪ <b>SNMP v1:</b> Use SNMP v1 for the connection. SNMP v1 only offers clear-text data transmission. <ul style="list-style-type: none"> <li>ⓘ SNMP v1 does not support 64-bit counters. This might result in invalid data when you monitor traffic via SNMP.</li> </ul> </li> <li>▪ <b>SNMP v2c (default):</b> Use SNMP v2c for the connection. SNMP v2c also only offers clear-text data transmission but it supports 64-bit counters.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ SNMP v3: Use SNMP v3 for the connection. SNMP v3 provides secure authentication and data encryption.</li> <li>ⓘ SNMP v3 has performance limitations because of the use of encryption. The main limiting factor is CPU power. Also keep in mind that SNMP v3, unlike SNMP v1 and v2c, does not scale with more CPU power. Because of this limitation, PRTG can only handle a limited number of requests per second so that you can use only a limited number of sensors using SNMP v3. If you see an increase in <a href="#">Interval Delay</a> or <a href="#">Open Requests</a> with the <a href="#">Probe Health</a> sensor, distribute the load over <a href="#">multiple probes</a> <small>[6198]</small>. SNMP v1 and SNMP v2c do not have this limitation.</li> </ul>
Community String	<p>This setting is only visible if you select SNMP v1 or SNMP v2c (default) above.</p> <p>Enter the community string of your device. This is like a clear-text password for simple authentication.</p> <p>ⓘ We recommend that you use the default value.</p>
Authentication Method	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Select the authentication method:</p> <ul style="list-style-type: none"> <li>▪ MD5 (default): Use message-digest algorithm 5 (MD5) for authentication.</li> <li>▪ SHA: Use Secure Hash Algorithm (SHA) for authentication.</li> <li>▪ SHA-224: Use SHA-224 for authentication.</li> <li>▪ SHA-256: Use SHA-256 for authentication.</li> <li>▪ SHA-384: Use SHA-384 for authentication.</li> <li>▪ SHA-512: Use SHA-512 for authentication.</li> </ul> <p>ⓘ If you do not want to use authentication but you need SNMP v3, for example, because your device requires <a href="#">context</a>, you can leave the Password field empty. In this case, PRTG uses <a href="#">SNMP_SEC_LEVEL_NOAUTH</a> and it entirely deactivates authentication.</p> <p>ⓘ The authentication method that you select must match the authentication method of your device.</p>
User Name	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter the user name for access to the target SNMP device.</p> <p>ⓘ The user name that you enter must match the user name of your device.</p>



Setting	Description
Password	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter the password for access to the target SNMP device.</p> <p> The password that you enter must match the password of your device.</p>
Encryption Type	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Select an encryption type:</p> <ul style="list-style-type: none"> <li>▪ DES (default): Use Data Encryption Standard (DES) as the encryption algorithm.</li> <li>▪ AES: Use Advanced Encryption Standard (AES) as the encryption algorithm.</li> <li>▪ AES-192: Use AES-192 as the encryption algorithm.</li> <li>▪ AES-256: Use AES-256 as the encryption algorithm.</li> </ul> <p> The encryption type that you select must match the encryption type of your device.</p>
Encryption Key	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter an encryption key. If you provide a key, PRTG encrypts SNMP data packets with the encryption algorithm that you selected above. Enter a string or leave the field empty.</p> <p> The encryption key that you enter must match the encryption key of your device. If the encryption keys do not match, you do not get an error message.</p>
Context Name	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter a context name only if the configuration of the device requires it. <b>Context</b> is a collection of management information that is accessible by an SNMP device. Enter a string.</p>
SNMP Port	<p>Enter the port for the connection to the SNMP target device. Enter an integer. The default port is <b>161</b>.</p> <p> We recommend that you use the default value.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).</p>


## Credentials for Database Management Systems


Click  to interrupt the [inheritance](#) .

 The settings you define in this section apply to the following sensors:

- [ADO SQL v2](#)
- [Microsoft SQL v2](#)
- [MySQL v2](#)
- [Oracle SQL v2](#)
- [PostgreSQL](#)


### Credentials for Database Management Systems

 inherit from

**Port** 


Default

Custom port for all database sensors

**Authentication Method** 

Windows authentication with impersonation (default)



SQL server authentication

**Timeout (Sec.)** 

60

Credentials for Database Management Systems

Setting	Description
Port	Select the port that PRTG uses for connections to the monitored databases:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Default: PRTG automatically determines the type of the database and uses the corresponding default port to connect. PRTG uses the following default ports: <ul style="list-style-type: none"> <li>▫ Microsoft SQL: <a href="#">1433</a></li> <li>▫ MySQL: <a href="#">3306</a></li> <li>▫ Oracle SQL: <a href="#">1521</a></li> <li>▫ PostgreSQL: <a href="#">5432</a></li> </ul> </li> <li>▪ Custom port for all database sensors: Select this option if your database management systems do not use the default ports. Enter a custom port for database connections below.</li> </ul>
Custom Port	<p>Enter a custom port for database connections. Enter an integer.</p> <p> PRTG uses this custom port for <a href="#">all</a> database sensors and for connections to <a href="#">all</a> your databases.</p>
Authentication Method	<p>Select the authentication method for the connection to the Structured Query Language (SQL) database:</p> <ul style="list-style-type: none"> <li>▪ Windows authentication with impersonation (default): PRTG uses the Windows credentials that you define in settings that are higher in the <a href="#">object hierarchy</a><sup>[132]</sup> for the database connection. <ul style="list-style-type: none"> <li> The user whose credentials PRTG uses needs to have permission to log in to the probe system with a database sensor. This is necessary for the impersonation.</li> </ul> </li> <li>▪ SQL server authentication: Use explicit credentials for database connections. Enter a user name and password below.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select SQL server authentication above.</a></p> <p>Enter the user name for the database connection.</p>
Password	<p><a href="#">This setting is only visible if you select SQL server authentication above.</a></p> <p>Enter the password for the database connection.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <a href="#">900</a> seconds (15 minutes).</p>

## Credentials for AWS

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:

- [AWS Alarm v2](#)
- [AWS Cost](#)
- [AWS EBS v2](#)
- [AWS EC2 v2](#)
- [AWS ELB v2](#)
- [AWS RDS v2](#)

■ For more information about the permissions that are necessary to query the AWS API, see the Knowledge Base: [How do I set permissions for the Amazon Web Services \(AWS\) API key to use certain sensors in PRTG?](#)

## Credentials for AWS

inherit from

**Access Key** ⓘ

---

**Secret Key** ⓘ

---

Credentials for AWS

Setting	Description
Access Key	Enter the Amazon Web Services (AWS) access key.
Secret Key	Enter the AWS secret key.

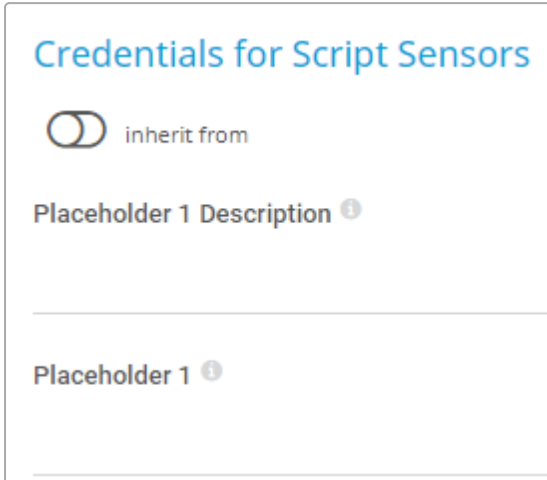
### Credentials for Script Sensors

Click  to interrupt the [inheritance](#) <sup>136</sup>.

ⓘ The settings you define in this section apply to the following sensors:

- [EXE/Script](#)
- [EXE/Script Advanced](#)
- [Python Script Advanced](#)

- [Script v2](#)
- [SSH Script](#)
- [SSH Script Advanced](#)



Credentials for Script Sensors

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder1</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder2</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder3</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.

Setting	Description
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder4</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder5</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.


### Credentials for Cisco Meraki


Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:

- [Cisco Meraki License](#)
- [Cisco Meraki Network Health](#)


## Credentials for Cisco Meraki

 inherit from

API Key 


.....

---

Meraki Dashboard API Endpoint 

api.meraki.com

Credentials for Cisco Meraki

Setting	Description
API Key	Enter an API key that the sensor uses for authentication against the Cisco Meraki Dashboard API.
Meraki Dashboard API Endpoint	Enter the endpoint for the Cisco Meraki Dashboard API. The default <a href="#">api.meraki.com</a> should be valid for most use cases.   See the Cisco Meraki Dashboard API documentation for other possible choices.


## Credentials for Dell EMC


Click  to interrupt the [inheritance](#) <sup>136</sup>.


 The settings you define in this section apply to the following sensors:


- [Dell EMC Unity Enclosure Health v2](#)
- [Dell EMC Unity File System v2](#)
- [Dell EMC Unity Storage Capacity v2](#)
- [Dell EMC Unity Storage LUN v2](#)
- [Dell EMC Unity Storage Pool v2](#)
- [Dell EMC Unity VMware Datastore v2](#)

### Credentials for Dell EMC

 inherit from

**User Name** 

**Password** 

**Port** 

Credentials for Dell EMC

Setting	Description
User Name	Enter the user name for access to the Dell EMC system.

Setting	Description
Password	Enter the password for access to the Dell EMC system.
Port	Enter the port for the connection to the Dell EMC system. The default port for secure connections is <a href="#">443</a> .


### Credentials for FortiGate


Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [FortiGate System Statistics](#)
- [FortiGate VPN Overview](#)


### Credentials for FortiGate

 inherit from

API Token 

●●●●●●●●

---

Port 

443

Credentials for FortiGate

Setting	Description
API Token	Enter the API token for access to the FortiGate system.
Port	Enter the port for the connection to the FortiGate system. The default port for secure connections is <a href="#">443</a> .

### Credentials for HPE 3PAR

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [HPE 3PAR Common Provisioning Group](#)



- [HPE 3PAR Drive Enclosure](#)
- [HPE 3PAR Virtual Volume](#)

## Credentials for HPE 3PAR

inherit from

User Name <sup>i</sup>

johnqpulic

Password <sup>i</sup>

●●●●●●●●●●●●●●●●

Protocol <sup>i</sup>

HTTPS (default)

HTTP


WSAPI Port <sup>i</sup>

8080

SSH Port <sup>i</sup>


22

Credentials for HPE 3PAR

Setting	Description
User Name	Enter the user name for access to the HPE 3PAR system.
Password	Enter the password for access to the HPE 3PAR system.
Protocol	<p>Select the protocol that you want to use for the connection to the HPE 3PAR system:</p> <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
WSAPI Port	<p>Enter the Web Services API (WSAPI) port for the connection to the HPE 3PAR system. The default port for secure connections is <b>8080</b> and the default port for unsecure connections is <b>8008</b>.</p> <p> For more information, see the Knowledge Base: <a href="#">Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?</a></p>
SSH Port	Enter the SSH port for the connection to the HPE 3PAR system. The default port for secure connections is <b>22</b> .

## Credentials for HTTP

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensor:

- [HTTP v2](#)

### Credentials for HTTP

inherit from

**Authentication Method** ⓘ

None (default)

Basic authentication

Bearer authentication

**Placeholder 1 Description** ⓘ

---

**Placeholder 1** ⓘ

---

Credentials for HTTP

Setting	Description
Authentication Method	<p>Select the authentication method for access to the server:</p> <ul style="list-style-type: none"> <li>▪ None (default): Use no authentication.</li> <li>▪ Basic authentication: Use basic authentication.</li> <li>▪ Bearer authentication: Use an OAuth2 bearer token.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter the user name for access to the server.</p>
Password	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter the password for access to the server.</p>
Bearer Token	<p><a href="#">This setting is only visible if you select Bearer authentication above.</a></p> <p>Enter a bearer token for access to the server.</p>

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder1</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder2</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder3</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder4</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder5</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.

## Credentials for Microsoft Azure

Click  to interrupt the [inheritance](#)<sup>136</sup>.



 The settings you define in this section apply to the following sensors:

- [Microsoft Azure SQL Database](#)
- [Microsoft Azure Storage Account](#)
- [Microsoft Azure Subscription Cost](#)
- [Microsoft Azure Virtual Machine](#)

The sensors use the credentials to authenticate with Microsoft Entra ID.

■ For more information about the credentials and permissions that are necessary use the Microsoft Azure sensors, see the Knowledge Base: [How do I obtain credentials and create custom roles for the Microsoft Azure sensors?](#)

### Credentials for Microsoft Azure

 inherit from  Local Probe

**Tenant ID** ⓘ

---

**Client ID** ⓘ

---


**Client Secret** ⓘ

---

**Subscription ID** ⓘ

---

**Microsoft Azure Management Endpoint** ⓘ

management.azure.com 

Credentials for Microsoft Azure

Setting	Description
Tenant ID	Enter the Microsoft Entra tenant ID.  A tenant ID must be a 32-digit sequence in hexadecimal notation.
Client ID	Enter the Microsoft Entra client ID.

Setting	Description
Client Secret	Enter the Microsoft Entra client secret.
Subscription ID	Enter the Microsoft Entra subscription ID.

## Credentials for MQTT

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:

- [MQTT Round Trip](#)
- [MQTT Statistics](#)
- [MQTT Subscribe Custom](#)

## Credentials for MQTT

inherit from

### Authentication Method i

- None (default)
- User name and password

### Port i

1883

### Transport-Level Security i


- Do not use transport-level security (default)
- Use transport-level security

Credentials for MQTT

Setting	Description
Authentication Method	<p>Select if you want to connect without credentials or define credentials for access to the MQTT broker:</p> <ul style="list-style-type: none"> <li>▪ None (default): Connect without credentials.</li> <li>▪ User name and password: Define credentials for the connection.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select User name and password above.</a></p> <p>Enter the user name for access to the Message Queue Telemetry Transport (MQTT) broker.</p>

Setting	Description
Password	<p>This setting is only visible if you select <a href="#">User name and password above</a>.</p> <p>Enter the password for access to the MQTT broker.</p>
Port	<p>Enter the port for the connection to the MQTT broker. The default port for secure connections is <b>8883</b> and the default port for unsecure connections is <b>1883</b>.</p>
Transport-Level Security	<p>Select if you want to use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection:</p> <ul style="list-style-type: none"> <li>▪ Do not use transport-level security (default): Establish the connection without connection security.</li> <li>▪ Use transport-level security: Establish the connection with the strongest SSL/TLS method that the target device provides.</li> </ul>
Server Authentication	<p>This setting is only visible if you select <a href="#">Use transport-level security above</a>.</p> <p>Select if you want to use a certificate for server authentication:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not use a certificate for server authentication.</li> <li>▪ Enable: Use a certificate for server authentication.</li> </ul>
CA Certificate	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Paste the certificate authority (CA) certificate for the verification of the MQTT broker.</p> <p> The certificate must be in Privacy-Enhanced Mail (PEM) format.</p>
Client Authentication	<p>This setting is only visible if you select <a href="#">Use transport-level security above</a>.</p> <p>Select if you want to use a certificate for client authentication:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not use a certificate for client authentication.</li> <li>▪ Enable: Use a certificate for client authentication.</li> </ul>
Client Certificate	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Paste the certificate that you created for authenticating the sensor against the MQTT broker.</p> <p> The certificate must be in PEM format.</p>
Client Key	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Enter the client key for access to the MQTT broker.</p>



Setting	Description
	 The client key must be in PEM format and it must be encrypted using the Client Key Password.
Client Key Password	This setting is only visible if you select Enable above.  Enter the password for the client key.

## Credentials for NetApp

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [NetApp Aggregate v2](#)
- [NetApp I/O v2](#)
- [NetApp LIF v2](#)
- [NetApp LUN v2](#)
- [NetApp NIC v2](#)
- [NetApp Physical Disk v2](#)
- [NetApp SnapMirror v2](#)
- [NetApp System Health v2](#)
- [NetApp Volume v2](#)

The sensors use the credentials for access to the ONTAP System Manager.

## Credentials for NetApp

inherit from Network-01f

**User Name** ⓘ  
johnqpublic

---

**Password** ⓘ  
.....

---

**Port** ⓘ  
443

---

**Protocol** ⓘ

HTTPS (default)

HTTP

Credentials for NetApp

Setting	Description
User Name	Enter a user name for access to the ONTAP System Manager.
Password	Enter the password for access to the ONTAP System Manager.
Port	Enter the port for the connection to the ONTAP System Manager. The default port for secure connections is <a href="#">443</a> .

Setting	Description
Protocol	Select the protocol that you want to use for the connection to the ONTAP System Manager: <ul style="list-style-type: none"><li>▪ HTTPS (default): Use HTTPS for the connection.</li><li>▪ HTTP: Use HTTP for the connection.</li></ul>

## Credentials for OPC UA

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [Beckhoff IPC System Health](#)
- [OPC UA Certificate](#)
- [OPC UA Custom](#)
- [OPC UA Server Status](#)

## Credentials for OPC UA

inherit from

Port <sup>i</sup>

4840

Server Path <sup>i</sup>

Security Mode <sup>i</sup>

None (default)

Sign

Sign & Encrypt



Authentication Method <sup>i</sup>

Anonymous (default)

User name and password

Credentials for OPC UA

Setting	Description
Port	Enter the port for the connection to the OPC Unified Architecture (OPC UA) server. The default port for secure connections is <a href="#">4840</a> .
Server Path	Enter the path of the OPC UA server endpoint if you run more than one server under the same IP address or DNS name.
Security Mode	Select if you want to use encryption: <ul style="list-style-type: none"> <li>▪ None (default): Do not use encryption.</li> <li>▪ Sign: Sign messages between the sensor and the OPC UA server.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Sign &amp; Encrypt: Sign and encrypt messages between the sensor and the OPC UA server.</li> </ul>
Security Policy	<p>This setting is only visible if you select Sign or Sign &amp; Encrypt above.</p> <p>Select if you want to use a security policy and define which policy you want to use:</p> <ul style="list-style-type: none"> <li>▪ None (default): Do not use a security policy.</li> <li>▪ Basic256Sha256: Use the Basic256Sha256 security policy.</li> <li>▪ Basic256: Use the Basic256 security policy.</li> </ul>
Client Certificate	<p>This setting is only visible if you select Sign or Sign &amp; Encrypt above.</p> <p>Enter the certificate that you created for authenticating the sensor against the OPC UA server.</p> <p> The certificate must meet the following requirements:</p> <ul style="list-style-type: none"> <li>▪ The key size must be 2048-bit or 4096-bit.</li> <li>▪ The secure hash algorithm must be <a href="#">SHA256</a>.</li> <li>▪ DataEncipherment must be part of the KeyUsage certificate extension.</li> <li>▪ A uniform resource indicator (URI) must be set in subjectAltName.</li> <li>▪ The certificate must be in Privacy-Enhanced Mail (PEM) format.</li> </ul>
Client Key	<p>This setting is only visible if you select Sign or Sign &amp; Encrypt above.</p> <p>Enter the client key for access to the OPC UA server.</p> <p> The client key must be in PEM format and it must be encrypted using the Client Key Password.</p>
Client Key Password	<p>This setting is only visible if you select Sign or Sign &amp; Encrypt above.</p> <p>Enter the password for the client key.</p>
Authentication Method	<p>Select if you want to connect without credentials or define credentials for access to the OPC UA server:</p> <ul style="list-style-type: none"> <li>▪ Anonymous (default): Connect without credentials.</li> <li>▪ User name and password: Define credentials for the connection.</li> </ul>

Setting	Description
	<p><b>i</b> Most OPC UA servers do not support User name and password authentication without a client certificate. To use User name and password authentication, select Sign or Sign &amp; Encrypt under Security Mode and Basic256Sha256 or Basic256 under Security Policy and enter the Client Certificate, Client Key, and Client Key Password that you want to use.</p> <p><b>i</b> If you select None (default) under Security Mode and use User name and password authentication, PRTG sends the unencrypted password to the OPC UA server.</p>
User Name	<p>This setting is only visible if you select User name and password <a href="#">above</a>.</p> <p>Enter the user name for access to the OPC UA server.</p>
Password	<p>This setting is only visible if you select User name and password <a href="#">above</a>.</p> <p>Enter the password for access to the OPC UA server.</p>

### Credentials for Soffico Orchestra

Click  to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensor:

- [Soffico Orchestra Channel Health](#)
- [Soffico Orchestra Scenario](#)

## Credentials for Soffico Orchestra

inherit from

### Authentication Method i

- None (default)  
 User name and password

### Timeout (Sec.) i

60

### Port i

8443

### Protocol i

- HTTPS (default)  
 HTTP

Credentials for Soffico Orchestra

Setting	Description
Authentication Method	Select if you want to connect without credentials or define credentials for access to the Orchestra platform: <ul style="list-style-type: none"> <li>None (default): Connect without credentials.</li> <li>User name and password: Define credentials for the connection.</li> </ul>
User Name	This setting is only visible if you select User name and password above. Enter the user name for access to the Orchestra platform.
Password	This setting is only visible if you select User name and password above.

Setting	Description
	Enter the password for access to the Orchestra platform.
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).
Port	Enter the port for the connection to the Orchestra platform. The default port for secure connections is <b>8443</b> and the default port for unsecure connections is <b>8019</b> .
Protocol	Select the protocol that you want to use for the connection to the Orchestra platform: <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>

### Credentials for Redfish

Click  to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

- [Redfish Power Supply](#)
- [Redfish System Health](#)
- [Redfish Virtual Disk](#)



### Credentials for Redfish

inherit from

**User Name** ⓘ

johnqpublic

---

**Password** ⓘ

●●●●●●●●

---

**Protocol** ⓘ

HTTPS (default)

HTTP

**Port** ⓘ

443

Credentials for Redfish

Setting	Description
User Name	Enter the user name for access to the Redfish system.
Password	Enter the password for access to the Redfish system.
Protocol	<p>Select the protocol that you want to use for the connection to the Redfish system:</p> <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
Port	Enter the port for the connection to the Redfish system. The default port for secure connections is 443.

## Credentials for REST API


Click  to interrupt the [inheritance](#) <sup>136</sup>.

 The settings you define in this section apply to the following sensor:

- [REST Custom v2](#)

### Credentials for REST API

inherit from

**Authentication Method** 

None (default)

Basic authentication

Bearer authentication

Credentials for REST API

Setting	Description
Authentication Method	Select the authentication method for access to the Representational State Transfer (REST) application programming interface (API): <ul style="list-style-type: none"> <li>▪ None (default): Use no authentication.</li> <li>▪ Basic authentication: Use basic authentication.</li> <li>▪ Bearer authentication: Use an OAuth2 bearer token.</li> </ul>
User Name	<a href="#">This setting is only visible if you select Basic authentication above.</a> Enter the user name for access to the REST API.
Password	<a href="#">This setting is only visible if you select Basic authentication above.</a> Enter the password for access to the REST API.
Bearer Token	<a href="#">This setting is only visible if you select Bearer authentication above.</a> Enter a bearer token for access to the REST API.
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.

Setting	Description
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <a href="#">%restplaceholder1</a> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <a href="#">%restplaceholder2</a> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <a href="#">%restplaceholder3</a> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <a href="#">%restplaceholder4</a> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <a href="#">%restplaceholder5</a> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.


## Credentials for Veeam

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [Veeam Backup Job Status](#)
- [Veeam Backup Job Status Advanced](#)

## Credentials for Veeam

 inherit from

**User Name** i

johnqpublic

---

**Password** i

●●●●●●●●●●●●●●●●●●●●

---

**Port** i

9398

Credentials for Veeam

Setting	Description
User Name	Enter the user name for access to the Veeam Backup Enterprise Manager.
Password	Enter the password for access to the Veeam Backup Enterprise Manager.
Port	Enter the port for the connection to the Veeam Backup Enterprise Manager. The default port for secure connections is <a href="#">9398</a> .

### Access Rights

Click  to interrupt the [inheritance](#) <sup>136</sup>.

### Access Rights

inherit from

**User Group Access** ⓘ

User Group	Rights
PRTG Users Group	Write access
Read-only User Group	Read access
SSO User Group	Inherited (No access)

Revert access rights of child objects to "inherited"

Access Rights

Setting	Description
User Group Access	<p>Select the <a href="#">user groups</a> <sup>[2912]</sup> that have access to the object. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights:</p> <ul style="list-style-type: none"> <li>▪ Inherited: Inherit the access rights settings of the parent object.</li> <li>▪ No access: Users in this user group cannot see or edit the object. The object neither shows up in lists nor in the device tree. <ul style="list-style-type: none"> <li>ⓘ There is one exception: If a user in this user group has access to a child object, the parent object is visible in the device tree but users in this user group cannot access it.</li> </ul> </li> <li>▪ Read access: Users in this group can see the object and view its monitoring results. They cannot edit any settings.</li> <li>▪ Write access: Users in this group can see the object, view its monitoring results, and edit its settings. They cannot edit its access rights settings.</li> <li>▪ Full access: Users in this group can see the object, view its monitoring results, edit its settings, and edit its access rights settings.</li> </ul> <p>To automatically set all child objects to inherit this object's access rights, select the Revert access rights of child objects to "inherited" option.</p> <p><span style="color: #0070C0;">■</span> For more information on access rights, see section <a href="#">Access Rights Management</a> <sup>[145]</sup>.</p>

- ❗ Click OK to save your settings. If you close the dialog without saving, all changes to the settings are lost.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?

- <https://kb.paessler.com/en/topic/89717>

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- <https://kb.paessler.com/en/topic/38083>

How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?


- <https://kb.paessler.com/en/topic/88462>

How do I obtain credentials and create custom roles for the Microsoft Azure sensors?

- <https://kb.paessler.com/en/topic/88625>

## 7.2.2 Add a Group




There are several ways to manually add a group:

- Select Devices | Add Group from the [main menu bar](#)<sup>[238]</sup>. A dialog appears that guides you through the process of adding a new group.
- Hover over  and select Add Group from the menu.
- Select Add Group from the [context menu](#)<sup>[229]</sup> of the probe or group to which you want to add the new group. This skips step 1 and leads you directly to [step 2](#)<sup>[316]</sup>.

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.


In this section:

- [Add a Group](#)<sup>[314]</sup>
- [Step 1: Select a Parent](#)<sup>[315]</sup>
- [Step 2: Define Group Settings](#)<sup>[316]</sup>
- [Basic Group Settings](#)<sup>[317]</sup>
- [Auto-Discovery Settings](#)<sup>[318]</sup>
- [Inherited Settings](#)<sup>[321]</sup>
- [Credentials for Windows Systems](#)<sup>[321]</sup>
- [Credentials for Linux/Solaris/macOS \(SSH/WBEM\) Systems](#)<sup>[323]</sup>
- [Credentials for VMware/XenServer](#)<sup>[327]</sup>
- [Credentials for SNMP Devices](#)<sup>[329]</sup>
- [Credentials for Database Management Systems](#)<sup>[334]</sup>
- [Credentials for AWS](#)<sup>[335]</sup>
- [Credentials for Script Sensors](#)<sup>[336]</sup>
- [Credentials for Cisco Meraki](#)<sup>[338]</sup>
- [Credentials for Dell EMC](#)<sup>[339]</sup>
- [Credentials for FortiGate](#)<sup>[340]</sup>
- [Credentials for HPE 3PAR](#)<sup>[340]</sup>
- [Credentials for HTTP](#)<sup>[342]</sup>
- [Credentials for Microsoft Azure](#)<sup>[344]</sup>
- [Credentials for MQTT](#)<sup>[346]</sup>
- [Credentials for NetApp](#)<sup>[349]</sup>
- [Credentials for OPC UA](#)<sup>[351]</sup>
- [Credentials for Soffico Orchestra](#)<sup>[354]</sup>
- [Credentials for Redfish](#)<sup>[356]</sup>

- [Credentials for REST API](#)  358
- [Credentials for Veeam](#)  359
- [Access Rights](#)  360

## Add a Group

The Add a Group dialog appears when you add a new group to a parent group. It only shows the settings that are required to create the group. Therefore, you do not see all settings in this dialog.

- ① You can change all settings on the Settings tab of the group later. For more information, see section [Group Settings](#)  526.



## Step 1: Select a Parent

**Add a Group** [Close]

### Select a Parent

Select a parent object for the group.

**PRTG Manual: Add a Group**

### Add a New Group

Organize your network devices in PRTG using **groups**. You can create as many groups and subgroups as you like.

If you want to automate the monitoring setup for a group of network devices, add an **auto-discovery group** to your group or probe. To do so, use the context menu of groups or probes or select **Devices | Add Auto-Discovery Group** from the main menu bar.

### Select a Probe or Group to Add the New Group to

Select a probe or group from the list. You can create new groups faster by right-clicking a probe or group in the device tree and selecting **Add Group** from the context menu.

Search... [Search Icon]

- Root
  - Local Probe
    - 1st group
      - MAIL
        - Group
      - ROUTER/SWITCHES
      - VMWARE
      - SNMP
        - Servers
      - DATABASES
      - MISC
        - CLOUD
      - Services
      - WINDOWS

[Cancel] [OK]

Add Group Assistant Step 1

Select the probe or group that you want to add the new group to. Click OK.

## Step 2: Define Group Settings

### Add a Group to Local Probe ✕

---

#### Define Group Settings

Specify credentials and access rights for your group, if necessary. All devices in this group will inherit these settings.

**PRTG Manual: Add a Group**

#### Add a New Group

Organize your network devices in PRTG using **groups**. You can create as many groups and subgroups as you like.

If you want to automate the monitoring setup for a group of network devices, add an **auto-discovery group** to your group or probe. To do so, use the context menu of groups or probes or select **Devices | Add Auto-Discovery Group** from the main menu bar.

#### Basic Group Settings

**Group Name** ⓘ

Group

**Tags** ⓘ

#### Auto-Discovery Settings

**Auto-Discovery Level** ⓘ

No auto-discovery (default)

Default auto-discovery (recommended)

Detailed auto-discovery

Auto-discovery with specific device templates

#### Credentials for Windows Systems

inherit from Local Probe (Domain or Computer Name: <empty>, User Name: ...)

Add Group Assistant Step 2

## Basic Group Settings

### Basic Group Settings

**Group Name** ⓘ

Group

---

**Tags** ⓘ

+

Basic Group Settings

Setting	Description
Group Name	<p>Enter a name to identify the group. By default, PRTG shows this name in the <a href="#">device tree</a><sup>[164]</sup>, as well as in <a href="#">alarms</a><sup>[202]</sup>, <a href="#">logs</a><sup>[210]</sup>, <a href="#">notifications</a><sup>[2735]</sup>, <a href="#">reports</a><sup>[2754]</sup>, <a href="#">maps</a><sup>[2776]</sup>, <a href="#">libraries</a><sup>[2738]</sup>, and <a href="#">tickets</a><sup>[213]</sup>.</p> <p>ⓘ If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Tags	<p>Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically <a href="#">inherited</a><sup>[138]</sup>.</p> <p>ⓘ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (&lt;&gt;).</p> <p>ⓘ For performance reasons, it can take some minutes until you can filter for new tags that you added.</p>

## Auto-Discovery

### Auto-Discovery Settings

**Auto-Discovery Level** ⓘ

- No auto-discovery (default)
- Default auto-discovery (recommended)
- Detailed auto-discovery
- Auto-discovery with specific device templates

Auto-Discovery Settings

Setting	Description
Auto-Discovery Level	<p>Select the level of detail for the <a href="#">auto-discovery</a><sup>[254]</sup>:</p> <ul style="list-style-type: none"> <li>▪ No auto-discovery: Select this option if you only want to manually create devices and sensors.</li> <li>▪ Standard auto-discovery (default): Create a set of standard sensors for standard monitoring. This option works fine for most installations.</li> <li>▪ Detailed auto-discovery: Create all standard sensors and additional sensors from detailed variants of device templates. As a result, you might get many sensors. This option is suitable for small network segments and whenever you want to monitor the maximum number of sensors available.</li> <li>▪ Auto-discovery with specific device templates: Customize the auto-discovery and select or combine standard, detailed, and custom device templates. Select one or more templates from the Device Templates list.</li> </ul> <p>ⓘ Auto-discoveries can be resource intensive. They are primarily intended for devices on the same network as your probes.</p>
Schedule	<p>Select when PRTG runs the auto-discovery:</p> <ul style="list-style-type: none"> <li>▪ Once (default): Run the auto-discovery only once. PRTG adds new devices and sensors once. If you select this option, you must manually <a href="#">start the auto-discovery</a><sup>[255]</sup>.</li> <li>▪ Hourly: Run the auto-discovery for new devices and sensors every 60 minutes. <ul style="list-style-type: none"> <li>ⓘ Use this option with caution. Frequent auto-discoveries might cause performance issues, in particular when PRTG scans large network segments every hour.</li> </ul> </li> <li>▪ Daily: Run the auto-discovery for new devices and sensors every 24 hours. The first auto-discovery runs immediately. All other discoveries start at the time that you define in the <a href="#">Monitoring</a><sup>[2875]</sup> settings, section Auto-Discovery.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Weekly: Run the auto-discovery for new devices and sensors every 7 days. The first auto-discovery runs immediately. All other discoveries start at the time that you define in the Monitoring settings, section Auto-Discovery.</li> </ul> <p><b>i</b> For performance reasons, PRTG sets Schedule to Once (default) on all devices that the scheduled auto-discovery creates.</p>
Device Templates	<p><b>This setting is only visible if you select</b> Auto-discovery with specific device templates <a href="#">above</a>.</p> <p>Select one or more device templates by enabling a check box in front of the template name. PRTG uses the device templates that you select for the auto-discovery on the device:</p> <ul style="list-style-type: none"> <li>▪ ADSL</li> <li>▪ Buffalo TeraStation NAS</li> <li>▪ Cisco ASA VPN</li> <li>▪ Cisco Device (Generic)</li> <li>▪ Dell EqualLogic</li> <li>▪ Dell MDi Disk</li> <li>▪ DNS Server</li> <li>▪ Environment Jakarta</li> <li>▪ Environment Poseidon</li> <li>▪ FTP Server</li> <li>▪ Generic Device (Ping Only)</li> <li>▪ Generic Device (SNMP Enabled)</li> <li>▪ Generic Device (SNMP Enabled, Detailed)</li> <li>▪ HTTP Web Server</li> <li>▪ Hyper-V Host Server</li> <li>▪ IPMI-enabled Device</li> <li>▪ Juniper NS Device</li> <li>▪ Linux/UNIX Device (SNMP or SSH Enabled)</li> <li>▪ Mail Server (Generic)</li> <li>▪ Mail Server (MS Exchange)</li> <li>▪ Microsoft SharePoint 2010</li> <li>▪ MQTT Round Trip</li> <li>▪ NAS LenovoEMC</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ NAS QNAP</li> <li>▪ NAS Synology</li> <li>▪ NetApp</li> <li>▪ NTP Server</li> <li>▪ OPC UA</li> <li>▪ Printer (Generic)</li> <li>▪ Printer (HP)</li> <li>▪ RDP Server</li> <li>▪ RMON-compatible Device</li> <li>▪ Server (Cisco UCS)</li> <li>▪ Server (Compaq/HP Agents)</li> <li>▪ Server (Dell)</li> <li>▪ Server (Fujitsu)</li> <li>▪ Server (IBM)</li> <li>▪ SNMP Rittal CMC III Hardware Status</li> <li>▪ SonicWall</li> <li>▪ SSL Security Check</li> <li>▪ Switch (Cisco Catalyst)</li> <li>▪ Switch (Cisco IOS Based)</li> <li>▪ Switch (HP Procurve)</li> <li>▪ UNIX/Linux Device</li> <li>▪ UPS Health (APC)</li> <li>▪ UPS Health (Generic)</li> <li>▪ UPS Health (Liebert)</li> <li>▪ VMware ESXi / vCenter Server</li> <li>▪ Web Server</li> <li>▪ Windows (Detailed via WMI)</li> <li>▪ Windows (via Remote PowerShell)</li> <li>▪ Windows (via WMI)</li> <li>▪ Windows IIS (via SNMP)</li> <li>▪ XenServer Hosts</li> <li>▪ XenServer Virtual Machines</li> </ul>

Setting	Description
	Once the auto-discovery is finished, PRTG creates a new <a href="#">ticket</a> <sup>[213]</sup> and lists the device templates that it used to create new sensors.

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#)<sup>[420]</sup> if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#)<sup>[136]</sup>.

## Credentials for Windows Systems

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

ⓘ The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">Active Directory Replication Errors</a></li> <li>▪ <a href="#">Event Log (Windows API)</a></li> <li>▪ <a href="#">Exchange Backup (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database DAG (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mail Queue (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mailbox (PowerShell)</a></li> <li>▪ <a href="#">Exchange Public Folder (PowerShell)</a></li> <li>▪ <a href="#">File</a></li> <li>▪ <a href="#">File Content</a></li> <li>▪ <a href="#">Folder</a></li> <li>▪ <a href="#">Hyper-V Cluster Shared Volume Disk Free</a></li> <li>▪ <a href="#">Hyper-V Host Server</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Windows MSMQ Queue Length</a></li> <li>▪ <a href="#">Windows Network Card</a></li> <li>▪ <a href="#">Windows Pagefile</a></li> <li>▪ <a href="#">Windows Physical Disk I/O</a></li> <li>▪ <a href="#">Windows Print Queue</a></li> <li>▪ <a href="#">Windows Process</a></li> <li>▪ <a href="#">Windows SMTP Service Received</a></li> <li>▪ <a href="#">Windows SMTP Service Sent</a></li> <li>▪ <a href="#">Windows System Uptime</a></li> <li>▪ <a href="#">Windows Updates Status (PowerShell)</a></li> <li>▪ <a href="#">WMI Battery</a></li> <li>▪ <a href="#">WMI Custom</a></li> <li>▪ <a href="#">WMI Custom String</a></li> <li>▪ <a href="#">WMI Disk Health</a></li> <li>▪ <a href="#">WMI Event Log</a></li> <li>▪ <a href="#">WMI Exchange Server</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">WMI Memory</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2005 (Deprecated)</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2008</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2012</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2014</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2016</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2017</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2019</a></li> <li>▪ <a href="#">WMI Remote Ping</a></li> <li>▪ <a href="#">WMI Security Center</a></li> <li>▪ <a href="#">WMI Service</a></li> <li>▪ <a href="#">WMI Share</a></li> <li>▪ <a href="#">WMI SharePoint Process</a></li> <li>▪ <a href="#">WMI Storage Pool</a></li> </ul>
--	---	--

<ul style="list-style-type: none"><li>▪ <a href="#">Hyper-V Virtual Machine</a></li><li>▪ <a href="#">Hyper-V Virtual Network Adapter</a></li><li>▪ <a href="#">Hyper-V Virtual Storage Device</a></li><li>▪ <a href="#">PerfCounter Custom</a></li><li>▪ <a href="#">PerfCounter IIS Application Pool</a></li><li>▪ <a href="#">Share Disk Free</a></li><li>▪ <a href="#">Windows CPU Load</a></li><li>▪ <a href="#">Windows IIS Application</a></li></ul>	<ul style="list-style-type: none"><li>▪ <a href="#">WMI Exchange Transport Queue</a></li><li>▪ <a href="#">WMI File</a></li><li>▪ <a href="#">WMI Free Disk Space (Multi Disk)</a></li><li>▪ <a href="#">WMI HDD Health</a></li><li>▪ <a href="#">WMI Logical Disk I/O</a></li></ul>	<ul style="list-style-type: none"><li>▪ <a href="#">WMI Terminal Services (Windows 2008+)</a></li><li>▪ <a href="#">WMI Terminal Services (Windows XP/Vista/2003)</a></li><li>▪ <a href="#">WMI UTC Time</a></li><li>▪ <a href="#">WMI Vital System Data v2</a></li><li>▪ <a href="#">WMI Volume</a></li><li>▪ <a href="#">WSUS Statistics</a></li></ul>
---	--	--

## Credentials for Windows Systems



inherit from

Domain or Computer Name i

www.example.com

User Name i

johnqpublic

Password i

.....

Credentials for Windows Systems



Setting	Description
Domain or Computer Name	<p>Enter the domain or computer name of the user account with which you want to access the Windows system. PRTG uses this account for Windows Management Instrumentation (WMI) sensors and other Windows sensors.</p> <p>If you want to use a Windows local user account on the target device, enter the computer name. If you want to use a Windows domain user account (recommended), enter the domain name. PRTG automatically adds a prefix to use the NT LAN Manager (NTLM) protocol if you do not explicitly define it. Do not leave this field empty.</p>
User Name	Enter the user name for access to the Windows system. Usually, you use credentials with administrator rights.
Password	Enter the password for access to the Windows system. Usually, you use credentials with administrator rights.

## Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

Click  to interrupt the [inheritance](#) 136.

 The settings you define in this section apply to the following sensors:

- [SFTP Secure File Transfer Protocol](#)
- [SSH Disk Free](#)
- [SSH INodes Free](#)
- [SSH Load Average](#)
- [SSH Meminfo](#)
- [SSH Remote Ping](#)
- [SSH SAN Enclosure](#)
- [SSH SAN Logical Disk](#)
- [SSH SAN Physical Disk](#)
- [SSH SAN System Health](#)
- [SSH Script](#)
- [SSH Script Advanced](#)
- [VMware Host Hardware \(WBEM\)](#)

## Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

inherit from

User Name <sup>i</sup>

johnqpublic

Authentication Method <sup>i</sup>

- Password (default)
- Private key

Password <sup>i</sup>

.....

WBEM Protocol <sup>i</sup>

- HTTP
- HTTPS (default)

WBEM Port <sup>i</sup>

- Default
- Custom

SSH Port <sup>i</sup>









22



SSH Rights Elevation <sup>i</sup>

- Run the command as the connecting user (default)
- Run the command as a different user using 'sudo' (with password)
- Run the command as a different user using 'sudo' (without password)
- Run the command as a different user using 'su'

SSH Connection Mode <sup>i</sup>

- Default
- Compatibility mode (deprecated)

Setting	Description
User Name	Enter the user name for access to the Linux/Solaris/macOS system via Secure Shell (SSH) and Web-based Enterprise Management (WBEM). Usually, you use credentials with administrator rights.
Authentication Method	<p>Select the authentication method for the login:</p> <ul style="list-style-type: none"> <li>▪ Password (default): Provide the password for the login.</li> <li>▪ Private key: Provide an RSA private key for authentication.</li> </ul> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For more information, see section <a href="#">Monitoring via SSH</a><sup>[8007]</sup>.</p>
Password	<p><b>This setting is only visible if you select Password (default) above.</b></p> <p>Enter a password for access to the Linux/Solaris/macOS system via SSH and WBEM. Usually, you use credentials with administrator rights.</p>
Private Key	<p><b>This setting is only visible if you select Private key above.</b></p> <p>Paste the entire RSA private key, including the <b>BEGIN</b> and <b>END</b> lines. Make sure that a corresponding public key exists on the target device.</p> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For more information, see section <a href="#">Monitoring via SSH</a><sup>[8007]</sup>.</p> <p> If you do not insert a private key for the first time but if you want to <b>change</b> the private key, you need to <a href="#">restart the PRTG core server service</a><sup>[2919]</sup> for the private key change to take effect.</p>
WBEM Protocol	<p>Select the protocol that you want to use for the connection to the system via WBEM:</p> <ul style="list-style-type: none"> <li>▪ HTTP: Use an unsecure connection for WBEM.</li> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection for WBEM.</li> </ul> <p> This setting is only relevant if you use WBEM sensors.</p>
WBEM Port	Select if you want to use one of the default ports for the connection to the system via WBEM or if you want to set a custom port:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Default: Use one of the default ports. The default port for unsecure connections is <a href="#">5988</a> and the default port for secure connections is <a href="#">5989</a>.</li> <li>▪ Custom: Use a custom port.</li> </ul> <p> This setting is only relevant if you use WBEM sensors.</p>
Custom WBEM Port	<p>This setting is only visible if you select Custom above.</p> <p>Enter a custom WBEM port. Enter an integer.</p>
SSH Port	<p>Enter the port for SSH connections. Enter an integer. The default port is <a href="#">22</a>.</p> <p> By default, PRTG automatically uses this setting for all <a href="#">SSH sensors</a> <small>3232</small> unless you define a different port number in the sensor settings.</p>
SSH Rights Elevation	<p>Select the rights that you want to use to run the command on the target system:</p> <ul style="list-style-type: none"> <li>▪ Run the command as the connecting user (default): Use the rights of the user who establishes the SSH connection.</li> <li>▪ Run the command as a different user using 'sudo' (with password): Use the rights of a different user with a password required for <a href="#">sudo</a> to run commands on the target system, for example, as a root user.</li> <li>▪ Run the command as a different user using 'sudo' (without password): Use the rights of a different user without a password required for <a href="#">sudo</a> to run commands on the target system, for example, as a root user.</li> <li>▪ Run the command as a different user using 'su': Use the rights of a different user with <a href="#">su</a> to run commands on the target system.</li> </ul>
Target System User Name	<p>This setting is only visible if you select an option that includes <a href="#">sudo</a> or <a href="#">su</a> above.</p> <p>Enter a user name to run the specified command on the target system as a different user than the root user. If you leave this field empty, you run the command as a root user. Make sure that you set the Linux password even if you use a public key or a private key for authentication. This is not necessary if the user is allowed to run the command without a password.</p>
Password	<p>This setting is only visible if you select an option that includes <a href="#">sudo</a> or <a href="#">su</a> with password above.</p> <p>Enter the password to run the <a href="#">sudo</a> command or the <a href="#">su</a> command.</p>

Setting	Description
SSH Connection Mode	<p>Select the connection mode that you want to use to <a href="#">access data with SSH sensors</a> <sup>3007</sup>:</p> <ul style="list-style-type: none"> <li>▪ Default: This is the default connection mode for SSH sensors. It provides the best performance and security.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default connection mode does not work on the target system. The compatibility mode is the connection mode that PRTG used in previous versions and it is deprecated.</li> </ul> <p><b>i</b> We strongly recommend that you use the default connection mode.</p> <p><b>i</b> You can also individually select the connection mode for each SSH sensor in the sensor settings.</p>

## Credentials for VMware/XenServer

Click  to interrupt the [inheritance](#) <sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

- [Citrix XenServer Host](#)
- [Citrix XenServer Virtual Machine](#)
- [VMware Datastore \(SOAP\)](#)
- [VMware Host Hardware \(WBEM\)](#)
- [VMware Host Hardware Status \(SOAP\)](#)
- [VMware Host Performance \(SOAP\)](#)
- [VMware Virtual Machine \(SOAP\)](#)

## Credentials for VMware/XenServer

inherit from

User Name i

johnqpublic

Password i

.....

VMware Protocol i

HTTPS (default)

HTTP

Credentials for VMw are/XenServer

Setting	Description
User Name	Enter the user name for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.
Password	Enter the password for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.  <span>i</span> Single sign-on (SSO) passwords for vSphere do not support special characters. For more information, see the VMware sensors sections.
VMware Protocol	Select the protocol for the connection to VMware ESXi, vCenter Server, or Citrix XenServer: <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
Session Handling	Select if you want to reuse a session for VMware sensors:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Reuse a session for multiple scans (default): Select this option if you want a VMware sensor to reuse a single session for multiple sensor scans to query data. With this option, the sensor does not need to log in and out for each sensor scan. We recommend that you use this option because it reduces network load and log entries on the target device. This can increase performance.</li> <li>▪ Create a new session for each scan: If you select this option, PRTG does not reuse a session and a VMware sensor has to log in and out for each sensor scan. This can decrease performance.</li> </ul>

## Credentials for SNMP Devices

Click  to interrupt the [inheritance](#) 136.

 The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">Cisco IP SLA</a></li> <li>▪ <a href="#">SNMP APC Hardware</a></li> <li>▪ <a href="#">SNMP Buffalo TS System Health</a></li> <li>▪ <a href="#">SNMP Cisco ADSL</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Connections</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Traffic</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Users</a></li> <li>▪ <a href="#">SNMP Cisco CBQoS</a></li> <li>▪ <a href="#">SNMP Cisco System Health</a></li> <li>▪ <a href="#">SNMP Cisco UCS Blade</a></li> <li>▪ <a href="#">SNMP Cisco UCS Chassis</a></li> <li>▪ <a href="#">SNMP Cisco UCS Physical Disk</a></li> <li>▪ <a href="#">SNMP Cisco UCS System Health</a></li> <li>▪ <a href="#">SNMP CPU Load</a></li> <li>▪ <a href="#">SNMP Custom</a></li> <li>▪ <a href="#">SNMP Custom Advanced</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">SNMP Fujitsu System Health v2</a></li> <li>▪ <a href="#">SNMP Hardware Status</a></li> <li>▪ <a href="#">SNMP HP LaserJet Hardware</a></li> <li>▪ <a href="#">SNMP HPE BladeSystem Blade</a></li> <li>▪ <a href="#">SNMP HPE BladeSystem Enclosure Health</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Logical Disk</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Memory Controller</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Network Interface</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Physical Disk</a></li> <li>▪ <a href="#">SNMP HPE ProLiant System Health</a></li> <li>▪ <a href="#">SNMP IBM System X Logical Disk</a></li> <li>▪ <a href="#">SNMP IBM System X Physical Disk</a></li> <li>▪ <a href="#">SNMP IBM System X Physical Memory</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">SNMP NetApp Enclosure</a></li> <li>▪ <a href="#">SNMP NetApp I/O</a></li> <li>▪ <a href="#">SNMP NetApp License</a></li> <li>▪ <a href="#">SNMP NetApp Logical Unit</a></li> <li>▪ <a href="#">SNMP NetApp Network Interface</a></li> <li>▪ <a href="#">SNMP NetApp System Health</a></li> <li>▪ <a href="#">SNMP Nutanix Cluster Health</a></li> <li>▪ <a href="#">SNMP Nutanix Hypervisor</a></li> <li>▪ <a href="#">SNMP Poseidon Environment</a></li> <li>▪ <a href="#">SNMP Printer</a></li> <li>▪ <a href="#">SNMP QNAP Logical Disk</a></li> <li>▪ <a href="#">SNMP QNAP Physical Disk</a></li> <li>▪ <a href="#">SNMP QNAP System Health</a></li> <li>▪ <a href="#">SNMP Rittal CMC III Hardware Status</a></li> <li>▪ <a href="#">SNMP RMON</a></li> <li>▪ <a href="#">SNMP SonicWall System Health</a></li> <li>▪ <a href="#">SNMP SonicWall VPN Traffic</a></li> </ul>
---	---	--

<ul style="list-style-type: none"><li>▪ <a href="#">SNMP Custom String</a></li><li>▪ <a href="#">SNMP Custom String Lookup</a></li><li>▪ <a href="#">SNMP Custom Table</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Logical Disk</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Member Health</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Physical Disk</a></li><li>▪ <a href="#">SNMP Dell Hardware</a></li><li>▪ <a href="#">SNMP Dell PowerEdge Physical Disk</a></li><li>▪ <a href="#">SNMP Dell PowerEdge System Health</a></li><li>▪ <a href="#">SNMP Disk Free</a></li></ul>	<ul style="list-style-type: none"><li>▪ <a href="#">SNMP IBM System X System Health</a></li><li>▪ <a href="#">SNMP interSeptor Pro Environment</a></li><li>▪ <a href="#">SNMP Juniper NS System Health</a></li><li>▪ <a href="#">SNMP LenovoEMC Physical Disk</a></li><li>▪ <a href="#">SNMP LenovoEMC System Health</a></li><li>▪ <a href="#">SNMP Library</a></li><li>▪ <a href="#">SNMP Linux Disk Free</a></li><li>▪ <a href="#">SNMP Linux Load Average</a></li><li>▪ <a href="#">SNMP Linux Meminfo</a></li><li>▪ <a href="#">SNMP Linux Physical Disk</a></li><li>▪ <a href="#">SNMP Memory</a></li><li>▪ <a href="#">SNMP NetApp Disk Free</a></li></ul>	<ul style="list-style-type: none"><li>▪ <a href="#">SNMP Synology Logical Disk</a></li><li>▪ <a href="#">SNMP Synology Physical Disk</a></li><li>▪ <a href="#">SNMP Synology System Health</a></li><li>▪ <a href="#">SNMP System Uptime</a></li><li>▪ <a href="#">SNMP Traffic</a></li><li>▪ <a href="#">SNMP Trap Receiver</a></li><li>▪ <a href="#">SNMP Windows Service</a></li></ul>
--	--	--



## Credentials for SNMP Devices

inherit from

**SNMP Version** ⓘ

SNMP v1

SNMP v2c (default)

SNMP v3

**Community String** ⓘ

public

**SNMP Port** ⓘ

161





**Timeout (Sec.)** ⓘ

5

Credentials for SNMP Devices

Setting	Description
SNMP Version	<p>Select the Simple Network Management Protocol (SNMP) version for the connection to the target SNMP device:</p> <ul style="list-style-type: none"> <li>SNMP v1: Use SNMP v1 for the connection. SNMP v1 only offers clear-text data transmission. <ul style="list-style-type: none"> <li>ⓘ SNMP v1 does not support 64-bit counters. This might result in invalid data when you monitor traffic via SNMP.</li> </ul> </li> <li>SNMP v2c (default): Use SNMP v2c for the connection. SNMP v2c also only offers clear-text data transmission but it supports 64-bit counters.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ SNMP v3: Use SNMP v3 for the connection. SNMP v3 provides secure authentication and data encryption.</li> <li>ⓘ SNMP v3 has performance limitations because of the use of encryption. The main limiting factor is CPU power. Also keep in mind that SNMP v3, unlike SNMP v1 and v2c, does not scale with more CPU power. Because of this limitation, PRTG can only handle a limited number of requests per second so that you can use only a limited number of sensors using SNMP v3. If you see an increase in <a href="#">Interval Delay</a> or <a href="#">Open Requests</a> with the <a href="#">Probe Health</a> sensor, distribute the load over <a href="#">multiple probes</a> <small>[3198]</small>. SNMP v1 and SNMP v2c do not have this limitation.</li> </ul>
Community String	<p><a href="#">This setting is only visible if you select SNMP v1 or SNMP v2c (default) above.</a></p> <p>Enter the community string of your device. This is like a clear-text password for simple authentication.</p> <p>ⓘ We recommend that you use the default value.</p>
Authentication Method	<p><a href="#">This setting is only visible if you select SNMP v3 above.</a></p> <p>Select the authentication method:</p> <ul style="list-style-type: none"> <li>▪ MD5 (default): Use message-digest algorithm 5 (MD5) for authentication.</li> <li>▪ SHA: Use Secure Hash Algorithm (SHA) for authentication.</li> <li>▪ SHA-224: Use SHA-224 for authentication.</li> <li>▪ SHA-256: Use SHA-256 for authentication.</li> <li>▪ SHA-384: Use SHA-384 for authentication.</li> <li>▪ SHA-512: Use SHA-512 for authentication.</li> </ul> <p>ⓘ If you do not want to use authentication but you need SNMP v3, for example, because your device requires <a href="#">context</a>, you can leave the Password field empty. In this case, PRTG uses <a href="#">SNMP_SEC_LEVEL_NOAUTH</a> and it entirely deactivates authentication.</p> <p>ⓘ The authentication method that you select must match the authentication method of your device.</p>
User Name	<p><a href="#">This setting is only visible if you select SNMP v3 above.</a></p> <p>Enter the user name for access to the target SNMP device.</p> <p>ⓘ The user name that you enter must match the user name of your device.</p>

Setting	Description
Password	<p><a href="#">This setting is only visible if you select SNMP v3 above.</a></p> <p>Enter the password for access to the target SNMP device.</p> <p> The password that you enter must match the password of your device.</p>
Encryption Type	<p><a href="#">This setting is only visible if you select SNMP v3 above.</a></p> <p>Select an encryption type:</p> <ul style="list-style-type: none"> <li>▪ DES (default): Use Data Encryption Standard (DES) as the encryption algorithm.</li> <li>▪ AES: Use Advanced Encryption Standard (AES) as the encryption algorithm.</li> <li>▪ AES-192: Use AES-192 as the encryption algorithm.</li> <li>▪ AES-256: Use AES-256 as the encryption algorithm.</li> </ul> <p> The encryption type that you select must match the encryption type of your device.</p>
Encryption Key	<p><a href="#">This setting is only visible if you select SNMP v3 above.</a></p> <p>Enter an encryption key. If you provide a key, PRTG encrypts SNMP data packets with the encryption algorithm that you selected above. Enter a string or leave the field empty.</p> <p> The encryption key that you enter must match the encryption key of your device. If the encryption keys do not match, you do not get an error message.</p>
Context Name	<p><a href="#">This setting is only visible if you select SNMP v3 above.</a></p> <p>Enter a context name only if the configuration of the device requires it. <b>Context</b> is a collection of management information that is accessible by an SNMP device. Enter a string.</p>
SNMP Port	<p>Enter the port for the connection to the SNMP target device. Enter an integer. The default port is <b>161</b>.</p> <p> We recommend that you use the default value.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).</p>


## Credentials for Database Management Systems


Click  to interrupt the [inheritance](#) .

 The settings you define in this section apply to the following sensors:

- [ADO SQL v2](#)
- [Microsoft SQL v2](#)
- [MySQL v2](#)
- [Oracle SQL v2](#)
- [PostgreSQL](#)


### Credentials for Database Management Systems

 inherit from

**Port** 


Default

Custom port for all database sensors

**Authentication Method** 

Windows authentication with impersonation (default)



SQL server authentication

**Timeout (Sec.)** 

60

Credentials for Database Management Systems

Setting	Description
Port	Select the port that PRTG uses for connections to the monitored databases:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Default: PRTG automatically determines the type of the database and uses the corresponding default port to connect. PRTG uses the following default ports: <ul style="list-style-type: none"> <li>▫ Microsoft SQL: <a href="#">1433</a></li> <li>▫ MySQL: <a href="#">3306</a></li> <li>▫ Oracle SQL: <a href="#">1521</a></li> <li>▫ PostgreSQL: <a href="#">5432</a></li> </ul> </li> <li>▪ Custom port for all database sensors: Select this option if your database management systems do not use the default ports. Enter a custom port for database connections below.</li> </ul>
Custom Port	<p>Enter a custom port for database connections. Enter an integer.</p> <p> PRTG uses this custom port for <a href="#">all</a> database sensors and for connections to <a href="#">all</a> your databases.</p>
Authentication Method	<p>Select the authentication method for the connection to the Structured Query Language (SQL) database:</p> <ul style="list-style-type: none"> <li>▪ Windows authentication with impersonation (default): PRTG uses the Windows credentials that you define in settings that are higher in the <a href="#">object hierarchy</a><sup>[132]</sup> for the database connection. <ul style="list-style-type: none"> <li> The user whose credentials PRTG uses needs to have permission to log in to the probe system with a database sensor. This is necessary for the impersonation.</li> </ul> </li> <li>▪ SQL server authentication: Use explicit credentials for database connections. Enter a user name and password below.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select SQL server authentication above.</a></p> <p>Enter the user name for the database connection.</p>
Password	<p><a href="#">This setting is only visible if you select SQL server authentication above.</a></p> <p>Enter the password for the database connection.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <a href="#">900</a> seconds (15 minutes).</p>

## Credentials for AWS

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:

- [AWS Alarm v2](#)
- [AWS Cost](#)
- [AWS EBS v2](#)
- [AWS EC2 v2](#)
- [AWS ELB v2](#)
- [AWS RDS v2](#)

■ For more information about the permissions that are necessary to query the AWS API, see the Knowledge Base: [How do I set permissions for the Amazon Web Services \(AWS\) API key to use certain sensors in PRTG?](#)

## Credentials for AWS

inherit from

**Access Key** ⓘ

---

**Secret Key** ⓘ

---

Credentials for AWS

Setting	Description
Access Key	Enter the Amazon Web Services (AWS) access key.
Secret Key	Enter the AWS secret key.

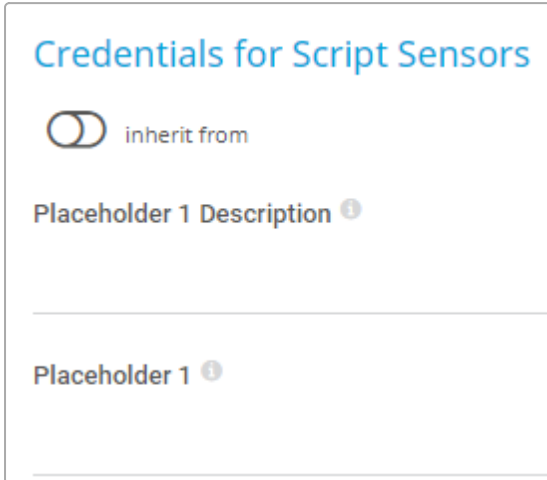
### Credentials for Script Sensors

Click  to interrupt the [inheritance](#) <sup>136</sup>.

ⓘ The settings you define in this section apply to the following sensors:

- [EXE/Script](#)
- [EXE/Script Advanced](#)
- [Python Script Advanced](#)

- [Script v2](#)
- [SSH Script](#)
- [SSH Script Advanced](#)



Credentials for Script Sensors

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder1</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder2</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder3</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.

Setting	Description
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder4</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder5</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.


### Credentials for Cisco Meraki


Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:


- [Cisco Meraki License](#)
- [Cisco Meraki Network Health](#)

## Credentials for Cisco Meraki


 inherit from

API Key  .....

---

Meraki Dashboard API Endpoint  [api.meraki.com](https://api.meraki.com)

Credentials for Cisco Meraki

Setting	Description
API Key	Enter an API key that the sensor uses for authentication against the Cisco Meraki Dashboard API.
Meraki Dashboard API Endpoint	Enter the endpoint for the Cisco Meraki Dashboard API. The default <a href="https://api.meraki.com">api.meraki.com</a> should be valid for most use cases.  See the Cisco Meraki Dashboard API documentation for other possible choices.




## Credentials for Dell EMC


Click  to interrupt the [inheritance](#) <sup>136</sup>.


 The settings you define in this section apply to the following sensors:


- [Dell EMC Unity Enclosure Health v2](#)
- [Dell EMC Unity File System v2](#)
- [Dell EMC Unity Storage Capacity v2](#)
- [Dell EMC Unity Storage LUN v2](#)
- [Dell EMC Unity Storage Pool v2](#)
- [Dell EMC Unity VMware Datastore v2](#)

### Credentials for Dell EMC

 inherit from

**User Name** 

**Password** 

**Port** 

Credentials for Dell EMC

Setting	Description
User Name	Enter the user name for access to the Dell EMC system.

Setting	Description
Password	Enter the password for access to the Dell EMC system.
Port	Enter the port for the connection to the Dell EMC system. The default port for secure connections is <a href="#">443</a> .


### Credentials for FortiGate


Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:


- [FortiGate System Statistics](#)
- [FortiGate VPN Overview](#)

### Credentials for FortiGate

 inherit from

API Token 

●●●●●●●●

Port 

443

Credentials for FortiGate

Setting	Description
API Token	Enter the API token for access to the FortiGate system.
Port	Enter the port for the connection to the FortiGate system. The default port for secure connections is <a href="#">443</a> .

### Credentials for HPE 3PAR

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [HPE 3PAR Common Provisioning Group](#)

- [HPE 3PAR Drive Enclosure](#)
- [HPE 3PAR Virtual Volume](#)

## Credentials for HPE 3PAR

inherit from

User Name <sup>i</sup>

johnqpulic

Password <sup>i</sup>

●●●●●●●●●●●●●●●●

Protocol <sup>i</sup>

HTTPS (default)

HTTP


WSAPI Port <sup>i</sup>

8080

SSH Port <sup>i</sup>

22

Credentials for HPE 3PAR

Setting	Description
User Name	Enter the user name for access to the HPE 3PAR system.
Password	Enter the password for access to the HPE 3PAR system.
Protocol	<p>Select the protocol that you want to use for the connection to the HPE 3PAR system:</p> <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
WSAPI Port	<p>Enter the Web Services API (WSAPI) port for the connection to the HPE 3PAR system. The default port for secure connections is <b>8080</b> and the default port for unsecure connections is <b>8008</b>.</p> <p> For more information, see the Knowledge Base: <a href="#">Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?</a></p>
SSH Port	Enter the SSH port for the connection to the HPE 3PAR system. The default port for secure connections is <b>22</b> .

## Credentials for HTTP

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensor:

- [HTTP v2](#)

### Credentials for HTTP

inherit from

**Authentication Method** ⓘ

None (default)

Basic authentication

Bearer authentication

**Placeholder 1 Description** ⓘ

---

**Placeholder 1** ⓘ

---

Credentials for HTTP

Setting	Description
Authentication Method	<p>Select the authentication method for access to the server:</p> <ul style="list-style-type: none"> <li>▪ None (default): Use no authentication.</li> <li>▪ Basic authentication: Use basic authentication.</li> <li>▪ Bearer authentication: Use an OAuth2 bearer token.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter the user name for access to the server.</p>
Password	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter the password for access to the server.</p>
Bearer Token	<p><a href="#">This setting is only visible if you select Bearer authentication above.</a></p> <p>Enter a bearer token for access to the server.</p>

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder1</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder2</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder3</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder4</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder5</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.

## Credentials for Microsoft Azure

Click  to interrupt the [inheritance](#)<sup>136</sup>.



 The settings you define in this section apply to the following sensors:

- [Microsoft Azure SQL Database](#)
- [Microsoft Azure Storage Account](#)
- [Microsoft Azure Subscription Cost](#)
- [Microsoft Azure Virtual Machine](#)

The sensors use the credentials to authenticate with Microsoft Entra ID.

■ For more information about the credentials and permissions that are necessary use the Microsoft Azure sensors, see the Knowledge Base: [How do I obtain credentials and create custom roles for the Microsoft Azure sensors?](#)

### Credentials for Microsoft Azure

 inherit from  Local Probe

**Tenant ID** ⓘ

---

**Client ID** ⓘ

---


**Client Secret** ⓘ

---

**Subscription ID** ⓘ

---

**Microsoft Azure Management Endpoint** ⓘ

management.azure.com 

Credentials for Microsoft Azure

Setting	Description
Tenant ID	Enter the Microsoft Entra tenant ID.  A tenant ID must be a 32-digit sequence in hexadecimal notation.
Client ID	Enter the Microsoft Entra client ID.

Setting	Description
Client Secret	Enter the Microsoft Entra client secret.
Subscription ID	Enter the Microsoft Entra subscription ID.

## Credentials for MQTT

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:

- [MQTT Round Trip](#)
- [MQTT Statistics](#)
- [MQTT Subscribe Custom](#)



## Credentials for MQTT

inherit from

### Authentication Method i

- None (default)
- User name and password

### Port i

1883


### Transport-Level Security i

- Do not use transport-level security (default)
- Use transport-level security

Credentials for MQTT

Setting	Description
Authentication Method	<p>Select if you want to connect without credentials or define credentials for access to the MQTT broker:</p> <ul style="list-style-type: none"> <li>▪ None (default): Connect without credentials.</li> <li>▪ User name and password: Define credentials for the connection.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select User name and password above.</a></p> <p>Enter the user name for access to the Message Queue Telemetry Transport (MQTT) broker.</p>

Setting	Description
Password	<p>This setting is only visible if you select <a href="#">User name and password above</a>.</p> <p>Enter the password for access to the MQTT broker.</p>
Port	<p>Enter the port for the connection to the MQTT broker. The default port for secure connections is <b>8883</b> and the default port for unsecure connections is <b>1883</b>.</p>
Transport-Level Security	<p>Select if you want to use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection:</p> <ul style="list-style-type: none"> <li>▪ Do not use transport-level security (default): Establish the connection without connection security.</li> <li>▪ Use transport-level security: Establish the connection with the strongest SSL/TLS method that the target device provides.</li> </ul>
Server Authentication	<p>This setting is only visible if you select <a href="#">Use transport-level security above</a>.</p> <p>Select if you want to use a certificate for server authentication:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not use a certificate for server authentication.</li> <li>▪ Enable: Use a certificate for server authentication.</li> </ul>
CA Certificate	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Paste the certificate authority (CA) certificate for the verification of the MQTT broker.</p> <p> The certificate must be in Privacy-Enhanced Mail (PEM) format.</p>
Client Authentication	<p>This setting is only visible if you select <a href="#">Use transport-level security above</a>.</p> <p>Select if you want to use a certificate for client authentication:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not use a certificate for client authentication.</li> <li>▪ Enable: Use a certificate for client authentication.</li> </ul>
Client Certificate	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Paste the certificate that you created for authenticating the sensor against the MQTT broker.</p> <p> The certificate must be in PEM format.</p>
Client Key	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Enter the client key for access to the MQTT broker.</p>

Setting	Description
	 The client key must be in PEM format and it must be encrypted using the Client Key Password.
Client Key Password	<p>This setting is only visible if you select Enable above.</p> <p>Enter the password for the client key.</p>

## Credentials for NetApp

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [NetApp Aggregate v2](#)
- [NetApp I/O v2](#)
- [NetApp LIF v2](#)
- [NetApp LUN v2](#)
- [NetApp NIC v2](#)
- [NetApp Physical Disk v2](#)
- [NetApp SnapMirror v2](#)
- [NetApp System Health v2](#)
- [NetApp Volume v2](#)

The sensors use the credentials for access to the ONTAP System Manager.

## Credentials for NetApp

inherit from Network-01f

**User Name** ⓘ  
johnqpublic

---

**Password** ⓘ  
.....

---

**Port** ⓘ  
443

---

**Protocol** ⓘ

HTTPS (default)

HTTP

Credentials for NetApp

Setting	Description
User Name	Enter a user name for access to the ONTAP System Manager.
Password	Enter the password for access to the ONTAP System Manager.
Port	Enter the port for the connection to the ONTAP System Manager. The default port for secure connections is <a href="#">443</a> .

Setting	Description
Protocol	Select the protocol that you want to use for the connection to the ONTAP System Manager: <ul style="list-style-type: none"><li>▪ HTTPS (default): Use HTTPS for the connection.</li><li>▪ HTTP: Use HTTP for the connection.</li></ul>

## Credentials for OPC UA

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [Beckhoff IPC System Health](#)
- [OPC UA Certificate](#)
- [OPC UA Custom](#)
- [OPC UA Server Status](#)

## Credentials for OPC UA

inherit from

Port <sup>i</sup>

4840

Server Path <sup>i</sup>

Security Mode <sup>i</sup>

None (default)

Sign

Sign & Encrypt



Authentication Method <sup>i</sup>

Anonymous (default)

User name and password

Credentials for OPC UA

Setting	Description
Port	Enter the port for the connection to the OPC Unified Architecture (OPC UA) server. The default port for secure connections is <a href="#">4840</a> .
Server Path	Enter the path of the OPC UA server endpoint if you run more than one server under the same IP address or DNS name.
Security Mode	Select if you want to use encryption: <ul style="list-style-type: none"> <li>▪ None (default): Do not use encryption.</li> <li>▪ Sign: Sign messages between the sensor and the OPC UA server.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Sign &amp; Encrypt: Sign and encrypt messages between the sensor and the OPC UA server.</li> </ul>
Security Policy	<p><a href="#">This setting is only visible if you select Sign or Sign &amp; Encrypt above.</a></p> <p>Select if you want to use a security policy and define which policy you want to use:</p> <ul style="list-style-type: none"> <li>▪ None (default): Do not use a security policy.</li> <li>▪ Basic256Sha256: Use the Basic256Sha256 security policy.</li> <li>▪ Basic256: Use the Basic256 security policy.</li> </ul>
Client Certificate	<p><a href="#">This setting is only visible if you select Sign or Sign &amp; Encrypt above.</a></p> <p>Enter the certificate that you created for authenticating the sensor against the OPC UA server.</p> <p> The certificate must meet the following requirements:</p> <ul style="list-style-type: none"> <li>▪ The key size must be 2048-bit or 4096-bit.</li> <li>▪ The secure hash algorithm must be <a href="#">SHA256</a>.</li> <li>▪ DataEncipherment must be part of the KeyUsage certificate extension.</li> <li>▪ A uniform resource indicator (URI) must be set in subjectAltName.</li> <li>▪ The certificate must be in Privacy-Enhanced Mail (PEM) format.</li> </ul>
Client Key	<p><a href="#">This setting is only visible if you select Sign or Sign &amp; Encrypt above.</a></p> <p>Enter the client key for access to the OPC UA server.</p> <p> The client key must be in PEM format and it must be encrypted using the Client Key Password.</p>
Client Key Password	<p><a href="#">This setting is only visible if you select Sign or Sign &amp; Encrypt above.</a></p> <p>Enter the password for the client key.</p>
Authentication Method	<p>Select if you want to connect without credentials or define credentials for access to the OPC UA server:</p> <ul style="list-style-type: none"> <li>▪ Anonymous (default): Connect without credentials.</li> <li>▪ User name and password: Define credentials for the connection.</li> </ul>

Setting	Description
	<p><b>i</b> Most OPC UA servers do not support User name and password authentication without a client certificate. To use User name and password authentication, select Sign or Sign &amp; Encrypt under Security Mode and Basic256Sha256 or Basic256 under Security Policy and enter the Client Certificate, Client Key, and Client Key Password that you want to use.</p> <p><b>i</b> If you select None (default) under Security Mode and use User name and password authentication, PRTG sends the unencrypted password to the OPC UA server.</p>
User Name	<p>This setting is only visible if you select User name and password <a href="#">above</a>.</p> <p>Enter the user name for access to the OPC UA server.</p>
Password	<p>This setting is only visible if you select User name and password <a href="#">above</a>.</p> <p>Enter the password for access to the OPC UA server.</p>

### Credentials for Soffico Orchestra

Click  to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensor:

- [Soffico Orchestra Channel Health](#)
- [Soffico Orchestra Scenario](#)



## Credentials for Soffico Orchestra

inherit from

### Authentication Method i

- None (default)  
 User name and password

### Timeout (Sec.) i

60

### Port i

8443

### Protocol i

- HTTPS (default)  
 HTTP

Credentials for Soffico Orchestra

Setting	Description
Authentication Method	Select if you want to connect without credentials or define credentials for access to the Orchestra platform: <ul style="list-style-type: none"> <li>None (default): Connect without credentials.</li> <li>User name and password: Define credentials for the connection.</li> </ul>
User Name	This setting is only visible if you select User name and password above. Enter the user name for access to the Orchestra platform.
Password	This setting is only visible if you select User name and password above.

Setting	Description
	Enter the password for access to the Orchestra platform.
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).
Port	Enter the port for the connection to the Orchestra platform. The default port for secure connections is <b>8443</b> and the default port for unsecure connections is <b>8019</b> .
Protocol	Select the protocol that you want to use for the connection to the Orchestra platform: <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>

### Credentials for Redfish

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [Redfish Power Supply](#)
- [Redfish System Health](#)
- [Redfish Virtual Disk](#)

### Credentials for Redfish

inherit from

**User Name** ⓘ  
johnqpublic

---

**Password** ⓘ  
●●●●●●●●

---

**Protocol** ⓘ

HTTPS (default)

HTTP

**Port** ⓘ  
443

Credentials for Redfish

Setting	Description
User Name	Enter the user name for access to the Redfish system.
Password	Enter the password for access to the Redfish system.
Protocol	<p>Select the protocol that you want to use for the connection to the Redfish system:</p> <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
Port	Enter the port for the connection to the Redfish system. The default port for secure connections is 443.

## Credentials for REST API


Click  to interrupt the [inheritance](#) <sup>136</sup>.

 The settings you define in this section apply to the following sensor:

- [REST Custom v2](#)

### Credentials for REST API

inherit from

**Authentication Method** 

None (default)

Basic authentication

Bearer authentication

Credentials for REST API

Setting	Description
Authentication Method	Select the authentication method for access to the Representational State Transfer (REST) application programming interface (API): <ul style="list-style-type: none"> <li>▪ None (default): Use no authentication.</li> <li>▪ Basic authentication: Use basic authentication.</li> <li>▪ Bearer authentication: Use an OAuth2 bearer token.</li> </ul>
User Name	<a href="#">This setting is only visible if you select Basic authentication above.</a> Enter the user name for access to the REST API.
Password	<a href="#">This setting is only visible if you select Basic authentication above.</a> Enter the password for access to the REST API.
Bearer Token	<a href="#">This setting is only visible if you select Bearer authentication above.</a> Enter a bearer token for access to the REST API.
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.

Setting	Description
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder1</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder2</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder3</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder4</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder5</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.


## Credentials for Veeam

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [Veeam Backup Job Status](#)
- [Veeam Backup Job Status Advanced](#)

## Credentials for Veeam

 inherit from

**User Name** i

johnqpublic

---

**Password** i

●●●●●●●●●●●●●●●●●●●●

---

**Port** i

9398

Credentials for Veeam

Setting	Description
User Name	Enter the user name for access to the Veeam Backup Enterprise Manager.
Password	Enter the password for access to the Veeam Backup Enterprise Manager.
Port	Enter the port for the connection to the Veeam Backup Enterprise Manager. The default port for secure connections is <a href="#">9398</a> .

### Access Rights

Click  to interrupt the [inheritance](#) <sup>136</sup>.

### Access Rights

inherit from


**User Group Access** ⓘ

User Group	Rights
PRTG Users Group	Write access
Read-only User Group	Read access
SSO User Group	Inherited (No access)

Revert access rights of child objects to "inherited"

Access Rights

Setting	Description
User Group Access	<p>Select the <a href="#">user groups</a> <sup>[2912]</sup> that have access to the object. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights:</p> <ul style="list-style-type: none"> <li>▪ Inherited: Inherit the access rights settings of the parent object.</li> <li>▪ No access: Users in this user group cannot see or edit the object. The object neither shows up in lists nor in the device tree. <ul style="list-style-type: none"> <li>ⓘ There is one exception: If a user in this user group has access to a child object, the parent object is visible in the device tree but users in this user group cannot access it.</li> </ul> </li> <li>▪ Read access: Users in this group can see the object and view its monitoring results. They cannot edit any settings.</li> <li>▪ Write access: Users in this group can see the object, view its monitoring results, and edit its settings. They cannot edit its access rights settings.</li> <li>▪ Full access: Users in this group can see the object, view its monitoring results, edit its settings, and edit its access rights settings.</li> </ul> <p>To automatically set all child objects to inherit this object's access rights, select the Revert access rights of child objects to "inherited" option.</p> <p><span style="color: #0070C0;">■</span> For more information on access rights, see section <a href="#">Access Rights Management</a> <sup>[145]</sup>.</p>

-  Click OK to save your settings. If you close the dialog without saving, all changes to the settings are lost.

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- <https://kb.paessler.com/en/topic/38083>

Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?

- <https://kb.paessler.com/en/topic/89717>

How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?

- <https://kb.paessler.com/en/topic/88462>


How do I obtain credentials and create custom roles for the Microsoft Azure sensors?

- <https://kb.paessler.com/en/topic/88625>



## 7.2.3 Add a Device





There are several ways to manually add a device:

- Select Devices | Add Device from the [main menu bar](#)<sup>[238]</sup>. A dialog appears that guides you through the process of adding a new device.
- Hover over  and select Add Device from the menu.
- Select Add Device from the [context menu](#)<sup>[229]</sup> of the group to which you want to add the new device. This skips step 1 and leads you directly to [step 2](#)<sup>[366]</sup>.

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

In this section:

- [Add a Device](#)<sup>[364]</sup>
- [Step 1: Select a Parent](#)<sup>[365]</sup>
- [Step 2: Define Device Settings](#)<sup>[366]</sup>
- [Basic Device Settings](#)<sup>[367]</sup>
- [Additional Device Information](#)<sup>[368]</sup>
- [Auto-Discovery Settings](#)<sup>[369]</sup>
- [Inherited Settings](#)<sup>[372]</sup>
- [Credentials for Windows Systems](#)<sup>[372]</sup>
- [Credentials for Linux/Solaris/macOS \(SSH/WBEM\) Systems](#)<sup>[375]</sup>
- [Credentials for VMware/XenServer](#)<sup>[379]</sup>
- [Credentials for SNMP Devices](#)<sup>[381]</sup>
- [Credentials for Database Management Systems](#)<sup>[386]</sup>
- [Credentials for AWS](#)<sup>[387]</sup>
- [Credentials for Script Sensors](#)<sup>[388]</sup>
- [Credentials for Cisco Meraki](#)<sup>[390]</sup>
- [Credentials for Dell EMC](#)<sup>[391]</sup>
- [Credentials for FortiGate](#)<sup>[392]</sup>
- [Credentials for HPE 3PAR](#)<sup>[392]</sup>
- [Credentials for HTTP](#)<sup>[394]</sup>
- [Credentials for Microsoft Azure](#)<sup>[396]</sup>
- [Credentials for MQTT](#)<sup>[398]</sup>
- [Credentials for NetApp](#)<sup>[400]</sup>
- [Credentials for OPC UA](#)<sup>[402]</sup>
- [Credentials for Soffico Orchestra](#)<sup>[405]</sup>

- [Credentials for Redfish](#)  407
- [Credentials for REST API](#)  409
- [Credentials for Veeam](#)  410
- [Access Rights](#)  411

## Add a Device

The Add a Device dialog appears when you add a new device to a group. It only shows the settings that are required to create the device. Therefore, you do not see all settings in this dialog.

- ⓘ You can change all settings on the Settings tab of the device later. For more information, see section [Device Settings](#)  597.

## Step 1: Select a Parent

**Add a Device** [X]

### Select a Parent

Select parent object for the device.

**PRTG Manual: Add a Device**

### Add a New Device

In PRTG, devices have one or more sensors. Devices are organized in groups. Devices and their sensors can use various inherited settings, such as scanning intervals or credentials.

### Select a Group from the List

Select a group from the list. You can create new devices faster by right-clicking a group in the device tree and selecting **Add Device** from the context menu.

Search... [Q]

- Root
  - Local Probe
    - 1st group
      - MAIL
        - Group
      - ROUTER/SWITCHES
      - VMWARE
      - SNMP
        - Servers
      - DATABASES
      - MISC
        - CLOUD
      - Services
      - WINDOWS

Cancel **OK**

Add Device Assistant Step 1

Select the group that you want to add the new device to. Click **OK**.

## Step 2: Define Device Settings

**Add Device to Group Local Probe**
✕

---

### Add a New Device

Define a device name and IP address, options for auto-discovery, and credential settings for Windows, Linux, VMware/XenServer, SNMP, and specific vendors, if necessary.

**PRTG Manual: Add a Device**

### Basic Device Settings

**Device Name** ⓘ

Device

---

**IP Version** ⓘ

IPv4 (default)

IPv6

**IPv4 Address/DNS Name** ⓘ

192.0.2.0

---

**Tags** ⓘ

+

---

### Additional Device Information

**Device Icon** ⓘ

<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Cancel
OK

Add Device Assistant Step 2

## Basic Device Settings

### Device Name and Address

**Device Name** ⓘ

Device

---

**IP Version** ⓘ

IPv4


IPv6

**IPv4 Address/DNS Name** ⓘ

192.0.2.0

---

**Tags** ⓘ



Basic Device Settings


Setting	Description
Device Name	<p>Enter a name to identify the device. By default, PRTG shows this name in the <a href="#">device tree</a> [164], as well as in <a href="#">alarms</a> [202], <a href="#">logs</a> [210], <a href="#">notifications</a> [2735], <a href="#">reports</a> [2754], <a href="#">maps</a> [2776], <a href="#">libraries</a> [2738], and <a href="#">tickets</a> [213].</p> <p>ⓘ If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
IP Version	<p>Select the IP protocol that PRTG uses to connect to the device:</p> <ul style="list-style-type: none"> <li>▪ IPv4: Use IP version 4 for all requests to the device.</li> <li>▪ IPv6: Use IP version 6 for all requests to the device.</li> </ul> <p>ⓘ The setting is valid for all sensors that you create on the device.</p>
IPv4 Address/DNS Name	<p>This setting is only visible if you select IPv4 above.</p>

Setting	Description
	<p>Enter the IP address or Domain Name System (DNS) name for the device. Most sensors that you create on this device inherit this setting and try to connect to this address for monitoring.</p> <p><b>i</b> Some sensors have their own setting for the IP address/DNS name to which they connect.</p>
IPv6 Address/DNS Name	<p><b>This setting is only visible if you select IPv6 above.</b></p> <p>Enter the IP address or Domain Name System (DNS) name for the device. Most sensors that you create on this device inherit this setting and try to connect to this address for monitoring.</p> <p><b>i</b> Some sensors have their own setting for the IP address/DNS name to which they connect.</p>
Tags	<p>Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically <a href="#">inherited</a><sup>138</sup>.</p> <p><b>i</b> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (&lt;&gt;).</p> <p><b>i</b> For performance reasons, it can take some minutes until you can filter for new tags that you added.</p>

### Additional Device Information

#### Additional Device Information

Device Icon **i**



Additional Device Information

Setting	Description
Device Icon	Select a device icon. PRTG shows it in the device tree.

## Auto-Discovery Settings

### Auto-Discovery Settings

**Auto-Discovery Level** ⓘ

- No auto-discovery (default)
- Default auto-discovery (recommended)
- Detailed auto-discovery
- Auto-discovery with specific device templates

Auto-Discovery Settings

Setting	Description
Auto-Discovery Level	<p>Select the level of detail for the <a href="#">auto-discovery</a> [254]:</p> <ul style="list-style-type: none"> <li>▪ No auto-discovery: Select this option if you only want to manually create devices and sensors.</li> <li>▪ Standard auto-discovery (default): Create a set of standard sensors for standard monitoring. This option works fine for most installations.</li> <li>▪ Detailed auto-discovery: Create all standard sensors and additional sensors from detailed variants of device templates. As a result, you might get many sensors. This option is suitable for small network segments and whenever you want to monitor the maximum number of sensors available.</li> <li>▪ Auto-discovery with specific device templates: Customize the auto-discovery and select or combine standard, detailed, and custom device templates. Select one or more templates from the Device Templates list.</li> </ul> <p>ⓘ Auto-discoveries can be resource intensive. They are primarily intended for devices on the same network as your probes.</p>
Schedule	<p>Select when PRTG runs the auto-discovery:</p> <ul style="list-style-type: none"> <li>▪ Once (default): Run the auto-discovery only once. PRTG adds new devices and sensors once. If you select this option, you must manually <a href="#">start the auto-discovery</a> [255].</li> </ul>


Setting	Description
	<ul style="list-style-type: none"> <li>▪ Hourly: Run the auto-discovery for new devices and sensors every 60 minutes.  <span style="color: red;">❗</span> Use this option with caution. Frequent auto-discoveries might cause performance issues, in particular when PRTG scans large network segments every hour.</li> <li>▪ Daily: Run the auto-discovery for new devices and sensors every 24 hours. The first auto-discovery runs immediately. All other discoveries start at the time that you define in the <a href="#">Monitoring</a> settings, section Auto-Discovery.</li> <li>▪ Weekly: Run the auto-discovery for new devices and sensors every 7 days. The first auto-discovery runs immediately. All other discoveries start at the time that you define in the Monitoring settings, section Auto-Discovery.</li> </ul> <p><span style="color: red;">❗</span> For performance reasons, PRTG sets Schedule to Once (default) on all devices that the scheduled auto-discovery creates.</p>
<p>Device Templates</p>	<p><span style="color: blue;">This setting is only visible if you select</span> Auto-discovery with specific device templates <a href="#">above</a>.</p> <p>Select one or more device templates by enabling a check box in front of the template name. PRTG uses the device templates that you select for the auto-discovery on the device:</p> <ul style="list-style-type: none"> <li>▪ ADSL</li> <li>▪ Buffalo TeraStation NAS</li> <li>▪ Cisco ASA VPN</li> <li>▪ Cisco Device (Generic)</li> <li>▪ Dell EqualLogic</li> <li>▪ Dell MDi Disk</li> <li>▪ DNS Server</li> <li>▪ Environment Jakarta</li> <li>▪ Environment Poseidon</li> <li>▪ FTP Server</li> <li>▪ Generic Device (Ping Only)</li> <li>▪ Generic Device (SNMP Enabled)</li> <li>▪ Generic Device (SNMP Enabled, Detailed)</li> <li>▪ HTTP Web Server</li> <li>▪ Hyper-V Host Server</li> <li>▪ IPMI-enabled Device</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ Juniper NS Device</li> <li>▪ Linux/UNIX Device (SNMP or SSH Enabled)</li> <li>▪ Mail Server (Generic)</li> <li>▪ Mail Server (MS Exchange)</li> <li>▪ Microsoft SharePoint 2010</li> <li>▪ MQTT Round Trip</li> <li>▪ NAS LenovoEMC</li> <li>▪ NAS QNAP</li> <li>▪ NAS Synology</li> <li>▪ NetApp</li> <li>▪ NTP Server</li> <li>▪ OPC UA</li> <li>▪ Printer (Generic)</li> <li>▪ Printer (HP)</li> <li>▪ RDP Server</li> <li>▪ RMON-compatible Device</li> <li>▪ Server (Cisco UCS)</li> <li>▪ Server (Compaq/HP Agents)</li> <li>▪ Server (Dell)</li> <li>▪ Server (Fujitsu)</li> <li>▪ Server (IBM)</li> <li>▪ SNMP Rittal CMC III Hardware Status</li> <li>▪ SonicWall</li> <li>▪ SSL Security Check</li> <li>▪ Switch (Cisco Catalyst)</li> <li>▪ Switch (Cisco IOS Based)</li> <li>▪ Switch (HP Procurve)</li> <li>▪ UNIX/Linux Device</li> <li>▪ UPS Health (APC)</li> <li>▪ UPS Health (Generic)</li> <li>▪ UPS Health (Liebert)</li> <li>▪ VMware ESXi / vCenter Server</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Web Server</li> <li>▪ Windows (Detailed via WMI)</li> <li>▪ Windows (via Remote PowerShell)</li> <li>▪ Windows (via WMI)</li> <li>▪ Windows IIS (via SNMP)</li> <li>▪ XenServer Hosts</li> <li>▪ XenServer Virtual Machines</li> </ul> <p>Once the auto-discovery is finished, PRTG creates a new <a href="#">ticket</a> and lists the device templates that it used to create new sensors.</p>

### Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

### Credentials for Windows Systems


Click  to interrupt the [inheritance](#).

 The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">Active Directory Replication Errors</a></li> <li>▪ <a href="#">Event Log (Windows API)</a></li> <li>▪ <a href="#">Exchange Backup (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database DAG (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mail Queue (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mailbox (PowerShell)</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Windows MSMQ Queue Length</a></li> <li>▪ <a href="#">Windows Network Card</a></li> <li>▪ <a href="#">Windows Pagefile</a></li> <li>▪ <a href="#">Windows Physical Disk I/O</a></li> <li>▪ <a href="#">Windows Print Queue</a></li> <li>▪ <a href="#">Windows Process</a></li> <li>▪ <a href="#">Windows SMTP Service Received</a></li> <li>▪ <a href="#">Windows SMTP Service Sent</a></li> <li>▪ <a href="#">Windows System Uptime</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">WMI Memory</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2005 (Deprecated)</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2008</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2012</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2014</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2016</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2017</a></li> </ul>
---	---	---

<ul style="list-style-type: none"> <li>▪ <a href="#">Exchange Public Folder (PowerShell)</a></li> <li>▪ <a href="#">File</a></li> <li>▪ <a href="#">File Content</a></li> <li>▪ <a href="#">Folder</a></li> <li>▪ <a href="#">Hyper-V Cluster Shared Volume Disk Free</a></li> <li>▪ <a href="#">Hyper-V Host Server</a></li> <li>▪ <a href="#">Hyper-V Virtual Machine</a></li> <li>▪ <a href="#">Hyper-V Virtual Network Adapter</a></li> <li>▪ <a href="#">Hyper-V Virtual Storage Device</a></li> <li>▪ <a href="#">PerfCounter Custom</a></li> <li>▪ <a href="#">PerfCounter IIS Application Pool</a></li> <li>▪ <a href="#">Share Disk Free</a></li> <li>▪ <a href="#">Windows CPU Load</a></li> <li>▪ <a href="#">Windows IIS Application</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Windows Updates Status (PowerShell)</a></li> <li>▪ <a href="#">WMI Battery</a></li> <li>▪ <a href="#">WMI Custom</a></li> <li>▪ <a href="#">WMI Custom String</a></li> <li>▪ <a href="#">WMI Disk Health</a></li> <li>▪ <a href="#">WMI Event Log</a></li> <li>▪ <a href="#">WMI Exchange Server</a></li> <li>▪ <a href="#">WMI Exchange Transport Queue</a></li> <li>▪ <a href="#">WMI File</a></li> <li>▪ <a href="#">WMI Free Disk Space (Multi Disk)</a></li> <li>▪ <a href="#">WMI HDD Health</a></li> <li>▪ <a href="#">WMI Logical Disk I/O</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">WMI Microsoft SQL Server 2019</a></li> <li>▪ <a href="#">WMI Remote Ping</a></li> <li>▪ <a href="#">WMI Security Center</a></li> <li>▪ <a href="#">WMI Service</a></li> <li>▪ <a href="#">WMI Share</a></li> <li>▪ <a href="#">WMI SharePoint Process</a></li> <li>▪ <a href="#">WMI Storage Pool</a></li> <li>▪ <a href="#">WMI Terminal Services (Windows 2008+)</a></li> <li>▪ <a href="#">WMI Terminal Services (Windows XP/Vista/2003)</a></li> <li>▪ <a href="#">WMI UTC Time</a></li> <li>▪ <a href="#">WMI Vital System Data v2</a></li> <li>▪ <a href="#">WMI Volume</a></li> <li>▪ <a href="#">WSUS Statistics</a></li> </ul>
---	--	--

## Credentials for Windows Systems

 inherit from

Domain or Computer Name 

www.example.com

User Name 

johnqpublic

Password 

.....

Credentials for Windows Systems

Setting	Description
Domain or Computer Name	<p>Enter the domain or computer name of the user account with which you want to access the Windows system. PRTG uses this account for Windows Management Instrumentation (WMI) sensors and other Windows sensors.</p> <p>If you want to use a Windows local user account on the target device, enter the computer name. If you want to use a Windows domain user account (recommended), enter the domain name. PRTG automatically adds a prefix to use the NT LAN Manager (NTLM) protocol if you do not explicitly define it. Do not leave this field empty.</p>
User Name	<p>Enter the user name for access to the Windows system. Usually, you use credentials with administrator rights.</p>
Password	<p>Enter the password for access to the Windows system. Usually, you use credentials with administrator rights.</p>

## Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

Click  to interrupt the [inheritance](#) .

 The settings you define in this section apply to the following sensors:

- [SFTP Secure File Transfer Protocol](#)
- [SSH Disk Free](#)
- [SSH INodes Free](#)
- [SSH Load Average](#)
- [SSH Meminfo](#)
- [SSH Remote Ping](#)
- [SSH SAN Enclosure](#)
- [SSH SAN Logical Disk](#)
- [SSH SAN Physical Disk](#)
- [SSH SAN System Health](#)
- [SSH Script](#)
- [SSH Script Advanced](#)
- [VMware Host Hardware \(WBEM\)](#)

## Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

inherit from

User Name <sup>i</sup>

johnqpublic

Authentication Method <sup>i</sup>

- Password (default)
- Private key

Password <sup>i</sup>

.....

WBEM Protocol <sup>i</sup>

- HTTP
- HTTPS (default)

WBEM Port <sup>i</sup>

- Default
- Custom

SSH Port <sup>i</sup>









22



SSH Rights Elevation <sup>i</sup>

- Run the command as the connecting user (default)
- Run the command as a different user using 'sudo' (with password)
- Run the command as a different user using 'sudo' (without password)
- Run the command as a different user using 'su'

SSH Connection Mode <sup>i</sup>

- Default
- Compatibility mode (deprecated)

Setting	Description
User Name	Enter the user name for access to the Linux/Solaris/macOS system via Secure Shell (SSH) and Web-based Enterprise Management (WBEM). Usually, you use credentials with administrator rights.
Authentication Method	<p>Select the authentication method for the login:</p> <ul style="list-style-type: none"> <li>▪ Password (default): Provide the password for the login.</li> <li>▪ Private key: Provide an RSA private key for authentication.</li> </ul> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For more information, see section <a href="#">Monitoring via SSH</a><sup>[8007]</sup>.</p>
Password	<p><b>This setting is only visible if you select Password (default) above.</b></p> <p>Enter a password for access to the Linux/Solaris/macOS system via SSH and WBEM. Usually, you use credentials with administrator rights.</p>
Private Key	<p><b>This setting is only visible if you select Private key above.</b></p> <p>Paste the entire RSA private key, including the <b>BEGIN</b> and <b>END</b> lines. Make sure that a corresponding public key exists on the target device.</p> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For more information, see section <a href="#">Monitoring via SSH</a><sup>[8007]</sup>.</p> <p> If you do not insert a private key for the first time but if you want to <b>change</b> the private key, you need to <a href="#">restart the PRTG core server service</a><sup>[2919]</sup> for the private key change to take effect.</p>
WBEM Protocol	<p>Select the protocol that you want to use for the connection to the system via WBEM:</p> <ul style="list-style-type: none"> <li>▪ HTTP: Use an unsecure connection for WBEM.</li> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection for WBEM.</li> </ul> <p> This setting is only relevant if you use WBEM sensors.</p>
WBEM Port	Select if you want to use one of the default ports for the connection to the system via WBEM or if you want to set a custom port:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Default: Use one of the default ports. The default port for unsecure connections is <a href="#">5988</a> and the default port for secure connections is <a href="#">5989</a>.</li> <li>▪ Custom: Use a custom port.</li> </ul> <p> This setting is only relevant if you use WBEM sensors.</p>
Custom WBEM Port	<p>This setting is only visible if you select Custom above.</p> <p>Enter a custom WBEM port. Enter an integer.</p>
SSH Port	<p>Enter the port for SSH connections. Enter an integer. The default port is <a href="#">22</a>.</p> <p> By default, PRTG automatically uses this setting for all <a href="#">SSH sensors</a> <small>(3232)</small> unless you define a different port number in the sensor settings.</p>
SSH Rights Elevation	<p>Select the rights that you want to use to run the command on the target system:</p> <ul style="list-style-type: none"> <li>▪ Run the command as the connecting user (default): Use the rights of the user who establishes the SSH connection.</li> <li>▪ Run the command as a different user using 'sudo' (with password): Use the rights of a different user with a password required for <a href="#">sudo</a> to run commands on the target system, for example, as a root user.</li> <li>▪ Run the command as a different user using 'sudo' (without password): Use the rights of a different user without a password required for <a href="#">sudo</a> to run commands on the target system, for example, as a root user.</li> <li>▪ Run the command as a different user using 'su': Use the rights of a different user with <a href="#">su</a> to run commands on the target system.</li> </ul>
Target System User Name	<p>This setting is only visible if you select an option that includes <a href="#">sudo</a> or <a href="#">su</a> above.</p> <p>Enter a user name to run the specified command on the target system as a different user than the root user. If you leave this field empty, you run the command as a root user. Make sure that you set the Linux password even if you use a public key or a private key for authentication. This is not necessary if the user is allowed to run the command without a password.</p>
Password	<p>This setting is only visible if you select an option that includes <a href="#">sudo</a> or <a href="#">su</a> with password above.</p> <p>Enter the password to run the <a href="#">sudo</a> command or the <a href="#">su</a> command.</p>



Setting	Description
SSH Connection Mode	<p>Select the connection mode that you want to use to <a href="#">access data with SSH sensors</a> <sup>3007</sup>:</p> <ul style="list-style-type: none"> <li>▪ Default: This is the default connection mode for SSH sensors. It provides the best performance and security.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default connection mode does not work on the target system. The compatibility mode is the connection mode that PRTG used in previous versions and it is deprecated.</li> </ul> <p><b>i</b> We strongly recommend that you use the default connection mode.</p> <p><b>i</b> You can also individually select the connection mode for each SSH sensor in the sensor settings.</p>

### Credentials for VMware/XenServer

Click  to interrupt the [inheritance](#) <sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

- [Citrix XenServer Host](#)
- [Citrix XenServer Virtual Machine](#)
- [VMware Datastore \(SOAP\)](#)
- [VMware Host Hardware \(WBEM\)](#)
- [VMware Host Hardware Status \(SOAP\)](#)
- [VMware Host Performance \(SOAP\)](#)
- [VMware Virtual Machine \(SOAP\)](#)

## Credentials for VMware/XenServer

inherit from

User Name i

johnqpublic

Password i

.....

VMware Protocol i

HTTPS (default)

HTTP

Credentials for VMw are/XenServer

Setting	Description
User Name	Enter the user name for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.
Password	Enter the password for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.  <span>i</span> Single sign-on (SSO) passwords for vSphere do not support special characters. For more information, see the VMware sensors sections.
VMware Protocol	Select the protocol for the connection to VMware ESXi, vCenter Server, or Citrix XenServer: <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
Session Handling	Select if you want to reuse a session for VMware sensors:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Reuse a session for multiple scans (default): Select this option if you want a VMware sensor to reuse a single session for multiple sensor scans to query data. With this option, the sensor does not need to log in and out for each sensor scan. We recommend that you use this option because it reduces network load and log entries on the target device. This can increase performance.</li> <li>▪ Create a new session for each scan: If you select this option, PRTG does not reuse a session and a VMware sensor has to log in and out for each sensor scan. This can decrease performance.</li> </ul>

## Credentials for SNMP Devices

Click  to interrupt the [inheritance](#) 136.

 The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">Cisco IP SLA</a></li> <li>▪ <a href="#">SNMP APC Hardware</a></li> <li>▪ <a href="#">SNMP Buffalo TS System Health</a></li> <li>▪ <a href="#">SNMP Cisco ADSL</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Connections</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Traffic</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Users</a></li> <li>▪ <a href="#">SNMP Cisco CBQoS</a></li> <li>▪ <a href="#">SNMP Cisco System Health</a></li> <li>▪ <a href="#">SNMP Cisco UCS Blade</a></li> <li>▪ <a href="#">SNMP Cisco UCS Chassis</a></li> <li>▪ <a href="#">SNMP Cisco UCS Physical Disk</a></li> <li>▪ <a href="#">SNMP Cisco UCS System Health</a></li> <li>▪ <a href="#">SNMP CPU Load</a></li> <li>▪ <a href="#">SNMP Custom</a></li> <li>▪ <a href="#">SNMP Custom Advanced</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">SNMP Fujitsu System Health v2</a></li> <li>▪ <a href="#">SNMP Hardware Status</a></li> <li>▪ <a href="#">SNMP HP LaserJet Hardware</a></li> <li>▪ <a href="#">SNMP HPE BladeSystem Blade</a></li> <li>▪ <a href="#">SNMP HPE BladeSystem Enclosure Health</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Logical Disk</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Memory Controller</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Network Interface</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Physical Disk</a></li> <li>▪ <a href="#">SNMP HPE ProLiant System Health</a></li> <li>▪ <a href="#">SNMP IBM System X Logical Disk</a></li> <li>▪ <a href="#">SNMP IBM System X Physical Disk</a></li> <li>▪ <a href="#">SNMP IBM System X Physical Memory</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">SNMP NetApp Enclosure</a></li> <li>▪ <a href="#">SNMP NetApp I/O</a></li> <li>▪ <a href="#">SNMP NetApp License</a></li> <li>▪ <a href="#">SNMP NetApp Logical Unit</a></li> <li>▪ <a href="#">SNMP NetApp Network Interface</a></li> <li>▪ <a href="#">SNMP NetApp System Health</a></li> <li>▪ <a href="#">SNMP Nutanix Cluster Health</a></li> <li>▪ <a href="#">SNMP Nutanix Hypervisor</a></li> <li>▪ <a href="#">SNMP Poseidon Environment</a></li> <li>▪ <a href="#">SNMP Printer</a></li> <li>▪ <a href="#">SNMP QNAP Logical Disk</a></li> <li>▪ <a href="#">SNMP QNAP Physical Disk</a></li> <li>▪ <a href="#">SNMP QNAP System Health</a></li> <li>▪ <a href="#">SNMP Rittal CMC III Hardware Status</a></li> <li>▪ <a href="#">SNMP RMON</a></li> <li>▪ <a href="#">SNMP SonicWall System Health</a></li> <li>▪ <a href="#">SNMP SonicWall VPN Traffic</a></li> </ul>
---	---	--

<ul style="list-style-type: none"><li>▪ <a href="#">SNMP Custom String</a></li><li>▪ <a href="#">SNMP Custom String Lookup</a></li><li>▪ <a href="#">SNMP Custom Table</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Logical Disk</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Member Health</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Physical Disk</a></li><li>▪ <a href="#">SNMP Dell Hardware</a></li><li>▪ <a href="#">SNMP Dell PowerEdge Physical Disk</a></li><li>▪ <a href="#">SNMP Dell PowerEdge System Health</a></li><li>▪ <a href="#">SNMP Disk Free</a></li></ul>	<ul style="list-style-type: none"><li>▪ <a href="#">SNMP IBM System X System Health</a></li><li>▪ <a href="#">SNMP interSeptor Pro Environment</a></li><li>▪ <a href="#">SNMP Juniper NS System Health</a></li><li>▪ <a href="#">SNMP LenovoEMC Physical Disk</a></li><li>▪ <a href="#">SNMP LenovoEMC System Health</a></li><li>▪ <a href="#">SNMP Library</a></li><li>▪ <a href="#">SNMP Linux Disk Free</a></li><li>▪ <a href="#">SNMP Linux Load Average</a></li><li>▪ <a href="#">SNMP Linux Meminfo</a></li><li>▪ <a href="#">SNMP Linux Physical Disk</a></li><li>▪ <a href="#">SNMP Memory</a></li><li>▪ <a href="#">SNMP NetApp Disk Free</a></li></ul>	<ul style="list-style-type: none"><li>▪ <a href="#">SNMP Synology Logical Disk</a></li><li>▪ <a href="#">SNMP Synology Physical Disk</a></li><li>▪ <a href="#">SNMP Synology System Health</a></li><li>▪ <a href="#">SNMP System Uptime</a></li><li>▪ <a href="#">SNMP Traffic</a></li><li>▪ <a href="#">SNMP Trap Receiver</a></li><li>▪ <a href="#">SNMP Windows Service</a></li></ul>
--	--	--

## Credentials for SNMP Devices

inherit from

**SNMP Version** ⓘ

SNMP v1

SNMP v2c (default)

SNMP v3

**Community String** ⓘ

public

**SNMP Port** ⓘ

161





**Timeout (Sec.)** ⓘ

5

Credentials for SNMP Devices

Setting	Description
SNMP Version	<p>Select the Simple Network Management Protocol (SNMP) version for the connection to the target SNMP device:</p> <ul style="list-style-type: none"> <li>SNMP v1: Use SNMP v1 for the connection. SNMP v1 only offers clear-text data transmission. <ul style="list-style-type: none"> <li>ⓘ SNMP v1 does not support 64-bit counters. This might result in invalid data when you monitor traffic via SNMP.</li> </ul> </li> <li>SNMP v2c (default): Use SNMP v2c for the connection. SNMP v2c also only offers clear-text data transmission but it supports 64-bit counters.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ SNMP v3: Use SNMP v3 for the connection. SNMP v3 provides secure authentication and data encryption.</li> <li>ⓘ SNMP v3 has performance limitations because of the use of encryption. The main limiting factor is CPU power. Also keep in mind that SNMP v3, unlike SNMP v1 and v2c, does not scale with more CPU power. Because of this limitation, PRTG can only handle a limited number of requests per second so that you can use only a limited number of sensors using SNMP v3. If you see an increase in <a href="#">Interval Delay</a> or <a href="#">Open Requests</a> with the <a href="#">Probe Health</a> sensor, distribute the load over <a href="#">multiple probes</a> <small>[3198]</small>. SNMP v1 and SNMP v2c do not have this limitation.</li> </ul>
Community String	<p><a href="#">This setting is only visible if you select SNMP v1 or SNMP v2c (default) above.</a></p> <p>Enter the community string of your device. This is like a clear-text password for simple authentication.</p> <p>ⓘ We recommend that you use the default value.</p>
Authentication Method	<p><a href="#">This setting is only visible if you select SNMP v3 above.</a></p> <p>Select the authentication method:</p> <ul style="list-style-type: none"> <li>▪ MD5 (default): Use message-digest algorithm 5 (MD5) for authentication.</li> <li>▪ SHA: Use Secure Hash Algorithm (SHA) for authentication.</li> <li>▪ SHA-224: Use SHA-224 for authentication.</li> <li>▪ SHA-256: Use SHA-256 for authentication.</li> <li>▪ SHA-384: Use SHA-384 for authentication.</li> <li>▪ SHA-512: Use SHA-512 for authentication.</li> </ul> <p>ⓘ If you do not want to use authentication but you need SNMP v3, for example, because your device requires <a href="#">context</a>, you can leave the Password field empty. In this case, PRTG uses <a href="#">SNMP_SEC_LEVEL_NOAUTH</a> and it entirely deactivates authentication.</p> <p>ⓘ The authentication method that you select must match the authentication method of your device.</p>
User Name	<p><a href="#">This setting is only visible if you select SNMP v3 above.</a></p> <p>Enter the user name for access to the target SNMP device.</p> <p>ⓘ The user name that you enter must match the user name of your device.</p>

Setting	Description
Password	<p>This setting is only visible if you select <a href="#">SNMP v3 above</a>.</p> <p>Enter the password for access to the target SNMP device.</p> <p> The password that you enter must match the password of your device.</p>
Encryption Type	<p>This setting is only visible if you select <a href="#">SNMP v3 above</a>.</p> <p>Select an encryption type:</p> <ul style="list-style-type: none"> <li>▪ DES (default): Use Data Encryption Standard (DES) as the encryption algorithm.</li> <li>▪ AES: Use Advanced Encryption Standard (AES) as the encryption algorithm.</li> <li>▪ AES-192: Use AES-192 as the encryption algorithm.</li> <li>▪ AES-256: Use AES-256 as the encryption algorithm.</li> </ul> <p> The encryption type that you select must match the encryption type of your device.</p>
Encryption Key	<p>This setting is only visible if you select <a href="#">SNMP v3 above</a>.</p> <p>Enter an encryption key. If you provide a key, PRTG encrypts SNMP data packets with the encryption algorithm that you selected above. Enter a string or leave the field empty.</p> <p> The encryption key that you enter must match the encryption key of your device. If the encryption keys do not match, you do not get an error message.</p>
Context Name	<p>This setting is only visible if you select <a href="#">SNMP v3 above</a>.</p> <p>Enter a context name only if the configuration of the device requires it. <b>Context</b> is a collection of management information that is accessible by an SNMP device. Enter a string.</p>
SNMP Port	<p>Enter the port for the connection to the SNMP target device. Enter an integer. The default port is <b>161</b>.</p> <p> We recommend that you use the default value.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).</p>


## Credentials for Database Management Systems


Click  to interrupt the [inheritance](#) .

 The settings you define in this section apply to the following sensors:

- [ADO SQL v2](#)
- [Microsoft SQL v2](#)
- [MySQL v2](#)
- [Oracle SQL v2](#)
- [PostgreSQL](#)


### Credentials for Database Management Systems

 inherit from

**Port** 


Default

Custom port for all database sensors

**Authentication Method** 

Windows authentication with impersonation (default)

SQL server authentication



**Timeout (Sec.)** 

60

Credentials for Database Management Systems

Setting	Description
Port	Select the port that PRTG uses for connections to the monitored databases:



Setting	Description
	<ul style="list-style-type: none"> <li>▪ Default: PRTG automatically determines the type of the database and uses the corresponding default port to connect. PRTG uses the following default ports: <ul style="list-style-type: none"> <li>▫ Microsoft SQL: <a href="#">1433</a></li> <li>▫ MySQL: <a href="#">3306</a></li> <li>▫ Oracle SQL: <a href="#">1521</a></li> <li>▫ PostgreSQL: <a href="#">5432</a></li> </ul> </li> <li>▪ Custom port for all database sensors: Select this option if your database management systems do not use the default ports. Enter a custom port for database connections below.</li> </ul>
Custom Port	<p>Enter a custom port for database connections. Enter an integer.</p> <p> PRTG uses this custom port for <a href="#">all</a> database sensors and for connections to <a href="#">all</a> your databases.</p>
Authentication Method	<p>Select the authentication method for the connection to the Structured Query Language (SQL) database:</p> <ul style="list-style-type: none"> <li>▪ Windows authentication with impersonation (default): PRTG uses the Windows credentials that you define in settings that are higher in the <a href="#">object hierarchy</a><sup>[132]</sup> for the database connection. <ul style="list-style-type: none"> <li> The user whose credentials PRTG uses needs to have permission to log in to the probe system with a database sensor. This is necessary for the impersonation.</li> </ul> </li> <li>▪ SQL server authentication: Use explicit credentials for database connections. Enter a user name and password below.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select SQL server authentication above.</a></p> <p>Enter the user name for the database connection.</p>
Password	<p><a href="#">This setting is only visible if you select SQL server authentication above.</a></p> <p>Enter the password for the database connection.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <a href="#">900</a> seconds (15 minutes).</p>

## Credentials for AWS

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:

- [AWS Alarm v2](#)
- [AWS Cost](#)
- [AWS EBS v2](#)
- [AWS EC2 v2](#)
- [AWS ELB v2](#)
- [AWS RDS v2](#)

■ For more information about the permissions that are necessary to query the AWS API, see the Knowledge Base: [How do I set permissions for the Amazon Web Services \(AWS\) API key to use certain sensors in PRTG?](#)

## Credentials for AWS

inherit from

**Access Key** ⓘ

---

**Secret Key** ⓘ

---

Credentials for AWS

Setting	Description
Access Key	Enter the Amazon Web Services (AWS) access key.
Secret Key	Enter the AWS secret key.

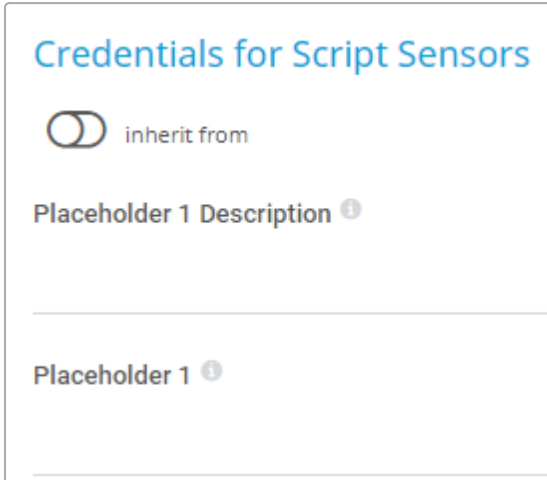
### Credentials for Script Sensors

Click  to interrupt the [inheritance](#) <sup>136</sup>.

ⓘ The settings you define in this section apply to the following sensors:

- [EXE/Script](#)
- [EXE/Script Advanced](#)
- [Python Script Advanced](#)

- [Script v2](#)
- [SSH Script](#)
- [SSH Script Advanced](#)



Credentials for Script Sensors

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder1</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder2</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder3</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.

Setting	Description
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder4</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder5</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.


### Credentials for Cisco Meraki


Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:


- [Cisco Meraki License](#)
- [Cisco Meraki Network Health](#)

## Credentials for Cisco Meraki


 inherit from

API Key  .....

---

Meraki Dashboard API Endpoint  [api.meraki.com](https://api.meraki.com)

Credentials for Cisco Meraki

Setting	Description
API Key	Enter an API key that the sensor uses for authentication against the Cisco Meraki Dashboard API.
Meraki Dashboard API Endpoint	Enter the endpoint for the Cisco Meraki Dashboard API. The default <a href="https://api.meraki.com">api.meraki.com</a> should be valid for most use cases.  See the Cisco Meraki Dashboard API documentation for other possible choices.


## Credentials for Dell EMC


Click  to interrupt the [inheritance](#) 136.


 The settings you define in this section apply to the following sensors:


- [Dell EMC Unity Enclosure Health v2](#)
- [Dell EMC Unity File System v2](#)
- [Dell EMC Unity Storage Capacity v2](#)
- [Dell EMC Unity Storage LUN v2](#)
- [Dell EMC Unity Storage Pool v2](#)
- [Dell EMC Unity VMware Datastore v2](#)

### Credentials for Dell EMC

 inherit from

**User Name** 

**Password** 

**Port** 

Credentials for Dell EMC

Setting	Description
User Name	Enter the user name for access to the Dell EMC system.

Setting	Description
Password	Enter the password for access to the Dell EMC system.
Port	Enter the port for the connection to the Dell EMC system. The default port for secure connections is <a href="#">443</a> .


### Credentials for FortiGate


Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [FortiGate System Statistics](#)
- [FortiGate VPN Overview](#)


### Credentials for FortiGate

 inherit from

API Token 

●●●●●●●●

---

Port 

443

Credentials for FortiGate

Setting	Description
API Token	Enter the API token for access to the FortiGate system.
Port	Enter the port for the connection to the FortiGate system. The default port for secure connections is <a href="#">443</a> .

### Credentials for HPE 3PAR

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [HPE 3PAR Common Provisioning Group](#)

- [HPE 3PAR Drive Enclosure](#)
- [HPE 3PAR Virtual Volume](#)

## Credentials for HPE 3PAR

inherit from

User Name <sup>i</sup>

johnqpulic

Password <sup>i</sup>

●●●●●●●●●●●●●●●●

Protocol <sup>i</sup>

HTTPS (default)

HTTP


WSAPI Port <sup>i</sup>

8080

SSH Port <sup>i</sup>

22

Credentials for HPE 3PAR

Setting	Description
User Name	Enter the user name for access to the HPE 3PAR system.
Password	Enter the password for access to the HPE 3PAR system.
Protocol	<p>Select the protocol that you want to use for the connection to the HPE 3PAR system:</p> <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
WSAPI Port	<p>Enter the Web Services API (WSAPI) port for the connection to the HPE 3PAR system. The default port for secure connections is <b>8080</b> and the default port for unsecure connections is <b>8008</b>.</p> <p> For more information, see the Knowledge Base: <a href="#">Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?</a></p>
SSH Port	Enter the SSH port for the connection to the HPE 3PAR system. The default port for secure connections is <b>22</b> .

## Credentials for HTTP

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensor:

- [HTTP v2](#)



### Credentials for HTTP

inherit from

**Authentication Method** ⓘ

None (default)

Basic authentication

Bearer authentication

**Placeholder 1 Description** ⓘ

---

**Placeholder 1** ⓘ

---

Credentials for HTTP

Setting	Description
Authentication Method	<p>Select the authentication method for access to the server:</p> <ul style="list-style-type: none"> <li>▪ None (default): Use no authentication.</li> <li>▪ Basic authentication: Use basic authentication.</li> <li>▪ Bearer authentication: Use an OAuth2 bearer token.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter the user name for access to the server.</p>
Password	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter the password for access to the server.</p>
Bearer Token	<p><a href="#">This setting is only visible if you select Bearer authentication above.</a></p> <p>Enter a bearer token for access to the server.</p>

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder1</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder2</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder3</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder4</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder5</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.

## Credentials for Microsoft Azure

**i** The settings you define in this section apply to the following sensors:



- [Microsoft Azure SQL Database](#)
- [Microsoft Azure Storage Account](#)

- [Microsoft Azure Subscription Cost](#)
- [Microsoft Azure Virtual Machine](#)

The sensors use the credentials to authenticate with Microsoft Entra ID.

■ For more information about the credentials and permissions that are necessary use the Microsoft Azure sensors, see the Knowledge Base: [How do I obtain credentials and create custom roles for the Microsoft Azure sensors?](#)

### Credentials for Microsoft Azure

 inherit from  Local Probe

**Tenant ID** ⓘ

---

**Client ID** ⓘ

---


**Client Secret** ⓘ

---

**Subscription ID** ⓘ

---

**Microsoft Azure Management Endpoint** ⓘ

management.azure.com 

Credentials for Microsoft Azure

Setting	Description
Tenant ID	Enter the Microsoft Entra tenant ID.  A tenant ID must be a 32-digit sequence in hexadecimal notation.
Client ID	Enter the Microsoft Entra client ID.
Client Secret	Enter the Microsoft Entra client secret.

Setting	Description
Subscription ID	Enter the Microsoft Entra subscription ID.

### Credentials for MQTT

Click  to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

- [MQTT Round Trip](#)
- [MQTT Statistics](#)
- [MQTT Subscribe Custom](#)

## Credentials for MQTT

inherit from

**Authentication Method** **i**

None (default)

User name and password

**Port** **i**

1883


---



**Transport-Level Security** **i**

Do not use transport-level security (default)

Use transport-level security

Credentials for MQTT

Setting	Description
Authentication Method	<p>Select if you want to connect without credentials or define credentials for access to the MQTT broker:</p> <ul style="list-style-type: none"> <li>▪ None (default): Connect without credentials.</li> <li>▪ User name and password: Define credentials for the connection.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select User name and password above.</a></p> <p>Enter the user name for access to the Message Queue Telemetry Transport (MQTT) broker.</p>
Password	<p><a href="#">This setting is only visible if you select User name and password above.</a></p> <p>Enter the password for access to the MQTT broker.</p>
Port	<p>Enter the port for the connection to the MQTT broker. The default port for secure connections is <b>8883</b> and the default port for unsecure connections is <b>1883</b>.</p>
Transport-Level Security	<p>Select if you want to use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection:</p> <ul style="list-style-type: none"> <li>▪ Do not use transport-level security (default): Establish the connection without connection security.</li> <li>▪ Use transport-level security: Establish the connection with the strongest SSL/TLS method that the target device provides.</li> </ul>
Server Authentication	<p><a href="#">This setting is only visible if you select Use transport-level security above.</a></p> <p>Select if you want to use a certificate for server authentication:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not use a certificate for server authentication.</li> <li>▪ Enable: Use a certificate for server authentication.</li> </ul>
CA Certificate	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Paste the certificate authority (CA) certificate for the verification of the MQTT broker.</p> <p> The certificate must be in Privacy-Enhanced Mail (PEM) format.</p>
Client Authentication	<p><a href="#">This setting is only visible if you select Use transport-level security above.</a></p> <p>Select if you want to use a certificate for client authentication:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not use a certificate for client authentication.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Enable: Use a certificate for client authentication.</li> </ul>
Client Certificate	<p>This setting is only visible if you select Enable above.</p> <p>Paste the certificate that you created for authenticating the sensor against the MQTT broker.</p> <p> The certificate must be in PEM format.</p>
Client Key	<p>This setting is only visible if you select Enable above.</p> <p>Enter the client key for access to the MQTT broker.</p> <p> The client key must be in PEM format and it must be encrypted using the Client Key Password.</p>
Client Key Password	<p>This setting is only visible if you select Enable above.</p> <p>Enter the password for the client key.</p>

## Credentials for NetApp

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:

- [NetApp Aggregate v2](#)
- [NetApp I/O v2](#)
- [NetApp LIF v2](#)
- [NetApp LUN v2](#)
- [NetApp NIC v2](#)
- [NetApp Physical Disk v2](#)
- [NetApp SnapMirror v2](#)
- [NetApp System Health v2](#)
- [NetApp Volume v2](#)

The sensors use the credentials for access to the ONTAP System Manager.

## Credentials for NetApp

inherit from Network-01f

**User Name** i

johnqpublic

---

**Password** i

.....

---

**Port** i

443

---

**Protocol** i

HTTPS (default)

HTTP

Credentials for NetApp

Setting	Description
User Name	Enter a user name for access to the ONTAP System Manager.
Password	Enter the password for access to the ONTAP System Manager.
Port	Enter the port for the connection to the ONTAP System Manager. The default port for secure connections is <a href="#">443</a> .

Setting	Description
Protocol	Select the protocol that you want to use for the connection to the ONTAP System Manager: <ul style="list-style-type: none"><li>▪ HTTPS (default): Use HTTPS for the connection.</li><li>▪ HTTP: Use HTTP for the connection.</li></ul>

## Credentials for OPC UA

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [Beckhoff IPC System Health](#)
- [OPC UA Certificate](#)
- [OPC UA Custom](#)
- [OPC UA Server Status](#)



## Credentials for OPC UA

inherit from

Port <sup>i</sup>

4840

Server Path <sup>i</sup>

Security Mode <sup>i</sup>

None (default)

Sign

Sign & Encrypt



Authentication Method <sup>i</sup>

Anonymous (default)

User name and password

Credentials for OPC UA

Setting	Description
Port	Enter the port for the connection to the OPC Unified Architecture (OPC UA) server. The default port for secure connections is <a href="#">4840</a> .
Server Path	Enter the path of the OPC UA server endpoint if you run more than one server under the same IP address or DNS name.
Security Mode	Select if you want to use encryption: <ul style="list-style-type: none"> <li>None (default): Do not use encryption.</li> <li>Sign: Sign messages between the sensor and the OPC UA server.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Sign &amp; Encrypt: Sign and encrypt messages between the sensor and the OPC UA server.</li> </ul>
Security Policy	<p>This setting is only visible if you select Sign or Sign &amp; Encrypt above.</p> <p>Select if you want to use a security policy and define which policy you want to use:</p> <ul style="list-style-type: none"> <li>▪ None (default): Do not use a security policy.</li> <li>▪ Basic256Sha256: Use the Basic256Sha256 security policy.</li> <li>▪ Basic256: Use the Basic256 security policy.</li> </ul>
Client Certificate	<p>This setting is only visible if you select Sign or Sign &amp; Encrypt above.</p> <p>Enter the certificate that you created for authenticating the sensor against the OPC UA server.</p> <p> The certificate must meet the following requirements:</p> <ul style="list-style-type: none"> <li>▪ The key size must be 2048-bit or 4096-bit.</li> <li>▪ The secure hash algorithm must be <a href="#">SHA256</a>.</li> <li>▪ DataEncipherment must be part of the KeyUsage certificate extension.</li> <li>▪ A uniform resource indicator (URI) must be set in subjectAltName.</li> <li>▪ The certificate must be in Privacy-Enhanced Mail (PEM) format.</li> </ul>
Client Key	<p>This setting is only visible if you select Sign or Sign &amp; Encrypt above.</p> <p>Enter the client key for access to the OPC UA server.</p> <p> The client key must be in PEM format and it must be encrypted using the Client Key Password.</p>
Client Key Password	<p>This setting is only visible if you select Sign or Sign &amp; Encrypt above.</p> <p>Enter the password for the client key.</p>
Authentication Method	<p>Select if you want to connect without credentials or define credentials for access to the OPC UA server:</p> <ul style="list-style-type: none"> <li>▪ Anonymous (default): Connect without credentials.</li> <li>▪ User name and password: Define credentials for the connection.</li> </ul>

Setting	Description
	<p><b>i</b> Most OPC UA servers do not support User name and password authentication without a client certificate. To use User name and password authentication, select Sign or Sign &amp; Encrypt under Security Mode and Basic256Sha256 or Basic256 under Security Policy and enter the Client Certificate, Client Key, and Client Key Password that you want to use.</p> <p><b>i</b> If you select None (default) under Security Mode and use User name and password authentication, PRTG sends the unencrypted password to the OPC UA server.</p>
User Name	<p>This setting is only visible if you select User name and password <a href="#">above</a>.</p> <p>Enter the user name for access to the OPC UA server.</p>
Password	<p>This setting is only visible if you select User name and password <a href="#">above</a>.</p> <p>Enter the password for access to the OPC UA server.</p>

### Credentials for Soffico Orchestra

Click  to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensor:

- [Soffico Orchestra Channel Health](#)
- [Soffico Orchestra Scenario](#)

## Credentials for Soffico Orchestra

inherit from

### Authentication Method i

- None (default)  
 User name and password

### Timeout (Sec.) i

60

### Port i

8443

### Protocol i

- HTTPS (default)  
 HTTP

Credentials for Soffico Orchestra

Setting	Description
Authentication Method	Select if you want to connect without credentials or define credentials for access to the Orchestra platform: <ul style="list-style-type: none"> <li>None (default): Connect without credentials.</li> <li>User name and password: Define credentials for the connection.</li> </ul>
User Name	<a href="#">This setting is only visible if you select User name and password above.</a> Enter the user name for access to the Orchestra platform.
Password	<a href="#">This setting is only visible if you select User name and password above.</a>

Setting	Description
	Enter the password for access to the Orchestra platform.
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).
Port	Enter the port for the connection to the Orchestra platform. The default port for secure connections is <b>8443</b> and the default port for unsecure connections is <b>8019</b> .
Protocol	Select the protocol that you want to use for the connection to the Orchestra platform: <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>

## Credentials for Redfish

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [Redfish Power Supply](#)
- [Redfish System Health](#)
- [Redfish Virtual Disk](#)

### Credentials for Redfish

inherit from

**User Name** ⓘ

johnqpublic

---

**Password** ⓘ

●●●●●●●●

---

**Protocol** ⓘ

HTTPS (default)

HTTP

**Port** ⓘ

443

Credentials for Redfish

Setting	Description
User Name	Enter the user name for access to the Redfish system.
Password	Enter the password for access to the Redfish system.
Protocol	<p>Select the protocol that you want to use for the connection to the Redfish system:</p> <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
Port	Enter the port for the connection to the Redfish system. The default port for secure connections is 443.

## Credentials for REST API


Click  to interrupt the [inheritance](#) 136.

 The settings you define in this section apply to the following sensor:

- [REST Custom v2](#)

### Credentials for REST API

inherit from

**Authentication Method** 

None (default)

Basic authentication

Bearer authentication

Credentials for REST API

Setting	Description
Authentication Method	<p>Select the authentication method for access to the Representational State Transfer (REST) application programming interface (API):</p> <ul style="list-style-type: none"> <li>▪ None (default): Use no authentication.</li> <li>▪ Basic authentication: Use basic authentication.</li> <li>▪ Bearer authentication: Use an OAuth2 bearer token.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter the user name for access to the REST API.</p>
Password	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter the password for access to the REST API.</p>
Bearer Token	<p><a href="#">This setting is only visible if you select Bearer authentication above.</a></p> <p>Enter a bearer token for access to the REST API.</p>
Placeholder 1 Description	<p>Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.</p>

Setting	Description
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder1</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder2</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder3</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder4</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder5</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.

## Credentials for Veeam


Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [Veeam Backup Job Status](#)
- [Veeam Backup Job Status Advanced](#)



## Credentials for Veeam

 inherit from

**User Name** i

johnqpublic

---

**Password** i

●●●●●●●●●●●●●●●●●●

---

**Port** i

9398

Credentials for Veeam

Setting	Description
User Name	Enter the user name for access to the Veeam Backup Enterprise Manager.
Password	Enter the password for access to the Veeam Backup Enterprise Manager.
Port	Enter the port for the connection to the Veeam Backup Enterprise Manager. The default port for secure connections is <a href="#">9398</a> .

### Access Rights

Click  to interrupt the [inheritance](#)<sup>136</sup>.

### Access Rights

inherit from


**User Group Access** ⓘ

User Group	Rights
PRTG Users Group	Write access
Read-only User Group	Read access
SSO User Group	Inherited (No access)

Revert access rights of child objects to "inherited"

Access Rights

Setting	Description
User Group Access	<p>Select the <a href="#">user groups</a> [2912] that have access to the object. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights:</p> <ul style="list-style-type: none"> <li>▪ Inherited: Inherit the access rights settings of the parent object.</li> <li>▪ No access: Users in this user group cannot see or edit the object. The object neither shows up in lists nor in the device tree. <ul style="list-style-type: none"> <li>ⓘ There is one exception: If a user in this user group has access to a child object, the parent object is visible in the device tree but users in this user group cannot access it.</li> </ul> </li> <li>▪ Read access: Users in this group can see the object and view its monitoring results. They cannot edit any settings.</li> <li>▪ Write access: Users in this group can see the object, view its monitoring results, and edit its settings. They cannot edit its access rights settings.</li> <li>▪ Full access: Users in this group can see the object, view its monitoring results, edit its settings, and edit its access rights settings.</li> </ul> <p>To automatically set all child objects to inherit this object's access rights, select the Revert access rights of child objects to "inherited" option.</p> <p><span style="color: #0070C0;">■</span> For more information on access rights, see section <a href="#">Access Rights Management</a> [145].</p>

-  Click OK to save your settings. If you close the dialog without saving, all changes to the settings are lost.

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- <https://kb.paessler.com/en/topic/38083>

Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?

- <https://kb.paessler.com/en/topic/89717>

How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?


- <https://kb.paessler.com/en/topic/88462>

How do I obtain credentials and create custom roles for the Microsoft Azure sensors?

- <https://kb.paessler.com/en/topic/88625>

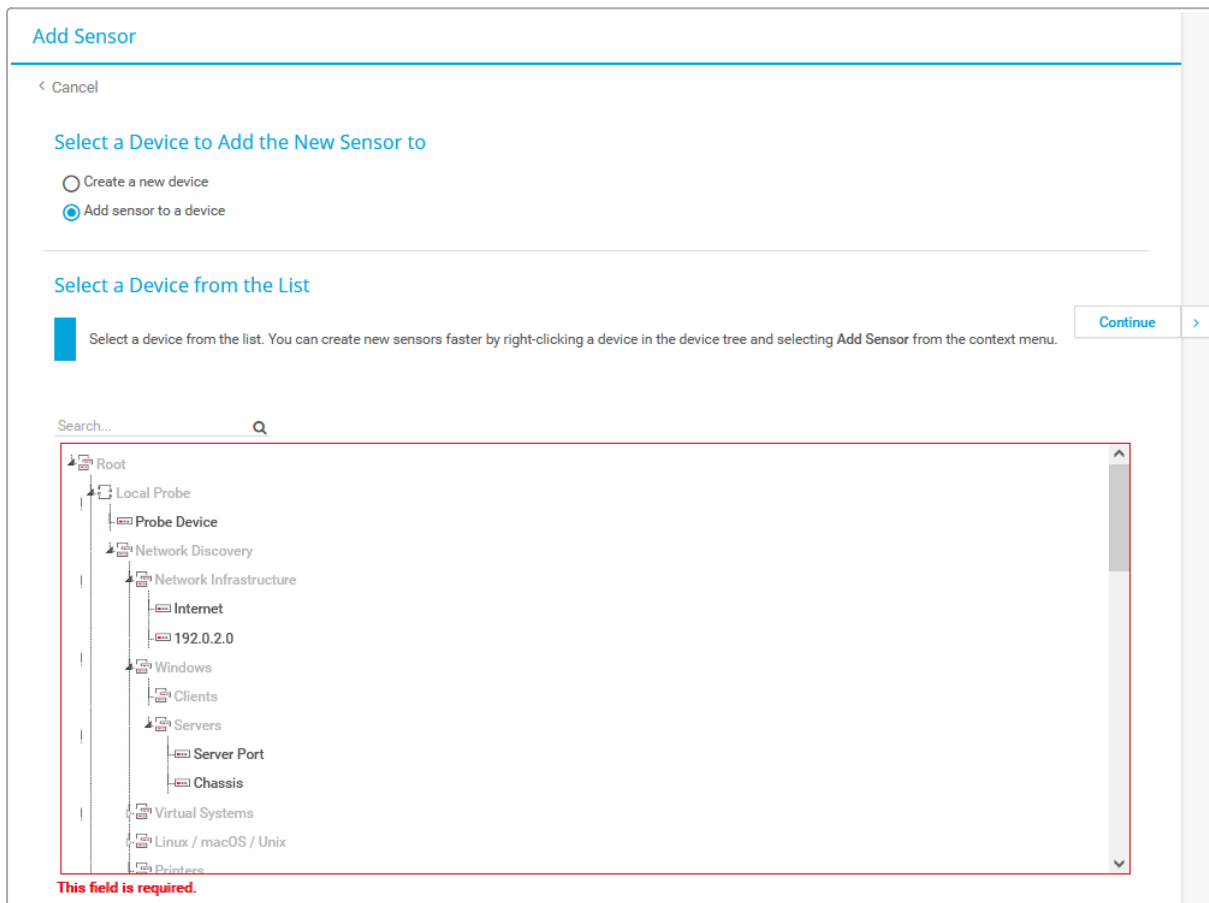
## 7.2.4 Add a Sensor

There are several ways to manually add a sensor:

- Select Sensors | Add Sensor from the [main menu bar](#)<sup>[241]</sup>. A dialog appears that guides you through the process of adding a new sensor.
- Hover over  and select Add Sensor from the menu.
- Select Add Sensor from the [context menu](#)<sup>[229]</sup> of a device to which you want to add the new sensor. This skips step 1 and leads you directly to [step 2](#)<sup>[416]</sup>.
- Click the Add Sensor button at the end of a device's sensor list on the device tree screen or above the geographical map on the right.

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

### Preparation: Select a Device

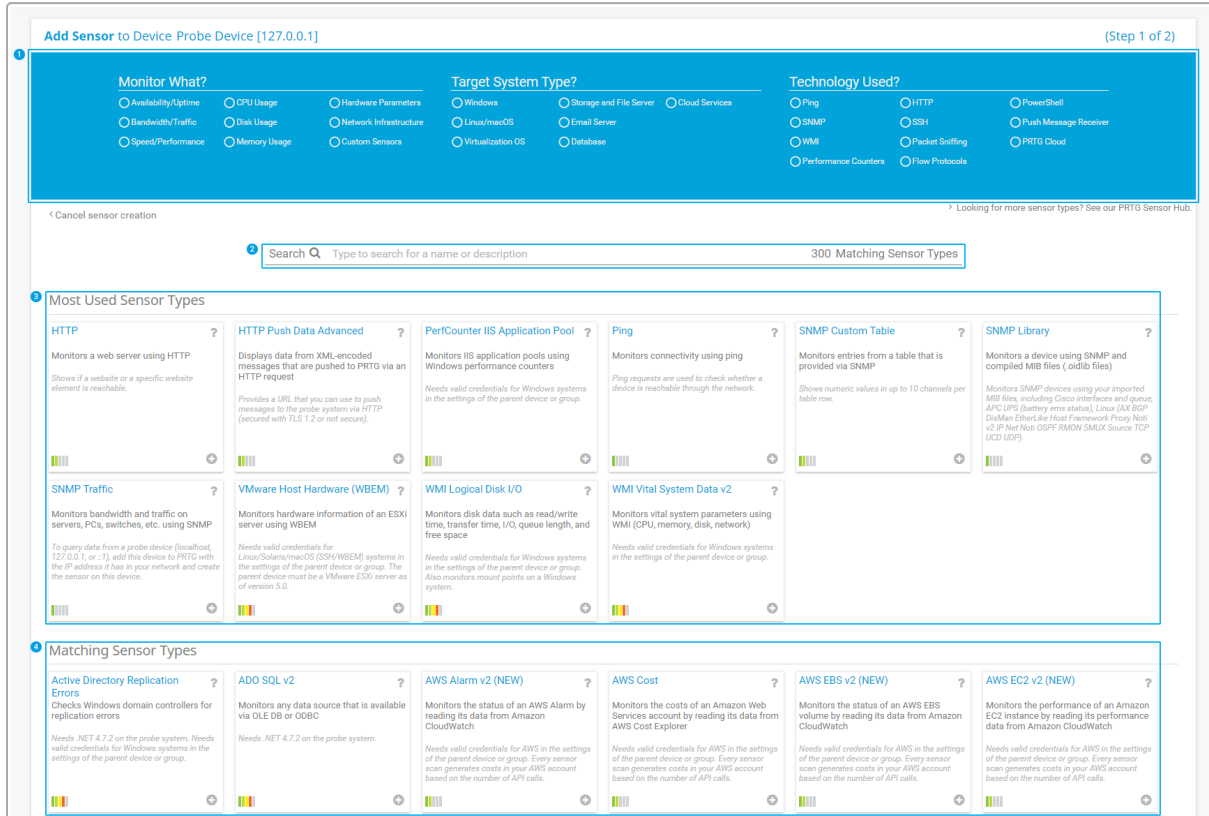


Add Sensor Assistant

1. Select Add sensor to a device.
2. Select the device you want to add the new sensor to.
3. Click Continue.

The Add Sensor dialog appears.

## Step 1: Choose Sensor

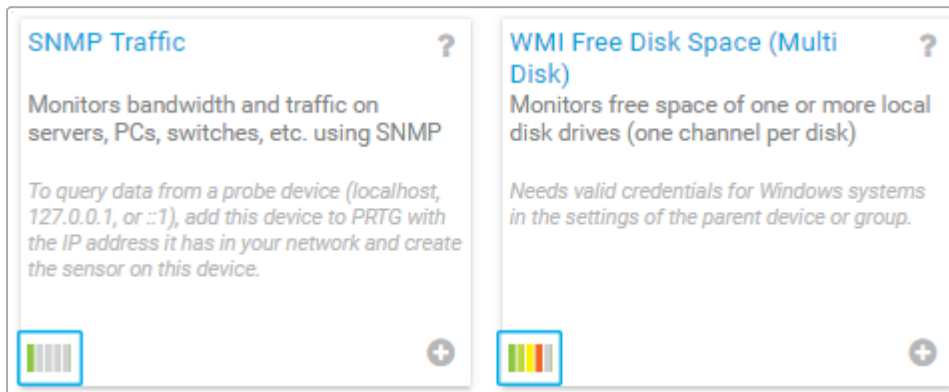


Add Sensor Dialog

In the Add Sensor dialog, the following actions are available:

- 1 Choose appropriate criteria to filter the sensors.
  - Select the type of parameter that you want to monitor via Monitor What?
  - Specify the type of target system that you want to monitor and see what sensors are available for this type of hardware via Target System Type?
  - Select the technology that you want to use for monitoring (for example SNMP or WMI) via Technology Used?
- 2 Enter (parts of) the name into the search box.
- 3 Go through the list of the most used sensor types.
  - ⓘ PRTG suggests sensors for the selected device. This recommendation is automatically calculated based on the current user's sensor usage. It shows the ten most commonly used sensors if there are already enough sensors for the recommendation to use.
- 4 Go through the list of all matching sensor types.
  - If you cannot find a suitable sensor, search for custom sensors in our [PRTG Sensor Hub](#). To do so, click Looking for more sensor types? above the search box or below the list of sensors.
  - For more information, see section [Available Sensor Types](#) <sup>[3263]</sup>, section PRTG Sensor Hub.
- Click the sensor box to select the sensor.

- ❶ If you are unsure which sensor provides the information that you need, we recommend that you use the filter categories to reduce the amount of matching sensor types.
- ❶ Also consider whether a sensor's [performance impact](#)<sup>[2952]</sup> is high or low. To do so, check the bar in the lower-left corner of the sensor box. For more information, see the Knowledge Base: [How can I speed up PRTG—especially for large installations?](#) (especially section 4 - Sensor Type and Monitoring).
- For an overview list of all sensors, including their performance impact, see section [Available Sensor Types](#)<sup>[3232]</sup>.



Sensor with Very Low Performance Impact and with High Performance Impact

- For more information about a sensor, click **?** to see the section of the respective sensor.

## Step 2: Define Sensor Settings

The [Add Sensor](#)<sup>[414]</sup> dialog appears when you manually add a new sensor to a device. It only shows the settings that are required to create the sensor. You can change nearly all settings on the sensor's Settings tab after creation.

- ❶ Enable check boxes in front of the respective lines to select the items. Use the check box in the table header to select all items or to cancel the selection. In large tables, use the search function in the upper-right corner.

Then, the sensor settings dialog opens where you can define the [sensor settings](#) and create the sensor.

- ❶ The settings that you select during sensor creation are valid for all sensors that you create when you finish the dialog.

## More

### ■ KNOWLEDGE BASE

How can I change the number of entries in most used sensor types?

- <https://kb.paessler.com/en/topic/59788>

How can I speed up PRTG—especially for large installations?

- <https://kb.paessler.com/en/topic/2733>

■ PAESSLER WEBSITE

You can find useful scripts for sensors in the PRTG Sensor Hub

- <https://www.paessler.com/sensor-hub>

## 7.3 Manage Device Tree

In the device tree, click the Management tab to enter a different view of your devices and sensors. While in this view, you can move monitoring objects via drag-and-drop. You can also select objects to view and edit their settings. Any changes that you make in this view immediately take effect. To arrange objects in the tree, you have the following options.

### Move or Clone a Sensor

You can change the position of a sensor on the same device or you can clone a sensor to a different device:

- On the same device, drag any sensor and drop it where you want it. The sensor moves to this position and the other sensors line up underneath it.
- Drag any sensor from a device and drop it on a different device to clone a sensor. This creates the same sensor with the same settings on the new device. The original sensor does not change.
  - ① Cloned sensors initially show the Paused [status](#)<sup>[227]</sup> to give you the chance to change any settings before monitoring starts. Check the settings and [resume](#)<sup>[227]</sup> monitoring.
  - ① You cannot clone **fixed** objects such as the root group, a probe device, or PRTG system-internal sensors.
  - ① To clone entire groups or devices, use the [clone object](#)<sup>[2714]</sup> feature in the object's [context menu](#)<sup>[229]</sup>.

### Move a Group or Device

You can change the position of a group or a device via drag-and-drop:

- On the same probe or group, drag any group or device and move it up or down the device tree. A small red arrow appears that shows the future position. When you drop the group or device, it moves to this position and the other probes, groups, and devices line up underneath it.
- Drag any group or device from one probe or group and drop it on a different probe or group. A small red arrow appears that shows the future position. When you drop the group or device, it moves to the new probe or group and the other groups and devices line up underneath it. This way, you can change the probe that a group or device is part of or you can add groups or devices to other groups.
- ① You cannot move the local probe, the hosted probe, or remote probes.

### Multi-Edit Object Settings

You can use multi-edit for object settings:




- Hold down the Ctrl key and select multiple objects of the same type, for example, multiple groups, devices, or sensors.
- In the dialog that appears, select the properties that you want to edit, change the respective settings, and click Save. The changes are applied to all selected objects.

The dialog is the same as described in section [Multi-Edit](#)<sup>[2720]</sup>.

### Related Topics

For other ways to arrange objects, see



- [Move Objects](#)  27121
- [Create Device Template](#)  27251
- [Clone Object](#)  27144

## 7.4 Root Group Settings

The root group is the highest instance in the object hierarchy and it is the parent to most other objects. Therefore, most objects inherit settings from the root group. So, before you create your own sensors, it is a good idea to review the root group's settings to make sure that they suit your needs.



















- ❗ If necessary, you can override every setting for every single child object. To do so, disable the respective inherit from option of an object.

### Root Group Settings

The following settings are available on the Settings tab. All of the settings that you define here can be inherited to all other objects in your setup.

- ❗ This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

In this section:

- [Basic Group Settings](#)  421
- [Location](#)  422
- [Credentials for Windows Systems](#)  422
- [Credentials for Linux/Solaris/macOS \(SSH/WBEM\) Systems](#)  424
- [Credentials for VMware/XenServer](#)  429
- [Credentials for SNMP Devices](#)  431
- [Credentials for Database Management Systems](#)  436
- [Credentials for AWS](#)  437
- [Credentials for Microsoft 365](#)  438
- [Credentials for Script Sensors](#)  440
- [Windows Compatibility Options](#)  441
- [SNMP Compatibility Options](#)  443
- [Proxy Settings](#)  448
- [Scanning Interval](#)  450
- [Schedules, Dependencies, and Maintenance Window](#)  452
- [Access Rights](#)  453
- [Channel Unit Configuration](#)  454
- [Advanced Network Analysis](#)  455

## Basic Group Settings

### Basic Group Settings

**Group Name** ⓘ

Root

---

**Monitoring Status** ⓘ

Started (default)

Paused


Basic Group Settings

Setting	Description
Group Name	<p>Enter a name to identify the group. By default, PRTG displays it in the <a href="#">device tree</a><sup>164</sup>.</p> <p>ⓘ If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Monitoring Status	<p>Select the monitoring status of the group:</p> <ul style="list-style-type: none"> <li>▪ Started (default): Monitor the group.</li> <li>▪ Paused: Pause monitoring for the group. All sensors on all devices in the group are in the Paused <a href="#">status</a><sup>227</sup> until you change this setting.</li> </ul>

## Location

**Location**

Location (for Geo Maps) ⓘ



Location

Setting	Description
Location (for Geo Maps)	<p>If you want to use <a href="#">Geo Maps</a><sup>2731</sup>, enter a location in the first line. Geographical maps then display objects like devices or groups with a status icon using a color code similar to the <a href="#">sensor status icons</a><sup>181</sup> (green–yellow–orange–red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, as PRTG automatically parses latitude and longitude, for example, enter <a href="#">49.452778 11.077778</a>, or <a href="#">enter 49.452778 any 11.077778 text</a>.</p> <p>A minus sign (-) in the first line hides an object from a geographical map. In this case, you can enter location information in line two and following.</p> <p>You can define a specific label for each location. Enter a string denoting the label in the first line and provide the coordinates in the second line. This geographical marker then shows the object with the label in the geographical map.</p> <p>ⓘ The preview map always has a road map layout regardless of the map layout you set in <a href="#">User Interface</a><sup>2859</sup>.</p>

## Credentials for Windows Systems

ⓘ The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">Active Directory Replication Errors</a></li> <li>▪ <a href="#">Event Log (Windows API)</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Windows MSMQ Queue Length</a></li> <li>▪ <a href="#">Windows Network Card</a></li> <li>▪ <a href="#">Windows Pagefile</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">WMI Memory</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2005 (Deprecated)</a></li> </ul>
--	---	--

<ul style="list-style-type: none"> <li>▪ <a href="#">Exchange Backup (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database DAG (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mail Queue (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mailbox (PowerShell)</a></li> <li>▪ <a href="#">Exchange Public Folder (PowerShell)</a></li> <li>▪ <a href="#">File</a></li> <li>▪ <a href="#">File Content</a></li> <li>▪ <a href="#">Folder</a></li> <li>▪ <a href="#">Hyper-V Cluster Shared Volume Disk Free</a></li> <li>▪ <a href="#">Hyper-V Host Server</a></li> <li>▪ <a href="#">Hyper-V Virtual Machine</a></li> <li>▪ <a href="#">Hyper-V Virtual Network Adapter</a></li> <li>▪ <a href="#">Hyper-V Virtual Storage Device</a></li> <li>▪ <a href="#">PerfCounter Custom</a></li> <li>▪ <a href="#">PerfCounter IIS Application Pool</a></li> <li>▪ <a href="#">Share Disk Free</a></li> <li>▪ <a href="#">Windows CPU Load</a></li> <li>▪ <a href="#">Windows IIS Application</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Windows Physical Disk I/O</a></li> <li>▪ <a href="#">Windows Print Queue</a></li> <li>▪ <a href="#">Windows Process</a></li> <li>▪ <a href="#">Windows SMTP Service Received</a></li> <li>▪ <a href="#">Windows SMTP Service Sent</a></li> <li>▪ <a href="#">Windows System Uptime</a></li> <li>▪ <a href="#">Windows Updates Status (PowerShell)</a></li> <li>▪ <a href="#">WMI Battery</a></li> <li>▪ <a href="#">WMI Custom</a></li> <li>▪ <a href="#">WMI Custom String</a></li> <li>▪ <a href="#">WMI Disk Health</a></li> <li>▪ <a href="#">WMI Event Log</a></li> <li>▪ <a href="#">WMI Exchange Server</a></li> <li>▪ <a href="#">WMI Exchange Transport Queue</a></li> <li>▪ <a href="#">WMI File</a></li> <li>▪ <a href="#">WMI Free Disk Space (Multi Disk)</a></li> <li>▪ <a href="#">WMI HDD Health</a></li> <li>▪ <a href="#">WMI Logical Disk I/O</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">WMI Microsoft SQL Server 2008</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2012</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2014</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2016</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2017</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2019</a></li> <li>▪ <a href="#">WMI Remote Ping</a></li> <li>▪ <a href="#">WMI Security Center</a></li> <li>▪ <a href="#">WMI Service</a></li> <li>▪ <a href="#">WMI Share</a></li> <li>▪ <a href="#">WMI SharePoint Process</a></li> <li>▪ <a href="#">WMI Storage Pool</a></li> <li>▪ <a href="#">WMI Terminal Services (Windows 2008+)</a></li> <li>▪ <a href="#">WMI Terminal Services (Windows XP/Vista/2003)</a></li> <li>▪ <a href="#">WMI UTC Time</a></li> <li>▪ <a href="#">WMI Vital System Data v2</a></li> <li>▪ <a href="#">WMI Volume</a></li> <li>▪ <a href="#">WSUS Statistics</a></li> </ul>
--	--	---

## Credentials for Windows Systems

**Domain or Computer Name** ⓘ

www.example.com

---

**User Name** ⓘ

johnqpublic

---

**Password** ⓘ

.....

Credentials for Windows Systems

Setting	Description
Domain or Computer Name	<p>Enter the domain or computer name of the user account with which you want to access the Windows system. PRTG uses this account for Windows Management Instrumentation (WMI) sensors and other Windows sensors.</p> <p>If you want to use a Windows local user account on the target device, enter the computer name. If you want to use a Windows domain user account (recommended), enter the domain name. PRTG automatically adds a prefix to use the NT LAN Manager (NTLM) protocol if you do not explicitly define it. Do not leave this field empty.</p>
User Name	<p>Enter the user name for access to the Windows system. Usually, you use credentials with administrator rights.</p>
Password	<p>Enter the password for access to the Windows system. Usually, you use credentials with administrator rights.</p>

### Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

ⓘ The settings you define in this section apply to the following sensors:

- [SFTP Secure File Transfer Protocol](#)
- [SSH Disk Free](#)

- [SSH INodes Free](#)
- [SSH Load Average](#)
- [SSH Meminfo](#)
- [SSH Remote Ping](#)
- [SSH SAN Enclosure](#)
- [SSH SAN Logical Disk](#)
- [SSH SAN Physical Disk](#)
- [SSH SAN System Health](#)
- [SSH Script](#)
- [SSH Script Advanced](#)
- [VMware Host Hardware \(WBEM\)](#)

## Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

User Name ⓘ

johnqpublic

Authentication Method ⓘ

- Password (default)
- Private key

Password ⓘ

.....

WBEM Protocol ⓘ

- HTTP
- HTTPS (default)

WBEM Port ⓘ

- Default (default)
- Custom

SSH Port ⓘ

22

SSH Rights Elevation ⓘ









- Run the command as the connecting user (default)
- Run the command as a different user using 'sudo' (with password)
- Run the command as a different user using 'sudo' (without password)
- Run the command as a different user using 'su'



SSH Connection Mode ⓘ

- Default
- Compatibility mode (deprecated)

Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems



Setting	Description
User Name	Enter the user name for access to the Linux/Solaris/macOS system via Secure Shell (SSH) and Web-based Enterprise Management (WBEM). Usually, you use credentials with administrator rights.
Authentication Method	<p>Select the authentication method for the login:</p> <ul style="list-style-type: none"> <li>▪ Password: Provide the password for the login.</li> <li>▪ Private key: Provide an RSA private key for authentication.</li> </ul> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For more information, see section <a href="#">Monitoring via SSH</a><sup>[3007]</sup>.</p>
Password	<p>This setting is only visible if you select Password above.</p> <p>Enter a password for access to the Linux/Solaris/macOS system via SSH and WBEM. Usually, you use credentials with administrator rights.</p>
Private Key	<p>This setting is only visible if you select Private key above.</p> <p>Paste the entire RSA private key, including the <b>BEGIN</b> and <b>END</b> lines. Make sure that a corresponding public key exists on the target device.</p> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For more information, see section <a href="#">Monitoring via SSH</a><sup>[3007]</sup>.</p> <p> If you do not insert a private key for the first time but if you want to <a href="#">change</a> the private key, you need to <a href="#">restart the PRTG core server service</a><sup>[2919]</sup> for the private key change to take effect.</p>
WBEM Protocol	<p>Select the protocol that you want to use for the connection to the system via WBEM:</p> <ul style="list-style-type: none"> <li>▪ HTTP: Use an unsecure connection for WBEM.</li> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection for WBEM.</li> </ul> <p> This setting is only relevant if you use WBEM sensors.</p>
WBEM Port	Select if you want to use one of the default ports for the connection to the system via WBEM or if you want to set a custom port:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Default: Use one of the default ports. The default port for unsecure connections is <a href="#">5988</a> and the default port for secure connections is <a href="#">5989</a>.</li> <li>▪ Custom: Use a custom port.</li> </ul> <p> This setting is only relevant if you use WBEM sensors.</p>
Custom WBEM Port	<p>This setting is only visible if you select Custom above.</p> <p>Enter a custom WBEM port. Enter an integer.</p>
SSH Port	<p>Enter the port for SSH connections. Enter an integer. The default port is <a href="#">22</a>.</p> <p> By default, PRTG automatically uses this setting for all <a href="#">SSH sensors</a> unless you define a different port number in the sensor settings.</p>
SSH Rights Elevation	<p>Select the rights that you want to use to run the command on the target system:</p> <ul style="list-style-type: none"> <li>▪ Run the command as the connecting user (default): Use the rights of the user who establishes the SSH connection.</li> <li>▪ Run the command as a different user using 'sudo' (with password): Use the rights of a different user with a password required for <a href="#">sudo</a> to run commands on the target system, for example, as a root user.</li> <li>▪ Run the command as a different user using 'sudo' (without password): Use the rights of a different user without a password required for <a href="#">sudo</a> to run commands on the target system, for example, as a root user.</li> <li>▪ Run the command as a different user using 'su': Use the rights of a different user with <a href="#">su</a> to run commands on the target system.</li> </ul>
Target System User Name	<p>This setting is only visible if you select an option that includes <a href="#">sudo</a> or <a href="#">su</a> above.</p> <p>Enter a user name to run the specified command on the target system as a different user than the root user. If you leave this field empty, you run the command as a root user. Make sure that you set the Linux password even if you use a public key or a private key for authentication. This is not necessary if the user is allowed to run the command without a password.</p>
Password	<p>This setting is only visible if you select an option that includes <a href="#">sudo</a> or <a href="#">su</a> with password above.</p> <p>Enter the password to run the <a href="#">sudo</a> command or the <a href="#">su</a> command.</p>

Setting	Description
SSH Connection Mode	<p>Select the connection mode that you want to use to <a href="#">access data with SSH sensors</a> <small>6007</small>:</p> <ul style="list-style-type: none"> <li>▪ Default: This is the default connection mode for SSH sensors. It provides the best performance and security.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default connection mode does not work on the target system. The compatibility mode is the connection mode that PRTG used in previous versions and it is deprecated.</li> </ul> <p><b>i</b> We strongly recommend that you use the default connection mode.</p> <p><b>i</b> You can also individually select the connection mode for each SSH sensor in the sensor settings.</p>

### Credentials for VMware/XenServer

**i** The settings you define in this section apply to the following sensors:

- [Citrix XenServer Host](#)
- [Citrix XenServer Virtual Machine](#)
- [VMware Datastore \(SOAP\)](#)
- [VMware Host Hardware \(WBEM\)](#)
- [VMware Host Hardware Status \(SOAP\)](#)
- [VMware Host Performance \(SOAP\)](#)
- [VMware Virtual Machine \(SOAP\)](#)

## Credentials for VMware/XenServer

User Name i

johnqpublic

Password i

.....

VMware Protocol i

- HTTPS (default)  
 HTTP

Session Handling i

- Reuse a session for multiple scans (default)  
 Create a new session for each scan

Credentials for VMware/XenServer

Setting	Description
User Name	Enter the user name for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.
Password	Enter the password for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.  <span>i</span> Single sign-on (SSO) passwords for vSphere do not support special characters. For more information, see the VMware sensors sections.
VMware Protocol	Select the protocol for the connection to VMware ESXi, vCenter Server, or Citrix XenServer: <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>

Setting	Description
Session Handling	<p>Select if you want to reuse a session for VMware sensors:</p> <ul style="list-style-type: none"> <li>▪ Reuse a session for multiple scans (default): Select this option if you want a VMware sensor to reuse a single session for multiple sensor scans to query data. With this option, the sensor does not need to log in and out for each sensor scan. We recommend that you use this option because it reduces network load and log entries on the target device. This can increase performance.</li> <li>▪ Create a new session for each scan: If you select this option, PRTG does not reuse a session and a VMware sensor has to log in and out for each sensor scan. This can decrease performance.</li> </ul>

## Credentials for SNMP Devices

**i** The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">Cisco IP SLA</a></li> <li>▪ <a href="#">SNMP APC Hardware</a></li> <li>▪ <a href="#">SNMP Buffalo TS System Health</a></li> <li>▪ <a href="#">SNMP Cisco ADSL</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Connections</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Traffic</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Users</a></li> <li>▪ <a href="#">SNMP Cisco CBQoS</a></li> <li>▪ <a href="#">SNMP Cisco System Health</a></li> <li>▪ <a href="#">SNMP Cisco UCS Blade</a></li> <li>▪ <a href="#">SNMP Cisco UCS Chassis</a></li> <li>▪ <a href="#">SNMP Cisco UCS Physical Disk</a></li> <li>▪ <a href="#">SNMP Cisco UCS System Health</a></li> <li>▪ <a href="#">SNMP CPU Load</a></li> <li>▪ <a href="#">SNMP Custom</a></li> <li>▪ <a href="#">SNMP Custom Advanced</a></li> <li>▪ <a href="#">SNMP Custom String</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">SNMP Fujitsu System Health v2</a></li> <li>▪ <a href="#">SNMP Hardware Status</a></li> <li>▪ <a href="#">SNMP HP LaserJet Hardware</a></li> <li>▪ <a href="#">SNMP HPE BladeSystem Blade</a></li> <li>▪ <a href="#">SNMP HPE BladeSystem Enclosure Health</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Logical Disk</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Memory Controller</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Network Interface</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Physical Disk</a></li> <li>▪ <a href="#">SNMP HPE ProLiant System Health</a></li> <li>▪ <a href="#">SNMP IBM System X Logical Disk</a></li> <li>▪ <a href="#">SNMP IBM System X Physical Disk</a></li> <li>▪ <a href="#">SNMP IBM System X Physical Memory</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">SNMP NetApp Enclosure</a></li> <li>▪ <a href="#">SNMP NetApp I/O</a></li> <li>▪ <a href="#">SNMP NetApp License</a></li> <li>▪ <a href="#">SNMP NetApp Logical Unit</a></li> <li>▪ <a href="#">SNMP NetApp Network Interface</a></li> <li>▪ <a href="#">SNMP NetApp System Health</a></li> <li>▪ <a href="#">SNMP Nutanix Cluster Health</a></li> <li>▪ <a href="#">SNMP Nutanix Hypervisor</a></li> <li>▪ <a href="#">SNMP Poseidon Environment</a></li> <li>▪ <a href="#">SNMP Printer</a></li> <li>▪ <a href="#">SNMP QNAP Logical Disk</a></li> <li>▪ <a href="#">SNMP QNAP Physical Disk</a></li> <li>▪ <a href="#">SNMP QNAP System Health</a></li> <li>▪ <a href="#">SNMP Rittal CMC III Hardware Status</a></li> <li>▪ <a href="#">SNMP RMON</a></li> <li>▪ <a href="#">SNMP SonicWall System Health</a></li> <li>▪ <a href="#">SNMP SonicWall VPN Traffic</a></li> <li>▪ <a href="#">SNMP Synology Logical Disk</a></li> </ul>
---	---	--

<ul style="list-style-type: none"><li>▪ <a href="#">SNMP Custom String Lookup</a></li><li>▪ <a href="#">SNMP Custom Table</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Logical Disk</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Member Health</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Physical Disk</a></li><li>▪ <a href="#">SNMP Dell Hardware</a></li><li>▪ <a href="#">SNMP Dell PowerEdge Physical Disk</a></li><li>▪ <a href="#">SNMP Dell PowerEdge System Health</a></li><li>▪ <a href="#">SNMP Disk Free</a></li></ul>	<ul style="list-style-type: none"><li>▪ <a href="#">SNMP IBM System X System Health</a></li><li>▪ <a href="#">SNMP interSeptor Pro Environment</a></li><li>▪ <a href="#">SNMP Juniper NS System Health</a></li><li>▪ <a href="#">SNMP LenovoEMC Physical Disk</a></li><li>▪ <a href="#">SNMP LenovoEMC System Health</a></li><li>▪ <a href="#">SNMP Library</a></li><li>▪ <a href="#">SNMP Linux Disk Free</a></li><li>▪ <a href="#">SNMP Linux Load Average</a></li><li>▪ <a href="#">SNMP Linux Meminfo</a></li><li>▪ <a href="#">SNMP Linux Physical Disk</a></li><li>▪ <a href="#">SNMP Memory</a></li><li>▪ <a href="#">SNMP NetApp Disk Free</a></li></ul>	<ul style="list-style-type: none"><li>▪ <a href="#">SNMP Synology Physical Disk</a></li><li>▪ <a href="#">SNMP Synology System Health</a></li><li>▪ <a href="#">SNMP System Uptime</a></li><li>▪ <a href="#">SNMP Traffic</a></li><li>▪ <a href="#">SNMP Trap Receiver</a></li><li>▪ <a href="#">SNMP Windows Service</a></li></ul>
---	--	---

## Credentials for SNMP Devices

### SNMP Version i

- SNMP v1
- SNMP v2c (default)
- SNMP v3

### Community String i

public

### SNMP Port i

161

### Timeout (Sec.) i

5

Credentials for SNMP Devices

Setting	Description
SNMP Version	<p>Select the Simple Network Management Protocol (SNMP) version for the connection to the target SNMP device:</p> <ul style="list-style-type: none"> <li>▪ <b>SNMP v1:</b> Use SNMP v1 for the connection. SNMP v1 only offers clear-text data transmission. <ul style="list-style-type: none"> <li><span style="color: red;">i</span> SNMP v1 does not support 64-bit counters. This might result in invalid data when you monitor traffic via SNMP.</li> </ul> </li> <li>▪ <b>SNMP v2c (default):</b> Use SNMP v2c for the connection. SNMP v2c also only offers clear-text data transmission but it supports 64-bit counters.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ SNMP v3: Use SNMP v3 for the connection. SNMP v3 provides secure authentication and data encryption.</li> <li>ⓘ SNMP v3 has performance limitations because of the use of encryption. The main limiting factor is CPU power. Also keep in mind that SNMP v3, unlike SNMP v1 and v2c, does not scale with more CPU power. Because of this limitation, PRTG can only handle a limited number of requests per second so that you can use only a limited number of sensors using SNMP v3. If you see an increase in <a href="#">Interval Delay</a> or <a href="#">Open Requests</a> with the <a href="#">Probe Health</a> sensor, distribute the load over <a href="#">multiple probes</a><sup>[6198]</sup>. SNMP v1 and SNMP v2c do not have this limitation.</li> </ul>
Community String	<p><a href="#">This setting is only visible if you select SNMP v1 or SNMP v2c (default) above.</a></p> <p>Enter the community string of your device. This is like a clear-text password for simple authentication.</p> <p>ⓘ We recommend that you use the default value.</p>
Authentication Method	<p><a href="#">This setting is only visible if you select SNMP v3 above.</a></p> <p>Select the authentication method:</p> <ul style="list-style-type: none"> <li>▪ MD5 (default): Use message-digest algorithm 5 (MD5) for authentication.</li> <li>▪ SHA: Use Secure Hash Algorithm (SHA) for authentication.</li> <li>▪ SHA-224: Use SHA-224 for authentication.</li> <li>▪ SHA-256: Use SHA-256 for authentication.</li> <li>▪ SHA-384: Use SHA-384 for authentication.</li> <li>▪ SHA-512: Use SHA-512 for authentication.</li> </ul> <p>ⓘ If you do not want to use authentication but you need SNMP v3, for example, because your device requires <a href="#">context</a>, you can leave the Password field empty. In this case, PRTG uses <a href="#">SNMP_SEC_LEVEL_NOAUTH</a> and it entirely deactivates authentication.</p> <p>ⓘ The authentication method that you select must match the authentication method of your device.</p>
User Name	<p><a href="#">This setting is only visible if you select SNMP v3 above.</a></p> <p>Enter the user name for access to the target SNMP device.</p> <p>ⓘ The user name that you enter must match the user name of your device.</p>



Setting	Description
Password	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter the password for access to the target SNMP device.</p> <p><b>i</b> The password that you enter must match the password of your device.</p>
Encryption Type	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Select an encryption type:</p> <ul style="list-style-type: none"> <li>▪ DES (default): Use Data Encryption Standard (DES) as the encryption algorithm.</li> <li>▪ AES: Use Advanced Encryption Standard (AES) as the encryption algorithm.</li> <li>▪ AES-192: Use AES-192 as the encryption algorithm.</li> <li>▪ AES-256: Use AES-256 as the encryption algorithm.</li> </ul> <p><b>i</b> The encryption type that you select must match the encryption type of your device.</p>
Encryption Key	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter an encryption key. If you provide a key, PRTG encrypts SNMP data packets with the encryption algorithm that you selected above. Enter a string or leave the field empty.</p> <p><b>i</b> The encryption key that you enter must match the encryption key of your device. If the encryption keys do not match, you do not get an error message.</p>
Context Name	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter a context name only if the configuration of the device requires it. <b>Context</b> is a collection of management information that is accessible by an SNMP device. Enter a string.</p>
SNMP Port	<p>Enter the port for the connection to the SNMP target device. Enter an integer. The default port is <b>161</b>.</p> <p><b>i</b> We recommend that you use the default value.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).</p>

## Credentials for Database Management Systems

**i** The settings you define in this section apply to the following sensors:

- [ADO SQL v2](#)
- [Microsoft SQL v2](#)
- [MySQL v2](#)
- [Oracle SQL v2](#)
- [PostgreSQL](#)

### Credentials for Database Management Systems

**Port** **i**

Default

Custom port for all database sensors

**Authentication Method** **i**

Windows authentication with impersonation (default)



SQL server authentication

**Timeout (Sec.)** **i**

60

Credentials for Database Management Systems

Setting	Description
Port	<p>Select the port that PRTG uses for connections to the monitored databases:</p> <ul style="list-style-type: none"> <li>▪ Default: PRTG automatically determines the type of the database and uses the corresponding default port to connect. PRTG uses the following default ports: <ul style="list-style-type: none"> <li>▫ Microsoft SQL: <a href="#">1433</a></li> <li>▫ MySQL: <a href="#">3306</a></li> <li>▫ Oracle SQL: <a href="#">1521</a></li> </ul> </li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▫ PostgreSQL: <a href="#">5432</a></li> <li>▪ Custom port for all database sensors: Select this option if your database management systems do not use the default ports. Enter a custom port for database connections below.</li> </ul>
Custom Port	<p>Enter a custom port for database connections. Enter an integer.</p> <p> PRTG uses this custom port for <b>all</b> database sensors and for connections to <b>all</b> your databases.</p>
Authentication Method	<p>Select the authentication method for the connection to the Structured Query Language (SQL) database:</p> <ul style="list-style-type: none"> <li>▪ Windows authentication with impersonation (default): PRTG uses the Windows credentials that you define in settings that are higher in the <a href="#">object hierarchy</a><sup>[132]</sup> for the database connection. <ul style="list-style-type: none"> <li> The user whose credentials PRTG uses needs to have permission to log in to the probe system with a database sensor. This is necessary for the impersonation.</li> </ul> </li> <li>▪ SQL server authentication: Use explicit credentials for database connections. Enter a user name and password below.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select SQL server authentication above.</a></p> <p>Enter the user name for the database connection.</p>
Password	<p><a href="#">This setting is only visible if you select SQL server authentication above.</a></p> <p>Enter the password for the database connection.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p>

## Credentials for AWS

 The settings you define in this section apply to the following sensors:

- [AWS Alarm v2](#)
- [AWS Cost](#)
- [AWS EBS v2](#)
- [AWS EC2 v2](#)
- [AWS ELB v2](#)
- [AWS RDS v2](#)

■ For more information about the permissions that are necessary to query the AWS API, see the Knowledge Base: [How do I set permissions for the Amazon Web Services \(AWS\) API key to use certain sensors in PRTG?](#)

Credentials for AWS

Setting	Description
Access Key	Enter the Amazon Web Services (AWS) access key.
Secret Key	Enter the AWS secret key.

## Credentials for Microsoft 365

ⓘ The settings you define in this section apply to the following sensors:

- [Microsoft 365 Mailbox](#)
- [Microsoft 365 Service Status](#)
- [Microsoft 365 Service Status Advanced](#)

The sensors use the credentials to authenticate with Microsoft Entra ID.

■ For more information about the credentials and the permissions that are necessary to use the Microsoft 365 Service Status sensor and the Microsoft 365 Service Status Advanced sensor, see the Knowledge Base: [How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?](#)

■ For more information about the credentials and the permissions that are necessary to use the Microsoft 365 Mailbox sensor, see the Knowledge Base: [How do I obtain credentials and set permissions for the Microsoft 365 Mailbox sensor?](#)

### Credentials for Microsoft 365

inherit from

Tenant ID ?

---

Client ID ?

---

Client Secret ?

---

OpenID Connect Configuration ?

Automatic (default)

Manual

Credentials for Microsoft 365

Setting	Description
Tenant ID	Enter the Microsoft Entra tenant ID. <span style="color: red; font-weight: bold;">i</span> A tenant ID must be a 32-digit sequence in hexadecimal notation.
Client ID	Enter the Microsoft Entra client ID.
Client Secret	Enter the Microsoft Entra client secret.
OpenID Connect Configuration	Select if you want to manually enter the authorization endpoint URL and token endpoint URL that PRTG uses to access Microsoft Graph: <ul style="list-style-type: none"> <li>▪ Automatic (default): PRTG automatically determines the authorization endpoint URL and the token endpoint URL.</li> <li>▪ Manual: Manually enter the authorization endpoint URL and the token endpoint URL.</li> </ul>
Authorization Endpoint	Enter the authorization endpoint URL including the server. Authorization endpoint URL example:


Setting	Description
	<pre>https://login.microsoftonline.com/&lt;tenant-ID&gt;/oauth2/v2.0/authorize</pre> <p><b>i</b> Make sure to replace &lt;tenant-ID&gt; with the <b>directory (tenant) ID</b> from Microsoft Entra ID.</p>
Token Endpoint	<p>Enter the token endpoint URL including the server.</p> <p>Token endpoint URL example:</p> <pre>https://login.microsoftonline.com/&lt;tenant-ID&gt;/oauth2/v2.0/token</pre> <p><b>i</b> Make sure to replace &lt;tenant-ID&gt; with the <b>directory (tenant) ID</b> from Microsoft Entra ID.</p>

### Credentials for Script Sensors

**i** The settings you define in this section apply to the following sensors:

- [EXE/Script](#)
- [EXE/Script Advanced](#)
- [Python Script Advanced](#)
- [Script v2](#)
- [SSH Script](#)
- [SSH Script Advanced](#)

### Credentials for Script Sensors

 inherit from

**Placeholder 1 Description** **i**

---

**Placeholder 1** **i**

Credentials for Script Sensors

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder1</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder2</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder3</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder4</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder5</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.

## Windows Compatibility Options

If you experience problems when you monitor via Windows sensors, use the following compatibility options for troubleshooting.

## Windows Compatibility Options

### Preferred Data Source <sup>i</sup>

- Performance counters and WMI as fallback
- Performance counters only
- WMI only (default)

### Timeout Method <sup>i</sup>

- Use 1.5× scanning interval (default)
- Set manually

Windows Compatibility Options

Setting	Description
Preferred Data Source	<p><sup>i</sup> This setting only applies to hybrid sensors that use both performance counters and Windows Management Instrumentation (WMI).</p> <p>Define the method that Windows sensors use to query data:</p> <ul style="list-style-type: none"> <li>▪ Performance counters and WMI as fallback: Try to query data via performance counters. If this is not possible, establish a connection via WMI.</li> <li>▪ Performance counters only: Query data via performance counters only. If this is not possible, the sensor returns no data.</li> <li>▪ WMI only (default): Query data via WMI only. If this is not possible, the sensor returns no data.</li> </ul>
Timeout Method	<p>Select the time that the sensor waits for the return of the WMI query before the sensor cancels the query and shows an error message:</p> <ul style="list-style-type: none"> <li>▪ Use 1.5× scanning interval (default): Multiply the scanning interval of the sensor by 1.5 and use the resulting value.</li> <li>▪ Set manually: Manually enter a timeout value.</li> </ul> <p><sup>i</sup> We recommend that you use the default value.</p> <p><sup>i</sup> If you experience ongoing timeout errors, try increasing the timeout value.</p>
Timeout (Sec.)	<p>This setting is only visible if you select <a href="#">Set manually</a> above.</p>



Setting	Description
	Enter the time the sensor waits for the return of its WMI query before it cancels it and shows an error message. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).

## SNMP Compatibility Options

If you experience problems when you monitor via Simple Network Management Protocol (SNMP) sensors, use the following compatibility options for troubleshooting.

## SNMP Compatibility Options

### SNMP Delay (ms)

0

### Failed Requests

- Retry (default)
- Do not retry

### Overflow Values

- Ignore (default)
- Handle overflow values as valid results

### Zero Values

- Ignore (default)
- Handle zero values as valid results for delta sensors

### 32-bit/64-bit Counters

- Use 64-bit counters if available (default)
- Use 32-bit counters only

### Request Mode

- Use multi get (default)
- Use single get







### Walk Mode

- Use GETBULK requests (default)
- Use GETNEXT requests

### Port Name Template

Setting	Description
SNMP Delay (ms)	<p>Enter the time in milliseconds (ms) that PRTG waits between two SNMP requests. You can define a delay between 0 and 100. Enter an integer.</p> <ul style="list-style-type: none"> <li><b>i</b> We recommend that you use the default value.</li> <li><b>i</b> If you experience SNMP connection failures, try increasing the delay.</li> </ul>
Failed Requests	<p>Select if an SNMP sensor tries again after a request fails:</p> <ul style="list-style-type: none"> <li>▪ <b>Retry (default):</b> Try again if an SNMP request fails. This can prevent false error messages because of temporary timeout failures.</li> <li>▪ <b>Do not retry:</b> Do not retry if an SNMP request fails. If you select this option, an SNMP sensor shows a Down status earlier.</li> </ul>
Overflow Values	<p>Select how PRTG handles overflow values. Some devices do not correctly handle internal buffer overflows. This can cause false peaks. PRTG can handle overflow values in two ways:</p> <ul style="list-style-type: none"> <li>▪ <b>Ignore (default):</b> Ignore overflow values and do not include them in the monitoring data. We recommend that you use this option.</li> <li>▪ <b>Handle overflow values as valid results:</b> Regard all overflow values as regular data and include them in the monitoring data.</li> </ul> <p><b>i</b> If you experience problems because of strange peaks in your data graphs, change this option. Peaks might indicate that the target device resets counters without an overflow. PRTG interprets such behavior as overflow that results in data peaks. Select the option Ignore (default) in this case. For more information, see the Knowledge Base: <a href="#">What is the Overflow Values setting in the SNMP Compatibility Options?</a></p>
Zero Values	<p>Select how PRTG handles zero values. Some devices send incorrect zero values. This can cause false peaks. PRTG can handle zero values in two ways:</p> <ul style="list-style-type: none"> <li>▪ <b>Ignore (default):</b> Ignore zero values and do not include them in the monitoring data. We recommend that you use this option.</li> </ul> <p><b>i</b> If you experience problems, try changing this option.</p> <ul style="list-style-type: none"> <li>▪ <b>Handle zero values as valid results for delta sensors:</b> Regard all zero values as regular data and include them in the monitoring data.</li> </ul>
32-bit/64-bit Counters	<p>Select the type of traffic counters that PRTG searches for on a device:</p> <ul style="list-style-type: none"> <li>▪ <b>Use 64-bit counters if available (default):</b> The interface scan uses 64-bit traffic counters, if available. This can avoid buffer overflows in the devices.</li> </ul> <p><b>i</b> We recommend that you use the default value.</p> <p><b>i</b> If you experience problems, try changing this option.</p>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Use 32-bit counters only: The interface scan always uses 32-bit traffic counters, even if 64-bit counters are available. This can make monitoring more reliable for some devices.</li> </ul>
Request Mode	<p>Select the request method that PRTG uses for SNMP sensors:</p> <ul style="list-style-type: none"> <li>▪ Use multi get (default): Bundle multiple SNMP requests into one request. We recommend that you use this option.</li> </ul> <p><b>i</b> If you experience problems, try changing this option.</p> <ul style="list-style-type: none"> <li>▪ Use single get: Use one request for each SNMP value. This can increase compatibility with older devices.</li> </ul> <p><b>i</b> PRTG uses <a href="#">paging</a> for SNMP requests. This means that if a sensor must query more than 20 object identifiers (OID), it automatically polls the OIDs in packages of 20 OIDs each.</p>
Walk Mode	<p>Select the kind of SNMP walk that PRTG uses for SNMP sensors:</p> <ul style="list-style-type: none"> <li>▪ Use GETBULK requests (default): Request the next <b>x</b> OIDs in one SNMP request. The default value is <b>10</b>. It is dynamic based on the response size.</li> </ul> <p><b>i</b> This option only works with devices that support SNMP as of version v2c. Make sure that you set the correct SNMP Version in the Credentials for SNMP Devices settings of the parent device or inherit it from objects that are higher in the <a href="#">object hierarchy</a> <sup>[132]</sup>.</p> <ul style="list-style-type: none"> <li>▪ Use GETNEXT requests: Request one OID at a time. This can increase compatibility with older devices or with devices that have insufficient SNMP BULKWALK support.</li> </ul>
Port Name Template	<p>Select how PRTG displays the name of SNMP sensors. Enter a template that uses several variables. When you add new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID, several fields with interface descriptions are usually available. They are different for every device and OID. PRTG uses the information in these fields to name the sensors. If a field is empty or if it is not available, PRTG adds an empty string to the name. By default, the port name template is <a href="#">([port]) [ifalias] [ifsensor]</a>, which creates a name like <b>(001) Ethernet1 Traffic</b>. You can use and combine any field names that are available at an OID of your device, for example:</p> <ul style="list-style-type: none"> <li>▪ [port]: The port number of the monitored interface.</li> <li>▪ [ifalias]: The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling.</li> <li>▪ [ifname]: The textual name of the monitored interface as assigned by the local device.</li> <li>▪ [ifdescr]: A textual string containing information about the target device or interface, for example, manufacturer, product name, or version.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ [ifspeed]: An estimate of the monitored interface's current bandwidth (Kbit/s).</li> <li>▪ [ifsensor]: The type of the sensor, this is <a href="#">Traffic</a> or <a href="#">RMON</a>. This helps to differentiate between <a href="#">SNMP Traffic</a> and <a href="#">SNMP RMON</a> sensors.</li> </ul> <p> For more information about SNMP sensor names, see the Knowledge Base: <a href="#">How can I change the defaults for names automatically generated for new SNMP sensors?</a></p>
Port Name Update	<p>Select how PRTG reacts if you change the names of ports in your physical device (for example, a switch or router):</p> <ul style="list-style-type: none"> <li>▪ Keep port names (use this if you edit the names in PRTG) (default): Do not automatically adjust sensor names. This is the best option if you want to manually change names in PRTG.</li> <li>▪ Automatically update sensor names if port names change in the device: If PRTG detects port name changes in your physical device, it tries to automatically adjust the sensor names accordingly.</li> </ul> <p> For more information about automatic name updates, see the Knowledge Base: <a href="#">Automatically update port name and number for SNMP Traffic sensors when the device changes them.</a></p>
Port Identification	<p>Select the field that PRTG uses for SNMP interface identification:</p> <ul style="list-style-type: none"> <li>▪ Automatic identification (default): Try the ifAlias field first to identify an SNMP interface and then try ifDescr. <ul style="list-style-type: none"> <li> PRTG does not automatically try ifName.</li> </ul> </li> <li>▪ Use IfAlias: For most devices, ifAlias is the best field to use for unique interface names.</li> <li>▪ Use IfDescr: Use this option if the port order of your device changes after a restart, and if no ifAlias field is available. For example, this is the best option for Cisco ASA devices. <ul style="list-style-type: none"> <li> If you use this option, it is important that your device returns unique interface names in the ifDescr field.</li> </ul> </li> <li>▪ Use IfName: You can also use this option if no unique ifAlias is available. <ul style="list-style-type: none"> <li> If you use this option, it is important that your device returns unique interface names in the ifName field.</li> </ul> </li> <li>▪ Do not update ports: Use this option to disable the automatic port identification.</li> </ul>
Start Interface Index	<p> This setting only applies to <a href="#">SNMP Traffic sensors</a> and to <a href="#">Cisco IP SLA sensors</a>.</p> <p>Enter the index at which PRTG starts to query the interface range during sensor creation. Enter <b>0</b> for the automatic mode.</p>

Setting	Description
	<p><b>i</b> We recommend that you use the default value.</p>
End Interface Index	<p><b>i</b> This setting only applies to <a href="#">SNMP Traffic sensors</a> and to <a href="#">Cisco IP SLA sensors</a>.</p> <p>Enter the index at which PRTG stops querying the interface range during sensor creation. Enter <b>0</b> for the automatic mode.</p> <p><b>i</b> We recommend that you use the default value.</p>

## Proxy Settings

**i** The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">AWS Alarm v2</a></li> <li>▪ <a href="#">AWS Cost</a></li> <li>▪ <a href="#">AWS EBS v2</a></li> <li>▪ <a href="#">AWS EC2 v2</a></li> <li>▪ <a href="#">AWS ELB v2</a></li> <li>▪ <a href="#">AWS RDS v2</a></li> <li>▪ <a href="#">Cisco Meraki License</a></li> <li>▪ <a href="#">Cisco Meraki Network Health</a></li> <li>▪ <a href="#">Cloud HTTP v2</a></li> <li>▪ <a href="#">Cloud Ping v2</a></li> <li>▪ <a href="#">Dell EMC Unity Enclosure Health v2</a></li> <li>▪ <a href="#">Dell EMC Unity File System v2</a></li> <li>▪ <a href="#">Dell EMC Unity Storage Capacity v2</a></li> <li>▪ <a href="#">Dell EMC Unity Storage LUN v2</a></li> <li>▪ <a href="#">Dell EMC Unity Storage Pool v2</a></li> <li>▪ <a href="#">Dell EMC Unity VMware Datastore v2</a></li> <li>▪ <a href="#">FortiGate System Statistics</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">HPE 3PAR Common Provisioning Group</a></li> <li>▪ <a href="#">HPE 3PAR Drive Enclosure</a></li> <li>▪ <a href="#">HPE 3PAR Virtual Volume</a></li> <li>▪ <a href="#">HTTP</a></li> <li>▪ <a href="#">HTTP v2</a></li> <li>▪ <a href="#">HTTP Advanced</a></li> <li>▪ <a href="#">HTTP Apache ModStatus PerfStats</a></li> <li>▪ <a href="#">HTTP Apache ModStatus Totals</a></li> <li>▪ <a href="#">HTTP Content</a></li> <li>▪ <a href="#">HTTP Data Advanced</a></li> <li>▪ <a href="#">HTTP Transaction</a></li> <li>▪ <a href="#">Microsoft 365 Mailbox</a></li> <li>▪ <a href="#">Microsoft 365 Service Status</a></li> <li>▪ <a href="#">Microsoft 365 Service Status Advanced</a></li> <li>▪ <a href="#">Microsoft Azure SQL Database</a></li> <li>▪ <a href="#">Microsoft Azure Storage Account</a></li> <li>▪ <a href="#">Microsoft Azure Subscription Cost</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">NetApp Aggregate v2</a></li> <li>▪ <a href="#">NetApp I/O v2</a></li> <li>▪ <a href="#">NetApp LIF v2</a></li> <li>▪ <a href="#">NetApp LUN v2</a></li> <li>▪ <a href="#">NetApp NIC v2</a></li> <li>▪ <a href="#">NetApp Physical Disk v2</a></li> <li>▪ <a href="#">NetApp SnapMirror v2</a></li> <li>▪ <a href="#">NetApp System Health v2</a></li> <li>▪ <a href="#">NetApp Volume v2</a></li> <li>▪ <a href="#">Redfish Power Supply</a></li> <li>▪ <a href="#">Redfish Virtual Disk</a></li> <li>▪ <a href="#">Redfish Power Supply</a></li> <li>▪ <a href="#">REST Custom</a></li> <li>▪ <a href="#">REST Custom v2</a></li> <li>▪ <a href="#">Soffico Orchestra Channel Health</a></li> <li>▪ <a href="#">Soffico Orchestra Scenario</a></li> <li>▪ <a href="#">Veeam Backup Job Status</a></li> <li>▪ <a href="#">Veeam Backup Job Status Advanced</a></li> <li>▪ <a href="#">Zoom Service Status</a></li> </ul>
--	--	--

- [FortiGate VPN Overview](#)
- [Microsoft Azure Virtual Machine](#)

The proxy settings determine how a sensor connects to a URL. You can enter data for an HTTP proxy server that sensors use when they connect via HTTP or HTTPS.

- ⓘ This setting only applies to sensors and how they monitor. For more information on how to change the proxy settings for the PRTG core server, see section [Core & Probes](#).
- ⓘ The [SSL Certificate](#) sensor and the [SSL Security Check](#) sensor do not support HTTP proxies but you can configure connections via SOCKS proxies in the sensors' settings:

## Proxy Settings

**IP Address/DNS Name** ⓘ

192.0.2.0

---

**Port** ⓘ

8080

---

**User Name** ⓘ

johnqpublic



---

**Password** ⓘ

.....

Proxy Settings

Setting	Description
IP Address/DNS Name	Enter the IP address or Domain Name System (DNS) name of the proxy server. If you leave this field empty, sensors do not use a proxy.  ⓘ PRTG currently supports only HTTP proxies.
Port	Enter the port number of the proxy. The default port is <b>8080</b> . Enter an integer.

Setting	Description
User Name	If the proxy requires authentication, enter the user name for the proxy login. Enter a string or leave the field empty.  Only basic authentication is available.
Password	If the proxy requires authentication, enter the password for the proxy login. Enter a string or leave the field empty.  Only basic authentication is available.

### Scanning Interval

#### Scanning Interval

**Scanning Interval** ⓘ

60 seconds

---

**If a Sensor Query Fails** ⓘ

Set sensor to warning status for 1 interval, then set to down status (default)

Scanning Interval

Setting	Description
Scanning Interval	Select a scanning interval from the dropdown list that determines the amount of time that the sensor waits between two scans: <ul style="list-style-type: none"> <li>▪ 30 seconds</li> <li>▪ 60 seconds</li> <li>▪ 5 minutes</li> <li>▪ 10 minutes</li> <li>▪ 15 minutes</li> <li>▪ 30 minutes</li> <li>▪ 1 hour</li> <li>▪ 4 hours</li> <li>▪ 6 hours</li> <li>▪ 12 hours</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ 24 hours</li> </ul> <p><b>i</b> You can change the available intervals in the <a href="#">system administration</a> <sup>[2870]</sup> of PRTG Network Monitor.</p>
<p>If a Sensor Scanning Fails</p>	<p>Select the number of scanning intervals that the sensor has time to reach and to check a device again if a sensor scanning fails. Depending on the option that you select, the sensor can try to reach and to check a device again several times before the sensor shows the Down <a href="#">status</a> <sup>[181]</sup>. This can avoid false alarms if the target device only has temporary issues. For previous scanning intervals with failed requests, the sensor shows the Warning status.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> <li>▪ Set sensor to down status immediately: Set the sensor to the Down status immediately after the first request fails.</li> <li>▪ Set sensor to warning status for 1 interval, then set to down status (default): Set the sensor to the Warning status after the first request fails. If the second request also fails, the sensor shows the Down status.</li> <li>▪ Set sensor to warning status for 2 intervals, then set to down status: Set the sensor to the Down status only after the third request fails.</li> <li>▪ Set sensor to warning status for 3 intervals, then set to down status: Set the sensor to the Down status only after the fourth request fails.</li> <li>▪ Set sensor to warning status for 4 intervals, then set to down status: Set the sensor to the Down status only after the fifth request fails.</li> <li>▪ Set sensor to warning status for 5 intervals, then set to down status: Set the sensor to the Down status only after the sixth request fails.</li> </ul> <p><b>i</b> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval before they show the Down status. It is not possible to immediately set a WMI sensor to the Down status, so the first option does not apply to these sensors. All other options can apply.</p> <p><b>i</b> If you define error limits for a sensor's channels, the sensor immediately shows the Down status. None of the interval options apply.</p> <p><b>i</b> If a channel uses <a href="#">lookup</a> <sup>[3181]</sup> values, the sensor immediately shows the Down status. None of the interval options apply.</p>

## Schedules, Dependencies, and Maintenance Window

### Schedules, Dependencies, and Maintenance Window

Schedules, dependencies, and maintenance windows always pause all sensors inside a group or device. This pausing is always inherited to all child objects and the inheritance cannot be disabled. Below you can set additional schedules, dependencies, or maintenance windows that will be used in parallel to any inherited setting.

#### Schedule ?

None

#### Maintenance Window ?

- Do not set up a one-time maintenance window (default)
- Set up a one-time maintenance window

Schedules, Dependencies, and Maintenance Window

Setting	Description
Schedule	<p>Select a schedule from the list. You can use schedules to monitor during a certain time span (days or hours) every week:</p> <ul style="list-style-type: none"> <li>▪ None</li> <li>▪ Saturdays</li> <li>▪ Sundays</li> <li>▪ Weekdays</li> <li>▪ Weekdays Eight-To-Eight (08:00 - 20:00)</li> <li>▪ Weekdays Nights (17:00 - 09:00)</li> <li>▪ Weekdays Nights (20:00 - 08:00)</li> <li>▪ Weekdays Nine-To-Five (09:00 - 17:00)</li> <li>▪ Weekends</li> </ul> <p><span>?</span> You can create schedules, edit schedules, or pause monitoring for a specific time span. For more information, see section <a href="#">Schedules</a> <small>2848</small>.</p>
Maintenance Window	<p>Select if you want to set up a one-time maintenance window:</p> <ul style="list-style-type: none"> <li>▪ Do not set up a one-time maintenance window (default): Do not set up a one-time maintenance window. Monitoring is always active.</li> <li>▪ Set up a one-time maintenance window: Set up a one-time maintenance window and pause monitoring for the selected object and all child objects. You can define a time span for the pause below.</li> </ul> <p><span>?</span> To close an active one-time maintenance window before the end date, select Do not set up a one-time maintenance window (default).</p>

Setting	Description
Maintenance Begins	<p><b>This setting is only visible if you select</b> Set up a one-time maintenance window <a href="#">above</a>.</p> <p>Use the date time picker to enter the start date and time of the one-time maintenance window.</p>
Maintenance Ends	<p><b>This setting is only visible if you select</b> Set up a one-time maintenance window <a href="#">above</a>.</p> <p>Use the date time picker to enter the end date and time of the one-time maintenance window.</p>

### Access Rights

## Access Rights

**User Group Access** ⓘ

<span style="font-size: 0.8em;">User Group</span>	<span style="font-size: 0.8em;">Rights</span>
PRTG Users Group	Full access

Revert children's access rights to inherited

Access Rights

Setting	Description
User Group Access	<p>Select the <a href="#">user groups</a> <sup>[2912]</sup> that have access to the object. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights:</p> <ul style="list-style-type: none"> <li>▪ Inherited: Inherit the access rights settings of the parent object.</li> <li>▪ No access: Users in this user group cannot see or edit the object. The object neither shows up in lists nor in the device tree. <ul style="list-style-type: none"> <li>ⓘ There is one exception: If a user in this user group has access to a child object, the parent object is visible in the device tree but users in this user group cannot access it.</li> </ul> </li> <li>▪ Read access: Users in this group can see the object and view its monitoring results. They cannot edit any settings.</li> <li>▪ Write access: Users in this group can see the object, view its monitoring results, and edit its settings. They cannot edit its access rights settings.</li> <li>▪ Full access: Users in this group can see the object, view its monitoring results, edit its settings, and edit its access rights settings.</li> </ul> <p>To automatically set all child objects to inherit this object's access rights, select the Revert access rights of child objects to "inherited" option.</p> <p><span style="color: blue;">■</span> For more information on access rights, see section <a href="#">Access Rights Management</a> <sup>[145]</sup>.</p>

### Channel Unit Configuration

Channel Unit Configuration	
Channel Unit Types ⓘ	
Channel Type	Unit
Bytes (Bandwidth)	MB
	Mbit <span style="float: right;">v / second</span>
Bytes (Memory)	GB
Bytes (Disk)	GB
Bytes (File)	MB

Channel Unit Configuration

Setting	Description
Channel Unit Types	<p>For each type of channel, select the unit in which PRTG displays the data. If you define this setting on probe, group, or device level, you can inherit these settings to all sensors underneath. You can set units for the following channel types (if available):</p> <ul style="list-style-type: none"> <li>▪ Bandwidth</li> <li>▪ Memory</li> <li>▪ Disk</li> <li>▪ File</li> <li>▪ Custom</li> </ul> <p><b>i</b> Custom channel types are only available on sensor level.</p> <p><b>i</b> Which channel units are available depends on the sensor type and the available parameters. If no configurable channels are available, this field shows <a href="#">No configurable channels</a>.</p>

### Advanced Network Analysis

#### Advanced Network Analysis

**Unusual Detection** ⓘ

Enable (default)  
 Disable

**Similar Sensors Detection** ⓘ

Enable (default)  
 Disable

**System Information** ⓘ

Enable (default)  
 Disable

Advanced Network Analysis

Setting	Description
Unusual Detection	Select if you want to use the <a href="#">unusual detection</a> <sup>[287]</sup> for sensors:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Enable (default): Activates the unusual detection for this object and, by default, for all objects underneath in the <a href="#">object hierarchy</a><sup>[132]</sup>. Sensors that are affected by this setting show the Unusual status if PRTG detects unusual activity.</li> <li>▪ Disable: Does not activate the unusual detection. PRTG ignores unusual values for sensors that are affected by this setting. These sensors do not show the Unusual status.</li> </ul> <p><b>i</b> You can configure the behavior of the unusual detection or completely disable it in the <a href="#">system settings</a><sup>[2871]</sup>.</p>
Similar Sensors Detection	<p>Select if you want to activate the <a href="#">similar sensors</a><sup>[192]</sup> analysis:</p> <ul style="list-style-type: none"> <li>▪ Enable (default): Activates the similar sensors detection for this object and, by default, for all objects underneath in the object hierarchy. PRTG considers all sensors that are affected by this setting during the similarity analysis.</li> <li>▪ Disable: Does not activate the similar sensors detection. PRTG does not consider sensors that are affected by this setting during the similarity analysis.</li> </ul> <p><b>i</b> You can configure the depth of the analysis of the similar sensors detection or completely disable it in the <a href="#">system settings</a><sup>[2873]</sup>.</p>
System Information	<p>Select if you want to retrieve and show <a href="#">system information</a><sup>[205]</sup> for your devices:</p> <ul style="list-style-type: none"> <li>▪ Enable (default): Activates the system information feature for this object and, by default, for all objects underneath in the hierarchy.</li> <li>▪ Disable: Does not activate the system information feature.</li> </ul> <p><b>i</b> The System Information feature is enabled by default. To retrieve the data, PRTG automatically uses the <a href="#">credentials for Windows systems</a><sup>[606]</sup> and the <a href="#">credentials for SNMP devices</a><sup>[615]</sup> that you entered in the device settings or that the device <a href="#">inherits</a><sup>[132]</sup> from a parent object like the root group. Consider this when you monitor devices that are outside of your local network, especially when you use <b>SNMP v1</b> or <b>SNMP v2c</b>, which do not provide encryption.</p> <p><b>☁</b> This setting is not available on the hosted probe of a PRTG Hosted Monitor instance.</p>

**i** Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

More

**■** KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- <https://kb.paessler.com/en/topic/38083>

What is the Overflow Values setting in the SNMP Compatibility Options?

- <https://kb.paessler.com/en/topic/43503>

How can I change the defaults for names automatically generated for new SNMP sensors?

- <https://kb.paessler.com/en/topic/7363>

Automatically update port name and number for SNMP Traffic sensors when the device changes them

- <https://kb.paessler.com/en/topic/25893>

## 7.5 Probe Settings

The following settings are available on the Settings tab of a probe.

- ❗ We recommend that you define as many settings as possible in the [root group settings](#) so that you can inherit them to all other objects in the [object hierarchy](#).
- ❗ This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

In this section:

- [Basic Probe Settings](#)
- [Location](#)
- [Credentials for Windows Systems](#)
- [Credentials for Linux/Solaris/macOS \(SSH/WBEM\) Systems](#)
- [Credentials for VMware/XenServer](#)
- [Credentials for SNMP Devices](#)
- [Credentials for Database Management Systems](#)
- [Credentials for AWS](#)
- [Credentials for Microsoft 365](#)
- [Credentials for Script Sensors](#)
- [Credentials for Cisco Meraki](#)
- [Credentials for Dell EMC](#)
- [Credentials for FortiGate](#)
- [Credentials for HPE 3PAR](#)
- [Credentials for HTTP](#)
- [Credentials for Microsoft Azure](#)
- [Credentials for MQTT](#)
- [Credentials for NetApp](#)
- [Credentials for OPC UA](#)
- [Credentials for Soffico Orchestra](#)
- [Credentials for Redfish](#)
- [Credentials for REST API](#)
- [Credentials for Veeam](#)
- [Windows Compatibility Options](#)
- [SNMP Compatibility Options](#)
- [Proxy Settings](#)



- [Scanning Interval](#) <sup>512</sup>
- [Schedules, Dependencies, and Maintenance Window](#) <sup>514</sup>
- [Access Rights](#) <sup>517</sup>
- [Channel Unit Configuration](#) <sup>518</sup>
- [Advanced Network Analysis](#) <sup>520</sup>
- [Administrative Probe Settings](#) <sup>521</sup>
- [Scheduled Restart Settings](#) <sup>523</sup>

## Basic Probe Settings

### Basic Probe Settings

**Probe Name** ⓘ

Local Probe

---

**Tags** ⓘ

+

---

**Monitoring Status** ⓘ

Started (default)

Paused




---

**Priority** ⓘ


★ ★ ★ ☆ ☆

Basic Probe Settings

Setting	Description
Probe Name	Enter a name to identify the probe. By default, PRTG shows this name in the <a href="#">device tree</a> <sup>164</sup> , as well as in <a href="#">alarms</a> <sup>202</sup> , <a href="#">logs</a> <sup>210</sup> , <a href="#">notifications</a> <sup>2735</sup> , <a href="#">reports</a> <sup>2754</sup> , <a href="#">maps</a> <sup>2776</sup> , <a href="#">libraries</a> <sup>2738</sup> , and <a href="#">tickets</a> <sup>213</sup> .

Setting	Description
	<p> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({}). For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Tags	<p>Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically <a href="#">inherited</a><sup>138</sup>.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (&lt;&gt;).</p> <p> For performance reasons, it can take some minutes until you can filter for new tags that you added.</p>
Monitoring Status	<p>Select the monitoring status of the probe:</p> <ul style="list-style-type: none"> <li>Started (default): Monitor the probe.</li> <li>Paused: Pause monitoring for the probe. All sensors on all devices on the probe are in the Paused <a href="#">status</a><sup>227</sup> until you change this setting.</li> </ul>
Priority	<p>Select a <a href="#">priority</a><sup>224</sup> for the probe. This setting determines the position of the probe in lists. The highest priority is at the top of a list. You can choose from the lowest priority (☆☆☆☆☆) to the highest priority (★★★★★).</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#)<sup>420</sup> if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#)<sup>136</sup>.

## Location

Click  to interrupt the [inheritance](#)<sup>136</sup>.

### Location

inherit from

Location (for Geo Maps) ⓘ



Location

Setting	Description
Location (for Geo Maps)	<p>If you want to use <a href="#">Geo Maps</a><sup>[2731]</sup>, enter a location in the first line. Geographical maps then display objects like devices or groups with a status icon using a color code similar to the <a href="#">sensor status icons</a><sup>[181]</sup> (green–yellow–orange–red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, as PRTG automatically parses latitude and longitude, for example, enter <a href="#">49.452778 11.077778</a>, or <a href="#">enter 49.452778 any 11.077778 text</a>.</p> <p>A minus sign (-) in the first line hides an object from a geographical map. In this case, you can enter location information in line two and following.</p> <p>You can define a specific label for each location. Enter a string denoting the label in the first line and provide the coordinates in the second line. This geographical marker then shows the object with the label in the geographical map.</p> <p>ⓘ The preview map always has a road map layout regardless of the map layout you set in <a href="#">User Interface</a><sup>[2859]</sup>.</p>

### Credentials for Windows Systems

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

ⓘ The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">Active Directory Replication Errors</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Windows MSMQ Queue Length</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">WMI Memory</a></li> </ul>
---	---	--

<ul style="list-style-type: none"> <li>▪ <a href="#">Event Log (Windows API)</a></li> <li>▪ <a href="#">Exchange Backup (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database DAG (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mail Queue (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mailbox (PowerShell)</a></li> <li>▪ <a href="#">Exchange Public Folder (PowerShell)</a></li> <li>▪ <a href="#">File</a></li> <li>▪ <a href="#">File Content</a></li> <li>▪ <a href="#">Folder</a></li> <li>▪ <a href="#">Hyper-V Cluster Shared Volume Disk Free</a></li> <li>▪ <a href="#">Hyper-V Host Server</a></li> <li>▪ <a href="#">Hyper-V Virtual Machine</a></li> <li>▪ <a href="#">Hyper-V Virtual Network Adapter</a></li> <li>▪ <a href="#">Hyper-V Virtual Storage Device</a></li> <li>▪ <a href="#">PerfCounter Custom</a></li> <li>▪ <a href="#">PerfCounter IIS Application Pool</a></li> <li>▪ <a href="#">Share Disk Free</a></li> <li>▪ <a href="#">Windows CPU Load</a></li> <li>▪ <a href="#">Windows IIS Application</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Windows Network Card</a></li> <li>▪ <a href="#">Windows Pagefile</a></li> <li>▪ <a href="#">Windows Physical Disk I/O</a></li> <li>▪ <a href="#">Windows Print Queue</a></li> <li>▪ <a href="#">Windows Process</a></li> <li>▪ <a href="#">Windows SMTP Service Received</a></li> <li>▪ <a href="#">Windows SMTP Service Sent</a></li> <li>▪ <a href="#">Windows System Uptime</a></li> <li>▪ <a href="#">Windows Updates Status (PowerShell)</a></li> <li>▪ <a href="#">WMI Battery</a></li> <li>▪ <a href="#">WMI Custom</a></li> <li>▪ <a href="#">WMI Custom String</a></li> <li>▪ <a href="#">WMI Disk Health</a></li> <li>▪ <a href="#">WMI Event Log</a></li> <li>▪ <a href="#">WMI Exchange Server</a></li> <li>▪ <a href="#">WMI Exchange Transport Queue</a></li> <li>▪ <a href="#">WMI File</a></li> <li>▪ <a href="#">WMI Free Disk Space (Multi Disk)</a></li> <li>▪ <a href="#">WMI HDD Health</a></li> <li>▪ <a href="#">WMI Logical Disk I/O</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">WMI Microsoft SQL Server 2005 (Deprecated)</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2008</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2012</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2014</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2016</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2017</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2019</a></li> <li>▪ <a href="#">WMI Remote Ping</a></li> <li>▪ <a href="#">WMI Security Center</a></li> <li>▪ <a href="#">WMI Service</a></li> <li>▪ <a href="#">WMI Share</a></li> <li>▪ <a href="#">WMI SharePoint Process</a></li> <li>▪ <a href="#">WMI Storage Pool</a></li> <li>▪ <a href="#">WMI Terminal Services (Windows 2008+)</a></li> <li>▪ <a href="#">WMI Terminal Services (Windows XP/Vista/2003)</a></li> <li>▪ <a href="#">WMI UTC Time</a></li> <li>▪ <a href="#">WMI Vital System Data v2</a></li> <li>▪ <a href="#">WMI Volume</a></li> <li>▪ <a href="#">WSUS Statistics</a></li> </ul>
---	--	---

## Credentials for Windows Systems

 inherit from

Domain or Computer Name 

www.example.com

User Name 

johnqpublic

Password 

.....

Credentials for Windows Systems

Setting	Description
Domain or Computer Name	<p>Enter the domain or computer name of the user account with which you want to access the Windows system. PRTG uses this account for Windows Management Instrumentation (WMI) sensors and other Windows sensors.</p> <p>If you want to use a Windows local user account on the target device, enter the computer name. If you want to use a Windows domain user account (recommended), enter the domain name. PRTG automatically adds a prefix to use the NT LAN Manager (NTLM) protocol if you do not explicitly define it. Do not leave this field empty.</p>
User Name	<p>Enter the user name for access to the Windows system. Usually, you use credentials with administrator rights.</p>
Password	<p>Enter the password for access to the Windows system. Usually, you use credentials with administrator rights.</p>

## Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

Click  to interrupt the [inheritance](#) .

 The settings you define in this section apply to the following sensors:

- [SFTP Secure File Transfer Protocol](#)
- [SSH Disk Free](#)
- [SSH INodes Free](#)
- [SSH Load Average](#)
- [SSH Meminfo](#)
- [SSH Remote Ping](#)
- [SSH SAN Enclosure](#)
- [SSH SAN Logical Disk](#)
- [SSH SAN Physical Disk](#)
- [SSH SAN System Health](#)
- [SSH Script](#)
- [SSH Script Advanced](#)
- [VMware Host Hardware \(WBEM\)](#)

## Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

inherit from

**User Name** ⓘ

johnqpublic

**Authentication Method** ⓘ

Password (default)

Private key

**Password** ⓘ

.....

**WBEM Protocol** ⓘ

HTTP

HTTPS (default)

**WBEM Port** ⓘ

Default

Custom

**SSH Port** ⓘ

22

**SSH Rights Elevation** ⓘ

Run the command as the connecting user (default)

Run the command as a different user using 'sudo' (with password)









Run the command as a different user using 'sudo' (without password)

Run the command as a different user using 'su'

**SSH Connection Mode** ⓘ



Default

Compatibility mode (deprecated)

Setting	Description
User Name	Enter the user name for access to the Linux/Solaris/macOS system via Secure Shell (SSH) and Web-based Enterprise Management (WBEM). Usually, you use credentials with administrator rights.
Authentication Method	<p>Select the authentication method for the login:</p> <ul style="list-style-type: none"> <li>▪ Password (default): Provide the password for the login.</li> <li>▪ Private key: Provide an RSA private key for authentication.</li> </ul> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For more information, see section <a href="#">Monitoring via SSH</a><sup>[3007]</sup>.</p>
Password	<p>This setting is only visible if you select Password (default) above.</p> <p>Enter a password for access to the Linux/Solaris/macOS system via SSH and WBEM. Usually, you use credentials with administrator rights.</p>
Private Key	<p>This setting is only visible if you select Private key above.</p> <p>Paste the entire RSA private key, including the <b>BEGIN</b> and <b>END</b> lines. Make sure that a corresponding public key exists on the target device.</p> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For more information, see section <a href="#">Monitoring via SSH</a><sup>[3007]</sup>.</p> <p> If you do not insert a private key for the first time but if you want to <a href="#">change</a> the private key, you need to <a href="#">restart the PRTG core server service</a><sup>[2919]</sup> for the private key change to take effect.</p>
WBEM Protocol	<p>Select the protocol that you want to use for the connection to the system via WBEM:</p> <ul style="list-style-type: none"> <li>▪ HTTP: Use an unsecure connection for WBEM.</li> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection for WBEM.</li> </ul> <p> This setting is only relevant if you use WBEM sensors.</p>
WBEM Port	Select if you want to use one of the default ports for the connection to the system via WBEM or if you want to set a custom port:



Setting	Description
	<ul style="list-style-type: none"> <li>▪ Default: Use one of the default ports. The default port for unsecure connections is <a href="#">5988</a> and the default port for secure connections is <a href="#">5989</a>.</li> <li>▪ Custom: Use a custom port.</li> </ul> <p><b>i</b> This setting is only relevant if you use WBEM sensors.</p>
Custom WBEM Port	<p>This setting is only visible if you select Custom above.</p> <p>Enter a custom WBEM port. Enter an integer.</p>
SSH Port	<p>Enter the port for SSH connections. Enter an integer. The default port is <a href="#">22</a>.</p> <p><b>i</b> By default, PRTG automatically uses this setting for all <a href="#">SSH sensors</a> unless you define a different port number in the sensor settings.</p>
SSH Rights Elevation	<p>Select the rights that you want to use to run the command on the target system:</p> <ul style="list-style-type: none"> <li>▪ Run the command as the connecting user (default): Use the rights of the user who establishes the SSH connection.</li> <li>▪ Run the command as a different user using 'sudo' (with password): Use the rights of a different user with a password required for <a href="#">sudo</a> to run commands on the target system, for example, as a root user.</li> <li>▪ Run the command as a different user using 'sudo' (without password): Use the rights of a different user without a password required for <a href="#">sudo</a> to run commands on the target system, for example, as a root user.</li> <li>▪ Run the command as a different user using 'su': Use the rights of a different user with <a href="#">su</a> to run commands on the target system.</li> </ul>
Target System User Name	<p>This setting is only visible if you select an option that includes <a href="#">sudo</a> or <a href="#">su</a> above.</p> <p>Enter a user name to run the specified command on the target system as a different user than the root user. If you leave this field empty, you run the command as a root user. Make sure that you set the Linux password even if you use a public key or a private key for authentication. This is not necessary if the user is allowed to run the command without a password.</p>
Password	<p>This setting is only visible if you select an option that includes <a href="#">sudo</a> or <a href="#">su</a> with password above.</p> <p>Enter the password to run the <a href="#">sudo</a> command or the <a href="#">su</a> command.</p>

Setting	Description
SSH Connection Mode	<p>Select the connection mode that you want to use to <a href="#">access data with SSH sensors</a> <sup>6007</sup>.</p> <ul style="list-style-type: none"> <li>▪ Default: This is the default connection mode for SSH sensors. It provides the best performance and security.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default connection mode does not work on the target system. The compatibility mode is the connection mode that PRTG used in previous versions and it is deprecated.</li> </ul> <p> We strongly recommend that you use the default connection mode.</p> <p> You can also individually select the connection mode for each SSH sensor in the sensor settings.</p>

## Credentials for VMware/XenServer

Click  to interrupt the [inheritance](#) <sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [Citrix XenServer Host](#)
- [Citrix XenServer Virtual Machine](#)
- [VMware Datastore \(SOAP\)](#)
- [VMware Host Hardware \(WBEM\)](#)
- [VMware Host Hardware Status \(SOAP\)](#)
- [VMware Host Performance \(SOAP\)](#)
- [VMware Virtual Machine \(SOAP\)](#)

## Credentials for VMware/XenServer

inherit from

User Name i

johnqpublic

Password i

.....

VMware Protocol i

HTTPS (default)

HTTP

Credentials for VMw are/XenServer

Setting	Description
User Name	Enter the user name for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.
Password	Enter the password for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.  <span>i</span> Single sign-on (SSO) passwords for vSphere do not support special characters. For more information, see the VMware sensors sections.
VMware Protocol	Select the protocol for the connection to VMware ESXi, vCenter Server, or Citrix XenServer: <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
Session Handling	Select if you want to reuse a session for VMware sensors:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Reuse a session for multiple scans (default): Select this option if you want a VMware sensor to reuse a single session for multiple sensor scans to query data. With this option, the sensor does not need to log in and out for each sensor scan. We recommend that you use this option because it reduces network load and log entries on the target device. This can increase performance.</li> <li>▪ Create a new session for each scan: If you select this option, PRTG does not reuse a session and a VMware sensor has to log in and out for each sensor scan. This can decrease performance.</li> </ul>

## Credentials for SNMP Devices

Click  to interrupt the [inheritance](#) 136.

 The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">Cisco IP SLA</a></li> <li>▪ <a href="#">SNMP APC Hardware</a></li> <li>▪ <a href="#">SNMP Buffalo TS System Health</a></li> <li>▪ <a href="#">SNMP Cisco ADSL</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Connections</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Traffic</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Users</a></li> <li>▪ <a href="#">SNMP Cisco CBQoS</a></li> <li>▪ <a href="#">SNMP Cisco System Health</a></li> <li>▪ <a href="#">SNMP Cisco UCS Blade</a></li> <li>▪ <a href="#">SNMP Cisco UCS Chassis</a></li> <li>▪ <a href="#">SNMP Cisco UCS Physical Disk</a></li> <li>▪ <a href="#">SNMP Cisco UCS System Health</a></li> <li>▪ <a href="#">SNMP CPU Load</a></li> <li>▪ <a href="#">SNMP Custom</a></li> <li>▪ <a href="#">SNMP Custom Advanced</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">SNMP Fujitsu System Health v2</a></li> <li>▪ <a href="#">SNMP Hardware Status</a></li> <li>▪ <a href="#">SNMP HP LaserJet Hardware</a></li> <li>▪ <a href="#">SNMP HPE BladeSystem Blade</a></li> <li>▪ <a href="#">SNMP HPE BladeSystem Enclosure Health</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Logical Disk</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Memory Controller</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Network Interface</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Physical Disk</a></li> <li>▪ <a href="#">SNMP HPE ProLiant System Health</a></li> <li>▪ <a href="#">SNMP IBM System X Logical Disk</a></li> <li>▪ <a href="#">SNMP IBM System X Physical Disk</a></li> <li>▪ <a href="#">SNMP IBM System X Physical Memory</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">SNMP NetApp Enclosure</a></li> <li>▪ <a href="#">SNMP NetApp I/O</a></li> <li>▪ <a href="#">SNMP NetApp License</a></li> <li>▪ <a href="#">SNMP NetApp Logical Unit</a></li> <li>▪ <a href="#">SNMP NetApp Network Interface</a></li> <li>▪ <a href="#">SNMP NetApp System Health</a></li> <li>▪ <a href="#">SNMP Nutanix Cluster Health</a></li> <li>▪ <a href="#">SNMP Nutanix Hypervisor</a></li> <li>▪ <a href="#">SNMP Poseidon Environment</a></li> <li>▪ <a href="#">SNMP Printer</a></li> <li>▪ <a href="#">SNMP QNAP Logical Disk</a></li> <li>▪ <a href="#">SNMP QNAP Physical Disk</a></li> <li>▪ <a href="#">SNMP QNAP System Health</a></li> <li>▪ <a href="#">SNMP Rittal CMC III Hardware Status</a></li> <li>▪ <a href="#">SNMP RMON</a></li> <li>▪ <a href="#">SNMP SonicWall System Health</a></li> <li>▪ <a href="#">SNMP SonicWall VPN Traffic</a></li> </ul>
---	---	--

<ul style="list-style-type: none"><li>▪ <a href="#">SNMP Custom String</a></li><li>▪ <a href="#">SNMP Custom String Lookup</a></li><li>▪ <a href="#">SNMP Custom Table</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Logical Disk</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Member Health</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Physical Disk</a></li><li>▪ <a href="#">SNMP Dell Hardware</a></li><li>▪ <a href="#">SNMP Dell PowerEdge Physical Disk</a></li><li>▪ <a href="#">SNMP Dell PowerEdge System Health</a></li><li>▪ <a href="#">SNMP Disk Free</a></li></ul>	<ul style="list-style-type: none"><li>▪ <a href="#">SNMP IBM System X System Health</a></li><li>▪ <a href="#">SNMP interSeptor Pro Environment</a></li><li>▪ <a href="#">SNMP Juniper NS System Health</a></li><li>▪ <a href="#">SNMP LenovoEMC Physical Disk</a></li><li>▪ <a href="#">SNMP LenovoEMC System Health</a></li><li>▪ <a href="#">SNMP Library</a></li><li>▪ <a href="#">SNMP Linux Disk Free</a></li><li>▪ <a href="#">SNMP Linux Load Average</a></li><li>▪ <a href="#">SNMP Linux Meminfo</a></li><li>▪ <a href="#">SNMP Linux Physical Disk</a></li><li>▪ <a href="#">SNMP Memory</a></li><li>▪ <a href="#">SNMP NetApp Disk Free</a></li></ul>	<ul style="list-style-type: none"><li>▪ <a href="#">SNMP Synology Logical Disk</a></li><li>▪ <a href="#">SNMP Synology Physical Disk</a></li><li>▪ <a href="#">SNMP Synology System Health</a></li><li>▪ <a href="#">SNMP System Uptime</a></li><li>▪ <a href="#">SNMP Traffic</a></li><li>▪ <a href="#">SNMP Trap Receiver</a></li><li>▪ <a href="#">SNMP Windows Service</a></li></ul>
--	--	--

## Credentials for SNMP Devices

inherit from

**SNMP Version** ⓘ

SNMP v1

SNMP v2c (default)

SNMP v3

**Community String** ⓘ

public

**SNMP Port** ⓘ

161





**Timeout (Sec.)** ⓘ

5

Credentials for SNMP Devices

Setting	Description
SNMP Version	<p>Select the Simple Network Management Protocol (SNMP) version for the connection to the target SNMP device:</p> <ul style="list-style-type: none"> <li>SNMP v1: Use SNMP v1 for the connection. SNMP v1 only offers clear-text data transmission. <ul style="list-style-type: none"> <li>ⓘ SNMP v1 does not support 64-bit counters. This might result in invalid data when you monitor traffic via SNMP.</li> </ul> </li> <li>SNMP v2c (default): Use SNMP v2c for the connection. SNMP v2c also only offers clear-text data transmission but it supports 64-bit counters.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ SNMP v3: Use SNMP v3 for the connection. SNMP v3 provides secure authentication and data encryption.</li> <li>ⓘ SNMP v3 has performance limitations because of the use of encryption. The main limiting factor is CPU power. Also keep in mind that SNMP v3, unlike SNMP v1 and v2c, does not scale with more CPU power. Because of this limitation, PRTG can only handle a limited number of requests per second so that you can use only a limited number of sensors using SNMP v3. If you see an increase in <a href="#">Interval Delay</a> or <a href="#">Open Requests</a> with the <a href="#">Probe Health</a> sensor, distribute the load over <a href="#">multiple probes</a> <sup>[6198]</sup>. SNMP v1 and SNMP v2c do not have this limitation.</li> </ul>
Community String	<p><a href="#">This setting is only visible if you select SNMP v1 or SNMP v2c (default) above.</a></p> <p>Enter the community string of your device. This is like a clear-text password for simple authentication.</p> <p>ⓘ We recommend that you use the default value.</p>
Authentication Method	<p><a href="#">This setting is only visible if you select SNMP v3 above.</a></p> <p>Select the authentication method:</p> <ul style="list-style-type: none"> <li>▪ MD5 (default): Use message-digest algorithm 5 (MD5) for authentication.</li> <li>▪ SHA: Use Secure Hash Algorithm (SHA) for authentication.</li> <li>▪ SHA-224: Use SHA-224 for authentication.</li> <li>▪ SHA-256: Use SHA-256 for authentication.</li> <li>▪ SHA-384: Use SHA-384 for authentication.</li> <li>▪ SHA-512: Use SHA-512 for authentication.</li> </ul> <p>ⓘ If you do not want to use authentication but you need SNMP v3, for example, because your device requires <a href="#">context</a>, you can leave the Password field empty. In this case, PRTG uses <a href="#">SNMP_SEC_LEVEL_NOAUTH</a> and it entirely deactivates authentication.</p> <p>ⓘ The authentication method that you select must match the authentication method of your device.</p>
User Name	<p><a href="#">This setting is only visible if you select SNMP v3 above.</a></p> <p>Enter the user name for access to the target SNMP device.</p> <p>ⓘ The user name that you enter must match the user name of your device.</p>

Setting	Description
Password	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter the password for access to the target SNMP device.</p> <p> The password that you enter must match the password of your device.</p>
Encryption Type	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Select an encryption type:</p> <ul style="list-style-type: none"> <li>▪ DES (default): Use Data Encryption Standard (DES) as the encryption algorithm.</li> <li>▪ AES: Use Advanced Encryption Standard (AES) as the encryption algorithm.</li> <li>▪ AES-192: Use AES-192 as the encryption algorithm.</li> <li>▪ AES-256: Use AES-256 as the encryption algorithm.</li> </ul> <p> The encryption type that you select must match the encryption type of your device.</p>
Encryption Key	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter an encryption key. If you provide a key, PRTG encrypts SNMP data packets with the encryption algorithm that you selected above. Enter a string or leave the field empty.</p> <p> The encryption key that you enter must match the encryption key of your device. If the encryption keys do not match, you do not get an error message.</p>
Context Name	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter a context name only if the configuration of the device requires it. <b>Context</b> is a collection of management information that is accessible by an SNMP device. Enter a string.</p>
SNMP Port	<p>Enter the port for the connection to the SNMP target device. Enter an integer. The default port is <b>161</b>.</p> <p> We recommend that you use the default value.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).</p>




## Credentials for Database Management Systems


Click  to interrupt the [inheritance](#) .

 The settings you define in this section apply to the following sensors:

- [ADO SQL v2](#)
- [Microsoft SQL v2](#)
- [MySQL v2](#)
- [Oracle SQL v2](#)
- [PostgreSQL](#)


### Credentials for Database Management Systems

 inherit from

**Port** 


Default

Custom port for all database sensors

**Authentication Method** 

Windows authentication with impersonation (default)



SQL server authentication

**Timeout (Sec.)** 

60

Credentials for Database Management Systems

Setting	Description
Port	Select the port that PRTG uses for connections to the monitored databases:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Default: PRTG automatically determines the type of the database and uses the corresponding default port to connect. PRTG uses the following default ports: <ul style="list-style-type: none"> <li>▫ Microsoft SQL: <a href="#">1433</a></li> <li>▫ MySQL: <a href="#">3306</a></li> <li>▫ Oracle SQL: <a href="#">1521</a></li> <li>▫ PostgreSQL: <a href="#">5432</a></li> </ul> </li> <li>▪ Custom port for all database sensors: Select this option if your database management systems do not use the default ports. Enter a custom port for database connections below.</li> </ul>
Custom Port	<p>Enter a custom port for database connections. Enter an integer.</p> <p> PRTG uses this custom port for <a href="#">all</a> database sensors and for connections to <a href="#">all</a> your databases.</p>
Authentication Method	<p>Select the authentication method for the connection to the Structured Query Language (SQL) database:</p> <ul style="list-style-type: none"> <li>▪ Windows authentication with impersonation (default): PRTG uses the Windows credentials that you define in settings that are higher in the <a href="#">object hierarchy</a> <sup>[132]</sup> for the database connection. <ul style="list-style-type: none"> <li> The user whose credentials PRTG uses needs to have permission to log in to the probe system with a database sensor. This is necessary for the impersonation.</li> </ul> </li> <li>▪ SQL server authentication: Use explicit credentials for database connections. Enter a user name and password below.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select SQL server authentication above.</a></p> <p>Enter the user name for the database connection.</p>
Password	<p><a href="#">This setting is only visible if you select SQL server authentication above.</a></p> <p>Enter the password for the database connection.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <a href="#">900</a> seconds (15 minutes).</p>

## Credentials for AWS

Click  to interrupt the [inheritance](#) <sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:

- [AWS Alarm v2](#)
- [AWS Cost](#)
- [AWS EBS v2](#)
- [AWS EC2 v2](#)
- [AWS ELB v2](#)
- [AWS RDS v2](#)

■ For more information about the permissions that are necessary to query the AWS API, see the Knowledge Base: [How do I set permissions for the Amazon Web Services \(AWS\) API key to use certain sensors in PRTG?](#)

## Credentials for AWS

inherit from

**Access Key** ⓘ

---

**Secret Key** ⓘ

---

Credentials for AWS

Setting	Description
Access Key	Enter the Amazon Web Services (AWS) access key.
Secret Key	Enter the AWS secret key.

### Credentials for Microsoft 365

Click to interrupt the [inheritance](#) <sup>136</sup>.

ⓘ The settings you define in this section apply to the following sensors:

- [Microsoft 365 Mailbox](#)
- [Microsoft 365 Service Status](#)
- [Microsoft 365 Service Status Advanced](#)

The sensors use the credentials to authenticate with Microsoft Entra ID.

■ For more information about the credentials and the permissions that are necessary to use the Microsoft 365 Service Status sensor and the Microsoft 365 Service Status Advanced sensor, see the Knowledge Base: [How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?](#)

■ For more information about the credentials and the permissions that are necessary to use the Microsoft 365 Mailbox sensor, see the Knowledge Base: [How do I obtain credentials and set permissions for the Microsoft 365 Mailbox sensor?](#)

### Credentials for Microsoft 365

inherit from

Tenant ID ⓘ

---

Client ID ⓘ

---

Client Secret ⓘ

---

OpenID Connect Configuration ⓘ

Automatic (default)

Manual

Credentials for Microsoft 365

Setting	Description
Tenant ID	Enter the Microsoft Entra tenant ID. <span style="color: red; font-weight: bold;">❗</span> A tenant ID must be a 32-digit sequence in hexadecimal notation.
Client ID	Enter the Microsoft Entra client ID.
Client Secret	Enter the Microsoft Entra client secret.

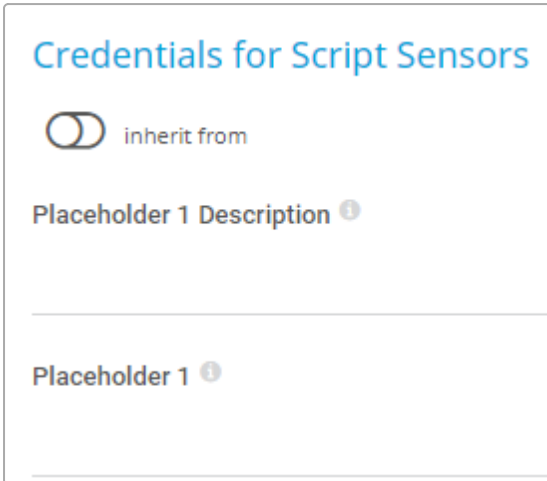
Setting	Description
OpenID Connect Configuration	<p>Select if you want to manually enter the authorization endpoint URL and token endpoint URL that PRTG uses to access Microsoft Graph:</p> <ul style="list-style-type: none"> <li>▪ Automatic (default): PRTG automatically determines the authorization endpoint URL and the token endpoint URL.</li> <li>▪ Manual: Manually enter the authorization endpoint URL and the token endpoint URL.</li> </ul>
Authorization Endpoint	<p>Enter the authorization endpoint URL including the server.</p> <p>Authorization endpoint URL example:</p> <pre>https://login.microsoftonline.com/&lt;tenant-ID&gt;/oauth2/v2.0/authorize</pre> <p><b>i</b> Make sure to replace &lt;tenant-ID&gt; with the <b>directory (tenant) ID</b> from Microsoft Entra ID.</p>
Token Endpoint	<p>Enter the token endpoint URL including the server.</p> <p>Token endpoint URL example:</p> <pre>https://login.microsoftonline.com/&lt;tenant-ID&gt;/oauth2/v2.0/token</pre> <p><b>i</b> Make sure to replace &lt;tenant-ID&gt; with the <b>directory (tenant) ID</b> from Microsoft Entra ID.</p>

## Credentials for Script Sensors

Click  to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

- [EXE/Script](#)
- [EXE/Script Advanced](#)
- [Python Script Advanced](#)
- [Script v2](#)
- [SSH Script](#)
- [SSH Script Advanced](#)



Credentials for Script Sensors

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder1</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder2</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder3</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder4</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.


Setting	Description
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder5</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.

### Credentials for Cisco Meraki

**i** The settings you define in this section apply to the following sensors:

- [Cisco Meraki License](#)
- [Cisco Meraki Network Health](#)

## Credentials for Cisco Meraki


inherit from

API Key **i**
.....

---

Meraki Dashboard API Endpoint **i**
api.meraki.com

Credentials for Cisco Meraki

Setting	Description
API Key	Enter an API key that the sensor uses for authentication against the Cisco Meraki Dashboard API.
Meraki Dashboard API Endpoint	Enter the endpoint for the Cisco Meraki Dashboard API. The default <a href="#">api.meraki.com</a> should be valid for most use cases.  <b>i</b> See the Cisco Meraki Dashboard API documentation for other possible choices.


### Credentials for Dell EMC

**i** The settings you define in this section apply to the following sensors:

- [Dell EMC Unity Enclosure Health v2](#)
- [Dell EMC Unity File System v2](#)
- [Dell EMC Unity Storage Capacity v2](#)

- [Dell EMC Unity Storage LUN v2](#)
- [Dell EMC Unity Storage Pool v2](#)
- [Dell EMC Unity VMware Datastore v2](#)

## Credentials for Dell EMC

 inherit from

**User Name** i

---

**Password** i

---

**Port** i

Credentials for Dell EMC

Setting	Description
User Name	Enter the user name for access to the Dell EMC system.
Password	Enter the password for access to the Dell EMC system.
Port	Enter the port for the connection to the Dell EMC system. The default port for secure connections is <a href="#">443</a> .

### Credentials for FortiGate

i The settings you define in this section apply to the following sensors:

- [FortiGate System Statistics](#)
- [FortiGate VPN Overview](#)



### Credentials for FortiGate

inherit from

API Token ⓘ

---

Port ⓘ

443

Credentials for FortiGate

Setting	Description
API Token	Enter the API token for access to the FortiGate system.
Port	Enter the port for the connection to the FortiGate system. The default port for secure connections is <a href="#">443</a> .

### Credentials for HPE 3PAR

ⓘ The settings you define in this section apply to the following sensors:

- [HPE 3PAR Common Provisioning Group](#)
- [HPE 3PAR Drive Enclosure](#)
- [HPE 3PAR Virtual Volume](#)

## Credentials for HPE 3PAR

inherit from

User Name <sup>i</sup>

johnqpulic

Password <sup>i</sup>

●●●●●●●●●●●●●●●●

Protocol <sup>i</sup>

HTTPS (default)

HTTP

WSAPI Port <sup>i</sup>

8080

SSH Port <sup>i</sup>

22

Credentials for HPE 3PAR

Setting	Description
User Name	Enter the user name for access to the HPE 3PAR system.

Setting	Description
Password	Enter the password for access to the HPE 3PAR system.
Protocol	<p>Select the protocol that you want to use for the connection to the HPE 3PAR system:</p> <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
WSAPI Port	<p>Enter the Web Services API (WSAPI) port for the connection to the HPE 3PAR system. The default port for secure connections is <b>8080</b> and the default port for unsecure connections is <b>8008</b>.</p> <p><b>i</b> For more information, see the Knowledge Base: <a href="#">Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?</a></p>
SSH Port	Enter the SSH port for the connection to the HPE 3PAR system. The default port for secure connections is <b>22</b> .

### Credentials for HTTP

**i** The settings you define in this section apply to the following sensor:

- [HTTP v2](#)

### Credentials for HTTP

inherit from

**Authentication Method** ⓘ

None (default)

Basic authentication

Bearer authentication

**Placeholder 1 Description** ⓘ

---

**Placeholder 1** ⓘ

---

Credentials for HTTP

Setting	Description
Authentication Method	<p>Select the authentication method for access to the server:</p> <ul style="list-style-type: none"> <li>▪ None (default): Use no authentication.</li> <li>▪ Basic authentication: Use basic authentication.</li> <li>▪ Bearer authentication: Use an OAuth2 bearer token.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter the user name for access to the server.</p>
Password	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter the password for access to the server.</p>
Bearer Token	<p><a href="#">This setting is only visible if you select Bearer authentication above.</a></p> <p>Enter a bearer token for access to the server.</p>

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder1</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder2</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder3</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder4</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder5</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.

## Credentials for Microsoft Azure

**i** The settings you define in this section apply to the following sensors:



- [Microsoft Azure SQL Database](#)
- [Microsoft Azure Storage Account](#)

- [Microsoft Azure Subscription Cost](#)
- [Microsoft Azure Virtual Machine](#)

The sensors use the credentials to authenticate with Microsoft Entra ID.

■ For more information about the credentials and permissions that are necessary use the Microsoft Azure sensors, see the Knowledge Base: [How do I obtain credentials and create custom roles for the Microsoft Azure sensors?](#)

### Credentials for Microsoft Azure

 inherit from  Local Probe

**Tenant ID** ⓘ

---

**Client ID** ⓘ

---


**Client Secret** ⓘ

---


**Subscription ID** ⓘ

---

**Microsoft Azure Management Endpoint** ⓘ

`management.azure.com` 

Credentials for Microsoft Azure

Setting	Description
Tenant ID	Enter the Microsoft Entra tenant ID.  A tenant ID must be a 32-digit sequence in hexadecimal notation.
Client ID	Enter the Microsoft Entra client ID.
Client Secret	Enter the Microsoft Entra client secret.

Setting	Description
Subscription ID	Enter the Microsoft Entra subscription ID.
Microsoft Azure Management Endpoint	<p>The Microsoft Azure API Management endpoint that all sensors on this object connect to. The default endpoint is <a href="https://management.azure.com">management.azure.com</a>.</p> <p><b>i</b> PRTG shows this value for reference purposes only. We strongly recommend that you only change it if the Paessler support team explicitly asks you to do so. Wrong usage can result in incorrect monitoring data.</p>

### Credentials for MQTT

**i** The settings you define in this section apply to the following sensors:

- [MQTT Round Trip](#)
- [MQTT Statistics](#)
- [MQTT Subscribe Custom](#)

## Credentials for MQTT

inherit from

### Authentication Method i

- None (default)
- User name and password

### Port i

1883


### Transport-Level Security i


- Do not use transport-level security (default)
- Use transport-level security

Credentials for MQTT

Setting	Description
Authentication Method	<p>Select if you want to connect without credentials or define credentials for access to the MQTT broker:</p> <ul style="list-style-type: none"> <li>▪ None (default): Connect without credentials.</li> <li>▪ User name and password: Define credentials for the connection.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select User name and password above.</a></p> <p>Enter the user name for access to the Message Queue Telemetry Transport (MQTT) broker.</p>



Setting	Description
Password	<p>This setting is only visible if you select <a href="#">User name and password above</a>.</p> <p>Enter the password for access to the MQTT broker.</p>
Port	<p>Enter the port for the connection to the MQTT broker. The default port for secure connections is <b>8883</b> and the default port for unsecure connections is <b>1883</b>.</p>
Transport-Level Security	<p>Select if you want to use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection:</p> <ul style="list-style-type: none"> <li>▪ Do not use transport-level security (default): Establish the connection without connection security.</li> <li>▪ Use transport-level security: Establish the connection with the strongest SSL/TLS method that the target device provides.</li> </ul>
Server Authentication	<p>This setting is only visible if you select <a href="#">Use transport-level security above</a>.</p> <p>Select if you want to use a certificate for server authentication:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not use a certificate for server authentication.</li> <li>▪ Enable: Use a certificate for server authentication.</li> </ul>
CA Certificate	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Paste the certificate authority (CA) certificate for the verification of the MQTT broker.</p> <p> The certificate must be in Privacy-Enhanced Mail (PEM) format.</p>
Client Authentication	<p>This setting is only visible if you select <a href="#">Use transport-level security above</a>.</p> <p>Select if you want to use a certificate for client authentication:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not use a certificate for client authentication.</li> <li>▪ Enable: Use a certificate for client authentication.</li> </ul>
Client Certificate	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Paste the certificate that you created for authenticating the sensor against the MQTT broker.</p> <p> The certificate must be in PEM format.</p>
Client Key	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Enter the client key for access to the MQTT broker.</p>

Setting	Description
	<p> The client key must be in PEM format and it must be encrypted using the Client Key Password.</p>
Client Key Password	<p>This setting is only visible if you select Enable above.</p> <p>Enter the password for the client key.</p>

## Credentials for NetApp

 The settings you define in this section apply to the following sensors:

- [NetApp Aggregate v2](#)
- [NetApp I/O v2](#)
- [NetApp LIF v2](#)
- [NetApp LUN v2](#)
- [NetApp NIC v2](#)
- [NetApp Physical Disk v2](#)
- [NetApp SnapMirror v2](#)
- [NetApp System Health v2](#)
- [NetApp Volume v2](#)

The sensors use the credentials for access to the ONTAP System Manager.

## Credentials for NetApp

inherit from Network-01f

**User Name** ⓘ  
johnqpublic

---

**Password** ⓘ  
.....

---

**Port** ⓘ  
443

---

**Protocol** ⓘ

HTTPS (default)

HTTP

Credentials for NetApp

Setting	Description
User Name	Enter a user name for access to the ONTAP System Manager.
Password	Enter the password for access to the ONTAP System Manager.
Port	Enter the port for the connection to the ONTAP System Manager. The default port for secure connections is <a href="#">443</a> .

Setting	Description
Protocol	Select the protocol that you want to use for the connection to the ONTAP System Manager: <ul style="list-style-type: none"><li>▪ HTTPS (default): Use HTTPS for the connection.</li><li>▪ HTTP: Use HTTP for the connection.</li></ul>

## Credentials for OPC UA

 The settings you define in this section apply to the following sensors:

- [Beckhoff IPC System Health](#)
- [OPC UA Certificate](#)
- [OPC UA Custom](#)
- [OPC UA Server Status](#)

## Credentials for OPC UA

inherit from

Port <sup>i</sup>

4840

Server Path <sup>i</sup>

Security Mode <sup>i</sup>

None (default)

Sign

Sign & Encrypt



Authentication Method <sup>i</sup>

Anonymous (default)

User name and password

Credentials for OPC UA

Setting	Description
Port	Enter the port for the connection to the OPC Unified Architecture (OPC UA) server. The default port for secure connections is <a href="#">4840</a> .
Server Path	Enter the path of the OPC UA server endpoint if you run more than one server under the same IP address or DNS name.
Security Mode	Select if you want to use encryption: <ul style="list-style-type: none"> <li>▪ None (default): Do not use encryption.</li> <li>▪ Sign: Sign messages between the sensor and the OPC UA server.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Sign &amp; Encrypt: Sign and encrypt messages between the sensor and the OPC UA server.</li> </ul>
Security Policy	<p>This setting is only visible if you select Sign or Sign &amp; Encrypt above.</p> <p>Select if you want to use a security policy and define which policy you want to use:</p> <ul style="list-style-type: none"> <li>▪ None (default): Do not use a security policy.</li> <li>▪ Basic256Sha256: Use the Basic256Sha256 security policy.</li> <li>▪ Basic256: Use the Basic256 security policy.</li> </ul>
Client Certificate	<p>This setting is only visible if you select Sign or Sign &amp; Encrypt above.</p> <p>Enter the certificate that you created for authenticating the sensor against the OPC UA server.</p> <p> The certificate must meet the following requirements:</p> <ul style="list-style-type: none"> <li>▪ The key size must be 2048-bit or 4096-bit.</li> <li>▪ The secure hash algorithm must be <a href="#">SHA256</a>.</li> <li>▪ DataEncipherment must be part of the KeyUsage certificate extension.</li> <li>▪ A uniform resource indicator (URI) must be set in subjectAltName.</li> <li>▪ The certificate must be in Privacy-Enhanced Mail (PEM) format.</li> </ul>
Client Key	<p>This setting is only visible if you select Sign or Sign &amp; Encrypt above.</p> <p>Enter the client key for access to the OPC UA server.</p> <p> The client key must be in PEM format and it must be encrypted using the Client Key Password.</p>
Client Key Password	<p>This setting is only visible if you select Sign or Sign &amp; Encrypt above.</p> <p>Enter the password for the client key.</p>
Authentication Method	<p>Select if you want to connect without credentials or define credentials for access to the OPC UA server:</p> <ul style="list-style-type: none"> <li>▪ Anonymous (default): Connect without credentials.</li> <li>▪ User name and password: Define credentials for the connection.</li> </ul>

Setting	Description
	<p><b>i</b> Most OPC UA servers do not support User name and password authentication without a client certificate. To use User name and password authentication, select Sign or Sign &amp; Encrypt under Security Mode and Basic256Sha256 or Basic256 under Security Policy and enter the Client Certificate, Client Key, and Client Key Password that you want to use.</p> <p><b>i</b> If you select None (default) under Security Mode and use User name and password authentication, PRTG sends the unencrypted password to the OPC UA server.</p>
User Name	<p>This setting is only visible if you select User name and password <a href="#">above</a>.</p> <p>Enter the user name for access to the OPC UA server.</p>
Password	<p>This setting is only visible if you select User name and password <a href="#">above</a>.</p> <p>Enter the password for access to the OPC UA server.</p>

### Credentials for Soffico Orchestra

**i** The settings you define in this section apply to the following sensor:

- [Soffico Orchestra Channel Health](#)
- [Soffico Orchestra Scenario](#)

## Credentials for Soffico Orchestra

inherit from

### Authentication Method i

- None (default)  
 User name and password

### Timeout (Sec.) i

60

### Port i

8443

### Protocol i

- HTTPS (default)  
 HTTP

Credentials for Soffico Orchestra

Setting	Description
Authentication Method	Select if you want to connect without credentials or define credentials for access to the Orchestra platform: <ul style="list-style-type: none"> <li>None (default): Connect without credentials.</li> <li>User name and password: Define credentials for the connection.</li> </ul>
User Name	This setting is only visible if you select User name and password above. Enter the user name for access to the Orchestra platform.
Password	This setting is only visible if you select User name and password above.



Setting	Description
	Enter the password for access to the Orchestra platform.
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).
Port	Enter the port for the connection to the Orchestra platform. The default port for secure connections is <b>8443</b> and the default port for unsecure connections is <b>8019</b> .
Protocol	Select the protocol that you want to use for the connection to the Orchestra platform: <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>

### Credentials for Redfish

**i** The settings you define in this section apply to the following sensors:

- [Redfish Power Supply](#)
- [Redfish System Health](#)
- [Redfish Virtual Disk](#)

### Credentials for Redfish

inherit from

**User Name** ⓘ

johnqpublic

---

**Password** ⓘ

●●●●●●●●

---

**Protocol** ⓘ

HTTPS (default)

HTTP

**Port** ⓘ

443

Credentials for Redfish

Setting	Description
User Name	Enter the user name for access to the Redfish system.
Password	Enter the password for access to the Redfish system.
Protocol	<p>Select the protocol that you want to use for the connection to the Redfish system:</p> <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
Port	Enter the port for the connection to the Redfish system. The default port for secure connections is 443.

## Credentials for REST API

**i** The settings you define in this section apply to the following sensor:

- [REST Custom v2](#)

### Credentials for REST API

inherit from

**Authentication Method** **i**

None (default)

Basic authentication

Bearer authentication

Credentials for REST API

Setting	Description
Authentication Method	Select the authentication method for access to the Representational State Transfer (REST) application programming interface (API): <ul style="list-style-type: none"> <li>▪ None (default): Use no authentication.</li> <li>▪ Basic authentication: Use basic authentication.</li> <li>▪ Bearer authentication: Use an OAuth2 bearer token.</li> </ul>
User Name	<a href="#">This setting is only visible if you select Basic authentication above.</a> Enter the user name for access to the REST API.
Password	<a href="#">This setting is only visible if you select Basic authentication above.</a> Enter the password for access to the REST API.
Bearer Token	<a href="#">This setting is only visible if you select Bearer authentication above.</a> Enter a bearer token for access to the REST API.
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.


Setting	Description
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder1</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder2</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder3</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder4</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder5</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.

## Credentials for Veeam

**i** The settings you define in this section apply to the following sensors:

- [Veeam Backup Job Status](#)
- [Veeam Backup Job Status Advanced](#)

## Credentials for Veeam

 inherit from

**User Name** i

johnqpublic

---

**Password** i

●●●●●●●●●●●●●●●●

---

**Port** i

9398

Credentials for Veeam

Setting	Description
User Name	Enter the user name for access to the Veeam Backup Enterprise Manager.
Password	Enter the password for access to the Veeam Backup Enterprise Manager.
Port	Enter the port for the connection to the Veeam Backup Enterprise Manager. The default port for secure connections is <a href="#">9398</a> .

### Windows Compatibility Options

Click  to interrupt the [inheritance](#)<sup>136</sup>.

If you experience problems when you monitor via Windows sensors, use the following compatibility options for troubleshooting.

## Windows Compatibility Options

inherit from

### Preferred Data Source <sup>i</sup>

- Performance counters and WMI as fallback
- Performance counters only
- WMI only (default)

### Timeout Method <sup>i</sup>

- Use 1.5x scanning interval (default)
- Set manually

Windows Compatibility Options

Setting	Description
Preferred Data Source	<p><sup>i</sup> This setting only applies to hybrid sensors that use both performance counters and Windows Management Instrumentation (WMI).</p> <p>Define the method that Windows sensors use to query data:</p> <ul style="list-style-type: none"> <li>▪ Performance counters and WMI as fallback: Try to query data via performance counters. If this is not possible, establish a connection via WMI.</li> <li>▪ Performance counters only: Query data via performance counters only. If this is not possible, the sensor returns no data.</li> <li>▪ WMI only (default): Query data via WMI only. If this is not possible, the sensor returns no data.</li> </ul>
Timeout Method	<p>Select the time that the sensor waits for the return of the WMI query before the sensor cancels the query and shows an error message:</p> <ul style="list-style-type: none"> <li>▪ Use 1.5x scanning interval (default): Multiply the scanning interval of the sensor by 1.5 and use the resulting value.</li> <li>▪ Set manually: Manually enter a timeout value.</li> </ul> <p><sup>i</sup> We recommend that you use the default value.</p> <p><sup>i</sup> If you experience ongoing timeout errors, try increasing the timeout value.</p>

Setting	Description
Timeout (Sec.)	<p>This setting is only visible if you select <a href="#">Set manually</a> <a href="#">above</a>.</p> <p>Enter the time the sensor waits for the return of its WMI query before it cancels it and shows an error message. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p>

## SNMP Compatibility Options

Click  to interrupt the [inheritance](#)<sup>136</sup>.

If you experience problems when you monitor via Simple Network Management Protocol (SNMP) sensors, use the following compatibility options for troubleshooting.

## SNMP Compatibility Options

inherit from

SNMP Delay (ms) <sup>i</sup>

0

---

Failed Requests <sup>i</sup>

Retry (default)

Do not retry

Overflow Values <sup>i</sup>

Ignore (default)

Handle overflow values as valid results

Zero Values <sup>i</sup>

Ignore (default)

Handle zero values as valid results for delta sensors

32-bit/64-bit Counters <sup>i</sup>

Use 64-bit counters if available (default)

Use 32-bit counters only

Request Mode <sup>i</sup>

Use multi get (default)

Use single get

Walk Mode <sup>i</sup>







Use GETBULK requests (default)




Use GETNEXT requests



Setting	Description
SNMP Delay (ms)	<p>Enter the time in milliseconds (ms) that PRTG waits between two SNMP requests. You can define a delay between 0 and 100. Enter an integer.</p> <ul style="list-style-type: none"> <li><span data-bbox="485 450 512 488">i</span> We recommend that you use the default value.</li> <li><span data-bbox="536 501 563 539">i</span> If you experience SNMP connection failures, try increasing the delay.</li> </ul>
Failed Requests	<p>Select if an SNMP sensor tries again after a request fails:</p> <ul style="list-style-type: none"> <li><span data-bbox="485 667 496 683">▪</span> <b>Retry (default):</b> Try again if an SNMP request fails. This can prevent false error messages because of temporary timeout failures.</li> <li><span data-bbox="485 757 496 772">▪</span> <b>Do not retry:</b> Do not retry if an SNMP request fails. If you select this option, an SNMP sensor shows a Down status earlier.</li> </ul>
Overflow Values	<p>Select how PRTG handles overflow values. Some devices do not correctly handle internal buffer overflows. This can cause false peaks. PRTG can handle overflow values in two ways:</p> <ul style="list-style-type: none"> <li><span data-bbox="485 981 496 996">▪</span> <b>Ignore (default):</b> Ignore overflow values and do not include them in the monitoring data. We recommend that you use this option.</li> <li><span data-bbox="485 1070 496 1086">▪</span> <b>Handle overflow values as valid results:</b> Regard all overflow values as regular data and include them in the monitoring data.</li> </ul> <p><span data-bbox="485 1144 512 1182">i</span> If you experience problems because of strange peaks in your data graphs, change this option. Peaks might indicate that the target device resets counters without an overflow. PRTG interprets such behavior as overflow that results in data peaks. Select the option Ignore (default) in this case. For more information, see the Knowledge Base: <a href="#">What is the Overflow Values setting in the SNMP Compatibility Options?</a></p>
Zero Values	<p>Select how PRTG handles zero values. Some devices send incorrect zero values. This can cause false peaks. PRTG can handle zero values in two ways:</p> <ul style="list-style-type: none"> <li><span data-bbox="485 1503 496 1518">▪</span> <b>Ignore (default):</b> Ignore zero values and do not include them in the monitoring data. We recommend that you use this option.</li> </ul> <p><span data-bbox="485 1585 512 1624">i</span> If you experience problems, try changing this option.</p> <ul style="list-style-type: none"> <li><span data-bbox="485 1637 496 1653">▪</span> <b>Handle zero values as valid results for delta sensors:</b> Regard all zero values as regular data and include them in the monitoring data.</li> </ul>
32-bit/64-bit Counters	<p>Select the type of traffic counters that PRTG searches for on a device:</p> <ul style="list-style-type: none"> <li><span data-bbox="485 1805 496 1821">▪</span> <b>Use 64-bit counters if available (default):</b> The interface scan uses 64-bit traffic counters, if available. This can avoid buffer overflows in the devices.</li> </ul> <p><span data-bbox="485 1910 512 1948">i</span> We recommend that you use the default value.</p> <p><span data-bbox="536 1962 563 2000">i</span> If you experience problems, try changing this option.</p>

Setting	Description
	<ul style="list-style-type: none"> <li>Use 32-bit counters only: The interface scan always uses 32-bit traffic counters, even if 64-bit counters are available. This can make monitoring more reliable for some devices.</li> </ul>
Request Mode	<p>Select the request method that PRTG uses for SNMP sensors:</p> <ul style="list-style-type: none"> <li>Use multi get (default): Bundle multiple SNMP requests into one request. We recommend that you use this option.</li> </ul> <p><b>i</b> If you experience problems, try changing this option.</p> <ul style="list-style-type: none"> <li>Use single get: Use one request for each SNMP value. This can increase compatibility with older devices.</li> </ul> <p><b>i</b> PRTG uses <a href="#">paging</a> for SNMP requests. This means that if a sensor must query more than 20 object identifiers (OID), it automatically polls the OIDs in packages of 20 OIDs each.</p>
Walk Mode	<p>Select the kind of SNMP walk that PRTG uses for SNMP sensors:</p> <ul style="list-style-type: none"> <li>Use GETBULK requests (default): Request the next <b>x</b> OIDs in one SNMP request. The default value is <b>10</b>. It is dynamic based on the response size.</li> </ul> <p><b>i</b> This option only works with devices that support SNMP as of version v2c. Make sure that you set the correct SNMP Version in the Credentials for SNMP Devices settings of the parent device or inherit it from objects that are higher in the <a href="#">object hierarchy</a><sup>132</sup>.</p> <ul style="list-style-type: none"> <li>Use GETNEXT requests: Request one OID at a time. This can increase compatibility with older devices or with devices that have insufficient SNMP BULKWALK support.</li> </ul>
Port Name Template	<p>Select how PRTG displays the name of SNMP sensors. Enter a template that uses several variables. When you add new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID, several fields with interface descriptions are usually available. They are different for every device and OID. PRTG uses the information in these fields to name the sensors. If a field is empty or if it is not available, PRTG adds an empty string to the name. By default, the port name template is <b>([port]) [ifalias] [ifsensor]</b>, which creates a name like <b>(001) Ethernet1 Traffic</b>. You can use and combine any field names that are available at an OID of your device, for example:</p> <ul style="list-style-type: none"> <li>[port]: The port number of the monitored interface.</li> <li>[ifalias]: The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling.</li> <li>[ifname]: The textual name of the monitored interface as assigned by the local device.</li> <li>[ifdescr]: A textual string containing information about the target device or interface, for example, manufacturer, product name, or version.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ [ifspeed]: An estimate of the monitored interface's current bandwidth (Kbit/s).</li> <li>▪ [ifsensor]: The type of the sensor, this is <a href="#">Traffic</a> or <a href="#">RMON</a>. This helps to differentiate between <a href="#">SNMP Traffic</a> and <a href="#">SNMP RMON</a> sensors.</li> </ul> <p> For more information about SNMP sensor names, see the Knowledge Base: <a href="#">How can I change the defaults for names automatically generated for new SNMP sensors?</a></p>
Port Name Update	<p>Select how PRTG reacts if you change the names of ports in your physical device (for example, a switch or router):</p> <ul style="list-style-type: none"> <li>▪ Keep port names (use this if you edit the names in PRTG) (default): Do not automatically adjust sensor names. This is the best option if you want to manually change names in PRTG.</li> <li>▪ Automatically update sensor names if port names change in the device: If PRTG detects port name changes in your physical device, it tries to automatically adjust the sensor names accordingly.</li> </ul> <p> For more information about automatic name updates, see the Knowledge Base: <a href="#">Automatically update port name and number for SNMP Traffic sensors when the device changes them.</a></p>
Port Identification	<p>Select the field that PRTG uses for SNMP interface identification:</p> <ul style="list-style-type: none"> <li>▪ Automatic identification (default): Try the ifAlias field first to identify an SNMP interface and then try ifDescr. <ul style="list-style-type: none"> <li> PRTG does not automatically try ifName.</li> </ul> </li> <li>▪ Use IfAlias: For most devices, ifAlias is the best field to use for unique interface names.</li> <li>▪ Use IfDescr: Use this option if the port order of your device changes after a restart, and if no ifAlias field is available. For example, this is the best option for Cisco ASA devices. <ul style="list-style-type: none"> <li> If you use this option, it is important that your device returns unique interface names in the ifDescr field.</li> </ul> </li> <li>▪ Use IfName: You can also use this option if no unique ifAlias is available. <ul style="list-style-type: none"> <li> If you use this option, it is important that your device returns unique interface names in the ifName field.</li> </ul> </li> <li>▪ Do not update ports: Use this option to disable the automatic port identification.</li> </ul>
Start Interface Index	<p> This setting only applies to <a href="#">SNMP Traffic sensors</a> and to <a href="#">Cisco IP SLA sensors</a>.</p> <p>Enter the index at which PRTG starts to query the interface range during sensor creation. Enter <b>0</b> for the automatic mode.</p>

Setting	Description
	<p> We recommend that you use the default value.</p>
End Interface Index	<p> This setting only applies to <a href="#">SNMP Traffic sensors</a> and to <a href="#">Cisco IP SLA sensors</a>.</p> <p>Enter the index at which PRTG stops querying the interface range during sensor creation. Enter 0 for the automatic mode.</p> <p> We recommend that you use the default value.</p>

## Proxy Settings

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:


<ul style="list-style-type: none"> <li>▪ <a href="#">AWS Alarm v2</a></li> <li>▪ <a href="#">AWS Cost</a></li> <li>▪ <a href="#">AWS EBS v2</a></li> <li>▪ <a href="#">AWS EC2 v2</a></li> <li>▪ <a href="#">AWS ELB v2</a></li> <li>▪ <a href="#">AWS RDS v2</a></li> <li>▪ <a href="#">Cisco Meraki License</a></li> <li>▪ <a href="#">Cisco Meraki Network Health</a></li> <li>▪ <a href="#">Cloud HTTP v2</a></li> <li>▪ <a href="#">Cloud Ping v2</a></li> <li>▪ <a href="#">Dell EMC Unity Enclosure Health v2</a></li> <li>▪ <a href="#">Dell EMC Unity File System v2</a></li> <li>▪ <a href="#">Dell EMC Unity Storage Capacity v2</a></li> <li>▪ <a href="#">Dell EMC Unity Storage LUN v2</a></li> <li>▪ <a href="#">Dell EMC Unity Storage Pool v2</a></li> <li>▪ <a href="#">Dell EMC Unity VMware Datastore v2</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">HPE 3PAR Common Provisioning Group</a></li> <li>▪ <a href="#">HPE 3PAR Drive Enclosure</a></li> <li>▪ <a href="#">HPE 3PAR Virtual Volume</a></li> <li>▪ <a href="#">HTTP</a></li> <li>▪ <a href="#">HTTP v2</a></li> <li>▪ <a href="#">HTTP Advanced</a></li> <li>▪ <a href="#">HTTP Apache ModStatus PerfStats</a></li> <li>▪ <a href="#">HTTP Apache ModStatus Totals</a></li> <li>▪ <a href="#">HTTP Content</a></li> <li>▪ <a href="#">HTTP Data Advanced</a></li> <li>▪ <a href="#">HTTP Transaction</a></li> <li>▪ <a href="#">Microsoft 365 Mailbox</a></li> <li>▪ <a href="#">Microsoft 365 Service Status</a></li> <li>▪ <a href="#">Microsoft 365 Service Status Advanced</a></li> <li>▪ <a href="#">Microsoft Azure SQL Database</a></li> <li>▪ <a href="#">Microsoft Azure Storage Account</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">NetApp Aggregate v2</a></li> <li>▪ <a href="#">NetApp I/O v2</a></li> <li>▪ <a href="#">NetApp LIF v2</a></li> <li>▪ <a href="#">NetApp LUN v2</a></li> <li>▪ <a href="#">NetApp NIC v2</a></li> <li>▪ <a href="#">NetApp Physical Disk v2</a></li> <li>▪ <a href="#">NetApp SnapMirror v2</a></li> <li>▪ <a href="#">NetApp System Health v2</a></li> <li>▪ <a href="#">NetApp Volume v2</a></li> <li>▪ <a href="#">Redfish Power Supply</a></li> <li>▪ <a href="#">Redfish Virtual Disk</a></li> <li>▪ <a href="#">Redfish Power Supply</a></li> <li>▪ <a href="#">REST Custom</a></li> <li>▪ <a href="#">REST Custom v2</a></li> <li>▪ <a href="#">Soffico Orchestra Channel Health</a></li> <li>▪ <a href="#">Soffico Orchestra Scenario</a></li> <li>▪ <a href="#">Veeam Backup Job Status</a></li> <li>▪ <a href="#">Veeam Backup Job Status Advanced</a></li> </ul>
---	---	---

<ul style="list-style-type: none"> <li>▪ <a href="#">FortiGate System Statistics</a></li> <li>▪ <a href="#">FortiGate VPN Overview</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Microsoft Azure Subscription Cost</a></li> <li>▪ <a href="#">Microsoft Azure Virtual Machine</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Zoom Service Status</a></li> </ul>
---	--	---

The proxy settings determine how a sensor connects to a URL. You can enter data for an HTTP proxy server that sensors use when they connect via HTTP or HTTPS.

- ⓘ This setting only applies to sensors and how they monitor. For more information on how to change the proxy settings for the PRTG core server, see section [Core & Probes](#)<sup>[2888]</sup>.
- ⓘ The [SSL Certificate](#) sensor and the [SSL Security Check](#) sensor do not support HTTP proxies but you can configure connections via SOCKS proxies in the sensors' settings:

### Proxy Settings

 inherit from

**IP Address/DNS Name** ⓘ

192.0.2.0

---

**Port** ⓘ

8080

---

**User Name** ⓘ

johnqpublic




---

**Password** ⓘ

.....

Proxy Settings

Setting	Description
IP Address/DNS Name	Enter the IP address or Domain Name System (DNS) name of the proxy server. If you leave this field empty, sensors do not use a proxy.

Setting	Description
	 PRTG currently supports only HTTP proxies.
Port	Enter the port number of the proxy. The default port is <b>8080</b> . Enter an integer.
User Name	If the proxy requires authentication, enter the user name for the proxy login. Enter a string or leave the field empty.   Only basic authentication is available.
Password	If the proxy requires authentication, enter the password for the proxy login. Enter a string or leave the field empty.   Only basic authentication is available.

### Scanning Interval

Click  to interrupt the [inheritance](#) .


#### Scanning Interval

inherit from

**Scanning Interval** 

60 seconds ▼

---

**If a Sensor Query Fails** 

Set sensor to warning status for 1 interval, then set to down status (default) ▼

Scanning Interval

Setting	Description
Scanning Interval	Select a scanning interval from the dropdown list that determines the amount of time that the sensor waits between two scans: <ul style="list-style-type: none"> <li>▪ 30 seconds</li> <li>▪ 60 seconds</li> <li>▪ 5 minutes</li> <li>▪ 10 minutes</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ 15 minutes</li> <li>▪ 30 minutes</li> <li>▪ 1 hour</li> <li>▪ 4 hours</li> <li>▪ 6 hours</li> <li>▪ 12 hours</li> <li>▪ 24 hours</li> </ul> <p><b>i</b> You can change the available intervals in the <a href="#">system administration</a> [2870] of PRTG Network Monitor.</p>
<p>If a Sensor Scanning Fails</p>	<p>Select the number of scanning intervals that the sensor has time to reach and to check a device again if a sensor scanning fails. Depending on the option that you select, the sensor can try to reach and to check a device again several times before the sensor shows the Down <a href="#">status</a> [181]. This can avoid false alarms if the target device only has temporary issues. For previous scanning intervals with failed requests, the sensor shows the Warning status.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> <li>▪ Set sensor to down status immediately: Set the sensor to the Down status immediately after the first request fails.</li> <li>▪ Set sensor to warning status for 1 interval, then set to down status (default): Set the sensor to the Warning status after the first request fails. If the second request also fails, the sensor shows the Down status.</li> <li>▪ Set sensor to warning status for 2 intervals, then set to down status: Set the sensor to the Down status only after the third request fails.</li> <li>▪ Set sensor to warning status for 3 intervals, then set to down status: Set the sensor to the Down status only after the fourth request fails.</li> <li>▪ Set sensor to warning status for 4 intervals, then set to down status: Set the sensor to the Down status only after the fifth request fails.</li> <li>▪ Set sensor to warning status for 5 intervals, then set to down status: Set the sensor to the Down status only after the sixth request fails.</li> </ul> <p><b>i</b> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval before they show the Down status. It is not possible to immediately set a WMI sensor to the Down status, so the first option does not apply to these sensors. All other options can apply.</p> <p><b>i</b> If you define error limits for a sensor's channels, the sensor immediately shows the Down status. None of the interval options apply.</p>

Setting	Description
	<p><b>i</b> If a channel uses <a href="#">lookup</a> values, the sensor immediately shows the Down status. None of the interval options apply.</p>

### Cluster Monitoring Exclusion

Click  to interrupt the [inheritance](#).

Setting	Description
Exclude Cluster Nodes	<p>This setting is only visible if you have a <a href="#">failover cluster</a>.</p> <p>Sometimes you want to keep a cluster node from monitoring the sensors that run on this probe, group, or device, for example, if a device is not reachable from every cluster node. Select the cluster nodes that you do not want to include in sensor scans. By default, all objects underneath the probe <a href="#">inherit</a> this setting.</p>

### Schedules, Dependencies, and Maintenance Window

**i** You cannot interrupt the inheritance for schedules, dependencies, and maintenance windows. The corresponding settings from the parent objects are always active. However, you can define additional schedules, dependencies, and maintenance windows. They are active at the same time as the parent objects' settings.



## Schedules, Dependencies, and Maintenance Window

inherit from

Schedules, dependencies, and maintenance windows always pause all sensors inside a group or device. This pausing is always inherited to all child objects and the inheritance cannot be disabled. Below you can set additional schedules, dependencies, or maintenance windows that will be used in parallel to any inherited setting.

### Schedule ⓘ

None

### Maintenance Window ⓘ




- Do not set up a one-time maintenance window (default)  
 Set up a one-time maintenance window

### Dependency Type ⓘ

- Use parent (default)  
 Select a sensor

Schedules, Dependencies, and Maintenance Window

Setting	Description
Schedule	<p>Select a schedule from the list. You can use schedules to monitor during a certain time span (days or hours) every week:</p> <ul style="list-style-type: none"> <li>▪ None</li> <li>▪ Saturdays</li> <li>▪ Sundays</li> <li>▪ Weekdays</li> <li>▪ Weekdays Eight-To-Eight (08:00 - 20:00)</li> <li>▪ Weekdays Nights (17:00 - 09:00)</li> <li>▪ Weekdays Nights (20:00 - 08:00)</li> <li>▪ Weekdays Nine-To-Five (09:00 - 17:00)</li> <li>▪ Weekends</li> </ul> <p><b>i</b> You can create schedules, edit schedules, or pause monitoring for a specific time span. For more information, see section <a href="#">Schedules</a> [2848].</p>
Maintenance Window	Select if you want to set up a one-time maintenance window:


Setting	Description
	<ul style="list-style-type: none"> <li>▪ Do not set up a one-time maintenance window (default): Do not set up a one-time maintenance window. Monitoring is always active.</li> <li>▪ Set up a one-time maintenance window: Set up a one-time maintenance window and pause monitoring for the selected object and all child objects. You can define a time span for the pause below.</li> </ul> <p><b>i</b> To cancel an active maintenance window before the defined end date, change the time entry under Maintenance Ends to a date in the past.</p>
Maintenance Begins	<p><b>This setting is only visible if you select</b> Set up a one-time maintenance window <a href="#">above</a>.</p> <p>Use the date time picker to enter the start date and time of the one-time maintenance window.</p>
Maintenance Ends	<p><b>This setting is only visible if you select</b> Set up a one-time maintenance window <a href="#">above</a>.</p> <p>Use the date time picker to enter the end date and time of the one-time maintenance window.</p>
Dependency Type	<p>Select a dependency type. You can use dependencies to pause monitoring for an object depending on the status of a different object:</p> <ul style="list-style-type: none"> <li>▪ Use parent (default): Use the dependency type of the parent object.</li> <li>▪ Select a sensor: Use the dependency type of the parent object. Additionally, pause the current object if a specific sensor is in the Down status or in the Paused status because of another dependency.</li> </ul> <p><b>i</b> You do not trigger a status change by dependency if you manually pause a master sensor or if you pause it by schedule.</p> <p><b>i</b> To test your <a href="#">dependencies</a> , select Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later, all dependent objects are paused. You can check all dependencies under Devices   Dependencies in the main menu bar.</p>
Dependency	<p><b>This setting is only visible if you select</b> Select a sensor <a href="#">above</a>.</p> <p>Click  and use the <a href="#">object selector</a>  to select a sensor on which the current object will depend.</p>
Dependency Delay (Sec.)	<p><b>This setting is only visible if you select</b> Select a sensor <a href="#">above</a>.</p> <p>Define a time span in seconds for the dependency delay.</p>

Setting	Description
	After the master sensor for this dependency returns to the Up status, PRTG additionally delays the monitoring of the dependent objects by the time span you define. This can prevent false alarms, for example, after a server restart or to give systems more time for all services to start. Enter an integer.

## Access Rights

Click  to interrupt the [inheritance](#) <sup>[136]</sup>.

### Access Rights

 inherit from

**User Group Access** ⓘ

User Group	Rights
PRTG Users Group	Write access
Read-only User Group	Read access
SSO User Group	Inherited (No access)

Revert access rights of child objects to "inherited"

Access Rights

Setting	Description
User Group Access	<p>Select the <a href="#">user groups</a><sup>[2912]</sup> that have access to the object. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights:</p> <ul style="list-style-type: none"> <li>▪ Inherited: Inherit the access rights settings of the parent object.</li> <li>▪ No access: Users in this user group cannot see or edit the object. The object neither shows up in lists nor in the device tree. <ul style="list-style-type: none"> <li>ⓘ There is one exception: If a user in this user group has access to a child object, the parent object is visible in the device tree but users in this user group cannot access it.</li> </ul> </li> <li>▪ Read access: Users in this group can see the object and view its monitoring results. They cannot edit any settings.</li> <li>▪ Write access: Users in this group can see the object, view its monitoring results, and edit its settings. They cannot edit its access rights settings.</li> <li>▪ Full access: Users in this group can see the object, view its monitoring results, edit its settings, and edit its access rights settings.</li> </ul> <p>To automatically set all child objects to inherit this object's access rights, select the Revert access rights of child objects to "inherited" option.</p> <p>■ For more information on access rights, see section <a href="#">Access Rights Management</a><sup>[145]</sup>.</p>









## Channel Unit Configuration

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

## Channel Unit Configuration

inherit from

### Channel Unit Types i

 Channel Type	 Unit
Bytes (Bandwidth)	MB 
	Mbit 
	/ sec... 
Bytes (Memory)	GB 
Bytes (Disk)	GB 
Bytes (File)	MB 


Channel Unit Configuration

Setting	Description
Channel Unit Types	<p>For each type of channel, select the unit in which PRTG displays the data. If you define this setting on probe, group, or device level, you can inherit these settings to all sensors underneath. You can set units for the following channel types (if available):</p> <ul style="list-style-type: none"> <li>▪ Bandwidth</li> <li>▪ Memory</li> <li>▪ Disk</li> <li>▪ File</li> <li>▪ Custom</li> </ul> <p><b>i</b> Custom channel types are only available on sensor level.</p> <p><b>i</b> Which channel units are available depends on the sensor type and the available parameters. If no configurable channels are available, this field shows <a href="#">No configurable channels</a>.</p>

### Advanced Network Analysis

Click  to interrupt the [inheritance](#) <sup>136</sup>.

#### Advanced Network Analysis

 inherit from

**Unusual Detection** **i**

Enable (default)  
 Disable

**Similar Sensors Detection** **i**

Enable (default)  
 Disable

**System Information** **i**

Enable (default)  
 Disable

Advanced Network Analysis

Setting	Description
Unusual Detection	<p>Select if you want to use the <a href="#">unusual detection</a> for sensors:</p> <ul style="list-style-type: none"> <li>▪ <b>Enable (default):</b> Activates the unusual detection for this object and, by default, for all objects underneath in the <a href="#">object hierarchy</a>. Sensors that are affected by this setting show the Unusual status if PRTG detects unusual activity.</li> <li>▪ <b>Disable:</b> Does not activate the unusual detection. PRTG ignores unusual values for sensors that are affected by this setting. These sensors do not show the Unusual status.</li> </ul> <p><b>i</b> You can configure the behavior of the unusual detection or completely disable it in the <a href="#">system settings</a>.</p>
Similar Sensors Detection	<p>Select if you want to activate the <a href="#">similar sensors</a> analysis:</p> <ul style="list-style-type: none"> <li>▪ <b>Enable (default):</b> Activates the similar sensors detection for this object and, by default, for all objects underneath in the object hierarchy. PRTG considers all sensors that are affected by this setting during the similarity analysis.</li> <li>▪ <b>Disable:</b> Does not activate the similar sensors detection. PRTG does not consider sensors that are affected by this setting during the similarity analysis.</li> </ul> <p><b>i</b> You can configure the depth of the analysis of the similar sensors detection or completely disable it in the <a href="#">system settings</a>.</p>
System Information	<p>Select if you want to retrieve and show <a href="#">system information</a> for your devices:</p> <ul style="list-style-type: none"> <li>▪ <b>Enable (default):</b> Activates the system information feature for this object and, by default, for all objects underneath in the hierarchy.</li> <li>▪ <b>Disable:</b> Does not activate the system information feature.</li> </ul> <p><b>i</b> The System Information feature is enabled by default. To retrieve the data, PRTG automatically uses the <a href="#">credentials for Windows systems</a> and the <a href="#">credentials for SNMP devices</a> that you entered in the device settings or that the device <a href="#">inherits</a> from a parent object like the root group. Consider this when you monitor devices that are outside of your local network, especially when you use <b>SNMP v1</b> or <b>SNMP v2c</b>, which do not provide encryption.</p> <p><b>☁</b> This setting is not available on the hosted probe of a PRTG Hosted Monitor instance.</p>

## Administrative Probe Settings

Define the IP address to use for outgoing monitoring requests.

- If more than one IP is available on the system, you can specify the IP address that PRTG uses for the outgoing monitoring requests of certain sensors.

- This setting is for sensors that use the following connection types: HTTP, Domain Name System (DNS), File Transfer Protocol (FTP), Internet Message Access Protocol (IMAP), Post Office Protocol version 3 (POP3), port, remote desktop, Simple Mail Transfer Protocol (SMTP), and Simple Network Management Protocol (SNMP).
  - The setting is valid for all monitoring requests that this probe sends.
  - This setting is useful for devices that expect a certain IP address when they are queried.
  - The default setting is auto. PRTG automatically selects an IP address.
- i** This feature does not support all sensors for technical reasons.
- i** If you change this setting, some sensors might stop working. For example, sensors might show the Down status if the selected IP address is blocked on the way to or directly on the target device.

## Administrative Probe Settings

**Outgoing IPv4** **i**

auto

192.0.2.0

192.0.2.1

192.0.2.3

**Outgoing IPv6** **i**

auto

2001:db8:3333:4444:5555:6666:7777:8888



2001:db8:3333:4444:CCCC:DDDD:EEEE:FFFF

2001:db8::1234:5678

Administrative Probe Settings

Setting	Description
Outgoing IPv4	Define the IP address for outgoing requests that use the IPv4 protocol. The list shows all available IP addresses on the system. Choose a specific IP address or select auto.
Outgoing IPv6	Define the IP address for outgoing requests that use the IPv6 protocol. The list shows all available IP addresses on the system. Choose a specific IP address or select auto.




Setting	Description
	<p> For more information, see section <a href="#">IPv6 Support</a><sup>[150]</sup>.</p>
Cluster Connectivity	<p>This setting is only visible if you have a <a href="#">failover cluster</a><sup>[128]</sup>.</p> <p>Define if the remote probe connects to all cluster nodes or only to the primary master node:</p> <ul style="list-style-type: none"> <li>▪ Remote probe sends data only to primary master node: The remote probe only connects to the primary master node. You are not able to review monitoring data on failover nodes. Consider this option if you have bandwidth limitations in your network or if the remote probe cannot access your failover nodes.</li> <li>▪ Remote probe sends data to all cluster nodes: The remote probe connects to all cluster nodes and sends monitoring data to the failover nodes in addition to the primary master node. The remote probe is visible on all of your cluster nodes as soon as it automatically connects to the correct IP addresses and ports of the failover nodes. If the primary master node fails, you can still see monitoring data of the remote probe.</li> </ul> <p> PRTG does not notify you if a remote probe is disconnected from a cluster node. Therefore, explicitly check on a cluster node if remote probes are connected (for example, via the device tree in the PRTG web interface on a cluster node).</p>

### Scheduled Restart Settings

 This setting is not available on the hosted probe of a PRTG Hosted Monitor instance.

## Scheduled Restart Settings

**Restart Options** 

- No scheduled system or service restart
- Scheduled restart of PRTG services
- Scheduled system restart (default)

Scheduled Restart Settings

Setting	Description
Restart Options	<p>Define if you want to schedule an automatic restart:</p> <ul style="list-style-type: none"> <li>▪ No scheduled system or service restart: Do not automatically perform a scheduled restart of services. We recommend that you manually restart the PRTG core server system every few weeks. You can initiate a restart of the PRTG probe service in the <a href="#">Administrative Tools</a> in the PRTG web interface.</li> <li>▪ Scheduled restart of PRTG services: Restart the PRTG probe service on the probe system. If you select this option on the local probe, the PRTG core server service restarts as well. Define a schedule under Restart Schedule.</li> <li>▪ Scheduled system restart (recommended): Define a schedule under Restart Schedule. We recommend that you restart probe systems once a month for best performance.</li> </ul>
Restart Schedule	<p>This setting is only visible if you select a schedule option above.</p> <p>Choose how often you want to restart the PRTG probe service or the probe system:</p> <ul style="list-style-type: none"> <li>▪ Once per week: Select a day and a time below.</li> <li>▪ Once per month (recommended): Select a day of the month and a time below.</li> </ul>
Day	<p>Select a day of the week (<a href="#">Monday</a> to <a href="#">Sunday</a>) or month (<a href="#">1st</a> to <a href="#">30th</a> or <a href="#">Last</a>). If you select Last, PRTG restarts the PRTG core server system on the last day of the month, regardless of how many days the month has.</p>
Time	<p>This setting is only visible if you select a schedule option above.</p> <p>Select a time for the planned restart.</p> <p><b>i</b> You get a Windows warning message 10 minutes before the restart to inform you about the restart if you are logged in to PRTG. The actual restart time can differ by up to 30 minutes from the time you enter here.</p>

**i** Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- <https://kb.paessler.com/en/topic/38083>

Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?

- <https://kb.paessler.com/en/topic/89717>

How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?

- <https://kb.paessler.com/en/topic/88462>

How do I obtain credentials and create custom roles for the Microsoft Azure sensors?

- <https://kb.paessler.com/en/topic/88625>

What is the Overflow Values setting in the SNMP Compatibility Options?

- <https://kb.paessler.com/en/topic/43503>

How can I change the defaults for names automatically generated for new SNMP sensors?

- <https://kb.paessler.com/en/topic/7363>

Automatically update port name and number for SNMP Traffic sensors when the device changes them

- <https://kb.paessler.com/en/topic/25893>










## 7.6 Group Settings

The following settings are available on the Settings tab of a group.

- ❗ This documentation does not refer to the settings of the root group. For more information, see section [Root Group Settings](#)<sup>[420]</sup>.
- ❗ We recommend that you define as many settings as possible in the [root group settings](#)<sup>[420]</sup> so that you can inherit them to all other objects in the [object hierarchy](#)<sup>[132]</sup>.
- ❗ This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.


In this section:

- [Basic Group Settings](#)<sup>[527]</sup>
- [Auto-Discovery Settings](#)<sup>[529]</sup>
- [Location](#)<sup>[535]</sup>
- [Credentials for Windows Systems](#)<sup>[536]</sup>
- [Credentials for Linux/Solaris/macOS \(SSH/WBEM\) Systems](#)<sup>[538]</sup>
- [Credentials for VMware/XenServer](#)<sup>[542]</sup>
- [Credentials for SNMP Devices](#)<sup>[544]</sup>
- [Credentials for Database Management Systems](#)<sup>[549]</sup>
- [Credentials for AWS](#)<sup>[550]</sup>
- [Credentials for Microsoft 365](#)<sup>[551]</sup>
- [Credentials for Script Sensors](#)<sup>[553]</sup>
- [Credentials for Cisco Meraki](#)<sup>[555]</sup>
- [Credentials for Dell EMC](#)<sup>[555]</sup>
- [Credentials for FortiGate](#)<sup>[557]</sup>
- [Credentials for HPE 3PAR](#)<sup>[557]</sup>
- [Credentials for HTTP](#)<sup>[559]</sup>
- [Credentials for Microsoft Azure](#)<sup>[561]</sup>
- [Credentials for MQTT](#)<sup>[563]</sup>
- [Credentials for NetApp](#)<sup>[566]</sup>
- [Credentials for OPC UA](#)<sup>[568]</sup>
- [Credentials for Soffico Orchestra](#)<sup>[571]</sup>
- [Credentials for Redfish](#)<sup>[573]</sup>
- [Credentials for REST API](#)<sup>[575]</sup>
- [Credentials for Veeam](#)<sup>[576]</sup>

- [Windows Compatibility Options](#)  577
- [SNMP Compatibility Options](#)  579
- [Proxy Settings](#)  584
- [Scanning Interval](#)  586
- [Schedules, Dependencies, and Maintenance Window](#)  588
- [Access Rights](#)  590
- [Channel Unit Configuration](#)  591
- [Advanced Network Analysis](#)  593
- [Number of Sensors Limitation](#)  595


## Basic Group Settings

### Basic Group Settings

**Group Name** 


Network Infrastructure


---


**Monitoring Status** 

Started (default)


Paused

**Parent Tags** 

**Tags** 



---

**Priority** 

★ ★ ★ ☆ ☆

Basic Group Settings

Setting	Description
Group Name	<p>Enter a name to identify the group. By default, PRTG shows this name in the <a href="#">device tree</a><sup>[164]</sup>, as well as in <a href="#">alarms</a><sup>[202]</sup>, <a href="#">logs</a><sup>[210]</sup>, <a href="#">notifications</a><sup>[2735]</sup>, <a href="#">reports</a><sup>[2754]</sup>, <a href="#">maps</a><sup>[2776]</sup>, <a href="#">libraries</a><sup>[2738]</sup>, and <a href="#">tickets</a><sup>[213]</sup>.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({}). For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Monitoring Status	<p>Select the monitoring status of the group:</p> <ul style="list-style-type: none"> <li>▪ Started (default): Monitor the group.</li> <li>▪ Paused: Pause monitoring for the group. All sensors on all devices in the group are in the Paused <a href="#">status</a><sup>[227]</sup> until you change this setting.</li> </ul>
Parent Tags	<p>Shows the <a href="#">tags</a><sup>[138]</sup> that this group <a href="#">inherits</a><sup>[138]</sup> from its parent <a href="#">probe</a><sup>[133]</sup>.</p> <p><b>i</b> This setting is for your information only. You cannot change it.</p>
Tags	<p>Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically <a href="#">inherited</a><sup>[138]</sup>.</p> <p><b>i</b> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (&lt;&gt;).</p> <p><b>i</b> For performance reasons, it can take some minutes until you can filter for new tags that you added.</p>
Priority	<p>Select a <a href="#">priority</a><sup>[224]</sup> for the group. This setting determines the position of the group in lists. The highest priority is at the top of a list. You can choose from the lowest priority (★☆☆☆☆) to the highest priority (★★★★★).</p>

## Auto-Discovery Settings

### Auto-Discovery Settings

**Auto-Discovery Level** ⓘ

- No auto-discovery (default)
- Default auto-discovery (recommended)
- Detailed auto-discovery
- Auto-discovery with specific device templates

Auto-Discovery Settings

Setting	Description
Auto-Discovery Level	<p>Select the level of detail for the <a href="#">auto-discovery</a> <sup>254</sup>:</p> <ul style="list-style-type: none"> <li>▪ No auto-discovery: Select this option if you only want to manually create devices and sensors.</li> <li>▪ Standard auto-discovery (default): Create a set of standard sensors for standard monitoring. This option works fine for most installations.</li> <li>▪ Detailed auto-discovery: Create all standard sensors and additional sensors from detailed variants of device templates. As a result, you might get many sensors. This option is suitable for small network segments and whenever you want to monitor the maximum number of sensors available.</li> <li>▪ Auto-discovery with specific device templates: Customize the auto-discovery and select or combine standard, detailed, and custom device templates. Select one or more templates from the Device Templates list.</li> </ul> <p> ⓘ Auto-discoveries can be resource intensive. They are primarily intended for devices on the same network as your probes.</p>
Device Templates	<p><b>This setting is only visible if you select</b> Auto-discovery with specific device templates <a href="#">above</a>.</p> <p>Select one or more device templates by enabling a check box in front of the template name. PRTG uses the device templates that you select for the auto-discovery on the device:</p> <ul style="list-style-type: none"> <li>▪ ADSL</li> <li>▪ Buffalo TeraStation NAS</li> <li>▪ Cisco ASA VPN</li> <li>▪ Cisco Device (Generic)</li> <li>▪ Dell EqualLogic</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Dell MDi Disk</li> <li>▪ DNS Server</li> <li>▪ Environment Jakarta</li> <li>▪ Environment Poseidon</li> <li>▪ FTP Server</li> <li>▪ Generic Device (Ping Only)</li> <li>▪ Generic Device (SNMP Enabled)</li> <li>▪ Generic Device (SNMP Enabled, Detailed)</li> <li>▪ HTTP Web Server</li> <li>▪ Hyper-V Host Server</li> <li>▪ IPMI-enabled Device</li> <li>▪ Juniper NS Device</li> <li>▪ Linux/UNIX Device (SNMP or SSH Enabled)</li> <li>▪ Mail Server (Generic)</li> <li>▪ Mail Server (MS Exchange)</li> <li>▪ Microsoft SharePoint 2010</li> <li>▪ MQTT Round Trip</li> <li>▪ NAS LenovoEMC</li> <li>▪ NAS QNAP</li> <li>▪ NAS Synology</li> <li>▪ NetApp</li> <li>▪ NTP Server</li> <li>▪ OPC UA</li> <li>▪ Printer (Generic)</li> <li>▪ Printer (HP)</li> <li>▪ RDP Server</li> <li>▪ RMON-compatible Device</li> <li>▪ Server (Cisco UCS)</li> <li>▪ Server (Compaq/HP Agents)</li> <li>▪ Server (Dell)</li> <li>▪ Server (Fujitsu)</li> <li>▪ Server (IBM)</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ SNMP Rittal CMC III Hardware Status</li> <li>▪ SonicWall</li> <li>▪ SSL Security Check</li> <li>▪ Switch (Cisco Catalyst)</li> <li>▪ Switch (Cisco IOS Based)</li> <li>▪ Switch (HP Procurve)</li> <li>▪ UNIX/Linux Device</li> <li>▪ UPS Health (APC)</li> <li>▪ UPS Health (Generic)</li> <li>▪ UPS Health (Liebert)</li> <li>▪ VMware ESXi / vCenter Server</li> <li>▪ Web Server</li> <li>▪ Windows (Detailed via WMI)</li> <li>▪ Windows (via Remote PowerShell)</li> <li>▪ Windows (via WMI)</li> <li>▪ Windows IIS (via SNMP)</li> <li>▪ XenServer Hosts</li> <li>▪ XenServer Virtual Machines</li> </ul> <p>Once the auto-discovery is finished, PRTG creates a new <a href="#">ticket</a><sup>[213]</sup> and lists the device templates that it used to create new sensors.</p>
Schedule	<p>Select when PRTG runs the auto-discovery:</p> <ul style="list-style-type: none"> <li>▪ Once (default): Run the auto-discovery only once. PRTG adds new devices and sensors once. If you select this option, you must manually <a href="#">start the auto-discovery</a><sup>[255]</sup>.</li> <li>▪ Hourly: Run the auto-discovery for new devices and sensors every 60 minutes. <ul style="list-style-type: none"> <li>ⓘ Use this option with caution. Frequent auto-discoveries might cause performance issues, in particular when PRTG scans large network segments every hour.</li> </ul> </li> <li>▪ Daily: Run the auto-discovery for new devices and sensors every 24 hours. The first auto-discovery runs immediately. All other discoveries start at the time that you define in the <a href="#">Monitoring</a><sup>[267]</sup> settings, section Auto-Discovery.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Weekly: Run the auto-discovery for new devices and sensors every 7 days. The first auto-discovery runs immediately. All other discoveries start at the time that you define in the Monitoring settings, section Auto-Discovery.</li> </ul> <p><b>i</b> For performance reasons, PRTG sets Schedule to Once (default) on all devices that the scheduled auto-discovery creates.</p>
<p>IP Address Selection Method</p>	<p>Select how you want to define the IP address range for the auto-discovery:</p> <ul style="list-style-type: none"> <li>▪ Class C base IP address with start/end (IPv4) (default): Enter an IPv4 class C address range.</li> <li>▪ List of individual IP addresses and DNS names (IPv4): Enter a list of individual IPv4 addresses or Domain Name System (DNS) names.</li> <li>▪ IP address and subnet (IPv4): Enter an IPv4 address and subnet mask.</li> <li>▪ IP address with octet range (IPv4): Enter an IPv4 address range for every IP octet individually. With this, you can define very customizable IP address ranges.</li> <li>▪ List of individual IP addresses and DNS names (IPv6): Enter a list of individual IPv6 addresses or DNS names.</li> <li>▪ Use computers from the Active Directory (maximum 1000 computers): Search in the Active Directory for computers to perform the auto-discovery. <ul style="list-style-type: none"> <li><b>i</b> Make sure that you specify your Active Directory domain in the <a href="#">Core &amp; Probes</a> settings.</li> </ul> </li> </ul> <p><b>i</b> PRTG can only discover subnets with up to 65,536 IP addresses. If you define a range with a higher number of addresses, the discovery stops before it is completed.</p>
<p>IPv4 Base</p>	<p><b>This setting is only visible if you select Class C base IP address with start/end (IPv4) (default) above.</b></p> <p>Enter a class C network as the IP base for the auto-discovery. Enter the first three octets of an IPv4 address, for example, <b>192.168.0</b>.</p>
<p>IPv4 Range Start</p>	<p><b>This setting is only visible if you select Class C base IP address with start/end (IPv4) (default) above.</b></p> <p>Enter the IP octet of the class C network (specified above) from which PRTG starts the auto-discovery. This completes the IP base to an IPv4 address. For example, enter <b>1</b> to discover from <b>192.168.0.1</b> onwards.</p>
<p>IPv4 Range End</p>	<p><b>This setting is only visible if you select Class C base IP address with start/end (IPv4) (default) above.</b></p>

Setting	Description
	Enter the IP octet of the class C network (specified above) at which PRTG stops the auto-discovery. This completes the IP base to an IPv4 address. For example, enter <b>254</b> to discover up to <b>192.168.0.254</b> .
IPv4/DNS Name List IPv6/DNS Name List	<p>This setting is only visible if you select List of individual IP addresses and DNS names (IPv4) or List of individual IP addresses and DNS names (IPv6) above.</p> <p>Enter a list of IP addresses or DNS names that the auto-discovery scans. Enter each address on a separate line.</p>
IPv4 and Subnet (IPv4)	<p>This setting is only visible if you select IP address and subnet (IPv4) above.</p> <p>Enter an expression in the format address/subnet, for example, <b>192.168.3.0/255.255.255.0</b>. You can also use the short form like <b>192.168.3.0/24</b>. If you want to include multiple addresses and subnets, enter them as a list separated by a comma, for example, <b>192.168.3.0/255.255.255.0, 192.169.0.0/255.255.255.0</b>. PRTG scans the complete host range (without network and broadcast address) that is defined by the IP address and the subnet mask.</p>
IP Address with Octet Range	<p>This setting is only visible if you select IP address with octet range (IPv4) above.</p> <p>Enter an expression in the format <b>a1.a2.a3.a4</b>, where <b>a1</b>, <b>a2</b>, <b>a3</b>, and <b>a4</b> are each a number between 0-255, or a range with two numbers and a hyphen like <b>1-127</b>. PRTG calculates all permutations of all ranges. For example, <b>10.0.1-10.1-100</b> results in 1,000 IP addresses that PRTG scans during the auto-discovery.</p>
Organizational Unit	<p>This setting is only visible if you select Use computers from the Active Directory (maximum 1000 computers) above.</p> <p>Enter an <b>organizational unit (OU)</b> to restrict the Active Directory search to computers that are part of this OU. For top-level OUs, use the distinguished name (DN) format without <b>OU=</b> and without the domain components (DCS). If you leave this field empty, there are not any restrictions.</p> <p>Example:</p> <ul style="list-style-type: none"> <li>For the DN <b>OU=Domain Controllers,DC=example,DC=com</b>, enter only <b>Domain Controllers</b>.</li> </ul> <p>If you have sub-OUs, use the DN format without the leading <b>OU=</b> and without the DCS.</p> <p>Examples:</p>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ For the DN <code>OU=webserver,OU=production,DC=example,DC=com</code>, enter only <code>webserver,OU=production</code>.</li> <li>▪ For the DN <code>OU=intranet,OU=webserver,OU=production,DC=example,DC=com</code>, enter only <code>intranet,OU=webserver,OU=production</code>.</li> </ul> <p><b>i</b> Make sure that the OU contains computer accounts. If the OU is empty, you receive an error message.</p> <p><b>i</b> Do not enter the domain components. PRTG automatically uses the domain components from the domain name you enter in the <a href="#">Core &amp; Probes</a> settings.</p>
Name Resolution	<p>Select how to monitor newly discovered devices. This only affects <a href="#">new devices</a>. This does not change the setting for other devices. Depending on your selection, the IP Address/DNS Name field of an <a href="#">added device</a> shows the DNS name or IP address that PRTG uses to access the target device:</p> <ul style="list-style-type: none"> <li>▪ Use DNS names (default): Monitor newly discovered devices via their DNS names (if available) We recommend that you use this option.</li> <li>▪ Use IP addresses: Monitor newly discovered devices via their IP addresses.</li> </ul> <p><b>i</b> This setting does not affect how PRTG shows the devices in the device tree.</p>
Device Rescan	<p>Select how to handle known devices:</p> <ul style="list-style-type: none"> <li>▪ Skip auto-discovery for existing devices/IP addresses (default): Do not rescan existing devices or IP addresses. PRTG only adds devices with new IP addresses or DNS names. PRTG does not add devices that that already exist in your configuration for example, in other groups. We recommend that you use this option.</li> <li>▪ Perform auto-discovery for existing devices/IP addresses: Rescan devices that have existing IP addresses with every auto-discovery. PRTG adds devices that already exist in other groups to this group and runs the auto-discovery on the newly added devices. <ul style="list-style-type: none"> <li><b>i</b> The auto-discovery does not run on devices that already exist in the group. If you want to run the auto-discovery for these devices, you must manually start the auto-discovery on them.</li> </ul> </li> </ul> <p><b>i</b> In certain cases, the IP resolution might not work and might result in PRTG not adding a device if it has the same local IP address as it does in a different LAN.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#)<sup>[420]</sup> if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#)<sup>[136]</sup>.


## Location

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

**Location**


inherit from

Location (for Geo Maps) <sup>?</sup>



Location

Setting	Description
Location (for Geo Maps)	<p>If you want to use <a href="#">Geo Maps</a><sup>[2731]</sup>, enter a location in the first line. Geographical maps then display objects like devices or groups with a status icon using a color code similar to the <a href="#">sensor status icons</a><sup>[181]</sup> (green–yellow–orange–red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, as PRTG automatically parses latitude and longitude, for example, enter <a href="#">49.452778 11.077778</a>, or <a href="#">enter 49.452778 any 11.077778 text</a>.</p> <p>A minus sign (-) in the first line hides an object from a geographical map. In this case, you can enter location information in line two and following.</p> <p>You can define a specific label for each location. Enter a string denoting the label in the first line and provide the coordinates in the second line. This geographical marker then shows the object with the label in the geographical map.</p>

Setting	Description
	<p> The preview map always has a road map layout regardless of the map layout you set in <a href="#">User Interface</a><sup>[2859]</sup>.</p>

## Credentials for Windows Systems


Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">Active Directory Replication Errors</a></li> <li>▪ <a href="#">Event Log (Windows API)</a></li> <li>▪ <a href="#">Exchange Backup (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database DAG (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mail Queue (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mailbox (PowerShell)</a></li> <li>▪ <a href="#">Exchange Public Folder (PowerShell)</a></li> <li>▪ <a href="#">File</a></li> <li>▪ <a href="#">File Content</a></li> <li>▪ <a href="#">Folder</a></li> <li>▪ <a href="#">Hyper-V Cluster Shared Volume Disk Free</a></li> <li>▪ <a href="#">Hyper-V Host Server</a></li> <li>▪ <a href="#">Hyper-V Virtual Machine</a></li> <li>▪ <a href="#">Hyper-V Virtual Network Adapter</a></li> <li>▪ <a href="#">Hyper-V Virtual Storage Device</a></li> <li>▪ <a href="#">PerfCounter Custom</a></li> <li>▪ <a href="#">PerfCounter IIS Application Pool</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Windows MSMQ Queue Length</a></li> <li>▪ <a href="#">Windows Network Card</a></li> <li>▪ <a href="#">Windows Pagefile</a></li> <li>▪ <a href="#">Windows Physical Disk I/O</a></li> <li>▪ <a href="#">Windows Print Queue</a></li> <li>▪ <a href="#">Windows Process</a></li> <li>▪ <a href="#">Windows SMTP Service Received</a></li> <li>▪ <a href="#">Windows SMTP Service Sent</a></li> <li>▪ <a href="#">Windows System Uptime</a></li> <li>▪ <a href="#">Windows Updates Status (PowerShell)</a></li> <li>▪ <a href="#">WMI Battery</a></li> <li>▪ <a href="#">WMI Custom</a></li> <li>▪ <a href="#">WMI Custom String</a></li> <li>▪ <a href="#">WMI Disk Health</a></li> <li>▪ <a href="#">WMI Event Log</a></li> <li>▪ <a href="#">WMI Exchange Server</a></li> <li>▪ <a href="#">WMI Exchange Transport Queue</a></li> <li>▪ <a href="#">WMI File</a></li> <li>▪ <a href="#">WMI Free Disk Space (Multi Disk)</a></li> <li>▪ <a href="#">WMI HDD Health</a></li> <li>▪ <a href="#">WMI Logical Disk I/O</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">WMI Memory</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2005 (Deprecated)</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2008</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2012</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2014</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2016</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2017</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2019</a></li> <li>▪ <a href="#">WMI Remote Ping</a></li> <li>▪ <a href="#">WMI Security Center</a></li> <li>▪ <a href="#">WMI Service</a></li> <li>▪ <a href="#">WMI Share</a></li> <li>▪ <a href="#">WMI SharePoint Process</a></li> <li>▪ <a href="#">WMI Storage Pool</a></li> <li>▪ <a href="#">WMI Terminal Services (Windows 2008+)</a></li> <li>▪ <a href="#">WMI Terminal Services (Windows XP/Vista/2003)</a></li> <li>▪ <a href="#">WMI UTC Time</a></li> <li>▪ <a href="#">WMI Vital System Data v2</a></li> <li>▪ <a href="#">WMI Volume</a></li> </ul>
--	---	--

<ul style="list-style-type: none"> <li>▪ <a href="#">Share Disk Free</a></li> <li>▪ <a href="#">Windows CPU Load</a></li> <li>▪ <a href="#">Windows IIS Application</a></li> </ul>		<ul style="list-style-type: none"> <li>▪ <a href="#">WSUS Statistics</a></li> </ul>
--	--	---

## Credentials for Windows Systems

 inherit from

**Domain or Computer Name** i

www.example.com

---

**User Name** i

johnqpublic

---

**Password** i

.....

Credentials for Windows Systems

Setting	Description
Domain or Computer Name	<p>Enter the domain or computer name of the user account with which you want to access the Windows system. PRTG uses this account for Windows Management Instrumentation (WMI) sensors and other Windows sensors.</p> <p>If you want to use a Windows local user account on the target device, enter the computer name. If you want to use a Windows domain user account (recommended), enter the domain name. PRTG automatically adds a prefix to use the NT LAN Manager (NTLM) protocol if you do not explicitly define it. Do not leave this field empty.</p>

Setting	Description
User Name	Enter the user name for access to the Windows system. Usually, you use credentials with administrator rights.
Password	Enter the password for access to the Windows system. Usually, you use credentials with administrator rights.

## Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

Click  to interrupt the [inheritance](#) <sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:

- [SFTP Secure File Transfer Protocol](#)
- [SSH Disk Free](#)
- [SSH INodes Free](#)
- [SSH Load Average](#)
- [SSH Meminfo](#)
- [SSH Remote Ping](#)
- [SSH SAN Enclosure](#)
- [SSH SAN Logical Disk](#)
- [SSH SAN Physical Disk](#)
- [SSH SAN System Health](#)
- [SSH Script](#)
- [SSH Script Advanced](#)
- [VMware Host Hardware \(WBEM\)](#)



## Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

inherit from

User Name <sup>i</sup>

johnqpublic

Authentication Method <sup>i</sup>

- Password (default)
- Private key

Password <sup>i</sup>

.....

WBEM Protocol <sup>i</sup>

- HTTP
- HTTPS (default)

WBEM Port <sup>i</sup>

- Default
- Custom

SSH Port <sup>i</sup>









22

SSH Rights Elevation <sup>i</sup>

- Run the command as the connecting user (default)
- Run the command as a different user using 'sudo' (with password)
- Run the command as a different user using 'sudo' (without password)
- Run the command as a different user using 'su'

SSH Connection Mode <sup>i</sup>

- Default
- Compatibility mode (deprecated)

Setting	Description
User Name	Enter the user name for access to the Linux/Solaris/macOS system via Secure Shell (SSH) and Web-based Enterprise Management (WBEM). Usually, you use credentials with administrator rights.
Authentication Method	<p>Select the authentication method for the login:</p> <ul style="list-style-type: none"> <li>▪ Password: Provide the password for the login.</li> <li>▪ Private key: Provide an RSA private key for authentication.</li> </ul> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For more information, see section <a href="#">Monitoring via SSH</a><sup>[3007]</sup>.</p>
Password	<p>This setting is only visible if you select Password above.</p> <p>Enter a password for access to the Linux/Solaris/macOS system via SSH and WBEM. Usually, you use credentials with administrator rights.</p>
Private Key	<p>This setting is only visible if you select Private key above.</p> <p>Paste the entire RSA private key, including the <b>BEGIN</b> and <b>END</b> lines. Make sure that a corresponding public key exists on the target device.</p> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For more information, see section <a href="#">Monitoring via SSH</a><sup>[3007]</sup>.</p> <p> If you do not insert a private key for the first time but if you want to <a href="#">change</a> the private key, you need to <a href="#">restart the PRTG core server service</a><sup>[2919]</sup> for the private key change to take effect.</p>
WBEM Protocol	<p>Select the protocol that you want to use for the connection to the system via WBEM:</p> <ul style="list-style-type: none"> <li>▪ HTTP: Use an unsecure connection for WBEM.</li> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection for WBEM.</li> </ul> <p> This setting is only relevant if you use WBEM sensors.</p>
WBEM Port	Select if you want to use one of the default ports for the connection to the system via WBEM or if you want to set a custom port:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Default: Use one of the default ports. The default port for unsecure connections is <a href="#">5988</a> and the default port for secure connections is <a href="#">5989</a>.</li> <li>▪ Custom: Use a custom port.</li> </ul> <p><b>i</b> This setting is only relevant if you use WBEM sensors.</p>
Custom WBEM Port	<p>This setting is only visible if you select Custom above.</p> <p>Enter a custom WBEM port. Enter an integer.</p>
SSH Port	<p>Enter the port for SSH connections. Enter an integer. The default port is <a href="#">22</a>.</p> <p><b>i</b> By default, PRTG automatically uses this setting for all <a href="#">SSH sensors</a> unless you define a different port number in the sensor settings.</p>
SSH Rights Elevation	<p>Select the rights that you want to use to run the command on the target system:</p> <ul style="list-style-type: none"> <li>▪ Run the command as the connecting user (default): Use the rights of the user who establishes the SSH connection.</li> <li>▪ Run the command as a different user using 'sudo' (with password): Use the rights of a different user with a password required for <a href="#">sudo</a> to run commands on the target system, for example, as a root user.</li> <li>▪ Run the command as a different user using 'sudo' (without password): Use the rights of a different user without a password required for <a href="#">sudo</a> to run commands on the target system, for example, as a root user.</li> <li>▪ Run the command as a different user using 'su': Use the rights of a different user with <a href="#">su</a> to run commands on the target system.</li> </ul>
Target System User Name	<p>This setting is only visible if you select an option that includes <a href="#">sudo</a> or <a href="#">su</a> above.</p> <p>Enter a user name to run the specified command on the target system as a different user than the root user. If you leave this field empty, you run the command as a root user. Make sure that you set the Linux password even if you use a public key or a private key for authentication. This is not necessary if the user is allowed to run the command without a password.</p>
Password	<p>This setting is only visible if you select an option that includes <a href="#">sudo</a> or <a href="#">su</a> with password above.</p> <p>Enter the password to run the <a href="#">sudo</a> command or the <a href="#">su</a> command.</p>

Setting	Description
SSH Connection Mode	<p>Select the connection mode that you want to use to <a href="#">access data with SSH sensors</a> <sup>6007</sup>.</p> <ul style="list-style-type: none"> <li>▪ Default: This is the default connection mode for SSH sensors. It provides the best performance and security.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default connection mode does not work on the target system. The compatibility mode is the connection mode that PRTG used in previous versions and it is deprecated.</li> </ul> <p><b>i</b> We strongly recommend that you use the default connection mode.</p> <p><b>i</b> You can also individually select the connection mode for each SSH sensor in the sensor settings.</p>

### Credentials for VMware/XenServer

Click  to interrupt the [inheritance](#) <sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

- [Citrix XenServer Host](#)
- [Citrix XenServer Virtual Machine](#)
- [VMware Datastore \(SOAP\)](#)
- [VMware Host Hardware \(WBEM\)](#)
- [VMware Host Hardware Status \(SOAP\)](#)
- [VMware Host Performance \(SOAP\)](#)
- [VMware Virtual Machine \(SOAP\)](#)

## Credentials for VMware/XenServer

inherit from

User Name i

johnqpublic

Password i

.....

VMware Protocol i

HTTPS (default)

HTTP

Credentials for VMw are/XenServer

Setting	Description
User Name	Enter the user name for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.
Password	Enter the password for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.  <span>i</span> Single sign-on (SSO) passwords for vSphere do not support special characters. For more information, see the VMware sensors sections.
VMware Protocol	Select the protocol for the connection to VMware ESXi, vCenter Server, or Citrix XenServer: <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
Session Handling	Select if you want to reuse a session for VMware sensors:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Reuse a session for multiple scans (default): Select this option if you want a VMware sensor to reuse a single session for multiple sensor scans to query data. With this option, the sensor does not need to log in and out for each sensor scan. We recommend that you use this option because it reduces network load and log entries on the target device. This can increase performance.</li> <li>▪ Create a new session for each scan: If you select this option, PRTG does not reuse a session and a VMware sensor has to log in and out for each sensor scan. This can decrease performance.</li> </ul>

## Credentials for SNMP Devices

Click  to interrupt the [inheritance](#) 136.

 The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">Cisco IP SLA</a></li> <li>▪ <a href="#">SNMP APC Hardware</a></li> <li>▪ <a href="#">SNMP Buffalo TS System Health</a></li> <li>▪ <a href="#">SNMP Cisco ADSL</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Connections</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Traffic</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Users</a></li> <li>▪ <a href="#">SNMP Cisco CBQoS</a></li> <li>▪ <a href="#">SNMP Cisco System Health</a></li> <li>▪ <a href="#">SNMP Cisco UCS Blade</a></li> <li>▪ <a href="#">SNMP Cisco UCS Chassis</a></li> <li>▪ <a href="#">SNMP Cisco UCS Physical Disk</a></li> <li>▪ <a href="#">SNMP Cisco UCS System Health</a></li> <li>▪ <a href="#">SNMP CPU Load</a></li> <li>▪ <a href="#">SNMP Custom</a></li> <li>▪ <a href="#">SNMP Custom Advanced</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">SNMP Fujitsu System Health v2</a></li> <li>▪ <a href="#">SNMP Hardware Status</a></li> <li>▪ <a href="#">SNMP HP LaserJet Hardware</a></li> <li>▪ <a href="#">SNMP HPE BladeSystem Blade</a></li> <li>▪ <a href="#">SNMP HPE BladeSystem Enclosure Health</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Logical Disk</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Memory Controller</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Network Interface</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Physical Disk</a></li> <li>▪ <a href="#">SNMP HPE ProLiant System Health</a></li> <li>▪ <a href="#">SNMP IBM System X Logical Disk</a></li> <li>▪ <a href="#">SNMP IBM System X Physical Disk</a></li> <li>▪ <a href="#">SNMP IBM System X Physical Memory</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">SNMP NetApp Enclosure</a></li> <li>▪ <a href="#">SNMP NetApp I/O</a></li> <li>▪ <a href="#">SNMP NetApp License</a></li> <li>▪ <a href="#">SNMP NetApp Logical Unit</a></li> <li>▪ <a href="#">SNMP NetApp Network Interface</a></li> <li>▪ <a href="#">SNMP NetApp System Health</a></li> <li>▪ <a href="#">SNMP Nutanix Cluster Health</a></li> <li>▪ <a href="#">SNMP Nutanix Hypervisor</a></li> <li>▪ <a href="#">SNMP Poseidon Environment</a></li> <li>▪ <a href="#">SNMP Printer</a></li> <li>▪ <a href="#">SNMP QNAP Logical Disk</a></li> <li>▪ <a href="#">SNMP QNAP Physical Disk</a></li> <li>▪ <a href="#">SNMP QNAP System Health</a></li> <li>▪ <a href="#">SNMP Rittal CMC III Hardware Status</a></li> <li>▪ <a href="#">SNMP RMON</a></li> <li>▪ <a href="#">SNMP SonicWall System Health</a></li> <li>▪ <a href="#">SNMP SonicWall VPN Traffic</a></li> </ul>
---	---	--

<ul style="list-style-type: none"><li>▪ <a href="#">SNMP Custom String</a></li><li>▪ <a href="#">SNMP Custom String Lookup</a></li><li>▪ <a href="#">SNMP Custom Table</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Logical Disk</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Member Health</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Physical Disk</a></li><li>▪ <a href="#">SNMP Dell Hardware</a></li><li>▪ <a href="#">SNMP Dell PowerEdge Physical Disk</a></li><li>▪ <a href="#">SNMP Dell PowerEdge System Health</a></li><li>▪ <a href="#">SNMP Disk Free</a></li></ul>	<ul style="list-style-type: none"><li>▪ <a href="#">SNMP IBM System X System Health</a></li><li>▪ <a href="#">SNMP interSeptor Pro Environment</a></li><li>▪ <a href="#">SNMP Juniper NS System Health</a></li><li>▪ <a href="#">SNMP LenovoEMC Physical Disk</a></li><li>▪ <a href="#">SNMP LenovoEMC System Health</a></li><li>▪ <a href="#">SNMP Library</a></li><li>▪ <a href="#">SNMP Linux Disk Free</a></li><li>▪ <a href="#">SNMP Linux Load Average</a></li><li>▪ <a href="#">SNMP Linux Meminfo</a></li><li>▪ <a href="#">SNMP Linux Physical Disk</a></li><li>▪ <a href="#">SNMP Memory</a></li><li>▪ <a href="#">SNMP NetApp Disk Free</a></li></ul>	<ul style="list-style-type: none"><li>▪ <a href="#">SNMP Synology Logical Disk</a></li><li>▪ <a href="#">SNMP Synology Physical Disk</a></li><li>▪ <a href="#">SNMP Synology System Health</a></li><li>▪ <a href="#">SNMP System Uptime</a></li><li>▪ <a href="#">SNMP Traffic</a></li><li>▪ <a href="#">SNMP Trap Receiver</a></li><li>▪ <a href="#">SNMP Windows Service</a></li></ul>
--	--	--

## Credentials for SNMP Devices

inherit from

### SNMP Version ?

SNMP v1

SNMP v2c (default)

SNMP v3

### Community String ?

public

### SNMP Port ?

161

### Timeout (Sec.) ?

5

Credentials for SNMP Devices

Setting	Description
SNMP Version	<p>Select the Simple Network Management Protocol (SNMP) version for the connection to the target SNMP device:</p> <ul style="list-style-type: none"> <li>SNMP v1: Use SNMP v1 for the connection. SNMP v1 only offers clear-text data transmission. <ul style="list-style-type: none"> <li><span>?</span> SNMP v1 does not support 64-bit counters. This might result in invalid data when you monitor traffic via SNMP.</li> </ul> </li> <li>SNMP v2c (default): Use SNMP v2c for the connection. SNMP v2c also only offers clear-text data transmission but it supports 64-bit counters.</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ SNMP v3: Use SNMP v3 for the connection. SNMP v3 provides secure authentication and data encryption.</li> <li>ⓘ SNMP v3 has performance limitations because of the use of encryption. The main limiting factor is CPU power. Also keep in mind that SNMP v3, unlike SNMP v1 and v2c, does not scale with more CPU power. Because of this limitation, PRTG can only handle a limited number of requests per second so that you can use only a limited number of sensors using SNMP v3. If you see an increase in <a href="#">Interval Delay</a> or <a href="#">Open Requests</a> with the <a href="#">Probe Health</a> sensor, distribute the load over <a href="#">multiple probes</a><sup>[6198]</sup>. SNMP v1 and SNMP v2c do not have this limitation.</li> </ul>
Community String	<p>This setting is only visible if you select SNMP v1 or SNMP v2c (default) above.</p> <p>Enter the community string of your device. This is like a clear-text password for simple authentication.</p> <p>ⓘ We recommend that you use the default value.</p>
Authentication Method	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Select the authentication method:</p> <ul style="list-style-type: none"> <li>▪ MD5 (default): Use message-digest algorithm 5 (MD5) for authentication.</li> <li>▪ SHA: Use Secure Hash Algorithm (SHA) for authentication.</li> <li>▪ SHA-224: Use SHA-224 for authentication.</li> <li>▪ SHA-256: Use SHA-256 for authentication.</li> <li>▪ SHA-384: Use SHA-384 for authentication.</li> <li>▪ SHA-512: Use SHA-512 for authentication.</li> </ul> <p>ⓘ If you do not want to use authentication but you need SNMP v3, for example, because your device requires <a href="#">context</a>, you can leave the Password field empty. In this case, PRTG uses <a href="#">SNMP_SEC_LEVEL_NOAUTH</a> and it entirely deactivates authentication.</p> <p>ⓘ The authentication method that you select must match the authentication method of your device.</p>
User Name	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter the user name for access to the target SNMP device.</p> <p>ⓘ The user name that you enter must match the user name of your device.</p>

Setting	Description
Password	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter the password for access to the target SNMP device.</p> <p><b>i</b> The password that you enter must match the password of your device.</p>
Encryption Type	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Select an encryption type:</p> <ul style="list-style-type: none"> <li>▪ DES (default): Use Data Encryption Standard (DES) as the encryption algorithm.</li> <li>▪ AES: Use Advanced Encryption Standard (AES) as the encryption algorithm.</li> <li>▪ AES-192: Use AES-192 as the encryption algorithm.</li> <li>▪ AES-256: Use AES-256 as the encryption algorithm.</li> </ul> <p><b>i</b> The encryption type that you select must match the encryption type of your device.</p>
Encryption Key	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter an encryption key. If you provide a key, PRTG encrypts SNMP data packets with the encryption algorithm that you selected above. Enter a string or leave the field empty.</p> <p><b>i</b> The encryption key that you enter must match the encryption key of your device. If the encryption keys do not match, you do not get an error message.</p>
Context Name	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter a context name only if the configuration of the device requires it. <b>Context</b> is a collection of management information that is accessible by an SNMP device. Enter a string.</p>
SNMP Port	<p>Enter the port for the connection to the SNMP target device. Enter an integer. The default port is <b>161</b>.</p> <p><b>i</b> We recommend that you use the default value.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).</p>


## Credentials for Database Management Systems


Click  to interrupt the [inheritance](#) .

 The settings you define in this section apply to the following sensors:

- [ADO SQL v2](#)
- [Microsoft SQL v2](#)
- [MySQL v2](#)
- [Oracle SQL v2](#)
- [PostgreSQL](#)


### Credentials for Database Management Systems

 inherit from

**Port** 


Default

Custom port for all database sensors

**Authentication Method** 

Windows authentication with impersonation (default)



SQL server authentication

**Timeout (Sec.)** 

60

Credentials for Database Management Systems

Setting	Description
Port	Select the port that PRTG uses for connections to the monitored databases:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Default: PRTG automatically determines the type of the database and uses the corresponding default port to connect. PRTG uses the following default ports: <ul style="list-style-type: none"> <li>▫ Microsoft SQL: <a href="#">1433</a></li> <li>▫ MySQL: <a href="#">3306</a></li> <li>▫ Oracle SQL: <a href="#">1521</a></li> <li>▫ PostgreSQL: <a href="#">5432</a></li> </ul> </li> <li>▪ Custom port for all database sensors: Select this option if your database management systems do not use the default ports. Enter a custom port for database connections below.</li> </ul>
Custom Port	<p>Enter a custom port for database connections. Enter an integer.</p> <p> PRTG uses this custom port for <a href="#">all</a> database sensors and for connections to <a href="#">all</a> your databases.</p>
Authentication Method	<p>Select the authentication method for the connection to the Structured Query Language (SQL) database:</p> <ul style="list-style-type: none"> <li>▪ Windows authentication with impersonation (default): PRTG uses the Windows credentials that you define in settings that are higher in the <a href="#">object hierarchy</a><sup>[132]</sup> for the database connection. <ul style="list-style-type: none"> <li> The user whose credentials PRTG uses needs to have permission to log in to the probe system with a database sensor. This is necessary for the impersonation.</li> </ul> </li> <li>▪ SQL server authentication: Use explicit credentials for database connections. Enter a user name and password below.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select SQL server authentication above.</a></p> <p>Enter the user name for the database connection.</p>
Password	<p><a href="#">This setting is only visible if you select SQL server authentication above.</a></p> <p>Enter the password for the database connection.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <a href="#">900</a> seconds (15 minutes).</p>

## Credentials for AWS

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:

- [AWS Alarm v2](#)
- [AWS Cost](#)
- [AWS EBS v2](#)
- [AWS EC2 v2](#)
- [AWS ELB v2](#)
- [AWS RDS v2](#)

■ For more information about the permissions that are necessary to query the AWS API, see the Knowledge Base: [How do I set permissions for the Amazon Web Services \(AWS\) API key to use certain sensors in PRTG?](#)

## Credentials for AWS

inherit from

**Access Key** ⓘ

---

**Secret Key** ⓘ

---

Credentials for AWS

Setting	Description
Access Key	Enter the Amazon Web Services (AWS) access key.
Secret Key	Enter the AWS secret key.

### Credentials for Microsoft 365

Click  to interrupt the [inheritance](#) <sup>136</sup>.

ⓘ The settings you define in this section apply to the following sensors:

- [Microsoft 365 Mailbox](#)
- [Microsoft 365 Service Status](#)
- [Microsoft 365 Service Status Advanced](#)

The sensors use the credentials to authenticate with Microsoft Entra ID.

■ For more information about the credentials and the permissions that are necessary to use the Microsoft 365 Service Status sensor and the Microsoft 365 Service Status Advanced sensor, see the Knowledge Base: [How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?](#)

■ For more information about the credentials and the permissions that are necessary to use the Microsoft 365 Mailbox sensor, see the Knowledge Base: [How do I obtain credentials and set permissions for the Microsoft 365 Mailbox sensor?](#)

### Credentials for Microsoft 365

inherit from

Tenant ID ⓘ

---

Client ID ⓘ

---

Client Secret ⓘ

---

OpenID Connect Configuration ⓘ

Automatic (default)

Manual

Credentials for Microsoft 365

Setting	Description
Tenant ID	Enter the Microsoft Entra tenant ID. <span style="color: red;">ⓘ</span> A tenant ID must be a 32-digit sequence in hexadecimal notation.
Client ID	Enter the Microsoft Entra client ID.
Client Secret	Enter the Microsoft Entra client secret.

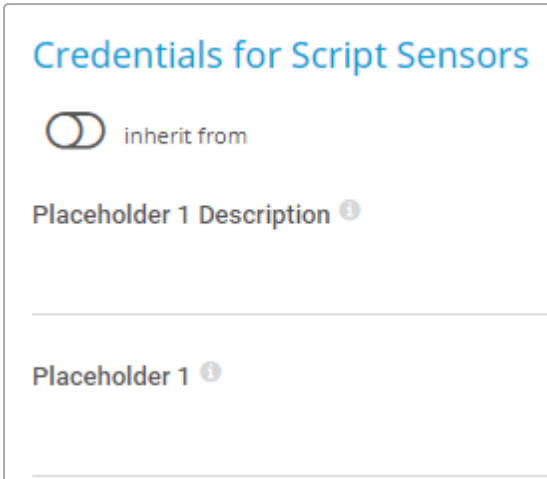
Setting	Description
OpenID Connect Configuration	<p>Select if you want to manually enter the authorization endpoint URL and token endpoint URL that PRTG uses to access Microsoft Graph:</p> <ul style="list-style-type: none"> <li>▪ Automatic (default): PRTG automatically determines the authorization endpoint URL and the token endpoint URL.</li> <li>▪ Manual: Manually enter the authorization endpoint URL and the token endpoint URL.</li> </ul>
Authorization Endpoint	<p>Enter the authorization endpoint URL including the server.</p> <p>Authorization endpoint URL example:</p> <pre>https://login.microsoftonline.com/&lt;tenant-ID&gt;/oauth2/v2.0/authorize</pre> <p><b>i</b> Make sure to replace &lt;tenant-ID&gt; with the <b>directory (tenant) ID</b> from Microsoft Entra ID.</p>
Token Endpoint	<p>Enter the token endpoint URL including the server.</p> <p>Token endpoint URL example:</p> <pre>https://login.microsoftonline.com/&lt;tenant-ID&gt;/oauth2/v2.0/token</pre> <p><b>i</b> Make sure to replace &lt;tenant-ID&gt; with the <b>directory (tenant) ID</b> from Microsoft Entra ID.</p>

## Credentials for Script Sensors

Click  to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

- [EXE/Script](#)
- [EXE/Script Advanced](#)
- [Python Script Advanced](#)
- [Script v2](#)
- [SSH Script](#)
- [SSH Script Advanced](#)



Credentials for Script Sensors

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder1</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder2</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder3</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder4</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.



Setting	Description
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder5</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.


### Credentials for Cisco Meraki


Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:


- [Cisco Meraki License](#)
- [Cisco Meraki Network Health](#)

## Credentials for Cisco Meraki


 inherit from

API Key  .....

---

Meraki Dashboard API Endpoint  `api.meraki.com`

Credentials for Cisco Meraki

Setting	Description
API Key	Enter an API key that the sensor uses for authentication against the Cisco Meraki Dashboard API.
Meraki Dashboard API Endpoint	Enter the endpoint for the Cisco Meraki Dashboard API. The default <a href="#">api.meraki.com</a> should be valid for most use cases.   See the Cisco Meraki Dashboard API documentation for other possible choices.

### Credentials for Dell EMC

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:

- [Dell EMC Unity Enclosure Health v2](#)
- [Dell EMC Unity File System v2](#)
- [Dell EMC Unity Storage Capacity v2](#)
- [Dell EMC Unity Storage LUN v2](#)
- [Dell EMC Unity Storage Pool v2](#)
- [Dell EMC Unity VMware Datastore v2](#)

## Credentials for Dell EMC

inherit from

**User Name** ⓘ

**Password** ⓘ

**Port** ⓘ

Credentials for Dell EMC

Setting	Description
User Name	Enter the user name for access to the Dell EMC system.
Password	Enter the password for access to the Dell EMC system.
Port	Enter the port for the connection to the Dell EMC system. The default port for secure connections is <a href="#">443</a> .


## Credentials for FortiGate


Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [FortiGate System Statistics](#)
- [FortiGate VPN Overview](#)


### Credentials for FortiGate

 inherit from

API Token 

●●●●●●●●

---

Port 

443

Credentials for FortiGate

Setting	Description
API Token	Enter the API token for access to the FortiGate system.
Port	Enter the port for the connection to the FortiGate system. The default port for secure connections is <a href="#">443</a> .

## Credentials for HPE 3PAR

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [HPE 3PAR Common Provisioning Group](#)
- [HPE 3PAR Drive Enclosure](#)
- [HPE 3PAR Virtual Volume](#)

## Credentials for HPE 3PAR

inherit from

User Name <sup>i</sup>

johnqpulic

Password <sup>i</sup>

●●●●●●●●●●●●●●●●

Protocol <sup>i</sup>

HTTPS (default)

HTTP

WSAPI Port <sup>i</sup>

8080

SSH Port <sup>i</sup>

22

Credentials for HPE 3PAR

Setting	Description
User Name	Enter the user name for access to the HPE 3PAR system.

Setting	Description
Password	Enter the password for access to the HPE 3PAR system.
Protocol	Select the protocol that you want to use for the connection to the HPE 3PAR system: <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
WSAPI Port	Enter the Web Services API (WSAPI) port for the connection to the HPE 3PAR system. The default port for secure connections is <b>8080</b> and the default port for unsecure connections is <b>8008</b> .  <i>i</i> For more information, see the Knowledge Base: <a href="#">Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?</a>
SSH Port	Enter the SSH port for the connection to the HPE 3PAR system. The default port for secure connections is <b>22</b> .

### Credentials for HTTP

Click  to interrupt the [inheritance](#)<sup>136</sup>.

*i* The settings you define in this section apply to the following sensor:

- [HTTP v2](#)

### Credentials for HTTP

inherit from

**Authentication Method** ⓘ

None (default)

Basic authentication

Bearer authentication

**Placeholder 1 Description** ⓘ

---

**Placeholder 1** ⓘ

---

Credentials for HTTP

Setting	Description
Authentication Method	<p>Select the authentication method for access to the server:</p> <ul style="list-style-type: none"> <li>▪ None (default): Use no authentication.</li> <li>▪ Basic authentication: Use basic authentication.</li> <li>▪ Bearer authentication: Use an OAuth2 bearer token.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter the user name for access to the server.</p>
Password	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter the password for access to the server.</p>
Bearer Token	<p><a href="#">This setting is only visible if you select Bearer authentication above.</a></p> <p>Enter a bearer token for access to the server.</p>

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder1</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder2</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder3</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder4</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder5</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.

## Credentials for Microsoft Azure

Click  to interrupt the [inheritance](#)<sup>136</sup>.



 The settings you define in this section apply to the following sensors:

- [Microsoft Azure SQL Database](#)
- [Microsoft Azure Storage Account](#)
- [Microsoft Azure Subscription Cost](#)
- [Microsoft Azure Virtual Machine](#)

The sensors use the credentials to authenticate with Microsoft Entra ID.

■ For more information about the credentials and permissions that are necessary use the Microsoft Azure sensors, see the Knowledge Base: [How do I obtain credentials and create custom roles for the Microsoft Azure sensors?](#)

### Credentials for Microsoft Azure

 inherit from  Local Probe

**Tenant ID** ⓘ

---

**Client ID** ⓘ

---


**Client Secret** ⓘ

---


**Subscription ID** ⓘ

---

**Microsoft Azure Management Endpoint** ⓘ

management.azure.com 

Credentials for Microsoft Azure

Setting	Description
Tenant ID	Enter the Microsoft Entra tenant ID.  A tenant ID must be a 32-digit sequence in hexadecimal notation.
Client ID	Enter the Microsoft Entra client ID.



Setting	Description
Client Secret	Enter the Microsoft Entra client secret.
Subscription ID	Enter the Microsoft Entra subscription ID.
Microsoft Azure Management Endpoint	<p>The Microsoft Azure API Management endpoint that all sensors on this object connect to. The default endpoint is <a href="https://management.azure.com">management.azure.com</a>.</p> <p><b>i</b> PRTG shows this value for reference purposes only. We strongly recommend that you only change it if the Paessler support team explicitly asks you to do so. Wrong usage can result in incorrect monitoring data.</p>

## Credentials for MQTT

Click  to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

- [MQTT Round Trip](#)
- [MQTT Statistics](#)
- [MQTT Subscribe Custom](#)

## Credentials for MQTT

inherit from

### Authentication Method i

- None (default)
- User name and password

### Port i

1883


### Transport-Level Security i

- Do not use transport-level security (default)
- Use transport-level security

Credentials for MQTT

Setting	Description
Authentication Method	<p>Select if you want to connect without credentials or define credentials for access to the MQTT broker:</p> <ul style="list-style-type: none"> <li>▪ None (default): Connect without credentials.</li> <li>▪ User name and password: Define credentials for the connection.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select User name and password above.</a></p> <p>Enter the user name for access to the Message Queue Telemetry Transport (MQTT) broker.</p>

Setting	Description
Password	<p>This setting is only visible if you select <a href="#">User name and password above</a>.</p> <p>Enter the password for access to the MQTT broker.</p>
Port	<p>Enter the port for the connection to the MQTT broker. The default port for secure connections is <b>8883</b> and the default port for unsecure connections is <b>1883</b>.</p>
Transport-Level Security	<p>Select if you want to use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection:</p> <ul style="list-style-type: none"> <li>▪ Do not use transport-level security (default): Establish the connection without connection security.</li> <li>▪ Use transport-level security: Establish the connection with the strongest SSL/TLS method that the target device provides.</li> </ul>
Server Authentication	<p>This setting is only visible if you select <a href="#">Use transport-level security above</a>.</p> <p>Select if you want to use a certificate for server authentication:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not use a certificate for server authentication.</li> <li>▪ Enable: Use a certificate for server authentication.</li> </ul>
CA Certificate	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Paste the certificate authority (CA) certificate for the verification of the MQTT broker.</p> <p> The certificate must be in Privacy-Enhanced Mail (PEM) format.</p>
Client Authentication	<p>This setting is only visible if you select <a href="#">Use transport-level security above</a>.</p> <p>Select if you want to use a certificate for client authentication:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not use a certificate for client authentication.</li> <li>▪ Enable: Use a certificate for client authentication.</li> </ul>
Client Certificate	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Paste the certificate that you created for authenticating the sensor against the MQTT broker.</p> <p> The certificate must be in PEM format.</p>
Client Key	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Enter the client key for access to the MQTT broker.</p>

Setting	Description
	 The client key must be in PEM format and it must be encrypted using the Client Key Password.
Client Key Password	<a href="#">This setting is only visible if you select Enable above.</a> Enter the password for the client key.

## Credentials for NetApp

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [NetApp Aggregate v2](#)
- [NetApp I/O v2](#)
- [NetApp LIF v2](#)
- [NetApp LUN v2](#)
- [NetApp NIC v2](#)
- [NetApp Physical Disk v2](#)
- [NetApp SnapMirror v2](#)
- [NetApp System Health v2](#)
- [NetApp Volume v2](#)

The sensors use the credentials for access to the ONTAP System Manager.

## Credentials for NetApp

inherit from Network-01f

**User Name** ⓘ  
johnqpublic

---

**Password** ⓘ  
.....

---

**Port** ⓘ  
443

---

**Protocol** ⓘ

HTTPS (default)

HTTP

Credentials for NetApp

Setting	Description
User Name	Enter a user name for access to the ONTAP System Manager.
Password	Enter the password for access to the ONTAP System Manager.
Port	Enter the port for the connection to the ONTAP System Manager. The default port for secure connections is <a href="#">443</a> .

Setting	Description
Protocol	Select the protocol that you want to use for the connection to the ONTAP System Manager: <ul style="list-style-type: none"><li>▪ HTTPS (default): Use HTTPS for the connection.</li><li>▪ HTTP: Use HTTP for the connection.</li></ul>

## Credentials for OPC UA

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [Beckhoff IPC System Health](#)
- [OPC UA Certificate](#)
- [OPC UA Custom](#)
- [OPC UA Server Status](#)

## Credentials for OPC UA

inherit from

Port <sup>i</sup>

4840

Server Path <sup>i</sup>

Security Mode <sup>i</sup>

None (default)

Sign

Sign & Encrypt



Authentication Method <sup>i</sup>

Anonymous (default)

User name and password

Credentials for OPC UA

Setting	Description
Port	Enter the port for the connection to the OPC Unified Architecture (OPC UA) server. The default port for secure connections is <a href="#">4840</a> .
Server Path	Enter the path of the OPC UA server endpoint if you run more than one server under the same IP address or DNS name.
Security Mode	Select if you want to use encryption: <ul style="list-style-type: none"> <li>▪ None (default): Do not use encryption.</li> <li>▪ Sign: Sign messages between the sensor and the OPC UA server.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Sign &amp; Encrypt: Sign and encrypt messages between the sensor and the OPC UA server.</li> </ul>
Security Policy	<p><a href="#">This setting is only visible if you select Sign or Sign &amp; Encrypt above.</a></p> <p>Select if you want to use a security policy and define which policy you want to use:</p> <ul style="list-style-type: none"> <li>▪ None (default): Do not use a security policy.</li> <li>▪ Basic256Sha256: Use the Basic256Sha256 security policy.</li> <li>▪ Basic256: Use the Basic256 security policy.</li> </ul>
Client Certificate	<p><a href="#">This setting is only visible if you select Sign or Sign &amp; Encrypt above.</a></p> <p>Enter the certificate that you created for authenticating the sensor against the OPC UA server.</p> <p> The certificate must meet the following requirements:</p> <ul style="list-style-type: none"> <li>▪ The key size must be 2048-bit or 4096-bit.</li> <li>▪ The secure hash algorithm must be <a href="#">SHA256</a>.</li> <li>▪ DataEncipherment must be part of the KeyUsage certificate extension.</li> <li>▪ A uniform resource indicator (URI) must be set in subjectAltName.</li> <li>▪ The certificate must be in Privacy-Enhanced Mail (PEM) format.</li> </ul>
Client Key	<p><a href="#">This setting is only visible if you select Sign or Sign &amp; Encrypt above.</a></p> <p>Enter the client key for access to the OPC UA server.</p> <p> The client key must be in PEM format and it must be encrypted using the Client Key Password.</p>
Client Key Password	<p><a href="#">This setting is only visible if you select Sign or Sign &amp; Encrypt above.</a></p> <p>Enter the password for the client key.</p>
Authentication Method	<p>Select if you want to connect without credentials or define credentials for access to the OPC UA server:</p> <ul style="list-style-type: none"> <li>▪ Anonymous (default): Connect without credentials.</li> <li>▪ User name and password: Define credentials for the connection.</li> </ul>



Setting	Description
	<p><b>i</b> Most OPC UA servers do not support User name and password authentication without a client certificate. To use User name and password authentication, select Sign or Sign &amp; Encrypt under Security Mode and Basic256Sha256 or Basic256 under Security Policy and enter the Client Certificate, Client Key, and Client Key Password that you want to use.</p> <p><b>i</b> If you select None (default) under Security Mode and use User name and password authentication, PRTG sends the unencrypted password to the OPC UA server.</p>
User Name	<p>This setting is only visible if you select User name and password <a href="#">above</a>.</p> <p>Enter the user name for access to the OPC UA server.</p>
Password	<p>This setting is only visible if you select User name and password <a href="#">above</a>.</p> <p>Enter the password for access to the OPC UA server.</p>

### Credentials for Soffico Orchestra

Click  to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensor:

- [Soffico Orchestra Channel Health](#)
- [Soffico Orchestra Scenario](#)

## Credentials for Soffico Orchestra

inherit from

### Authentication Method i

- None (default)  
 User name and password

### Timeout (Sec.) i

60

### Port i

8443

### Protocol i

- HTTPS (default)  
 HTTP

Credentials for Soffico Orchestra

Setting	Description
Authentication Method	Select if you want to connect without credentials or define credentials for access to the Orchestra platform: <ul style="list-style-type: none"> <li>None (default): Connect without credentials.</li> <li>User name and password: Define credentials for the connection.</li> </ul>
User Name	<a href="#">This setting is only visible if you select User name and password above.</a> Enter the user name for access to the Orchestra platform.
Password	<a href="#">This setting is only visible if you select User name and password above.</a>

Setting	Description
	Enter the password for access to the Orchestra platform.
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).
Port	Enter the port for the connection to the Orchestra platform. The default port for secure connections is <b>8443</b> and the default port for unsecure connections is <b>8019</b> .
Protocol	Select the protocol that you want to use for the connection to the Orchestra platform: <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>

### Credentials for Redfish

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [Redfish Power Supply](#)
- [Redfish System Health](#)
- [Redfish Virtual Disk](#)

### Credentials for Redfish

inherit from

**User Name** ⓘ

johnqpublic

---

**Password** ⓘ

●●●●●●●●

---

**Protocol** ⓘ

HTTPS (default)

HTTP

**Port** ⓘ

443

Credentials for Redfish

Setting	Description
User Name	Enter the user name for access to the Redfish system.
Password	Enter the password for access to the Redfish system.
Protocol	<p>Select the protocol that you want to use for the connection to the Redfish system:</p> <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
Port	Enter the port for the connection to the Redfish system. The default port for secure connections is 443.

## Credentials for REST API


Click  to interrupt the [inheritance](#) <sup>136</sup>.

 The settings you define in this section apply to the following sensor:

- [REST Custom v2](#)

### Credentials for REST API

inherit from

**Authentication Method** 

None (default)

Basic authentication

Bearer authentication

Credentials for REST API

Setting	Description
Authentication Method	<p>Select the authentication method for access to the Representational State Transfer (REST) application programming interface (API):</p> <ul style="list-style-type: none"> <li>▪ None (default): Use no authentication.</li> <li>▪ Basic authentication: Use basic authentication.</li> <li>▪ Bearer authentication: Use an OAuth2 bearer token.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter the user name for access to the REST API.</p>
Password	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter the password for access to the REST API.</p>
Bearer Token	<p><a href="#">This setting is only visible if you select Bearer authentication above.</a></p> <p>Enter a bearer token for access to the REST API.</p>
Placeholder 1 Description	<p>Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.</p>

Setting	Description
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder1</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder2</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder3</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder4</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder5</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.


## Credentials for Veeam

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [Veeam Backup Job Status](#)
- [Veeam Backup Job Status Advanced](#)

## Credentials for Veeam

 inherit from

**User Name** i

johnqpublic

---

**Password** i

●●●●●●●●●●●●●●●●●●●●

---

**Port** i

9398

Credentials for Veeam

Setting	Description
User Name	Enter the user name for access to the Veeam Backup Enterprise Manager.
Password	Enter the password for access to the Veeam Backup Enterprise Manager.
Port	Enter the port for the connection to the Veeam Backup Enterprise Manager. The default port for secure connections is <a href="#">9398</a> .

### Windows Compatibility Options

Click  to interrupt the [inheritance](#)<sup>136</sup>.

If you experience problems when you monitor via Windows sensors, use the following compatibility options for troubleshooting.

## Windows Compatibility Options

inherit from

### Preferred Data Source <sup>i</sup>

- Performance counters and WMI as fallback
- Performance counters only
- WMI only (default)

### Timeout Method <sup>i</sup>

- Use 1.5x scanning interval (default)
- Set manually

Windows Compatibility Options

Setting	Description
Preferred Data Source	<p><sup>i</sup> This setting only applies to hybrid sensors that use both performance counters and Windows Management Instrumentation (WMI).</p> <p>Define the method that Windows sensors use to query data:</p> <ul style="list-style-type: none"> <li>▪ Performance counters and WMI as fallback: Try to query data via performance counters. If this is not possible, establish a connection via WMI.</li> <li>▪ Performance counters only: Query data via performance counters only. If this is not possible, the sensor returns no data.</li> <li>▪ WMI only (default): Query data via WMI only. If this is not possible, the sensor returns no data.</li> </ul>
Timeout Method	<p>Select the time that the sensor waits for the return of the WMI query before the sensor cancels the query and shows an error message:</p> <ul style="list-style-type: none"> <li>▪ Use 1.5x scanning interval (default): Multiply the scanning interval of the sensor by 1.5 and use the resulting value.</li> <li>▪ Set manually: Manually enter a timeout value.</li> </ul> <p><sup>i</sup> We recommend that you use the default value.</p> <p><sup>i</sup> If you experience ongoing timeout errors, try increasing the timeout value.</p>



Setting	Description
Timeout (Sec.)	<p>This setting is only visible if you select <a href="#">Set manually</a> <a href="#">above</a>.</p> <p>Enter the time the sensor waits for the return of its WMI query before it cancels it and shows an error message. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p>

### SNMP Compatibility Options

Click  to interrupt the [inheritance](#)<sup>136</sup>.

If you experience problems when you monitor via Simple Network Management Protocol (SNMP) sensors, use the following compatibility options for troubleshooting.

## SNMP Compatibility Options

inherit from

SNMP Delay (ms) <sup>i</sup>

0

---

Failed Requests <sup>i</sup>

Retry (default)

Do not retry

Overflow Values <sup>i</sup>

Ignore (default)

Handle overflow values as valid results

Zero Values <sup>i</sup>

Ignore (default)

Handle zero values as valid results for delta sensors

32-bit/64-bit Counters <sup>i</sup>

Use 64-bit counters if available (default)

Use 32-bit counters only

Request Mode <sup>i</sup>

Use multi get (default)

Use single get







Walk Mode <sup>i</sup>




Use GETBULK requests (default)

Use GETNEXT requests

Setting	Description
SNMP Delay (ms)	<p>Enter the time in milliseconds (ms) that PRTG waits between two SNMP requests. You can define a delay between 0 and 100. Enter an integer.</p> <ul style="list-style-type: none"> <li><span data-bbox="485 450 512 488">i</span> We recommend that you use the default value.</li> <li><span data-bbox="536 501 563 539">i</span> If you experience SNMP connection failures, try increasing the delay.</li> </ul>
Failed Requests	<p>Select if an SNMP sensor tries again after a request fails:</p> <ul style="list-style-type: none"> <li><span data-bbox="485 667 496 683">▪</span> <b>Retry (default):</b> Try again if an SNMP request fails. This can prevent false error messages because of temporary timeout failures.</li> <li><span data-bbox="485 752 496 768">▪</span> <b>Do not retry:</b> Do not retry if an SNMP request fails. If you select this option, an SNMP sensor shows a Down status earlier.</li> </ul>
Overflow Values	<p>Select how PRTG handles overflow values. Some devices do not correctly handle internal buffer overflows. This can cause false peaks. PRTG can handle overflow values in two ways:</p> <ul style="list-style-type: none"> <li><span data-bbox="485 981 496 996">▪</span> <b>Ignore (default):</b> Ignore overflow values and do not include them in the monitoring data. We recommend that you use this option.</li> <li><span data-bbox="485 1066 496 1081">▪</span> <b>Handle overflow values as valid results:</b> Regard all overflow values as regular data and include them in the monitoring data.</li> </ul> <p><span data-bbox="485 1144 512 1182">i</span> If you experience problems because of strange peaks in your data graphs, change this option. Peaks might indicate that the target device resets counters without an overflow. PRTG interprets such behavior as overflow that results in data peaks. Select the option Ignore (default) in this case. For more information, see the Knowledge Base: <a href="#">What is the Overflow Values setting in the SNMP Compatibility Options?</a></p>
Zero Values	<p>Select how PRTG handles zero values. Some devices send incorrect zero values. This can cause false peaks. PRTG can handle zero values in two ways:</p> <ul style="list-style-type: none"> <li><span data-bbox="485 1503 496 1518">▪</span> <b>Ignore (default):</b> Ignore zero values and do not include them in the monitoring data. We recommend that you use this option.</li> </ul> <p><span data-bbox="485 1581 512 1619">i</span> If you experience problems, try changing this option.</p> <ul style="list-style-type: none"> <li><span data-bbox="485 1637 496 1653">▪</span> <b>Handle zero values as valid results for delta sensors:</b> Regard all zero values as regular data and include them in the monitoring data.</li> </ul>
32-bit/64-bit Counters	<p>Select the type of traffic counters that PRTG searches for on a device:</p> <ul style="list-style-type: none"> <li><span data-bbox="485 1805 496 1821">▪</span> <b>Use 64-bit counters if available (default):</b> The interface scan uses 64-bit traffic counters, if available. This can avoid buffer overflows in the devices.</li> </ul> <p><span data-bbox="485 1912 512 1951">i</span> We recommend that you use the default value.</p> <p><span data-bbox="536 1964 563 2002">i</span> If you experience problems, try changing this option.</p>

Setting	Description
	<ul style="list-style-type: none"> <li>Use 32-bit counters only: The interface scan always uses 32-bit traffic counters, even if 64-bit counters are available. This can make monitoring more reliable for some devices.</li> </ul>
Request Mode	<p>Select the request method that PRTG uses for SNMP sensors:</p> <ul style="list-style-type: none"> <li>Use multi get (default): Bundle multiple SNMP requests into one request. We recommend that you use this option.</li> </ul> <p><b>i</b> If you experience problems, try changing this option.</p> <ul style="list-style-type: none"> <li>Use single get: Use one request for each SNMP value. This can increase compatibility with older devices.</li> </ul> <p><b>i</b> PRTG uses <a href="#">paging</a> for SNMP requests. This means that if a sensor must query more than 20 object identifiers (OID), it automatically polls the OIDs in packages of 20 OIDs each.</p>
Walk Mode	<p>Select the kind of SNMP walk that PRTG uses for SNMP sensors:</p> <ul style="list-style-type: none"> <li>Use GETBULK requests (default): Request the next <b>x</b> OIDs in one SNMP request. The default value is <b>10</b>. It is dynamic based on the response size.</li> </ul> <p><b>i</b> This option only works with devices that support SNMP as of version v2c. Make sure that you set the correct SNMP Version in the Credentials for SNMP Devices settings of the parent device or inherit it from objects that are higher in the <a href="#">object hierarchy</a><sup>132</sup>.</p> <ul style="list-style-type: none"> <li>Use GETNEXT requests: Request one OID at a time. This can increase compatibility with older devices or with devices that have insufficient SNMP BULKWALK support.</li> </ul>
Port Name Template	<p>Select how PRTG displays the name of SNMP sensors. Enter a template that uses several variables. When you add new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID, several fields with interface descriptions are usually available. They are different for every device and OID. PRTG uses the information in these fields to name the sensors. If a field is empty or if it is not available, PRTG adds an empty string to the name. By default, the port name template is <b>([port]) [ifalias] [ifsensor]</b>, which creates a name like <b>(001) Ethernet1 Traffic</b>. You can use and combine any field names that are available at an OID of your device, for example:</p> <ul style="list-style-type: none"> <li>[port]: The port number of the monitored interface.</li> <li>[ifalias]: The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling.</li> <li>[ifname]: The textual name of the monitored interface as assigned by the local device.</li> <li>[ifdescr]: A textual string containing information about the target device or interface, for example, manufacturer, product name, or version.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ [ifspeed]: An estimate of the monitored interface's current bandwidth (Kbit/s).</li> <li>▪ [ifsensor]: The type of the sensor, this is <a href="#">Traffic</a> or <a href="#">RMON</a>. This helps to differentiate between <a href="#">SNMP Traffic</a> and <a href="#">SNMP RMON</a> sensors.</li> </ul> <p> For more information about SNMP sensor names, see the Knowledge Base: <a href="#">How can I change the defaults for names automatically generated for new SNMP sensors?</a></p>
Port Name Update	<p>Select how PRTG reacts if you change the names of ports in your physical device (for example, a switch or router):</p> <ul style="list-style-type: none"> <li>▪ Keep port names (use this if you edit the names in PRTG) (default): Do not automatically adjust sensor names. This is the best option if you want to manually change names in PRTG.</li> <li>▪ Automatically update sensor names if port names change in the device: If PRTG detects port name changes in your physical device, it tries to automatically adjust the sensor names accordingly.</li> </ul> <p> For more information about automatic name updates, see the Knowledge Base: <a href="#">Automatically update port name and number for SNMP Traffic sensors when the device changes them.</a></p>
Port Identification	<p>Select the field that PRTG uses for SNMP interface identification:</p> <ul style="list-style-type: none"> <li>▪ Automatic identification (default): Try the ifAlias field first to identify an SNMP interface and then try ifDescr. <ul style="list-style-type: none"> <li> PRTG does not automatically try ifName.</li> </ul> </li> <li>▪ Use IfAlias: For most devices, ifAlias is the best field to use for unique interface names.</li> <li>▪ Use IfDescr: Use this option if the port order of your device changes after a restart, and if no ifAlias field is available. For example, this is the best option for Cisco ASA devices. <ul style="list-style-type: none"> <li> If you use this option, it is important that your device returns unique interface names in the ifDescr field.</li> </ul> </li> <li>▪ Use IfName: You can also use this option if no unique ifAlias is available. <ul style="list-style-type: none"> <li> If you use this option, it is important that your device returns unique interface names in the ifName field.</li> </ul> </li> <li>▪ Do not update ports: Use this option to disable the automatic port identification.</li> </ul>
Start Interface Index	<p> This setting only applies to <a href="#">SNMP Traffic sensors</a> and to <a href="#">Cisco IP SLA sensors</a>.</p> <p>Enter the index at which PRTG starts to query the interface range during sensor creation. Enter <b>0</b> for the automatic mode.</p>

Setting	Description
	<p> We recommend that you use the default value.</p>
End Interface Index	<p> This setting only applies to <a href="#">SNMP Traffic sensors</a> and to <a href="#">Cisco IP SLA sensors</a>.</p> <p>Enter the index at which PRTG stops querying the interface range during sensor creation. Enter 0 for the automatic mode.</p> <p> We recommend that you use the default value.</p>

## Proxy Settings

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">AWS Alarm v2</a></li> <li>▪ <a href="#">AWS Cost</a></li> <li>▪ <a href="#">AWS EBS v2</a></li> <li>▪ <a href="#">AWS EC2 v2</a></li> <li>▪ <a href="#">AWS ELB v2</a></li> <li>▪ <a href="#">AWS RDS v2</a></li> <li>▪ <a href="#">Cisco Meraki License</a></li> <li>▪ <a href="#">Cisco Meraki Network Health</a></li> <li>▪ <a href="#">Cloud HTTP v2</a></li> <li>▪ <a href="#">Cloud Ping v2</a></li> <li>▪ <a href="#">Dell EMC Unity Enclosure Health v2</a></li> <li>▪ <a href="#">Dell EMC Unity File System v2</a></li> <li>▪ <a href="#">Dell EMC Unity Storage Capacity v2</a></li> <li>▪ <a href="#">Dell EMC Unity Storage LUN v2</a></li> <li>▪ <a href="#">Dell EMC Unity Storage Pool v2</a></li> <li>▪ <a href="#">Dell EMC Unity VMware Datastore v2</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">HPE 3PAR Common Provisioning Group</a></li> <li>▪ <a href="#">HPE 3PAR Drive Enclosure</a></li> <li>▪ <a href="#">HPE 3PAR Virtual Volume</a></li> <li>▪ <a href="#">HTTP</a></li> <li>▪ <a href="#">HTTP v2</a></li> <li>▪ <a href="#">HTTP Advanced</a></li> <li>▪ <a href="#">HTTP Apache ModStatus PerfStats</a></li> <li>▪ <a href="#">HTTP Apache ModStatus Totals</a></li> <li>▪ <a href="#">HTTP Content</a></li> <li>▪ <a href="#">HTTP Data Advanced</a></li> <li>▪ <a href="#">HTTP Transaction</a></li> <li>▪ <a href="#">Microsoft 365 Mailbox</a></li> <li>▪ <a href="#">Microsoft 365 Service Status</a></li> <li>▪ <a href="#">Microsoft 365 Service Status Advanced</a></li> <li>▪ <a href="#">Microsoft Azure SQL Database</a></li> <li>▪ <a href="#">Microsoft Azure Storage Account</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">NetApp Aggregate v2</a></li> <li>▪ <a href="#">NetApp I/O v2</a></li> <li>▪ <a href="#">NetApp LIF v2</a></li> <li>▪ <a href="#">NetApp LUN v2</a></li> <li>▪ <a href="#">NetApp NIC v2</a></li> <li>▪ <a href="#">NetApp Physical Disk v2</a></li> <li>▪ <a href="#">NetApp SnapMirror v2</a></li> <li>▪ <a href="#">NetApp System Health v2</a></li> <li>▪ <a href="#">NetApp Volume v2</a></li> <li>▪ <a href="#">Redfish Power Supply</a></li> <li>▪ <a href="#">Redfish Virtual Disk</a></li> <li>▪ <a href="#">Redfish Power Supply</a></li> <li>▪ <a href="#">REST Custom</a></li> <li>▪ <a href="#">REST Custom v2</a></li> <li>▪ <a href="#">Soffico Orchestra Channel Health</a></li> <li>▪ <a href="#">Soffico Orchestra Scenario</a></li> <li>▪ <a href="#">Veeam Backup Job Status</a></li> <li>▪ <a href="#">Veeam Backup Job Status Advanced</a></li> </ul>
---	---	---

<ul style="list-style-type: none"> <li>▪ <a href="#">FortiGate System Statistics</a></li> <li>▪ <a href="#">FortiGate VPN Overview</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Microsoft Azure Subscription Cost</a></li> <li>▪ <a href="#">Microsoft Azure Virtual Machine</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Zoom Service Status</a></li> </ul>
---	--	---

The proxy settings determine how a sensor connects to a URL. You can enter data for an HTTP proxy server that sensors use when they connect via HTTP or HTTPS.

- ❗ This setting only applies to sensors and how they monitor. For more information on how to change the proxy settings for the PRTG core server, see section [Core & Probes](#)<sup>[2888]</sup>.
- ❗ The [SSL Certificate](#) sensor and the [SSL Security Check](#) sensor do not support HTTP proxies but you can configure connections via SOCKS proxies in the sensors' settings:

### Proxy Settings

inherit from

**IP Address/DNS Name** ⓘ

192.0.2.0

---

**Port** ⓘ

8080

---

**User Name** ⓘ

johnqpublic




---

**Password** ⓘ

.....

Proxy Settings

Setting	Description
IP Address/DNS Name	Enter the IP address or Domain Name System (DNS) name of the proxy server. If you leave this field empty, sensors do not use a proxy.

Setting	Description
	 PRTG currently supports only HTTP proxies.
Port	Enter the port number of the proxy. The default port is <b>8080</b> . Enter an integer.
User Name	If the proxy requires authentication, enter the user name for the proxy login. Enter a string or leave the field empty.   Only basic authentication is available.
Password	If the proxy requires authentication, enter the password for the proxy login. Enter a string or leave the field empty.   Only basic authentication is available.

### Scanning Interval

Click  to interrupt the [inheritance](#) .

#### Scanning Interval

inherit from

**Scanning Interval** 

60 seconds ▼

---

**If a Sensor Query Fails** 


Set sensor to warning status for 1 interval, then set to down status (default) ▼

Scanning Interval

Setting	Description
Scanning Interval	Select a scanning interval from the dropdown list that determines the amount of time that the sensor waits between two scans: <ul style="list-style-type: none"> <li>▪ 30 seconds</li> <li>▪ 60 seconds</li> <li>▪ 5 minutes</li> <li>▪ 10 minutes</li> </ul>




Setting	Description
	<ul style="list-style-type: none"> <li>▪ 15 minutes</li> <li>▪ 30 minutes</li> <li>▪ 1 hour</li> <li>▪ 4 hours</li> <li>▪ 6 hours</li> <li>▪ 12 hours</li> <li>▪ 24 hours</li> </ul> <p><b>i</b> You can change the available intervals in the <a href="#">system administration</a> [2870] of PRTG Network Monitor.</p>
<p>If a Sensor Scanning Fails</p>	<p>Select the number of scanning intervals that the sensor has time to reach and to check a device again if a sensor scanning fails. Depending on the option that you select, the sensor can try to reach and to check a device again several times before the sensor shows the Down <a href="#">status</a> [187]. This can avoid false alarms if the target device only has temporary issues. For previous scanning intervals with failed requests, the sensor shows the Warning status.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> <li>▪ Set sensor to down status immediately: Set the sensor to the Down status immediately after the first request fails.</li> <li>▪ Set sensor to warning status for 1 interval, then set to down status (default): Set the sensor to the Warning status after the first request fails. If the second request also fails, the sensor shows the Down status.</li> <li>▪ Set sensor to warning status for 2 intervals, then set to down status: Set the sensor to the Down status only after the third request fails.</li> <li>▪ Set sensor to warning status for 3 intervals, then set to down status: Set the sensor to the Down status only after the fourth request fails.</li> <li>▪ Set sensor to warning status for 4 intervals, then set to down status: Set the sensor to the Down status only after the fifth request fails.</li> <li>▪ Set sensor to warning status for 5 intervals, then set to down status: Set the sensor to the Down status only after the sixth request fails.</li> </ul> <p><b>i</b> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval before they show the Down status. It is not possible to immediately set a WMI sensor to the Down status, so the first option does not apply to these sensors. All other options can apply.</p> <p><b>i</b> If you define error limits for a sensor's channels, the sensor immediately shows the Down status. None of the interval options apply.</p>

Setting	Description
	<p> If a channel uses <a href="#">lookup</a> values, the sensor immediately shows the Down status. None of the interval options apply.</p>

## Schedules, Dependencies, and Maintenance Window

Click  to interrupt the [inheritance](#).

### Schedules, Dependencies, and Maintenance Window

 inherit from

*Schedules, dependencies, and maintenance windows always pause all sensors inside a group or device. This pausing is always inherited to all child objects and the inheritance cannot be disabled. Below you can set additional schedules, dependencies, or maintenance windows that will be used in parallel to any inherited setting.*

**Schedule** ⓘ

None ▼

---

**Maintenance Window** ⓘ

Do not set up a one-time maintenance window (default)

Set up a one-time maintenance window

**Dependency Type** ⓘ


Use parent (default)

Select a sensor

Schedules, Dependencies, and Maintenance Window

Setting	Description
Schedule	<p>Select a schedule from the list. You can use schedules to monitor during a certain time span (days or hours) every week:</p> <ul style="list-style-type: none"> <li>▪ None</li> <li>▪ Saturdays</li> <li>▪ Sundays</li> <li>▪ Weekdays</li> <li>▪ Weekdays Eight-To-Eight (08:00 - 20:00)</li> <li>▪ Weekdays Nights (17:00 - 09:00)</li> </ul>


Setting	Description
	<ul style="list-style-type: none"> <li>▪ Weekdays Nights (20:00 - 08:00)</li> <li>▪ Weekdays Nine-To-Five (09:00 - 17:00)</li> <li>▪ Weekends</li> </ul> <p><b>i</b> You can create schedules, edit schedules, or pause monitoring for a specific time span. For more information, see section <a href="#">Schedules</a> <sup>[2848]</sup>.</p>
Maintenance Window	<p>Select if you want to set up a one-time maintenance window:</p> <ul style="list-style-type: none"> <li>▪ Do not set up a one-time maintenance window (default): Do not set up a one-time maintenance window. Monitoring is always active.</li> <li>▪ Set up a one-time maintenance window: Set up a one-time maintenance window and pause monitoring for the selected object and all child objects. You can define a time span for the pause below.</li> </ul> <p><b>i</b> To cancel an active maintenance window before the defined end date, change the time entry under Maintenance Ends to a date in the past.</p>
Maintenance Begins	<p><b>This setting is only visible if you select</b> Set up a one-time maintenance window <a href="#">above</a>.</p> <p>Use the date time picker to enter the start date and time of the one-time maintenance window.</p>
Maintenance Ends	<p><b>This setting is only visible if you select</b> Set up a one-time maintenance window <a href="#">above</a>.</p> <p>Use the date time picker to enter the end date and time of the one-time maintenance window.</p>
Dependency Type	<p>Select a dependency type. You can use dependencies to pause monitoring for an object depending on the status of a different object:</p> <ul style="list-style-type: none"> <li>▪ Use parent (default): Use the dependency type of the parent object.</li> <li>▪ Select a sensor: Use the dependency type of the parent object. Additionally, pause the current object if a specific sensor is in the Down status or in the Paused status because of another dependency.</li> </ul> <p><b>i</b> You do not trigger a status change by dependency if you manually pause a master sensor or if you pause it by schedule.</p> <p><b>i</b> To test your <a href="#">dependencies</a> <sup>[2728]</sup>, select Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later, all dependent objects are paused. You can check all dependencies under Devices   Dependencies in the main menu bar.</p>
Dependency	<p><b>This setting is only visible if you select</b> Select a sensor <a href="#">above</a>.</p>

Setting	Description
	Click  and use the <a href="#">object selector</a> <sup>[222]</sup> to select a sensor on which the current object will depend.
Dependency Delay (Sec.)	<p>This setting is only visible if you select <a href="#">Select a sensor above</a>.</p> <p>Define a time span in seconds for the dependency delay.</p> <p>After the master sensor for this dependency returns to the Up status, PRTG additionally delays the monitoring of the dependent objects by the time span you define. This can prevent false alarms, for example, after a server restart or to give systems more time for all services to start. Enter an integer.</p>

### Access Rights

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

#### Access Rights


 inherit from

**User Group Access** ⓘ

User Group	Rights
PRTG Users Group	Write access
Read-only User Group	Read access
SSO User Group	Inherited (No access)

Revert access rights of child objects to "inherited"

Access Rights

Setting	Description
User Group Access	<p>Select the <a href="#">user groups</a><sup>[2912]</sup> that have access to the object. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights:</p> <ul style="list-style-type: none"> <li>▪ Inherited: Inherit the access rights settings of the parent object.</li> <li>▪ No access: Users in this user group cannot see or edit the object. The object neither shows up in lists nor in the device tree. <ul style="list-style-type: none"> <li>ⓘ There is one exception: If a user in this user group has access to a child object, the parent object is visible in the device tree but users in this user group cannot access it.</li> </ul> </li> <li>▪ Read access: Users in this group can see the object and view its monitoring results. They cannot edit any settings.</li> <li>▪ Write access: Users in this group can see the object, view its monitoring results, and edit its settings. They cannot edit its access rights settings.</li> <li>▪ Full access: Users in this group can see the object, view its monitoring results, edit its settings, and edit its access rights settings.</li> </ul> <p>To automatically set all child objects to inherit this object's access rights, select the Revert access rights of child objects to "inherited" option.</p> <p> For more information on access rights, see section <a href="#">Access Rights Management</a><sup>[145]</sup>.</p>









## Channel Unit Configuration

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

## Channel Unit Configuration

inherit from

### Channel Unit Types i

 Channel Type	 Unit
Bytes (Bandwidth)	MB 
	Mbit 
	/ sec... 
Bytes (Memory)	GB 
Bytes (Disk)	GB 
Bytes (File)	MB 


Channel Unit Configuration

Setting	Description
Channel Unit Types	<p>For each type of channel, select the unit in which PRTG displays the data. If you define this setting on probe, group, or device level, you can inherit these settings to all sensors underneath. You can set units for the following channel types (if available):</p> <ul style="list-style-type: none"> <li>▪ Bandwidth</li> <li>▪ Memory</li> <li>▪ Disk</li> <li>▪ File</li> <li>▪ Custom</li> </ul> <p><b>i</b> Custom channel types are only available on sensor level.</p> <p><b>i</b> Which channel units are available depends on the sensor type and the available parameters. If no configurable channels are available, this field shows <a href="#">No configurable channels</a>.</p>

### Advanced Network Analysis

Click  to interrupt the [inheritance](#) <sup>136</sup>.

#### Advanced Network Analysis

 inherit from

**Unusual Detection** **i**

Enable (default)

Disable

**Similar Sensors Detection** **i**

Enable (default)

Disable

**System Information** **i**

Enable (default)

Disable

Advanced Network Analysis

Setting	Description
Unusual Detection	<p>Select if you want to use the <a href="#">unusual detection</a> for sensors:</p> <ul style="list-style-type: none"> <li>▪ <b>Enable (default):</b> Activates the unusual detection for this object and, by default, for all objects underneath in the <a href="#">object hierarchy</a>. Sensors that are affected by this setting show the Unusual status if PRTG detects unusual activity.</li> <li>▪ <b>Disable:</b> Does not activate the unusual detection. PRTG ignores unusual values for sensors that are affected by this setting. These sensors do not show the Unusual status.</li> </ul> <p><b>i</b> You can configure the behavior of the unusual detection or completely disable it in the <a href="#">system settings</a>.</p>
Similar Sensors Detection	<p>Select if you want to activate the <a href="#">similar sensors</a> analysis:</p> <ul style="list-style-type: none"> <li>▪ <b>Enable (default):</b> Activates the similar sensors detection for this object and, by default, for all objects underneath in the object hierarchy. PRTG considers all sensors that are affected by this setting during the similarity analysis.</li> <li>▪ <b>Disable:</b> Does not activate the similar sensors detection. PRTG does not consider sensors that are affected by this setting during the similarity analysis.</li> </ul> <p><b>i</b> You can configure the depth of the analysis of the similar sensors detection or completely disable it in the <a href="#">system settings</a>.</p>
System Information	<p>Select if you want to retrieve and show <a href="#">system information</a> for your devices:</p> <ul style="list-style-type: none"> <li>▪ <b>Enable (default):</b> Activates the system information feature for this object and, by default, for all objects underneath in the hierarchy.</li> <li>▪ <b>Disable:</b> Does not activate the system information feature.</li> </ul> <p><b>i</b> The System Information feature is enabled by default. To retrieve the data, PRTG automatically uses the <a href="#">credentials for Windows systems</a> and the <a href="#">credentials for SNMP devices</a> that you entered in the device settings or that the device <a href="#">inherits</a> from a parent object like the root group. Consider this when you monitor devices that are outside of your local network, especially when you use <b>SNMP v1</b> or <b>SNMP v2c</b>, which do not provide encryption.</p> <p><b>☁</b> This setting is not available on the hosted probe of a PRTG Hosted Monitor instance.</p>



## Number of Sensors Limitation

### Number of Sensors Limitation

**Sensor Limit** ⓘ

Allow unlimited number of sensors (default)

Limit number of sensors

Number of Sensors Limitation

Setting	Description
Sensor Limit	<p>Define a limit for the maximum number of sensors in this group, including subgroups:</p> <ul style="list-style-type: none"> <li>▪ Allow unlimited number of sensors (default): Do not limit the number of sensors for this group. Any number of sensors are allowed in this group and its subgroups.</li> <li>▪ Limit number of sensors: Set a limit for the number of sensors in this group. Only a defined number of sensors are allowed in this group and its subgroups. If the amount of sensors exceeds the limit, PRTG sets the surplus sensors to the Paused status.</li> </ul>
Maximum Number of Sensors	<p><b>This setting is only visible if you select Limit number of sensors above.</b></p> <p>Define how many sensors are allowed in this group and its subgroups. Sensors that exceed this group sensor limit are set to the Paused state. Enter an integer.</p> <p>ⓘ Sensors that are in the Paused state count for this group limit as well (for example, manually paused sensors or sensors that are paused by dependency or schedule), but not for the number of available sensors in your license.</p> <p>ⓘ Manually paused sensors override the sensor message <b>exceeds group sensor limit</b>.</p>

ⓘ Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- <https://kb.paessler.com/en/topic/38083>

Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?

- <https://kb.paessler.com/en/topic/89717>

How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?

- <https://kb.paessler.com/en/topic/88462>

How do I obtain credentials and create custom roles for the Microsoft Azure sensors?

- <https://kb.paessler.com/en/topic/88625>

What is the Overflow Values setting in the SNMP Compatibility Options?

- <https://kb.paessler.com/en/topic/43503>

How can I change the defaults for names automatically generated for new SNMP sensors?

- <https://kb.paessler.com/en/topic/7363>

Automatically update port name and number for SNMP Traffic sensors when the device changes them

- <https://kb.paessler.com/en/topic/25893>

## 7.7 Device Settings

The following settings are available on the Settings tab of a device.

- ❗ We recommend that you define as many settings as possible in the [root group settings](#) so that you can inherit them to all other objects in the [object hierarchy](#).











For device settings, you can also use multi-edit. This enables you to change the settings of many devices at the same time.

- For more information, see section [Multi-Edit](#).

- ❗ This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

In this section:

- [Basic Device Settings](#)
- [Additional Device Information](#)
- [Auto-Discovery Settings](#)
- [Location](#)
- [Credentials for Windows Systems](#)
- [Credentials for Linux/Solaris/macOS \(SSH/WBEM\) Systems](#)
- [Credentials for VMware/XenServer](#)
- [Credentials for SNMP Devices](#)
- [Credentials for Database Management Systems](#)
- [Credentials for AWS](#)
- [Credentials for Microsoft 365](#)
- [Credentials for Script Sensors](#)
- [Credentials for Cisco Meraki](#)
- [Credentials for Dell EMC](#)
- [Credentials for FortiGate](#)
- [Credentials for HPE 3PAR](#)
- [Credentials for HTTP](#)
- [Credentials for Microsoft Azure](#)
- [Credentials for MQTT](#)
- [Credentials for NetApp](#)
- [Credentials for OPC UA](#)
- [Credentials for Soffico Orchestra](#)
- [Credentials for Redfish](#)

- [Credentials for REST API](#)  646
- [Credentials for Veeam](#)  647
- [Windows Compatibility Options](#)  648
- [SNMP Compatibility Options](#)  650
- [Proxy Settings](#)  655
- [Scanning Interval](#)  657
- [Schedules, Dependencies, and Maintenance Window](#)  659
- [Access Rights](#)  661
- [Channel Unit Configuration](#)  662
- [Advanced Network Analysis](#)  664

## Basic Device Settings

### Basic Device Settings

**Device Name** ⓘ

Device

---

**Monitoring Status** ⓘ

Started (default)

Paused

**IP Version** ⓘ

IPv4

IPv6

**IPv4 Address/DNS Name** ⓘ

192.0.2.0

---

**Parent Tags** ⓘ

**Tags** ⓘ

---

**Priority** ⓘ

★★★★☆

Basic Device Settings


Setting	Description
Device Name	<p>Enter a name to identify the device. By default, PRTG shows this name in the <a href="#">device tree</a><sup>[164]</sup>, as well as in <a href="#">alarms</a><sup>[202]</sup>, <a href="#">logs</a><sup>[210]</sup>, <a href="#">notifications</a><sup>[2735]</sup>, <a href="#">reports</a><sup>[2754]</sup>, <a href="#">maps</a><sup>[2776]</sup>, <a href="#">libraries</a><sup>[2738]</sup>, and <a href="#">tickets</a><sup>[213]</sup>.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Monitoring Status	<p>Select the monitoring status of the device:</p> <ul style="list-style-type: none"> <li>Started (default): Monitor the device.</li> <li>Paused: Pause monitoring for the device. All sensors on the device are in the Paused <a href="#">status</a><sup>[227]</sup> until you change this setting.</li> </ul>
IP Version	<p>Select the IP protocol that PRTG uses to connect to the device:</p> <ul style="list-style-type: none"> <li>IPv4: Use IP version 4 for all requests to the device.</li> <li>IPv6: Use IP version 6 for all requests to the device.</li> </ul> <p><b>i</b> The setting is valid for all sensors that you create on the device.</p>
IPv4 Address/DNS Name	<p><a href="#">This setting is only visible if you select IPv4 above.</a></p> <p>Enter the IP address or Domain Name System (DNS) name for the device. Most sensors that you create on this device inherit this setting and try to connect to this address for monitoring.</p> <p><b>i</b> Some sensors have their own setting for the IP address/DNS name to which they connect.</p>
IPv6 Address/DNS Name	<p><a href="#">This setting is only visible if you select IPv6 above.</a></p> <p>Enter the IP address or Domain Name System (DNS) name for the device. Most sensors that you create on this device inherit this setting and try to connect to this address for monitoring.</p> <p><b>i</b> Some sensors have their own setting for the IP address/DNS name to which they connect.</p>
Parent Tags	<p>Shows <a href="#">tags</a><sup>[138]</sup> that this device <a href="#">inherits</a><sup>[138]</sup> from its parent <a href="#">group</a><sup>[133]</sup> and its parent <a href="#">probe</a><sup>[133]</sup>.</p> <p><b>i</b> This setting is for your information only. You cannot change it.</p>

Setting	Description
Tags	<p>Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically <a href="#">inherited</a><sup>138</sup>.</p> <ul style="list-style-type: none"> <li><b>i</b> We recommend that you use the default value. You can also add additional tags.</li> <li><b>i</b> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (&lt;&gt;).</li> <li><b>i</b> For performance reasons, it can take some minutes until you can filter for new tags that you added.</li> </ul>
Priority	<p>Select a <a href="#">priority</a><sup>224</sup> for the device. This setting determines the position of the group in lists. The highest priority is at the top of a list. You can choose from the lowest priority (☆☆☆☆☆) to the highest priority (★★★★★).</p>

### Additional Device Information

#### Additional Device Information

**Device Icon** ⓘ



**Service URL** ⓘ

---

Additional Device Information

Setting	Description
Device Icon	Select a device icon. PRTG shows it in the device tree.
Service URL	Specify a URL to open directly when you select Device Tools   Go to Service URL from the <a href="#">context menu</a> <sup>[229]</sup> of the device. For example, you can configure this option to open the address <a href="http://www.example.com/service.html">http://www.example.com/service.html</a> . Enter a valid URL or leave the field empty.

### Auto-Discovery Settings

## Device Identification and Auto-Discovery

**Auto-Discovery Level** ⓘ

- No auto-discovery
- Standard auto-discovery (default)
- Detailed auto-discovery
- Auto-discovery with specific device templates

Auto-Discovery Settings

Setting	Description
Auto-Discovery Level	<p>Select the level of detail for the <a href="#">auto-discovery</a><sup>[254]</sup>:</p> <ul style="list-style-type: none"> <li>▪ <b>No auto-discovery:</b> Select this option if you only want to manually create devices and sensors.</li> <li>▪ <b>Standard auto-discovery (default):</b> Create a set of standard sensors for standard monitoring. This option works fine for most installations.</li> <li>▪ <b>Detailed auto-discovery:</b> Create all standard sensors and additional sensors from detailed variants of device templates. As a result, you might get many sensors. This option is suitable for small network segments and whenever you want to monitor the maximum number of sensors available.</li> <li>▪ <b>Auto-discovery with specific device templates:</b> Customize the auto-discovery and select or combine standard, detailed, and custom device templates. Select one or more templates from the Device Templates list.</li> </ul>




Setting	Description
	<p><b>i</b> Auto-discoveries can be resource intensive. They are primarily intended for devices on the same network as your probes.</p>
<p>Schedule</p>	<p>Select when PRTG runs the auto-discovery:</p> <ul style="list-style-type: none"> <li>▪ Once (default): Run the auto-discovery only once. PRTG adds new devices and sensors once. If you select this option, you must manually <a href="#">start the auto-discovery</a> <sup>[255]</sup>.</li> <li>▪ Hourly: Run the auto-discovery for new devices and sensors every 60 minutes. <ul style="list-style-type: none"> <li><b>i</b> Use this option with caution. Frequent auto-discoveries might cause performance issues, in particular when PRTG scans large network segments every hour.</li> </ul> </li> <li>▪ Daily: Run the auto-discovery for new devices and sensors every 24 hours. The first auto-discovery runs immediately. All other discoveries start at the time that you define in the <a href="#">Monitoring</a> <sup>[2875]</sup> settings, section Auto-Discovery.</li> <li>▪ Weekly: Run the auto-discovery for new devices and sensors every 7 days. The first auto-discovery runs immediately. All other discoveries start at the time that you define in the Monitoring settings, section Auto-Discovery.</li> </ul> <p><b>i</b> For performance reasons, PRTG sets Schedule to Once (default) on all devices that the scheduled auto-discovery creates.</p>
<p>Device Templates</p>	<p><a href="#">This setting is only visible if you select</a> Auto-discovery with specific device templates <a href="#">above</a>.</p> <p>Select one or more device templates by enabling a check box in front of the template name. PRTG uses the device templates that you select for the auto-discovery on the device:</p> <ul style="list-style-type: none"> <li>▪ ADSL</li> <li>▪ Buffalo TeraStation NAS</li> <li>▪ Cisco ASA VPN</li> <li>▪ Cisco Device (Generic)</li> <li>▪ Dell EqualLogic</li> <li>▪ Dell MDi Disk</li> <li>▪ DNS Server</li> <li>▪ Environment Jakarta</li> <li>▪ Environment Poseidon</li> <li>▪ FTP Server</li> <li>▪ Generic Device (Ping Only)</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Generic Device (SNMP Enabled)</li> <li>▪ Generic Device (SNMP Enabled, Detailed)</li> <li>▪ HTTP Web Server</li> <li>▪ Hyper-V Host Server</li> <li>▪ IPMI-enabled Device</li> <li>▪ Juniper NS Device</li> <li>▪ Linux/UNIX Device (SNMP or SSH Enabled)</li> <li>▪ Mail Server (Generic)</li> <li>▪ Mail Server (MS Exchange)</li> <li>▪ Microsoft SharePoint 2010</li> <li>▪ MQTT Round Trip</li> <li>▪ NAS LenovoEMC</li> <li>▪ NAS QNAP</li> <li>▪ NAS Synology</li> <li>▪ NetApp</li> <li>▪ NTP Server</li> <li>▪ OPC UA</li> <li>▪ Printer (Generic)</li> <li>▪ Printer (HP)</li> <li>▪ RDP Server</li> <li>▪ RMON-compatible Device</li> <li>▪ Server (Cisco UCS)</li> <li>▪ Server (Compaq/HP Agents)</li> <li>▪ Server (Dell)</li> <li>▪ Server (Fujitsu)</li> <li>▪ Server (IBM)</li> <li>▪ SNMP Rittal CMC III Hardware Status</li> <li>▪ SonicWall</li> <li>▪ SSL Security Check</li> <li>▪ Switch (Cisco Catalyst)</li> <li>▪ Switch (Cisco IOS Based)</li> <li>▪ Switch (HP Procurve)</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ UNIX/Linux Device</li> <li>▪ UPS Health (APC)</li> <li>▪ UPS Health (Generic)</li> <li>▪ UPS Health (Liebert)</li> <li>▪ VMware ESXi / vCenter Server</li> <li>▪ Web Server</li> <li>▪ Windows (Detailed via WMI)</li> <li>▪ Windows (via Remote PowerShell)</li> <li>▪ Windows (via WMI)</li> <li>▪ Windows IIS (via SNMP)</li> <li>▪ XenServer Hosts</li> <li>▪ XenServer Virtual Machines</li> </ul> <p>Once the auto-discovery is finished, PRTG creates a new <a href="#">ticket</a><sup>[213]</sup> and lists the device templates that it used to create new sensors.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#)<sup>[420]</sup> if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#)<sup>[136]</sup>.

## Location

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

### Location

inherit from

Location (for Geo Maps) ⓘ



Location

Setting	Description
Location (for Geo Maps)	<p>If you want to use <a href="#">Geo Maps</a><sup>[2731]</sup>, enter a location in the first line. Geographical maps then display objects like devices or groups with a status icon using a color code similar to the <a href="#">sensor status icons</a><sup>[181]</sup> (green–yellow–orange–red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, as PRTG automatically parses latitude and longitude, for example, enter <a href="#">49.452778 11.077778</a>, or <a href="#">enter 49.452778 any 11.077778 text</a>.</p> <p>A minus sign (-) in the first line hides an object from a geographical map. In this case, you can enter location information in line two and following.</p> <p>You can define a specific label for each location. Enter a string denoting the label in the first line and provide the coordinates in the second line. This geographical marker then shows the object with the label in the geographical map.</p> <p>ⓘ The preview map always has a road map layout regardless of the map layout you set in <a href="#">User Interface</a><sup>[2859]</sup>.</p>

### Credentials for Windows Systems


Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

ⓘ The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">Active Directory Replication Errors</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Windows MSMQ Queue Length</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">WMI Memory</a></li> </ul>
---	---	--

<ul style="list-style-type: none"> <li>▪ <a href="#">Event Log (Windows API)</a></li> <li>▪ <a href="#">Exchange Backup (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database (PowerShell)</a></li> <li>▪ <a href="#">Exchange Database DAG (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mail Queue (PowerShell)</a></li> <li>▪ <a href="#">Exchange Mailbox (PowerShell)</a></li> <li>▪ <a href="#">Exchange Public Folder (PowerShell)</a></li> <li>▪ <a href="#">File</a></li> <li>▪ <a href="#">File Content</a></li> <li>▪ <a href="#">Folder</a></li> <li>▪ <a href="#">Hyper-V Cluster Shared Volume Disk Free</a></li> <li>▪ <a href="#">Hyper-V Host Server</a></li> <li>▪ <a href="#">Hyper-V Virtual Machine</a></li> <li>▪ <a href="#">Hyper-V Virtual Network Adapter</a></li> <li>▪ <a href="#">Hyper-V Virtual Storage Device</a></li> <li>▪ <a href="#">PerfCounter Custom</a></li> <li>▪ <a href="#">PerfCounter IIS Application Pool</a></li> <li>▪ <a href="#">Share Disk Free</a></li> <li>▪ <a href="#">Windows CPU Load</a></li> <li>▪ <a href="#">Windows IIS Application</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Windows Network Card</a></li> <li>▪ <a href="#">Windows Pagefile</a></li> <li>▪ <a href="#">Windows Physical Disk I/O</a></li> <li>▪ <a href="#">Windows Print Queue</a></li> <li>▪ <a href="#">Windows Process</a></li> <li>▪ <a href="#">Windows SMTP Service Received</a></li> <li>▪ <a href="#">Windows SMTP Service Sent</a></li> <li>▪ <a href="#">Windows System Uptime</a></li> <li>▪ <a href="#">Windows Updates Status (PowerShell)</a></li> <li>▪ <a href="#">WMI Battery</a></li> <li>▪ <a href="#">WMI Custom</a></li> <li>▪ <a href="#">WMI Custom String</a></li> <li>▪ <a href="#">WMI Disk Health</a></li> <li>▪ <a href="#">WMI Event Log</a></li> <li>▪ <a href="#">WMI Exchange Server</a></li> <li>▪ <a href="#">WMI Exchange Transport Queue</a></li> <li>▪ <a href="#">WMI File</a></li> <li>▪ <a href="#">WMI Free Disk Space (Multi Disk)</a></li> <li>▪ <a href="#">WMI HDD Health</a></li> <li>▪ <a href="#">WMI Logical Disk I/O</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">WMI Microsoft SQL Server 2005 (Deprecated)</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2008</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2012</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2014</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2016</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2017</a></li> <li>▪ <a href="#">WMI Microsoft SQL Server 2019</a></li> <li>▪ <a href="#">WMI Remote Ping</a></li> <li>▪ <a href="#">WMI Security Center</a></li> <li>▪ <a href="#">WMI Service</a></li> <li>▪ <a href="#">WMI Share</a></li> <li>▪ <a href="#">WMI SharePoint Process</a></li> <li>▪ <a href="#">WMI Storage Pool</a></li> <li>▪ <a href="#">WMI Terminal Services (Windows 2008+)</a></li> <li>▪ <a href="#">WMI Terminal Services (Windows XP/Vista/2003)</a></li> <li>▪ <a href="#">WMI UTC Time</a></li> <li>▪ <a href="#">WMI Vital System Data v2</a></li> <li>▪ <a href="#">WMI Volume</a></li> <li>▪ <a href="#">WSUS Statistics</a></li> </ul>
---	--	---

## Credentials for Windows Systems

 inherit from

Domain or Computer Name 

www.example.com

User Name 

johnqpublic

Password 

.....

Credentials for Windows Systems

Setting	Description
Domain or Computer Name	<p>Enter the domain or computer name of the user account with which you want to access the Windows system. PRTG uses this account for Windows Management Instrumentation (WMI) sensors and other Windows sensors.</p> <p>If you want to use a Windows local user account on the target device, enter the computer name. If you want to use a Windows domain user account (recommended), enter the domain name. PRTG automatically adds a prefix to use the NT LAN Manager (NTLM) protocol if you do not explicitly define it. Do not leave this field empty.</p>
User Name	<p>Enter the user name for access to the Windows system. Usually, you use credentials with administrator rights.</p>
Password	<p>Enter the password for access to the Windows system. Usually, you use credentials with administrator rights.</p>

## Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

Click  to interrupt the [inheritance](#) .

 The settings you define in this section apply to the following sensors:

- [SFTP Secure File Transfer Protocol](#)
- [SSH Disk Free](#)
- [SSH INodes Free](#)
- [SSH Load Average](#)
- [SSH Meminfo](#)
- [SSH Remote Ping](#)
- [SSH SAN Enclosure](#)
- [SSH SAN Logical Disk](#)
- [SSH SAN Physical Disk](#)
- [SSH SAN System Health](#)
- [SSH Script](#)
- [SSH Script Advanced](#)
- [VMware Host Hardware \(WBEM\)](#)

## Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

inherit from

User Name <sup>i</sup>

johnqpublic

Authentication Method <sup>i</sup>

- Password (default)
- Private key

Password <sup>i</sup>

.....

WBEM Protocol <sup>i</sup>

- HTTP
- HTTPS (default)

WBEM Port <sup>i</sup>

- Default
- Custom

SSH Port <sup>i</sup>

22









SSH Rights Elevation <sup>i</sup>

- Run the command as the connecting user (default)
- Run the command as a different user using 'sudo' (with password)
- Run the command as a different user using 'sudo' (without password)
- Run the command as a different user using 'su'

SSH Connection Mode <sup>i</sup>

- Default
- Compatibility mode (deprecated)



Setting	Description
User Name	Enter the user name for access to the Linux/Solaris/macOS system via Secure Shell (SSH) and Web-based Enterprise Management (WBEM). Usually, you use credentials with administrator rights.
Authentication Method	<p>Select the authentication method for the login:</p> <ul style="list-style-type: none"> <li>▪ Password (default): Provide the password for the login.</li> <li>▪ Private key: Provide an RSA private key for authentication.</li> </ul> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For more information, see section <a href="#">Monitoring via SSH</a><sup>[3007]</sup>.</p>
Password	<p>This setting is only visible if you select Password (default) above.</p> <p>Enter a password for access to the Linux/Solaris/macOS system via SSH and WBEM. Usually, you use credentials with administrator rights.</p>
Private Key	<p>This setting is only visible if you select Private key above.</p> <p>Paste the entire RSA private key, including the <b>BEGIN</b> and <b>END</b> lines. Make sure that a corresponding public key exists on the target device.</p> <p> PRTG can only handle keys in the OpenSSH format that are not encrypted. You cannot use password-protected keys.</p> <p> PRTG only supports RSA keys. It does not support DSA keys.</p> <p> For more information, see section <a href="#">Monitoring via SSH</a><sup>[3007]</sup>.</p> <p> If you do not insert a private key for the first time but if you want to <a href="#">change</a> the private key, you need to <a href="#">restart the PRTG core server service</a><sup>[2919]</sup> for the private key change to take effect.</p>
WBEM Protocol	<p>Select the protocol that you want to use for the connection to the system via WBEM:</p> <ul style="list-style-type: none"> <li>▪ HTTP: Use an unsecure connection for WBEM.</li> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection for WBEM.</li> </ul> <p> This setting is only relevant if you use WBEM sensors.</p>
WBEM Port	Select if you want to use one of the default ports for the connection to the system via WBEM or if you want to set a custom port:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Default: Use one of the default ports. The default port for unsecure connections is <a href="#">5988</a> and the default port for secure connections is <a href="#">5989</a>.</li> <li>▪ Custom: Use a custom port.</li> </ul> <p><b>i</b> This setting is only relevant if you use WBEM sensors.</p>
Custom WBEM Port	<p>This setting is only visible if you select Custom above.</p> <p>Enter a custom WBEM port. Enter an integer.</p>
SSH Port	<p>Enter the port for SSH connections. Enter an integer. The default port is <a href="#">22</a>.</p> <p><b>i</b> By default, PRTG automatically uses this setting for all <a href="#">SSH sensors</a> unless you define a different port number in the sensor settings.</p>
SSH Rights Elevation	<p>Select the rights that you want to use to run the command on the target system:</p> <ul style="list-style-type: none"> <li>▪ Run the command as the connecting user (default): Use the rights of the user who establishes the SSH connection.</li> <li>▪ Run the command as a different user using 'sudo' (with password): Use the rights of a different user with a password required for <a href="#">sudo</a> to run commands on the target system, for example, as a root user.</li> <li>▪ Run the command as a different user using 'sudo' (without password): Use the rights of a different user without a password required for <a href="#">sudo</a> to run commands on the target system, for example, as a root user.</li> <li>▪ Run the command as a different user using 'su': Use the rights of a different user with <a href="#">su</a> to run commands on the target system.</li> </ul>
Target System User Name	<p>This setting is only visible if you select an option that includes <a href="#">sudo</a> or <a href="#">su</a> above.</p> <p>Enter a user name to run the specified command on the target system as a different user than the root user. If you leave this field empty, you run the command as a root user. Make sure that you set the Linux password even if you use a public key or a private key for authentication. This is not necessary if the user is allowed to run the command without a password.</p>
Password	<p>This setting is only visible if you select an option that includes <a href="#">sudo</a> or <a href="#">su</a> with password above.</p> <p>Enter the password to run the <a href="#">sudo</a> command or the <a href="#">su</a> command.</p>

Setting	Description
SSH Connection Mode	<p>Select the connection mode that you want to use to <a href="#">access data with SSH sensors</a> <sup>6007</sup>.</p> <ul style="list-style-type: none"> <li>▪ Default: This is the default connection mode for SSH sensors. It provides the best performance and security.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default connection mode does not work on the target system. The compatibility mode is the connection mode that PRTG used in previous versions and it is deprecated.</li> </ul> <p><b>i</b> We strongly recommend that you use the default connection mode.</p> <p><b>i</b> You can also individually select the connection mode for each SSH sensor in the sensor settings.</p>

### Credentials for VMware/XenServer

Click  to interrupt the [inheritance](#) <sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

- [Citrix XenServer Host](#)
- [Citrix XenServer Virtual Machine](#)
- [VMware Datastore \(SOAP\)](#)
- [VMware Host Hardware \(WBEM\)](#)
- [VMware Host Hardware Status \(SOAP\)](#)
- [VMware Host Performance \(SOAP\)](#)
- [VMware Virtual Machine \(SOAP\)](#)

## Credentials for VMware/XenServer

inherit from

User Name i

johnqpublic

Password i

.....

VMware Protocol i

HTTPS (default)

HTTP

Credentials for VMw are/XenServer

Setting	Description
User Name	Enter the user name for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.
Password	Enter the password for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.  <span>i</span> Single sign-on (SSO) passwords for vSphere do not support special characters. For more information, see the VMware sensors sections.
VMware Protocol	Select the protocol for the connection to VMware ESXi, vCenter Server, or Citrix XenServer: <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
Session Handling	Select if you want to reuse a session for VMware sensors:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Reuse a session for multiple scans (default): Select this option if you want a VMware sensor to reuse a single session for multiple sensor scans to query data. With this option, the sensor does not need to log in and out for each sensor scan. We recommend that you use this option because it reduces network load and log entries on the target device. This can increase performance.</li> <li>▪ Create a new session for each scan: If you select this option, PRTG does not reuse a session and a VMware sensor has to log in and out for each sensor scan. This can decrease performance.</li> </ul>

### Credentials for SNMP Devices

Click  to interrupt the [inheritance](#) 136.

 The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">Cisco IP SLA</a></li> <li>▪ <a href="#">SNMP APC Hardware</a></li> <li>▪ <a href="#">SNMP Buffalo TS System Health</a></li> <li>▪ <a href="#">SNMP Cisco ADSL</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Connections</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Traffic</a></li> <li>▪ <a href="#">SNMP Cisco ASA VPN Users</a></li> <li>▪ <a href="#">SNMP Cisco CBQoS</a></li> <li>▪ <a href="#">SNMP Cisco System Health</a></li> <li>▪ <a href="#">SNMP Cisco UCS Blade</a></li> <li>▪ <a href="#">SNMP Cisco UCS Chassis</a></li> <li>▪ <a href="#">SNMP Cisco UCS Physical Disk</a></li> <li>▪ <a href="#">SNMP Cisco UCS System Health</a></li> <li>▪ <a href="#">SNMP CPU Load</a></li> <li>▪ <a href="#">SNMP Custom</a></li> <li>▪ <a href="#">SNMP Custom Advanced</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">SNMP Fujitsu System Health v2</a></li> <li>▪ <a href="#">SNMP Hardware Status</a></li> <li>▪ <a href="#">SNMP HP LaserJet Hardware</a></li> <li>▪ <a href="#">SNMP HPE BladeSystem Blade</a></li> <li>▪ <a href="#">SNMP HPE BladeSystem Enclosure Health</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Logical Disk</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Memory Controller</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Network Interface</a></li> <li>▪ <a href="#">SNMP HPE ProLiant Physical Disk</a></li> <li>▪ <a href="#">SNMP HPE ProLiant System Health</a></li> <li>▪ <a href="#">SNMP IBM System X Logical Disk</a></li> <li>▪ <a href="#">SNMP IBM System X Physical Disk</a></li> <li>▪ <a href="#">SNMP IBM System X Physical Memory</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">SNMP NetApp Enclosure</a></li> <li>▪ <a href="#">SNMP NetApp I/O</a></li> <li>▪ <a href="#">SNMP NetApp License</a></li> <li>▪ <a href="#">SNMP NetApp Logical Unit</a></li> <li>▪ <a href="#">SNMP NetApp Network Interface</a></li> <li>▪ <a href="#">SNMP NetApp System Health</a></li> <li>▪ <a href="#">SNMP Nutanix Cluster Health</a></li> <li>▪ <a href="#">SNMP Nutanix Hypervisor</a></li> <li>▪ <a href="#">SNMP Poseidon Environment</a></li> <li>▪ <a href="#">SNMP Printer</a></li> <li>▪ <a href="#">SNMP QNAP Logical Disk</a></li> <li>▪ <a href="#">SNMP QNAP Physical Disk</a></li> <li>▪ <a href="#">SNMP QNAP System Health</a></li> <li>▪ <a href="#">SNMP Rittal CMC III Hardware Status</a></li> <li>▪ <a href="#">SNMP RMON</a></li> <li>▪ <a href="#">SNMP SonicWall System Health</a></li> <li>▪ <a href="#">SNMP SonicWall VPN Traffic</a></li> </ul>
---	---	--

<ul style="list-style-type: none"><li>▪ <a href="#">SNMP Custom String</a></li><li>▪ <a href="#">SNMP Custom String Lookup</a></li><li>▪ <a href="#">SNMP Custom Table</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Logical Disk</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Member Health</a></li><li>▪ <a href="#">SNMP Dell EqualLogic Physical Disk</a></li><li>▪ <a href="#">SNMP Dell Hardware</a></li><li>▪ <a href="#">SNMP Dell PowerEdge Physical Disk</a></li><li>▪ <a href="#">SNMP Dell PowerEdge System Health</a></li><li>▪ <a href="#">SNMP Disk Free</a></li></ul>	<ul style="list-style-type: none"><li>▪ <a href="#">SNMP IBM System X System Health</a></li><li>▪ <a href="#">SNMP interSeptor Pro Environment</a></li><li>▪ <a href="#">SNMP Juniper NS System Health</a></li><li>▪ <a href="#">SNMP LenovoEMC Physical Disk</a></li><li>▪ <a href="#">SNMP LenovoEMC System Health</a></li><li>▪ <a href="#">SNMP Library</a></li><li>▪ <a href="#">SNMP Linux Disk Free</a></li><li>▪ <a href="#">SNMP Linux Load Average</a></li><li>▪ <a href="#">SNMP Linux Meminfo</a></li><li>▪ <a href="#">SNMP Linux Physical Disk</a></li><li>▪ <a href="#">SNMP Memory</a></li><li>▪ <a href="#">SNMP NetApp Disk Free</a></li></ul>	<ul style="list-style-type: none"><li>▪ <a href="#">SNMP Synology Logical Disk</a></li><li>▪ <a href="#">SNMP Synology Physical Disk</a></li><li>▪ <a href="#">SNMP Synology System Health</a></li><li>▪ <a href="#">SNMP System Uptime</a></li><li>▪ <a href="#">SNMP Traffic</a></li><li>▪ <a href="#">SNMP Trap Receiver</a></li><li>▪ <a href="#">SNMP Windows Service</a></li></ul>
--	--	--

## Credentials for SNMP Devices

inherit from

**SNMP Version** ⓘ

SNMP v1

SNMP v2c (default)

SNMP v3

**Community String** ⓘ

public

**SNMP Port** ⓘ

161

**Timeout (Sec.)** ⓘ





5

Credentials for SNMP Devices

Setting	Description
SNMP Version	<p>Select the Simple Network Management Protocol (SNMP) version for the connection to the target SNMP device:</p> <ul style="list-style-type: none"> <li>▪ <b>SNMP v1:</b> Use SNMP v1 for the connection. SNMP v1 only offers clear-text data transmission. <ul style="list-style-type: none"> <li>ⓘ SNMP v1 does not support 64-bit counters. This might result in invalid data when you monitor traffic via SNMP.</li> </ul> </li> <li>▪ <b>SNMP v2c (default):</b> Use SNMP v2c for the connection. SNMP v2c also only offers clear-text data transmission but it supports 64-bit counters.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ SNMP v3: Use SNMP v3 for the connection. SNMP v3 provides secure authentication and data encryption.</li> <li>ⓘ SNMP v3 has performance limitations because of the use of encryption. The main limiting factor is CPU power. Also keep in mind that SNMP v3, unlike SNMP v1 and v2c, does not scale with more CPU power. Because of this limitation, PRTG can only handle a limited number of requests per second so that you can use only a limited number of sensors using SNMP v3. If you see an increase in <a href="#">Interval Delay</a> or <a href="#">Open Requests</a> with the <a href="#">Probe Health</a> sensor, distribute the load over <a href="#">multiple probes</a> <small>[6198]</small>. SNMP v1 and SNMP v2c do not have this limitation.</li> </ul>
Community String	<p>This setting is only visible if you select SNMP v1 or SNMP v2c (default) above.</p> <p>Enter the community string of your device. This is like a clear-text password for simple authentication.</p> <p>ⓘ We recommend that you use the default value.</p>
Authentication Method	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Select the authentication method:</p> <ul style="list-style-type: none"> <li>▪ MD5 (default): Use message-digest algorithm 5 (MD5) for authentication.</li> <li>▪ SHA: Use Secure Hash Algorithm (SHA) for authentication.</li> <li>▪ SHA-224: Use SHA-224 for authentication.</li> <li>▪ SHA-256: Use SHA-256 for authentication.</li> <li>▪ SHA-384: Use SHA-384 for authentication.</li> <li>▪ SHA-512: Use SHA-512 for authentication.</li> </ul> <p>ⓘ If you do not want to use authentication but you need SNMP v3, for example, because your device requires <a href="#">context</a>, you can leave the Password field empty. In this case, PRTG uses <a href="#">SNMP_SEC_LEVEL_NOAUTH</a> and it entirely deactivates authentication.</p> <p>ⓘ The authentication method that you select must match the authentication method of your device.</p>
User Name	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter the user name for access to the target SNMP device.</p> <p>ⓘ The user name that you enter must match the user name of your device.</p>



Setting	Description
Password	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter the password for access to the target SNMP device.</p> <p> The password that you enter must match the password of your device.</p>
Encryption Type	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Select an encryption type:</p> <ul style="list-style-type: none"> <li>▪ DES (default): Use Data Encryption Standard (DES) as the encryption algorithm.</li> <li>▪ AES: Use Advanced Encryption Standard (AES) as the encryption algorithm.</li> <li>▪ AES-192: Use AES-192 as the encryption algorithm.</li> <li>▪ AES-256: Use AES-256 as the encryption algorithm.</li> </ul> <p> The encryption type that you select must match the encryption type of your device.</p>
Encryption Key	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter an encryption key. If you provide a key, PRTG encrypts SNMP data packets with the encryption algorithm that you selected above. Enter a string or leave the field empty.</p> <p> The encryption key that you enter must match the encryption key of your device. If the encryption keys do not match, you do not get an error message.</p>
Context Name	<p>This setting is only visible if you select SNMP v3 above.</p> <p>Enter a context name only if the configuration of the device requires it. <b>Context</b> is a collection of management information that is accessible by an SNMP device. Enter a string.</p>
SNMP Port	<p>Enter the port for the connection to the SNMP target device. Enter an integer. The default port is <b>161</b>.</p> <p> We recommend that you use the default value.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).</p>


## Credentials for Database Management Systems


Click  to interrupt the [inheritance](#) .

 The settings you define in this section apply to the following sensors:

- [ADO SQL v2](#)
- [Microsoft SQL v2](#)
- [MySQL v2](#)
- [Oracle SQL v2](#)
- [PostgreSQL](#)


### Credentials for Database Management Systems

 inherit from

**Port** 


Default

Custom port for all database sensors

**Authentication Method** 

Windows authentication with impersonation (default)



SQL server authentication

**Timeout (Sec.)** 

60

Credentials for Database Management Systems

Setting	Description
Port	Select the port that PRTG uses for connections to the monitored databases:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Default: PRTG automatically determines the type of the database and uses the corresponding default port to connect. PRTG uses the following default ports: <ul style="list-style-type: none"> <li>▫ Microsoft SQL: <a href="#">1433</a></li> <li>▫ MySQL: <a href="#">3306</a></li> <li>▫ Oracle SQL: <a href="#">1521</a></li> <li>▫ PostgreSQL: <a href="#">5432</a></li> </ul> </li> <li>▪ Custom port for all database sensors: Select this option if your database management systems do not use the default ports. Enter a custom port for database connections below.</li> </ul>
Custom Port	<p>Enter a custom port for database connections. Enter an integer.</p> <p> PRTG uses this custom port for <a href="#">all</a> database sensors and for connections to <a href="#">all</a> your databases.</p>
Authentication Method	<p>Select the authentication method for the connection to the Structured Query Language (SQL) database:</p> <ul style="list-style-type: none"> <li>▪ Windows authentication with impersonation (default): PRTG uses the Windows credentials that you define in settings that are higher in the <a href="#">object hierarchy</a><sup>132</sup> for the database connection. <ul style="list-style-type: none"> <li> The user whose credentials PRTG uses needs to have permission to log in to the probe system with a database sensor. This is necessary for the impersonation.</li> </ul> </li> <li>▪ SQL server authentication: Use explicit credentials for database connections. Enter a user name and password below.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select SQL server authentication above.</a></p> <p>Enter the user name for the database connection.</p>
Password	<p><a href="#">This setting is only visible if you select SQL server authentication above.</a></p> <p>Enter the password for the database connection.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <a href="#">900</a> seconds (15 minutes).</p>

## Credentials for AWS

Click  to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

- [AWS Alarm v2](#)
- [AWS Cost](#)
- [AWS EBS v2](#)
- [AWS EC2 v2](#)
- [AWS ELB v2](#)
- [AWS RDS v2](#)

**■** For more information about the permissions that are necessary to query the AWS API, see the Knowledge Base: [How do I set permissions for the Amazon Web Services \(AWS\) API key to use certain sensors in PRTG?](#)

## Credentials for AWS

inherit from

**Access Key** **i**

---

**Secret Key** **i**

---

Credentials for AWS

Setting	Description
Access Key	Enter the Amazon Web Services (AWS) access key.
Secret Key	Enter the AWS secret key.

### Credentials for Microsoft 365

Click to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

- [Microsoft 365 Mailbox](#)
- [Microsoft 365 Service Status](#)

- [Microsoft 365 Service Status Advanced](#)

The sensors use the credentials to authenticate with Microsoft Entra ID.

■ For more information about the credentials and the permissions that are necessary to use the Microsoft 365 Service Status sensor and the Microsoft 365 Service Status Advanced sensor, see the Knowledge Base: [How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?](#)

■ For more information about the credentials and the permissions that are necessary to use the Microsoft 365 Mailbox sensor, see the Knowledge Base: [How do I obtain credentials and set permissions for the Microsoft 365 Mailbox sensor?](#)

### Credentials for Microsoft 365

inherit from

**Tenant ID** ⓘ

---

**Client ID** ⓘ

---

**Client Secret** ⓘ

---

**OpenID Connect Configuration** ⓘ

Automatic (default)

Manual

Credentials for Microsoft 365

Setting	Description
Tenant ID	Enter the Microsoft Entra tenant ID. <span style="color: red;">ⓘ</span> A tenant ID must be a 32-digit sequence in hexadecimal notation.
Client ID	Enter the Microsoft Entra client ID.
Client Secret	Enter the Microsoft Entra client secret.

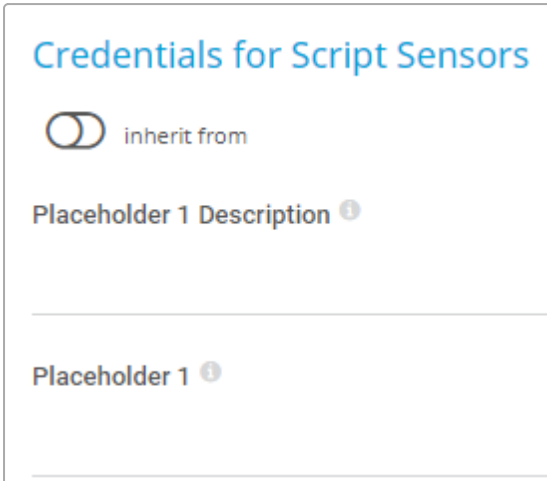
Setting	Description
OpenID Connect Configuration	<p>Select if you want to manually enter the authorization endpoint URL and token endpoint URL that PRTG uses to access Microsoft Graph:</p> <ul style="list-style-type: none"> <li>▪ Automatic (default): PRTG automatically determines the authorization endpoint URL and the token endpoint URL.</li> <li>▪ Manual: Manually enter the authorization endpoint URL and the token endpoint URL.</li> </ul>
Authorization Endpoint	<p>Enter the authorization endpoint URL including the server.</p> <p>Authorization endpoint URL example:</p> <pre>https://login.microsoftonline.com/&lt;tenant-ID&gt;/oauth2/v2.0/authorize</pre> <p><b>i</b> Make sure to replace &lt;tenant-ID&gt; with the <b>directory (tenant) ID</b> from Microsoft Entra ID.</p>
Token Endpoint	<p>Enter the token endpoint URL including the server.</p> <p>Token endpoint URL example:</p> <pre>https://login.microsoftonline.com/&lt;tenant-ID&gt;/oauth2/v2.0/token</pre> <p><b>i</b> Make sure to replace &lt;tenant-ID&gt; with the <b>directory (tenant) ID</b> from Microsoft Entra ID.</p>

## Credentials for Script Sensors

Click  to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

- [EXE/Script](#)
- [EXE/Script Advanced](#)
- [Python Script Advanced](#)
- [Script v2](#)
- [SSH Script](#)
- [SSH Script Advanced](#)



Credentials for Script Sensors

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder1</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder2</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder3</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder4</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.

Setting	Description
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder5</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.


### Credentials for Cisco Meraki


Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:


- [Cisco Meraki License](#)
- [Cisco Meraki Network Health](#)

## Credentials for Cisco Meraki


 inherit from

API Key  .....

---

Meraki Dashboard API Endpoint  `api.meraki.com`

Credentials for Cisco Meraki

Setting	Description
API Key	Enter an API key that the sensor uses for authentication against the Cisco Meraki Dashboard API.
Meraki Dashboard API Endpoint	Enter the endpoint for the Cisco Meraki Dashboard API. The default <a href="#">api.meraki.com</a> should be valid for most use cases.   See the Cisco Meraki Dashboard API documentation for other possible choices.

### Credentials for Dell EMC


Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:



- [Dell EMC Unity Enclosure Health v2](#)
- [Dell EMC Unity File System v2](#)
- [Dell EMC Unity Storage Capacity v2](#)
- [Dell EMC Unity Storage LUN v2](#)
- [Dell EMC Unity Storage Pool v2](#)
- [Dell EMC Unity VMware Datastore v2](#)

## Credentials for Dell EMC

 inherit from

**User Name** i

johnqpublic

---

**Password** i

●●●●●●●●●●

---

**Port** i

443

Credentials for Dell EMC

Setting	Description
User Name	Enter the user name for access to the Dell EMC system.
Password	Enter the password for access to the Dell EMC system.
Port	Enter the port for the connection to the Dell EMC system. The default port for secure connections is <a href="#">443</a> .

## Credentials for FortiGate

Click  to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

- [FortiGate System Statistics](#)
- [FortiGate VPN Overview](#)

### Credentials for FortiGate

inherit from

API Token **i**

●●●●●●●●

---

Port **i**

443

Credentials for FortiGate

Setting	Description
API Token	Enter the API token for access to the FortiGate system.
Port	Enter the port for the connection to the FortiGate system. The default port for secure connections is <a href="#">443</a> .

## Credentials for HPE 3PAR

Click  to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

- [HPE 3PAR Common Provisioning Group](#)
- [HPE 3PAR Drive Enclosure](#)
- [HPE 3PAR Virtual Volume](#)

## Credentials for HPE 3PAR

inherit from

User Name <sup>i</sup>

johnqpulic

Password <sup>i</sup>

●●●●●●●●●●●●●●●●

Protocol <sup>i</sup>

HTTPS (default)

HTTP

WSAPI Port <sup>i</sup>

8080

SSH Port <sup>i</sup>

22

Credentials for HPE 3PAR

Setting	Description
User Name	Enter the user name for access to the HPE 3PAR system.

Setting	Description
Password	Enter the password for access to the HPE 3PAR system.
Protocol	Select the protocol that you want to use for the connection to the HPE 3PAR system: <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
WSAPI Port	Enter the Web Services API (WSAPI) port for the connection to the HPE 3PAR system. The default port for secure connections is <b>8080</b> and the default port for unsecure connections is <b>8008</b> .  <i>i</i> For more information, see the Knowledge Base: <a href="#">Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?</a>
SSH Port	Enter the SSH port for the connection to the HPE 3PAR system. The default port for secure connections is <b>22</b> .

## Credentials for HTTP

Click  to interrupt the [inheritance](#)<sup>136</sup>.

*i* The settings you define in this section apply to the following sensor:

- [HTTP v2](#)

### Credentials for HTTP

inherit from

**Authentication Method** ⓘ

None (default)

Basic authentication

Bearer authentication

**Placeholder 1 Description** ⓘ

---

**Placeholder 1** ⓘ

---

Credentials for HTTP

Setting	Description
Authentication Method	<p>Select the authentication method for access to the server:</p> <ul style="list-style-type: none"> <li>▪ None (default): Use no authentication.</li> <li>▪ Basic authentication: Use basic authentication.</li> <li>▪ Bearer authentication: Use an OAuth2 bearer token.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter the user name for access to the server.</p>
Password	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter the password for access to the server.</p>
Bearer Token	<p><a href="#">This setting is only visible if you select Bearer authentication above.</a></p> <p>Enter a bearer token for access to the server.</p>

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder1</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder2</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder3</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder4</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add <code>%httpplaceholder5</code> in the URL, POST Body, and Custom Headers fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.

## Credentials for Microsoft Azure

Click  to interrupt the [inheritance](#)<sup>136</sup>.



 The settings you define in this section apply to the following sensors:

- [Microsoft Azure SQL Database](#)
- [Microsoft Azure Storage Account](#)
- [Microsoft Azure Subscription Cost](#)
- [Microsoft Azure Virtual Machine](#)

The sensors use the credentials to authenticate with Microsoft Entra ID.

■ For more information about the credentials and permissions that are necessary use the Microsoft Azure sensors, see the Knowledge Base: [How do I obtain credentials and create custom roles for the Microsoft Azure sensors?](#)

### Credentials for Microsoft Azure

 inherit from  Local Probe

**Tenant ID** ⓘ

---

**Client ID** ⓘ

---


**Client Secret** ⓘ

---

**Subscription ID** ⓘ

---

**Microsoft Azure Management Endpoint** ⓘ

management.azure.com 

Credentials for Microsoft Azure

Setting	Description
Tenant ID	Enter the Microsoft Entra tenant ID. <span style="color: red;">ⓘ</span> A tenant ID must be a 32-digit sequence in hexadecimal notation.
Client ID	Enter the Microsoft Entra client ID.

Setting	Description
Client Secret	Enter the Microsoft Entra client secret.
Subscription ID	Enter the Microsoft Entra subscription ID.
Microsoft Azure Management Endpoint	<p>The Microsoft Azure API Management endpoint that all sensors on this object connect to. The default endpoint is <a href="https://management.azure.com">management.azure.com</a>.</p> <p><b>i</b> PRTG shows this value for reference purposes only. We strongly recommend that you only change it if the Paessler support team explicitly asks you to do so. Wrong usage can result in incorrect monitoring data.</p>

## Credentials for MQTT

Click  to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensors:

- [MQTT Round Trip](#)
- [MQTT Statistics](#)
- [MQTT Subscribe Custom](#)



## Credentials for MQTT

inherit from

### Authentication Method i

- None (default)
- User name and password

### Port i

1883


### Transport-Level Security i

- Do not use transport-level security (default)
- Use transport-level security

Credentials for MQTT

Setting	Description
Authentication Method	<p>Select if you want to connect without credentials or define credentials for access to the MQTT broker:</p> <ul style="list-style-type: none"> <li>▪ None (default): Connect without credentials.</li> <li>▪ User name and password: Define credentials for the connection.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select User name and password above.</a></p> <p>Enter the user name for access to the Message Queue Telemetry Transport (MQTT) broker.</p>

Setting	Description
Password	<p>This setting is only visible if you select <a href="#">User name and password above</a>.</p> <p>Enter the password for access to the MQTT broker.</p>
Port	<p>Enter the port for the connection to the MQTT broker. The default port for secure connections is <b>8883</b> and the default port for unsecure connections is <b>1883</b>.</p>
Transport-Level Security	<p>Select if you want to use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection:</p> <ul style="list-style-type: none"> <li>▪ Do not use transport-level security (default): Establish the connection without connection security.</li> <li>▪ Use transport-level security: Establish the connection with the strongest SSL/TLS method that the target device provides.</li> </ul>
Server Authentication	<p>This setting is only visible if you select <a href="#">Use transport-level security above</a>.</p> <p>Select if you want to use a certificate for server authentication:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not use a certificate for server authentication.</li> <li>▪ Enable: Use a certificate for server authentication.</li> </ul>
CA Certificate	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Paste the certificate authority (CA) certificate for the verification of the MQTT broker.</p> <p> The certificate must be in Privacy-Enhanced Mail (PEM) format.</p>
Client Authentication	<p>This setting is only visible if you select <a href="#">Use transport-level security above</a>.</p> <p>Select if you want to use a certificate for client authentication:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not use a certificate for client authentication.</li> <li>▪ Enable: Use a certificate for client authentication.</li> </ul>
Client Certificate	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Paste the certificate that you created for authenticating the sensor against the MQTT broker.</p> <p> The certificate must be in PEM format.</p>
Client Key	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Enter the client key for access to the MQTT broker.</p>

Setting	Description
	 The client key must be in PEM format and it must be encrypted using the Client Key Password.
Client Key Password	<p>This setting is only visible if you select Enable above.</p> <p>Enter the password for the client key.</p>

## Credentials for NetApp

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [NetApp Aggregate v2](#)
- [NetApp I/O v2](#)
- [NetApp LIF v2](#)
- [NetApp LUN v2](#)
- [NetApp NIC v2](#)
- [NetApp Physical Disk v2](#)
- [NetApp SnapMirror v2](#)
- [NetApp System Health v2](#)
- [NetApp Volume v2](#)

The sensors use the credentials for access to the ONTAP System Manager.

## Credentials for NetApp

inherit from Network-01f

**User Name** ⓘ  
johnqpublic

---

**Password** ⓘ  
.....

---

**Port** ⓘ  
443

---

**Protocol** ⓘ

HTTPS (default)

HTTP

Credentials for NetApp

Setting	Description
User Name	Enter a user name for access to the ONTAP System Manager.
Password	Enter the password for access to the ONTAP System Manager.
Port	Enter the port for the connection to the ONTAP System Manager. The default port for secure connections is <a href="#">443</a> .

Setting	Description
Protocol	Select the protocol that you want to use for the connection to the ONTAP System Manager: <ul style="list-style-type: none"><li>▪ HTTPS (default): Use HTTPS for the connection.</li><li>▪ HTTP: Use HTTP for the connection.</li></ul>

## Credentials for OPC UA

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [Beckhoff IPC System Health](#)
- [OPC UA Certificate](#)
- [OPC UA Custom](#)
- [OPC UA Server Status](#)

## Credentials for OPC UA

inherit from

Port <sup>i</sup>

4840

Server Path <sup>i</sup>

Security Mode <sup>i</sup>

None (default)

Sign

Sign & Encrypt



Authentication Method <sup>i</sup>

Anonymous (default)

User name and password

Credentials for OPC UA

Setting	Description
Port	Enter the port for the connection to the OPC Unified Architecture (OPC UA) server. The default port for secure connections is <a href="#">4840</a> .
Server Path	Enter the path of the OPC UA server endpoint if you run more than one server under the same IP address or DNS name.
Security Mode	Select if you want to use encryption: <ul style="list-style-type: none"> <li>▪ None (default): Do not use encryption.</li> <li>▪ Sign: Sign messages between the sensor and the OPC UA server.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Sign &amp; Encrypt: Sign and encrypt messages between the sensor and the OPC UA server.</li> </ul>
Security Policy	<p><a href="#">This setting is only visible if you select Sign or Sign &amp; Encrypt above.</a></p> <p>Select if you want to use a security policy and define which policy you want to use:</p> <ul style="list-style-type: none"> <li>▪ None (default): Do not use a security policy.</li> <li>▪ Basic256Sha256: Use the Basic256Sha256 security policy.</li> <li>▪ Basic256: Use the Basic256 security policy.</li> </ul>
Client Certificate	<p><a href="#">This setting is only visible if you select Sign or Sign &amp; Encrypt above.</a></p> <p>Enter the certificate that you created for authenticating the sensor against the OPC UA server.</p> <p> The certificate must meet the following requirements:</p> <ul style="list-style-type: none"> <li>▪ The key size must be 2048-bit or 4096-bit.</li> <li>▪ The secure hash algorithm must be <a href="#">SHA256</a>.</li> <li>▪ DataEncipherment must be part of the KeyUsage certificate extension.</li> <li>▪ A uniform resource indicator (URI) must be set in subjectAltName.</li> <li>▪ The certificate must be in Privacy-Enhanced Mail (PEM) format.</li> </ul>
Client Key	<p><a href="#">This setting is only visible if you select Sign or Sign &amp; Encrypt above.</a></p> <p>Enter the client key for access to the OPC UA server.</p> <p> The client key must be in PEM format and it must be encrypted using the Client Key Password.</p>
Client Key Password	<p><a href="#">This setting is only visible if you select Sign or Sign &amp; Encrypt above.</a></p> <p>Enter the password for the client key.</p>
Authentication Method	<p>Select if you want to connect without credentials or define credentials for access to the OPC UA server:</p> <ul style="list-style-type: none"> <li>▪ Anonymous (default): Connect without credentials.</li> <li>▪ User name and password: Define credentials for the connection.</li> </ul>

Setting	Description
	<p><b>i</b> Most OPC UA servers do not support User name and password authentication without a client certificate. To use User name and password authentication, select Sign or Sign &amp; Encrypt under Security Mode and Basic256Sha256 or Basic256 under Security Policy and enter the Client Certificate, Client Key, and Client Key Password that you want to use.</p> <p><b>i</b> If you select None (default) under Security Mode and use User name and password authentication, PRTG sends the unencrypted password to the OPC UA server.</p>
User Name	<p>This setting is only visible if you select User name and password <a href="#">above</a>.</p> <p>Enter the user name for access to the OPC UA server.</p>
Password	<p>This setting is only visible if you select User name and password <a href="#">above</a>.</p> <p>Enter the password for access to the OPC UA server.</p>

### Credentials for Soffico Orchestra

Click  to interrupt the [inheritance](#)<sup>136</sup>.

**i** The settings you define in this section apply to the following sensor:

- [Soffico Orchestra Channel Health](#)
- [Soffico Orchestra Scenario](#)



## Credentials for Soffico Orchestra

inherit from

### Authentication Method i

- None (default)  
 User name and password

### Timeout (Sec.) i

60

### Port i

8443

### Protocol i

- HTTPS (default)  
 HTTP

Credentials for Soffico Orchestra

Setting	Description
Authentication Method	<p>Select if you want to connect without credentials or define credentials for access to the Orchestra platform:</p> <ul style="list-style-type: none"> <li>▪ None (default): Connect without credentials.</li> <li>▪ User name and password: Define credentials for the connection.</li> </ul>
User Name	<p>This setting is only visible if you select User name and password above.</p> <p>Enter the user name for access to the Orchestra platform.</p>
Password	<p>This setting is only visible if you select User name and password above.</p>

Setting	Description
	Enter the password for access to the Orchestra platform.
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).
Port	Enter the port for the connection to the Orchestra platform. The default port for secure connections is <b>8443</b> and the default port for unsecure connections is <b>8019</b> .
Protocol	Select the protocol that you want to use for the connection to the Orchestra platform: <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>

### Credentials for Redfish

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [Redfish Power Supply](#)
- [Redfish System Health](#)
- [Redfish Virtual Disk](#)

### Credentials for Redfish

inherit from

**User Name** ⓘ

johnqpublic

---

**Password** ⓘ

●●●●●●●●

---

**Protocol** ⓘ

HTTPS (default)

HTTP

**Port** ⓘ

443

Credentials for Redfish

Setting	Description
User Name	Enter the user name for access to the Redfish system.
Password	Enter the password for access to the Redfish system.
Protocol	<p>Select the protocol that you want to use for the connection to the Redfish system:</p> <ul style="list-style-type: none"> <li>▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ HTTP: Use an unsecure connection.</li> </ul>
Port	Enter the port for the connection to the Redfish system. The default port for secure connections is 443.

## Credentials for REST API


Click  to interrupt the [inheritance](#) 136.

 The settings you define in this section apply to the following sensor:

- [REST Custom v2](#)

### Credentials for REST API

inherit from

**Authentication Method** 

None (default)

Basic authentication

Bearer authentication

Credentials for REST API

Setting	Description
Authentication Method	Select the authentication method for access to the Representational State Transfer (REST) application programming interface (API): <ul style="list-style-type: none"> <li>▪ None (default): Use no authentication.</li> <li>▪ Basic authentication: Use basic authentication.</li> <li>▪ Bearer authentication: Use an OAuth2 bearer token.</li> </ul>
User Name	<a href="#">This setting is only visible if you select Basic authentication above.</a> Enter the user name for access to the REST API.
Password	<a href="#">This setting is only visible if you select Basic authentication above.</a> Enter the password for access to the REST API.
Bearer Token	<a href="#">This setting is only visible if you select Bearer authentication above.</a> Enter a bearer token for access to the REST API.
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.

Setting	Description
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder1</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder2</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder3</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder4</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add <code>%restplaceholder5</code> in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.


## Credentials for Veeam

Click  to interrupt the [inheritance](#)<sup>136</sup>.

 The settings you define in this section apply to the following sensors:

- [Veeam Backup Job Status](#)
- [Veeam Backup Job Status Advanced](#)

## Credentials for Veeam

 inherit from

**User Name** i

**Password** i

**Port** i

Credentials for Veeam

Setting	Description
User Name	Enter the user name for access to the Veeam Backup Enterprise Manager.
Password	Enter the password for access to the Veeam Backup Enterprise Manager.
Port	Enter the port for the connection to the Veeam Backup Enterprise Manager. The default port for secure connections is <a href="#">9398</a> .

### Windows Compatibility Options

Click  to interrupt the [inheritance](#)<sup>136</sup>.

If you experience problems when you monitor via Windows sensors, use the following compatibility options for troubleshooting.

## Windows Compatibility Options

inherit from

### Preferred Data Source ⓘ

- Performance counters and WMI as fallback
- Performance counters only
- WMI only (default)

### Timeout Method ⓘ

- Use 1.5× scanning interval (default)
- Set manually

Windows Compatibility Options

Setting	Description
Preferred Data Source	<p><span>ⓘ</span> This setting only applies to hybrid sensors that use both performance counters and Windows Management Instrumentation (WMI).</p> <p>Define the method that Windows sensors use to query data:</p> <ul style="list-style-type: none"> <li>▪ Performance counters and WMI as fallback: Try to query data via performance counters. If this is not possible, establish a connection via WMI.</li> <li>▪ Performance counters only: Query data via performance counters only. If this is not possible, the sensor returns no data.</li> <li>▪ WMI only (default): Query data via WMI only. If this is not possible, the sensor returns no data.</li> </ul>
Timeout Method	<p>Select the time that the sensor waits for the return of the WMI query before the sensor cancels the query and shows an error message:</p> <ul style="list-style-type: none"> <li>▪ Use 1.5× scanning interval (default): Multiply the scanning interval of the sensor by 1.5 and use the resulting value.</li> <li>▪ Set manually: Manually enter a timeout value.</li> </ul> <p><span>ⓘ</span> We recommend that you use the default value.</p> <p><span>ⓘ</span> If you experience ongoing timeout errors, try increasing the timeout value.</p>

Setting	Description
Timeout (Sec.)	<p>This setting is only visible if you select <a href="#">Set manually</a> <a href="#">above</a>.</p> <p>Enter the time the sensor waits for the return of its WMI query before it cancels it and shows an error message. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p>

## SNMP Compatibility Options

Click  to interrupt the [inheritance](#)<sup>136</sup>.

If you experience problems when you monitor via Simple Network Management Protocol (SNMP) sensors, use the following compatibility options for troubleshooting.



## SNMP Compatibility Options

inherit from

SNMP Delay (ms) <sup>i</sup>

0

---

Failed Requests <sup>i</sup>

Retry (default)

Do not retry

Overflow Values <sup>i</sup>

Ignore (default)

Handle overflow values as valid results

Zero Values <sup>i</sup>

Ignore (default)

Handle zero values as valid results for delta sensors

32-bit/64-bit Counters <sup>i</sup>

Use 64-bit counters if available (default)

Use 32-bit counters only

Request Mode <sup>i</sup>

Use multi get (default)

Use single get







Walk Mode <sup>i</sup>




Use GETBULK requests (default)

Use GETNEXT requests

Setting	Description
SNMP Delay (ms)	<p>Enter the time in milliseconds (ms) that PRTG waits between two SNMP requests. You can define a delay between 0 and 100. Enter an integer.</p> <ul style="list-style-type: none"> <li><span data-bbox="485 450 512 488">i</span> We recommend that you use the default value.</li> <li><span data-bbox="536 501 563 539">i</span> If you experience SNMP connection failures, try increasing the delay.</li> </ul>
Failed Requests	<p>Select if an SNMP sensor tries again after a request fails:</p> <ul style="list-style-type: none"> <li><span data-bbox="485 669 496 685">▪</span> <b>Retry (default):</b> Try again if an SNMP request fails. This can prevent false error messages because of temporary timeout failures.</li> <li><span data-bbox="485 752 496 768">▪</span> <b>Do not retry:</b> Do not retry if an SNMP request fails. If you select this option, an SNMP sensor shows a Down status earlier.</li> </ul>
Overflow Values	<p>Select how PRTG handles overflow values. Some devices do not correctly handle internal buffer overflows. This can cause false peaks. PRTG can handle overflow values in two ways:</p> <ul style="list-style-type: none"> <li><span data-bbox="485 983 496 999">▪</span> <b>Ignore (default):</b> Ignore overflow values and do not include them in the monitoring data. We recommend that you use this option.</li> <li><span data-bbox="485 1066 496 1081">▪</span> <b>Handle overflow values as valid results:</b> Regard all overflow values as regular data and include them in the monitoring data.</li> </ul> <p><span data-bbox="485 1144 512 1182">i</span> If you experience problems because of strange peaks in your data graphs, change this option. Peaks might indicate that the target device resets counters without an overflow. PRTG interprets such behavior as overflow that results in data peaks. Select the option Ignore (default) in this case. For more information, see the Knowledge Base: <a href="#">What is the Overflow Values setting in the SNMP Compatibility Options?</a></p>
Zero Values	<p>Select how PRTG handles zero values. Some devices send incorrect zero values. This can cause false peaks. PRTG can handle zero values in two ways:</p> <ul style="list-style-type: none"> <li><span data-bbox="485 1505 496 1520">▪</span> <b>Ignore (default):</b> Ignore zero values and do not include them in the monitoring data. We recommend that you use this option.</li> </ul> <p><span data-bbox="485 1583 512 1621">i</span> If you experience problems, try changing this option.</p> <ul style="list-style-type: none"> <li><span data-bbox="485 1639 496 1655">▪</span> <b>Handle zero values as valid results for delta sensors:</b> Regard all zero values as regular data and include them in the monitoring data.</li> </ul>
32-bit/64-bit Counters	<p>Select the type of traffic counters that PRTG searches for on a device:</p> <ul style="list-style-type: none"> <li><span data-bbox="485 1805 496 1821">▪</span> <b>Use 64-bit counters if available (default):</b> The interface scan uses 64-bit traffic counters, if available. This can avoid buffer overflows in the devices.</li> </ul> <p><span data-bbox="485 1912 512 1951">i</span> We recommend that you use the default value.</p> <p><span data-bbox="536 1964 563 2002">i</span> If you experience problems, try changing this option.</p>

Setting	Description
	<ul style="list-style-type: none"> <li>Use 32-bit counters only: The interface scan always uses 32-bit traffic counters, even if 64-bit counters are available. This can make monitoring more reliable for some devices.</li> </ul>
Request Mode	<p>Select the request method that PRTG uses for SNMP sensors:</p> <ul style="list-style-type: none"> <li>Use multi get (default): Bundle multiple SNMP requests into one request. We recommend that you use this option.</li> </ul> <p><b>i</b> If you experience problems, try changing this option.</p> <ul style="list-style-type: none"> <li>Use single get: Use one request for each SNMP value. This can increase compatibility with older devices.</li> </ul> <p><b>i</b> PRTG uses <a href="#">paging</a> for SNMP requests. This means that if a sensor must query more than 20 object identifiers (OID), it automatically polls the OIDs in packages of 20 OIDs each.</p>
Walk Mode	<p>Select the kind of SNMP walk that PRTG uses for SNMP sensors:</p> <ul style="list-style-type: none"> <li>Use GETBULK requests (default): Request the next <b>x</b> OIDs in one SNMP request. The default value is <b>10</b>. It is dynamic based on the response size.</li> </ul> <p><b>i</b> This option only works with devices that support SNMP as of version v2c. Make sure that you set the correct SNMP Version in the Credentials for SNMP Devices settings of the parent device or inherit it from objects that are higher in the <a href="#">object hierarchy</a><sup>132</sup>.</p> <ul style="list-style-type: none"> <li>Use GETNEXT requests: Request one OID at a time. This can increase compatibility with older devices or with devices that have insufficient SNMP BULKWALK support.</li> </ul>
Port Name Template	<p>Select how PRTG displays the name of SNMP sensors. Enter a template that uses several variables. When you add new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID, several fields with interface descriptions are usually available. They are different for every device and OID. PRTG uses the information in these fields to name the sensors. If a field is empty or if it is not available, PRTG adds an empty string to the name. By default, the port name template is <b>([port]) [ifalias] [ifsensor]</b>, which creates a name like <b>(001) Ethernet1 Traffic</b>. You can use and combine any field names that are available at an OID of your device, for example:</p> <ul style="list-style-type: none"> <li>[port]: The port number of the monitored interface.</li> <li>[ifalias]: The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling.</li> <li>[ifname]: The textual name of the monitored interface as assigned by the local device.</li> <li>[ifdescr]: A textual string containing information about the target device or interface, for example, manufacturer, product name, or version.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ [ifspeed]: An estimate of the monitored interface's current bandwidth (Kbit/s).</li> <li>▪ [ifsensor]: The type of the sensor, this is <a href="#">Traffic</a> or <a href="#">RMON</a>. This helps to differentiate between <a href="#">SNMP Traffic</a> and <a href="#">SNMP RMON</a> sensors.</li> </ul> <p> For more information about SNMP sensor names, see the Knowledge Base: <a href="#">How can I change the defaults for names automatically generated for new SNMP sensors?</a></p>
Port Name Update	<p>Select how PRTG reacts if you change the names of ports in your physical device (for example, a switch or router):</p> <ul style="list-style-type: none"> <li>▪ Keep port names (use this if you edit the names in PRTG) (default): Do not automatically adjust sensor names. This is the best option if you want to manually change names in PRTG.</li> <li>▪ Automatically update sensor names if port names change in the device: If PRTG detects port name changes in your physical device, it tries to automatically adjust the sensor names accordingly.</li> </ul> <p> For more information about automatic name updates, see the Knowledge Base: <a href="#">Automatically update port name and number for SNMP Traffic sensors when the device changes them.</a></p>
Port Identification	<p>Select the field that PRTG uses for SNMP interface identification:</p> <ul style="list-style-type: none"> <li>▪ Automatic identification (default): Try the ifAlias field first to identify an SNMP interface and then try ifDescr. <ul style="list-style-type: none"> <li> PRTG does not automatically try ifName.</li> </ul> </li> <li>▪ Use IfAlias: For most devices, ifAlias is the best field to use for unique interface names.</li> <li>▪ Use IfDescr: Use this option if the port order of your device changes after a restart, and if no ifAlias field is available. For example, this is the best option for Cisco ASA devices. <ul style="list-style-type: none"> <li> If you use this option, it is important that your device returns unique interface names in the ifDescr field.</li> </ul> </li> <li>▪ Use IfName: You can also use this option if no unique ifAlias is available. <ul style="list-style-type: none"> <li> If you use this option, it is important that your device returns unique interface names in the ifName field.</li> </ul> </li> <li>▪ Do not update ports: Use this option to disable the automatic port identification.</li> </ul>
Start Interface Index	<p> This setting only applies to <a href="#">SNMP Traffic sensors</a> and to <a href="#">Cisco IP SLA sensors</a>.</p> <p>Enter the index at which PRTG starts to query the interface range during sensor creation. Enter <b>0</b> for the automatic mode.</p>

Setting	Description
	<p> We recommend that you use the default value.</p>
End Interface Index	<p> This setting only applies to <a href="#">SNMP Traffic sensors</a> and to <a href="#">Cisco IP SLA sensors</a>.</p> <p>Enter the index at which PRTG stops querying the interface range during sensor creation. Enter 0 for the automatic mode.</p> <p> We recommend that you use the default value.</p>

## Proxy Settings

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

 The settings you define in this section apply to the following sensors:

<ul style="list-style-type: none"> <li>▪ <a href="#">AWS Alarm v2</a></li> <li>▪ <a href="#">AWS Cost</a></li> <li>▪ <a href="#">AWS EBS v2</a></li> <li>▪ <a href="#">AWS EC2 v2</a></li> <li>▪ <a href="#">AWS ELB v2</a></li> <li>▪ <a href="#">AWS RDS v2</a></li> <li>▪ <a href="#">Cisco Meraki License</a></li> <li>▪ <a href="#">Cisco Meraki Network Health</a></li> <li>▪ <a href="#">Cloud HTTP v2</a></li> <li>▪ <a href="#">Cloud Ping v2</a></li> <li>▪ <a href="#">Dell EMC Unity Enclosure Health v2</a></li> <li>▪ <a href="#">Dell EMC Unity File System v2</a></li> <li>▪ <a href="#">Dell EMC Unity Storage Capacity v2</a></li> <li>▪ <a href="#">Dell EMC Unity Storage LUN v2</a></li> <li>▪ <a href="#">Dell EMC Unity Storage Pool v2</a></li> <li>▪ <a href="#">Dell EMC Unity VMware Datastore v2</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">HPE 3PAR Common Provisioning Group</a></li> <li>▪ <a href="#">HPE 3PAR Drive Enclosure</a></li> <li>▪ <a href="#">HPE 3PAR Virtual Volume</a></li> <li>▪ <a href="#">HTTP</a></li> <li>▪ <a href="#">HTTP v2</a></li> <li>▪ <a href="#">HTTP Advanced</a></li> <li>▪ <a href="#">HTTP Apache ModStatus PerfStats</a></li> <li>▪ <a href="#">HTTP Apache ModStatus Totals</a></li> <li>▪ <a href="#">HTTP Content</a></li> <li>▪ <a href="#">HTTP Data Advanced</a></li> <li>▪ <a href="#">HTTP Transaction</a></li> <li>▪ <a href="#">Microsoft 365 Mailbox</a></li> <li>▪ <a href="#">Microsoft 365 Service Status</a></li> <li>▪ <a href="#">Microsoft 365 Service Status Advanced</a></li> <li>▪ <a href="#">Microsoft Azure SQL Database</a></li> <li>▪ <a href="#">Microsoft Azure Storage Account</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">NetApp Aggregate v2</a></li> <li>▪ <a href="#">NetApp I/O v2</a></li> <li>▪ <a href="#">NetApp LIF v2</a></li> <li>▪ <a href="#">NetApp LUN v2</a></li> <li>▪ <a href="#">NetApp NIC v2</a></li> <li>▪ <a href="#">NetApp Physical Disk v2</a></li> <li>▪ <a href="#">NetApp SnapMirror v2</a></li> <li>▪ <a href="#">NetApp System Health v2</a></li> <li>▪ <a href="#">NetApp Volume v2</a></li> <li>▪ <a href="#">Redfish Power Supply</a></li> <li>▪ <a href="#">Redfish Virtual Disk</a></li> <li>▪ <a href="#">Redfish Power Supply</a></li> <li>▪ <a href="#">REST Custom</a></li> <li>▪ <a href="#">REST Custom v2</a></li> <li>▪ <a href="#">Soffico Orchestra Channel Health</a></li> <li>▪ <a href="#">Soffico Orchestra Scenario</a></li> <li>▪ <a href="#">Veeam Backup Job Status</a></li> <li>▪ <a href="#">Veeam Backup Job Status Advanced</a></li> </ul>
---	---	---

<ul style="list-style-type: none"> <li>▪ <a href="#">FortiGate System Statistics</a></li> <li>▪ <a href="#">FortiGate VPN Overview</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Microsoft Azure Subscription Cost</a></li> <li>▪ <a href="#">Microsoft Azure Virtual Machine</a></li> </ul>	<ul style="list-style-type: none"> <li>▪ <a href="#">Zoom Service Status</a></li> </ul>
---	--	---

The proxy settings determine how a sensor connects to a URL. You can enter data for an HTTP proxy server that sensors use when they connect via HTTP or HTTPS.

- ⓘ This setting only applies to sensors and how they monitor. For more information on how to change the proxy settings for the PRTG core server, see section [Core & Probes](#)<sup>[2888]</sup>.
- ⓘ The [SSL Certificate](#) sensor and the [SSL Security Check](#) sensor do not support HTTP proxies but you can configure connections via SOCKS proxies in the sensors' settings:

## Proxy Settings

inherit from

**IP Address/DNS Name** ⓘ

192.0.2.0

---

**Port** ⓘ

8080

---

**User Name** ⓘ

johnqpublic




---

**Password** ⓘ

.....

Proxy Settings

Setting	Description
IP Address/DNS Name	Enter the IP address or Domain Name System (DNS) name of the proxy server. If you leave this field empty, sensors do not use a proxy.

Setting	Description
	 PRTG currently supports only HTTP proxies.
Port	Enter the port number of the proxy. The default port is <b>8080</b> . Enter an integer.
User Name	If the proxy requires authentication, enter the user name for the proxy login. Enter a string or leave the field empty.   Only basic authentication is available.
Password	If the proxy requires authentication, enter the password for the proxy login. Enter a string or leave the field empty.   Only basic authentication is available.

### Scanning Interval

Click  to interrupt the [inheritance](#) .

#### Scanning Interval

inherit from

**Scanning Interval** 

60 seconds ▼

---

**If a Sensor Query Fails** 


Set sensor to warning status for 1 interval, then set to down status (default) ▼

Scanning Interval

Setting	Description
Scanning Interval	Select a scanning interval from the dropdown list that determines the amount of time that the sensor waits between two scans: <ul style="list-style-type: none"> <li>▪ 30 seconds</li> <li>▪ 60 seconds</li> <li>▪ 5 minutes</li> <li>▪ 10 minutes</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ 15 minutes</li> <li>▪ 30 minutes</li> <li>▪ 1 hour</li> <li>▪ 4 hours</li> <li>▪ 6 hours</li> <li>▪ 12 hours</li> <li>▪ 24 hours</li> </ul> <p><b>i</b> You can change the available intervals in the <a href="#">system administration</a> [2870] of PRTG Network Monitor.</p>
<p>If a Sensor Scanning Fails</p>	<p>Select the number of scanning intervals that the sensor has time to reach and to check a device again if a sensor scanning fails. Depending on the option that you select, the sensor can try to reach and to check a device again several times before the sensor shows the Down <a href="#">status</a> [187]. This can avoid false alarms if the target device only has temporary issues. For previous scanning intervals with failed requests, the sensor shows the Warning status.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> <li>▪ Set sensor to down status immediately: Set the sensor to the Down status immediately after the first request fails.</li> <li>▪ Set sensor to warning status for 1 interval, then set to down status (default): Set the sensor to the Warning status after the first request fails. If the second request also fails, the sensor shows the Down status.</li> <li>▪ Set sensor to warning status for 2 intervals, then set to down status: Set the sensor to the Down status only after the third request fails.</li> <li>▪ Set sensor to warning status for 3 intervals, then set to down status: Set the sensor to the Down status only after the fourth request fails.</li> <li>▪ Set sensor to warning status for 4 intervals, then set to down status: Set the sensor to the Down status only after the fifth request fails.</li> <li>▪ Set sensor to warning status for 5 intervals, then set to down status: Set the sensor to the Down status only after the sixth request fails.</li> </ul> <p><b>i</b> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval before they show the Down status. It is not possible to immediately set a WMI sensor to the Down status, so the first option does not apply to these sensors. All other options can apply.</p> <p><b>i</b> If you define error limits for a sensor's channels, the sensor immediately shows the Down status. None of the interval options apply.</p>




Setting	Description
	<p> If a channel uses <a href="#">lookup</a> values, the sensor immediately shows the Down status. None of the interval options apply.</p>

## Schedules, Dependencies, and Maintenance Window

Click  to interrupt the [inheritance](#).

### Schedules, Dependencies, and Maintenance Window

 inherit from

*Schedules, dependencies, and maintenance windows always pause all sensors inside a group or device. This pausing is always inherited to all child objects and the inheritance cannot be disabled. Below you can set additional schedules, dependencies, or maintenance windows that will be used in parallel to any inherited setting.*

**Schedule** ⓘ

None ▼

---

**Maintenance Window** ⓘ

Do not set up a one-time maintenance window (default)

Set up a one-time maintenance window

**Dependency Type** ⓘ


Use parent (default)

Select a sensor

Schedules, Dependencies, and Maintenance Window

Setting	Description
Schedule	<p>Select a schedule from the list. You can use schedules to monitor during a certain time span (days or hours) every week:</p> <ul style="list-style-type: none"> <li>▪ None</li> <li>▪ Saturdays</li> <li>▪ Sundays</li> <li>▪ Weekdays</li> <li>▪ Weekdays Eight-To-Eight (08:00 - 20:00)</li> <li>▪ Weekdays Nights (17:00 - 09:00)</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Weekdays Nights (20:00 - 08:00)</li> <li>▪ Weekdays Nine-To-Five (09:00 - 17:00)</li> <li>▪ Weekends</li> </ul> <p><b>i</b> You can create schedules, edit schedules, or pause monitoring for a specific time span. For more information, see section <a href="#">Schedules</a> <sup>[2848]</sup>.</p>
Maintenance Window	<p>Select if you want to set up a one-time maintenance window:</p> <ul style="list-style-type: none"> <li>▪ Do not set up a one-time maintenance window (default): Do not set up a one-time maintenance window. Monitoring is always active.</li> <li>▪ Set up a one-time maintenance window: Set up a one-time maintenance window and pause monitoring for the selected object and all child objects. You can define a time span for the pause below.</li> </ul> <p><b>i</b> To cancel an active maintenance window before the defined end date, change the time entry under Maintenance Ends to a date in the past.</p>
Maintenance Begins	<p><b>This setting is only visible if you select</b> Set up a one-time maintenance window <a href="#">above</a>.</p> <p>Use the date time picker to enter the start date and time of the one-time maintenance window.</p>
Maintenance Ends	<p><b>This setting is only visible if you select</b> Set up a one-time maintenance window <a href="#">above</a>.</p> <p>Use the date time picker to enter the end date and time of the one-time maintenance window.</p>
Dependency Type	<p>Select a dependency type. You can use dependencies to pause monitoring for an object depending on the status of a different object:</p> <ul style="list-style-type: none"> <li>▪ Use parent (default): Use the dependency type of the parent object.</li> <li>▪ Select a sensor: Use the dependency type of the parent object. Additionally, pause the current object if a specific sensor is in the Down status or in the Paused status because of another dependency.</li> </ul> <p><b>i</b> You do not trigger a status change by dependency if you manually pause a master sensor or if you pause it by schedule.</p> <p><b>i</b> To test your <a href="#">dependencies</a> <sup>[2728]</sup>, select Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later, all dependent objects are paused. You can check all dependencies under Devices   Dependencies in the main menu bar.</p>
Dependency	<p><b>This setting is only visible if you select</b> Select a sensor <a href="#">above</a>.</p>

Setting	Description
	Click  and use the <a href="#">object selector</a> <sup>[222]</sup> to select a sensor on which the current object will depend.
Dependency Delay (Sec.)	<p>This setting is only visible if you select <a href="#">Select a sensor above</a>.</p> <p>Define a time span in seconds for the dependency delay.</p> <p>After the master sensor for this dependency returns to the Up status, PRTG additionally delays the monitoring of the dependent objects by the time span you define. This can prevent false alarms, for example, after a server restart or to give systems more time for all services to start. Enter an integer.</p>

### Access Rights

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

#### Access Rights


inherit from

**User Group Access** ⓘ

User Group	Rights
PRTG Users Group	Write access
Read-only User Group	Read access
SSO User Group	Inherited (No access)

Revert access rights of child objects to "inherited"

Access Rights

Setting	Description
User Group Access	<p>Select the <a href="#">user groups</a><sup>[2912]</sup> that have access to the object. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights:</p> <ul style="list-style-type: none"> <li>▪ Inherited: Inherit the access rights settings of the parent object.</li> <li>▪ No access: Users in this user group cannot see or edit the object. The object neither shows up in lists nor in the device tree. <ul style="list-style-type: none"> <li>ⓘ There is one exception: If a user in this user group has access to a child object, the parent object is visible in the device tree but users in this user group cannot access it.</li> </ul> </li> <li>▪ Read access: Users in this group can see the object and view its monitoring results. They cannot edit any settings.</li> <li>▪ Write access: Users in this group can see the object, view its monitoring results, and edit its settings. They cannot edit its access rights settings.</li> <li>▪ Full access: Users in this group can see the object, view its monitoring results, edit its settings, and edit its access rights settings.</li> </ul> <p>To automatically set all child objects to inherit this object's access rights, select the Revert access rights of child objects to "inherited" option.</p> <p> For more information on access rights, see section <a href="#">Access Rights Management</a><sup>[145]</sup>.</p>









## Channel Unit Configuration

Click  to interrupt the [inheritance](#)<sup>[136]</sup>.

## Channel Unit Configuration

inherit from

### Channel Unit Types i

 Channel Type	 Unit
Bytes (Bandwidth)	MB 
	Mbit 
	/ sec... 
Bytes (Memory)	GB 
Bytes (Disk)	GB 
Bytes (File)	MB 


Channel Unit Configuration

Setting	Description
Channel Unit Types	<p>For each type of channel, select the unit in which PRTG displays the data. If you define this setting on probe, group, or device level, you can inherit these settings to all sensors underneath. You can set units for the following channel types (if available):</p> <ul style="list-style-type: none"> <li>▪ Bandwidth</li> <li>▪ Memory</li> <li>▪ Disk</li> <li>▪ File</li> <li>▪ Custom</li> </ul> <p><b>i</b> Custom channel types are only available on sensor level.</p> <p><b>i</b> Which channel units are available depends on the sensor type and the available parameters. If no configurable channels are available, this field shows <a href="#">No configurable channels</a>.</p>

### Advanced Network Analysis

Click  to interrupt the [inheritance](#) <sup>136</sup>.

#### Advanced Network Analysis

 inherit from

**Unusual Detection** **i**

Enable (default)  
 Disable

**Similar Sensors Detection** **i**

Enable (default)  
 Disable

**System Information** **i**

Enable (default)  
 Disable

Advanced Network Analysis

Setting	Description
Unusual Detection	<p>Select if you want to use the <a href="#">unusual detection</a> for sensors:</p> <ul style="list-style-type: none"> <li>Enable (default): Activates the unusual detection for this object and, by default, for all objects underneath in the <a href="#">object hierarchy</a>. Sensors that are affected by this setting show the Unusual status if PRTG detects unusual activity.</li> <li>Disable: Does not activate the unusual detection. PRTG ignores unusual values for sensors that are affected by this setting. These sensors do not show the Unusual status.</li> </ul> <p><b>i</b> You can configure the behavior of the unusual detection or completely disable it in the <a href="#">system settings</a>.</p>
Similar Sensors Detection	<p>Select if you want to activate the <a href="#">similar sensors</a> analysis:</p> <ul style="list-style-type: none"> <li>Enable (default): Activates the similar sensors detection for this object and, by default, for all objects underneath in the object hierarchy. PRTG considers all sensors that are affected by this setting during the similarity analysis.</li> <li>Disable: Does not activate the similar sensors detection. PRTG does not consider sensors that are affected by this setting during the similarity analysis.</li> </ul> <p><b>i</b> You can configure the depth of the analysis of the similar sensors detection or completely disable it in the <a href="#">system settings</a>.</p>
System Information	<p>Select if you want to retrieve and show <a href="#">system information</a> for your devices:</p> <ul style="list-style-type: none"> <li>Enable (default): Activates the system information feature for this object and, by default, for all objects underneath in the hierarchy.</li> <li>Disable: Does not activate the system information feature.</li> </ul> <p><b>i</b> The System Information feature is enabled by default. To retrieve the data, PRTG automatically uses the <a href="#">credentials for Windows systems</a> and the <a href="#">credentials for SNMP devices</a> that you entered in the device settings or that the device <a href="#">inherits</a> from a parent object like the root group. Consider this when you monitor devices that are outside of your local network, especially when you use <a href="#">SNMP v1</a> or <a href="#">SNMP v2c</a>, which do not provide encryption.</p> <p><b>☁</b> This setting is not available on the hosted probe of a PRTG Hosted Monitor instance.</p>

More

**KNOWLEDGE BASE**

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- <https://kb.paessler.com/en/topic/38083>

Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?

- <https://kb.paessler.com/en/topic/89717>

How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?

- <https://kb.paessler.com/en/topic/88462>

How do I obtain credentials and create custom roles for the Microsoft Azure sensors?

- <https://kb.paessler.com/en/topic/88625>

What is the Overflow Values setting in the SNMP Compatibility Options?

- <https://kb.paessler.com/en/topic/43503>

How can I change the defaults for names automatically generated for new SNMP sensors?

- <https://kb.paessler.com/en/topic/7363>

Automatically update port name and number for SNMP Traffic sensors when the device changes them

- <https://kb.paessler.com/en/topic/25893>



## 7.8 Sensor Settings

There is a dedicated section for every sensor with details about the available settings.

### Basic Sensor Settings

Every sensor has the same basic settings.

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  X +

**Priority** ⓘ ★★★★☆

Basic Sensor Settings

Setting	Description
Sensor Name	<p>Enter a name to identify the sensor. By default, PRTG shows this name in the <a href="#">device tree</a>, as well as in <a href="#">alarms</a>, <a href="#">logs</a>, <a href="#">notifications</a>, <a href="#">reports</a>, <a href="#">maps</a>, <a href="#">libraries</a>, and <a href="#">tickets</a>.</p> <p> ⓘ If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Parent Tags	<p>The <a href="#">tags</a> that the sensor <a href="#">inherits</a> from its parent <a href="#">device</a>, parent <a href="#">group</a>, and parent <a href="#">probe</a>.</p> <p> ⓘ This setting is for your information only. You cannot change it.</p>
Tags	<p>Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically <a href="#">inherited</a>.</p> <p> ⓘ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (&lt;&gt;).</p> <p> ⓘ For performance reasons, it can take some minutes until you can filter for new tags that you added.</p> <p> ⓘ Every sensor has <a href="#">default tags</a>. For more information, see the specific sensor settings section.</p>

Setting	Description
Priority	Select a priority for the sensor. This setting determines the position of the sensor in lists. The highest priority is at the top of a list. Choose from the lowest priority ( ★☆☆☆☆ ) to the highest priority ( ★★★★★ ).

■ For more information, see section [Available Sensor Types](#).

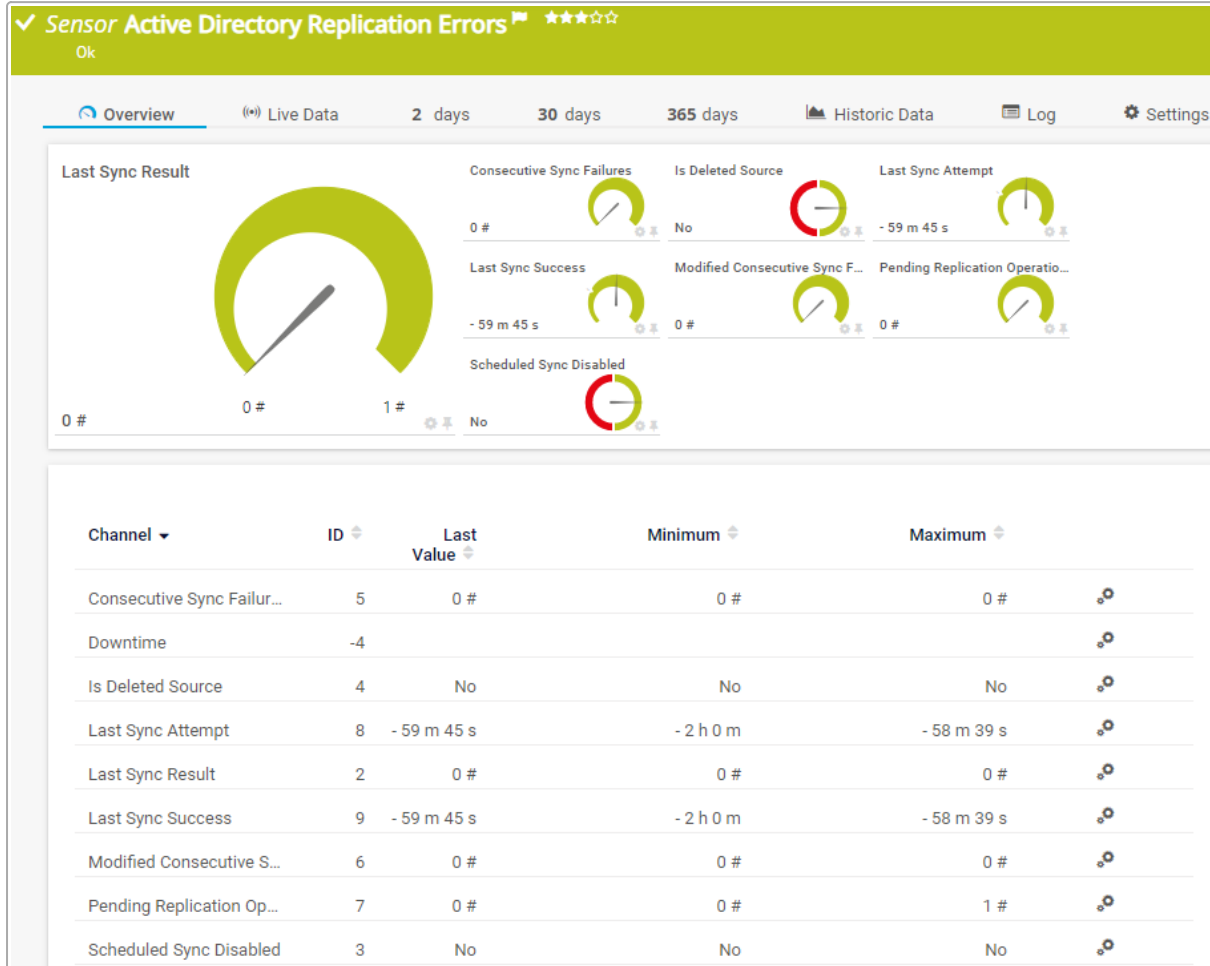
■ For sensor settings, multi-edit is also available. This lets you to change properties of many sensors at the same time. For more information, see section [Multi-Edit](#).

To detect unexpected correlations between your network components, PRTG provides a [similar sensors](#) analysis.

ⓘ Usually, a sensor connects to the IP Address/DNS Name of the parent device. See the [device settings](#) for details. For some sensors, you can explicitly define the monitoring target in the sensor settings.

## 7.8.1 Active Directory Replication Errors Sensor

The Active Directory Replication Errors sensor checks a Windows domain controller (DC) for replication errors.



Active Directory Replication Errors Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>673</sup>.

### Sensor in Other Languages

- Dutch: Active Directory Replicatie Fouten
- French: Active Directory erreurs de réplication
- German: Active Directory Replikationsfehler
- Japanese: AD レプリケーションエラー監視
- Portuguese: Erros de replicação Active Directory
- Russian: Ошибки репликации Active Directory
- Simplified Chinese: 活动目录复制错误
- Spanish: Errores de replicación Active Directory

## Remarks

Consider the following [remarks](#) <sup>670</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Member of Windows domain	This sensor only works if the probe system is part of the domain whose Active Directory you want to monitor.
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node. If the sensor shows the error PE087, additionally install .NET 3.5 on the probe system.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Windows Server	We recommend Windows Server 2016 on the probe system for best performance of this sensor.
Parent device	This sensor requires that the parent device is a DC.
Credentials	<p>This sensor requires credentials for Windows systems. Otherwise, the sensor cannot correctly connect.</p> <p> We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system.</p>
IPv6	This sensor supports IPv6.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ 
 ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- ptfsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Settings

### Sensor Settings

**Replication Neighbor** ⓘ Example

---

**Naming Context** ⓘ Configuration (default)

Sensor Settings

Setting	Description
Replication Neighbor	The replication neighbor whose replication connection this sensor monitors.
Naming Context	<p>Select the Active Directory naming context that you want to monitor:</p> <ul style="list-style-type: none"> <li>▪ Configuration (default): Includes information about partitions, sites, services, or the Active Directory schema.</li> <li>▪ Schema: Includes the information by which objects, classes, and attributes that are used in the Active Directory are defined.</li> <li>▪ DomainDnsZones: Includes information about the domain controllers that are in the domain.</li> <li>▪ Domain: Includes domain information that is replicated to this domain's domain controllers, for example information about computers or users. <ul style="list-style-type: none"> <li><span style="color: red;">ⓘ</span> The probe system must be part of the domain whose naming context you want to monitor.</li> </ul> </li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>ForestDnsZones: Includes information about domain controllers in the forest.</li> </ul> <p><b>i</b> You cannot change this value after sensor creation.</p>

## Debug Options

**Debug Options**

**Result Handling** **i**
 Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**


**Primary Channel** **i** Downtime

---


**Graph Type** **i**
 Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are</p>

Setting	Description
	<p>available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Setting	Description
Consecutive Sync Failures	The number of consecutive synchronization failures
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Setting	Description
Is Deleted Source	If the source is deleted <ul style="list-style-type: none"> <li>▪ Up status: No</li> <li>▪ Down status: Yes</li> </ul>
Last Sync Attempt	The time of the last synchronization attempt
Last Sync Result	The result of the last synchronization  This channel is the primary channel by default.
Last Sync Success	The time of the last synchronization success
Modified Consecutive Sync Failures	The number of modified, consecutive synchronization failures
Pending Replication Operations	The number of pending replication operations
Scheduled Sync Disabled	If the scheduled synchronization is disabled <ul style="list-style-type: none"> <li>▪ Up status: No</li> <li>▪ Down status: Yes</li> </ul>

## More

### ■ KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How do I monitor Active Directory (AD) replication without domain admin rights?

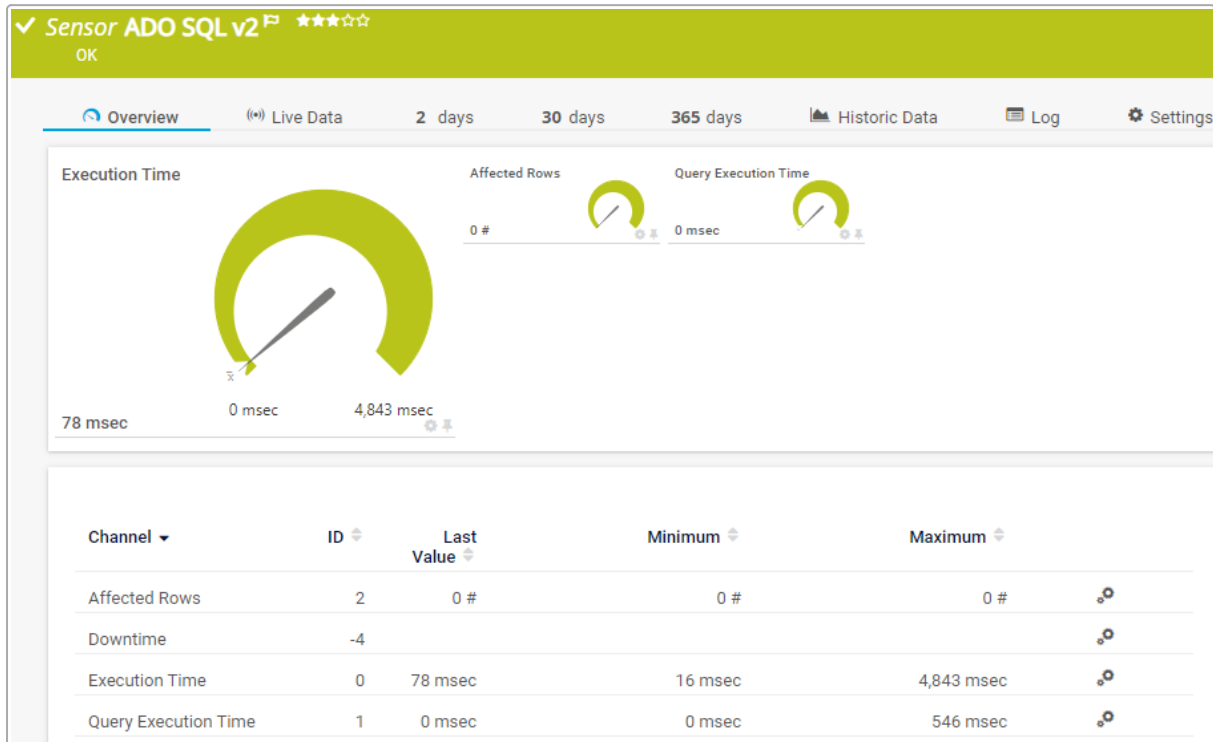
- <https://kb.paessler.com/en/topic/91620>



## 7.8.2 ADO SQL v2 Sensor

The ADO SQL v2 sensor monitors a database via an ActiveX Data Objects (ADO) connection and it executes a Structured Query Language (SQL) query.

- ⓘ This sensor can monitor any data source that is available via Object Linking and Embedding, Database (OLE DB) or Open Database Connectivity (ODBC).



ADO SQL v2 Sensor

- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>685</sup>.

### Sensor in Other Languages

- Dutch: ADO SQL v2
- French: ADO SQL v2
- German: ADO SQL v2
- Japanese: ADO SQL v2
- Portuguese: ADO SQL v2
- Russian: ADO SQL v2
- Simplified Chinese: ADO SQL v2
- Spanish: ADO SQL v2

### Remarks

Consider the following [remarks](#)<sup>675</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
SQL query storage	This sensor requires that you store the SQL query in a file on the probe system. In a cluster, copy the file to every cluster node.  ■ For more information, see the Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a>
.NET 4.7.2 or later	This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.  ❗ If the framework is missing, you cannot create this sensor.  ■ For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a>
ODBC connection	If you use an ODBC connection, define the ODBC connection in the Windows ODBC Connection Manager first. If it is a 64-bit Windows, define the ODBC connection as an ODBC 32-bit connection.IPv6
Lookups	This sensor can use <a href="#">lookups</a> <sup>682</sup> . Select Lookup as Channel #x Unit and define the lookup file in Channel #x Lookup.
Credentials	Define the credentials for database management systems in settings that are higher in the object hierarchy.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">How to set up the SQL v2 sensors in PRTG? Is there a guide?</a></li> <li>▪ Knowledge Base: <a href="#">How can I monitor strings from an SQL database and show a sensor status depending on it?</a></li> <li>▪ Knowledge Base: <a href="#">How can I monitor error tables in SQL databases?</a></li> <li>▪ Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a></li> </ul>
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.
IPv6	This sensor supports IPv6.

## Basic Sensor Settings

Basic Sensor Settings

Sensor Name ⓘ Example Name

---

Tags ⓘ exampletag ✕ +

---

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- sqlsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Database Specific

Database Specific

Connection String ⓘ `Provider=SQLOLEDB.1;Data Source=10.0.0.200\SQLEXPRESS;User ID=user;Password=userpass;Initial Catalog=Northwind`

Database Specific

Setting	Description
Connection String	<p>Enter the connection string that this sensor uses to connect to the database. A connection string can look like this, for example:</p> <p style="color: #0070C0;"><code>Provider=SQLOLEDB.1;Data Source=10.0.0.200\SQLEXPRESS;User ID=user;Password=userpass;Initial Catalog=Northwind</code></p> <p><span style="color: #C00000; font-weight: bold;">ⓘ</span> For ODBC connections, you must enter <a href="#">MSDASQL</a> as provider, for example <code>Provider=MSDASQL;DSN=_my_odbc_sqlserver</code>.</p> <p><span style="color: #C00000; font-weight: bold;">ⓘ</span> You can use the placeholders <code>%dbloginuser</code> and <code>%dbloginpassword</code>. PRTG replaces them with the <a href="#">credentials for database management systems</a> of the parent device.</p>

## Data

**Data**

SQL Query File ⓘ *Demo Serveruptime.sql*

Input Parameter Handling ⓘ  Do not use input parameter (default)  
 Use input parameter

Transaction Handling ⓘ  Do not use transaction (default)  
 Use transaction and always roll back  
 Use transaction and commit on success

Data Processing ⓘ *Only execute query (default)*

Result Handling ⓘ  Discard result (default)  
 Store result

Sensor Display

Setting	Description
SQL Query File	<p>Select the SQL query file that includes a valid SQL statement that the sensor executes on the server with every scanning interval. The list contains SQL scripts from the \Custom Sensors\sql subfolder of the <a href="#">PRTG program directory</a> on the probe system. Store your script there. If you use the script on a cluster probe, you must store the script on all cluster nodes.</p> <p>A correct expression in the file could be: <code>SELECT AVG(UnitPrice) FROM Products</code>. If you want to use transactions, separate the individual steps with semicolons ";".</p> <p> ⓘ Note that with each request, PRTG transfers the full result set, so use filters and limits in your query.</p> <p> ⓘ The demo script Demo Serveruptime.sql is available by default. You can use it to monitor the uptime of the target server.</p> <p> ■ See also the Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a></p> <p> ⓘ You cannot change this value after sensor creation.</p>
Input Parameter Handling	<p>Define if you want to pass a parameter to the SQL query file:</p> <ul style="list-style-type: none"> <li>▪ Do not use input parameter (default): Execute the SQL query file without using variables.</li> <li>▪ Use input parameter: Execute an SQL query file that contains a variable. Provide the parameter that you want to use in the query below.</li> </ul>

Setting	Description
Input Parameter	<p><b>This setting is only visible if you select Use input parameter above.</b></p> <p>Enter the parameter that you want to pass to the SQL query file. This parameter replaces the variables <code>@prtg</code>, <code>:prtg</code>, or <code>?</code> in the SQL query, considering the general rules for SQL variables.</p> <p>You can also use PRTG placeholders for custom sensors (command-line parameters) as input parameters, for example, <code>%sensorid</code> or <code>%deviceid</code>. For more information, see section <a href="#">Custom Sensors</a>.</p> <p><b>i</b> Provide strings as they are and do not surround them with quotation marks. PRTG automatically and correctly inserts string parameters into the query.</p>
Transaction Handling	<p>Define if you want to use transactions and if they affect the database content:</p> <ul style="list-style-type: none"> <li>▪ Do not use transaction (default): Do not execute transactions.</li> <li>▪ Use transaction and always roll back: The query does not change data in the database. In the SQL query file, separate the single steps of the transaction with semicolons.</li> <li>▪ Use transaction and commit on success: The query changes data in the database. The changes only apply if all execution steps succeed without any errors. In the SQL query file, separate the single steps of the transaction with semicolons.</li> </ul>
Data Processing	<p>Define whether the sensor processes data from the database:</p> <ul style="list-style-type: none"> <li>▪ Only execute query (default): Only show information about the number of affected rows and the execution time of the query. Affected rows are rows that were changed by the query (for example, created, deleted, or edited).</li> <li>▪ Count table rows: Execute a <code>SELECT</code> statement and monitor how many rows of the data table this statement returns.</li> <li>▪ Process data table: Read and analyze the data table. If you select this option, the sensor counts rows with <code>SELECT</code> statements as well.</li> </ul> <p><b>i</b> You cannot change this value after sensor creation.</p>
DBNull Handling	<p><b>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</b></p> <p>Define the sensor behavior if the query returns <code>DBNull</code>:</p> <ul style="list-style-type: none"> <li>▪ Error: Show the Down status if the query returns <code>DBNull</code>.</li> <li>▪ Number 0: Recognize the result <code>DBNull</code> as a valid value and interpret it as the number <code>0</code>.</li> </ul>

Setting	Description
<p>Select Channel Value by</p>	<p><b>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</b></p> <p>Define how to select the desired cell in the database table:</p> <ul style="list-style-type: none"> <li>▪ Column number: Determine the channel value by using the value in row 0 of the column whose number you specify in Channel #x Column Number.</li> <li>▪ Column name: Determine the channel value by using the value in row 0 of the column whose name you specify in Channel #x Column Name.</li> <li>▪ Row number: Determine the channel value by using the value in column 0 of the row whose number you specify in Channel #x Row Number.</li> <li>▪ Key value pair: Determine the channel value by searching in column 0 for the key you specify in Channel #x Key and by returning the value in column 1 of the same row where the key value was found.</li> </ul> <p><b>i</b> Defining how the desired cell in the database table is selected is necessary to configure the cells that are used in the channels.</p> <p><b>i</b> The option you select here also defines the method of how to optionally determine a value for the sensor message. For more information, see setting Use Data Table Value in Message.</p> <p><b>■</b> For an example for channel value selection, see section <a href="#">Monitoring Databases</a>.</p>
<p>Channel #2 - #10</p>	<p><b>This setting is only visible if you select Process data table above.</b></p> <p>You can define up to 10 channels. You must define at least one channel, so you see all available settings for <b>Channel #1</b>. Specify how to handle all other possible channels:</p> <ul style="list-style-type: none"> <li>▪ Disable: Do not create this channel.</li> <li>▪ Enable: Create this channel.</li> </ul> <p><b>i</b> It is not possible to enable or disable channels after sensor creation.</p>
<p>Channel #x Name</p>	<p><b>This setting is only visible if you select Process data table above.</b></p> <p>Enter a name for the channel. Enter a string. The sensor dynamically generates channels with this name as identifier.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>

Setting	Description
Channel #x Column Number	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation and if you select Column number for the setting Select Channel Value by.</p> <p>Provide the number of the column to use to determine the channel value in row 0. Enter an integer.</p>
Channel #x Column Name	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation and if you select Column name for the setting Select Channel Value by.</p> <p>Provide the name of the column to use to determine the channel value in row 0. Enter an integer.</p>
Channel #x Row Number	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation and if you select Row number for the setting Select Channel Value by.</p> <p>Provide the number of the column to use to determine the channel value in row 0. Enter an integer.</p>
Channel #x Key	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation and if you select Key value pair for the setting Select Channel Value by.</p> <p>Provide the key to search for in column 0 of the data table. The value in column 1 of the same row where the key value was found to use to determine the channel value. Enter a string.</p>
Channel #x Mode	<p>This setting is only visible if you select Process data table above.</p> <p>Define how to display the determined value in the channel:</p> <ul style="list-style-type: none"> <li>▪ Absolute (default): Show the value as the sensor retrieves it from the data table.</li> <li>▪ Difference: The sensor calculates and shows the difference between the last and the current value returned from the data table. <ul style="list-style-type: none"> <li>ⓘ This mode is not compatible with the unit Lookup.</li> <li>ⓘ This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative and decreasing values.</li> </ul> </li> <li>▪ Absolute (recommended): Show the value as the sensor retrieves it from the data table.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Difference: The sensor calculates and shows the difference between the last and the current value returned from the data table.</li> <li>ⓘ This mode is not compatible with the unit Lookup.</li> <li>ⓘ This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative and decreasing values.</li> <li>ⓘ You cannot change this value after sensor creation.</li> </ul>
<p>Channel #x Unit</p>	<p>This setting is only visible if you select Process data table above.</p> <p>Define the unit of the channel value:</p> <ul style="list-style-type: none"> <li>▪ BytesBandwidth</li> <li>▪ BytesMemory</li> <li>▪ BytesDisk</li> <li>▪ Temperature</li> <li>▪ Percent</li> <li>▪ TimeResponse</li> <li>▪ TimeSeconds</li> <li>▪ TimeHours</li> <li>▪ Count</li> <li>▪ CPU</li> <li>▪ BytesFile</li> <li>▪ SpeedDisk</li> <li>▪ SpeedNet</li> <li>▪ Custom</li> <li>▪ Lookup</li> </ul> <p>■ For more information about the available units, see section <a href="#">Custom Sensors</a>.</p> <p>ⓘ To use <a href="#">lookups</a> with this channel, select Lookup and define the lookup file in Channel #x Lookup. Do not use Custom if you use lookups with this sensor.</p> <p>ⓘ It is not possible to use the unit Lookup in combination with the Difference mode. You are not able to create the sensor in this case.</p>
<p>Channel #x Custom Unit</p>	<p>This setting is only visible if you select the channel unit Custom above.</p> <p>Define a unit for the channel value. Enter a string.</p>



Setting	Description
Channel #x Lookup	<p>This setting is only visible if you select the channel unit <a href="#">Lookup</a> above.</p> <p>Select a <a href="#">lookup</a> file that you want to use with this channel.</p>
Use Data Table Value in Message	<p>This setting is only visible if you select <a href="#">Process data table</a> for the setting <a href="#">Data Processing</a> during sensor creation.</p> <p>Define if the sensor message shows a value from the data table:</p> <ul style="list-style-type: none"> <li>▪ <b>Disable:</b> Do not use a custom sensor message.</li> <li>▪ <b>Enable:</b> Define a custom sensor message with a defined value of the data table. Define the value selection below.</li> </ul> <p><b>i</b> The method of how to determine a value for the sensor message is defined in the setting <a href="#">Select Channel Value by</a> above.</p>
Message Column Number	<p>This setting is only visible if you select <a href="#">Process data table</a> for the setting <a href="#">Data Processing</a> during sensor creation, if you select <a href="#">Column name</a> for the setting <a href="#">Select Channel Value by</a>, and if you select <a href="#">Enable</a> above.</p> <p>Enter the number of a column. The sensor message shows the value in row 0 of this column. Enter an integer.</p>
Message Column Name	<p>This setting is only visible if you select <a href="#">Process data table</a> for the setting <a href="#">Data Processing</a> during sensor creation, if you select <a href="#">Column name</a> for the setting <a href="#">Select Channel Value by</a>, and if you select <a href="#">Enable</a> above.</p> <p>Enter the name of a column. The sensor message shows the value in row 0 of this column. Enter a string.</p> <p><b>i</b> Columns start with index 0.</p>
Message Row Number	<p>This setting is only visible if you select <a href="#">Process data table</a> for the setting <a href="#">Data Processing</a> during sensor creation, if you select <a href="#">Row number</a> for the setting <a href="#">Select Channel Value by</a>, and if you select <a href="#">Enable</a> above.</p> <p>Enter the name of a column. The sensor message shows the value in row 0 of this column. Enter the number of a row. The sensor message shows the value in column 0 of this row. Enter an integer.</p> <p><b>i</b> Rows start with index 0.</p>
Message Key	<p>This setting is only visible if you select <a href="#">Process data table</a> for the setting <a href="#">Data Processing</a> during sensor creation, if you select <a href="#">Key value pair</a> for the setting <a href="#">Select Channel Value by</a>, and if you select <a href="#">Enable</a> above.</p>

Setting	Description
	Enter a key to search for in column 0 of the data table. The sensor message shows the value in column 1 of the row where the key was found. Enter a string.
Message	<p><b>This setting is only visible if you select Enable above.</b></p> <p>Define the sensor message. Enter a string. Use the placeholder {0} at the position where you want to display the value.</p> <p>Example: <b>The message is {0}</b></p> <p><b>i</b> PRTG does not support the number sign (#) in sensor messages. If a message contains a number sign, PRTG clips the message at this point.</p>
If Message Changes	<p><b>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</b></p> <p>Define what the sensor does when its message changes:</p> <ul style="list-style-type: none"> <li>Ignore (default): Do nothing.</li> <li>Trigger 'change' notification: Send an internal message that indicates a change. <ul style="list-style-type: none"> <li><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</li> </ul> </li> </ul>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display


**Sensor Display**

Primary Channel **i** Downtime


---


Graph Type **i** 
 Show channels independently (default)
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Affected Rows	The number of rows that were addressed by the query (including <b>SELECT</b> statements if you process data tables)

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Execution Time	The execution time of the entire request (including connection buildup, query execution, transaction handling, disconnection)  <span style="font-size: 1.2em;">i</span> This channel is the primary channel by default.
Query Execution Time	The execution time of the specified query

## SQL Variables

You can use the following variables in the SQL query file to be replaced by an input parameter. This is useful if you have various SQL sensors with queries that differ in only one parameter.

- Microsoft SQL, MySQL, PostgreSQL: @prtg
- Oracle SQL: :prtg
- ADO SQL: ? (question mark)

i @prtg, :prtg, and ? are common SQL query parameters and they are used in a parameterized SQL query. This means that the query and the parameter are forwarded without any changes to the database. This leads to some restrictions on the database side. For example, you cannot use variables as placeholders for table names or as lists in IN operators.

Examples for variables usage:

```
SELECT * FROM Table WHERE name = @prtg
SELECT @prtg FROM Table
```

## More

### ■ KNOWLEDGE BASE

How to set up the SQL v2 sensors in PRTG? Is there a guide?

- <https://kb.paessler.com/en/topic/70618>

How can I monitor strings from an SQL database and show a sensor status depending on it?

- <https://kb.paessler.com/en/topic/63259>

How can I monitor error tables in SQL databases?

- <https://kb.paessler.com/en/topic/70774>

Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

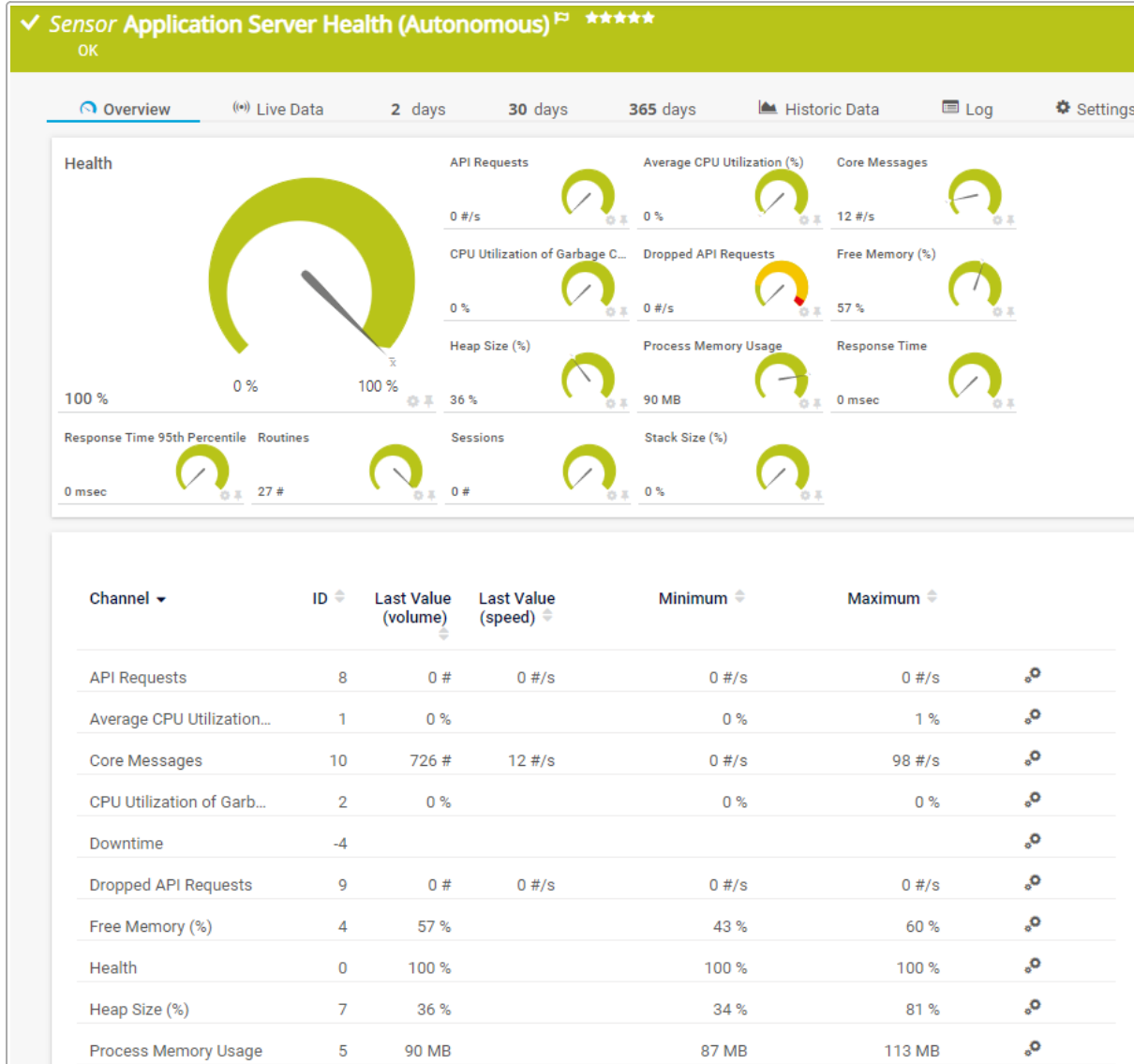
- <https://kb.paessler.com/en/topic/61108>

How do I monitor the size of a Microsoft SQL Server database?

- <https://kb.paessler.com/en/topic/18183>

### 7.8.3 Application Server Health (Autonomous) Sensor

The Application Server Health (Autonomous) sensor monitors the health of the PRTG application server and checks various parameters that can affect the quality of the monitoring results.



Application Server Health (Autonomous) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

#### Sensor in Other Languages

- Dutch: Application Server Health (Autonom)
- French: État du serveur d'application (autonome)
- German: Zustand des PRTG Application Servers (Autonom)
- Japanese: アプリケーションサーバーの正常性 (自律)
- Portuguese: Funcionamento do servidor de aplicativos (autônomo)

- Russian: Состояние сервера приложений (автономного)
- Simplified Chinese: 应用程序服务器运行状况(自治)
- Spanish: Salud de servidor de aplicaciones (autónomo)

## Remarks

Consider the following [remarks](#)<sup>689</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <b>very low</b> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Sensor creation	PRTG automatically creates this sensor. You cannot add it manually.
New UI and API	This sensor is part of the new UI and API. For more information, see the Knowledge Base: <a href="#">I want to use the new UI and new API. What do I need to know?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- appserverhealthsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.



Channel	Description
API Requests	The number of API requests
Average CPU Utilization (%)	The CPU usage of the PRTG application server process (%)
Core Messages	The number of messages that the PRTG application server receives from the PRTG core server
CPU Utilization of Garbage Collector (%)	The CPU usage of the PRTG application server garbage collector (%)
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Dropped API Requests	<p>The number of API requests per second that were dropped due to timeouts</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: <b>5</b></li> <li>▪ Upper warning limit: <b>1</b></li> </ul>
Free Memory (%)	The free system memory of the PRTG application server system (%)
Health	<p>The sums of the PRTG application server state as a value between 100% (healthy) and 0% (unhealthy). Investigate if values are frequently under 100%.</p> <p><b>i</b> This channel is the primary channel by default.</p>
Heap Size (%)	The heap size of the memory that the PRTG application server uses (%)
Process Memory Usage	The memory usage of the PRTG application server process
Response Time	The average response time of the new API
Response Time 95th Percentile	The 95th percentile of the response time of the new API
Routines	The number of concurrently running routines in the PRTG application server
Sessions	The number of active user sessions

Channel	Description
Stack Size (%)	The relative stack size of the memory that the PRTG application server uses (%)

## More

### KNOWLEDGE BASE

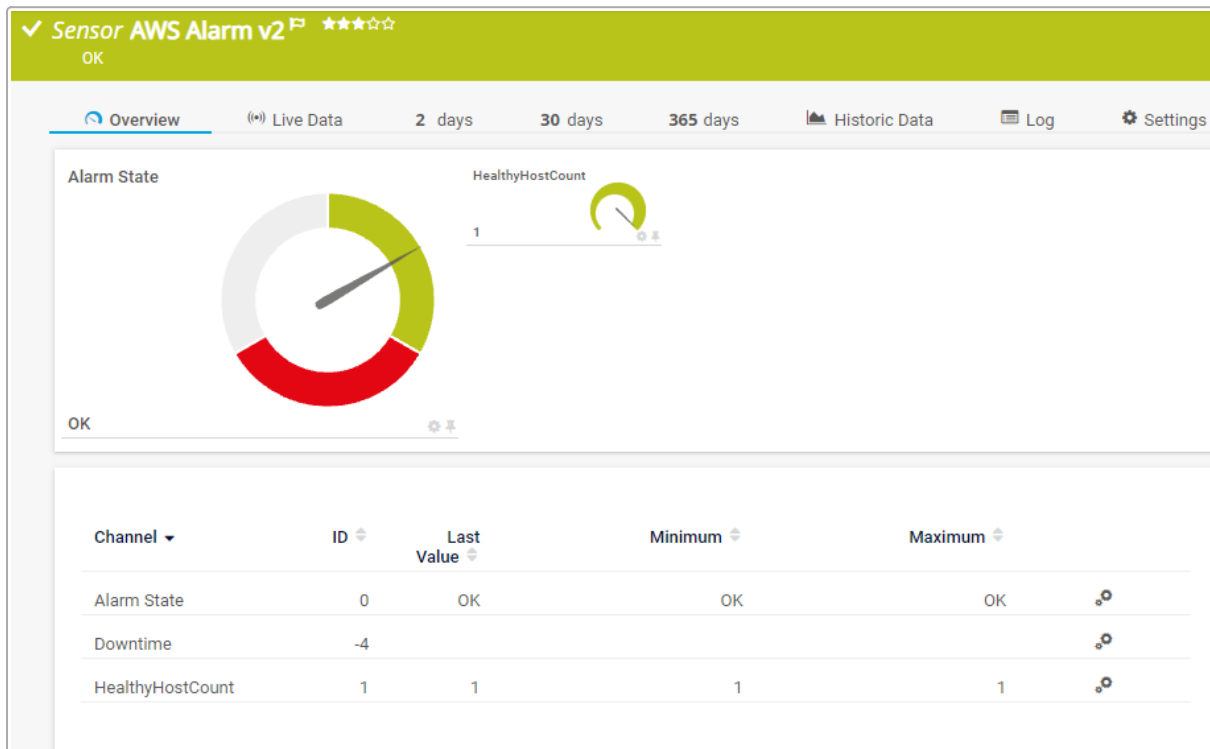
I want to use the new UI and new API. What do I need to know?

- <https://kb.paessler.com/en/topic/90008>

## 7.8.4 AWS Alarm v2 Sensor

The AWS Alarm v2 sensor monitors the status of an Amazon Web Services (AWS) alarm by reading its data from Amazon CloudWatch via the [AWS API](#).

- i If you use the same Identity and Access Management (IAM) policy that you use for this sensor, you must update it. For more information, see the Knowledge Base: [How do I set permissions for the Amazon Web Services \(AWS\) API key to use certain sensors in PRTG?](#)
- i If you monitor an AWS alarm that is based on a metric math expression, this sensor does not create an additional channel that monitors the math expression.



AWS Alarm v2 Sensor

- For a list of regions that this sensor supports, see section [Supported AWS Regions and Their Codes](#).
- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: AWS Alarm v2
- French: Alarme AWS v2
- German: AWS Alarm v2
- Japanese: AWS Alarm v2
- Portuguese: Alarme da AWS v2
- Russian: Аварийный сигнал AWS v2

- Simplified Chinese: AWS 警报 v2
- Spanish: Alarma AWS v2

## Remarks

Consider the following [remarks](#) <sup>694</sup> and requirements for this sensor:

Remark	Description
Permissions for the AWS API key	This sensor requires permissions for the <a href="#">AWS API key</a> .  ■ For more information, see the Knowledge Base: <a href="#">How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?</a>
Credentials	This sensor requires credentials for AWS.
Alarms	This sensor supports <a href="#">MetricAlarm</a> and <a href="#">CompositeAlarm</a> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Pricing	Amazon can charge you based on the number of API calls that the sensor sends to the Amazon servers. For more information, see <a href="#">Amazon CloudWatch Pricing – Amazon Web Services (AWS)</a> .
Add Sensor dialog	It can take up to several minutes before objects appear in the Add Sensor dialog.
Scanning interval	This sensor has a fixed minimum scanning interval for performance reasons. You cannot use a shorter scanning interval. Consequently, shorter scanning intervals in the <a href="#">Monitoring</a> settings are not available for this sensor.  <ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">5 minutes</a>.</li> </ul>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- alarm
- aws
- cloudwatch
- cloudwatchsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## AWS Alarm Specific

### AWS Alarm Specific

**Name** ⓘ Example

**Type** ⓘ Metric

**Description** ⓘ No description

**Region** ⓘ US East (Ohio)

AWS Alarm Specific

Setting	Description
Name	The name of the AWS alarm that this sensor monitors.
Type	The type of the AWS alarm that this sensor monitors.
Description	The description of the AWS alarm that this sensor monitors.
Region	The region in which the AWS alarm that this sensor monitors occurs.

Setting	Description
	<p>■ For a list of regions that this sensor supports, see section <a href="#">Supported AWS Regions and Their Codes</a>.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Alarm State	<p>The alarm status</p> <p>ⓘ This channel is the primary channel by default.</p>

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Metric]	The metric on which the alarm is based

## More

### ■ KNOWLEDGE BASE

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- <https://kb.paessler.com/en/topic/38083>

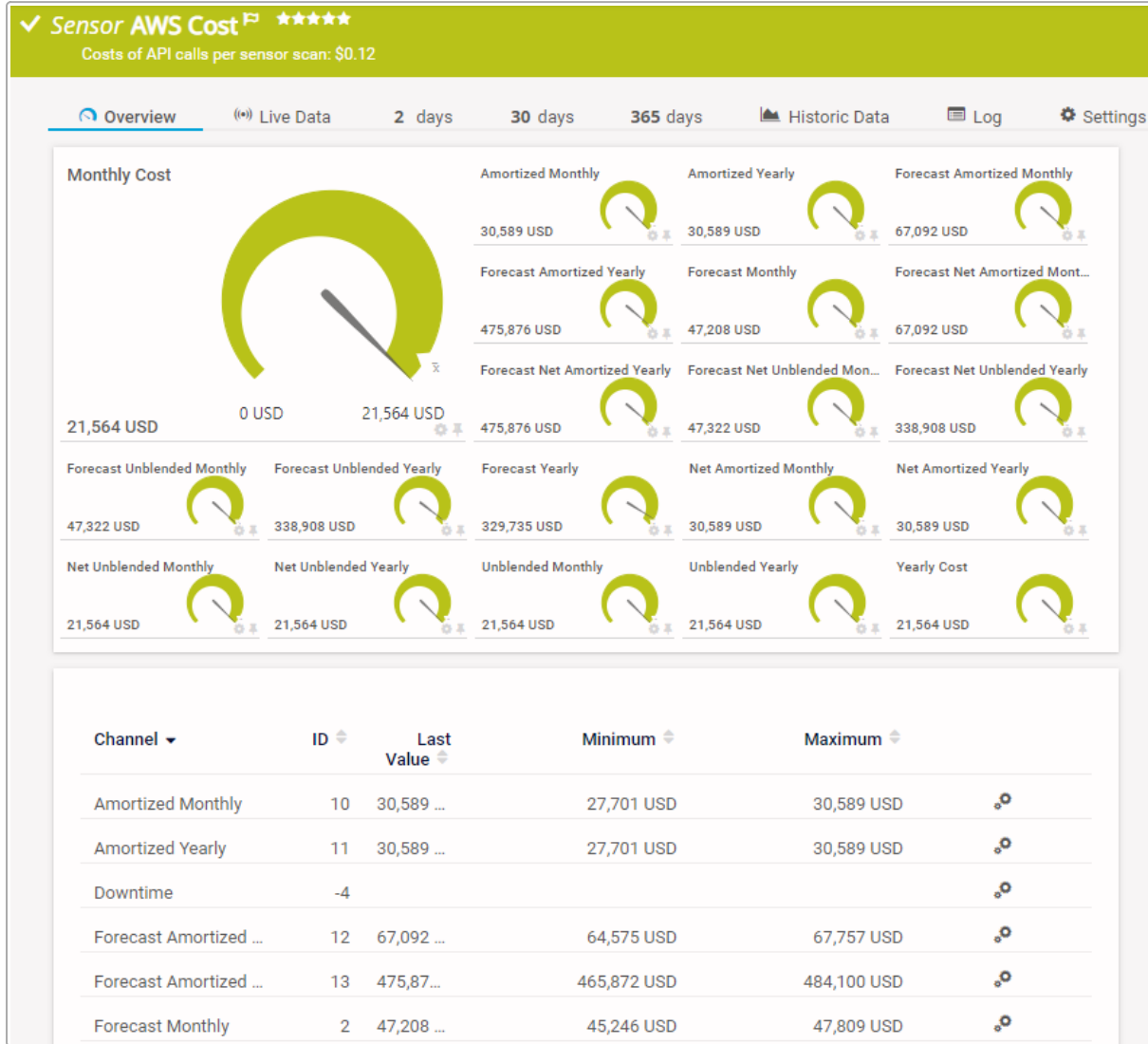
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>



### 7.8.5 AWS Cost Sensor

The AWS Cost sensor monitors the cost of an Amazon Web Services (AWS) account by reading its data from the [AWS Cost Explorer API](#).



AWS Cost Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

#### Sensor in Other Languages

- Dutch: AWS Kosten
- French: Coût AWS
- German: AWS Kosten
- Japanese: AWS Cost
- Portuguese: Custo da AWS
- Russian: Затраты AWS

- Simplified Chinese: AWS 成本
- Spanish: Costo AWS

## Remarks

Consider the following [remarks](#) <sup>700</sup> and requirements for this sensor:

Remark	Description
AWS Cost Explorer	This sensor requires that you activate the <a href="#">AWS Cost Explorer</a> in your AWS account.
IAM User and Role Access to Billing Information	This sensor requires that you enable <a href="#">IAM User and Role Access to Billing Information</a> in your AWS account.
Permissions for the AWS API key	<p>This sensor requires permissions for the <a href="#">AWS API key</a>.</p> <p> The AWS API key requires the following permissions to query data from the AWS API:</p> <ul style="list-style-type: none"> <li>▪ "ce:GetCostAndUsage"</li> <li>▪ "ce:GetCostForecast"</li> <li>▪ "ce:GetDimensionValues"</li> <li>▪ "ce:GetCostAndUsageWithResources"</li> <li>▪ "ce:GetUsageForecast"</li> </ul> <p> For more information, see the Knowledge Base: <a href="#">How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?</a></p>
Credentials	This sensor requires credentials for AWS.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Sensor creation	After sensor creation, the first data is available after 24 hours. Forecast data is available after a few days.
Scanning interval	<p>This sensor has a fixed minimum scanning interval for performance reasons. You cannot use a shorter scanning interval. Consequently, shorter scanning intervals in the <a href="#">Monitoring</a> settings are not available for this sensor.</p> <ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 hour</a>.</li> </ul>

Remark	Description
	<ul style="list-style-type: none"> <li>The recommended scanning interval of this sensor is <b>6 hours</b>. You can use a shorter scanning interval but it could create extra costs.</li> </ul>
Pricing	Amazon charges you for each API call that this sensor sends to the Amazon servers. For more information, see <a href="#">AWS Cost Management Pricing   Amazon Simple Storage Service</a> .
Sensor creation	You can only set up this sensor for one AWS account per PRTG installation.
Knowledge Base	<p>Knowledge Base: <a href="#">What settings do I have to define in my AWS account to set up the AWS Cost sensor?</a></p> <p>Knowledge Base: <a href="#">How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?</a></p>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag x +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- aws
- awscost
- cost

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## AWS Cost Specific

**AWS Cost Specific**

**Additional Cost Types** ⓘ  Disable (default)  
 Enable

**Additional Forecast Types** ⓘ  Disable (default)  
 Enable (creates additional fees)

AWS Cost Specific

Setting	Description
Additional Cost Types	<p>PRTG creates two default channels for blended monthly and yearly cost. If you select this option, you can select additional cost types for which PRTG creates additional channels.</p> <ul style="list-style-type: none"> <li>▪ Enable</li> <li>▪ Disable</li> </ul>
Select Additional Cost Types	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Select additional cost types:</p> <ul style="list-style-type: none"> <li>▪ Amortized cost</li> <li>▪ Net amortized cost</li> <li>▪ Unblended cost</li> <li>▪ Net unblended cost</li> </ul> <p> ⓘ PRTG creates two overview channels (monthly and yearly) for every additional cost type that you select.</p>
Additional Forecast Types	<p>PRTG does not automatically create additional forecast channels. If you select this option, you can select additional forecast types to create additional forecast channels:</p> <ul style="list-style-type: none"> <li>▪ Enable</li> <li>▪ Disable</li> </ul>
Select Additional Forecast Types	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Select additional forecast types:</p> <ul style="list-style-type: none"> <li>▪ Blended cost (default)</li> <li>▪ Amortized cost</li> <li>▪ Net amortized cost</li> <li>▪ Unblended cost</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Net unblended cost</li> </ul> <p><b>i</b> PRTG creates two overview channels (monthly and yearly) for every additional forecast type that you select. Every forecast type that you select creates additional fees. Deselect a forecast type if you no longer want the according channels to create additional fees. You can still see the channels, but they do not receive data anymore.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Amortized Monthly	The amortized cost per month
Amortized Yearly	The amortized cost per year

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Forecast Amortized Monthly	The forecast for amortized cost per month
Forecast Amortized Yearly	The forecast for amortized cost per year
Forecast Monthly	The forecast for cost per month
Forecast Net Amortized Monthly	The forecast for net amortized cost per month
Forecast Net Amortized Yearly	The forecast for net amortized cost per year
Forecast Net Unblended Monthly	The forecast for net unblended cost per month
Forecast Net Unblended Yearly	The forecast for net unblended cost per year
Forecast Unblended Monthly	The forecast for unblended cost per month
Forecast Unblended Yearly	The forecast for unblended cost per year
Forecast Yearly	The forecast for cost per year
Monthly Cost	The monthly cost  This channel is the primary channel by default.
Net Amortized Monthly	The net amortized cost per month
Net Amortized Yearly	The net amortized cost per year
Net Unblended Monthly	The net unblended cost per month
Net Unblended Yearly	The net unblended cost per year

Channel	Description
Unblended Monthly	The unblended cost per month
Unblended Yearly	The unblended cost per year
Yearly Cost	The cost per year

## More

### ■ KNOWLEDGE BASE

What settings do I have to define in my AWS account to set up the AWS Cost sensor?

- <https://kb.paessler.com/en/topic/87401>

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- <https://kb.paessler.com/en/topic/38083>

What security features does PRTG include?

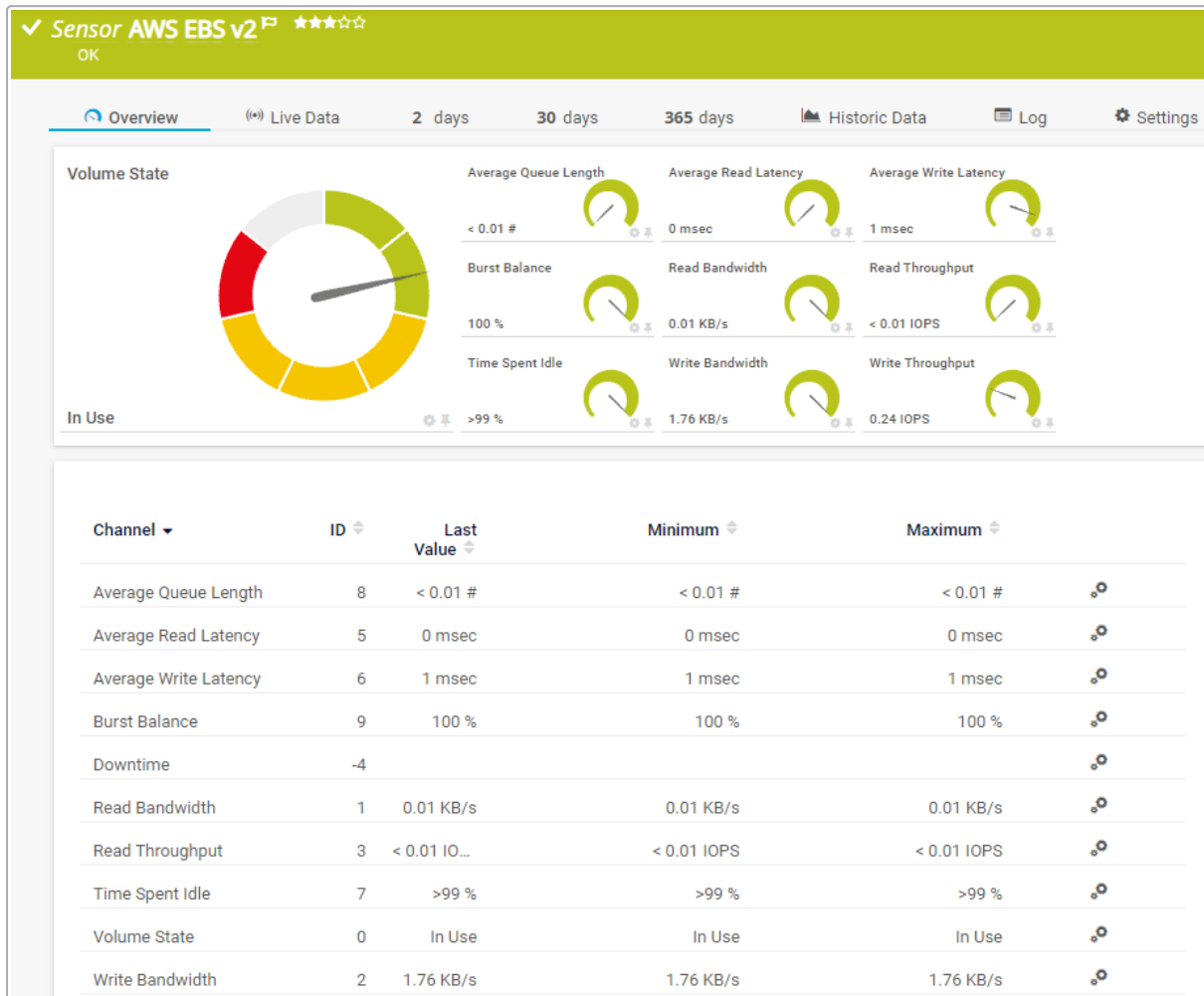
- <https://kb.paessler.com/en/topic/61108>



## 7.8.6 AWS EBS v2 Sensor

The AWS EBS v2 sensor monitors the performance of an Amazon Web Services (AWS) Elastic Block Store (EBS) volume by reading its data from Amazon CloudWatch via the [AWS API](#).

**i** If you use the same Identity and Access Management (IAM) policy that you use for this sensor, you must update it. For more information, see the Knowledge Base: [How do I set permissions for the Amazon Web Services \(AWS\) API key to use certain sensors in PRTG?](#)



AWS EBS v2 Sensor

- For a list of metrics that this sensor supports, see section [Supported Metrics](#)<sup>[711]</sup>.
- For a list of dimensions that this sensor supports, see section [Supported Dimensions](#)<sup>[712]</sup>.
- For a list of regions that this sensor supports, see section [Supported AWS Regions and Their Codes](#).
- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[712]</sup>.

## Sensor in Other Languages

- Dutch: AWS EBS v2
- French: AWS EBS v2
- German: AWS EBS v2
- Japanese: AWS EBS v2
- Portuguese: AWS EBS v2
- Russian: AWS EBS v2
- Simplified Chinese: AWS EBS v2
- Spanish: AWS EBS v2

## Remarks

Consider the following [remarks](#) <sup>708</sup> and requirements for this sensor:

Remark	Description
Permissions for the AWS API key	This sensor requires permissions for the <a href="#">AWS API key</a> .  ■ For more information, see the Knowledge Base: <a href="#">How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?</a>
Credentials	This sensor requires credentials for AWS.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Pricing	Amazon can charge you based on the number of API calls that the sensor sends to the Amazon servers. For more information, see <a href="#">Amazon CloudWatch Pricing – Amazon Web Services (AWS)</a> .
Add Sensor dialog	It can take up to several minutes before objects appear in the Add Sensor dialog.
Scanning interval	This sensor has a fixed minimum scanning interval for performance reasons. You cannot use a shorter scanning interval. Consequently, shorter scanning intervals in the <a href="#">Monitoring</a> settings are not available for this sensor.  ▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a> .

Remark	Description
	<ul style="list-style-type: none"> <li>The recommended scanning interval of this sensor is <b>5 minutes</b>.</li> </ul>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- aws
- cloudwatch
- cloudwatchsensor
- ebs

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### AWS EBS Specific

#### AWS EBS Specific

**ID** ⓘ *vol-1a2b3c4d5e6f7g8h*

---

**Name** ⓘ *Example*

---

**Region** ⓘ *Europe (Ireland)*

AWS EBS Specific

Setting	Description
ID	The ID of the AWS EBS volume that this sensor monitors.
Name	The name of the AWS EBS volume that this sensor monitors.

Setting	Description
Region	<p>The region in which the AWS EBS instance runs.</p> <p>■ For a list of regions that this sensor supports, see section <a href="#">Supported AWS Regions and Their Codes</a>.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

## Supported Metrics

The AWS EBS v2 sensor supports the following metrics:

- BurstBalance (Average)
- VolumeIdleTime (Sum)
- VolumeQueueLength (Average)
- VolumeReadBytes (Sum)
- VolumeReadOps (Sum)
- VolumeTotalReadTime (Average)
- VolumeTotalWriteTime (Average)
- VolumeWriteBytes (Sum)

- VolumeWriteOps (Sum)

## Supported Dimensions

The AWS EBS v2 sensor supports the following dimensions:

- Volume

## Channel List

- i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Average Queue Length	The average queue lengths
Average Read Latency	The average read latency
Average Write Latency	The average write latency
Burst Balance	The burst balance
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Read Bandwidth	The read bandwidth
Read Throughput	The read throughput in IOPS
Time Spent Idle	The time spent idle (%)
Volume State	<p>The volume status</p> <ul style="list-style-type: none"> <li>▪ Up status: Available, In Use</li> <li>▪ Warning status: Creating, Deleting, Deleted</li> <li>▪ Down status: Error</li> <li>▪ Unknown status: Not Set</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Write Bandwidth	The write bandwidth
Write Throughput	The write throughput in IOPS

## More

### ■ KNOWLEDGE BASE

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- <https://kb.paessler.com/en/topic/38083>

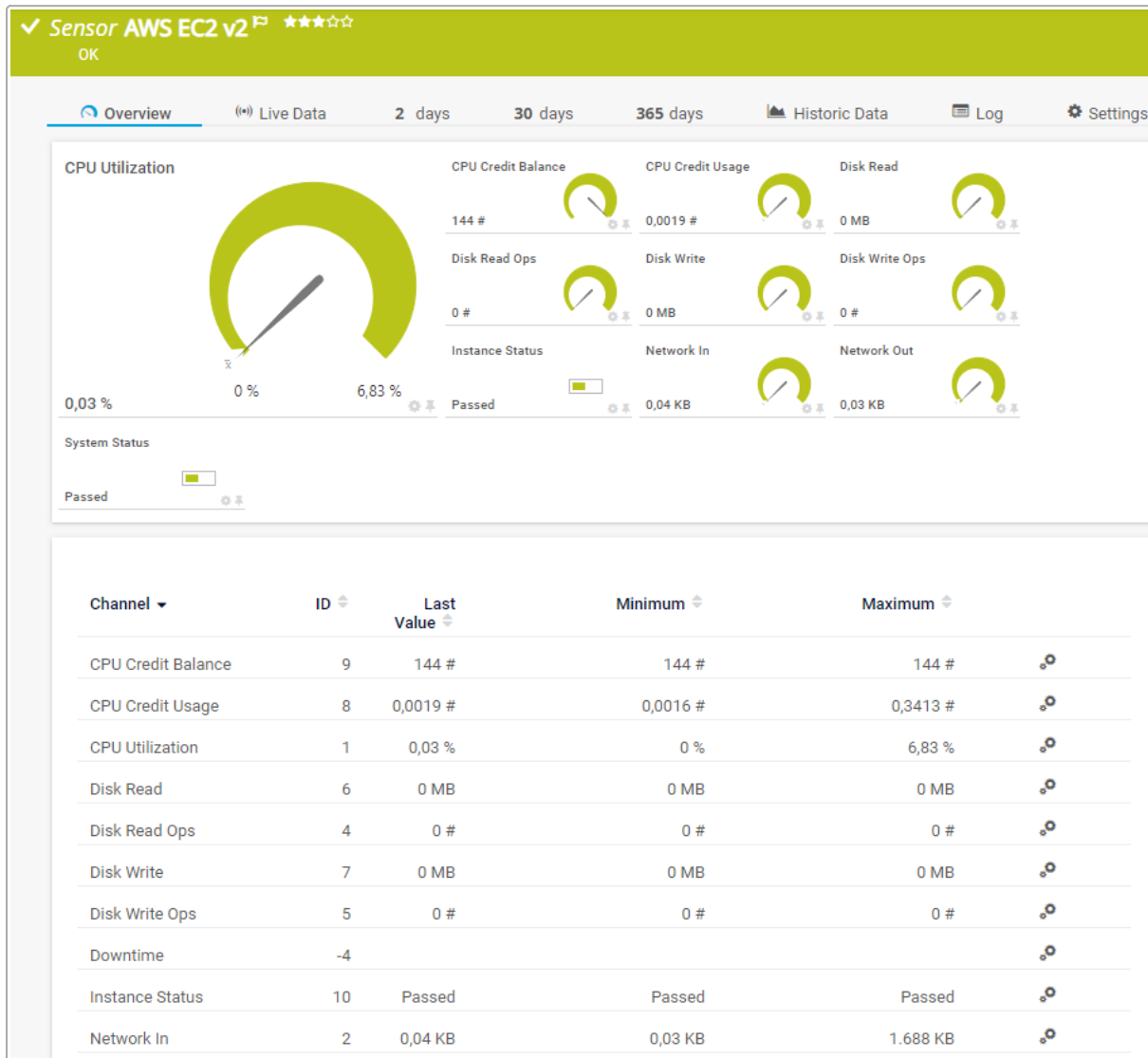
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

### 7.8.7 AWS EC2 v2 Sensor

The AWS EC2 v2 sensor monitors the performance of an Amazon Web Services (AWS) Elastic Compute Cloud (EC2) instance by reading its data from Amazon CloudWatch via the [AWS API](#).

**i** If you use the same Identity and Access Management (IAM) policy that you use for this sensor, you must update it. For more information, see the Knowledge Base: [How do I set permissions for the Amazon Web Services \(AWS\) API key to use certain sensors in PRTG?](#)



AWS EC2 v2 Sensor

- For a list of metrics that this sensor supports, see section [Supported Metrics](#)<sup>[718]</sup>.
- For a list of dimensions that this sensor supports, see section [Supported Dimensions](#)<sup>[719]</sup>.
- For a list of regions that this sensor supports, see section [Supported AWS Regions and Their Codes](#).
- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[719]</sup>.



## Sensor in Other Languages

- Dutch: AWS EC2 v2
- French: AWS EC2 v2
- German: AWS EC2 v2
- Japanese: AWS EC2 v2
- Portuguese: AWS EC2 v2
- Russian: AWS EC2 v2
- Simplified Chinese: AWS EC2 v2
- Spanish: AWS EC2 v2

## Remarks

Consider the following [remarks](#) <sup>715</sup> and requirements for this sensor:

Remark	Description
Permissions for the AWS API key	This sensor requires permissions for the <a href="#">AWS API key</a> .  ■ For more information, see the Knowledge Base: <a href="#">How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?</a>
Credentials	This sensor requires credentials for AWS.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Pricing	Amazon can charge you based on the number of API calls that the sensor sends to the Amazon servers. For more information, see <a href="#">Amazon CloudWatch Pricing – Amazon Web Services (AWS)</a> .
Add Sensor dialog	It can take up to several minutes before objects appear in the Add Sensor dialog.
Scanning interval	This sensor has a fixed minimum scanning interval for performance reasons. You cannot use a shorter scanning interval. Consequently, shorter scanning intervals in the <a href="#">Monitoring</a> settings are not available for this sensor.  ▪ The minimum scanning interval of this sensor is <a href="#">5 minutes</a> .

Remark	Description
	<ul style="list-style-type: none"> <li>The recommended scanning interval of this sensor is <b>5 minutes</b>.</li> </ul>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- aws
- cloudwatch
- cloudwatchsensor
- ec2

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### AWS EC2 Specific

#### AWS EC2 Specific

**ID** ⓘ *i-1a2b3c4d5e6f7g8h*

---

**Name** ⓘ *Example*

---

**Region** ⓘ *Europe (Ireland)*

AWS EC2 Specific

Setting	Description
ID	The ID of the AWS EC2 instance that this sensor monitors.
Name	The name of the AWS EC2 instance that this sensor monitors.

Setting	Description
Region	<p>The region in which the AWS EC2 instance runs.</p> <p>■ For a list of regions that this sensor supports, see section <a href="#">Supported AWS Regions and Their Codes</a>.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Supported Metrics

The AWS EC2 v2 sensor supports the following metrics:

- CPUCreditBalance (Average)
- CPUCreditUsage (Average)
- CPUUtilization (Average)
- DiskReadBytes (Average)
- DiskReadOps (Average)
- DiskWriteBytes (Average)
- DiskWriteOps (Average)
- NetworkIn (Average)

- NetworkOut (Average)
- StatusCheckFailed (Average)
- StatusCheckFailed\_Instance (Average)
- StatusCheckFailed\_System (Average)

## Supported Dimensions

The AWS EC2 v2 sensor supports the following dimensions:

- Instance

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CPU Credit Balance	The CPU credit balance
CPU Credit Usage	The CPU credit usage
CPU Utilization	The CPU usage <b>i</b> This channel is the primary channel by default.
Disk Read	The disk read speed
Disk Read Ops	The number of disk read operations
Disk Write	The disk write speed
Disk Write Ops	The number of disk write operations
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Instance Status	The AWS EC2 instance status <ul style="list-style-type: none"> <li>▪ Up status: Passed</li> <li>▪ Down status: Failed</li> </ul>
Network In	The incoming network load

Channel	Description
Network Out	The outgoing network load
System Status	The AWS EC2 system status <ul style="list-style-type: none"><li>▪ Up status: Passed</li><li>▪ Down status: Failed</li></ul>

## More

### KNOWLEDGE BASE

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- <https://kb.paessler.com/en/topic/38083>

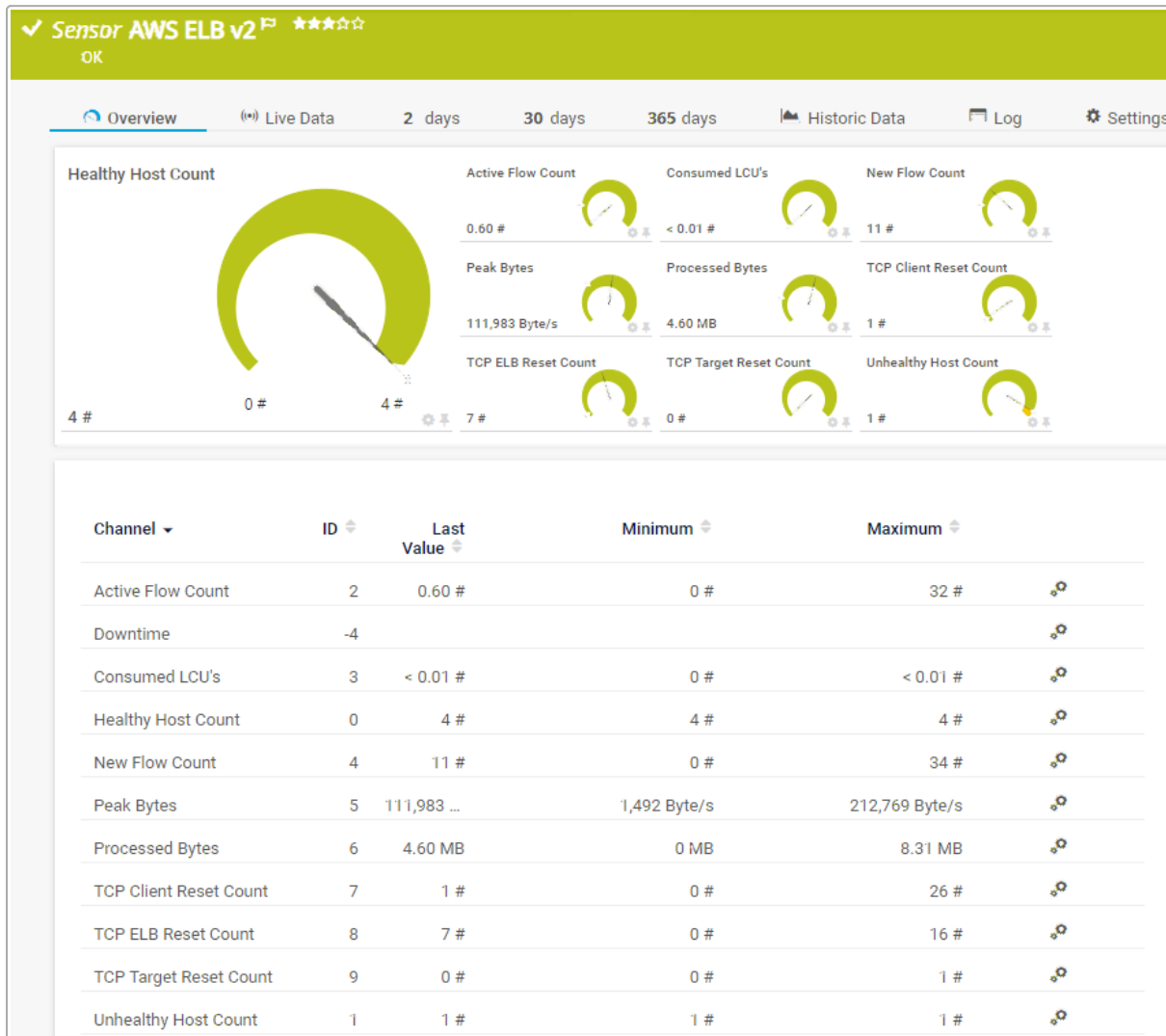
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

### 7.8.8 AWS ELB v2 Sensor

The AWS ELB v2 sensor monitors the performance of an Amazon Web Services (AWS) Elastic Load Balancing (ELB) load balancer by reading its data from Amazon CloudWatch via the [AWS API](#).

**i** If you use the same Identity and Access Management (IAM) policy that you use for this sensor, you must update it. For more information, see the Knowledge Base: [How do I set permissions for the Amazon Web Services \(AWS\) API key to use certain sensors in PRTG?](#)



AWS ELB v2 Sensor

- For a list of metrics that this sensor supports, see section [Supported Metrics](#)<sup>[725]</sup>.
- For a list of dimensions that this sensor supports, see section [Supported Dimensions](#)<sup>[726]</sup>.
- For a list of regions that this sensor supports, see section [Supported AWS Regions and Their Codes](#).
- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[728]</sup>.

## Sensor in Other Languages

- Dutch: AWS ELB v2
- French: AWS ELB v2
- German: AWS ELB v2
- Japanese: AWS ELB v2
- Portuguese: AWS ELB v2
- Russian: AWS ELB v2
- Simplified Chinese: AWS ELB v2
- Spanish: AWS ELB v2

## Remarks

Consider the following [remarks](#) <sup>722</sup> and requirements for this sensor:

Remark	Description
Permissions for the AWS API key	This sensor requires permissions for the <a href="#">AWS API key</a> .  ■ For more information, see the Knowledge Base: <a href="#">How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?</a>
Credentials	This sensor requires credentials for AWS.
Load balancers	This sensor supports <a href="#">Application Load Balancer</a> and <a href="#">Network Load Balancer</a> .
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Pricing	Amazon can charge you based on the number of API calls that the sensor sends to the Amazon servers. For more information, see <a href="#">Amazon CloudWatch Pricing – Amazon Web Services (AWS)</a> .
Add Sensor dialog	It can take up to several minutes before objects appear in the Add Sensor dialog.
Scanning interval	This sensor has a fixed minimum scanning interval for performance reasons. You cannot use a shorter scanning interval. Consequently, shorter scanning intervals in the <a href="#">Monitoring</a> settings are not available for this sensor. <ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">5 minutes</a>.</li> </ul>



Remark	Description
IPv6	This sensor supports IPv6.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- aws
- cloudwatch
- cloudwatchsensor
- elb

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### AWS ELB Specific

#### AWS ELB Specific

**ID** ⓘ *app/example/123456789*

---

**Name** ⓘ *Example*

---

**Type** ⓘ *application*

---

**Region** ⓘ *US East (Ohio)*

AWS ELB Specific

Setting	Description
ID	The ID of the AWS ELB load balancer that this sensor monitors.

Setting	Description
Name	The name of the AWS ELB load balancer that this sensor monitors.
Type	The type of the AWS ELB load balancer that this sensor monitors.
Region	<p>The region in which the AWS ELB load balancer runs.</p> <p>■ For a list of regions that this sensor supports, see section <a href="#">Supported AWS Regions and Their Codes</a>.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

## Supported Metrics

The AWS ELB v2 sensor supports the following metrics:

- ActiveConnectionCount (Sum)
- ActiveFlowCount (Average)
- ConsumedLCUs (Sum)
- HealthyHostCount (Minimum)
- HTTPCode\_ELB\_4XX\_Count (Sum)
- HTTPCode\_ELB\_5XX\_Count (Sum)
- HTTPCode\_Target\_4XX\_Count (Sum)
- HTTPCode\_Target\_5XX\_Count (Sum)

- NewConnectionCount (Sum)
- NewFlowCount (Sum)
- PeakBytesPerSecond (Maximum)
- RuleEvaluations (Sum)
- TargetConnectionErrorCount (Sum)
- TargetResponseTime (Average)
- TCP\_Client\_Reset\_Count (Sum)
- TCP\_ELB\_Reset\_Count (Sum)
- TCP\_Target\_Reset\_Count (Sum)
- UnhealthyHostCount (Maximum)

### Supported Dimensions

The AWS ELB v2 sensor supports the following dimensions:

- Load Balancer

### Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Active Connection Count	The number of concurrent active TCP connections
Active Flow Count	The number of concurrent flows
Consumed LCU's	The number of LCU used by the load balancer
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
ELB 4XX Count	The number of HTTP 4XX client error codes
ELB 5XX Count	The number of HTTP 5XX server error codes
Healthy Host Count	The number of targets that are considered healthy
New Connection Count	The number of new TCP connections

Channel	Description
New Flow Count	The number of new flows
Peak Bytes	The highest average throughput
Processed Bytes	The number of bytes processed
Rule Evaluations	The number of rules processed
Target 4XX Count	The number of HTTP response codes generated by the targets
Target 5XX Count	The number of HTTP response codes generated by the targets
Target Connection Error Count	The number of connections that were not successfully established
Target Response Time	The response time of the target
TCP Client Reset Count	The number of RST packets sent from a client to a target
TCP ELB Reset Count	The number of RST packets generated by the load balancer
TCP Target Reset Count	The number of RST packets sent from a target to a client
Unhealthy Host Count	The number of targets that are considered unhealthy

## More

### ■ KNOWLEDGE BASE

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- <https://kb.paessler.com/en/topic/38083>

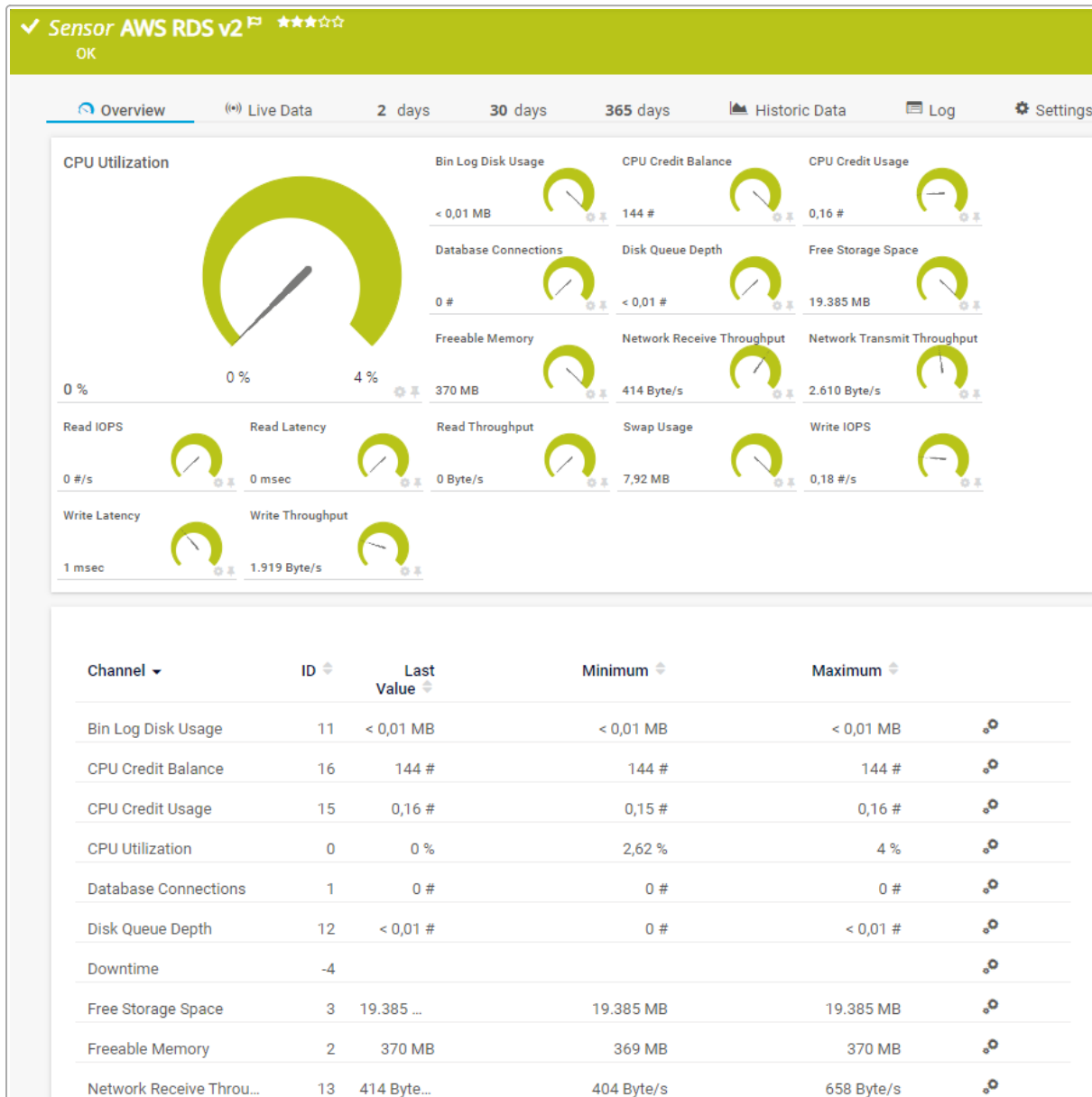
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

### 7.8.9 AWS RDS v2 Sensor

The AWS RDS v2 sensor monitors the performance of a Amazon Web Services (AWS) Relational Database Service (RDS) database by reading its data from Amazon CloudWatch via the [AWS API](#).

**i** If you use the same Identity and Access Management (IAM) policy that you use for this sensor, you must update it. For more information, see the Knowledge Base: [How do I set permissions for the Amazon Web Services \(AWS\) API key to use certain sensors in PRTG?](#)



AWS RDS v2 Sensor

- For a list of metrics that this sensor supports, see section [Supported Metrics](#)<sup>[732]</sup>.
- For a list of dimensions that this sensor supports, see section [Supported Dimensions](#)<sup>[733]</sup>.
- For a list of regions that this sensor supports, see section [Supported AWS Regions and Their Codes](#).

■ For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[733]</sup>.

### Sensor in Other Languages

- Dutch: AWS RDS v2
- French: AWS RDS v2
- German: AWS RDS v2
- Japanese: AWS RDS v2
- Portuguese: AWS RDS v2
- Russian: AWS RDS v2
- Simplified Chinese: AWS RDS v2
- Spanish: AWS RDS v2

### Remarks

Consider the following [remarks](#)<sup>[729]</sup> and requirements for this sensor:

Remark	Description
Permissions for the AWS API key	This sensor requires permissions for the <a href="#">AWS API key</a> . ■ For more information, see the Knowledge Base: <a href="#">How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?</a>
Credentials	This sensor requires credentials for AWS.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Pricing	Amazon can charge you based on the number of API calls that the sensor sends to the Amazon servers. For more information, see <a href="#">Amazon CloudWatch Pricing – Amazon Web Services (AWS)</a> .
Add Sensor dialog	It can take up to several minutes before objects appear in the Add Sensor dialog.
Scanning interval	This sensor has a fixed minimum scanning interval for performance reasons. You cannot use a shorter scanning interval. Consequently, shorter scanning intervals in the <a href="#">Monitoring</a> settings are not available for this sensor. ■ The minimum scanning interval of this sensor is <a href="#">5 minutes</a> .

Remark	Description
	<ul style="list-style-type: none"> <li>The recommended scanning interval of this sensor is <b>5 minutes</b>.</li> </ul>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- aws
- cloudwatch
- cloudwatchsensor
- rds

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### AWS RDS Specific

#### AWS RDS Specific

**Database Identifier** ⓘ *example-database-identifier*

---

**Engine** ⓘ *postgres*

---

**Region** ⓘ *US East (Ohio)*

AWS RDS Specific

Setting	Description
Database Identifier	The database identifier of the AWS RDS database that this sensor monitors.



Setting	Description
Engine	The engine family name of the AWS RDS database that this sensor monitors.
Region	The region in which the AWS RDS instance runs.  ■ For a list of regions that this sensor supports, see section <a href="#">Supported AWS Regions and Their Codes</a> .

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.  ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.
Graph Type	Define how this sensor shows different channels: <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a> ).
Stack Unit	<b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b> .  Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

## Supported Metrics

The AWS RDS v2 sensor supports the following metrics:

- BinLogDiskUsage (MB)
- CPUUtilization (Average)
- CPUCreditUsage (Average)
- CPUCreditBalance (Average)
- DatabaseConnections (Count)
- DiskQueueDepth (Count)
- FreeableMemory (MB)
- FreeStorageSpace (MB)

- NetworkReceiveThroughput (Byte/Second)
- NetworkTransmitThroughput (Byte/Second)
- ReadIOPS (Count/Second)
- ReadLatency (Milliseconds)
- ReadThroughput (Byte/Second)
- ReplicaLag (Milliseconds)
- SwapUsage (MB)
- WriteIOPS (Count/Second)
- WriteLatency (Milliseconds)
- WriteThroughput (Byte/Second)

### Supported Dimensions

The AWS RDS v2 sensor supports the following dimensions:

- DBInstanceIdentifier

### Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Bin Log Disk Usage	The bin log disk usage
CPU Credit Balance	The CPU credit balance
CPU Credit Usage	The CPU credit usage
CPU Utilization	The CPU usage <b>i</b> This channel is the primary channel by default.
Database Connections	The average number of database connections in use
Disk Queue Depth	The number of outstanding read and write requests waiting to access the disk
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Free Storage Space	The amount of available storage space
Freeable Memory	The freeable memory
Network Receive Throughput	The incoming (receive) network traffic
Network Transmit Throughput	The outgoing (transmit) network traffic
Read IOPS	The average number of disk read IOPS
Read Latency	The read latency
Read Throughput	The average number of bytes read from disk
Replica Lag	The amount of time a read replica DB instance lags behind the source DB instance
Swap Usage	The swap usage
Write IOPS	The average number of disk write IOPS
Write Latency	The average amount of time taken per disk read and write operation
Write Throughput	The number of disk write operations

## More

### ■ KNOWLEDGE BASE

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

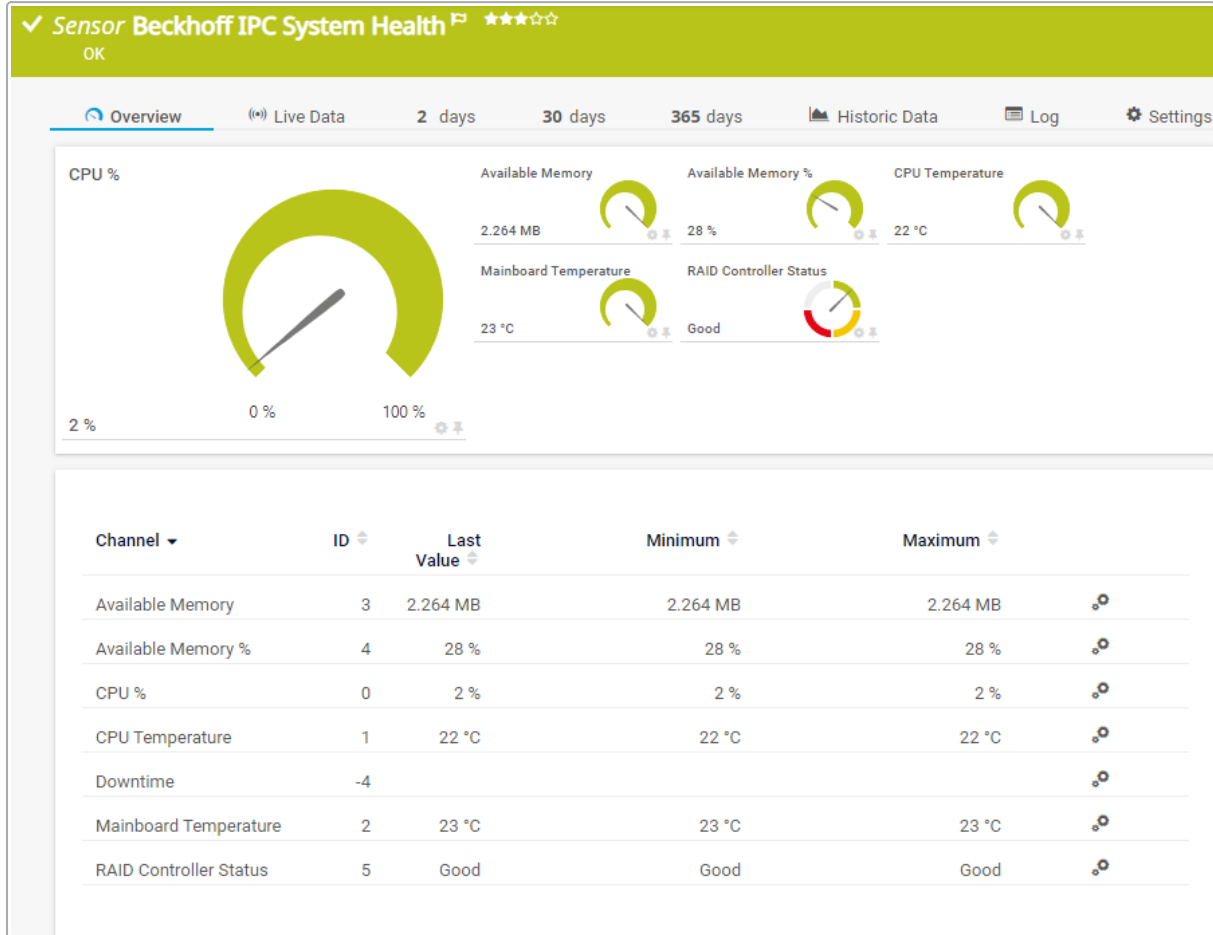
- <https://kb.paessler.com/en/topic/38083>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.10 Beckhoff IPC System Health Sensor

The Beckhoff IPC System Health sensor monitors the system health of a Beckhoff Industrial PC (IPC) via OPC Unified Architecture (OPC UA).



Beckhoff IPC System Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>738</sup>.

### Sensor in Other Languages

- Dutch: Beckhoff IPC Systeemstatus
- French: Beckhoff IPC état du système
- German: Beckhoff IPC Systemzustand
- Japanese: Beckhoff IPC システム正常性
- Portuguese: Saúde do sistema Beckhoff IPC
- Russian: Работоспособность системы Beckhoff IPC
- Simplified Chinese: Beckhoff IPC 系统健康状况
- Spanish: Salud del sistema Beckhoff IPC

## Remarks

Consider the following [remarks](#)<sup>[736]</sup> and requirements for this sensor:

Remark	Description
Valid port	This sensor requires a valid port.
Credentials	This sensor requires credentials for OPC UA in the settings of the parent device.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- opcua

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Available Memory	The available memory
Available Memory %	The available memory (%)
CPU %	The CPU load (%)
CPU Temperature	The CPU temperature
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Mainboard Temperature	The mainboard temperature



Channel	Description
RAID Controller Status	The RAID controller status <ul style="list-style-type: none"><li>▪ Up status: Good</li><li>▪ Warning status: Offline</li><li>▪ Down status: Failed</li><li>▪ Unknown status: Power Off</li></ul>

## More

### KNOWLEDGE BASE

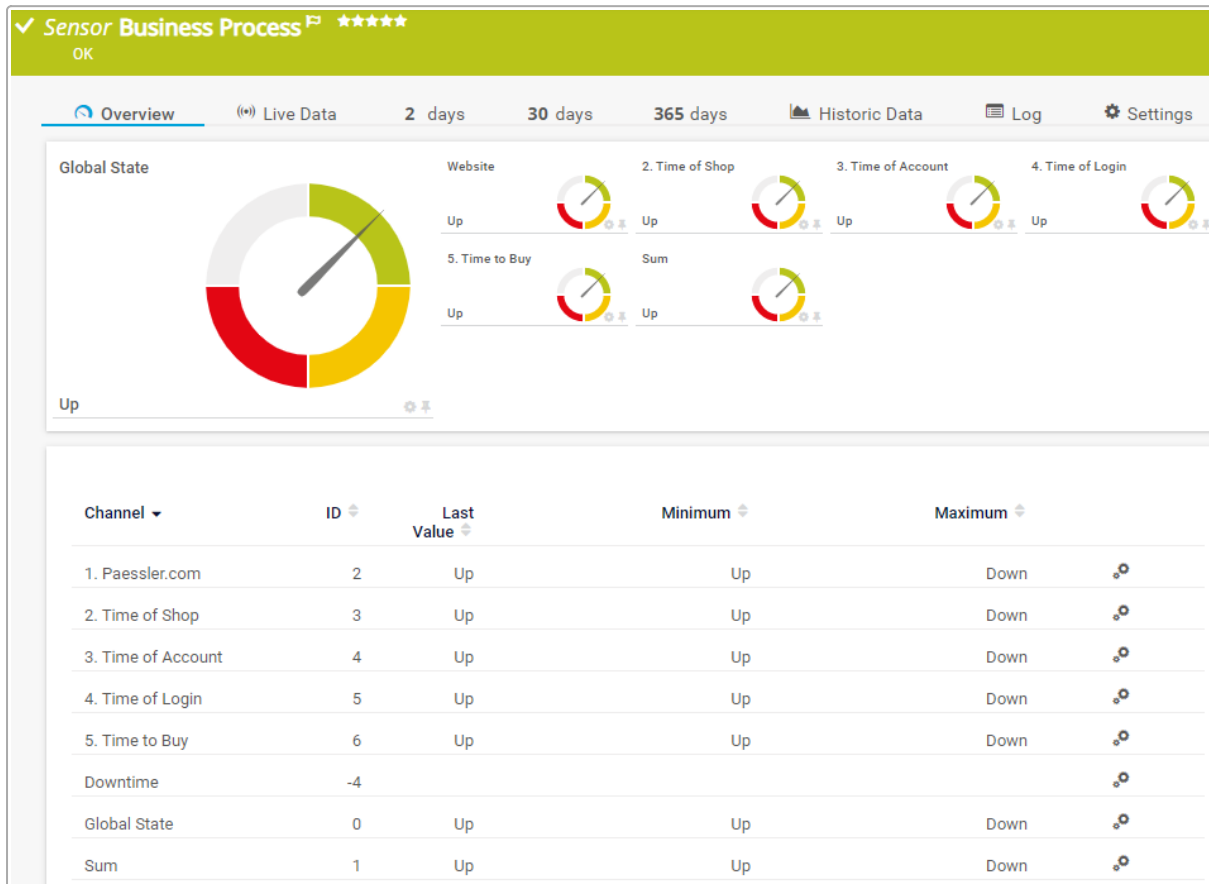
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.11 Business Process Sensor

The Business Process sensor gives you a summarized status of entire business processes while monitoring several process components. This means that you can create a customized sensor with channels based on data from other sensors ("source sensors") that are specific to your network.

**i** If you want to process values from other sensors and you want to perform calculations with these values, for example, use the [Sensor Factory](#)<sup>[1757]</sup> sensor.



Business Process Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[747]</sup>.

### Sensor in Other Languages

- Dutch: Bedrijfs Proces
- French: Processus métier
- German: Business Process
- Japanese: ビジネスプロセス
- Portuguese: Processo empresarial
- Russian: Бизнес-процесс
- Simplified Chinese: 业务进程

- Spanish: Proceso empresarial

## Remarks

Consider the following [remarks](#)<sup>[741]</sup> and requirements for this sensor:

Remark	Description
Channels	This sensor does not officially support more than <a href="#">50 channels</a> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Knowledge Base	Knowledge Base: <a href="#">How does the Business Process sensor calculate summarized sensor states?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  X +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- businessprocesssensor
- factorysensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Business Process Specific Settings

**Business Process Specific Settings**

**States and Conditions**

Step 1. The sensor maps object states to object conditions. The following object states are mapped to the "up" condition:

Up, Warning, Unusual, Down (Partial), Unknown (Collecting)

The following object states are mapped to the "down" condition:

Down, Unknown (None), Paused, Down (Acknowledged)

See the [PRTG Manual](#) for the reasoning behind this behavior.  
A probe, group, or device that you add to a channel is in the "up" condition as long as none of its sensors are in the "down" condition.

Step 2. The Business Process sensor compares the percentage of the "up" conditions of the objects in a channel with the thresholds you define. If the percentage of objects in the "up" condition is smaller than indicated by your warning or error threshold, the channel will be in an overall "warning" or "down" status respectively.


Step 3. The Global State channel of the Business Process sensor always shows the "most severe" status that at least one of your channels has.

Channel Name	Error	Warning	Objects	
Channel 1	50	25	<span style="color: green;">✔</span> Battery: SMP D... <span style="color: blue;">✕</span>	⊕
Channel 2	50	75	<span style="color: green;">✔</span> SSH Disk Free <span style="color: blue;">✕</span>	⊕
Channel 3	50	75	<span style="color: gray;">?</span> CPU Load <span style="color: blue;">✕</span>	⊕
Enter Channel Name	50	75		

Business Process Specific Settings

Setting	Description
Channel Name	<p>Enter a name for the channel. To add a new channel to this sensor, click the Enter Channel Name field, enter a name for the channel, and confirm with the Enter or Tab key.</p> <p><b>i</b> It might take several sensor scans until new channel names or changes to channel names become visible.</p>
Error Threshold %	<p>Set a percentage limit to define when the channel displays the Down status. Enter an integer. The default value is <b>50%</b>.</p> <p><b>i</b> This value depends on how many objects you feed into a Business Process channel.</p> <p>If the percentage of source objects in the "up" condition is less than the error threshold defines, the channel and the Global State channel of the Business Process sensor show the Down status.</p> <p>PRTG maps the following <a href="#">sensor states</a> to the "up" condition ▲ for a Business Process channel:</p> <ul style="list-style-type: none"> <li>▪ Up</li> <li>▪ Warning</li> <li>▪ Unusual</li> <li>▪ Down (Partial)</li> </ul>

Setting	Description
	<p>PRTG maps all other sensor states to the "down" condition ▼ (see <a href="#">Up and Down Conditions</a><sup>[744]</sup>).</p> <p>For example, if you define 4 source sensors for a channel, an error threshold of 50% means that 3 source sensors must be in the "down" condition to set this channel to the Down status. So, 50% means that more than half of the source sensors must <b>not</b> be in the "up" condition to set the sensor to the Down status.</p> <p>■ For more information, an illustration of the business process mechanisms, and some use cases for the Business Process sensor, see the table <a href="#">below</a><sup>[744]</sup> and the Knowledge Base: <a href="#">How can I use the Business Process sensor?</a></p>
Warning Threshold %	<p>Set a percentage limit to define when the channel displays the Warning status. Enter an integer. The default value is 75%.</p> <p>ⓘ This value depends on how many objects you feed into a Business Process channel.</p> <p>If the percentage of source objects in the "up" condition is less than the threshold defines, the channel and the Global State channel of the Business Process sensor show the Warning status.</p> <p>PRTG maps the following sensor states to the "up" condition ▲ for a Business Process channel:</p> <ul style="list-style-type: none"> <li>▪ Up</li> <li>▪ Warning</li> <li>▪ Unusual</li> <li>▪ Down (Partial)</li> </ul> <p>PRTG maps all other sensor states to the "down" condition ▼ (see <a href="#">Up and Down Conditions</a><sup>[744]</sup>).</p> <p>For example, if you define 4 source sensors for a channel, a warning threshold of 75% means that all 4 source sensors must be in the "down" condition to set this channel to the Warning status. So, 75% means that more than three out of four of the source sensors must <b>not</b> be in the "up" condition to set the sensor to the Warning status.</p> <p>■ For more information, an illustration of the business process mechanisms, and some use cases for the Business Process sensor, see the table <a href="#">below</a><sup>[744]</sup> and the Knowledge Base: <a href="#">How can I use the Business Process sensor?</a></p>
Objects	<p>Enter the objects that you want to have in a channel by clicking 🍀. This way, you can select the desired objects from the device tree with the <a href="#">object selector</a>. You can also start to type the object's ID, name, or a tag. PRTG then suggests the possible objects.</p>

Setting	Description
	<p>You can add sensors, devices, groups, and probes to a channel. Each object you add is weighted equally, no matter if it is a single sensor or a device with many sensors. To give more weight to a specific object, add it several times. For example, add the object twice to give double weight to it, add it three times to give it triple weight.</p> <p> A probe, group, or device is in the "up" condition ▲ as long as it does not contain any sensors in the "down" condition ▼.</p>

## Up and Down Conditions

The Business Process "up" ▲ and "down" ▼ conditions are different from the normal Up and Down sensor states. This is necessary for the Business Process sensor to calculate summarized states and to show a calculated result for an entire business process. This table illustrates which sensor status leads to which Business Process condition.

### The Relation Between Object States And Business Process Conditions

Channel Object Status	Business Process Condition	Reason: Why does a specific sensor status correspond to a specific Business Process condition?
 Up	Up ▲	The monitored object works, so everything is fine.
 Warning	Up ▲	The sensor might show a warning, but the monitored object still works.
 Down (Partial)	Up ▲	This status is available in a cluster and is displayed if at least one cluster node reports the sensor as in the Up status and at least one cluster node reports it as in the Down status. With at least one Up report, the monitored object is supposed to be working and meets the Business Process "up" condition.
 Unusual	Up ▲	The sensor might show unusual values, but the monitored object works.
 Collecting	Up ▲	The sensor is still waiting for more monitoring data to definitely decide on the sensor status, but so far the monitored object works. This PRTG internal status is visualized as the Unknown status in the PRTG web interface.
 Down	Down ▼	The monitored object does not work.

Channel Object Status	Business Process Condition		Reason: Why does a specific sensor status correspond to a specific Business Process condition?
Unknown	Down		The sensor does not know if the monitored object works, for example because it has not yet received any data or because it has not received any data for a certain amount of time.
None	Down		The sensor has not yet received any monitoring data from the monitored object. This PRTG internal status is visualized as the Unknown status in the PRTG web interface.
Paused	Down		The monitored object does not work and monitoring has been paused, for example actively by the user, by inheritance, or by schedules. It might be convenient to exclude regularly or frequently paused objects from your business process monitoring, so you do not give more weight than necessary to a Business Process "down" condition because of issues you already know about.
Down (Acknowledged)	Down		The monitored object does not work and someone already knows.

**i** If you encounter issues with your Business Process sensor and want to [contact the Paessler support team](#), send us your [exact configuration](#). Click in the upper-right corner of the Business Process Specific Settings table to copy your configuration:

### Business Process Specific Settings

**States and Conditions** *Step 1. The sensor maps object states to object conditions. The following object states are mapped to the "up" condition:*  
Up, Warning, Unusual, Down (Partial), Unknown (Collecting)

*The following object states are mapped to the "down" condition:*  
Down, Unknown (None), Paused, Down (Acknowledged)

*See the PRTG Manual for the reasoning behind this behavior. A probe, group, or device that you add to a channel is in the "up" condition as long as none of its sensors are in the "down" condition.*

*Step 2. The Business Process sensor compares the percentage of the "up" conditions of the objects in a channel with the thresholds you define. If the percentage of objects in the "up" condition is smaller than indicated by your warning or error threshold, the channel will be in an overall "warning" or "down" status respectively.*

*Step 3. The Global State channel of the Business Process sensor always shows the "most severe" status that at least one of your channels has.*

Channel Name	Error	Threshold %	Warning	Objects	
Sum		50	75	<input checked="" type="checkbox"/> Ping <input type="checkbox"/>	
Website		50	75	<input checked="" type="checkbox"/> Ping <input type="checkbox"/>	

The Business Process Sensor Configuration Clipboard

A window opens that contains your configuration. Copy the highlighted text and paste it into the [support form](#) to send it to the Paessler support team.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).



## Channel List

- i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
[Channel]	<p>The summarized status of the objects contained in each channel according to the individually defined error and warning thresholds</p> <ul style="list-style-type: none"> <li>▪ Up status: Up</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Down</li> <li>▪ Unknown status: Inactive</li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p> <p><b>i</b> The Business Process sensor never shows values in the Downtime channel because they cannot be calculated for this sensor.</p>
Global State	<p>The overall and summarized status of all channels in the Global State channel</p> <ul style="list-style-type: none"> <li>▪ Up status: Up</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Down</li> <li>▪ Unknown status: Inactive</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

How does the Business Process sensor calculate summarized sensor states?

- <https://kb.paessler.com/en/topic/66647>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How can I use the Business Process sensor?

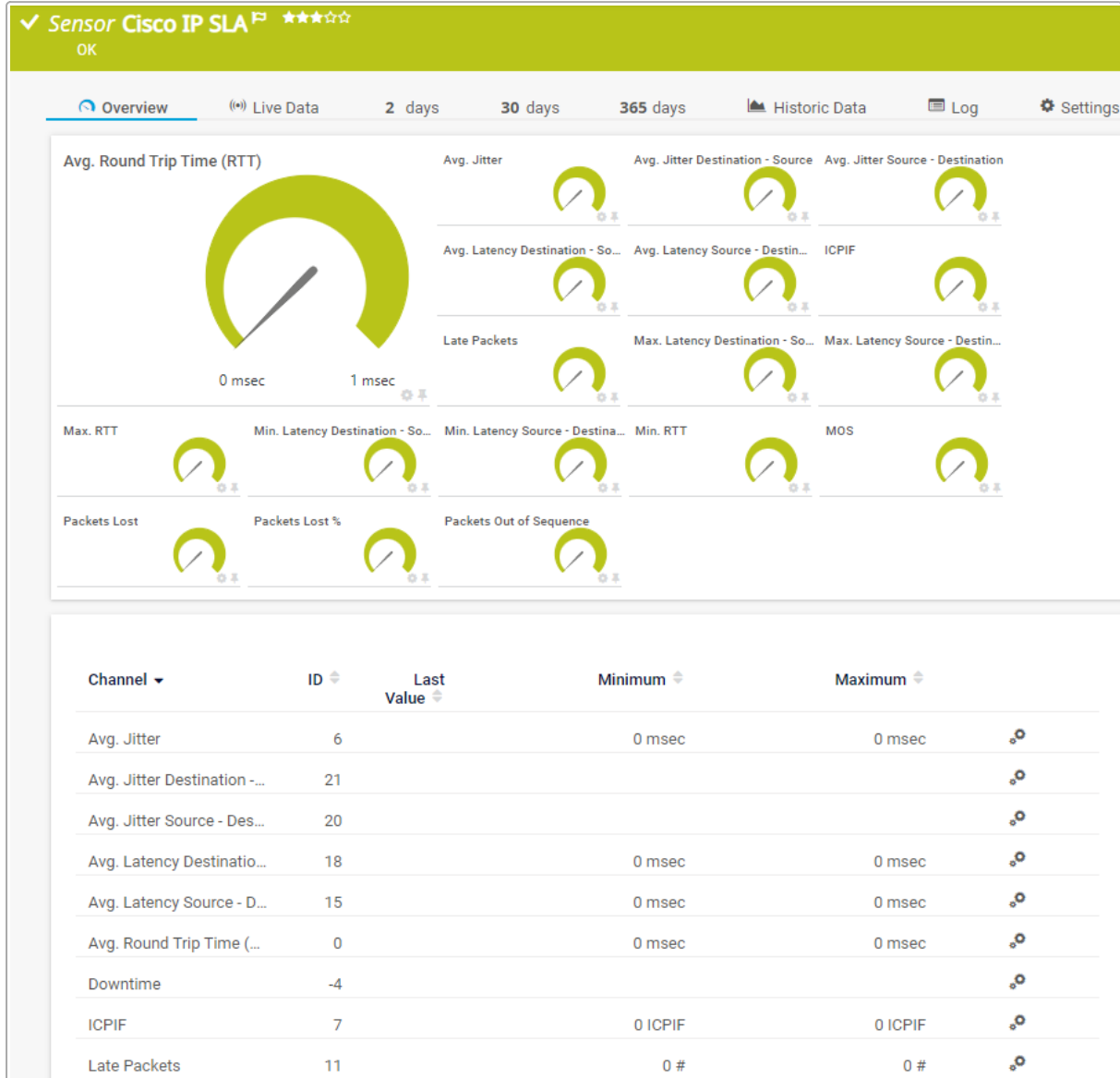
- <https://kb.paessler.com/en/topic/67109>

How can I avoid numerous notifications for branch offices?

- <https://kb.paessler.com/en/topic/86094>

## 7.8.12 Cisco IP SLA Sensor

The Cisco IP SLA sensor monitors Voice over IP (VoIP) network parameters using IP service level agreements (SLA) from Cisco via the Simple Network Management Protocol (SNMP).



Cisco IP SLA Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Cisco IP SLA
- French: Cisco IP SLA
- German: Cisco IP SLA
- Japanese: Cisco IP SLA

- Portuguese: Cisco IP SLA
- Russian: Cisco IP SLA
- Simplified Chinese: Cisco IP SLA
- Spanish: Cisco IP SLA

## Remarks

Consider the following [remarks](#) <sup>749</sup> and requirements for this sensor:

Remark	Description
IPv4	This sensor only supports IPv4.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Object identifiers (OID)	If the object identifiers (OID) that this sensor uses are not available on the target device, the sensor shows the error message: <a href="#">No such object (SNMP error # 222)</a> . If this occurs, open the SNMP Compatibility Options <a href="#">setting</a> of the parent device or group and set the Request Mode to Use single get.
Sensor creation	If there is a very large number of IP SLAs available during sensor creation, we recommend that you limit the result set by using the Start Interface Index and End Interface Index options in the SNMP Compatibility Options setting of the parent device or group.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ  ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- ipslasensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## IP SLA Specific

**IP SLA Specific**

**ID** ⓘ 23

**Type** ⓘ *path-jitter*

**Name (Tag)** ⓘ *Example*

**Owner** ⓘ *(Not defined)*

**Frequency** ⓘ 60

IP SLA Specific

Setting	Description
ID	<p>The ID of the SLA that this sensor monitors.</p> <p>This sensor can support the following operations with the specified type IDs:</p> <ul style="list-style-type: none"> <li>▪ echo (1)</li> <li>▪ pathEcho (2)</li> <li>▪ fileIO (3)</li> <li>▪ script (4)</li> <li>▪ udpEcho (5)</li> <li>▪ tcpConnect (6)</li> <li>▪ http (7)</li> <li>▪ dns (8)</li> <li>▪ jitter (9)</li> <li>▪ dlsn (10)</li> <li>▪ dhcp (11)</li> <li>▪ ftp (12)</li> <li>▪ icmp-jitter (16)</li> <li>▪ path-jitter (23)</li> </ul>

Setting	Description
	<p><b>i</b> The numbers are the IDs of the SLA types as reported by the target device. PRTG translates them into the corresponding strings. These IDs are independent of the IDs that you see in the Add Sensor dialog. If the target device returns other values, this sensor shows an error message that says that it cannot find the type.</p> <p><b>i</b> Packet loss values are summarized but have no explicit channel for source-destination or destination-source values.</p>
Type	The type of the SLA that this sensor monitors.
Name (Tag)	The name of the SLA that this sensor monitors.
Owner	The owner of the SLA that this sensor monitors.
Frequency	The frequency of the SLA that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>

Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Avg. Jitter	The average jitter
Avg. Jitter Destination - Source	The average jitter between destination and source
Avg. Jitter Source - Destination	The average jitter between source and destination
Avg. Latency Destination - Source	The average latency between destination and source
Avg. Latency Source - Destination	The average latency between source and destination
Average Round Trip Time (RTT)	<p>The average RTT</p> <p> This channel is the primary channel by default.</p>

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
ICPIF	The ICPIF
Late Packets	The number of late packets
Max. Latency Destination - Source	The maximum latency between destination and source
Max. Latency Source - Destination	The maximum latency between source and destination
Max. RTT	The maximum RTT
Min. Latency Destination - Source	The minimum latency between destination and source
Min. Latency Source - Destination	The minimum latency between source and destination
Min. RTT	The minimum RTT
MOS	The MOS
Packets Lost	The number of lost packets
Packets Lost %	The number of lost packets (%)
Packets Out of Sequence	The number of out-of-sequence packets

## More

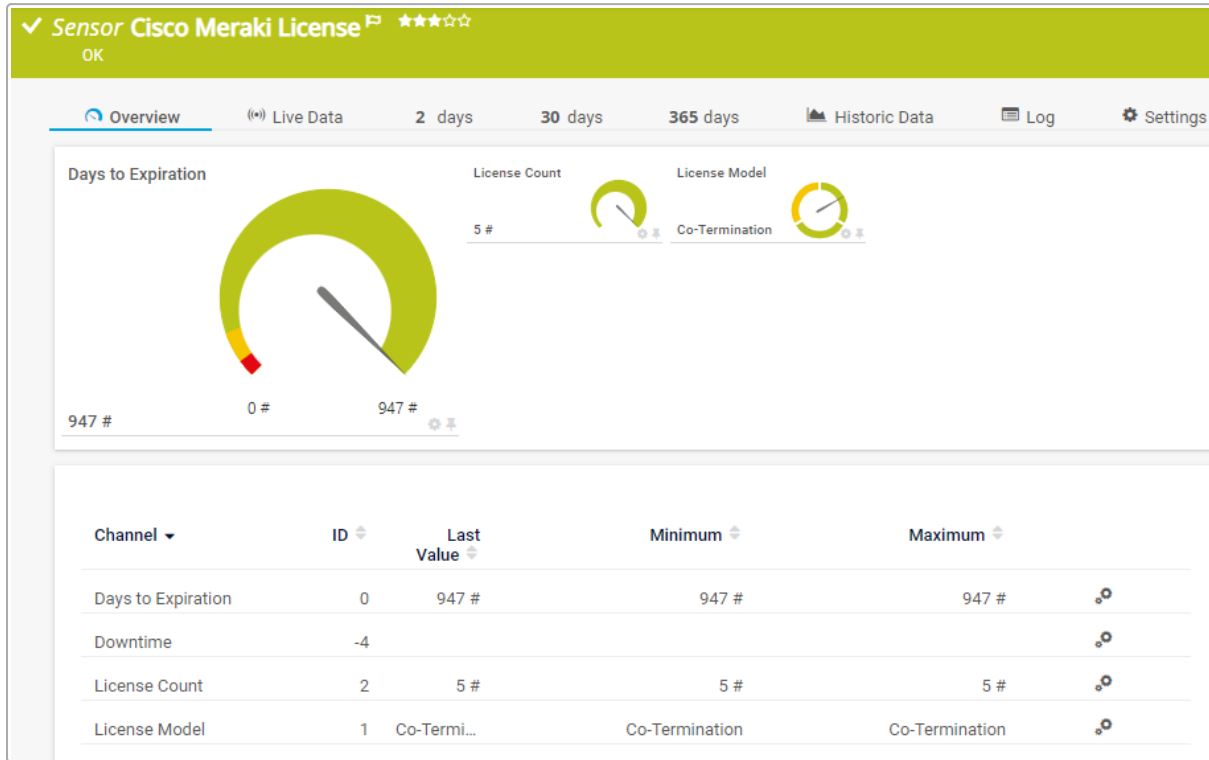
### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.13 Cisco Meraki License Sensor

The Cisco Meraki License sensor monitors Meraki licenses of an organization via the [Cisco Meraki Dashboard API](#).



Cisco Meraki License Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Cisco Meraki Licentie
- French: Cisco Meraki licence
- German: Cisco Meraki Lizenz
- Japanese: Cisco Meraki ライセンス
- Portuguese: Licença da Cisco Meraki
- Russian: Лицензия Cisco Meraki
- Simplified Chinese: Cisco Meraki 许可证
- Spanish: Licencia Cisco Meraki

### Remarks

Consider the following [remarks](#) and requirements for this sensor:



Remark	Description
Enabled organization API access	This sensor requires that you enable the access of an organization to the <a href="#">Cisco Meraki Dashboard API</a> .  ⓘ If the API access for an organization is disabled, you must enable it manually. For more information, see <a href="#">Cisco Meraki Dashboard API: Enable API Access</a> .
API key	This sensor requires an API key with <a href="#">Cisco Meraki Dashboard API</a> permissions.  ⓘ The API key that this sensor uses must inherit the permissions of a <a href="#">Cisco Meraki Dashboard Administrator account</a> with at least <a href="#">Read-only admin</a> permissions.  ⓘ The API key inherits the permissions of the <a href="#">Cisco Meraki Dashboard Administrator account</a> that was used to generate the API key.
Credentials	This sensor requires credentials for Cisco Meraki.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">10 seconds</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">6 hours</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cisco
- license
- meraki

For more information about basic sensor settings, see section [Sensor Settings](#).

### Cisco Meraki Specific

**Cisco Meraki Specific** Organization ⓘ *ExampleOrganization*

Cisco Meraki Specific

Setting	Description
Organization	The name of the organization that the monitored licenses belong to.

### Sensor Display

**Sensor Display** Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>

Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**

Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><span style="font-size: 0.8em;">☁</span> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><span style="font-size: 0.8em;">ⓘ</span> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

- i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Days to Expiration	<p>The days to expiration</p> <p><b>i</b> This channel is the primary channel by default.</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: <a href="#">30 days</a></li> <li>▪ Lower warning limit: <a href="#">90 days</a></li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
License Count	<p>The number of licenses</p>
License Model	<p>The license model of the monitored license</p> <ul style="list-style-type: none"> <li>▪ Up status: Co-Termination, Per-Device</li> <li>▪ Warning status: Unknown</li> </ul>

## More

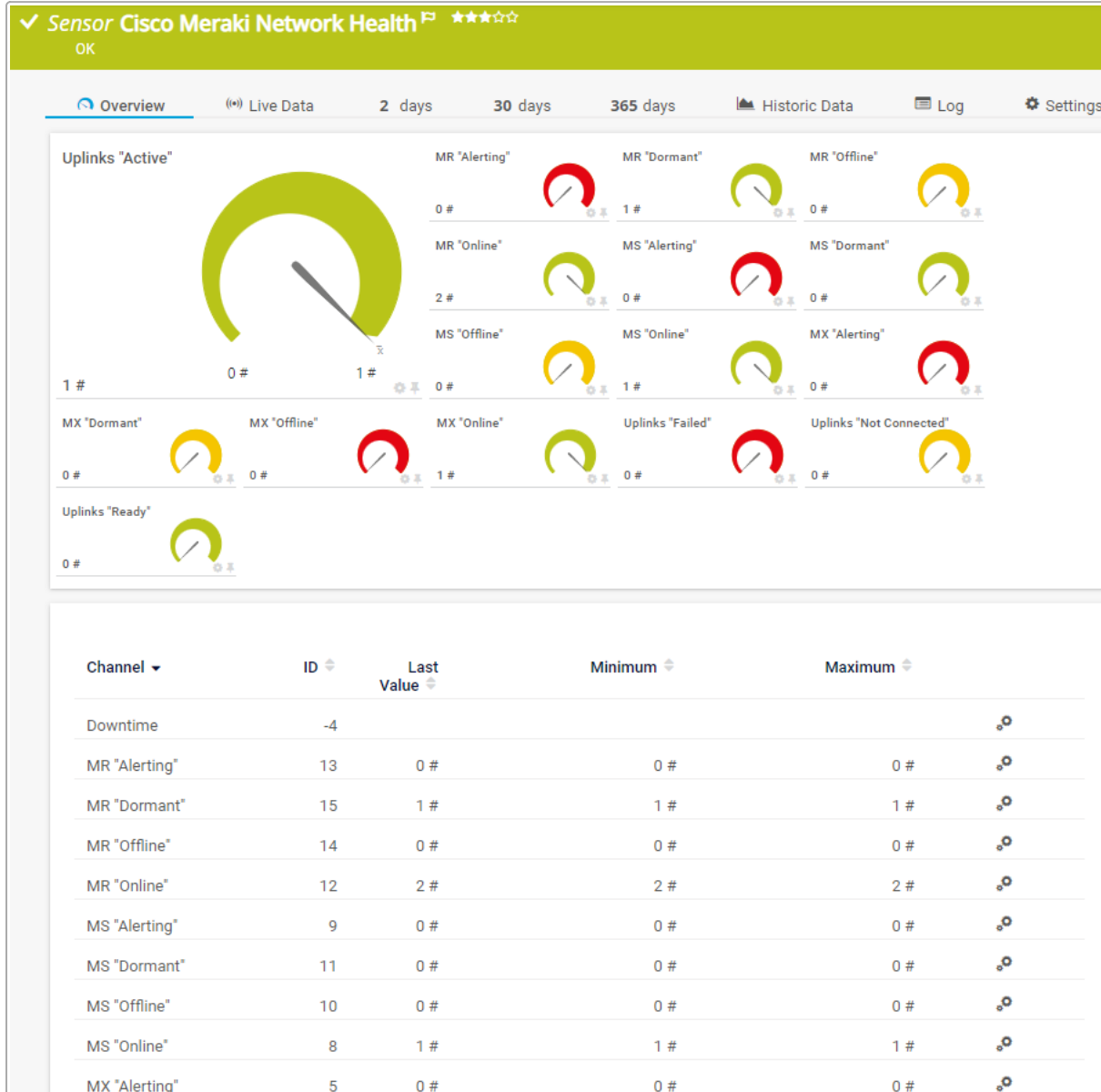
### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.14 Cisco Meraki Network Health Sensor

The Cisco Meraki Network Health sensor monitors the health of Cisco Meraki network devices via the [Cisco Meraki Dashboard API](#).



Cisco Meraki Network Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Cisco Meraki Network Status
- French: Cisco Meraki état du réseau
- German: Cisco Meraki Netzwerkzustand
- Japanese: Cisco Meraki ネットワークの正常性

- Portuguese: Cisco Meraki Network Health
- Russian: Работоспособность сети Cisco Meraki
- Simplified Chinese: Cisco Meraki 网络运行情况
- Spanish: Salud de la red Cisco Meraki

## Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Enabled organization API access	This sensor requires that you enable the access of an organization to the <a href="#">Cisco Meraki Dashboard API</a> .  ⓘ If the API access for an organization is disabled, you must enable it manually. For more information, see <a href="#">Cisco Meraki Dashboard API: Enable API Access</a> .
Credentials	This sensor requires credentials for Cisco Meraki.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <b>10 seconds</b>.</li> <li>▪ The recommended scanning interval of this sensor is <b>5 minutes</b>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cisco

- meraki

For more information about basic sensor settings, see section [Sensor Settings](#) [667].

### Cisco Meraki Specific

**Cisco Meraki Specific**

**Network** ⓘ *ExampleNetwork*

**Organization** ⓘ *ExampleOrganization*

Cisco Meraki Specific

Setting	Description
Network	The name of the network that this sensor monitors.
Organization	The name of the organization that the monitored network belongs to.

### Sensor Display

**Sensor Display**

**Primary Channel** ⓘ Downtime

**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>

Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**

Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><span style="font-size: 0.8em;">☁</span> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><span style="font-size: 0.8em;">ⓘ</span> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.


■ For more information, see section [Inheritance of Settings](#).



## Channel List

- i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
IOT "Alerting"	IOT devices in alerting status
IOT "Dormant"	IOT devices in dormant status
IOT "Offline"	IOT devices in offline status
IOT "Online"	IOT devices in online status
MR "Alerting"	Meraki Radios (MR) devices in alerting status
MR "Dormant"	MR devices in dormant status
MR "Offline"	MR devices in offline status
MR "Online"	MR devices in online status
MS "Alerting"	Meraki Switching (MS) devices in alerting status
MS "Dormant"	MS devices in dormant status
MS "Offline"	MS devices in offline status
MS "Online"	MS devices in online status
MX "Alerting"	Meraki Security (MX) devices in alerting status
MX "Dormant"	MX devices in dormant status
MX "Offline"	MX devices in offline status
MX "Online"	MX devices in online status
Uplinks "Active"	Uplinks in active status

Channel	Description
	 This channel is the primary channel by default.
Uplinks "Failed"	Uplinks in failed status
Uplinks "Not Connected"	Uplinks in not connected status
Uplinks "Ready"	Uplinks in ready status

## More

### KNOWLEDGE BASE

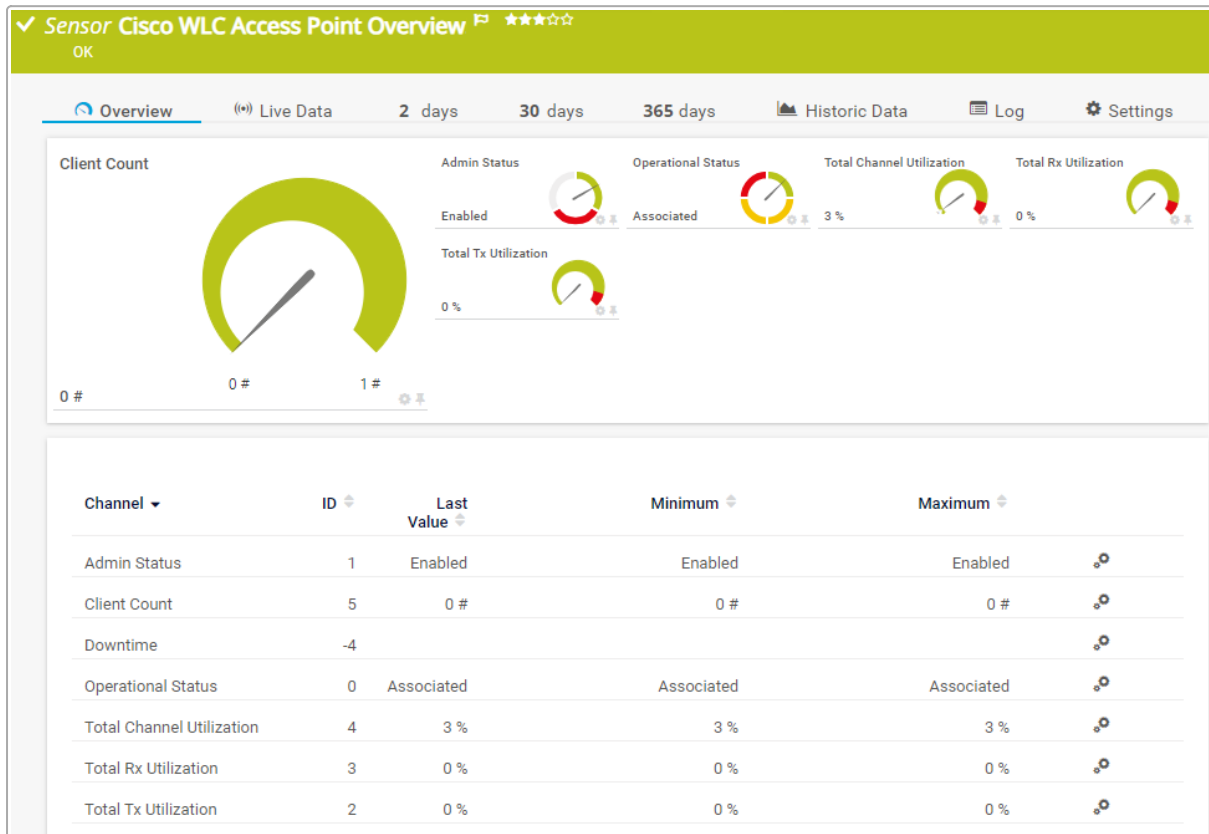
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.15 Cisco WLC Access Point Overview Sensor (BETA)

The Cisco WLC Access Point Overview sensor monitors the operational status of a wireless LAN controller (WLC) access point and provides a sum of various network utilization metrics of the available slots.

**BETA** This sensor is in beta status. The operating methods and the available settings are still subject to change. Do not expect that all functions work properly, or that this sensor works as expected at all.



Cisco WLC Access Point Overview Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Cisco WLC Access Point Overview
- French: Cisco WLC Access Point Overview
- German: Cisco WLC Access Point Overview
- Japanese: Cisco WLC Access Point Overview
- Portuguese: Cisco WLC Access Point Overview
- Russian: Cisco WLC Access Point Overview
- Simplified Chinese: Cisco WLC Access Point Overview
- Spanish: Cisco WLC Access Point Overview

## Remarks

Consider the following [remarks](#) <sup>766</sup> and requirements for this sensor:

Remark	Description
Enabled Beta Sensors experimental feature	This sensor requires that the Beta Sensors <a href="#">experimental feature</a> is enabled.  ■ For more information, see the Knowledge Base: <a href="#">What are beta sensors and how can I use them?</a>
Credentials	This sensor requires credentials for SNMP in settings that are higher in the <a href="#">object hierarchy</a> .
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Scanning interval	The recommended scanning interval of this sensor is <a href="#">5 minutes</a> .

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  X +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cisco
- snmp
- wlc

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Cisco WLC Access Point Specific

### Cisco WLC Access Point Overview Specific

**MAC Address** ⓘ A1:B2:C3:D4:E5:F6

---

**Name** ⓘ Example Access Point

---

**Number of Slots** ⓘ 3

Cisco WLC Access Point Specific

Setting	Description
MAC Address	<p>The MAC address of the access point that this sensor monitors.</p> <p>ⓘ PRTG shows this value for reference purposes only. We strongly recommend that you only change it if the Paessler support team explicitly asks you to do so. Wrong usage can result in incorrect monitoring data.</p>
Name	The name of the access point.
Number of Slots	The number of available slots in the access point.

## Sensor Display

### Sensor Display

**Primary Channel** ⓘ Downtime

---


**Graph Type** ⓘ

Show channels independently (default)

Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	Define how this sensor shows different channels:

Setting	Description
	<ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>



## Debug Options

### Debug Options


**Result Handling** 

- Discard result (default)
- Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>




## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Admin Status	The admin status <ul style="list-style-type: none"> <li>▪ Up status: Enabled</li> <li>▪ Down status: Unknown</li> <li>▪ Unknown status: Disabled</li> </ul>
Client Count	The number of clients <p> This channel is the primary channel by default.</p>
Clients with Poor SNR Count	The number of clients with a poor signal-to-noise ratio (SNR) <p> This channel is only available for the Cisco 5500 series.</p>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Operational Status	The operational status <ul style="list-style-type: none"> <li>▪ Up status: Associated</li> <li>▪ Warning status: Disassociating, Downloading</li> <li>▪ Down status: Unknown</li> </ul>
Total Tx Utilization	The total percentage of transmit utilization across all slots in the access point <p> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: <a href="#">90%</a></li> </ul>

Channel	Description
Total Rx Utilization	<p>The total percentage of receive utilization across all slots in the access point</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: 90%</li> </ul>
Total Channel Utilization	<p>The total percentage of channel utilization across all slots in the access point</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: 90%</li> </ul>

## More

### ■ KNOWLEDGE BASE

What are beta sensors and how can I use them?

- <https://kb.paessler.com/en/topic/88697>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>



## 7.8.16 Citrix XenServer Host Sensor

The Citrix XenServer Host sensor monitors a Xen host server via HTTP.



Citrix XenServer Host Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).



### Sensor in Other Languages

- Dutch: Citrix XenServer Host
- French: Citrix XenServer serveur hôte
- German: Citrix XenServer Host
- Japanese: Citrix XenServer ホスト
- Portuguese: Host Citrix XenServer
- Russian: Узел Citrix XenServer
- Simplified Chinese: Citrix XenServer 主机

- Spanish: Host Citrix XenServer


## Remarks

Consider the following [remarks](#) <sup>772</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <b>high</b> performance impact. We recommend that you use no more than <b>200</b> of this sensor on each probe.
.NET 4.7.2 or later	This sensor requires <b>.NET 4.7.2 or later</b> from Microsoft on the probe system. In a cluster, install it on every cluster node.   If the framework is missing, you cannot create this sensor.   For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a>
Parent device	<ul style="list-style-type: none"> <li>▪ This sensor requires that the parent device is a Citrix XenServer as of version 5.0.</li> <li>▪ This sensor requires that the parent device represents one host server of your XenServer pool.</li> </ul>
Credentials	This sensor requires credentials for VMware/XenServer.
TLS 1.2	This sensor does not fully support Transport Layer Security (TLS) 1.2 connections. You cannot add it to XenServers with the security protocol setting "TLS 1.2 only".
IPv4	This sensor only supports IPv4.
Add Sensor dialog	PRTG also includes hosts that do not run in the Add Sensor dialog.

## Monitoring a XenServer Pool

In a XenServer pool, there is one "pool master" that manages the pool. Incoming queries on any host are automatically forwarded to the pool master. If you want to monitor your VMs or host servers, create respective sensors on a device that represents **one** host server of your pool. Internal processes make sure that monitoring takes place and continues independently from the physical host.

-  In the device tree, the sensors for VMs always remain on the host you originally created them on, also if they are currently running on a different host.

## Basic Sensor Settings

**Basic Sensor Settings**

Sensor Name ⓘ Example Name

Tags ⓘ  X +

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- xenhostsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Host Settings

**Host Settings**

UUID ⓘ 1111aaaa-22bb-cc33-dd44-555555555555

Name ⓘ Example

Host Settings

Setting	Description
UUID	<p>The universally unique identifier (UUID) of the host that this sensor monitors.</p> <p><b>i</b> PRTG shows this value for reference purposes only. We strongly recommend that you only change it if the Paessler support team explicitly asks you to do so. Wrong usage can result in incorrect monitoring data.</p>
Name	The name of the host that this sensor monitors.

## Debug Options

**Debug Options**

**Result Handling** ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**


**Primary Channel** ⓘ Downtime

---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CPU [Value] Usage	The CPU usage <ul style="list-style-type: none"> <li> This channel is the primary channel by default.</li> </ul>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Load Average	The load average amount
VMs Running	The number of running VMs
Total Memory Free	The total memory available

Channel	Description
Total Memory Used	The total memory used

## More

### KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

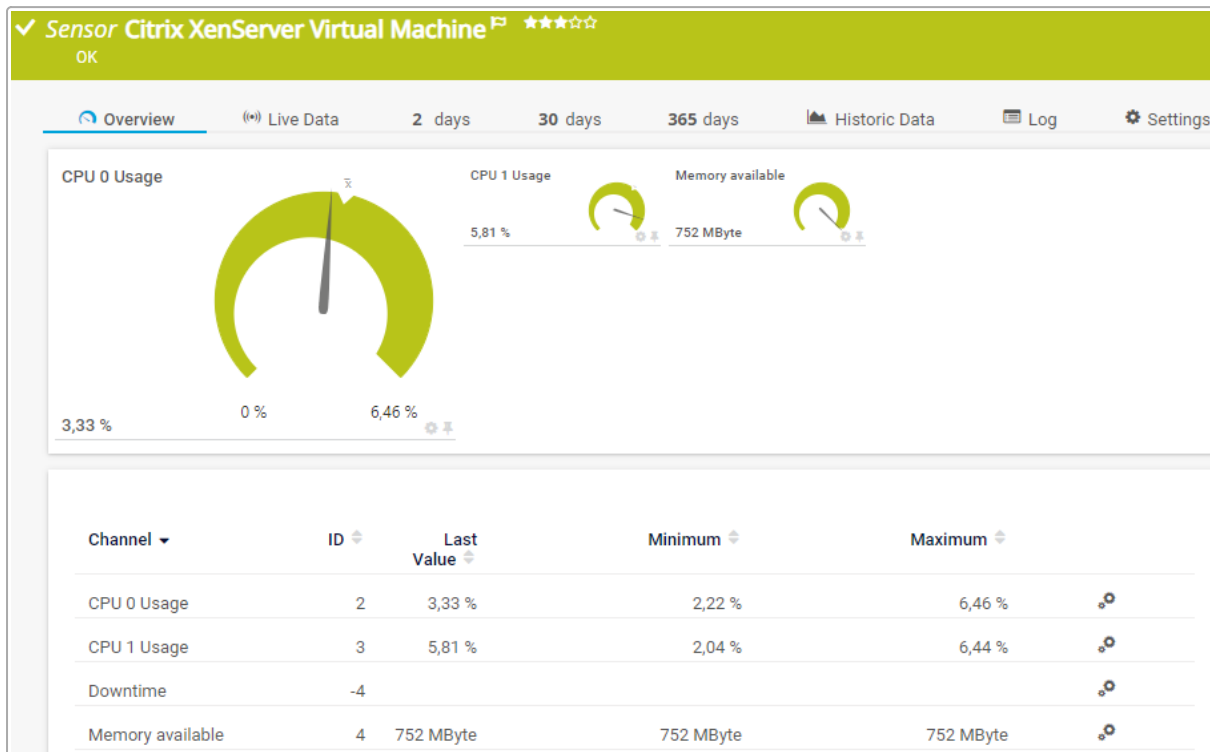
- <https://kb.paessler.com/en/topic/61108>

Does PRTG impair my Citrix environment?

- <https://kb.paessler.com/en/topic/61880>

## 7.8.17 Citrix XenServer Virtual Machine Sensor

The Citrix XenServer Virtual Machine sensor monitors a virtual machine (VM) on a XenServer via HTTP.



Citrix XenServer Virtual Machine Sensor



For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Citrix XenServer Virtuele Machine
- French: Citrix XenServer machine virtuelle
- German: Citrix XenServer Virtuelle Maschine
- Japanese: Citrix XenServer 仮想マシン
- Portuguese: Máquina virtual Citrix XenServer
- Russian: Виртуальная машина Citrix XenServer
- Simplified Chinese: Citrix XenServer 虚拟机
- Spanish: Máquina virtual Citrix XenServer


### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Parent device	<ul style="list-style-type: none"> <li>▪ This sensor requires that the parent device is a Citrix XenServer as of version 5.0.</li> <li>▪ This sensor requires that the parent device represents one host server of your XenServer pool.</li> </ul>
Credentials	This sensor requires credentials for VMware/XenServer.
TLS 1.2	This sensor does not fully support Transport Layer Security (TLS) 1.2 connections. You cannot add it to XenServers with the security protocol setting "TLS 1.2 only".
IPv4	This sensor only supports IPv4.
Add Sensor dialog	PRTG requests a full list of all VMs that are configured on the Citrix XenServer, including VMs that do not run. Therefore, it might take a few seconds before the Add Sensor dialog loads.

## Monitoring a XenServer Pool

In a XenServer pool, there is one "pool master" that manages the pool. Incoming queries on any host are automatically forwarded to the pool master. If you want to monitor your VMs or host servers, create respective sensors on a device that represents [one](#) host server of your pool. Internal processes make sure that monitoring takes place and continues independently from the physical host.

 In the device tree, the sensors for VMs always remain on the host you originally created them on, also if they are currently running on a different host.



## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ

**Priority** ⓘ

Example Name

---

exampletag ✕ +

---

★★★★☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- xenvmsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Virtual Machine Settings

### Virtual Machine Settings

**UUID** ⓘ

**Name** ⓘ

1111aaaa-22bb-cc33-dd44-555555eeeeee

---

Example

Virtual Machine Settings

Setting	Description
UUID	<p>The universally unique identifier (UUID) of the VM that this sensor monitors.</p> <p><span style="color: #dc3545; font-weight: bold;">i</span> PRTG shows this value for reference purposes only. We strongly recommend that you only change it if the Paessler support team explicitly asks you to do so. Wrong usage can result in incorrect monitoring data.</p>
Name	The name of the VM that this sensor monitors.

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

Sensor Display

**Primary Channel** ⓘ

Downtime

---


**Graph Type** ⓘ

Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>


Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CPU [Value] Usage	The CPU usage <ul style="list-style-type: none"> <li> This channel is the primary channel by default.</li> </ul>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Memory Available	The available memory
Memory Used	The used memory
VM Balloon Driver Target	The balloon driver target size

## More

### ■ KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

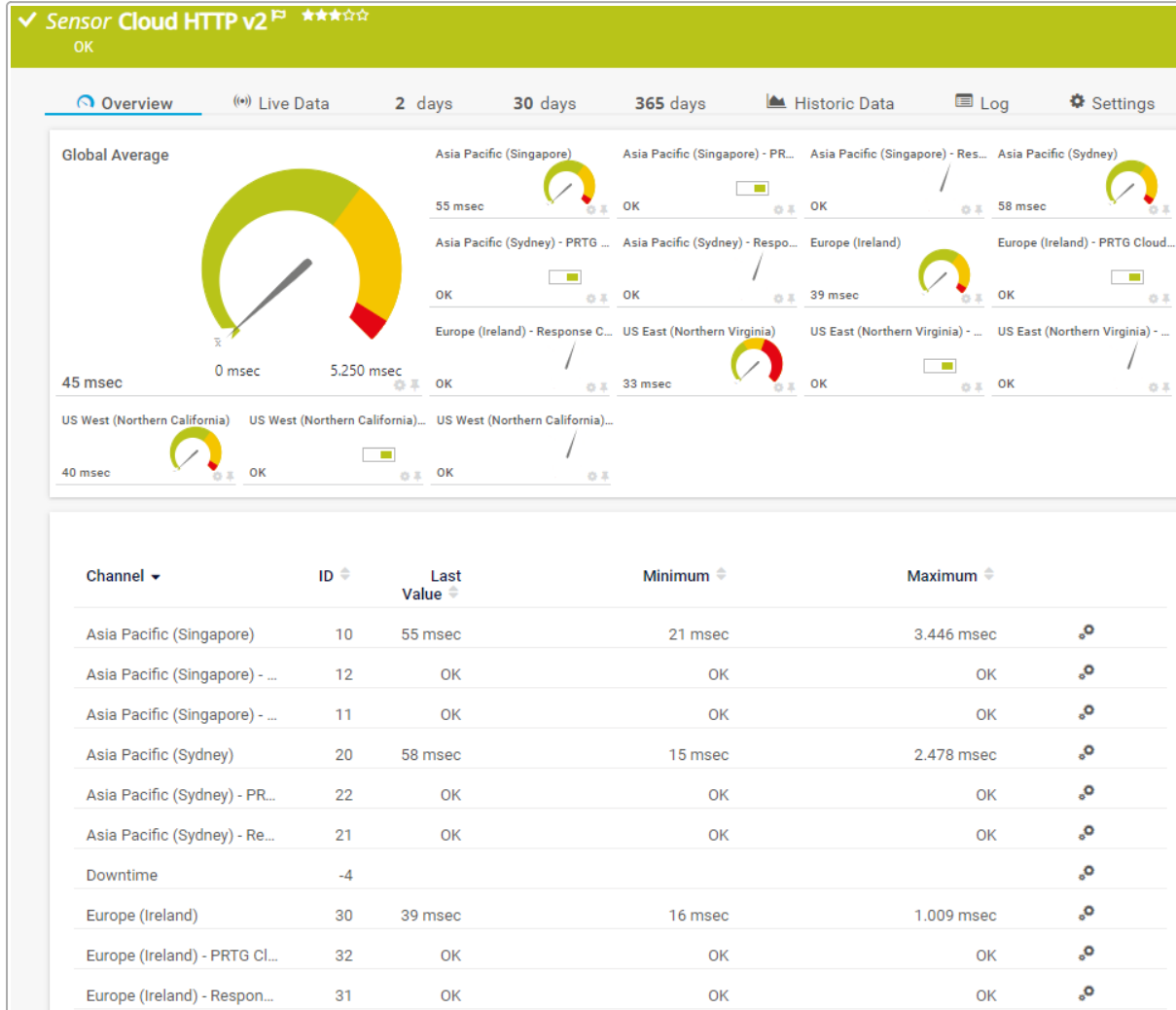
- <https://kb.paessler.com/en/topic/61108>

Does PRTG impair my Citrix environment?

- <https://kb.paessler.com/en/topic/61880>

## 7.8.18 Cloud HTTP v2 Sensor

The Cloud HTTP v2 sensor monitors the loading time of a web server via HTTP from different locations worldwide via the PRTG Cloud. The locations are distributed among four continents around the globe.



Cloud HTTP v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Cloud HTTP v2
- French: Cloud HTTP v2
- German: Cloud HTTP v2
- Japanese: クラウド HTTP v2
- Portuguese: Cloud HTTP v2
- Russian: Cloud HTTP v2
- Simplified Chinese: Cloud HTTP v2

- Spanish: Nube HTTP v2

## Remarks

Consider the following [remarks](#)<sup>[784]</sup> and requirements for this sensor:

Remark	Description
Internet access	<ul style="list-style-type: none"> <li>▪ The probe system requires access to the internet and must be able to reach <a href="https://api.prtgcloud.com:443">https://api.prtgcloud.com:443</a> to communicate with the PRTG Cloud.</li> <li>▪ This sensor requires that the address in the settings of the parent device is reachable via the internet.</li> </ul>
Smart URL replacement	This sensor supports <a href="#">smart URL replacement</a> <sup>[788]</sup> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Probe system	To monitor a probe system, enter the URL of the probe system that is reachable via the internet as Custom URL in the <a href="#">Cloud HTTP Specific</a> <sup>[785]</sup> settings or add a device with the URL in the settings of the device.
Inheritance	This sensor inherits <a href="#">proxy settings</a> from the parent device.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">5 minutes</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.
Knowledge Base	Knowledge Base: <a href="#">What is the PRTG Cloud Bot?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cloud
- cloudhttpsensor
- http

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Cloud HTTP Specific

### Cloud HTTP Specific





**URL** ⓘ  Inherit (default)  
 Custom

**Request Method** ⓘ  GET (default)  
 POST  
 HEAD

**Region** ⓘ  Asia Pacific (Singapore)  
 Asia Pacific (Sydney)  
 Europe (Ireland)  
 US East (Northern Virginia)  
 US West (Northern California)

**Timeout (Sec.)** ⓘ

Cloud HTTP Specific

Setting	Description
URL	<p>Select if you want to inherit the URL from the parent device or if you want to enter a custom URL:</p> <ul style="list-style-type: none"> <li>▪ Inherit (default)</li> <li>▪ Custom</li> </ul>
Custom URL	<p><b>This setting is only visible if you select Custom above.</b></p> <p>Enter the URL that you want to monitor.</p> <p> The URL must be valid and <a href="#">URL encoded</a>.</p> <p> You can enter a URL that leads to a web page, for example, to measure the page source code's loading time, or you can enter the URL of an image or other page asset to measure this element's availability and loading time.</p> <p> PRTG uses a smart URL replacement with which you can use the parent device's IP address or Domain Name System (DNS) name setting as part of the URL. For more information, see section <a href="#">Smart URL Replacement</a><sup>[788]</sup>.</p>
Request Method	<p>Select an HTTP request method to determine how the sensor requests the URL:</p> <ul style="list-style-type: none"> <li>▪ GET (default): Directly request the web page. We recommend that you use this setting for a simple check of a web page.</li> <li>▪ POST: Send post form data to the URL.</li> <li>▪ HEAD: Only request the HTTP header from the server without the actual web page. <ul style="list-style-type: none"> <li> This setting saves bandwidth because it transfers less data. However, we do not recommend this setting because the measured request time is not the request time that the users experience and you might not be notified of slow results or timeouts.</li> </ul> </li> </ul>
Postdata	<p><b>This setting is only visible if you select POST above.</b></p> <p>Enter the data part for the POST request.</p>
Region	<p>Select the regions from which you want to check the service:</p> <ul style="list-style-type: none"> <li>▪ Asia Pacific (Singapore)</li> <li>▪ Asia Pacific (Sydney)</li> <li>▪ Europe (Ireland)</li> <li>▪ US East (Northern Virginia)</li> <li>▪ US West (Northern California)</li> </ul>



Setting	Description
	<b>i</b> PRTG creates two channels for every region that you select.
Timeout (Sec.)	Enter a timeout in seconds for the ping. If the reply takes longer than this value, PRTG cancels the request and shows an error message. Enter an integer. You can enter a value between <b>1</b> and <b>30</b> seconds.

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

Graph Type **i**  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.  <b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.
Graph Type	Define how this sensor shows different channels: <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a> ).
Stack Unit	<b>This setting is only visible if you select Stack channels on top of each other above.</b>  Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can only enter the protocol followed by a colon and three forward slashes (this means that you can enter either [http://](#) or [https://](#), or even a simple forward slash / as the equivalent for [http://](#)). PRTG automatically fills in the parent device's IP Address/DNS Name in front of the third forward slash.

Whether this results in a valid URL or not depends on the IP address or Domain Name System (DNS) name of the parent device. In combination with cloning devices, you can use smart URL replacement to create many similar devices.

For example, if you create a device with the DNS name [www.example.com](#) and you add an HTTP sensor to it, you can provide values in the following ways:

- If you enter [https://](#) in the URL field, PRTG automatically creates the URL [https://www.example.com/](#)

- If you enter [/help](#) in the URL field, PRTG automatically creates and monitor the URL <http://www.example.com/help>
- It is also possible to provide a port number in the URL field. It is taken over by the device's DNS name and is internally added, for example, <http://:8080/>

**i** Smart URL replacement does not work for sensors that run on the probe device.

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Asia Pacific (Singapore)	The response time of the target server at the location <b>i</b> This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: <a href="#">5000 msec</a></li> <li>▪ Upper warning limit: <a href="#">3333 msec</a></li> </ul>
Asia Pacific (Singapore) - HTTP Response Code	The response code of the target server at the location
Asia Pacific (Singapore) - PRTG Cloud Response	If the PRTG Cloud query was successful or not <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Down status: Failed</li> </ul>
Asia Pacific (Sydney)	The response time of the target server at the location <b>i</b> This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: <a href="#">5000 msec</a></li> <li>▪ Upper warning limit: <a href="#">3333 msec</a></li> </ul>
Asia Pacific (Sydney) - HTTP Response Code	The response code of the target server at the location
Asia Pacific (Sydney) - PRTG Cloud Response	If the PRTG Cloud query was successful or not <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Down status: Failed</li> </ul>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Europe (Ireland)	The response time of the target server at the location ⓘ This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: 5000 msec</li> <li>▪ Upper warning limit: 3333 msec</li> </ul>
Europe (Ireland) - HTTP Response Code	The response code of the target server at the location
Europe (Ireland) - PRTG Cloud Response	If the PRTG Cloud query was successful or not <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Down status: Failed</li> </ul>
Global Average	The average global loading time ⓘ This channel is the primary channel by default. ⓘ This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: 5000 msec</li> <li>▪ Upper warning limit: 3333 msec</li> </ul>
US East (Northern Virginia)	The response time of the target server at the location ⓘ This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: 5000 msec</li> <li>▪ Upper warning limit: 3333 msec</li> </ul>
US East (Northern Virginia) - HTTP Response Code	The response code of the target server at the location
US East (Northern Virginia) - PRTG Cloud Response	If the PRTG Cloud query was successful or not <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Down status: Failed</li> </ul>
US West (Northern California)	The response time of the target server at the location ⓘ This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: 5000 msec</li> <li>▪ Upper warning limit: 3333 msec</li> </ul>

Channel	Description
US West (Northern California) - HTTP Response Code	The response code of the target server at the location
US West (Northern California) - PRTG Cloud Response	If the PRTG Cloud query was successful or not <ul style="list-style-type: none"><li>▪ Up status: OK</li><li>▪ Down status: Failed</li></ul>

## More

### KNOWLEDGE BASE

What is the PRTG Cloud Bot?

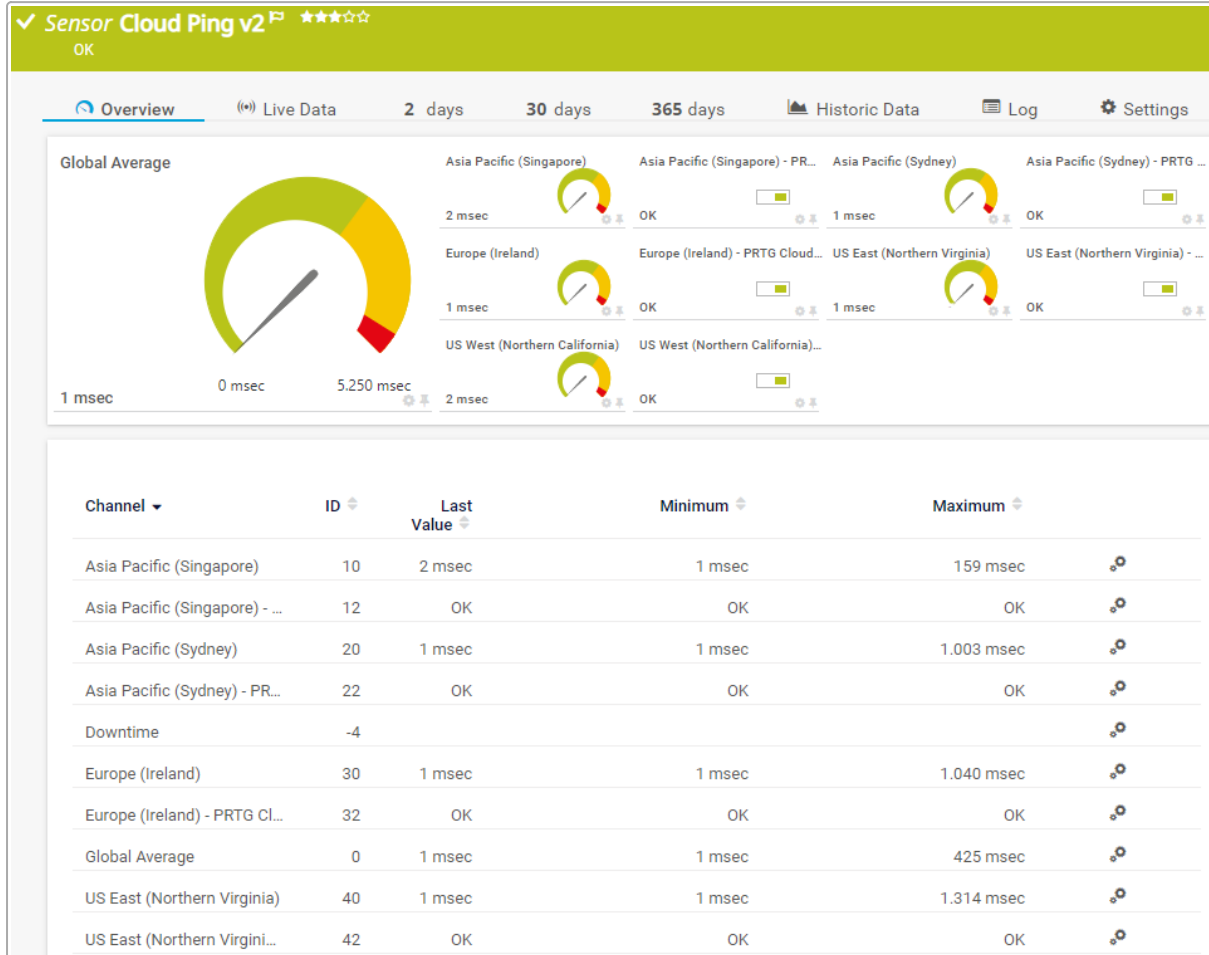
- <https://kb.paessler.com/en/topic/65719>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.19 Cloud Ping v2 Sensor

The Cloud Ping v2 sensor monitors the Transmission Control Protocol (TCP) ping times to its parent device from different locations worldwide via the PRTG Cloud. The locations are distributed among four continents around the globe.



Cloud Ping v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Cloud Ping v2
- French: Cloud Ping v2
- German: Cloud Ping v2
- Japanese: クラウド Ping v2
- Portuguese: Cloud Ping v2
- Russian: Cloud Ping v2
- Simplified Chinese: Cloud Ping v2
- Spanish: Nube ping v2

## Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Internet access	<ul style="list-style-type: none"> <li>The probe system requires access to the internet and must be able to reach <a href="https://api.prtgcloud.com:443">https://api.prtgcloud.com:443</a> to communicate with the PRTG Cloud.</li> <li>This sensor requires that the address in the settings of the parent device is reachable via the internet.</li> </ul>
Localhost	You cannot use this sensor to monitor localhost (127.0.0.1).
IPv4	This sensor only supports IPv4.
Performance impact	This sensor has a <b>low</b> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Probe system	To monitor the probe system, enter the IP address or the fully qualified domain name (FQDN) of the probe system that is reachable via the internet as Custom Target Address in the <a href="#">Cloud Ping Specific</a> settings or add a device with the IP address or the DNS name of the probe system.
TCP	This sensor uses Transmission Control Protocol (TCP) ping.
Inheritance	This sensor inherits <a href="#">proxy settings</a> from the parent device.
Scanning interval	<ul style="list-style-type: none"> <li>The minimum scanning interval of this sensor is <b>1 minute</b>.</li> <li>The recommended scanning interval of this sensor is <b>5 minutes</b>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.
Knowledge Base	Knowledge Base: <a href="#">What is the PRTG Cloud Bot?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cloud
- cloudpingsensor
- ping

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>[667]</sup>.

## Cloud Ping Specific

### Cloud Ping Specific

**Target Address** ⓘ  Inherit (default)  
 Custom

---

**Port** ⓘ 80

---

**Ping Count** ⓘ 1

---

**Region** ⓘ



- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Europe (Ireland)
- US East (Northern Virginia)
- US West (Northern California)

---

**Timeout (Sec.)** ⓘ 5


Cloud Ping Specific



Setting	Description
Target Address	Select if you want to inherit the IP address or the FQDN from the parent device or if you want to enter a custom target address: <ul style="list-style-type: none"> <li>▪ Inherit (default)</li> <li>▪ Custom</li> </ul>
Custom Target Address	<a href="#">This setting is only visible if you select Custom above.</a> Enter the IP address or the FQDN of the target device.
Port	Enter the number of the port that this sensor uses for TCP ping. The default port is <a href="#">80</a> .  This sensor does not support port 25.
Ping Count	Enter the number of pings that PRTG sends in a row to the parent device in one scanning interval. Enter an integer. The minimum value is <a href="#">1</a> . The maximum value is <a href="#">10</a> .
Region	Select the regions from which you want to check the service: <ul style="list-style-type: none"> <li>▪ Asia Pacific (Singapore)</li> <li>▪ Asia Pacific (Sydney)</li> <li>▪ Europe (Ireland)</li> <li>▪ US East (Northern Virginia)</li> <li>▪ US West (Northern California)</li> </ul>
Timeout (Sec.)	Enter a timeout in seconds <a href="#">per ping</a> . You can enter a value between <a href="#">1</a> and <a href="#">30</a> seconds.  The actual timeout duration depends on the number of pings that you entered under Ping Count. PRTG calculates this value by multiplying <a href="#">Ping Count</a> by <a href="#">Timeout (Sec.)</a> .




## Sensor Display

**Sensor Display**

Primary Channel  Downtime


Graph Type 
 Show channels independently (default)  
 Stack channels on top of each other

Sensor Display


Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><a href="#">This setting is only visible if you select</a> Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**


**Result Handling** 
 Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Asia Pacific (Singapore)	<p>The response time of the target server at the location</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: <a href="#">5000 msec</a></li> <li>▪ Upper warning limit: <a href="#">3333 msec</a></li> </ul>
Asia Pacific (Singapore) - PRTG Cloud Response	<p>If the PRTG Cloud query was successful or not</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Down status: Failed</li> </ul>
Asia Pacific (Sydney)	<p>The response time of the target server at the location</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: <a href="#">5000 msec</a></li> <li>▪ Upper warning limit: <a href="#">3333 msec</a></li> </ul>
Asia Pacific (Sydney) - PRTG Cloud Response	<p>If the PRTG Cloud query was successful or not</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Down status: Failed</li> </ul>

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Europe (Ireland)	The response time of the target server at the location ⓘ This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: <a href="#">5000 msec</a></li> <li>▪ Upper warning limit: <a href="#">3333 msec</a></li> </ul>
Europe (Ireland) - PRTG Cloud Response	If the PRTG Cloud query was successful or not <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Down status: Failed</li> </ul>
Global Average	The average global response time ⓘ This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: <a href="#">5000 msec</a></li> <li>▪ Upper warning limit: <a href="#">3333 msec</a></li> </ul> ⓘ This channel is the primary channel by default.
US East (Northern Virginia)	The response time of the target server at the location ⓘ This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: <a href="#">5000 msec</a></li> <li>▪ Upper warning limit: <a href="#">3333 msec</a></li> </ul>
US East (Northern Virginia) - PRTG Cloud Response	If the PRTG Cloud query was successful or not <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Down status: Failed</li> </ul>
US West (Northern California)	The response time of the target server at the location ⓘ This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: <a href="#">5000 msec</a></li> <li>▪ Upper warning limit: <a href="#">3333 msec</a></li> </ul>
US West (Northern California) - PRTG Cloud Response	If the PRTG Cloud query was successful or not <ul style="list-style-type: none"> <li>▪ Up status: OK</li> </ul>

Channel	Description
	<ul style="list-style-type: none"><li>▪ Down status: Failed</li></ul>

## More

### KNOWLEDGE BASE

What is the PRTG Cloud Bot?

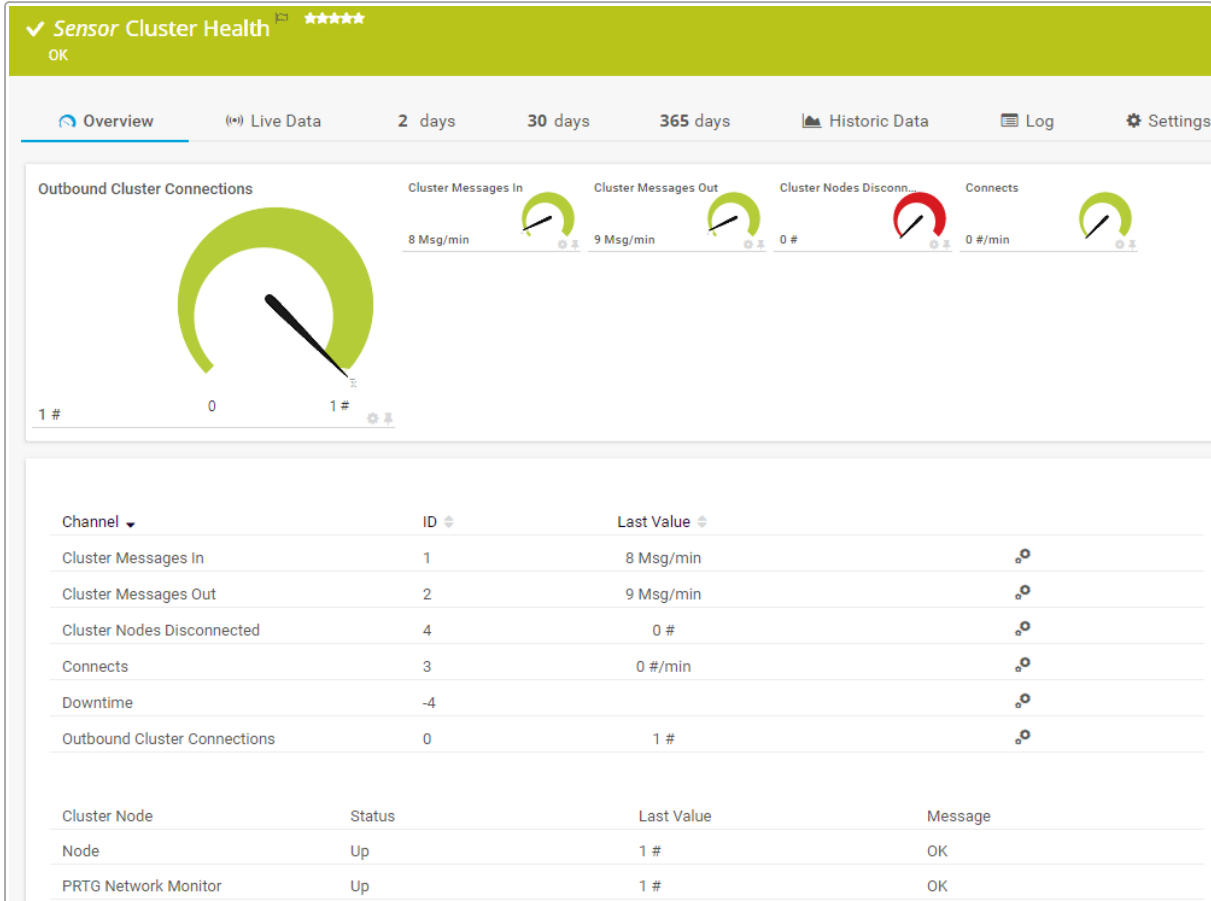
- <https://kb.paessler.com/en/topic/65719>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.20 Cluster Health Sensor

The Cluster Health sensor monitors the health of a [failover cluster](#) and indicates the system health status of PRTG.



Cluster Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Cluster Status
- French: État du cluster
- German: Cluster-Zustand
- Japanese: クラスターの正常性
- Portuguese: Funcionamento do cluster
- Russian: Работоспособность кластера
- Simplified Chinese: 群集健康状况
- Spanish: Salud de clúster

## Remarks

Consider the following [remarks](#)<sup>[801]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <b>very low</b> performance impact.
Sensor creation	PRTG automatically creates this sensor with a cluster installation. You cannot manually delete it or add it.
Down status	If at least one cluster node is disconnected, this sensor shows the Down <a href="#">status</a> by default.
Cluster node states	You can review the states of each cluster node on this sensor's Overview tab.
Cluster node data	You can choose the cluster node for which you want to show data (or for all cluster nodes) on the monitoring data review tabs. For more information, see the Knowledge Base: <a href="#">What options do I have to review my monitoring data in detail?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- clusterhealthsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.



Channel	Description
Cluster Messages In	The number of ingoing cluster messages per minute
Cluster Messages Out	The number of outgoing cluster messages per minute
Cluster Nodes Disconnected	The number of disconnected cluster nodes ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper error limit: 0</li> </ul>
Connects	The number of connects per minute
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Outbound Cluster Connections	The number of outbound cluster connections ⓘ This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

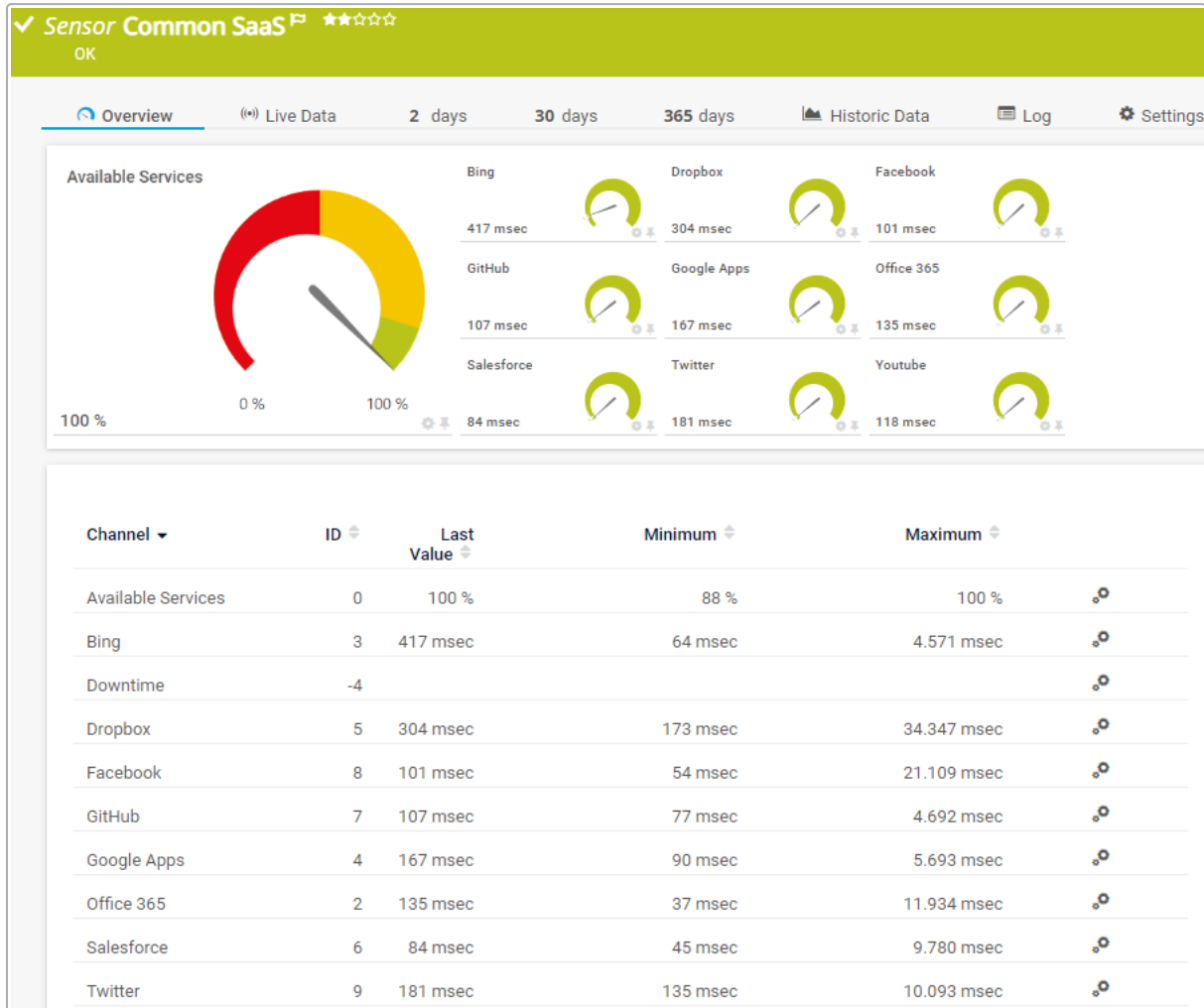
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.21 Common SaaS Sensor

The Common SaaS sensor monitors the availability of several software as a service (SaaS) providers.

**i** With this sensor, you can get alarms if your cloud services are not reachable.



Common SaaS Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Algemene SaaS
- French: SaaS courants
- German: Verbreitete SaaS-Dienste
- Japanese: Common SaaS
- Portuguese: SaaS Comuns
- Russian: Общий для SaaS
- Simplified Chinese: 常用 SaaS

- Spanish: SaaS común

## Remarks

Consider the following [remarks](#) <sup>805</sup> and requirements for this sensor:

Remark	Description
Internet access	This sensor requires that the probe system has access to the internet.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Scanning interval	This sensor has a fixed scanning interval of <a href="#">15 minutes</a> . You cannot change it.
Sensor creation	PRTG automatically creates this sensor on every probe device. If the probe system has no connection to the internet, manually <a href="#">pause</a> or <a href="#">delete</a> this sensor to avoid error messages.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- commonsaas
- saas

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Debug Options

**Debug Options**

**Result Handling** ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

**Primary Channel** ⓘ Downtime  


---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Available Services	<p>The available services (%)</p> <ul style="list-style-type: none"> <li><b>i</b> This channel is the primary channel by default.</li> <li><b>i</b> This channel has default limits:                             <ul style="list-style-type: none"> <li>Lower error limit: <a href="#">50</a></li> <li>Lower warning limit: <a href="#">90</a></li> </ul> </li> </ul>
Bing	The response time of the SaaS provider
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Dropbox	The response time of the SaaS provider
Facebook	The response time of the SaaS provider
GitHub	The response time of the SaaS provider
Google Apps	The response time of the SaaS provider
Office 365	The response time of the SaaS provider
Salesforce	The response time of the SaaS provider
Twitter	The response time of the SaaS provider
Youtube	The response time of the SaaS provider

## More

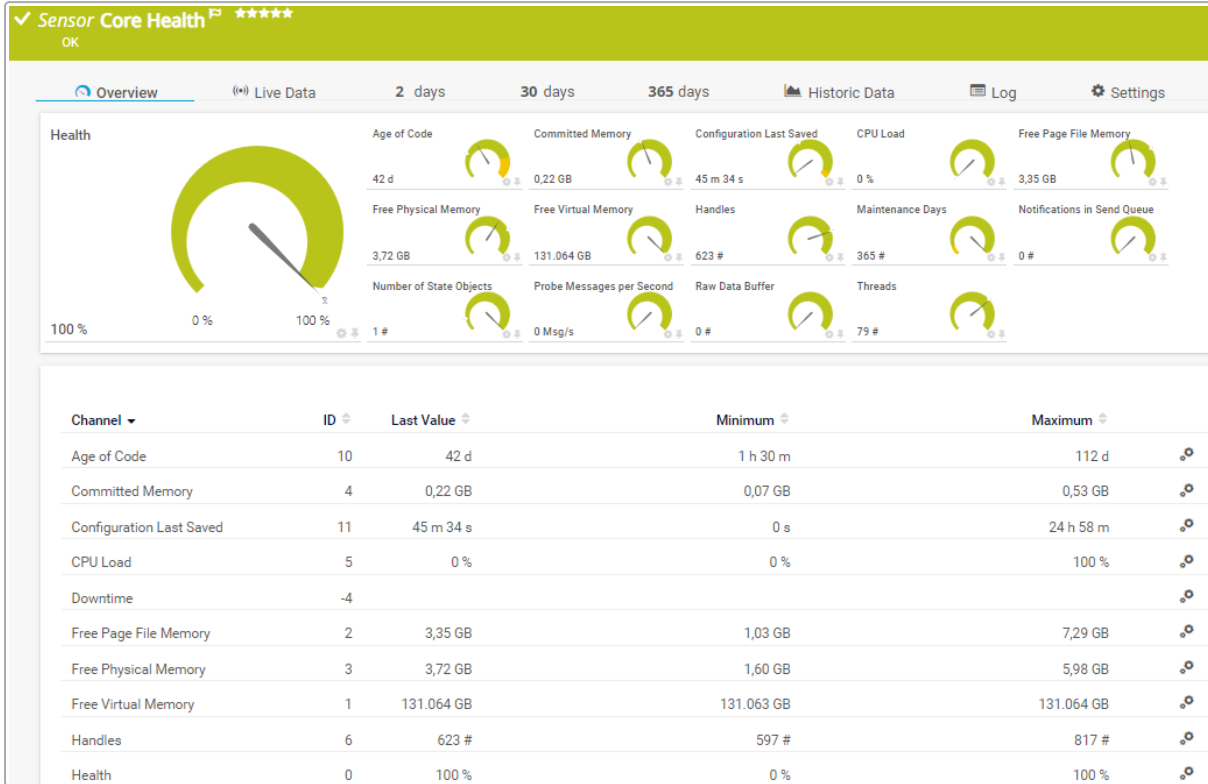
### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.22 Core Health Sensor

The Core Health sensor is a probe-dependent sensor that monitors internal PRTG parameters. It shows the status of the PRTG core server and checks various parameters of the PRTG core server that have an impact on the stability of the system.



Core Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Core Status
- French: État du serveur central
- German: Serverzustand
- Japanese: コアの正常性
- Portuguese: Funcionamento do servidor central
- Russian: Работоспособность базового сервера
- Simplified Chinese: 核心健康状况
- Spanish: Salud de servidor central

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <b>very low</b> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Sensor creation	PRTG automatically creates this sensor. You cannot delete it.
Sensor usage	You can only set up this sensor on a local probe device.
Memory information	You can also find information related to PRTG core server system memory under Setup   PRTG Status.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- corehealthsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Display

#### Sensor Display

**Primary Channel** ⓘ Downtime

---


**Graph Type** ⓘ

Show channels independently (default)


Stack channels on top of each other


Sensor Display



Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.




 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Age of Code	<p>The time that has passed since the last update of your PRTG core server. Update regularly to get the best security and stability for PRTG, as well as the latest features. We recommend that you use the <a href="#">auto-update</a> to automatically get new versions.</p>

Channel	Description
	<p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper warning limit: <a href="#">7776000 seconds</a></li> </ul>
Committed Memory	The amount of memory committed to the PRTG core server as reported by the memory manager
Configuration Last Saved	<p>The time passed since the configuration file was last saved successfully. PRTG saves the configuration every 24 hours. If the configuration cannot be saved, PRTG creates a ticket as soon as the saving process has failed, and warns you via this channel after 26 hours. None of your changes to PRTG can be saved if this happens. In this case, restart your PRTG core server to save the file.</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper warning limit: <a href="#">93600 seconds</a></li> </ul>
CPU Load	The CPU load (%). Extensive CPU load can lead to false, incomplete, and incorrect monitoring results. This value should usually stay below 50%.
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Page File Memory	The amount of free page file memory that is available on the system. Page file memory is aggregated RAM and the size of page file. It is the maximum amount of memory that is available on the system to be used for all running processes. If it gets too low, the system can break down, and at least some applications throw <a href="#">Out of memory</a> errors.
Free Physical Memory	The amount of free physical memory that is available on the system. This is the RAM that is physically built into the computer. If it gets too low, the system becomes very slow and PRTG no longer works in a useful way. Some sensors might not be displayed correctly and show the Unknown status.
Free Virtual Memory	The address space on the system that PRTG can access. PRTG cannot use more memory than reported here, which is independent from free page file and physical memory. On a 32-bit operating system, the maximum is <a href="#">2 GB</a> ( <a href="#">3 GB</a> with special settings under Windows). On a 64-bit operating system, it is <a href="#">4 GB</a> if PRTG runs as a 32-bit version, and <a href="#">unlimited</a> if it runs as a 64-bit version (PRTG core server only). If the free virtual memory gets too low, PRTG throws <a href="#">Out of memory</a> errors or the message <a href="#">not enough storage to process this command</a> . This message is visible in the Core log.

Channel	Description
Handles	The counter for the data structures of the operating system. It is responsible for internal resource management. Investigate obviously increasing values that occur repeatedly.
Health	The sum of the PRTG core server state as a value between 100% (healthy) and 0% (failing). Investigate frequent or repeated health values below 100%.   This channel is the primary channel by default.
Maintenance Days	The remaining maintenance days of your PRTG Network Monitor license. If your maintenance is going to expire soon, act in time to make sure that you continue to get updates and access to new features for PRTG Network Monitor.   PRTG Hosted Monitor shows a fixed value here for technical reasons.   This channel has default limits: <ul style="list-style-type: none"> <li>▪ Lower error limit: 0</li> <li>▪ Lower warning limit: 30</li> </ul>
Notifications in Send Queue	The number of notifications that are in the send queue
Number of State Objects	The number of user-specific state objects that are found in the memory of the PRTG core server system
Probe Messages per Second	The number of messages sent from all probes to the PRTG core server
Raw Data Buffer	The amount of raw data that is temporarily stored on the physical memory during I/O operations on the disk. Usually, this value should be 0 (or very low). Investigate increasing values.
Threads	The number of program parts that are running simultaneously. This number can increase with heavy load. Usually, this number should not exceed 100.

## More

### KNOWLEDGE BASE

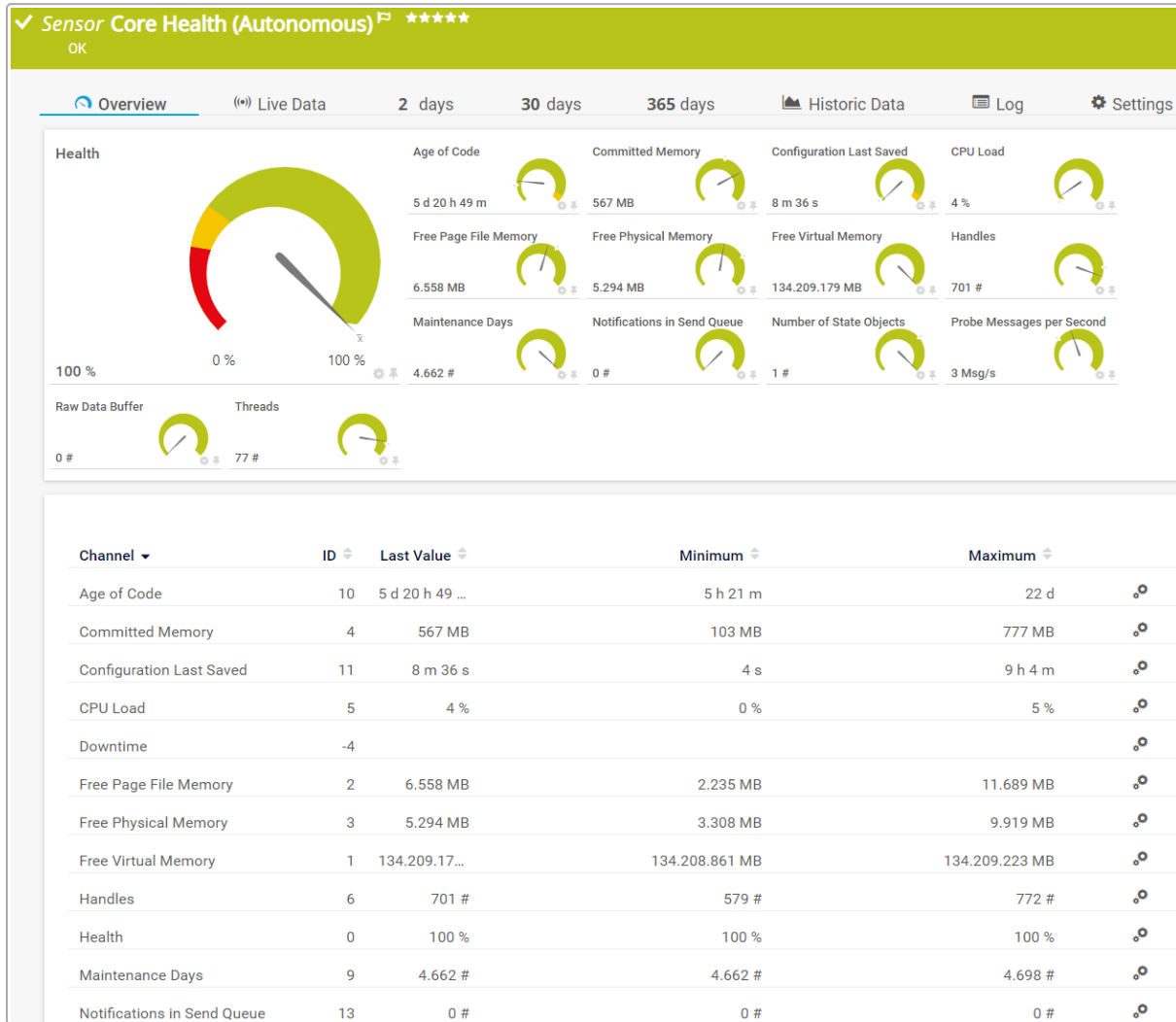
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

### 7.8.23 Core Health (Autonomous) Sensor

The Core Health (Autonomous) sensor is a probe-independent sensor that monitors internal PRTG parameters. It shows the status of the PRTG core server and checks various parameters of the PRTG core server that have an impact on the stability of the system.

**i** The Core Health (Autonomous) sensor has the same functionality as the [Core Health](#) sensor. The only difference is that the Core Health (Autonomous) sensor runs independently of the probe. This means that if the probe disconnects, this sensor still monitors the status of the PRTG core server.



Core Health (Autonomous) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

#### Sensor in Other Languages

- Dutch: Core Health (autonom)
- French: État du serveur central (autonome)
- German: Serverzustand (Autonom)
- Japanese: コアの正常性 (自律)

- Portuguese: Funcionamento do servidor central (autônomo)
- Russian: Работоспособность базового сервера (автономно)
- Simplified Chinese: 核心健康状况 (自主程序)
- Spanish: Salud de servidor central (autónomo)

## Remarks

Consider the following [remarks](#) <sup>815</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Sensor creation	PRTG automatically creates this sensor. You cannot delete it.
Sensor creation	You cannot add this sensor to a probe.
Memory information	You can also find information related to PRTG core server system memory under Setup   PRTG Status.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- autonomous
- corehealthsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings




By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Age of Code	<p>The time that has passed since the last update of your PRTG core server. Update regularly to get the best security and stability for PRTG, as well as the latest features. We recommend that you use the <a href="#">auto-update</a> to automatically get new versions.</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper warning limit: <a href="#">7776000 seconds</a></li> </ul>
Committed Memory	<p>The amount of memory committed to the PRTG core server as reported by the memory manager</p>
Configuration Last Saved	<p>The time passed since the configuration file was last saved successfully. PRTG saves the configuration every 24 hours. If the configuration cannot be saved, PRTG creates a ticket as soon as the saving process has failed, and warns you via this channel after 26 hours. None of your changes to PRTG can be saved if this happens. In this case, restart your PRTG core server to save the file.</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper warning limit: <a href="#">93600 seconds</a></li> </ul>
CPU Load	<p>The CPU load (%). Extensive CPU load can lead to false, incomplete, and incorrect monitoring results. This value should usually stay below 50%.</p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Free Page File Memory	<p>The amount of free page file memory that is available on the system. Page file memory is aggregated RAM and the size of page file. It is the maximum amount of memory that is available on the system to be used for all running processes. If it gets too low, the system can break down, and at least some applications throw <a href="#">Out of memory</a> errors.</p>
Free Physical Memory	<p>The amount of free physical memory that is available on the system. This is the RAM that is physically built into the computer. If it gets too low, the system becomes very slow and PRTG no longer works in a useful way. Some sensors might not be displayed correctly and show the Unknown status.</p>

Channel	Description
Free Virtual Memory	The address space on the system that PRTG can access. PRTG cannot use more memory than reported here, which is independent from free page file and physical memory. On a 32-bit operating system, the maximum is <b>2 GB</b> (3 GB with special settings under Windows). On a 64-bit operating system, it is <b>4 GB</b> if PRTG runs as a 32-bit version, and <b>unlimited</b> if it runs as a 64-bit version (PRTG core server only). If the free virtual memory gets too low, PRTG throws <b>Out of memory</b> errors or the message <b>not enough storage to process this command</b> . This message is visible in the Core log.
Handles	The counter for the data structures of the operating system. It is responsible for internal resource management. Investigate obviously increasing values that occur repeatedly.
Health	The sum of the PRTG core server state as a value between 100% (healthy) and 0% (failing). Investigate frequent or repeated health values below 100%.   This channel is the primary channel by default.
Maintenance Days	The remaining maintenance days of your PRTG Network Monitor license. If your maintenance is going to expire soon, act in time to make sure that you continue to get updates and access to new features for PRTG Network Monitor.   PRTG Hosted Monitor shows a fixed value here for technical reasons.   This channel has default limits: <ul style="list-style-type: none"> <li>▪ Lower error limit: <b>0</b></li> <li>▪ Lower warning limit: <b>30</b></li> </ul>
Notifications in Send Queue	The number of notifications that are in the send queue
Number of State Objects	The number of user-specific state objects that are found in the memory of the PRTG core server system
Probe Messages per Second	The number of messages sent from all probes to the PRTG core server
Raw Data Buffer	The amount of raw data that is temporarily stored on the physical memory during I/O operations on the disk. Usually, this value should be 0 (or very low). Investigate increasing values.



Channel	Description
Threads	The number of program parts that are running simultaneously. This number can increase with heavy load. Usually, this number should not exceed 100.

## More

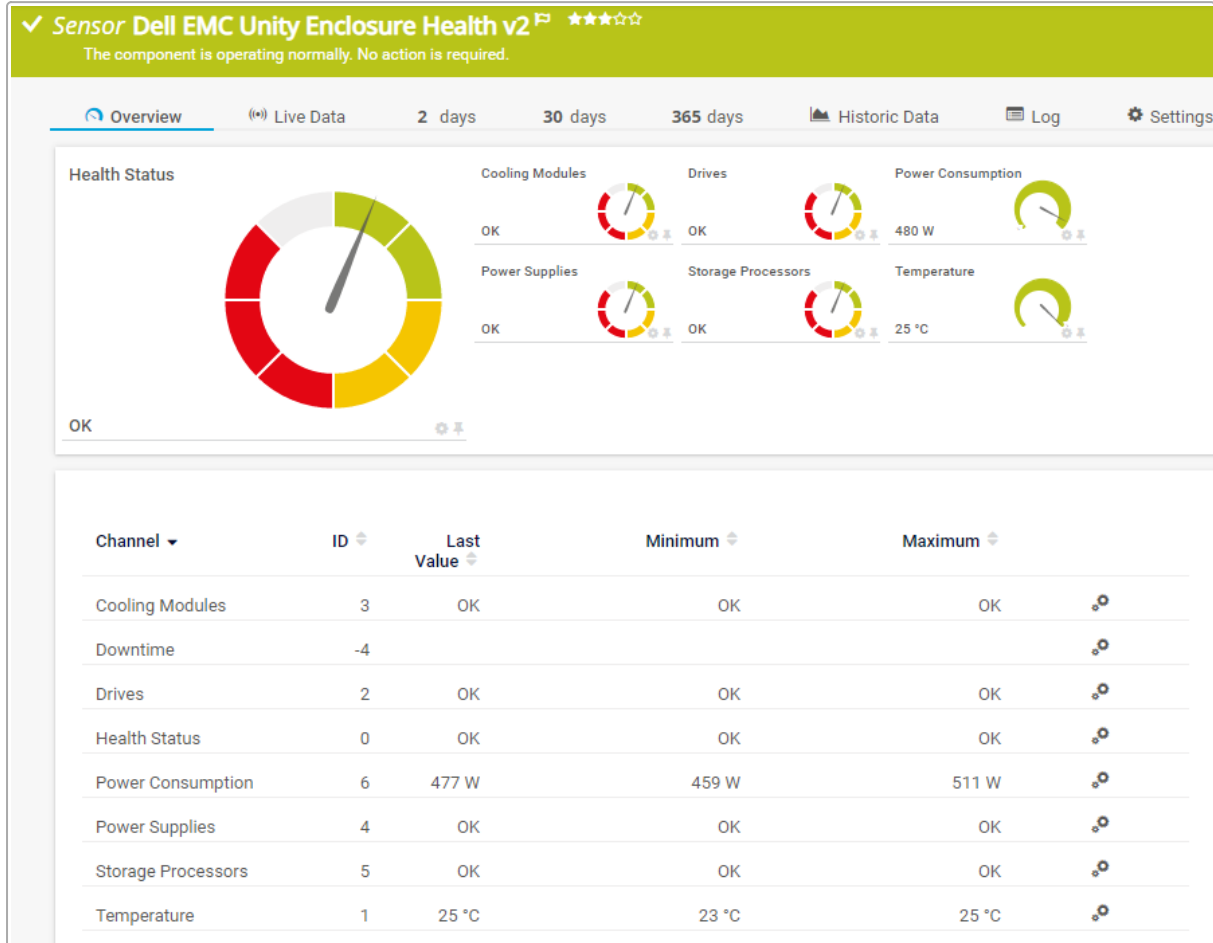
### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.24 Dell EMC Unity Enclosure Health v2 Sensor

The Dell EMC Unity Enclosure Health v2 sensor monitors the health of a disk-array enclosure (DAE) or a physical or virtual disk processor enclosure (DPE) on a Dell EMC storage system via the Representational State Transfer (REST) application programming interface (API).



Dell EMC Unity Enclosure Health v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) <sup>824</sup>.

### Sensor in Other Languages

- Dutch: Dell EMC Unity Enclosure Health v2
- French: Dell EMC Unity état du boîtier v2
- German: Dell EMC Unity Zustand des Gehäuses v2
- Japanese: Dell EMC Unity Enclosure Health v2
- Portuguese: Saúde do sistema Dell EMC Unity v2
- Russian: Работоспособность дисковой полки Dell EMC Unity v2
- Simplified Chinese: Dell EMC Unity 外壳运行状况 v2
- Spanish: Dell EMC Unity salud del gabinete v2

## Remarks

Consider the following [remarks](#) <sup>821</sup> and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for Dell EMC.
Unity OE 5.x	This sensor only supports systems from the Dell EMC Unity family with <a href="#">Unity OE 5.x</a> .
REST API	Dell EMC systems that provide a REST API are <a href="#">EMC Unity Family</a> , <a href="#">EMC Unity All Flash</a> , <a href="#">EMC Unity Hybrid</a> , and <a href="#">EMC UnityVSA</a> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">5 minutes</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ exampletag ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Example Name

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- dellemc
- dellemcenclosure
- dellemcstorage

- restsensor

For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Dell EMC Specific

**Dell EMC Specific**

Enclosure Name ⓘ *Example*

Enclosure Type ⓘ *25 Drive 12G DPE*

Dell EMC Specific

Setting	Description
Enclosure Name	The name of the enclosure that this sensor monitors.
Enclosure Type	The type of the enclosure that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ *Downtime*

Graph Type ⓘ

Show channels independently (default)

Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>

Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**

Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><span style="font-size: 0.8em;">☁</span> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><span style="font-size: 0.8em;">ⓘ</span> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Cooling Modules	<p>The cooling modules status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK, OK But Minor Warning</li> <li>▪ Warning status: Degraded, Minor Issue</li> <li>▪ Down status: Major Issue, Critical Issue, Non Recoverable</li> <li>▪ Unknown status: Unknown</li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Drives	<p>The drives status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK, OK But Minor Warning</li> <li>▪ Warning status: Degraded, Minor Issue</li> <li>▪ Down status: Major Issue, Critical Issue, Non Recoverable</li> <li>▪ Unknown status: Unknown</li> </ul>
Health Status	<p>The health status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK, OK But Minor Warning</li> <li>▪ Warning status: Degraded, Minor Issue</li> <li>▪ Down status: Major Issue, Critical Issue, Non Recoverable</li> <li>▪ Unknown status: Unknown</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Link Control Cards	<p>The link control cards status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK, OK But Minor Warning</li> <li>▪ Warning status: Degraded, Minor Issue</li> <li>▪ Down status: Major Issue, Critical Issue, Non Recoverable</li> <li>▪ Unknown status: Unknown</li> </ul>
Power Consumption	<p>The power consumption</p>

Channel	Description
Power Supplies	The power supplies status <ul style="list-style-type: none"><li>▪ Up status: OK, OK But Minor Warning</li><li>▪ Warning status: Degraded, Minor Issue</li><li>▪ Down status: Major Issue, Critical Issue, Non Recoverable</li><li>▪ Unknown status: Unknown</li></ul>
Temperature	The temperature of the enclosure

## More

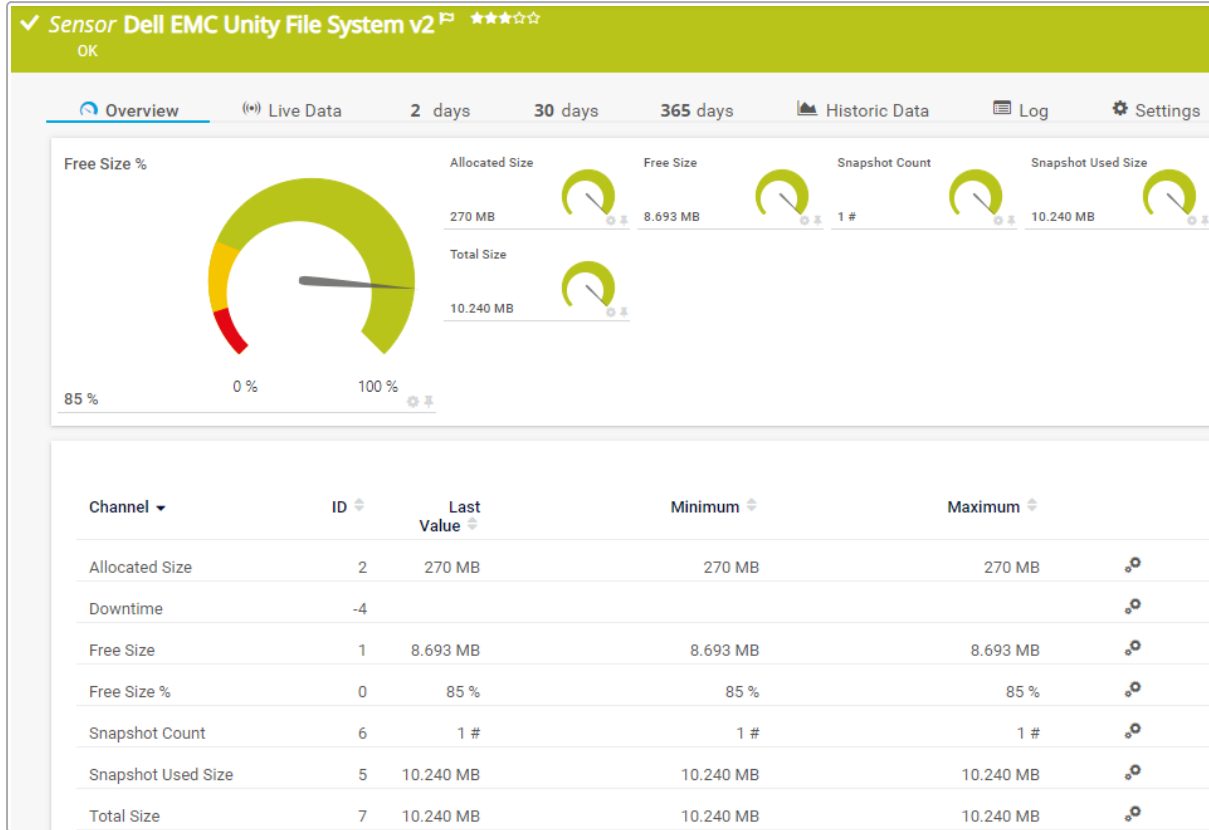
### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.25 Dell EMC Unity File System v2 Sensor

The Dell EMC Unity File System v2 sensor monitors a file system on a Dell EMC storage system via the Representational State Transfer (REST) application programming interface (API).



Dell EMC Unity File System v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Dell EMC Unity Bestandssysteem v2
- French: Dell EMC Unity système de fichiers v2
- German: Dell EMC Unity Dateisystem v2
- Japanese: Dell EMC Unity File System v2
- Portuguese: Sistema de arquivos Dell EMC Unity v2
- Russian: Файловая система Dell EMC Unity v2
- Simplified Chinese: Dell EMC Unity 文件系统 v2
- Spanish: Dell EMC Unity sistema de archivo v2

### Remarks

Consider the following [remarks](#) and requirements for this sensor:



Remark	Description
Credentials	This sensor requires credentials for Dell EMC.
Unity OE 5.x	This sensor only supports systems from the Dell EMC Unity family with <a href="#">Unity OE 5.x</a> .
REST API	Dell EMC systems that provide a REST API are <a href="#">EMC Unity Family</a> , <a href="#">EMC Unity All Flash</a> , <a href="#">EMC Unity Hybrid</a> , and <a href="#">EMC UnityVSA</a> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">5 minutes</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- dellemc
- dellemcfilesystem
- dellemcstorage
- emcfilesystemsensor
- emcsensor
- restsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Dell EMC Specific

**Dell EMC Specific**

**File System Name** ⓘ *Example*

**File System Type** ⓘ *Thin*

**Protocol** ⓘ *CIFS/SMB Share*

Dell EMC Specific

Setting	Description
File System Name	The name of the file system that this sensor monitors.
File System Type	The type of the file system that this sensor monitors.
Protocol	The protocol under which the monitored file system operates.

## Sensor Display


**Sensor Display**

**Primary Channel** ⓘ *Downtime*

**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.  ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.
Graph Type	Define how this sensor shows different channels: <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>



## Debug Options

**Debug Options**


Result Handling 

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Allocated Size	The allocated size
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Size	The free size
Free Size %	<p>The free size (%)</p> <p>ⓘ This channel is the primary channel by default.</p> <p>ⓘ This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: <a href="#">10%</a></li> <li>▪ Lower warning limit: <a href="#">25%</a></li> </ul>
Snapshot Count	The snapshot count
Snapshot Used Size	The used snapshot size
Total Size	The total size

## More

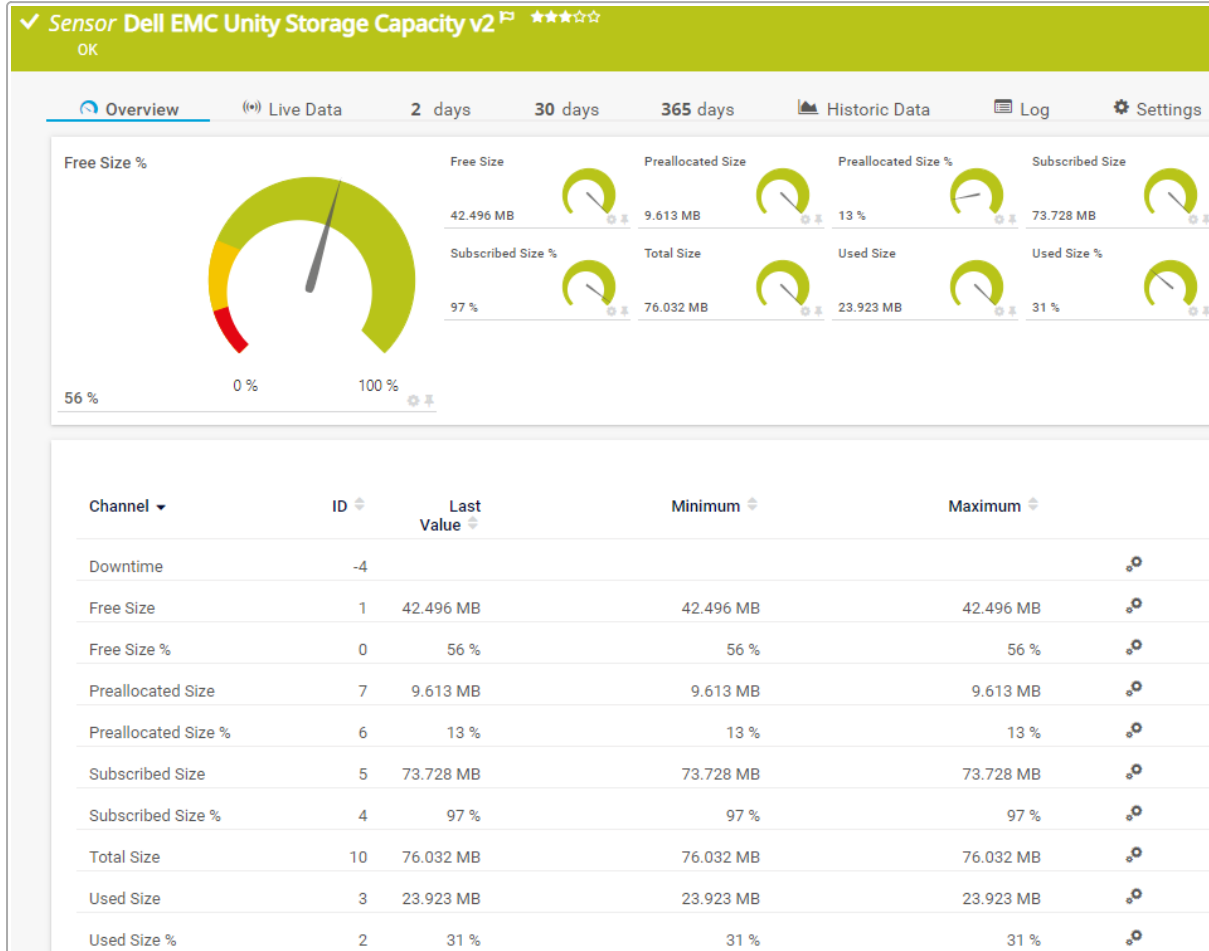
### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.26 Dell EMC Unity Storage Capacity v2 Sensor

The Dell EMC Unity Storage Capacity v2 sensor monitors a Dell EMC storage system via the Representational State Transfer (REST) application programming interface (API).



Dell EMC Unity Storage Capacity v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>834</sup>.

### Sensor in Other Languages

- Dutch: Dell EMC Unity opslagcapaciteit v2
- French: Dell EMC Unity capacité de stockage v2
- German: Dell EMC Unity Speicherkapazität v2
- Japanese: Dell EMC Unity Storage Capacity v2
- Portuguese: Capacidade de armazenamento Dell EMC Unity v2
- Russian: Емкость хранилища Dell EMC Unity v2
- Simplified Chinese: Dell EMC Unity 存储容量 v2
- Spanish: Dell EMC Unity capacidad de almacenamiento v2

## Remarks

Consider the following [remarks](#) <sup>832</sup> and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for Dell EMC.
Unity OE 5.x	This sensor only supports systems from the Dell EMC Unity family with <a href="#">Unity OE 5.x</a> .
REST API	Dell EMC systems that provide a REST API are <a href="#">EMC Unity Family</a> , <a href="#">EMC Unity All Flash</a> , <a href="#">EMC Unity Hybrid</a> , and <a href="#">EMC UnityVSA</a> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">5 minutes</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  X +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- dellemc
- dellemccapacity
- dellemcstorage
- emccapacitysensor

- emcsensor
- restsensor

For more information about basic sensor settings, see section [Sensor Settings](#).

## Sensor Display

**Sensor Display**

**Primary Channel** ⓘ Downtime

---

**Graph Type** ⓘ

Show channels independently (default)

Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**

**Result Handling** ⓘ


Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Size	The free size
Free Size %	<p>The free size (%)</p> <p>ⓘ This channel is the primary channel by default.</p> <p>ⓘ This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: <a href="#">10%</a></li> <li>▪ Lower warning limit: <a href="#">25%</a></li> </ul>



Channel	Description
Preallocated Size	The preallocated size
Preallocated Size %	The preallocated size (%)
Subscribed Size	The subscribed size
Subscribed Size %	The subscribed size (%)
Total Size	The total size
Used Size	The used size
Used Size %	The used size (%)

## More

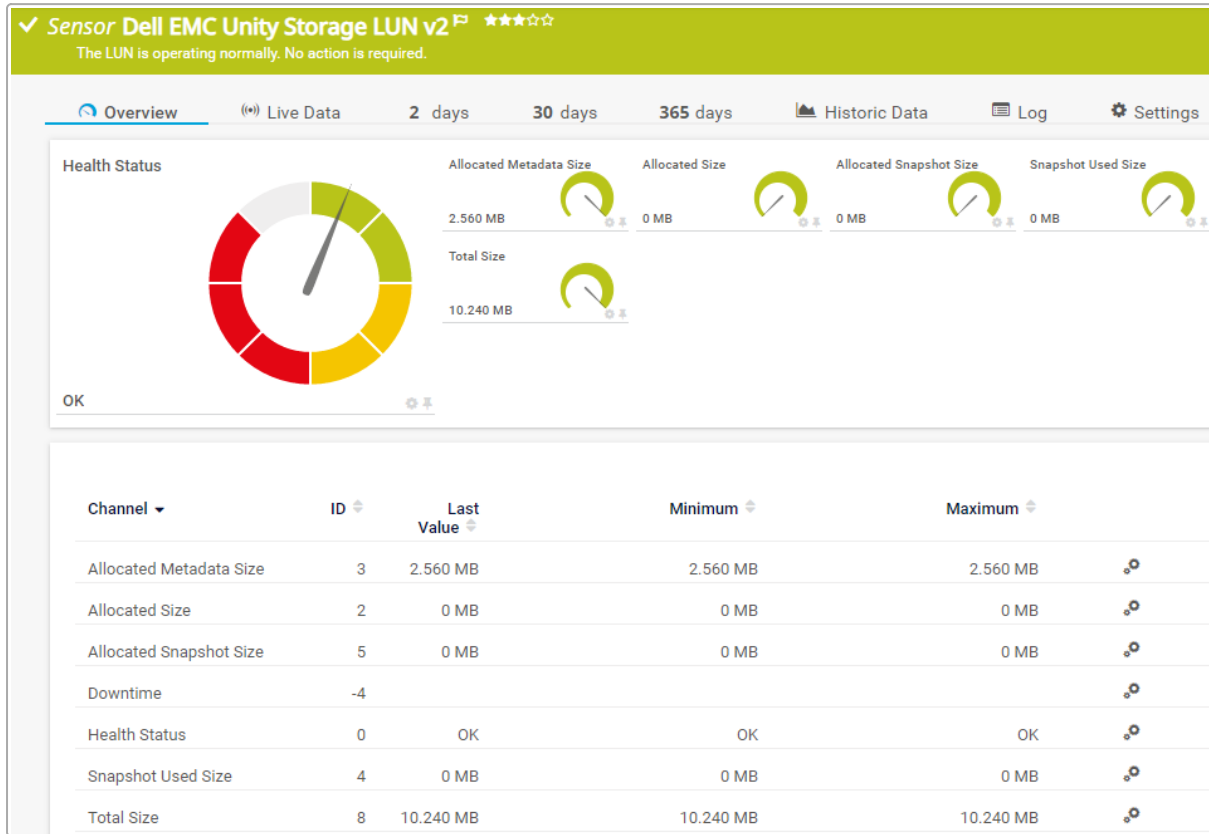
### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.27 Dell EMC Unity Storage LUN v2 Sensor

The Dell EMC Unity Storage LUN v2 sensor monitors a logical unit number (LUN) on a Dell EMC storage system via the Representational State Transfer (REST) application programming interface (API).



Dell EMC Unity Storage LUN v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Dell EMC Unity Opslag LUN v2
- French: Dell EMC Unity LUN de stockage v2
- German: Dell EMC Unity LUN-Speicher v2
- Japanese: Dell EMC Unity Storage LUN v2
- Portuguese: LUN de armazenamento Dell EMC Unity v2
- Russian: LUN хранилища Dell EMC Unity v2
- Simplified Chinese: Dell EMC Unity 存储 LUN v2
- Spanish: Dell EMC Unity almacenamiento LUN v2

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for Dell EMC.
Unity OE 5.x	This sensor only supports systems from the Dell EMC Unity family with <a href="#">Unity OE 5.x</a> .
REST API	Dell EMC systems that provide a REST API are <a href="#">EMC Unity Family</a> , <a href="#">EMC Unity All Flash</a> , <a href="#">EMC Unity Hybrid</a> , and <a href="#">EMC UnityVSA</a> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">5 minutes</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- dellemc
- dellemclun
- dellemcstorage
- emclunsensor
- emcsensor
- restsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Dell EMC Specific

**Dell EMC Specific**

**LUN Name** ⓘ *LUN\_02*

**LUN ID** ⓘ *sv\_15*

Dell EMC Specific

Setting	Description
LUN Name	The name of the LUN that this sensor monitors.
LUN ID	The ID of the LUN that this sensor monitors.

### Sensor Display

**Sensor Display**

**Primary Channel** ⓘ Downtime

**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>

Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**

Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><span style="font-size: 0.8em;">☁</span> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><span style="font-size: 0.8em;">ⓘ</span> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Allocated Metadata Size	The allocated metadata size
Allocated Size	The allocated size
Allocated Snapshot Size	The allocated snapshot size
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Health Status	<p>The health status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK, OK But Minor Warning</li> <li>▪ Warning status: Degraded, Minor Issue</li> <li>▪ Down status: Major Issue, Critical Issue, Non Recoverable</li> <li>▪ Unknown status: Unknown</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Snapshot Used Size	The used snapshot size
Total Size	The total size

## More

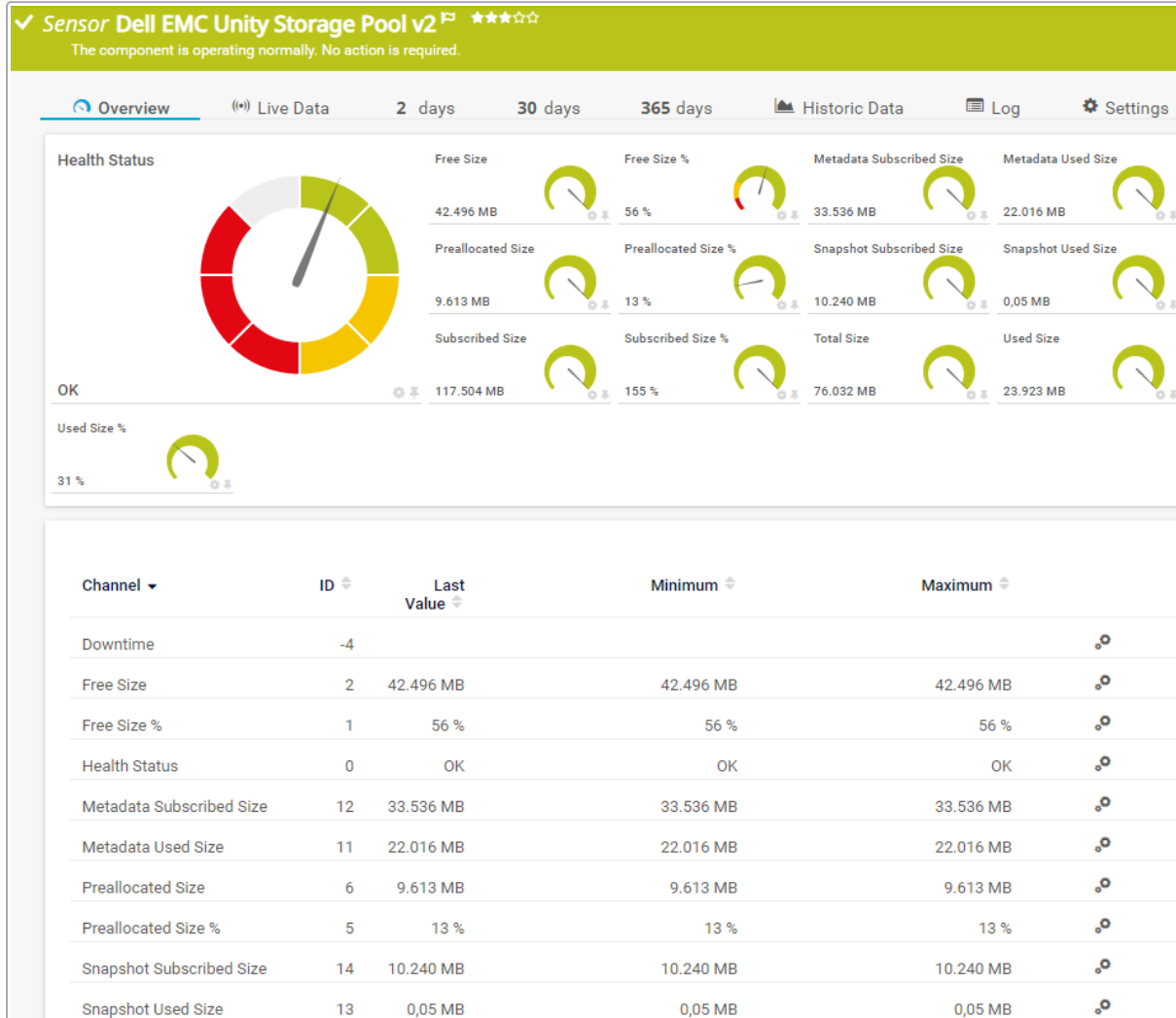
### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.28 Dell EMC Unity Storage Pool v2 Sensor

The Dell EMC Unity Storage Pool v2 sensor monitors a storage pool on a Dell EMC storage system via the Representational State Transfer (REST) application programming interface (API).



Dell EMC Unity Storage Pool v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[845]</sup>.

### Sensor in Other Languages

- Dutch: Dell EMC Unity Opslagpool v2
- French: Dell EMC Unity pool de stockage v2
- German: Dell EMC Unity Speicherpool v2
- Japanese: Dell EMC Unity Storage Pool v2
- Portuguese: Pool de armazenamento Dell EMC Unity v2
- Russian: Пул носителей Dell EMC Unity v2
- Simplified Chinese: Dell EMC Unity 存储池 v2

- Spanish: Dell EMC Unity grupo de almacenamiento v2

## Remarks

Consider the following [remarks](#) <sup>[842]</sup> and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for Dell EMC.
Unity OE 5.x	This sensor only supports systems from the Dell EMC Unity family with <a href="#">Unity OE 5.x</a> .
REST API	Dell EMC systems that provide a REST API are <a href="#">EMC Unity Family</a> , <a href="#">EMC Unity All Flash</a> , <a href="#">EMC Unity Hybrid</a> , and <a href="#">EMC UnityVSA</a> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">5 minutes</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  X +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- dellemc



- dellemcpool
- dellemcstorage
- emcpoolsensor
- emcsensor
- restsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Dell EMC Specific

**Dell EMC Specific**

Storage Pool Name ⓘ *Datstore*

Storage Pool ID ⓘ *pool\_1*

Dell EMC Specific

Setting	Description
Storage Pool Name	The name of the storage pool that this sensor monitors.
Storage Pool ID	The ID of the storage pool that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ *Downtime*


Graph Type ⓘ

Show channels independently (default)

Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	Define how this sensor shows different channels:



Setting	Description
	<ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


### Debug Options

**Result Handling** 
  
 Discard result (default)
   
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>



## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Size	The free size
Free Size %	The free size (%)  This channel has default limits: <ul style="list-style-type: none"> <li>▪ Lower error limit: <a href="#">10%</a></li> <li>▪ Lower warning limit: <a href="#">25%</a></li> </ul>
Health Status	The health status <ul style="list-style-type: none"> <li>▪ Up status: OK, OK But Minor Warning</li> <li>▪ Warning status: Degraded, Minor Issue</li> <li>▪ Down status: Major Issue, Critical Issue, Non Recoverable</li> <li>▪ Unknown status: Unknown</li> </ul>  This channel is the primary channel by default.
Metadata Subscribed Size	The subscribed metadata size
Metadata Used Size	The used metadata size
Preallocated Size	The preallocated size
Preallocated Size %	The preallocated size (%)

Channel	Description
Snapshot Subscribed Size	The subscribed snapshot size
Snapshot Used Size	The used snapshot size
Subscribed Size	The subscribed size
Subscribed Size %	The subscribed size (%)
Total Size	The total size
Used Size	The used size
Used Size %	The used size (%)

## More

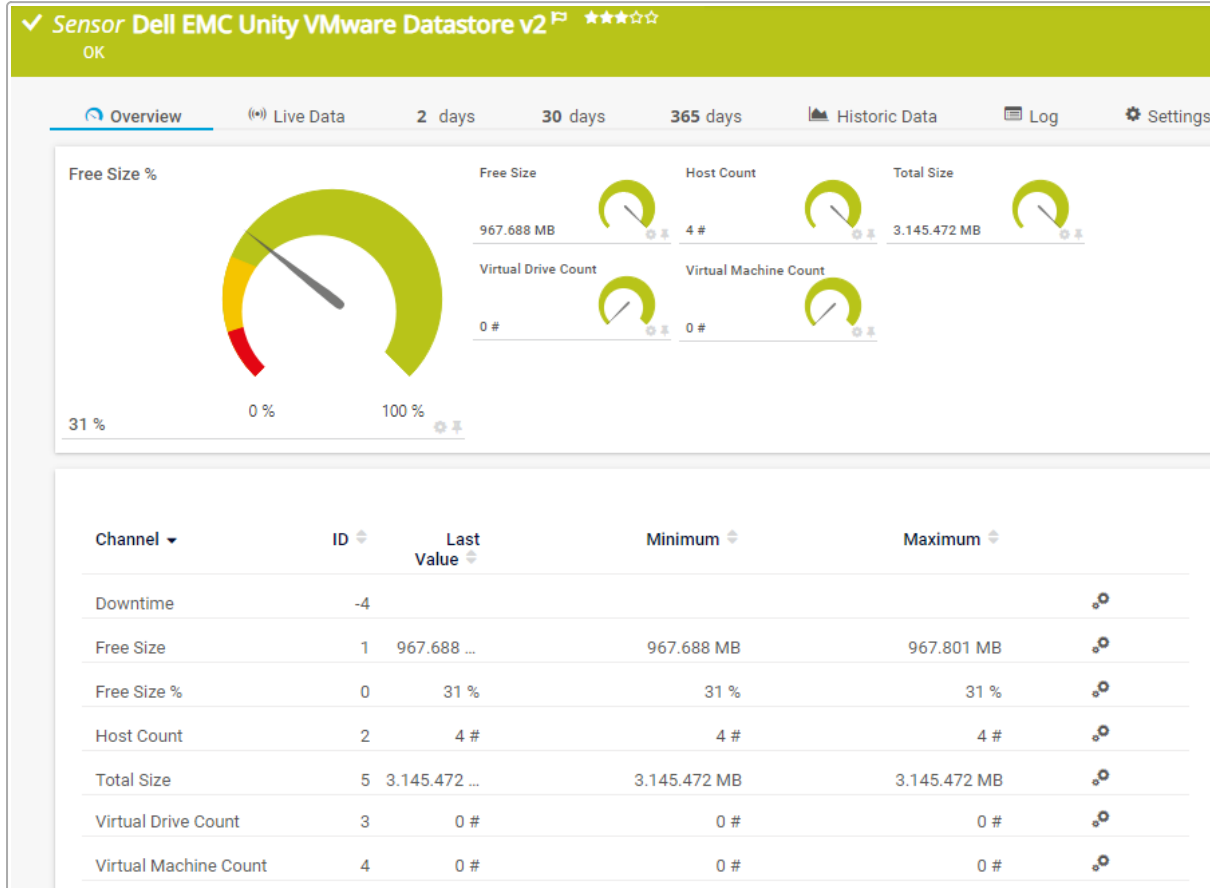
### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.29 Dell EMC Unity VMware Datastore v2 Sensor

The Dell EMC Unity VMware Datastore v2 sensor monitors a VMware datastore on a Dell EMC storage system via the Representational State Transfer (REST) application programming interface (API).



Dell EMC Unity VMw are Datastore v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Dell EMC Unity VMware Datastore v2
- French: Dell EMC Unity VMware datastore v2
- German: Dell EMC Unity VMware-Datenspeicher v2
- Japanese: Dell EMC Unity VMware Datastore v2
- Portuguese: Repositório de dados VMware Dell EMC Unity v2
- Russian: Хранилище данных VMware Dell EMC Unity v2
- Simplified Chinese: Dell EMC Unity VMware 数据存储 v2
- Spanish: Dell EMC Unity almacén de datos VMware v2

## Remarks

Consider the following [remarks](#) <sup>848</sup> and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for Dell EMC.
Unity OE 5.x	This sensor only supports systems from the Dell EMC Unity family with <a href="#">Unity OE 5.x</a> .
REST API	Dell EMC systems that provide a REST API are <a href="#">EMC Unity Family</a> , <a href="#">EMC Unity All Flash</a> , <a href="#">EMC Unity Hybrid</a> , and <a href="#">EMC UnityVSA</a> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">5 minutes</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ

**Priority** ⓘ

Example Name

exampletag

✕ +

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- dellemc
- dellemcdatastore
- dellemcvmware
- emcsensor

- restsensor

For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Dell EMC Specific

**Dell EMC Specific**

VMware Datastore Name ⓘ VMFS\_01

VMware Datastore Type ⓘ VMFS version 6

Dell EMC Specific

Setting	Description
VMware Datastore Name	The name of the VMware datastore that this sensor monitors.
VMware Datastore Type	The type of the VMware datastore that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>

Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).



## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Size	The free size
Free Size %	<p>The free size (%)</p> <p><b>i</b> This channel is the primary channel by default.</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: 10%</li> <li>▪ Lower warning limit: 25%</li> </ul>
Host Count	The number of hosts
Total Size	The total size
Virtual Drive Count	The number of virtual drives
Virtual Machine Count	The number of virtual machines

## More

### ■ KNOWLEDGE BASE

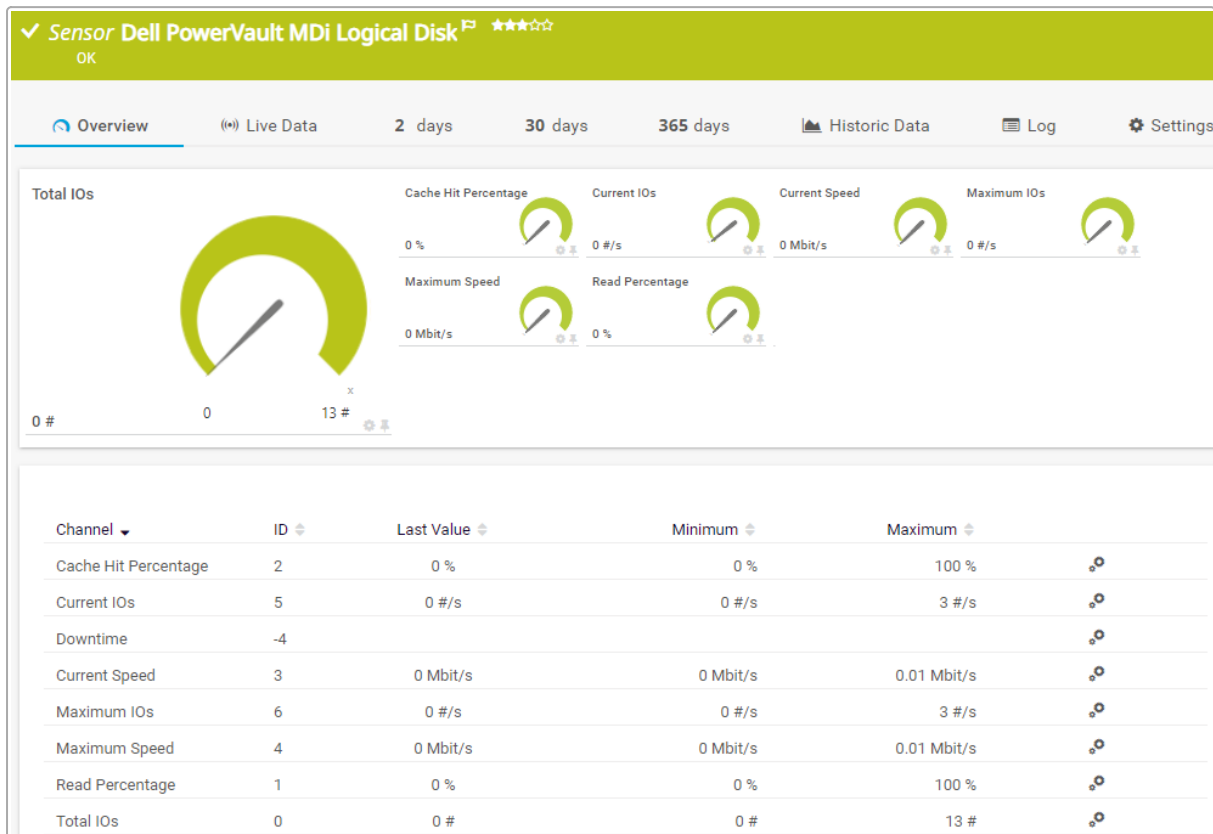
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.30 Dell PowerVault MDi Logical Disk Sensor

The Dell PowerVault MDi Logical Disk sensor monitors a virtual disk on a Dell PowerVault system.

- i** This sensor supports Dell PowerVault [MD3000i](#), [MD3420](#), [MD3620i](#), [MD3000f](#), [MD3620f](#), or [MD3820i](#), and might support other models.



Dell PowerVault MDi Logical Disk Sensor




- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Dell PowerVault MDi Logische Schijf
- French: Dell PowerVault MDi disque logique
- German: Dell PowerVault MDi Logischer Datenträger
- Japanese: Dell PowerVault MDi 論理ディスク
- Portuguese: Disco lógico Dell PowerVault MDi
- Russian: Логический диск Dell PowerVault MDi
- Simplified Chinese: Dell PowerVault MDi 逻辑磁盘
- Spanish: Disco lógico Dell PowerVault MDi

## Remarks

Consider the following [remarks](#) <sup>853</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Dell Modular Disk Storage Manager	<p>This sensor requires <a href="#">Dell Modular Disk Storage Manager</a> on the probe system. You must install it on the probe system (on every cluster node, if on a cluster probe). For details about setup, see section More below.</p> <p> Create this sensor on a device that has the IP address of the SAN configured in the IP Address/DNS Name field of the sensor settings.</p> <p> For more information, see the Knowledge Base: <a href="#">Where do I find the Dell PowerVault Modular Disk Storage Manager for use with my MDi SAN?</a></p>
IP address	This sensor requires the IP address of the storage area network (SAN) in the settings of the parent device.
Dell PowerVault models	This sensor supports <a href="#">Dell PowerVault MD3000i</a> , <a href="#">MD3420</a> , <a href="#">MD3620i</a> , <a href="#">MD3000f</a> , <a href="#">MD3620f</a> , or <a href="#">MD3820i</a> , and might support other models.
IPv4	This sensor only supports IPv4.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- powervault

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Settings

**Sensor Settings**

Important: The Dell Modular Disk Storage Manager needs to be installed on the probe system.

Virtual Disk ⓘ

Result Handling ⓘ  Discard result (default)  
 Store result

Sensor Settings

Setting	Description
Virtual Disk	The name of the virtual disk that this sensor monitors.
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display


**Sensor Display**

Primary Channel ⓘ


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>

Setting	Description
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Cache Hit Percentage	The cache hits (%)
Current IOs	The number of current I/O operations
Current Speed	The current disk speed
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Maximum IOs	The maximum number of I/O operations
Maximum Speed	The maximum disk speed
Read Percentage	The read operations (%)
Total IOs	The total number of I/O operations  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

Where do I find the Dell PowerVault Modular Disk Storage Manager for use with my MDi SAN?

- <https://kb.paessler.com/en/topic/38743>

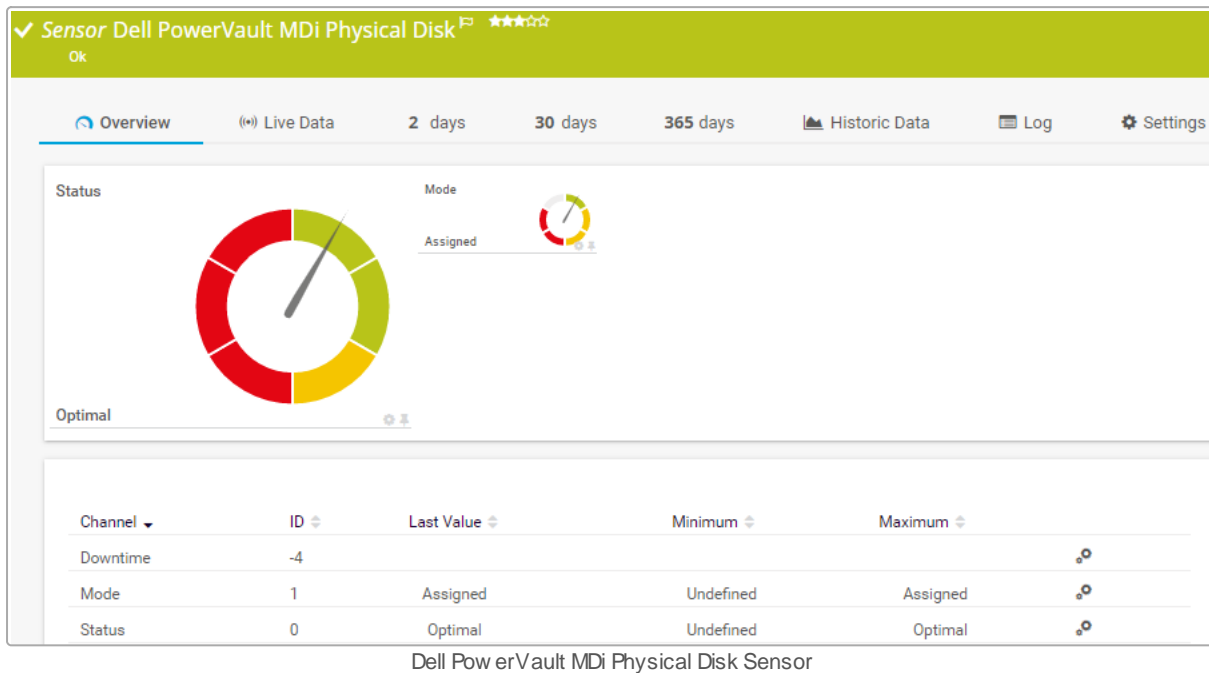
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.31 Dell PowerVault MDi Physical Disk Sensor

The Dell PowerVault MDi Physical Disk sensor monitors a physical disk on a Dell PowerVault system.

- i** This sensor supports Dell PowerVault [MD3000i](#), [MD3420](#), [MD3620i](#), [MD3000f](#), [MD3620f](#), or [MD3820i](#), and might support other models.





- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[860]</sup>.

### Sensor in Other Languages

- Dutch: Dell PowerVault MDi Fysieke Schijf
- French: Dell PowerVault MDi disque physique
- German: Dell PowerVault MDi Physikalischer Datenträger
- Japanese: Dell PowerVault MDi 物理ディスク
- Portuguese: Disco físico Dell PowerVault MDi
- Russian: Физический диск Dell PowerVault MDi
- Simplified Chinese: Dell PowerVault MDi 物理磁盘
- Spanish: Disco físico Dell PowerVault MDi

### Remarks

Consider the following [remarks](#)<sup>[857]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Dell Modular Disk Storage Manager	This sensor requires <a href="#">Dell Modular Disk Storage Manager</a> on the probe system. You must install it on the probe system (on every cluster node, if on a cluster probe). For details about setup, see section More below.   Create this sensor on a device that has the IP address of the SAN configured in the IP Address/DNS Name field of the sensor settings.
IP address	This sensor requires the IP address of the storage area network (SAN) in the settings of the parent device.
Dell PowerVault models	This sensor supports <a href="#">Dell PowerVault MD3000i</a> , <a href="#">MD3420</a> , <a href="#">MD3620i</a> , <a href="#">MD3000f</a> , <a href="#">MD3620f</a> , or <a href="#">MD3820i</a> , and might support other models.
Multiple drawers	This sensor only supports devices with one drawer of hard-drives. Multiple drawers are not supported and prevent sensor creation.
IPv6	This sensor supports IPv6.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- powervault



■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Settings

**Sensor Settings**

Important: The Dell Modular Disk Storage Manager needs to be installed on the probe system.

Physical Disk ⓘ Disk1

Result Handling ⓘ  Discard result (default)  
 Store result

Sensor Settings

Setting	Description
Physical Disk	The physical disk that this sensor monitors.
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>

Setting	Description
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

This sensor shows the status and mode of the physical disk in the channels as reported in the [Modular Disk Storage Manager](#). Status and mode combined indicate the particular status of a redundant array of independent disks (RAID) controller physical disk. The table below provides you with the status description according to the Dell documentation:

Status Channel	Mode Channel	Description
Up status: Optimal	Unassigned	The physical disk in the indicated slot is unused and available to be configured
	Assigned	The physical disk in the indicated slot is configured as part of a disk group

Status Channel	Mode Channel	Description
	Hot Spare Standby	The physical disk in the indicated slot is configured as a hot spare
	Hot Spare In Use	The physical disk in the indicated slot is in use as a hot spare within a disk group
Down status: Failed	<ul style="list-style-type: none"> <li>▪ Assigned</li> <li>▪ Unassigned</li> <li>▪ Hot Spare In Use</li> <li>▪ Hot Spare Standby</li> </ul>	The physical disk in the indicated slot has failed because of an unrecoverable error, an incorrect drive type or drive size, or by its operational state being set to failed
Up status: Replaced	Assigned	The physical disk in the indicated slot has been replaced and is ready to be, or is actively being, configured into a disk group
Down status: Pending Failure	<ul style="list-style-type: none"> <li>▪ Assigned</li> <li>▪ Unassigned</li> <li>▪ Hot Spare In Use</li> <li>▪ Hot Spare Standby</li> </ul>	A S.M.A.R.T. error has been detected on the physical disk in the indicated slot
Warning status: None	None	The indicated slot is empty, or the array cannot detect the physical disk
Down status: Undefined		

## More

### ■ KNOWLEDGE BASE

Where do I find the Dell PowerVault Modular Disk Storage Manager for use with my MDi SAN?

- <https://kb.paessler.com/en/topic/38743>

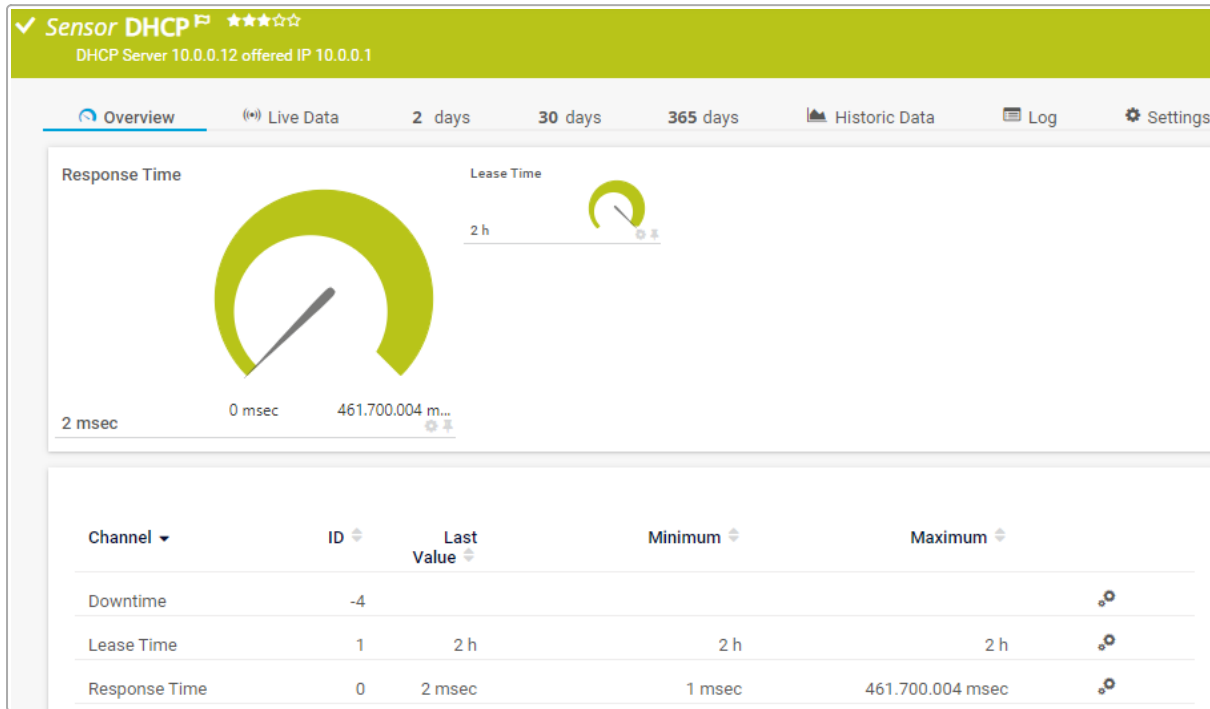
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.32 DHCP Sensor

The DHCP sensor monitors a Dynamic Host Configuration Protocol (DHCP) server. It sends a broadcast message to the network and waits for a DHCP server to respond.

**i** This sensor shows the address of the server and the offered IP address in the sensor message. You can check the server's response via [regular expressions](#).



DHCP Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: DHCP
- French: DHCP
- German: DHCP
- Japanese: DHCP
- Portuguese: DHCP
- Russian: DHCP
- Simplified Chinese: DHCP
- Spanish: DHCP

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Sensor creation	You can create this sensor only on a <a href="#">probe device</a> .
Static IP address	The probe device where you create this sensor must have a static IP address. It cannot get its IP address from DHCP because this can cause a DHCP failure that results in a severe issue for the probe device so that you risk losing monitoring data.
IPv4	This sensor only supports IPv4.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
DHCP unavailable	This sensor shows a timeout error if no DHCP is available, or if you use more than two DHCP sensors per device.
Link-local address	Adding this sensor on a link-local address is valid and is not prohibited. However, as this is a local IP address, the sensor does not receive any data and shows a timeout error.
Add Sensor dialog	Choose the network card on the probe system that is used to send the broadcast message in the Add Sensor dialog.
Knowledge Base	Knowledge Base: <a href="#">How can I monitor a DHCP server in a specific network if there are several DHCP networks?</a>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- dhcpsensor

For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## DHCP Specific

**DHCP Specific**

MAC Address ⓘ

Client IP Address ⓘ  Do not check the IP address using a regular expression  
 Check the IP address using a regular expression


Server IP Address ⓘ  Do not check the IP address using a regular expression  
 Check the IP address using a regular expression

Timeout (Sec.) ⓘ 10

If Server Changes ⓘ  Ignore (default)  
 Write log entry

If IP Address Changes ⓘ  Ignore (default)  
 Write log entry

DHCP Specific

Setting	Description
MAC Address	The MAC address of the network adapter that sends the broadcast message to the network.
Client IP Address	Specify if you want to check the returned client IP address with a regular expression (regex): <ul style="list-style-type: none"> <li>Do not check the IP address using a regular expression: The IP address only appears in the sensor message without further processing.</li> <li>Check the IP address using a regular expression: Enter the regex that you want to use below.</li> </ul>
Client IP Address Must Include (Down Status if Not Included)	<p><b>This setting is only visible if you select</b> Check the IP address using a regular expression <a href="#">above</a>.</p> <p>In the response of the DHCP server, search by using a regex. If the response for the client IP address <b>does not contain</b> this string, the sensor shows the Down <a href="#">status</a>.</p> <p> For example, enter <code>10\.\0\.\5\.\.*</code> to make sure that any answering DHCP server returns any client IP address starting with <code>10.0.5.</code> If it does not, the sensor shows the Down status. Leave this field empty if you do not want to use it.</p>

Setting	Description
	<p><b>i</b> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</p>
Client IP Address Must Not Include (Down Status if Included)	<p><b>This setting is only visible if you select</b> Check the IP address using a regular expression <a href="#">above</a>.</p> <p>In the response of the DHCP server, search by using a regex. If the response for the client IP address <b>contains</b> this string, this sensor shows the Down status. See the example above. Leave this field empty if you do not want to use it.</p> <p><b>i</b> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</p>
Server IP Address	<p>Specify if you want to check the returned server IP address with a regex:</p> <ul style="list-style-type: none"> <li>▪ Do not check the IP address using a regular expression: The IP address only appears in the sensor message without further processing.</li> <li>▪ Check the IP address using a regular expression: Enter the regex that you want to use below.</li> </ul>
Server IP Address Must Include (Down Status if Not Included)	<p><b>This setting is only visible if you select</b> Check the IP address using a regular expression <a href="#">above</a>.</p> <p>In the response of the DHCP server, search by using a regex. If the response for the server IP address <b>does not contain</b> this string, this sensor shows the Down status. See the example above. Leave this field empty if you do not want to use it.</p> <p><b>i</b> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</p>
Server IP Address Must Not Include (Down Status if Included)	<p><b>This setting is only visible if you select</b> Check the IP address using a regular expression <a href="#">above</a>.</p> <p>In the response of the DHCP server, search by using a regex. If the response for the server IP address <b>contains</b> this string, this sensor shows the Down status. See the example above. Leave this field empty if you do not want to use it.</p> <p><b>i</b> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p>

Setting	Description
	<p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
If Server Changes	<p>If there is more than one DHCP server in the network that can respond to the broadcast message, the sensor can receive a response from a different DHCP server compared to the last scan of the sensor. In this case, PRTG can write an entry to the system <a href="#">logs</a>. Define what PRTG does if DHCP servers change:</p> <ul style="list-style-type: none"> <li>Ignore (default): Do nothing.</li> <li>Write log entry: Write an entry to the system logs whenever the DHCP server changes between two sensor scans.</li> </ul> <p><b>i</b> Regardless of this setting, entries are always added to the <a href="#">sensor log</a>.</p>
If IP Address Changes	<p>If the IP address offered by the DHCP server changes between two sensor scans, PRTG can write an entry to the system logs. Define what PRTG does if IP addresses change:</p> <ul style="list-style-type: none"> <li>Ignore (default): Do nothing.</li> <li>Write log entry: Write an entry to the system logs whenever the DHCP server offers a different IP address compared to the last sensor scan.</li> </ul> <p><b>i</b> Regardless of this setting, entries are always added to the <a href="#">sensor log</a>.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i**    Downtime

---

Graph Type **i**     Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⚙</b> below a channel gauge on the sensor's Overview tab.</p>



Setting	Description
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Lease Time	The lease time reported by the server
Response Time	<p>The response time</p> <p><b>i</b> This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

How can I monitor a DHCP server in a specific network if there are several DHCP networks?

- <https://kb.paessler.com/en/topic/64601>

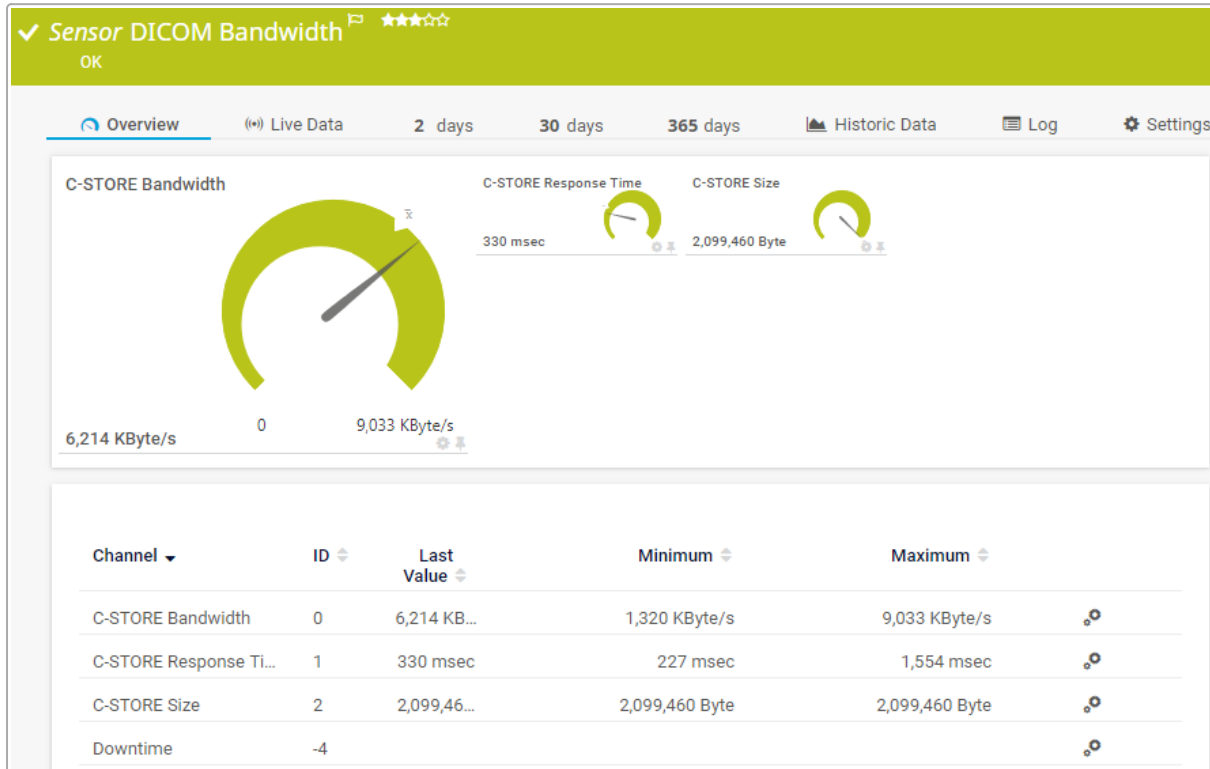
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

### 7.8.33 DICOM Bandwidth Sensor

The DICOM Bandwidth sensor monitors the bandwidth usage of a C-STORE request to a Digital Imaging and Communications in Medicine (DICOM) capable device. It sends one or more DICOM images and files that you have stored in a folder on a local disk or share and checks if the DICOM device can handle the C-STORE request.

**i** You can use this sensor to test your picture archiving and communication system (PACS), for example.



DICOM Bandwidth Sensor



■ For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>873</sup>.

#### Sensor in Other Languages

- Dutch: DICOM Bandbreedte
- French: Bande passante (DICOM)
- German: DICOM-Bandbreite
- Japanese: DICOM 帯域幅
- Portuguese: Largura de banda DICOM
- Russian: Пропускная способность DICOM
- Simplified Chinese: DICOM 带宽
- Spanish: Ancho de banda DICOM

## Remarks

Consider the following [remarks](#) <sup>870</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
IPv6	This sensor supports IPv6.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- bandwidth
- dicom

 For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## DICOM Connection

### DICOM Connection

Calling Application Entity Title ⓘ	PRTG
Called Application Entity Title ⓘ	ABC
Port ⓘ	104
Timeout (Sec.) ⓘ	60

DICOM Connection



Setting	Description
Calling Application Entity Title	Enter the Application Entity Title (AET) of PRTG to initialize a DICOM connection. ⓘ The AET is case-sensitive and does not support special characters.
Called Application Entity Title	Enter the AET of the target system to initialize a DICOM connection. ⓘ The AET is case-sensitive and does not support special characters.
Port	Enter the port of the DICOM interface to use for the connection. The default port is 104.
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is 900 seconds (15 minutes). ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.

## Bandwidth Settings

### Bandwidth Settings

File Path ⓘ	C:\DICOM
-------------	----------

Bandwidth Settings



Setting	Description
File Path	<p>Enter the full path to the folder where you have stored your DICOM files and images (ending with <code>.dcm</code>). This sensor sends all files to the DICOM enabled device via a C-STORE request to measure bandwidth. You can use any folder on a disk or share that the probe system has access to.</p> <p> For example, enter <code>C:\DICOM</code> to send files that are stored in a folder named <code>DICOM</code> on the probe system.</p> <p> The path must contain <code>*.dcm</code> files. Enter the path without a backslash (<code>\</code>) at the end.</p>

## Debug Options

**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the <code>\Logs\sensors</code> subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are <code>Result of Sensor [ID].txt</code>, <code>Result of Sensor [ID].Data.txt</code>, and <code>Result of Sensor [ID].log</code>. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display


**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
C-STORE Bandwidth	<p>The bandwidth usage of the sent files</p> <p><b>i</b> This channel is the primary channel by default.</p>

Channel	Description
C-STORE Response Time	The response time of the C-STORE request
C-STORE Size	The total size of the sent files
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

## More

### KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

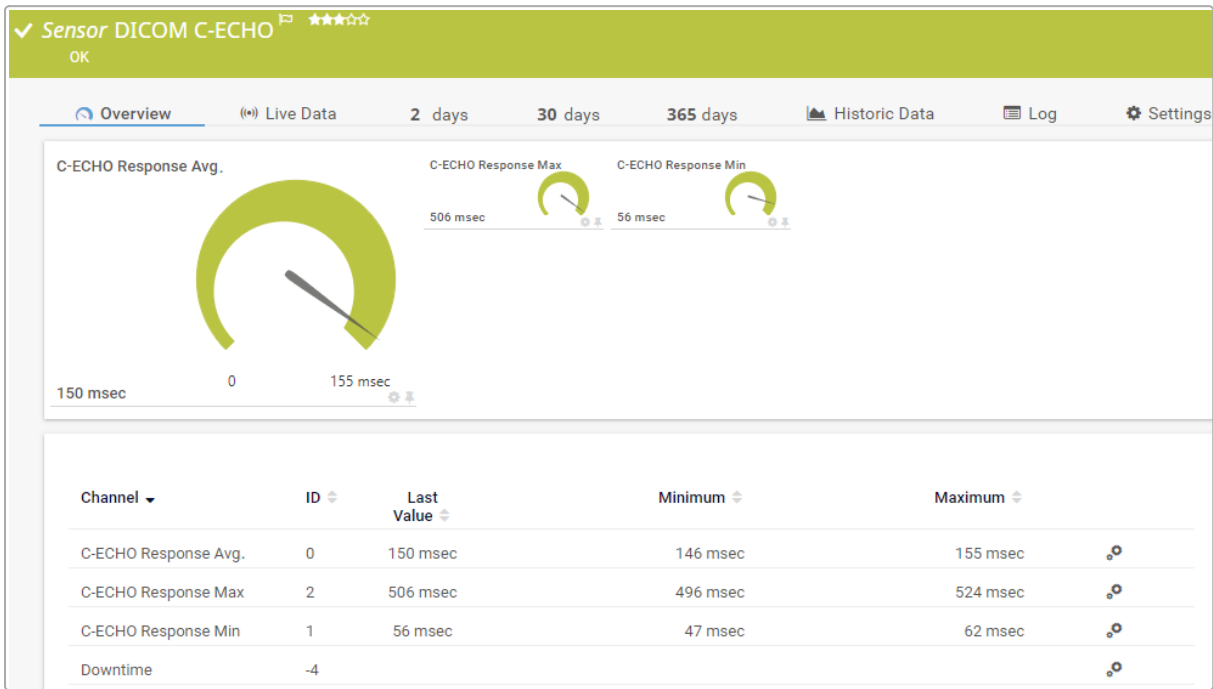
- <https://kb.paessler.com/en/topic/61108>



### 7.8.34 DICOM C-ECHO Sensor

The DICOM C-ECHO sensor monitors the availability of Digital Imaging and Communications in Medicine (DICOM) capable systems and devices by sending C-ECHO requests to the target system. C-ECHO is also known as DICOM-Ping.

- ❶ You can use this sensor to verify that the DICOM handshake is executed and that your target system is capable of answering DICOM messages.



DICOM C-ECHO Sensor



- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[879]</sup>.

#### Sensor in Other Languages

- Dutch: DICOM C-ECHO
- French: C-ECHO (DICOM)
- German: DICOM-C-ECHO
- Japanese: DICOM C-ECHO
- Portuguese: C-ECHO DICOM
- Russian: DICOM C-ECHO
- Simplified Chinese: DICOM C-ECHO
- Spanish: C-ECHO DICOM

#### Remarks

Consider the following [remarks](#)<sup>[875]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
IPv6	This sensor supports IPv6.

### Basic Sensor Settings

#### Basic Sensor Settings

Sensor Name ⓘ

Tags ⓘ

Priority ⓘ

Example Name

---

exampletag X +

---

★★★★☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cecho
- dicom
- ping

 For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## DICOM Connection

### DICOM Connection

Calling Application Entity Title ⓘ	PRTG
Called Application Entity Title ⓘ	ABC
Port ⓘ	104
Timeout (Sec.) ⓘ	60

DICOM Connection

Setting	Description
Calling Application Entity Title	Enter the Application Entity Title (AET) of PRTG to initialize a DICOM connection. ⓘ The AET is case-sensitive and does not support special characters.
Called Application Entity Title	Enter the AET of the target system to initialize a DICOM connection. ⓘ The AET is case-sensitive and does not support special characters.
Port	Enter the port of the DICOM interface to use for the connection. The default port is <b>104</b> .
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes). ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.

## C-ECHO Settings

### C-ECHO Settings

C-ECHO Count ⓘ	5
Ping Delay (ms) ⓘ	10

C-ECHO Settings

Setting	Description
C-ECHO Count	Enter the number of C-ECHO requests that the sensor sends in a row for one scanning interval. Enter an integer. The default value is <b>5</b> .
Ping Delay (ms)	Enter the time in milliseconds (ms) the sensor waits between two C-ECHO requests. Enter an integer. The default value is <b>10</b> .  <i>i</i> Make sure that the C-ECHO count multiplied by the delay does not exceed the scanning interval of the sensor.

### Debug Options

**Debug Options**

Result Handling *i*

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><i>☁</i> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><i>i</i> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### Sensor Display

**Sensor Display**


Primary Channel *i*    Downtime

---


Graph Type *i*


Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
C-ECHO Response Avg.	<p>The average response time of the C-ECHO request</p> <p><b>i</b> This channel is the primary channel by default.</p>

Channel	Description
C-ECHO Response Max	The maximum response time of the C-ECHO request
C-ECHO Response Min	The minimum response time of the C-ECHO request
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

## More

### KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

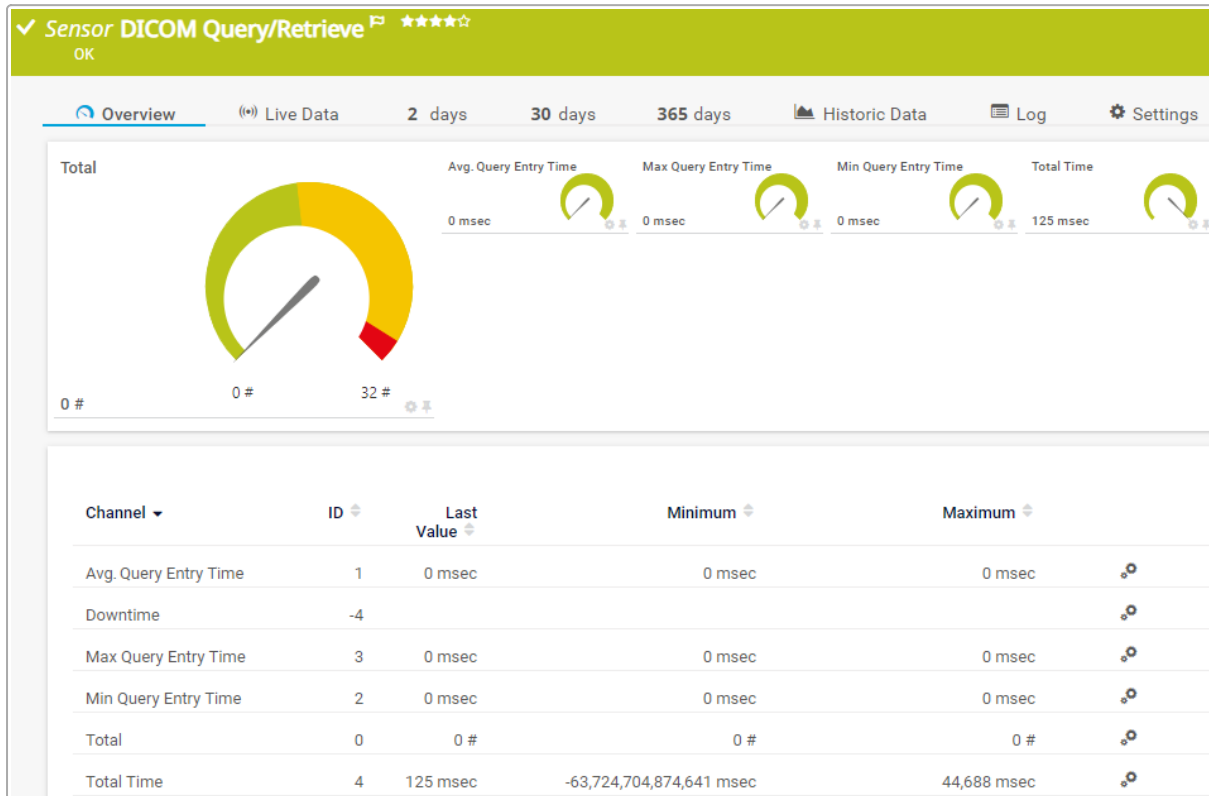
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.35 DICOM Query/Retrieve Sensor

The DICOM Query/Retrieve sensor monitors the C-FIND capability of Digital Imaging and Communications in Medicine (DICOM) capable systems and devices. It sends a C-FIND request or Modality Worklist (MWL) query to the target device and counts all found items.

**i** You can specify search levels to only count specific items.



DICOM Query/Retrieve Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: DICOM Query/Retrieve
- French: Requête/récupération (DICOM)
- German: DICOM-Abfrage
- Japanese: DICOM クエリ/取得
- Portuguese: Consulta/recuperação DICOM
- Russian: Запрос/получение DICOM
- Simplified Chinese: DICOM 查询/检索
- Spanish: Consulta/Recuperación DICOM

## Remarks

Consider the following [remarks](#)<sup>[882]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
.NET 4.7.2 or later	This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.  <span style="color: red;">i</span> If the framework is missing, you cannot create this sensor.  <span style="color: blue;">■</span> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a>
IPv6	This sensor supports IPv6.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag x +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- dicom
- query
- retrieve

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.



### DICOM Connection

#### DICOM Connection

Calling Application Entity Title ⓘ	PRTG
Called Application Entity Title ⓘ	ABC
Port ⓘ	104
Timeout (Sec.) ⓘ	60

DICOM Connection

Setting	Description
Calling Application Entity Title	Enter the Application Entity Title (AET) of PRTG to initialize a DICOM connection. ⓘ The AET is case-sensitive and does not support special characters.
Called Application Entity Title	Enter the AET of the target system to initialize a DICOM connection. ⓘ The AET is case-sensitive and does not support special characters.
Port	Enter the port of the DICOM interface to use for the connection. The default port is 104.
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is 900 seconds (15 minutes). ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.

### Query/Retrieve Settings

#### Query/Retrieve Settings

C-FIND Level ⓘ	<input checked="" type="radio"/> Patient <input type="radio"/> Study <input type="radio"/> Series <input type="radio"/> Worklist
Search Key ⓘ	*

Query/Retrieve Settings

Setting	Description
C-FIND Level	<p>Define the search level of the C-FIND request:</p> <ul style="list-style-type: none"> <li>▪ Patient: Retrieve data from the patient column via C-FIND. Enter a search key below.</li> <li>▪ Study: Retrieve data from the study column via C-FIND. Enter a search key and a modality below.</li> <li>▪ Series: Retrieve data from the series column via C-FIND. Enter a search key and a modality below.</li> <li>▪ Worklist: Use an MWL query to retrieve data from the worklist. Enter a filter field, a filter string, and a channel field below.</li> </ul>
Search Key	<p><b>This setting is only visible if you select Patient, Study, or Series above.</b></p> <p>Enter a key that you want to search for, for example, an instance Unique Identifier (UID), series UID, patient UID, or enter an asterisk (*) to search for all items. Enter a string.</p>
Modality	<p><b>This setting is only visible if select Study or Series above.</b></p> <p>Enter a modality in short form that you want to search for, for example, CT, MRI, US, or enter an asterisk (*) to search for all modalities. Enter a string.</p>
Filter Field	<p><b>This setting is only visible if you select Worklist above.</b></p> <p>Define a field of the worklist that you want to filter for:</p> <ul style="list-style-type: none"> <li>▪ Station AET</li> <li>▪ Station Name</li> <li>▪ Modality</li> </ul>
Filter String	<p><b>This setting is only visible if you select Worklist above.</b></p> <p>Enter a string that you want to filter for, for example, a station name, station AET, modality, or an asterisk (*) to filter for all items.</p>
Channel Naming	<p><b>This setting is only visible if you select Worklist above.</b></p> <p>Define which field you want to use to name the channels:</p> <ul style="list-style-type: none"> <li>▪ Station AET</li> <li>▪ Station Name</li> <li>▪ Modality</li> </ul>

## Debug Options

**Debug Options**

**Result Handling** ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**


**Primary Channel** ⓘ Downtime

---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>


Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.


 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Avg. Query Entry Time	The average query entry time
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Max Query Entry Time	The maximum query entry time
Min Query Entry Time	The minimum query entry time
Total	<p>The total number of items found</p> <p> This channel is the primary channel by default.</p>

Channel	Description
Total Time	The total time of the C-FIND request or MWL query

 This sensor also adds channels for the number of items in each field it finds.

## More

### KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

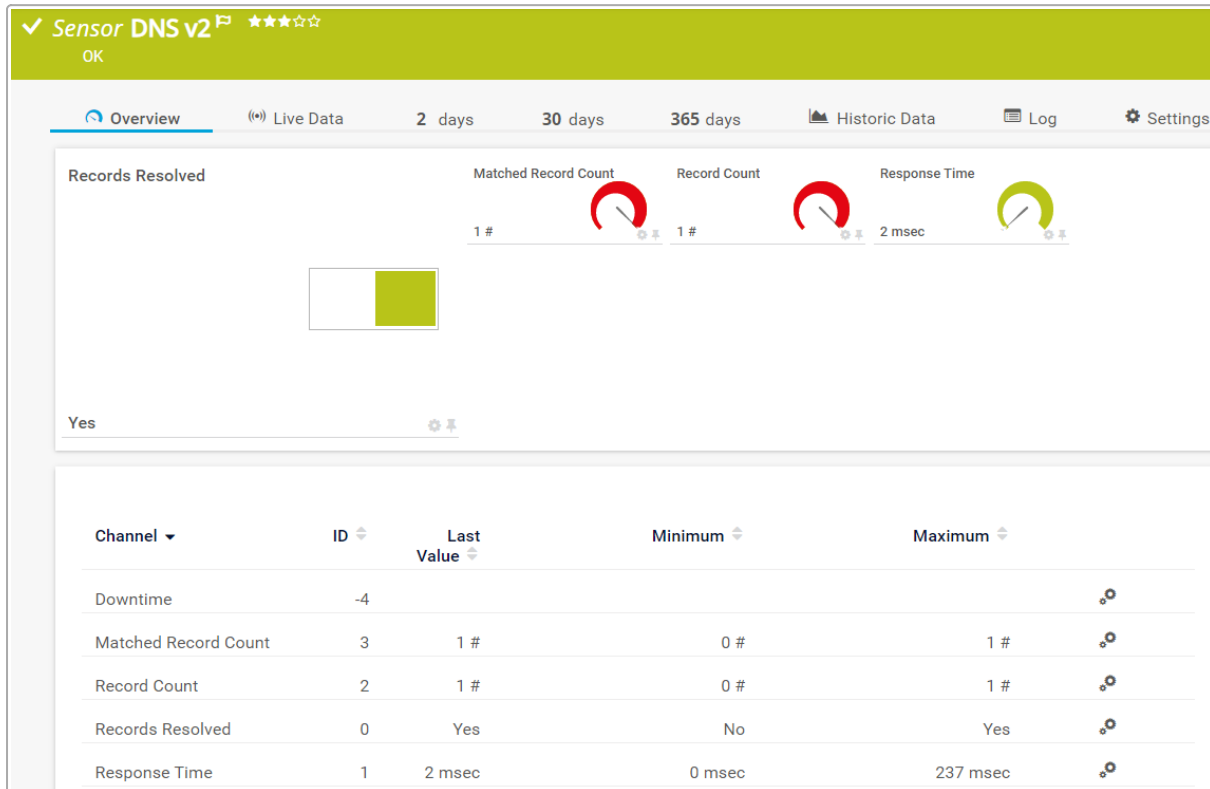
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

### 7.8.36 DNS v2 Sensor

The DNS v2 sensor monitors a Domain Name System (DNS) server, resolves domain name records, and compares them to a filter.

**i** This sensor can show the Down status if the DNS server does not correctly resolve a specified domain name



DNS v2 Sensor

**■** For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

#### Sensor in Other Languages

- Dutch: DNS v2
- French: DNS v2
- German: DNS v2
- Japanese: DNS v2
- Portuguese: DNS v2
- Russian: DNS v2
- Simplified Chinese: DNS v2
- Spanish: DNS v2

## Remarks

Consider the following [remarks](#) <sup>689</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- dns
- dnssensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## DNS Sensor Specific

### DNS Sensor Specific

**Domain Name** ⓘ

**Query Type** ⓘ

- Host address IPv4 (A) (default)
- Host address IPv6 (AAAA)
- Canonical name for an alias (CNAME)
- Mail exchange (MX)
- Naming authority pointer (NAPTR)
- Authoritative name server (NS)
- PTR resource record (PTR)
- Start of authority (SOA)
- Text resource record (TXT)
- Any (depends on the DNS server configuration)

**Timeout (Sec.)** ⓘ

**Filter Usage** ⓘ

- Do not use a filter (default)
- Use a filter

**Port** ⓘ

DNS Sensor Specific

Setting	Description
Domain Name	<p>Enter the DNS name to resolve.</p> <p> ⓘ If you use the query type PTR resource record (PTR), enter a proper reverse DNS representation of the IP address. For example, <a href="#">1.0.0.127.in-addr.arpa</a>.</p>
Query Type	<p>Select the query type that the sensor sends to the DNS server:</p> <ul style="list-style-type: none"> <li>▪ Host address IPv4 (A) (default)</li> <li>▪ Host address IPv6 (AAAA)</li> <li>▪ Canonical name for an alias (CNAME)</li> <li>▪ Mail exchange (MX)</li> <li>▪ Naming authority pointer (NAPTR)</li> <li>▪ Authoritative name server (NS)</li> <li>▪ PTR resource record (PTR)</li> <li>▪ Start of authority (SOA)</li> <li>▪ Text resource record (TXT)</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>Any (depends on the DNS server configuration)</li> </ul>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p> <p><b>i</b> The timeout value must be shorter than the scanning interval of the sensor.</p>
Filter Usage	<p>Define if the sensor checks for a specific filter value in the response:</p> <ul style="list-style-type: none"> <li>Do not use a filter (default): Do not check the response.</li> <li>Use a filter: Use a filter to check the response. Define the filter value below.</li> </ul>
Filter Value	<p><b>This setting is only visible if you select Use a filter above.</b></p> <p>Enter one or more filter values. For an A record, the filter value can be an IP address like <b>127.0.0.1</b>, for example. The filter value can also contain a wildcard (*) to match any content, for example <b>127.*.1</b>. You can specify multiple filter values by using a comma as separator, for example <b>172.217.*.1,172.217.*.2</b>.</p>
Port	<p>Enter the number of the port to which this sensor connects. This must be the port on which the parent device answers queries. The default port is <b>53</b>.</p> <p><b>i</b> We recommend that you use the default value.</p> <p><b>i</b> This sensor connects to the IP address or the DNS name of the <a href="#">parent device</a>.</p>

## Sensor Display

**Sensor Display**




Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)


Stack channels on top of each other

Sensor Display


Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><a href="#">This setting is only visible if you select</a> Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**


**Result Handling** 
 Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Matched Record Count	The number of matched records (if you use a filter)
Record Count	The number of records
Records Resolved	<p>If records were resolved</p> <ul style="list-style-type: none"> <li>▪ Up status: Yes</li> <li>▪ Down status: No</li> </ul>
Response Time	<p>The response time</p> <p><b>i</b> This channel is the primary channel by default.</p>

## More

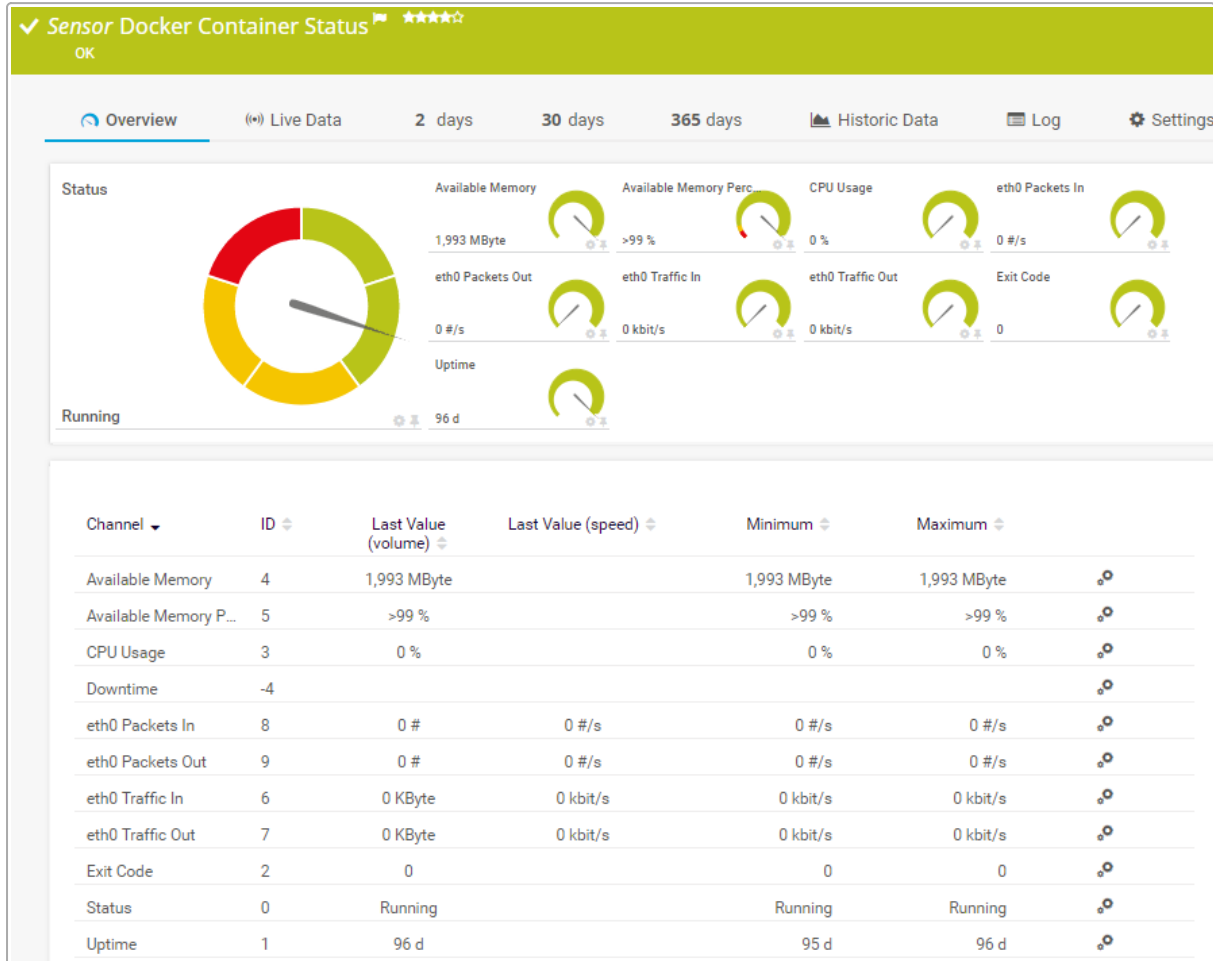
### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.37 Docker Container Status Sensor

The Docker Container Status sensor monitors the status of a Docker container.



Docker Container Status Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Docker Container Status
- French: Statut de conteneur Docker
- German: Docker-Container-Zustand
- Japanese: Docker コンテナの状態
- Portuguese: Status do contêiner Docker
- Russian: Статус контейнера Docker
- Simplified Chinese: Docker 容器状态
- Spanish: Estado de contenedor Docker.

## Remarks

Consider the following [remarks](#)<sup>895</sup> and requirements for this sensor:

Remark	Description
Certificate and private key	This sensor requires certificates and private keys to monitor Docker.  For more information on how to create a Docker certificate, see the Knowledge Base: <a href="#">How can I create private key and certificate for the Docker sensor?</a>
Parent device	This sensor requires that the parent device is the Docker machine on which the container that you want to monitor runs.
Authentication	This sensor requires an authentication with a certificate and a private key before you can add it. Provide the Port (usually <b>2376</b> ), Private Key, and Certificate and click OK.
IPv4	This sensor only supports IPv4.
Performance impact	This sensor has a <b>low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  X +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- docker
- dockercontainer

 For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Docker Credentials

**Docker Credentials**

Port ⓘ 2376

---

Private Key ⓘ

---

Certificate ⓘ

Docker Credentials

Setting	Description
Port	Enter the number of the port to which this sensor connects. The default port on which Docker over Transport Layer Security (TLS) runs is <a href="#">2376</a> .
Private Key	<p>Provide the private key for the connection to Docker. If you have already created a key, you can use it here. Otherwise, create a key on Docker first.</p> <p>Open the key with a text editor, copy everything that the file includes, and paste it here. Usually, the key starts with <code>-----BEGIN RSA PRIVATE KEY-----</code> and ends with <code>-----END RSA PRIVATE KEY-----</code></p> <p>■ For more information on how to create a Docker certificate, see the Knowledge Base: <a href="#">How can I create private key and certificate for the Docker sensor?</a></p>
Certificate	<p>Provide the certificate for the connection to Docker. If you have already created a certificate, you can use it here. Otherwise, create a certificate on Docker first.</p> <p>Open the certificate with a text editor, copy everything that the file includes, and paste it here. Usually, the certificate starts with <code>-----BEGIN CERTIFICATE-----</code> and ends with <code>-----END CERTIFICATE-----</code></p> <p>■ For more information on how to create a Docker certificate, see the Knowledge Base: <a href="#">How can I create private key and certificate for the Docker sensor?</a></p>

## Docker Specific

**Docker Specific**

Container ID ⓘ //1111aaaa-22bb-cc33-dd44-555555eeeeeee

Container Name ⓘ Example

Image ⓘ sath89/oracle-12c

Container Identification ⓘ  By container ID (default)  
 By container name

Result Handling ⓘ  Discard result  
 Store result

Docker Specific

Setting	Description
Container ID	The ID of the Docker container that this sensor monitors.
Container Name	The name of the Docker container that this sensor monitors.
Image	The name of the image that was used to create the Docker container that this sensor monitors.
Container Identification	<p>Define how the sensor identifies the Docker container that it monitors:</p> <ul style="list-style-type: none"> <li>▪ By container ID (default): Use the ID of the Docker container for identification.</li> <li>▪ By container name: Use the name of the Docker container for identification.</li> </ul> <p> ⓘ Use this option if the IDs of your Docker containers regularly change, for example, because of nightly deployments of your Docker containers.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].Data.txt, Result of Sensor [ID]_1.json, and Result of Sensor [ID]_2.json. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.



Channel	Description
Available Memory	The available memory
Available Memory %	<p>The available memory (%)</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: 5%</li> <li>▪ Lower warning limit: 10%</li> </ul>
CPU Usage	The CPU usage
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Eth0 Packets In	The number of ingoing packets
Eth0 Packets Out	The number of outgoing packets
Eth0 Traffic In	The incoming traffic
Eth0 Traffic Out	The outgoing traffic
Exit Code	The exit code
Status	<p>The overall status</p> <ul style="list-style-type: none"> <li>▪ Up status: Create, Running</li> <li>▪ Warning status: Paused, Restarting</li> <li>▪ Down status: Exited</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Uptime	The uptime

## More

### ■ KNOWLEDGE BASE

How can I create private key and certificate for the Docker sensor?

- <https://kb.paessler.com/en/topic/67250>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

### 7.8.38 Enterprise Virtual Array Sensor

The Enterprise Virtual Array sensor monitors an HPE Storage Enterprise Virtual Array (EVA) via the [sssu.exe](#) from [HPE P6000 Command View Software](#) (previously known as HP Command View EVA Software).

■ For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>903</sup>.

#### Sensor in Other Languages

- Dutch: Enterprise Virtual Array
- French: Enterprise Virtual Array
- German: Enterprise Virtual Array
- Japanese: Enterprise Virtual Array
- Portuguese: Enterprise Virtual Array
- Russian: Enterprise Virtual Array
- Simplified Chinese: Enterprise Virtual Array
- Spanish: Enterprise Virtual Array

#### Remarks

Consider the following [remarks](#)<sup>900</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
HPE P6000 Command View Software	This sensor requires the <a href="#">HPE P6000 Command View Software</a> on the probe system, or the alternative described in the Knowledge Base: <a href="#">Do I really have to install the whole Command View on the probe to use the EVA sensor?</a>
Credentials	This sensor requires that you explicitly specify the credentials for the EVA in the sensor settings.
IPv6	This sensor supports IPv6.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Add Sensor

Setting	Description
Scanning Mode	<p>Specify the depth of the meta-scan:</p> <ul style="list-style-type: none"> <li>▪ Basic mode: We recommend that you use this scanning mode. Various modules of your EVA are available for monitoring.</li> <li>▪ Detailed mode: PRTG scans for each disk of your EVA. It lists every disk in the module selection.</li> </ul>

## Basic Sensor Settings

**Basic Sensor Settings**

Sensor Name ⓘ Example Name

Tags ⓘ  X +

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- eva

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## EVA Credentials

Setting	Description
User Name	Enter the user name for the EVA.
Password	Enter the password for the EVA.

## EVA Settings

Setting	Description
Module	The module that this sensor monitors.  <b>i</b> You can edit this setting if, for example, you rename the module or move it to a different folder. This way, PRTG can find the module again and you do not lose the monitoring history.
System	The system of the module that this sensor monitors.
Module Type	The type of the module that this sensor monitors.
Description	The description of the module that this sensor monitors.
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime


---

Graph Type **i**  Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.  <b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.

Setting	Description
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

This sensor can show the status of several HPE EVA modules:

- System controllers
- Enclosures
- Disks
- Disk groups
- Folders
- Hosts
- Snapshots
- Data replication
- Cabinets

- If the devices have measuring tools for fans and temperature, this sensor displays corresponding data as well.

For these EVA components, this sensor can show the following:

- Operational status
- Predicted failures
- Accessible media
- Allocation in percent
- Availability for VRaids in bytes
- Exaggerated bytes
- Group host access
- Number of grouped and ungrouped disks
- Age of snapshots
- License status

## More

### KNOWLEDGE BASE

Do I really have to install the whole Command View on the probe to use the EVA sensor?

- <https://kb.paessler.com/en/topic/55983>

What security features does PRTG include?

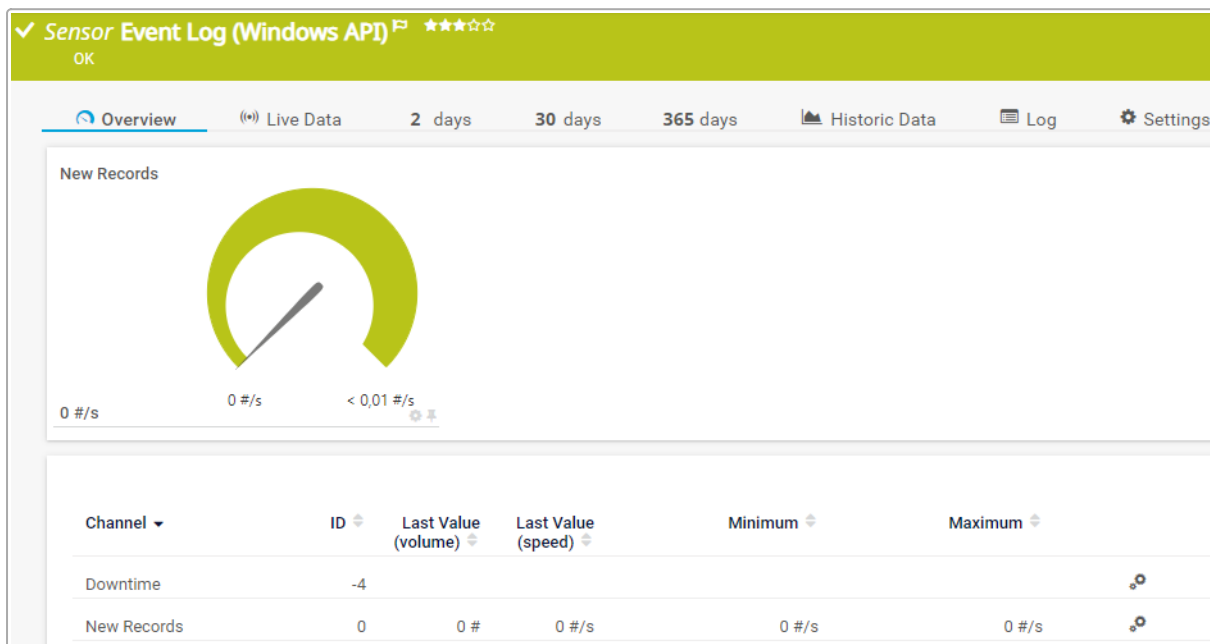
- <https://kb.paessler.com/en/topic/61108>

### 7.8.39 Event Log (Windows API) Sensor

#### Important Notice

This sensor might not work anymore after Windows updates of June 2021. For more information, see the Knowledge Base: [My Event Log \(Windows API\) sensors fail after installing Windows updates. What can I do?](#)

The Event Log (Windows API) sensor monitors event log entries via the Windows application programming interface (API).



Event Log (Windows API) Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

#### Sensor in Other Languages

- Dutch: Event Log (Windows API)
- French: Journal des événements (API Windows)
- German: Ereignisprotokoll (Windows API)
- Japanese: イベントログ (Windows API)
- Portuguese: Log de eventos (Windows API)
- Russian: Журнал событий (API Windows)
- Simplified Chinese: 事件日志 (Windows API)
- Spanish: Registro de eventos (Windows API)

## Remarks

Consider the following [remarks](#)<sup>[906]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
IPv6	This sensor supports IPv6.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">My Event Log (Windows API) sensors fail after installing Windows updates. What can I do?</a></li> <li>Knowledge Base: <a href="#">My Event Log sensor ignores changes in the event log. What can I do?</a></li> <li>Knowledge Base: <a href="#">How can I configure sensors using speed limits to keep the status for more than one interval?</a></li> </ul>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiapieventlogsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.



## Windows API Event Log Specific

### Windows API Event Log Specific

**Log File** ⓘ

- Application
- System
- Security
- Directory Service
- DNS Server
- File Replication Service

Windows API Event Log Specific

Setting	Description
Log File	<p>The Windows event log provides several log files. Specify the log file that this sensor monitors:</p> <ul style="list-style-type: none"> <li>▪ Application</li> <li>▪ System</li> <li>▪ Security</li> <li>▪ Directory Service</li> <li>▪ DNS Server</li> <li>▪ File Replication Service</li> </ul>

## Filter Event Log Entries

### Filter Event Log Entries

**Event Type** ⓘ

Any (default)

Error

Warning

Information

Security Audit Success

Security Audit Failure

**Filter by Source** ⓘ

Disable (default)

Enable

**Filter by ID** ⓘ

Disable (default)

Enable

**Filter by Category** ⓘ

Disable (default)

Enable

**Filter by User** ⓘ

Disable (default)

Enable

**Filter by Computer** ⓘ

Disable (default)

Enable




**Filter by Message** ⓘ

Disable (default)

Enable

Filter Event Log Entries

Setting	Description
Event Type	<p>Specify the type of event that this sensor processes:</p> <ul style="list-style-type: none"> <li>▪ Any</li> <li>▪ Error</li> <li>▪ Warning</li> <li>▪ Information</li> <li>▪ Security Audit Success</li> <li>▪ Security Audit Failure</li> </ul>

Setting	Description
	<p> The sensor cannot process other event types.</p>
Filter by Source	<p>Filter all received events for a certain event source:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not filter events.</li> <li>▪ Enable: Filter events. <ul style="list-style-type: none"> <li> The sensor only processes messages that match the value that you define below.</li> </ul> </li> </ul>
Filter Type	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Select the filter type:</p> <ul style="list-style-type: none"> <li>▪ Include filter: Include the specified value and disregard all other values.</li> <li>▪ Exclude filter: Exclude the specified value and regard all other values.</li> </ul>
Match String (Event Source)	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Enter an event source that you want to filter for. Depending on the kind of filter, the sensor either processes the event source (Include filter option) or it does not process it (Exclude filter option). Enter a string.</p>
Filter by ID	<p>Filter all received events for a certain event ID:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not filter events.</li> <li>▪ Enable: Filter events. <ul style="list-style-type: none"> <li> The sensor only processes messages that match the value that you define below.</li> </ul> </li> </ul>
Filter Type	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Select the filter type:</p> <ul style="list-style-type: none"> <li>▪ Include filter: Include the specified value and disregard all other values.</li> <li>▪ Exclude filter: Exclude the specified value and regard all other values.</li> </ul>
Match Values (Event ID)	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Enter an event ID that you want to filter for. Depending on the kind of filter, the sensor either processes the event ID (Include filter option) or it does not process it (Exclude filter option).</p> <p> The Event Log (Windows API) supports more than one event ID. You can enter a comma-separated list of event IDs to filter for more than one ID. For example, <a href="#">1100,4627,4747,4884,5050,6422</a>.</p>

Setting	Description
Filter by Category	<p>Filter all received events for a certain event category:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not filter events.</li> <li>▪ Enable: Filter events. <ul style="list-style-type: none"> <li>ⓘ The sensor only processes messages that match the value that you define below.</li> </ul> </li> </ul>
Filter Type	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Select the filter type:</p> <ul style="list-style-type: none"> <li>▪ Include filter: Include the specified value and disregard all other values.</li> <li>▪ Exclude filter: Exclude the specified value and regard all other values.</li> </ul>
Match String (Event Category)	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Enter a category that you want to filter for. Depending on the kind of filter, the sensor either processes the event category (Include filter option) or it does not process it (Exclude filter option). Enter a string.</p>
Filter by User	<p>Filter all received events for a certain event user:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not filter events.</li> <li>▪ Enable: Filter events. <ul style="list-style-type: none"> <li>ⓘ The sensor only processes messages that match the value that you define below.</li> </ul> </li> </ul>
Filter Type	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Select the filter type:</p> <ul style="list-style-type: none"> <li>▪ Include filter: Include the specified value and disregard all other values.</li> <li>▪ Exclude filter: Exclude the specified value and regard all other values.</li> </ul>
Match String (Event User)	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Enter a user name that you want to filter for. Depending on the kind of filter, the sensor either processes the event user (Include filter option) or it does not process it (Exclude filter option). Enter a string.</p>
Filter by Computer	<p>Filter all received events for a certain event computer:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not filter events.</li> <li>▪ Enable: Filter events. <ul style="list-style-type: none"> <li>ⓘ The sensor only processes messages that match the value that you define below.</li> </ul> </li> </ul>

Setting	Description
Filter Type	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Select the filter type:</p> <ul style="list-style-type: none"> <li>▪ Include filter: Include the specified value and disregard all other values.</li> <li>▪ Exclude filter: Exclude the specified value and regard all other values.</li> </ul>
Match String (Event Computer)	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Enter a computer name that you want to filter for. Depending on the kind of filter, the sensor either processes the event computer (Include filter option) or it does not process it (Exclude filter option). Enter a string.</p>
Filter by Message	<p>Filter all received events for a certain event message:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not filter events.</li> <li>▪ Enable: Filter events. <ul style="list-style-type: none"> <li>ⓘ The sensor only processes messages that match the value that you define below.</li> </ul> </li> </ul>
Filter Type	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Select the filter type:</p> <ul style="list-style-type: none"> <li>▪ Include filter: Include the specified value and disregard all other values.</li> <li>▪ Exclude filter: Exclude the specified value and regard all other values.</li> </ul>
Match String (Event Message)	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Enter a message that you want to filter for. Depending on the kind of filter, the sensor either processes the event message (Include filter option) or it does not process it (Exclude filter option). Enter a string.</p> <ul style="list-style-type: none"> <li>ⓘ This sensor only checks the <a href="#">last</a> line of the event message for the entered string. This matches the <code>&lt;Data&gt;</code> section of the XML that you can see on the Details tab in the Event Viewer. If you want to check the <a href="#">entire</a> event message, use the WMI Event Log sensor.</li> <li>ⓘ You must use the percent sign (%) as wildcard for any or no character if you want to check if the string is part of the last line of the event message. Otherwise, the whole last line of the event message must match the string.</li> </ul>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
New Records	The number of new records <b>i</b> This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

My Event Log (Windows API) sensors fail after installing Windows updates. What can I do?

- <https://kb.paessler.com/en/topic/89751>

My Event Log sensor ignores changes in the event log. What can I do?

- <https://kb.paessler.com/en/topic/59803>

How can I configure sensors using speed limits to keep the status for more than one interval?

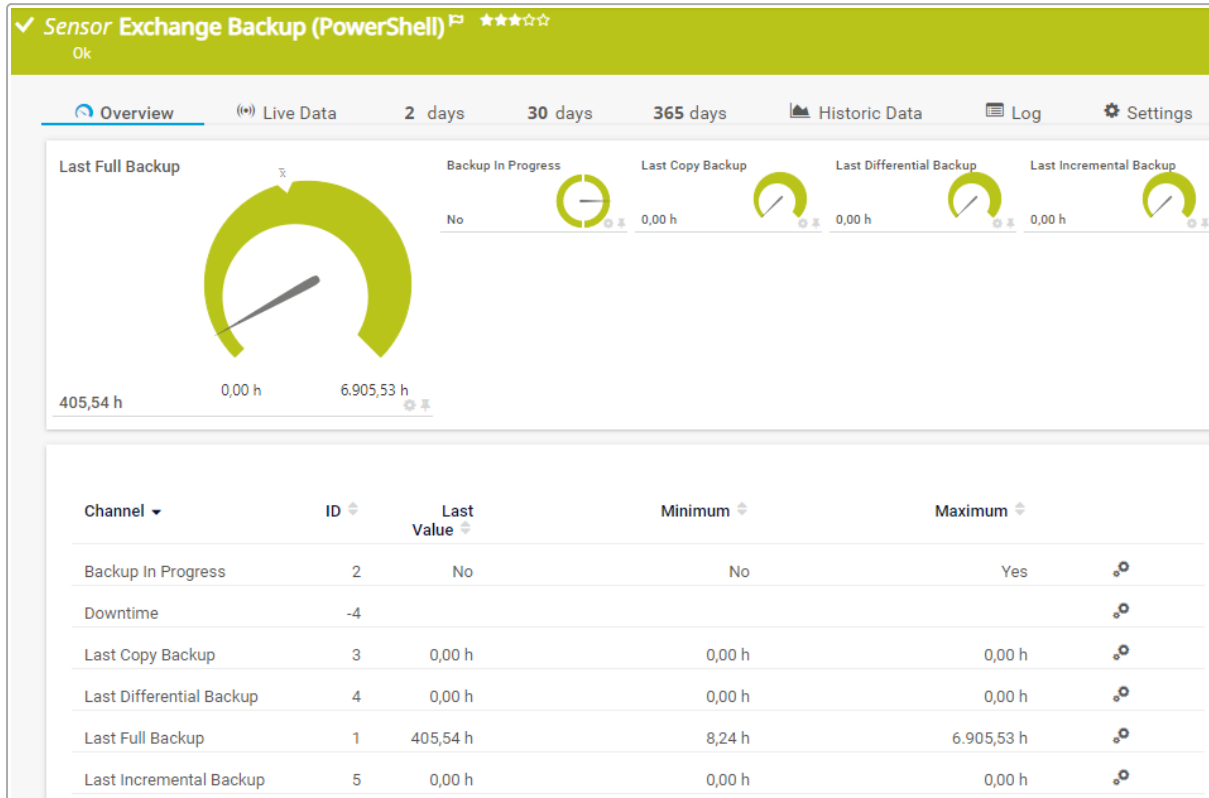
- <https://kb.paessler.com/en/topic/73212>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.40 Exchange Backup (PowerShell) Sensor

The Exchange Backup (PowerShell) sensor monitors backups of an Exchange server via Remote PowerShell.



Exchange Backup (PowerShell) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Exchange Backup (PowerShell)
- French: Exchange sauvegarde (PowerShell)
- German: Exchange-Sicherung (PowerShell)
- Japanese: Exchange バックアップ (PowerShell)
- Portuguese: Backup Exchange (PowerShell)
- Russian: Резервная копия Exchange (PowerShell)
- Simplified Chinese: Exchange 备份 (PowerShell)
- Spanish: Copia de seguridad Exchange (PowerShell)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:



Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Exchange user account permissions	<p>This sensor requires Exchange user account permissions.</p> <p><b>i</b> This sensor requires a user account that must be either in the Exchange management role group <a href="#">View-Only Organization Management</a> or be in a group with the following assigned management roles:</p> <ul style="list-style-type: none"> <li>▫ <a href="#">Monitoring</a></li> <li>▫ <a href="#">View-Only Configuration</a></li> <li>▫ <a href="#">View-Only Recipients</a></li> </ul>
Remote PowerShell and Remote Exchange Management Shell	<p>This sensor requires <a href="#">Remote PowerShell</a> and <a href="#">Remote Exchange Management Shell</a> on the target system and <a href="#">PowerShell</a> on the probe system. Also make sure you have at least <a href="#">PowerShell 2.0</a> installed on the probe system.</p> <p><b>i</b> In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message <a href="#">The WSMAN provider host process did not return a proper response</a>. In this case, increase the memory limit for Remote PowerShell.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">How do I enable and use remote commands in Windows PowerShell?</a> and <a href="#">How can I increase memory for Remote PowerShell?</a></p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p><b>i</b> If the framework is missing, you cannot create this sensor.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Parent device	This sensor requires that the parent device is the Exchange server (as of version 2016) that hosts the database that you want to monitor.
Credentials	This sensor requires credentials for Windows systems.
FQDN	<p>This sensor requires the <a href="#">fully qualified domain name (FQDN)</a> of the Exchange server in the settings of the parent device. In the <a href="#">device settings</a> of the Exchange server, provide the FQDN instead of the IP address.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">I have problems with the PowerShell Exchange sensors, what can I do?</a></p>

Remark	Description
IPv4	This sensor only supports IPv4.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Knowledge Base	Knowledge Base: <a href="#">Where can I find more information about PowerShell sensors?</a>
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

**Tags** ⓘ exampletag ✕ ⊕

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- backup
- exchange
- powershell

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Settings

#### Sensor Settings

**Database** ⓘ Database 1

**Result Handling** ⓘ

Discard result (default)

Store result

Sensor Settings

Setting	Description
Database	The name of the database that this sensor monitors.
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---


Graph Type **i**  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>+</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other above.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Backup In Progress	If a backup is running <ul style="list-style-type: none"> <li>▪ Up status: No, Yes</li> </ul>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Last Copy Backup	The time since the last copy backup
Last Differential Backup	The time since the last differential backup
Last Full Backup	The time since the last full backup <p> This channel is the primary channel by default.</p>
Last Incremental Backup	The time since the last incremental backup

## More

■ KNOWLEDGE BASE

Where can I find more information about PowerShell sensors?

- <https://kb.paessler.com/en/topic/62451>

How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

How can I increase memory for Remote PowerShell?

- <https://kb.paessler.com/en/topic/61922>

I have problems with the PowerShell Exchange sensors, what can I do?

- <https://kb.paessler.com/en/topic/54353>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My PowerShell sensor returns an error message. What can I do?

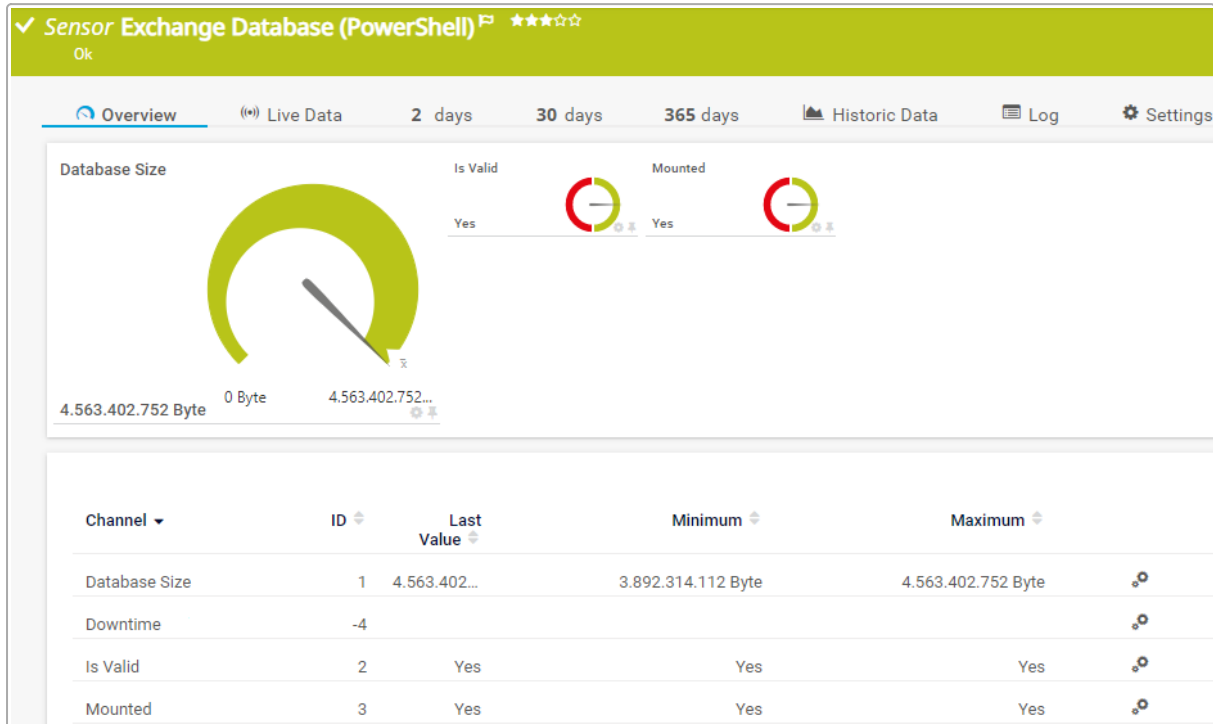
- <https://kb.paessler.com/en/topic/59473>

I get the error "WinRM cannot process the request" when I try to use a PowerShell sensor

- <https://kb.paessler.com/en/topic/59745>

## 7.8.41 Exchange Database (PowerShell) Sensor

The Exchange Database (PowerShell) sensor monitors database information of an Exchange server via Remote PowerShell.



Exchange Database (PowerShell) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Exchange Database (PowerShell)
- French: Exchange base de données (PowerShell)
- German: Exchange-Datenbank (PowerShell)
- Japanese: Exchange データベース (PowerShell)
- Portuguese: Banco de dados Exchange (PowerShell)
- Russian: База данных Exchange (PowerShell)
- Simplified Chinese: Exchange 数据库 (PowerShell)
- Spanish: Base de datos Exchange (PowerShell)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Exchange user account permissions	<p>This sensor requires Exchange user account permissions.</p> <p><b>i</b> This sensor requires a user account that must be either in the Exchange management role group <a href="#">View-Only Organization Management</a> or be in a group with the following assigned management roles:</p> <ul style="list-style-type: none"> <li>▫ <a href="#">Monitoring</a></li> <li>▫ <a href="#">View-Only Configuration</a></li> <li>▫ <a href="#">View-Only Recipients</a></li> </ul>
Remote PowerShell and Remote Exchange Management Shell	<p>This sensor requires <a href="#">Remote PowerShell</a> and <a href="#">Remote Exchange Management Shell</a> on the target system and <a href="#">PowerShell</a> on the probe system. Also make sure you have at least <a href="#">PowerShell 2.0</a> installed on the probe system.</p> <p><b>i</b> In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message <a href="#">The WSMAN provider host process did not return a proper response</a>. In this case, increase the memory limit for Remote PowerShell.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">How do I enable and use remote commands in Windows PowerShell?</a> and <a href="#">How can I increase memory for Remote PowerShell?</a></p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p><b>i</b> If the framework is missing, you cannot create this sensor.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Parent device	This sensor requires that the parent device is the Exchange server (as of version 2016) that hosts the database that you want to monitor.
Credentials	This sensor requires credentials for Windows systems.
FQDN	<p>This sensor requires the <a href="#">fully qualified domain name (FQDN)</a> of the Exchange server in the settings of the parent device. In the <a href="#">device settings</a> of the Exchange server, provide the FQDN instead of the IP address.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">I have problems with the PowerShell Exchange sensors, what can I do?</a></p>

Remark	Description
IPv4	This sensor only supports IPv4.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">Where can I find more information about PowerShell sensors?</a></li> <li>Knowledge Base: <a href="#">How can I monitor additional values of Exchange databases?</a></li> </ul>
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- database
- exchange
- powershell

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

### Sensor Settings

#### Sensor Settings

**Database** ⓘ *Mailbox Database*

**AutoRemount Database** ⓘ  Try to remount  
 Do not try to remount, report the current reading

**Result Handling** ⓘ  Discard result (default)  
 Store result

Sensor Settings



Setting	Description
Database	The name of the database that this sensor monitors.
AutoRemount Database	Define if you want the sensor to try to automatically remount the database if it is unmounted: <ul style="list-style-type: none"> <li>Try to remount</li> <li>Do not try to remount, report the current reading</li> </ul>
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**


Primary Channel **ⓘ** Downtime

---


Graph Type **ⓘ**
 Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor. <p><b>i</b> You can set a different primary channel later by clicking <b>⚙</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	Define how this sensor shows different channels: <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Database Size	<p>The size of the database</p> <ul style="list-style-type: none"> <li> This channel is the primary channel by default.</li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Is Valid	<p>If the database is recognized as valid</p> <ul style="list-style-type: none"> <li>Up status: Yes</li> <li>Down status: Critical Issue, Major Issue, Non Recoverable</li> </ul>
Mounted	<p>If the database is mounted</p>

Channel	Description
	<ul style="list-style-type: none"><li>▪ Up status: Yes</li><li>▪ Down status: No</li></ul>

## More

### KNOWLEDGE BASE

Where can I find more information about PowerShell sensors?

- <https://kb.paessler.com/en/topic/62451>

How can I monitor additional values of Exchange databases?

- <https://kb.paessler.com/en/topic/63229>

How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

How can I increase memory for Remote PowerShell?

- <https://kb.paessler.com/en/topic/61922>

I have problems with the PowerShell Exchange sensors, what can I do?

- <https://kb.paessler.com/en/topic/54353>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My PowerShell sensor returns an error message. What can I do?

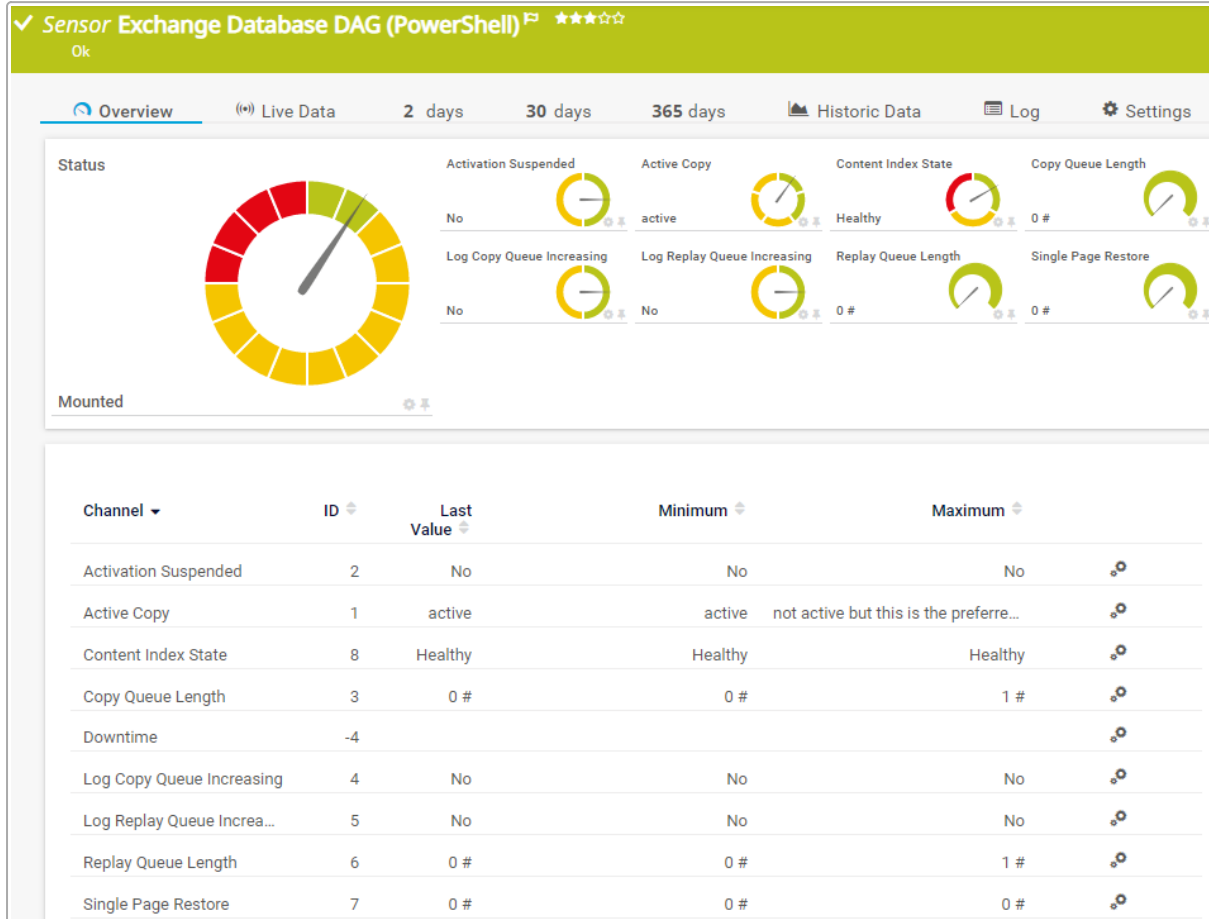
- <https://kb.paessler.com/en/topic/59473>

I get the error "WinRM cannot process the request" when I try to use a PowerShell sensor

- <https://kb.paessler.com/en/topic/59745>

## 7.8.42 Exchange Database DAG (PowerShell) Sensor

The Exchange Database DAG (PowerShell) sensor monitors the Database Availability Group (DAG) status of a database on an Exchange server via Remote PowerShell.



Exchange Database DAG (PowerShell) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Exchange Database DAG (PowerShell)
- French: Exchange base de données DAG (PowerShell)
- German: Exchange-Datenbank DAG (PowerShell)
- Japanese: Exchange データベース DAG (PowerShell)
- Portuguese: Banco de dados DAG Exchange (PowerShell)
- Russian: DAG базы данных Exchange (PowerShell)
- Simplified Chinese: Exchange 数据库 DAG (PowerShell)
- Spanish: Base de datos DAG Exchange (PowerShell)

## Remarks

Consider the following [remarks](#) <sup>927</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Exchange user account permissions	<p>This sensor requires Exchange user account permissions.</p> <p><b>i</b> This sensor requires a user account that must be either in the Exchange management role group <a href="#">View-Only Organization Management</a> or be in a group with the following assigned management roles:</p> <ul style="list-style-type: none"> <li>▫ <a href="#">Monitoring</a></li> <li>▫ <a href="#">View-Only Configuration</a></li> <li>▫ <a href="#">View-Only Recipients</a></li> </ul>
Valid DAG	This sensor requires that the Exchange server is part of a valid DAG. For more information, see the Knowledge Base: <a href="#">Why doesn't PRTG show available databases when adding the Exchange Database DAG (PowerShell) sensor?</a>
Remote PowerShell and Remote Exchange Management Shell	<p>This sensor requires <a href="#">Remote PowerShell</a> and <a href="#">Remote Exchange Management Shell</a> on the target system and <a href="#">PowerShell</a> on the probe system. Also make sure you have at least <a href="#">PowerShell 2.0</a> installed on the probe system.</p> <p><b>i</b> In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message <a href="#">The WSMAN provider host process did not return a proper response</a>. In this case, increase the memory limit for Remote PowerShell.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">How do I enable and use remote commands in Windows PowerShell?</a> and <a href="#">How can I increase memory for Remote PowerShell?</a></p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p><b>i</b> If the framework is missing, you cannot create this sensor.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Parent device	This sensor requires that the parent device is the Exchange server (as of version 2016) that hosts the database that you want to monitor.
Credentials	This sensor requires credentials for Windows systems.

Remark	Description
FQDN	<p>This sensor requires the <a href="#">fully qualified domain name (FQDN)</a> of the Exchange server in the settings of the parent device. In the <a href="#">device settings</a> of the Exchange server, provide the FQDN instead of the IP address.</p> <p>■ For more information, see the Knowledge Base: <a href="#">I have problems with the PowerShell Exchange sensors, what can I do?</a></p>
IPv4	This sensor only supports IPv4.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Target device	Make sure that the Exchange database is mounted on the target device. Otherwise, you might not be able to properly add this sensor.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">Where can I find more information about PowerShell sensors?</a></li> <li>Knowledge Base: <a href="#">How can I monitor additional values of Exchange databases?</a></li> </ul>
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- dag
- database
- exchange
- powershell

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Sensor Settings

**Sensor Settings**

Database ⓘ Database 1

Result Handling ⓘ  Discard result (default)  
 Store result

Sensor Settings

Setting	Description
Database	The name of the database that this sensor monitors.
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>

Setting	Description
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Activation Suspended	<p>If the activation is suspended</p> <ul style="list-style-type: none"> <li>Up status: No</li> <li>Warning status: Yes</li> </ul>
Active Copy	<p>The copy status</p> <ul style="list-style-type: none"> <li>Up status: Active, Not Active</li> <li>Warning status: Active But Not On The Preferred Server, Could Not Read Activation Preference, Not Active But This Is The Preferred Server</li> </ul>



Channel	Description
Content Index State	<p>The content index status</p> <ul style="list-style-type: none"> <li>Up status: Healthy, Not Supported In 2019</li> <li>Warning status: Crawling</li> <li>Down status: Error</li> </ul>
Copy Queue Length	The number of items in the copy queue
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Log Copy Queue Increasing	<p>If the log copy queue is increasing</p> <ul style="list-style-type: none"> <li>Up status: No</li> <li>Warning status: Yes</li> </ul>
Log Replay Queue Increasing	<p>If the log replay queue is increasing</p> <ul style="list-style-type: none"> <li>Up status: No</li> <li>Warning status: Yes</li> </ul>
Replay Queue Length	The number of items in the replay queue
Single Page Restore	The number of single page restores
Status	<p>The overall DAG status</p> <ul style="list-style-type: none"> <li>Up status: Healthy, Mounted</li> <li>Warning status: Disconnected and Healthy, Disconnected and Resynchronizing, Dismounting, Initializing, Mounting, Resynchronizing, Seeding, SeedingSource, SinglePageRestore, Suspended</li> <li>Down status: Dismounted, Failed, Failed and Suspended, Service Down</li> </ul> <p> This channel is the primary channel by default.</p>

## More

### KNOWLEDGE BASE

Why doesn't PRTG show available databases when adding the Exchange Database DAG (PowerShell) sensor?

- <https://kb.paessler.com/en/topic/82242>

Where can I find more information about PowerShell sensors?

- <https://kb.paessler.com/en/topic/62451>

How can I monitor additional values of Exchange databases?

- <https://kb.paessler.com/en/topic/63229>

How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

How can I increase memory for Remote PowerShell?

- <https://kb.paessler.com/en/topic/61922>

I have problems with the PowerShell Exchange sensors, what can I do?

- <https://kb.paessler.com/en/topic/54353>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My PowerShell sensor returns an error message. What can I do?

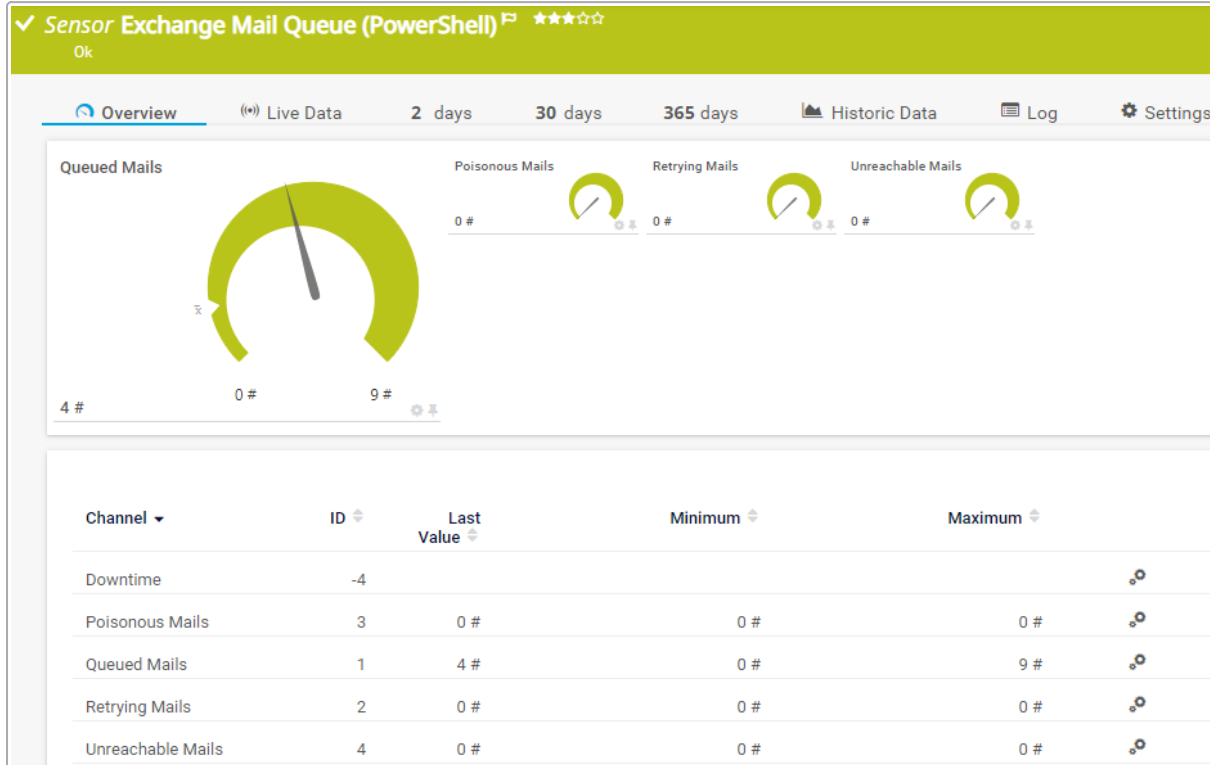
- <https://kb.paessler.com/en/topic/59473>

I get the error "WinRM cannot process the request" when I try to use a PowerShell sensor

- <https://kb.paessler.com/en/topic/59745>

### 7.8.43 Exchange Mail Queue (PowerShell) Sensor

The Exchange Mail Queue (PowerShell) sensor monitors the number of items in the outgoing mail queue of an Exchange server via Remote PowerShell.



Exchange Mail Queue (PowerShell) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

#### Sensor in Other Languages

- Dutch: Exchange Mail Wachtrij (PowerShell)
- French: Exchange file d'attente de messagerie (PowerShell)
- German: Exchange-Nachrichtenwarteschlange (PowerShell)
- Japanese: Exchange Mail キュー (PowerShell)
- Portuguese: Fila de e-mails Exchange (PowerShell)
- Russian: Очередь почтовых сообщений Exchange (PowerShell)
- Simplified Chinese: Exchange 邮件队列 (PowerShell)
- Spanish: Cola de correo Exchange (PowerShell)

#### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Exchange user account permissions	<p>This sensor requires Exchange user account permissions.</p> <p><b>i</b> This sensor requires a user account that must be either in the Exchange management role group <a href="#">View-Only Organization Management</a> or be in a group with the following assigned management roles:</p> <ul style="list-style-type: none"> <li>▫ <a href="#">Monitoring</a></li> <li>▫ <a href="#">View-Only Configuration</a></li> <li>▫ <a href="#">View-Only Recipients</a></li> </ul>
Remote PowerShell and Remote Exchange Management Shell	<p>This sensor requires <a href="#">Remote PowerShell</a> and <a href="#">Remote Exchange Management Shell</a> on the target system and <a href="#">PowerShell</a> on the probe system. Also make sure you have at least <a href="#">PowerShell 2.0</a> installed on the probe system.</p> <p><b>i</b> In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message <a href="#">The WSMAN provider host process did not return a proper response</a>. In this case, increase the memory limit for Remote PowerShell.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">How do I enable and use remote commands in Windows PowerShell?</a> and <a href="#">How can I increase memory for Remote PowerShell?</a></p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p><b>i</b> If the framework is missing, you cannot create this sensor.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Parent device	This sensor requires that the parent device is the Exchange server (as of version 2016) that hosts the database that you want to monitor.
FQDN	<p>This sensor requires the <a href="#">fully qualified domain name (FQDN)</a> of the Exchange server in the settings of the parent device. In the <a href="#">device settings</a> of the Exchange server, provide the FQDN instead of the IP address.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">I have problems with the PowerShell Exchange sensors, what can I do?</a></p>
Authentication	This sensor only supports <a href="#">Kerberos authentication</a> .

Remark	Description
IPv4	This sensor only supports IPv4.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">Where can I find more information about PowerShell sensors?</a></li> <li>Knowledge Base: <a href="#">What types of Exchange transport queues are there?</a></li> </ul>
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★★★★☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- exchange
- mailqueue
- powershell

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

### Sensor Settings

#### Sensor Settings

**Result Handling** ⓘ

Discard result (default)

Store result

Sensor Settings

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>+</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Poisonous Mails	The number of poisonous mails
Queued Mails	The number of queued mails  This channel is the primary channel by default.
Retrying Mails	The number of retrying mails
Unreachable Mails	The number of unreachable mails

## More

### ■ KNOWLEDGE BASE

Where can I find more information about PowerShell sensors?

- <https://kb.paessler.com/en/topic/62451>

What types of Exchange transport queues are there?

- <https://kb.paessler.com/en/topic/55413>

How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

How can I increase memory for Remote PowerShell?

- <https://kb.paessler.com/en/topic/61922>

I have problems with the PowerShell Exchange sensors, what can I do?

- <https://kb.paessler.com/en/topic/54353>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My PowerShell sensor returns an error message. What can I do?

- <https://kb.paessler.com/en/topic/59473>

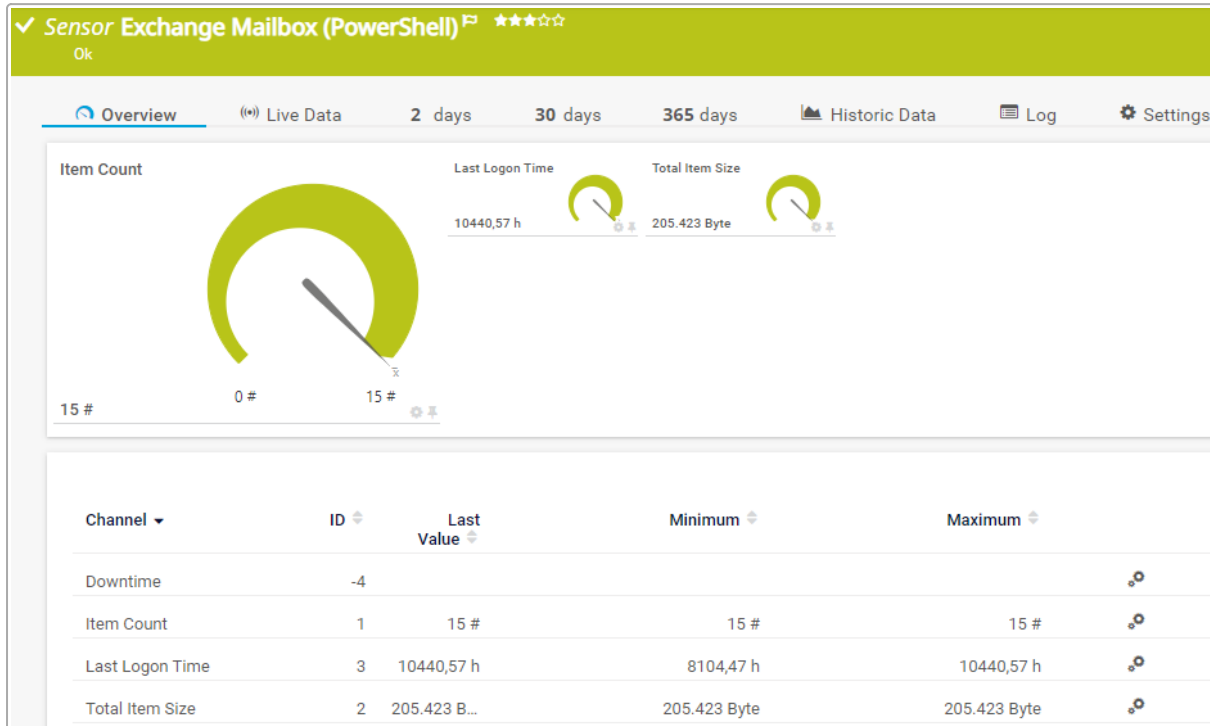
I get the error "WinRM cannot process the request" when I try to use a PowerShell sensor

- <https://kb.paessler.com/en/topic/59745>



## 7.8.44 Exchange Mailbox (PowerShell) Sensor

The Exchange Mailbox (PowerShell) sensor monitors mailboxes of an Exchange server via Remote PowerShell.



Exchange Mailbox (PowerShell) Sensor





For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Exchange Postbus (PowerShell)
- French: Exchange boîte aux lettres (PowerShell)
- German: Exchange-Postfach (PowerShell)
- Japanese: Exchange Mailbox( PowerShell)
- Portuguese: Caixa de correio Exchange (PowerShell)
- Russian: Почтовый ящик Exchange (PowerShell)
- Simplified Chinese: Exchange 邮箱 (PowerShell)
- Spanish: Buzón Exchange (PowerShell)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Elevated rights	This sensor requires elevated rights for the user of this sensor on the Exchange system. It is not sufficient to have administrative rights. For more information, see the Knowledge Base: <a href="#">I have problems with the PowerShell Exchange sensors, what can I do?</a> (solution (2) in the reply).
Remote PowerShell and Remote Exchange Management Shell	<p>This sensor requires <a href="#">Remote PowerShell</a> and <a href="#">Remote Exchange Management Shell</a> on the target system and <a href="#">PowerShell</a> on the probe system. Also make sure you have at least <a href="#">PowerShell 2.0</a> installed on the probe system.</p> <p> In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message <a href="#">The WSMAN provider host process did not return a proper response</a>. In this case, increase the memory limit for Remote PowerShell.</p> <p> For more information, see the Knowledge Base: <a href="#">How do I enable and use remote commands in Windows PowerShell?</a> and <a href="#">How can I increase memory for Remote PowerShell?</a></p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Parent device	This sensor requires that the parent device is the Exchange server (as of version 2016) that hosts the database that you want to monitor.
FQDN	<p>This sensor requires the <a href="#">fully qualified domain name (FQDN)</a> of the Exchange server in the settings of the parent device. In the <a href="#">device settings</a> of the Exchange server, provide the FQDN instead of the IP address.</p> <p> For more information, see the Knowledge Base: <a href="#">I have problems with the PowerShell Exchange sensors, what can I do?</a></p>
Credentials	This sensor requires credentials for Windows systems.
IPv4	This sensor only supports IPv4.
Knowledge Base	Knowledge Base: <a href="#">Where can I find more information about PowerShell sensors?</a>

Remark	Description
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- exchange
- mailbox
- powershell

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Settings

#### Sensor Settings

**Mailbox Name** ⓘ Mailbox1

---

**Result Handling** ⓘ   
 Discard result  
 Store result

Sensor Settings

Setting	Description
Mailbox Name	The name of the mailbox that this sensor monitors.
Result Handling	Define what PRTG does with the sensor result:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**


Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Item Count	The number of items  This channel is the primary channel by default.
Last Logon Time	The time since the last mailbox login
Total Item Size	The total size of items

## More

### ■ KNOWLEDGE BASE

I have problems with the PowerShell Exchange sensors, what can I do?

- <https://kb.paessler.com/en/topic/54353>

Where can I find more information about PowerShell sensors?

- <https://kb.paessler.com/en/topic/62451>

How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

How can I increase memory for Remote PowerShell?

- <https://kb.paessler.com/en/topic/61922>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My PowerShell sensor returns an error message. What can I do?

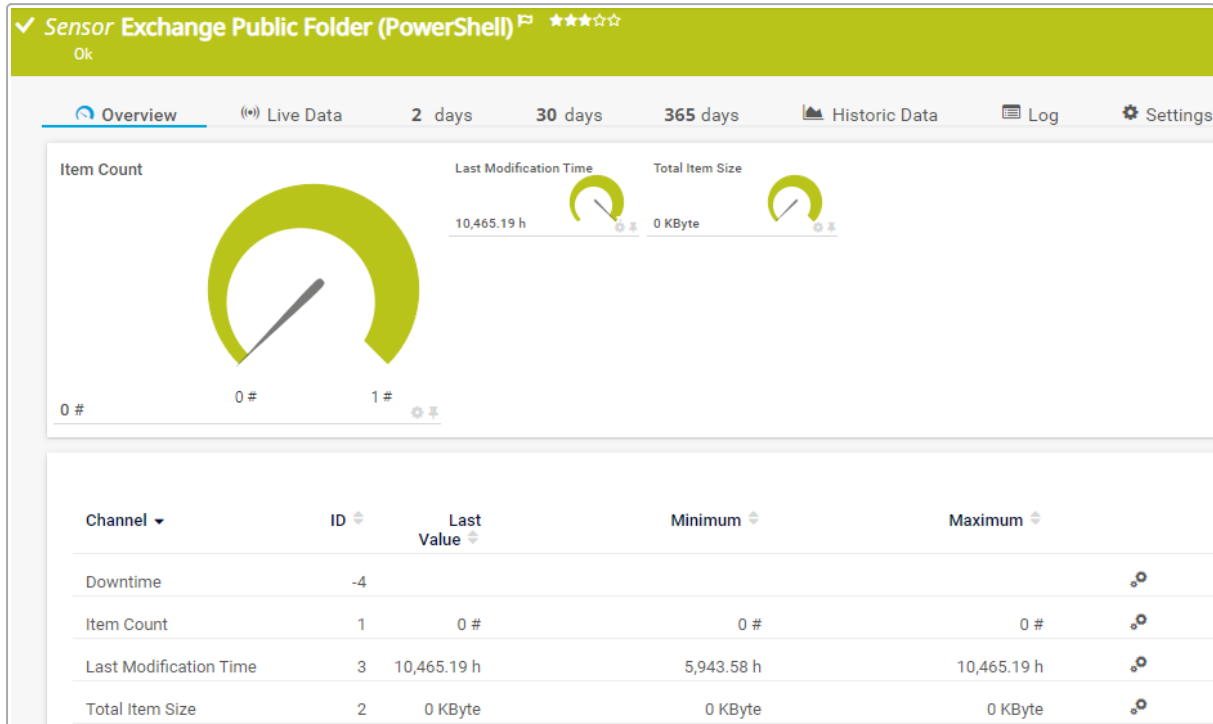
- <https://kb.paessler.com/en/topic/59473>

I get the error "WinRM cannot process the request" when I try to use a PowerShell sensor

- <https://kb.paessler.com/en/topic/59745>

## 7.8.45 Exchange Public Folder (PowerShell) Sensor

The Exchange Public Folder (PowerShell) sensor monitors the public folders and subfolders of an Exchange server via Remote PowerShell.



Exchange Public Folder (PowerShell) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[949]</sup>.

### Sensor in Other Languages

- Dutch: Exchange Openbare Map (PowerShell)
- French: Exchange dossier public (PowerShell)
- German: Exchange Öffentlicher Ordner (PowerShell)
- Japanese: Exchange パブリックフォルダー (PowerShell)
- Portuguese: Pasta pública Exchange (PowerShell)
- Russian: Общая папка Exchange (PowerShell)
- Simplified Chinese: Exchange 公共文件夹 (PowerShell)
- Spanish: Carpeta pública Exchange (PowerShell)

### Remarks

Consider the following [remarks](#)<sup>[945]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Exchange user account permissions	<p>This sensor requires Exchange user account permissions.</p> <p><b>i</b> This sensor requires a user account that must be either in the Exchange management role group <a href="#">View-Only Organization Management</a> or be in a group with the following assigned management roles:</p> <ul style="list-style-type: none"> <li>▫ <a href="#">Monitoring</a></li> <li>▫ <a href="#">View-Only Configuration</a></li> <li>▫ <a href="#">View-Only Recipients</a></li> </ul>
Remote PowerShell and Remote Exchange Management Shell	<p>This sensor requires <a href="#">Remote PowerShell</a> and <a href="#">Remote Exchange Management Shell</a> on the target system and <a href="#">PowerShell</a> on the probe system. Also make sure you have at least <a href="#">PowerShell 2.0</a> installed on the probe system.</p> <p><b>i</b> In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message <a href="#">The WSMAN provider host process did not return a proper response</a>. In this case, increase the memory limit for Remote PowerShell.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">How do I enable and use remote commands in Windows PowerShell?</a> and <a href="#">How can I increase memory for Remote PowerShell?</a></p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p><b>i</b> If the framework is missing, you cannot create this sensor.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Parent device	This sensor requires that the parent device is the Exchange server (as of version 2016) that hosts the database that you want to monitor.
Credentials	This sensor requires credentials for Windows systems.
FQDN	<p>This sensor requires the <a href="#">fully qualified domain name (FQDN)</a> of the Exchange server in the settings of the parent device. In the <a href="#">device settings</a> of the Exchange server, provide the FQDN instead of the IP address.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">I have problems with the PowerShell Exchange sensors, what can I do?</a></p>



Remark	Description
IPv4	This sensor only supports IPv4.
Knowledge Base	Knowledge Base: <a href="#">Where can I find more information about PowerShell sensors?</a>
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- exchange
- powershell
- publicfolder

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Settings

#### Sensor Settings

**Public Folder** ⓘ Folder1

---

**Result Handling** ⓘ  Discard result  
 Store result

Sensor Settings

Setting	Description
Public Folder	The name of the public folder that this sensor monitors.
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other above.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Item Count	The number of items  This channel is the primary channel by default.
Last Modification Time	The time since the last access
Total Item Size	The total size of items

## More

### ■ KNOWLEDGE BASE

Where can I find more information about PowerShell sensors?

- <https://kb.paessler.com/en/topic/62451>

How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

How can I increase memory for Remote PowerShell?

- <https://kb.paessler.com/en/topic/61922>

I have problems with the PowerShell Exchange sensors, what can I do?

- <https://kb.paessler.com/en/topic/54353>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My PowerShell sensor returns an error message. What can I do?

- <https://kb.paessler.com/en/topic/59473>

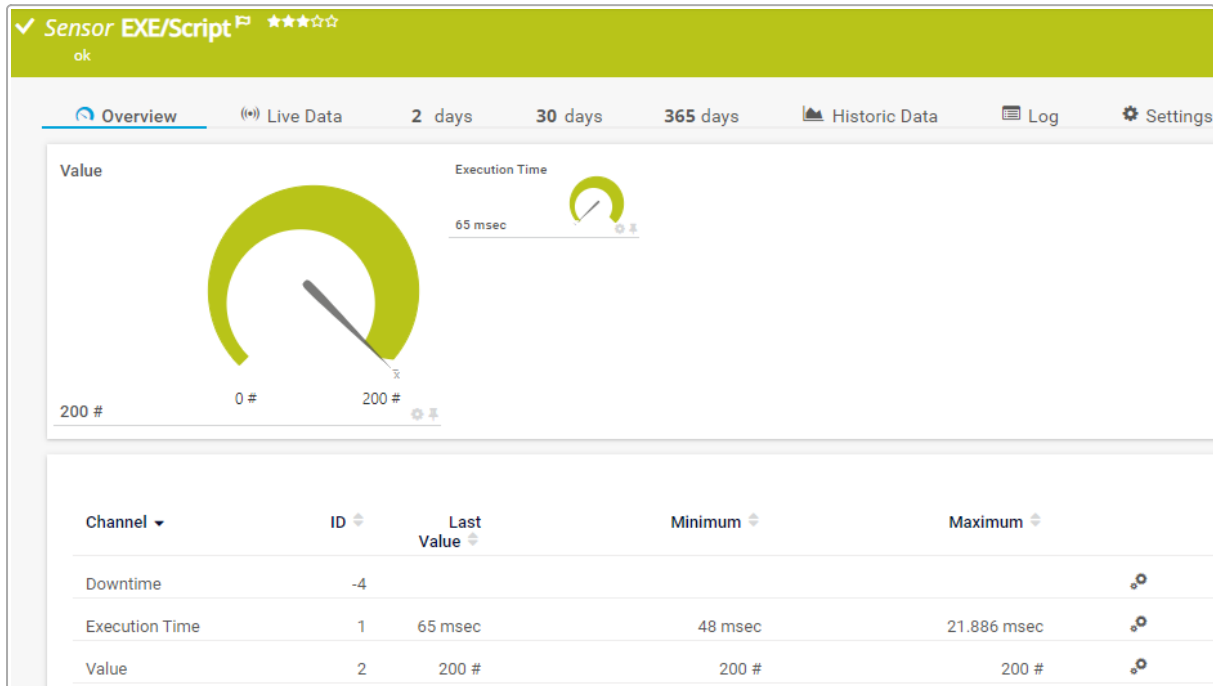
I get the error "WinRM cannot process the request" when I try to use a PowerShell sensor

- <https://kb.paessler.com/en/topic/59745>

## 7.8.46 EXE/Script Sensor

The EXE/Script sensor runs an executable file (.exe) or a script (batch file, VBScript, PowerShell) on the probe system. This option is available as part of the PRTG API.

**i** If you want to execute a custom Windows Management Instrumentation Query Language (WQL) script, use the [WMI Custom](#) <sup>[2482]</sup> sensor.



EXE/Script Sensor





**■** For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) <sup>[959]</sup>.

### Sensor in Other Languages

- Dutch: EXE/Script
- French: Script/EXE
- German: Programm/Skript
- Japanese: EXE/スクリプト
- Portuguese: EXE/Script
- Russian: EXE/скрипт
- Simplified Chinese: EXE/脚本
- Spanish: EXE/Script

### Remarks

Consider the following [remarks](#) <sup>[951]</sup> and requirements for this sensor:

Remark	Description
Remote PowerShell	<p>This sensor requires that Remote PowerShell is enabled on the target system and PowerShell 3.0 on both the probe system and the target system.</p> <p> Also make sure that you have at least <a href="#">PowerShell 3.0</a> installed on both the probe system and the target system. If you receive an error message regarding issues with the WinRM connection, make sure that remote commands have been enabled in PowerShell. For more information, see the Knowledge Base: <a href="#">How do I enable and use remote commands in Windows PowerShell?</a></p>
File storage	<p>The sensor requires the executable or script file to be stored on the probe system. In a cluster, copy the file to every cluster node.</p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Windows Server	<p>We recommend Windows Server 2016 on the probe system for best performance of this sensor.</p>
IPv6	<p>This sensor supports IPv6.</p>
Performance impact	<p>This sensor has a <a href="#">low</a> performance impact.</p>
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">What is the Mutex Name in the EXE/Script sensor settings?</a></li> <li>▪ Knowledge Base: <a href="#">How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?</a></li> <li>▪ Knowledge Base: <a href="#">How can I show special characters with EXE/Script sensors?</a></li> <li>▪ Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a></li> </ul>
Hosted probe	<p> You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.</p>
Custom scripts on Windows Consumer Editions	<p>To run a script in PRTG on this sensor, you have to open Windows PowerShell with administrator rights and enter the following command: <a href="#">powershell.exe Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope LocalMachine</a></p>

## Add Sensor

Setting	Description
Channel Name	<p>Enter a name for the channel. Enter a string. This is for display purposes only.</p> <p><b>i</b> You can change this value later in the <a href="#">channel settings</a> of this sensor.</p>
Unit String	<p>Enter the unit for the values that this sensor returns. Enter a string.</p> <p><b>i</b> PRTG uses the unit string for display purposes and shows it in graphs, data tables, and gauges.</p> <p><b>i</b> You can change this value later in the <a href="#">channel settings</a> of this sensor.</p>

## Basic Sensor Settings

**Basic Sensor Settings**

Sensor Name **i**

Tags **i**  **x** **+**

Priority **i** ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:


- exesensor

**■** For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Credentials for Script Sensors

Click  to interrupt the [inheritance](#).

### Credentials for Script Sensors

 inherit from

Placeholder 1 Description ⓘ

---

Placeholder 1 ⓘ

---

Credentials for Script Sensors

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder1</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder2</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder3</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder4</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder5</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.



## Sensor Settings

**Sensor Settings**

Note: The EXE file must run on the computer where the parent probe is installed, not on the parent device. The working directory for EXE files is the probe directory. .vbs files, .ps1 files, or other script files might use different working directories.

EXE/Script <sup>?</sup> Demo Batchfile - Returns 200.bat ▼

Parameters <sup>?</sup> \_\_\_\_\_

Environment <sup>?</sup>  Default  
 Set placeholders as environment values

Security Context <sup>?</sup>  Use security context of PRTG probe service (default)  
 Use Windows credentials from parent device

Mutex Name <sup>?</sup> \_\_\_\_\_

Timeout (Sec.) <sup>?</sup> 60

Value Type <sup>?</sup>  Integer (default)  
 Float  
 Counter

Channel Name <sup>?</sup> Value








Unit String <sup>?</sup> #

If Value Changes <sup>?</sup>  Ignore (default)  
 Trigger 'change' notification

Result Handling <sup>?</sup>  Discard result (default)  
 Store result  
 Store result in case of error

Sensor Settings

Setting	Description
EXE/Script	<p>Select an executable file from the list. The sensor executes it with every scanning interval.</p> <p>The list contains all files in the corresponding \Custom Sensors\EXE subfolder of the <a href="#">PRTG program directory</a> on the probe system. For a file to appear in this list, store the file ending in .bat, .cmd, .exe, .ps1, or .vbs into this subfolder.</p> <p><b>i</b> To show the expected sensor values and states, your files must use the correct format for the returned values (in this case, <a href="#">value:message</a> to standard output). The exit code of the file determines the <a href="#">sensor status</a>.</p> <p><b>i</b> If you use a PowerShell script (.ps1) and if the PowerShell Security Enhancement <a href="#">experimental feature</a> is enabled, scripts that use the <a href="#">write-host</a> cmdlet to provide their output to PRTG do not work. Use the <a href="#">write-output</a> cmdlet instead.</p>

Setting	Description
	<ul style="list-style-type: none"> <li> If you use custom sensors on the <a href="#">cluster probe</a>, copy your files to every cluster node.</li> <li> For more information on how to create custom sensors and for the return format, see section <a href="#">Custom Sensors</a>.</li> <li> You cannot change this value after sensor creation.</li> </ul>
Parameters	<p>If your executable or script file catches command-line parameters, you can define them here. You can use placeholders as well. Enter a string or leave the field empty.</p> <ul style="list-style-type: none"> <li> For a full list of all placeholders, see section <a href="#">Custom Sensors</a>.</li> <li> You cannot use environmental variables in this setting. Define environmental variables directly in your script or update the environmental variable values on your system.</li> <li> You need to escape special characters and whitespaces in your parameters and surround them with double quotation marks (""). See section <a href="#">Escape Special Characters and Whitespaces in Parameters</a> for details.</li> </ul>
Environment	<p>Select whether PRTG command-line parameters are also available as environment parameters:</p> <ul style="list-style-type: none"> <li>▪ Default environment: Do not provide values of PRTG placeholders in the environment. Select this secure option if you are not sure.</li> <li>▪ Set placeholders as environment values: Define if command-line parameters of PRTG are also available as environment parameters in your executable or script. For example, you can read and use the current host value of the parent device from within your script. This option can pose a security risk because credentials are exposed in several variables. It is not possible to use the environment variables in the parameters setting for batch scripts (.bat) for security reasons.</li> </ul> <ul style="list-style-type: none"> <li> For a full list of all available variables, see section <a href="#">Custom Sensors</a>.</li> </ul>
Security Context	<p>Define the Windows user account that the sensor uses to run the executable or script file:</p> <ul style="list-style-type: none"> <li>▪ Use security context of PRTG probe service: Run the file under the same Windows user account that the probe system runs under. By default, this is the Windows system user account.</li> <li>▪ Use Windows credentials from parent device: Use the Windows user account in the <a href="#">parent device settings</a>.</li> </ul>
Mutex Name	<p>Define a mutual exclusion (mutex) name for the process. Enter a string or leave the field empty.</p>

Setting	Description
	<p><b>i</b> PRTG executes all EXE/Script sensors that have the same mutex serially, not simultaneously. This is useful if you use a lot of sensors and you want to avoid high resource usage caused by simultaneously running processes.</p> <p><b>■</b> See the Knowledge Base: <a href="#">What is the Mutex Name in the EXE/Script sensor settings?</a></p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
Value Type	<p>Define the type of the values that your executable or script file returns:</p> <ul style="list-style-type: none"> <li>▪ Integer: An integer is expected as return value. If the script returns a float, PRTG displays the value <b>0</b>.</li> <li>▪ Float: A float is expected as return value, with a dot (.) between the predecimal position and the decimal places. <ul style="list-style-type: none"> <li><b>i</b> The sensor also displays integers unless they produce a buffer overflow.</li> </ul> </li> <li>▪ Counter: Your script returns an integer that increases. PRTG shows the difference between the values of two sensor scans. <ul style="list-style-type: none"> <li><b>i</b> A counter <b>must</b> return an integer. It does not support float values.</li> <li><b>i</b> The sensor does not support string values. <ul style="list-style-type: none"> <li><b>i</b> You cannot change this value after sensor creation.</li> </ul> </li> </ul> </li> </ul>
If Value Changes	<p>Define what the sensor does when its value changes:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> <li>▪ Trigger 'change' notification: Send an internal message that indicates a change. <ul style="list-style-type: none"> <li><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</li> </ul> </li> </ul>
Result Handling	<p>Define what the sensor does with the result that the executable file gives back:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Store result in case of error: Store the last sensor result only if the sensor shows the Down status.</li> </ul> <p><b>i</b> Select this option if you do not want failures to be overwritten by a following success of the script.</p> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Execution Time	The execution time  This channel is the primary channel by default.
[Value]	The value that the executable file or script file returns in one channel ■ For more information about the return value format, see section <a href="#">Custom Sensors</a> .

## More

### ■ KNOWLEDGE BASE

What is the Mutex Name in the EXE/Script sensor settings?

▪ <https://kb.paessler.com/en/topic/6673>

How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

▪ <https://kb.paessler.com/en/topic/11283>

How can I show special characters with EXE/Script sensors?

▪ <https://kb.paessler.com/en/topic/64817>

Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

▪ <https://kb.paessler.com/en/topic/75372>

Which .NET version does PRTG require?

▪ <https://kb.paessler.com/en/topic/60543>

How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

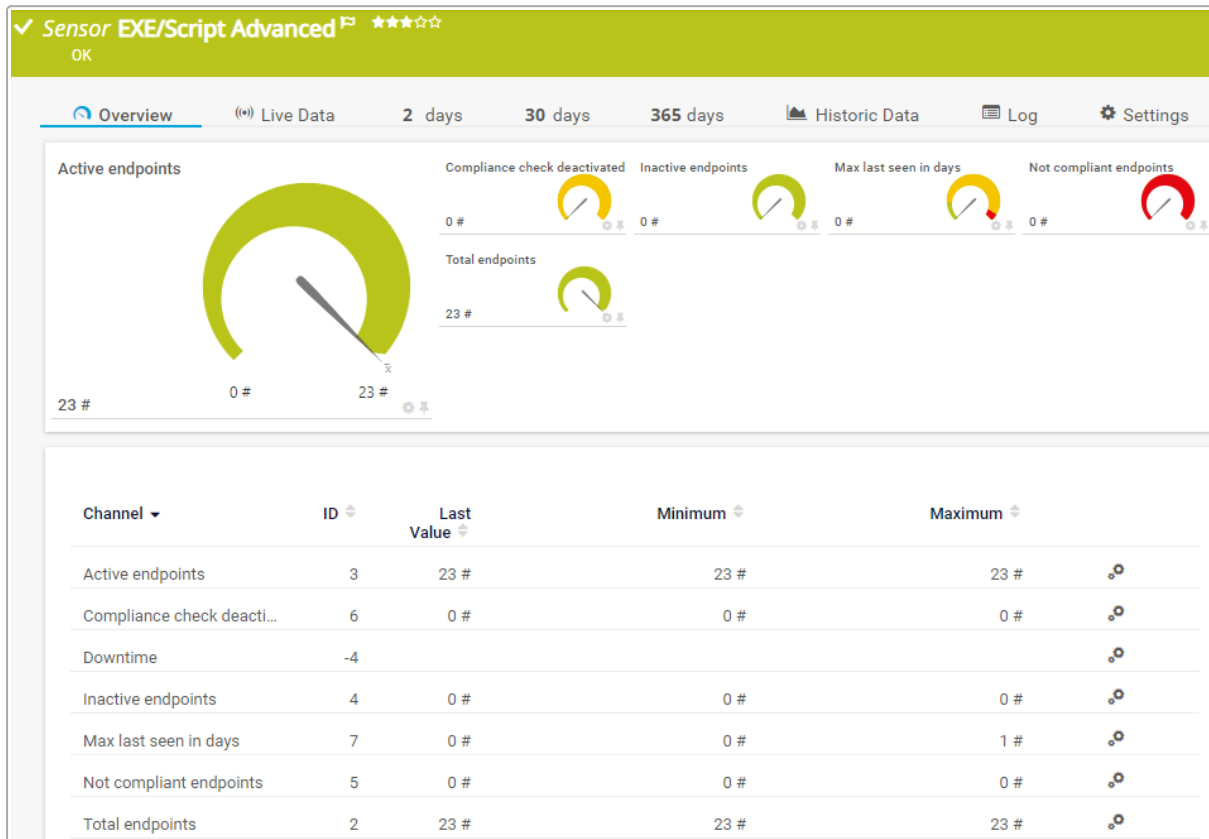
For which sensor types do you recommend at least Windows Server 2016 and why?

- <https://kb.paessler.com/en/topic/64331>

## 7.8.47 EXE/Script Advanced Sensor

The EXE/Script Advanced sensor runs an executable file (.exe) or a script (batch file, VBScript, PowerShell) on the probe system. This option is available as part of the PRTG API.

- i The return value of this sensor must be valid Extensible Markup Language (XML) or JavaScript Object Notation (JSON).
- i If you want to execute a custom Windows Management Instrumentation Query Language (WQL) script, use the [WMI Custom](#) <sup>[2482]</sup> sensor.



EXE/Script Advanced Sensor

■ For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) <sup>[968]</sup>.




### Sensor in Other Languages

- Dutch: EXE/Script Geavanceerd
- French: Script/EXE avancé
- German: Programm/Skript (Erweitert)
- Japanese: EXE/スクリプト(アドバンスト)
- Portuguese: EXE/Script avançado
- Russian: Расширенный сенсор EXE/скрипта
- Simplified Chinese: 高级 EXE/脚本


- Spanish: EXE/Script (avanzado)

## Remarks

Consider the following [remarks](#) <sup>962</sup> and requirements for this sensor:

Remark	Description
Remote PowerShell	<p>This sensor requires that Remote PowerShell is enabled on the target system and PowerShell 3.0 on both the probe system and the target system.</p> <p> Also make sure that you have at least <a href="#">PowerShell 3.0</a> installed on both the probe system and the target system. If you receive an error message regarding issues with the WinRM connection, make sure that remote commands have been enabled in PowerShell. For more information, see the Knowledge Base: <a href="#">How do I enable and use remote commands in Windows PowerShell?</a></p>
File storage	<p>The sensor requires the executable or script file to be stored on the probe system. In a cluster, copy the file to every cluster node.</p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Windows Server	<p>We recommend Windows Server 2016 on the probe system for best performance of this sensor.</p>
Channels	<p>This sensor does not officially support more than <a href="#">50 channels</a>.</p>
IPv6	<p>This sensor supports IPv6.</p>
Performance impact	<p>This sensor has a <a href="#">medium</a> performance impact.</p>
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">What is the Mutex Name in the EXE/Script sensor settings?</a></li> <li>▪ Knowledge Base: <a href="#">How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?</a></li> <li>▪ Knowledge Base: <a href="#">How can I show special characters with EXE/Script sensors?</a></li> <li>▪ Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a></li> </ul>



Remark	Description
	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">How can I use meta-scans for custom EXE/Script sensors?</a></li> </ul>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.
Custom scripts on Windows Consumer Editions	To run a script in PRTG on this sensor, you have to open Windows PowerShell with administrator rights and enter the following command: <code>powershell.exe Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope LocalMachine</code>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★★★★☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- xmlsensorsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Credentials for Script Sensors

Click  to interrupt the [inheritance](#).

#### Credentials for Script Sensors

 inherit from

**Placeholder 1 Description** ⓘ

**Placeholder 1** ⓘ

Credentials for Script Sensors

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder1</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder2</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder3</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder4</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder5</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.

## Sensor Settings

**Sensor Settings**

*The EXE file has to run on the computer where the parent probe is installed, not on the parent device. The working directory for EXE files is the probe directory. .vbs files, .ps1 files, or other script files might use different working directories.*

EXE/Script ⓘ Demo Batchfile - Returns static values in four channels.bat ▾

Parameters ⓘ

Environment ⓘ  Default  
 Set placeholders as environment values

Security Context ⓘ  Use security context of PRTG probe service (default)  
 Use Windows credentials from parent device

Mutex Name ⓘ

Timeout (Sec.) ⓘ 60

Result Handling ⓘ  Discard result (default)  
 Store result  
 Store result in case of error

Sensor Settings

Setting	Description
EXE/Script	<p>Select an executable file from the list. The sensor executes it with every scanning interval.</p> <p>The list contains all files in the corresponding \Custom Sensors\EXE subfolder of the <a href="#">PRTG program directory</a> on the probe system. For a file to appear in this list, store the file ending in .bat, .cmd, .exe, .ps1, or .vbs into this subfolder.</p> <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> To show the expected values and sensor states, your files must return the expected XML or JSON format to standard output. Values and message must be embedded in the XML or JSON.</li> <li><span style="color: red;">❗</span> If you use a PowerShell script (.ps1) and if the PowerShell Security Enhancement <a href="#">experimental feature</a> is enabled, scripts that use the <a href="#">write-host</a> cmdlet to provide their output to PRTG do not work. Use the <a href="#">write-output</a> cmdlet instead.</li> <li><span style="color: red;">❗</span> If you use custom sensors on the <a href="#">cluster probe</a>, copy your files to every cluster node.</li> </ul> <p><span style="color: blue;">■</span> For more information on how to create custom sensors and for the return format, see section <a href="#">Custom Sensors</a>.</p> <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> You cannot change this value after sensor creation.</li> </ul>

Setting	Description
Parameters	<p>If your executable or script file catches command-line parameters, you can define them here. You can use placeholders as well. Enter a string or leave the field empty.</p> <ul style="list-style-type: none"> <li><span style="color: #0070C0;">■</span> For a full list of all placeholders, see section <a href="#">Custom Sensors</a>.</li> <li><span style="color: #C00000;">ⓘ</span> You cannot use environmental variables in this setting. Define environmental variables directly in your script or update the environmental variable values on your system.</li> <li><span style="color: #C00000;">ⓘ</span> You need to escape special characters and whitespaces in your parameters and surround them with double quotation marks ("). See section <a href="#">Escape Special Characters and Whitespaces in Parameters</a> for details.</li> </ul>
Environment	<p>Select whether PRTG command-line parameters are also available as environment parameters:</p> <ul style="list-style-type: none"> <li>▪ Default environment: Do not provide values of PRTG placeholders in the environment. Select this secure option if you are not sure.</li> <li>▪ Set placeholders as environment values: Define if command-line parameters of PRTG are also available as environment parameters in your executable or script. For example, you can read and use the current host value of the parent device from within your script. This option can pose a security risk because credentials are exposed in several variables. It is not possible to use the environment variables in the parameters setting for batch scripts (.bat) for security reasons.</li> </ul> <ul style="list-style-type: none"> <li><span style="color: #0070C0;">■</span> For a full list of all available variables, see section <a href="#">Custom Sensors</a>.</li> </ul>
Security Context	<p>Define the Windows user account that the sensor uses to run the executable or script file:</p> <ul style="list-style-type: none"> <li>▪ Use security context of PRTG probe service: Run the file under the same Windows user account that the probe system runs under. By default, this is the Windows system user account.</li> <li>▪ Use Windows credentials from parent device: Use the Windows user account in the <a href="#">parent device settings</a>.</li> </ul>
Mutex Name	<p>Define a mutual exclusion (mutex) name for the process. Enter a string or leave the field empty.</p> <ul style="list-style-type: none"> <li><span style="color: #C00000;">ⓘ</span> PRTG executes all EXE/Script sensors that have the same mutex serially, not simultaneously. This is useful if you use a lot of sensors and you want to avoid high resource usage caused by simultaneously running processes.</li> <li><span style="color: #0070C0;">■</span> See the Knowledge Base: <a href="#">What is the Mutex Name in the EXE/Script sensor settings?</a></li> </ul>

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
Result Handling	<p>Define what the sensor does with the result that the executable file gives back:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> <li>▪ Store result in case of error: Store the last sensor result only if the sensor shows the Down status.</li> </ul> <p><b>i</b> Select this option if you do not want failures to be overwritten by a following success of the script.</p> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**



Primary Channel ⓘ Downtime

---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⚙</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p> <ul style="list-style-type: none"> <li> The Stack Unit setting for stacking graphs only works if you explicitly define the same <code>&lt;unit&gt;</code> for at least two channels. For more information about sensor settings, see section <a href="#">Custom Sensors</a>.</li> </ul>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	<p>The values that the executable file or script file returns in several channels</p> <ul style="list-style-type: none"> <li> For more information about the return value format, see section <a href="#">Custom Sensors</a>.</li> </ul>

## More

### ■ KNOWLEDGE BASE

What is the Mutex Name in the EXE/Script sensor settings?

- <https://kb.paessler.com/en/topic/6673>

How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- <https://kb.paessler.com/en/topic/11283>

How can I show special characters with EXE/Script sensors?

- <https://kb.paessler.com/en/topic/64817>

Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

How can I use meta-scans for custom EXE/Script sensors?

- <https://kb.paessler.com/en/topic/68109>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

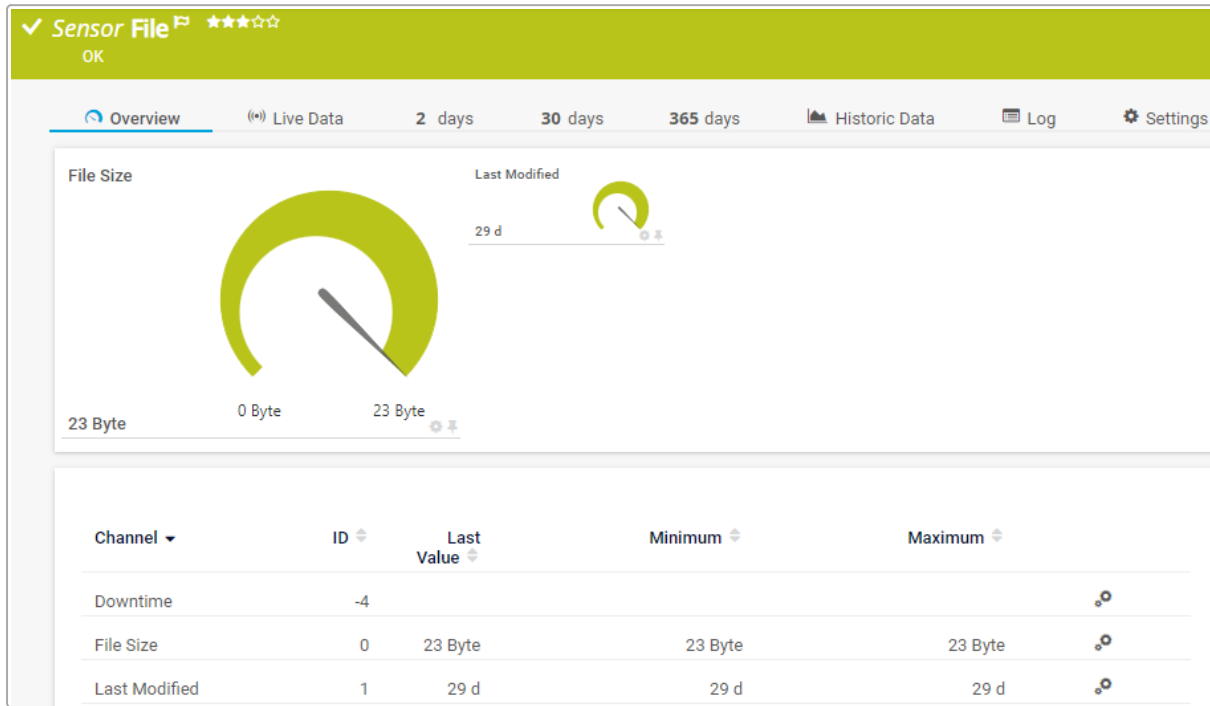
For which sensor types do you recommend at least Windows Server 2016 and why?

- <https://kb.paessler.com/en/topic/64331>

## 7.8.48 File Sensor

The File sensor monitors a file located on the local disk on the probe system, parent device, or a file that is accessible via Server Message Block (SMB). You can monitor changes to the file content and file time stamp.

**i** In contrast to the [Folder](#)<sup>[983]</sup> sensor, you can also monitor changes to the actual content of a file.



File Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[974]</sup>.

### Sensor in Other Languages

- Dutch: Bestand
- French: Fichier
- German: Datei
- Japanese: ファイル
- Portuguese: Arquivo
- Russian: Файл
- Simplified Chinese: 文件
- Spanish: Archivo

### Remarks

Consider the following [remarks](#)<sup>[970]</sup> and requirements for this sensor:



Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
LanmanServer service	<p>This sensor requires that the <a href="#">LanmanServer</a> service runs on the target system.</p> <ul style="list-style-type: none"> <li><span>ⓘ</span> The display name of the service is <a href="#">Server</a>.</li> <li><span>ⓘ</span> To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.</li> </ul>
IPv6	This sensor supports IPv6.
FQDN	Try the fully qualified domain name (FQDN) of the target system if the sensor does not get a connection with the IP address.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032</a></li> <li>▪ Knowledge Base: <a href="#">Can I use placeholders in file names to monitor log files?</a></li> </ul>
Hosted probe	<span>☁</span> You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- filesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Specific

**Sensor Specific**

**File Name** ⓘ C:\Windows\file.txt

---

**Sensor Behavior** ⓘ  Show down status if file does not exist  
 Show down status if file exists

**If Content Changes** ⓘ  Ignore (default)  
 Trigger 'change' notification

**If Time Stamp Changes** ⓘ  Ignore (default)  
 Trigger 'change' notification

Sensor Specific

Setting	Description
File Name	<p>Enter the full path to the file that this sensor monitors. For example, enter C:\Windows\file.txt. to monitor a file on the probe system.</p> <p>If you use a local path, the sensor only looks for the target file on the probe system, not on the parent device. To monitor a file on the parent device, use the dollar sign (\$) like C\$\User\username\file.txt.</p> <p>If the file is located on a network device, use the Universal Naming Convention (UNC) path <b>without</b> the server part (only enter share\folder\file.txt). The sensor inherits the server part (\\server\ from the <a href="#">parent device settings</a>. Enter a valid path and file name.</p> <p><b>ⓘ</b> To monitor Windows shares, the <a href="#">LanmanServer</a> service must run on the target system.</p> <p><b>ⓘ</b> The File sensor supports wildcards (*). For example, you can enter <a href="#">C:\Windows\*.txt</a> as File Name and select Show down status if file exists below if you want the sensor to show the Down <a href="#">status</a> if a .txt file exists in the defined directory.</p>
Sensor Behavior	<p>Define when the sensor shows the Down status:</p> <ul style="list-style-type: none"> <li>▪ Show down status if file does not exist: Show the Down status if the file <b>does not</b> exist.</li> <li>▪ Show down status if file exists: Show the Down status if the file <b>does</b> exist.</li> </ul>
If Content Changes	<p>Define what the sensor does if the content of the file changes (based on a checksum):</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Trigger 'change' notification: Send an internal message that indicates a change.                             <ul style="list-style-type: none"> <li><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</li> </ul> </li> </ul>
If Time Stamp Changes	<p>Define what the sensor does if the time stamp of the file changes:</p> <ul style="list-style-type: none"> <li>Ignore (default): Do nothing.</li> <li>Trigger 'change' notification: Send an internal message that indicates a change.                             <ul style="list-style-type: none"> <li><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</li> </ul> </li> </ul>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <ul style="list-style-type: none"> <li><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</li> </ul>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.



## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
File Size	The file size  This channel is the primary channel by default.
Last Modified	The time since the last modification of the file  The sensor shows a negative value if the date of a modified file is in the future.

## More

### ■ KNOWLEDGE BASE

What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032

- <https://kb.paessler.com/en/topic/513>

Can I use placeholders in file names to monitor log files?

- <https://kb.paessler.com/en/topic/67965>

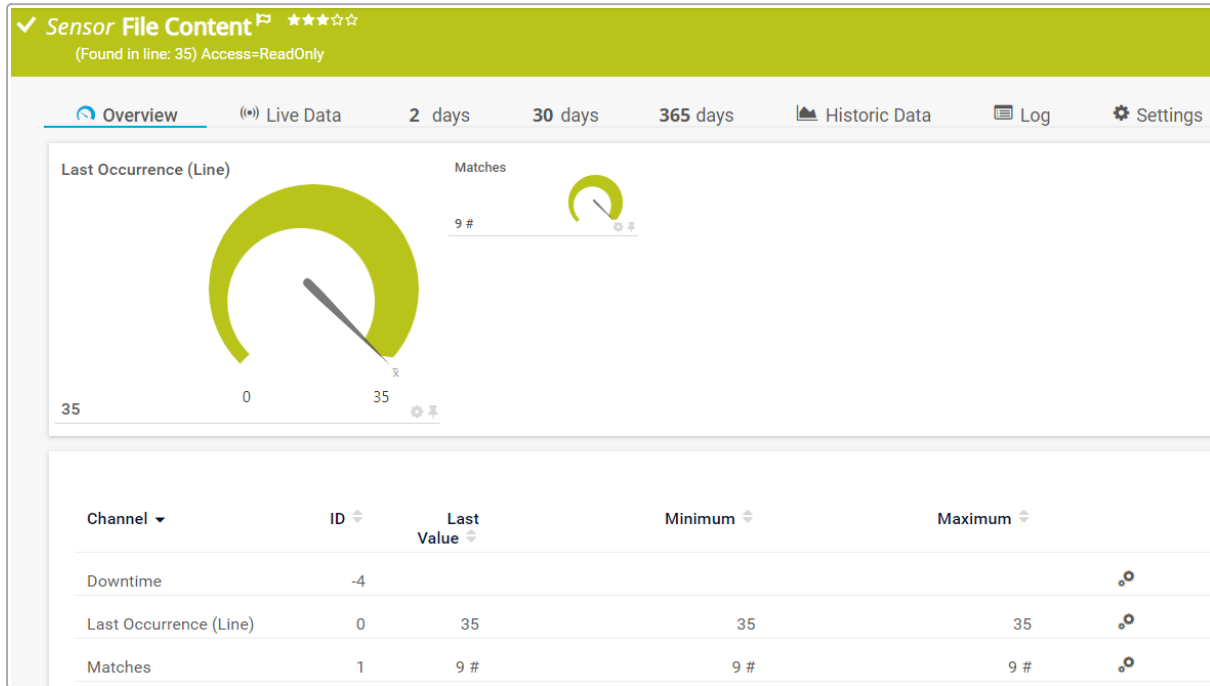
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.49 File Content Sensor

The File Content sensor checks a text file (for example, a log file) for certain strings.

**i** Additionally, this sensor quotes matching lines in the sensor message.



File Content Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Bestands inhoud
- French: Contenu du fichier
- German: Datei-Inhalt
- Japanese: ファイルの内容
- Portuguese: Conteúdo de arquivo
- Russian: Содержимое файла
- Simplified Chinese: 文件内容
- Spanish: Contenido de archivo

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
LanmanServer service	This sensor requires that the <a href="#">LanmanServer</a> service runs on the target system. <ul style="list-style-type: none"> <li><span>ⓘ</span> The display name of the service is <a href="#">Server</a>.</li> <li><span>ⓘ</span> To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.</li> </ul>
UTF-16 encoded files	This sensor does not support UTF-16 encoded files. Try a custom sensor like the <a href="#">EXE/Script</a> <sup>[951]</sup> sensor or the <a href="#">EXE/Script Advanced</a> <sup>[961]</sup> sensor.
Binary files	This sensor does not officially support binary files. If you want to monitor them anyway, select Always transmit the entire file in the <a href="#">sensor settings</a> <sup>[979]</sup> .
Unix line feeds	This sensor supports Unix line feeds.
IPv6	This sensor supports IPv6.
Linux system	To monitor files on a Linux system, the folder must be accessible via Server Message Block (SMB).
FQDN	Try the fully qualified domain name (FQDN) of the target system if the sensor does not get a connection with the IP address.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★★★☆

Example Name

---

exampletag ✕ +

---

★★★★☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- filesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Specific

**Sensor Specific**

**File Name** ⓘ C:\Windows\file.txt

---

**Search String** ⓘ test

---

**Search Method** ⓘ  Simple string search  
 Regular expression

**File Transmission Handling** ⓘ  Only transmit new lines at the end of the file (default, BETA)  
 Always transmit the entire file

**File Encoding** ⓘ  Windows-1252 (default)  
 UTF-8  
 UTF-16

**Sensor Behavior** ⓘ  Show warning status when the string is not found  
 Show warning status when the string is found

**If Value Changes** ⓘ  Ignore (default)  
 Trigger 'change' notification

Sensor Specific

Setting	Description
File Name	<p>Enter the full path to the file that this sensor monitors. For example, enter C:\Windows\file.txt. to monitor a file on the probe system.</p> <p>If you use a local path, the sensor only looks for the target file on the probe system, not on the parent device. To monitor a file on the parent device, use the dollar sign (\$) like C\$\User\username\file.txt.</p> <p>If the file is located on a network device, use the Universal Naming Convention (UNC) path <b>without</b> the server part (only enter share\folder\file.txt). The sensor inherits the server part (\\server\ from the <a href="#">parent device settings</a>. Enter a valid path and file name.</p> <p><b>i</b> To monitor Windows shares, the <a href="#">LanmanServer</a> service must run on the target system.</p> <p><b>i</b> To monitor Linux files, the folder with these files must be accessible via SMB.</p>



Setting	Description
	<p><b>i</b> Note that it might produce a high amount of network traffic if you define that PRTG queries an entire file on your network with every scanning interval.</p>
Search String	<p>Define the string that you want to search the file for. You can enter a simple string in plain text or a <a href="#">regular expression (regex)</a>.</p> <p><b>i</b> The search string must be case-sensitive.</p>
Search Method	<p>Define the method with which you want to provide the search string:</p> <ul style="list-style-type: none"> <li>▪ Simple string search (default): Search for a simple string in plain text.</li> </ul> <p><b>i</b> The characters <code>*</code> and <code>?</code> work as placeholders. <code>*</code> stands for no number or any number of characters and <code>?</code> stands for exactly one character. You cannot change this behavior. The literal search for these characters is only possible with a regex.</p> <ul style="list-style-type: none"> <li>▪ Regular expression: Search with a regex.</li> </ul> <p><b>i</b> The pattern must be in <b>one</b> line and only the <b>last</b> matching line is returned.</p> <p><b>i</b> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</p>
File Transmission Handling	<p>Define in which way the sensor transmits the target file to PRTG:</p> <ul style="list-style-type: none"> <li>▪ Only transmit new lines at the end of the file (default): Send the entire file to PRTG only with the first scanning interval. With the following scanning intervals, the sensor only transmits new lines at the end of the file. It does not send old lines but it still counts them. This option improves the performance of the sensor. <b>BETA</b> This option is in beta status. Do not expect that it works as expected in every usage scenario.</li> <li>▪ Always transmit the entire file: Send the entire file to PRTG with every scanning interval. If this results in too much traffic on the target system, we recommend that you choose Only transmit new lines at the end of the file (default) instead.</li> </ul> <p>This sensor can only transmit new lines in the following cases:</p> <ul style="list-style-type: none"> <li>▪ the file is bigger than in the previous scanning interval, and</li> <li>▪ the last line in the file is still in the same place in the file.</li> </ul> <p><b>i</b> This sensor supports Windows and Linux line endings (<b>CRLF</b> or <b>LF</b>).</p>
File Encoding	<p>Specify the encoding of the file that this sensor monitors:</p> <ul style="list-style-type: none"> <li>▪ Windows-1252 (default)</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>UTF-8</li> <li>UTF-16</li> </ul>
Sensor Behavior	<p>Define the condition for which the sensor shows the Warning <a href="#">status</a>:</p> <ul style="list-style-type: none"> <li>Show warning status when the string is not found (default): Show the Warning status if there is <b>no</b> match. Otherwise it remains in the Up status.</li> <li>Show warning status when the string is found: Show the Warning status if there <b>is</b> a match. Otherwise it remains in the Up status.</li> </ul>
If Value Changes	<p>Define what the sensor does if the value of the Last Occurrence (Line) channel changes:</p> <ul style="list-style-type: none"> <li>Ignore (default): Do nothing.</li> <li>Trigger 'change' notification: Send an internal message that indicates a change. <ul style="list-style-type: none"> <li><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</li> </ul> </li> <li><b>i</b> This sensor does <b>not</b> trigger the notification when the number of Matches changes.</li> </ul>

## Debug Options

**Debug Options**

Result Handling **i**  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> <li><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</li> </ul>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Last Occurrence (Line)	The line number of the last match  This channel is the primary channel by default.
Matches	The number of matches

## More

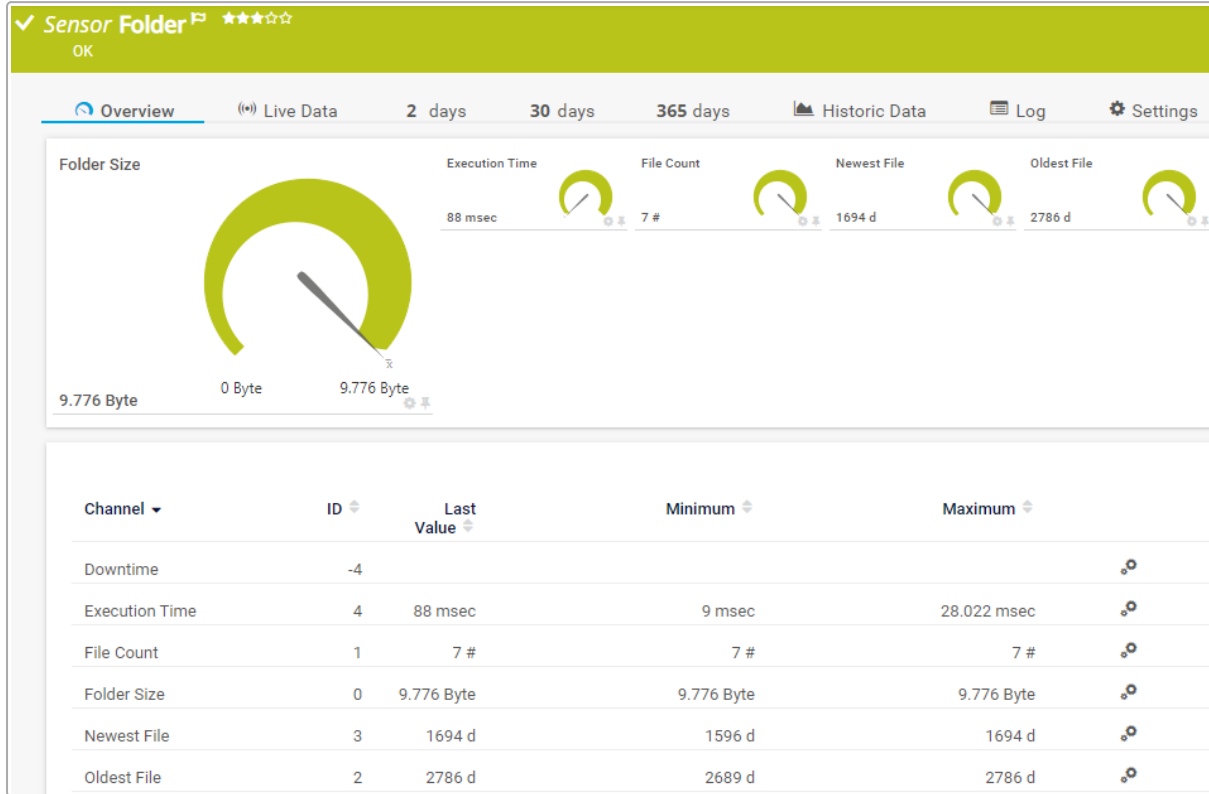
### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.50 Folder Sensor

The Folder sensor monitors a folder via Server Message Block (SMB). You can monitor file changes and file ages.



Folder Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Map
- French: Dossier
- German: Ordner
- Japanese: フォルダ
- Portuguese: Pasta
- Russian: Папка
- Simplified Chinese: 文件夹
- Spanish: Carpeta

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
LanmanServer service	This sensor requires that the <a href="#">LanmanServer</a> service runs on the target system. <i>i</i> The display name of the service is <a href="#">Server</a> . <i>i</i> To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.
IPv6	This sensor supports IPv6.
File count	This sensor counts all files in a folder, including hidden files.
Knowledge Base	Knowledge Base: <a href="#">What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032</a>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Add Sensor

Setting	Description
File Age Check	Specify if the sensor monitors the folder for certain file ages and shows a corresponding <a href="#">status</a> : <ul style="list-style-type: none"> <li>▪ Do not check: Do not check the age of the files in the folder:</li> <li>▪ Show warning status if older: Set the sensor to the Warning status if one of the files in the folder is older than a specific limit unit.</li> <li>▪ Show down status if older: Set the sensor to the Down status if one of the files in the folder is older than a specific limit unit.</li> <li>▪ Show warning status if younger: Set the sensor to the Warning status if one of the files in the folder is younger than a specific limit unit.</li> <li>▪ Show down status if younger: Set the sensor to the Down status if one of the files in the folder is younger than a specific limit unit.</li> </ul> <i>i</i> You can change this setting later via the Limits section in the <a href="#">channel settings</a> of Newest File and Oldest File.

Setting	Description
File Age Limit	<p>This setting is only visible if you select a file age check above.</p> <p>Enter the age of a file in the folder that triggers the sensor status change if the age falls below a specific value or if it is exceeded. Enter an integer. Define the limit unit below.</p> <p><b>i</b> You can change this setting later via the Limits section in the <a href="#">channel settings</a> of Newest File and Oldest File.</p>
File Age Limit Unit	<p>This setting is only visible if you select a file age check above.</p> <p>Specify the unit for the file age value:</p> <ul style="list-style-type: none"> <li>▪ Days: Select this option if the File Age Limit is a number of days.</li> <li>▪ Hours: Select this option if the File Age Limit is a number of hours.</li> <li>▪ Minutes: Select this option if the File Age Limit is a number of minutes.</li> </ul> <p><b>i</b> You can change this setting later via the Limits section in the <a href="#">channel settings</a> of Newest File and Oldest File.</p>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

Example Name

**Tags** ⓘ

exampletag x +

**Priority** ⓘ

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- foldersensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Folder Monitor

**Folder Monitor**

Folder Name ⓘ C:\Windows

---

Recurse Subfolders ⓘ  Do not recurse subfolders  
 Monitor the folder and its subfolders (recursive)

If Content Changes ⓘ  Ignore (default)  
 Trigger 'change' notification

Timeout (Sec.) ⓘ 300

---

Note: You can set up file age checks in the settings of the channels Oldest File and Newest File. Enter your desired thresholds (in seconds) in the channel settings section Limits.

Folder Monitor

Setting	Description
Folder Name	<p>Enter the full path to the folder that this sensor monitors. For example, enter <a href="#">C:\Windows</a> to monitor a folder on the probe system.</p> <p>If you use a local path, the sensor only looks for the target folder on the probe system and not on the parent device. To monitor a folder on the parent device, use a dollar sign (\$) in the path. For example, enter <a href="#">C\$\Windows</a>.</p> <p>If the folder is located on a network device, use the Universal Naming Convention (UNC) path without the server part (only enter share\folder). The sensor inherits the server part (\\server\) from the <a href="#">parent device settings</a>. Enter a valid path name.</p> <p><b>i</b> To monitor Windows shares, the <a href="#">LanmanServer</a> service must run on the target system.</p>
Recurse Subfolders	<p>Specify if the sensor includes subfolders in the folder monitoring:</p> <ul style="list-style-type: none"> <li>▪ Do not recurse subfolders (default): Only monitor the folder. Do not monitor its subfolders.</li> <li>▪ Monitor the folder and its subfolders (recursive): Monitor the folder and all of its subfolders.</li> </ul> <p><b>i</b> If you recurse subfolders in large directories that have a high number of branches, this might cause timeout errors or performance issues.</p>
If Content Changes	<p>Define what the sensor does if the content or file name of the folder changes, or if there are new or deleted files:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> <li>▪ Trigger 'change' notification: Send an internal message that indicates a change.</li> </ul> <p><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</p>



Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

## Debug Options

**Debug Options**

**Result Handling** ?
 Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display


**Sensor Display**

**Primary Channel** ? Downtime


---


**Graph Type** ?
 Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings




By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Execution Time	The execution time
File Count	The number of files in the folder  The sensor counts all files in a folder, including <a href="#">hidden files</a> .
Folder Size	The folder size  This channel is the primary channel by default.
Newest File	The time since the newest modification of a file in the folder (newest file)  The sensor shows a negative value if the date of a modified file is in the future.
Oldest File	The time since the oldest modification of a file in the folder (oldest file)

## More

### ■ KNOWLEDGE BASE

What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032

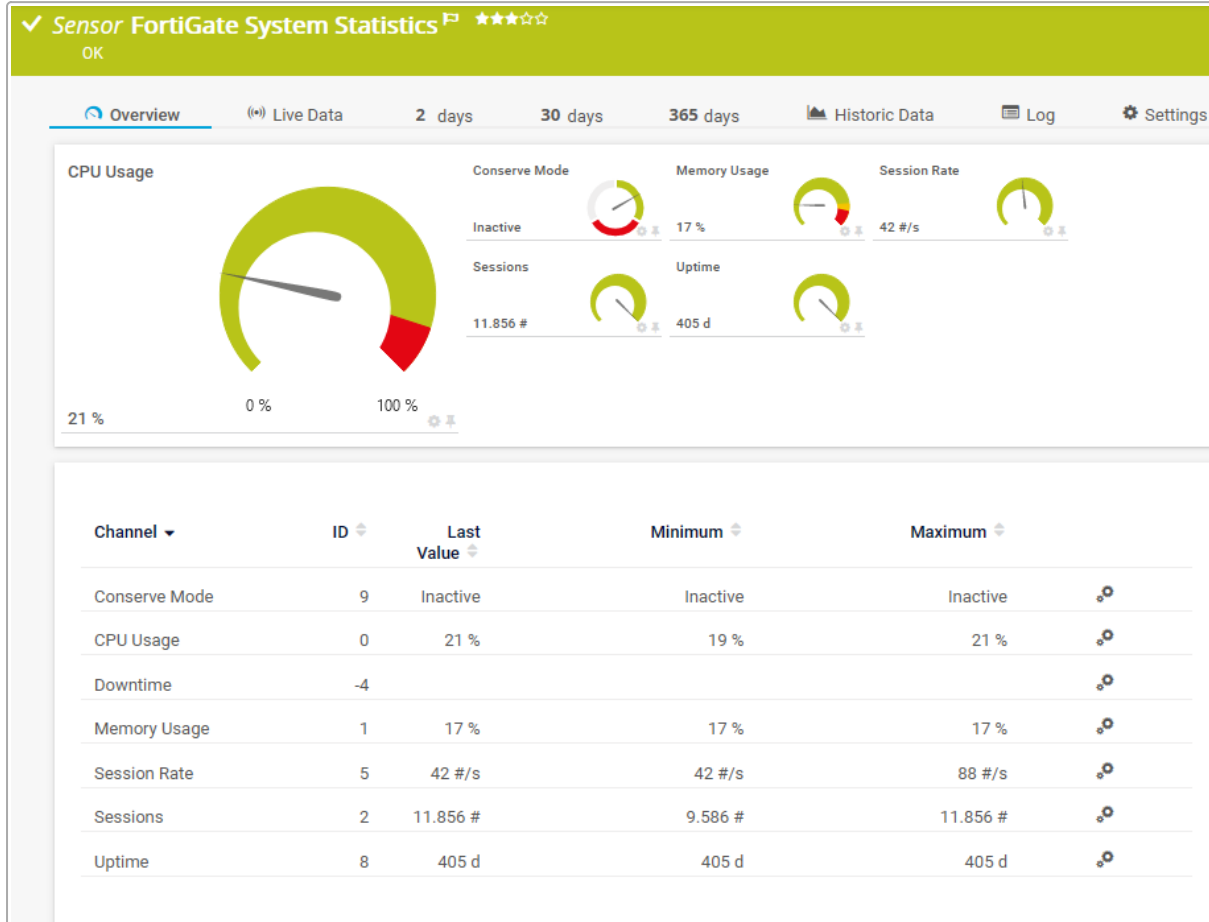
- <https://kb.paessler.com/en/topic/513>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.51 FortiGate System Statistics Sensor

The FortiGate System Statistics sensor monitors the system health of a Fortinet FortiGate firewall via the Representational State Transfer (REST) application programming interface (API).



FortiGate System Statistics Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: FortiGate System Statistieken
- French: Statistiques du système FortiGate
- German: FortiGate-Systemstatistiken
- Japanese: FortiGate システム統計
- Portuguese: Estatísticas do sistema FortiGate
- Russian: Системная статистика FortiGate
- Simplified Chinese: FortiGate 系统统计
- Spanish: Estadísticas del sistema FortiGate

## Remarks

Consider the following [remarks](#)<sup>[991]</sup> and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for FortiGate.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">5 minutes</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  X +

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- firewall
- fortigate
- fortinet
- fortios
- systemstatistics

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Conserve Mode	<p>The conserve mode status</p> <ul style="list-style-type: none"> <li>▪ Up status: Inactive</li> <li>▪ Down status: Active</li> <li>▪ Unknown status: Unknown</li> </ul>
CPU Usage	<p>The CPU usage</p> <p>ⓘ This channel is the primary channel by default.</p> <p>ⓘ This channel has a default limit:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: <b>90%</b></li> </ul>

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Memory Usage	The memory usage (%) ⓘ This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: 88%</li> <li>▪ Upper warning limit: 82%</li> </ul>
Session Rate	The number of sessions
Sessions	The total number of sessions
Uptime	The uptime

## More

### ■ KNOWLEDGE BASE

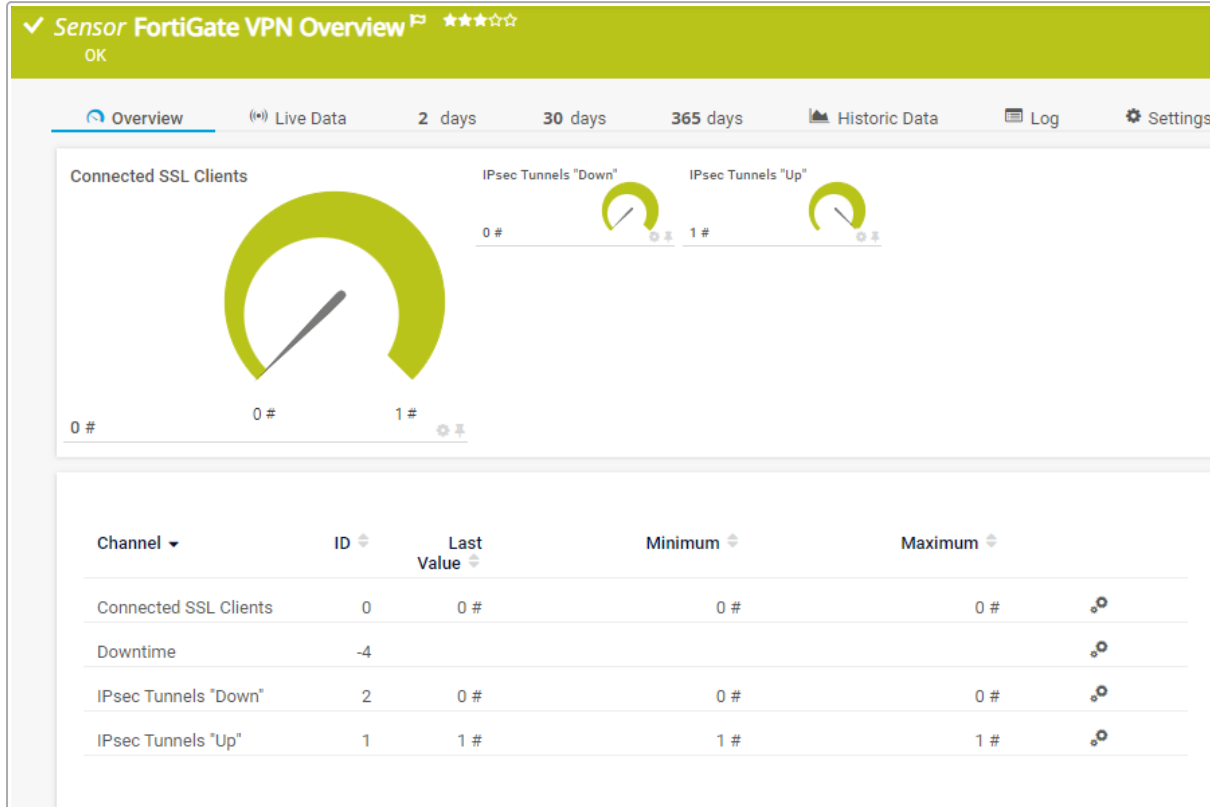
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>



## 7.8.52 FortiGate VPN Overview Sensor

The FortiGate VPN Overview sensor monitors the virtual private network (VPN) connections of a Fortinet FortiGate system via the Representational State Transfer (REST) application programming interface (API).



FortiGate VPN Overview Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: FortiGate VPN Overzicht
- French: FortiGate VPN vue d'ensemble
- German: FortiGate VPN-Übersicht
- Japanese: FortiGate VPN の概要
- Portuguese: Visão geral da VPN FortiGate
- Russian: Обзор VPN FortiGate
- Simplified Chinese: FortiGate VPN 概述
- Spanish: Resumen de la VPN FortiGate

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for FortiGate.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Scanning interval	<ul style="list-style-type: none"> <li>The minimum scanning interval of this sensor is <b>1 minute</b>.</li> <li>The recommended scanning interval of this sensor is <b>5 minutes</b>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ ★★★★☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- fortigate
- fortinet
- fortios
- vpn

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### FortiGate Specific

#### FortiGate Specific

**Ignored VPNs** ⓘ

FortiGate Specific

Setting	Description
Ignored VPNs	<p>Enter the name of any VPN that this sensor should ignore. Ignored VPNs do not affect the status of the sensor. Enter one VPN per line.</p> <p><b>i</b> The name that you enter must be case-sensitive.</p>

## Sensor Display


**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Connected SSL Clients	The number of SSL clients that are connected
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
IPsec Tunnels "Down"	The number of IPsec tunnels that are down
IPsec Tunnels "Up"	The number of IPsec tunnels that are up

## More

### ■ KNOWLEDGE BASE

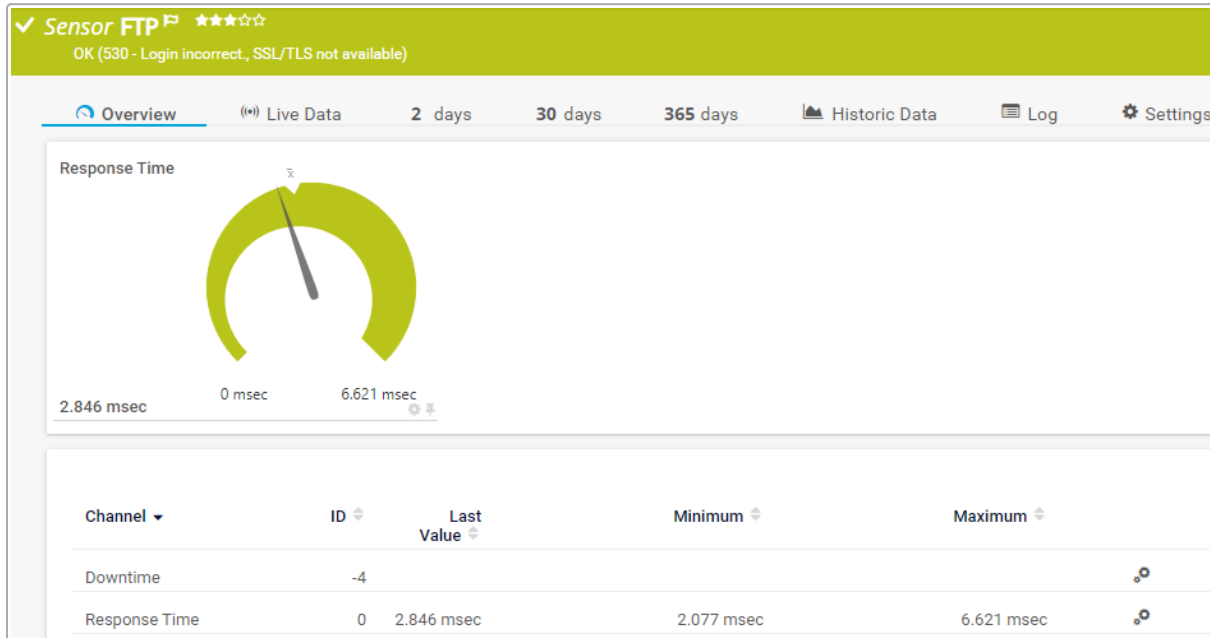
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

### 7.8.53 FTP Sensor

The FTP sensor monitors file servers via the File Transfer Protocol (FTP) and FTP over SSL (FTPS).

**i** This sensor also shows the response message of the server in the sensor message.



FTP Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

#### Sensor in Other Languages

- Dutch: FTP
- French: FTP
- German: FTP
- Japanese: FTP
- Portuguese: FTP
- Russian: FTP
- Simplified Chinese: FTP
- Spanish: FTP

#### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv4	This sensor only supports IPv4.
Performance impact	This sensor has a <b>medium</b> performance impact.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- ftpsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Specific

#### Sensor Specific

**Timeout (Sec.)** ⓘ

**Port** ⓘ

**FTP Mode** ⓘ  Active mode  
 Passive mode (default)

Sensor Specific

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p> ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

Setting	Description
Port	<p>Enter the number of the FTP port that the sensor tries to connect to. Enter an integer. The default port number is 21.</p> <p><b>i</b> We recommend that you use the default value.</p> <p><b>i</b> If the connection is unsuccessful, try a different port number.</p>
FTP Mode	<p>Define the FTP connection mode that the sensor uses for the connection to the FTP server:</p> <ul style="list-style-type: none"> <li>Active mode: Try to establish a command channel by connecting to FTP port 21 and a data channel by connecting to FTP port 20. If you cannot establish a connection, use the passive mode.</li> <li>Passive mode (default): Try to establish a command channel by connecting to FTP port 21 and send a command to the FTP server in order to receive an FTP port for the data channel.</li> </ul> <p><b>i</b> We recommend that you use the default value.</p>

## Connection Security

**Connection Security**

**Transport-Level Security** **i**
 Use transport-level security if available  
 Enforce transport-level security  
 Do not use transport-level security

Connection Security

Setting	Description
Transport-Level Security	<p>Specify if the sensor uses connection security:</p> <ul style="list-style-type: none"> <li>Use transport-level security if available: This sensor tries to connect via Secure Sockets Layer (SSL)/Transport Layer Security (TLS). It automatically determines whether to connect via the explicit mode or the implicit mode. If the server does not support SSL/TLS, the sensor tries to connect without connection security and shows the Up status if this works.</li> <li>Enforce transport-level security: The connection <b>must</b> be established via SSL/TLS (in the explicit mode or the implicit mode). Otherwise, this sensor shows the Down status.</li> <li>Do not use transport-level security (default): The sensor connects to the FTP server without connection security.</li> </ul> <p><b>i</b> See the sensor logs to see which method the sensor previously used to connect to the FTP server.</p>



## Authentication

**Authentication**

User Name ⓘ johnqpublic

Password ⓘ .....

Result Handling ⓘ  Discard result (default)  
 Store result

Authentication

Setting	Description
User Name	<p>Enter a user name for the FTP login. Enter a string or leave the field empty.</p> <p> ⓘ The default user name is <a href="#">anonymous</a>. If the sensor cannot log on to the FTP server with this user name (or a different user name that you define), the sensor message shows that the credentials are incorrect but the sensor remains in the Up status.</p>
Password	<p>Enter a password for the FTP login. Enter a string or leave the field empty.</p> <p> ⓘ If the sensor cannot log on to the FTP server with this password, the sensor message shows that the credentials are incorrect but the sensor remains in the Up status.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Response Time	The response time  This channel is the primary channel by default.

## More

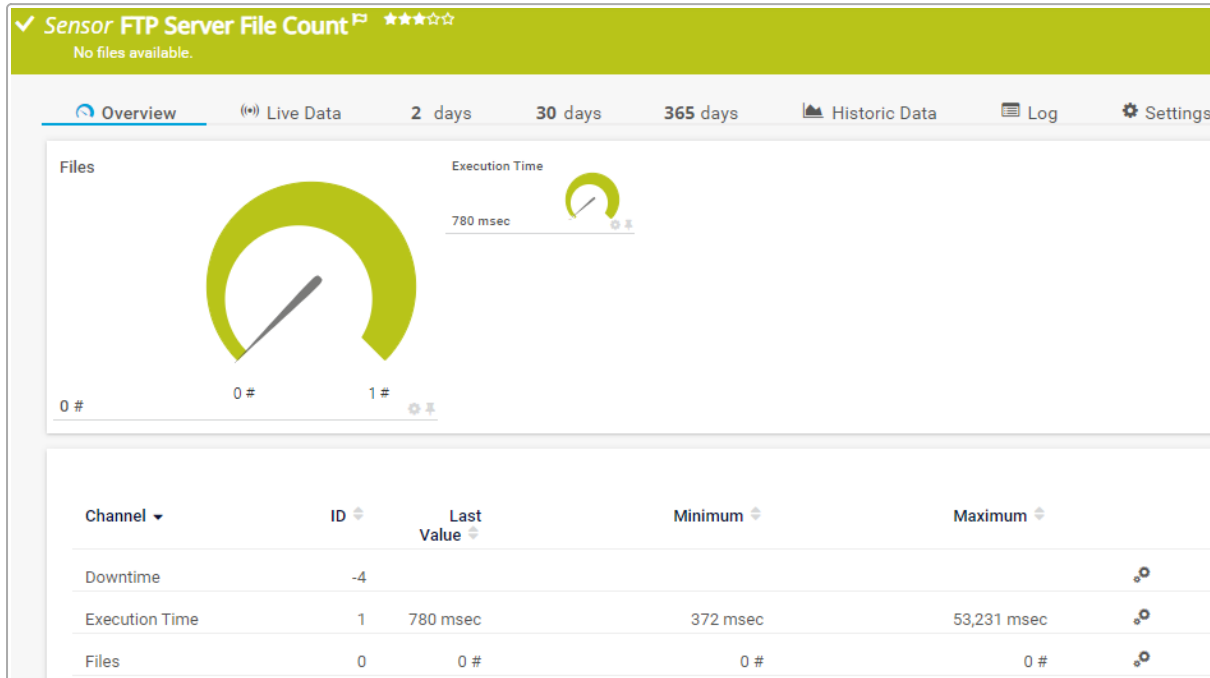
### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.54 FTP Server File Count Sensor

The FTP Server File Count sensor logs in to a File Transfer Protocol (FTP) server and can monitor changes to files.



FTP Server File Count Sensor



For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: FTP Server File Aantal
- French: Serveur FTP compteur de fichiers
- German: FTP-Server Dateianzahl
- Japanese: FTP サーバーファイルカウント
- Portuguese: Contagem de arquivos servidor FTP
- Russian: Количество файлов на FTP-сервере
- Simplified Chinese: FTP 服务器文件计数
- Spanish: Número de archivos en servidor FTP

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node. If the sensor shows the error PE087, additionally install .NET 3.5 on the probe system.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Windows Server	We recommend Windows Server 2016 on the probe system for best performance of this sensor.
IPv6	This sensor supports IPv6.

## Basic Sensor Settings

**Basic Sensor Settings**

Sensor Name ⓘ Example Name

---

Tags ⓘ  X +

---

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- ptfsensor

 For more information about basic sensor settings, see section [Sensor Settings](#) .

## Sensor Settings

### Sensor Settings

**FTP Mode** ⓘ  Active mode  
 Passive mode

**Check Method** ⓘ  URL  
 Folder on parent device

**FTP URL** ⓘ

**User Name** ⓘ

**Password** ⓘ

**File Count** ⓘ  Total number of files  
 Only new files



**Connection Security** ⓘ  Do not use transport-level security  
 Enforce transport-level security

**If Value Changes** ⓘ  Ignore (default)  
 Trigger 'change' notification

Sensor Settings


Setting	Description
FTP Mode	<p>Define the FTP connection mode that the sensor uses for the connection to the FTP server:</p> <ul style="list-style-type: none"> <li>▪ Active mode: If you cannot establish a connection, use the passive mode.</li> </ul> <p> ⓘ We recommend that you use the default value.</p> <ul style="list-style-type: none"> <li>▪ Passive mode</li> </ul>
Check Method	<p>Define how to access the FTP server directory that this sensor monitors:</p> <ul style="list-style-type: none"> <li>▪ URL: This sensor uses a URL of an FTP server to access the target directory. Define the URL below.</li> <li>▪ Folder on parent device: This sensor uses the IP address or Domain Name System (DNS) name of the parent device and monitors a folder on this device. Define the folder below.</li> </ul>

Setting	Description
FTP URL	<p>This setting is only visible if you select <a href="#">URL</a> above.</p> <p>Enter the URL that this sensor checks. The URL can look like this: <a href="#">ftp://10.0.0.1/upload</a></p> <p><b>i</b> If you use this method, this sensor does <b>not</b> use the IP Address/DNS Name of the parent device.</p> <p><b>i</b> You can add a port number to the URL by using a colon, for example <a href="#">ftp://10.0.0.1/upload:21</a>.</p>
FTP Port	<p>This setting is only visible if you select <a href="#">Folder</a> on parent device above.</p> <p>Enter the number of the port to which this sensor connects. The default port is <b>21</b>.</p>
FTP Folder	<p>This setting is only visible if you select <a href="#">Folder</a> on parent device above.</p> <p>Enter the name of the folder on the parent device that this sensor monitors, for example <a href="#">upload</a>.</p>
Recurse Subfolders	<p>This setting is only visible if you select <a href="#">Folder</a> on parent device above.</p> <p>Define if the sensor additionally monitors the subfolders of the FTP folder:</p> <ul style="list-style-type: none"> <li>▪ Do not recurse subfolders (default): Only monitor the folder. Do not monitor its subfolders.</li> <li>▪ Monitor the folder and its subfolders (recursive): Monitor the folder and all of its subfolders.</li> </ul> <p><b>i</b> If you recurse subfolders in large directories that have a high number of branches, this might cause timeout errors or performance issues.</p>
User Name	Enter the user name for the FTP server login. Enter a string.
Password	Define the password for the FTP server login. Enter a string.
File Count	<p>Define which files the sensor counts:</p> <ul style="list-style-type: none"> <li>▪ Total number of files: Always show the total number of all files in the folder.</li> <li>▪ Only new files: Only show the number of new files since the last scanning interval. You can define the frequency of sensor scans in section <a href="#">Scanning Interval</a> <small>1011</small>.</li> </ul> <p><b>i</b> With every scanning interval, the sensor considers any new files from the previous scanning interval to be old.</p>

Setting	Description
Connection Security	<p>Define the security of the connection:</p> <ul style="list-style-type: none"> <li>Do not use transport-level security (default): The sensor connects without connection security.</li> <li>Enforce transport-level security: The sensor establishes the connection to the FTP server via Secure Sockets Layer (SSL)/Transport Layer Security (TLS) in explicit mode.</li> </ul> <p> This sensor only supports SSL/TLS in explicit mode.</p>
If Value Changes	<p>Define what the sensor does when its value changes:</p> <ul style="list-style-type: none"> <li>Ignore (default): Do nothing.</li> <li>Trigger 'change' notification: Send an internal message that indicates a change.</li> </ul> <p> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</p>



## Debug Options

**Debug Options**

Result Handling 

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> </ul> <p>Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</p> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>



## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Execution Time	The execution time
Files	The number of files that are available in the directory listing  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

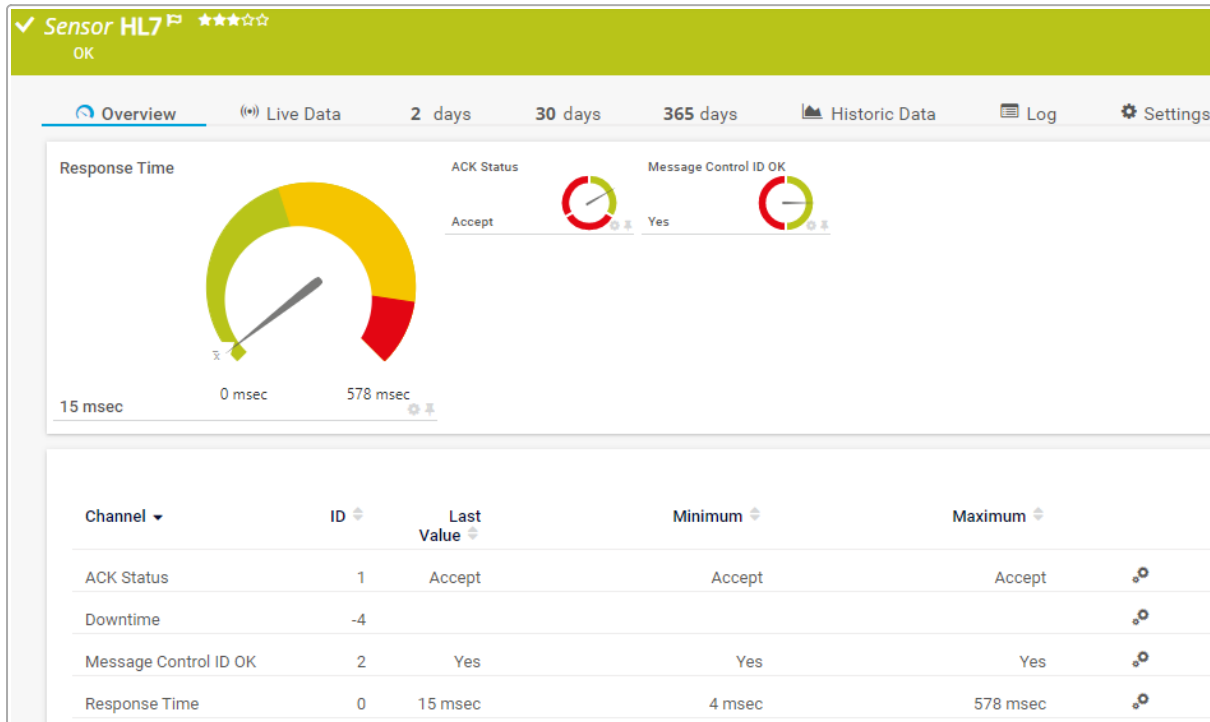
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.55 HL7 Sensor

The HL7 sensor monitors the availability of Health Level 7 (HL7) interfaces. It sends an HL7 message to the target device and checks for a valid response.

- ① You can define your own messages in HL7 format as .hl7 files in the [PRTG program directory](#). This sensor sends them to the HL7-capable system with each scanning interval.



HL7 Sensor



- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1018</sup>.

### Sensor in Other Languages

- Dutch: HL7
- French: HL7
- German: HL7
- Japanese: HL7
- Portuguese: HL7
- Russian: HL7
- Simplified Chinese: HL7
- Spanish: HL7

### Remarks

Consider the following [remarks](#)<sup>1013</sup> and requirements for this sensor:

Remark	Description
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★★★★☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- dicom
- hl7

 For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### HL7 Connection

#### HL7 Connection

**Port** ⓘ

**Timeout (Sec.)** ⓘ

HL7 Connection

Setting	Description
Port	Enter the port of the HL7 interface that the sensor uses for the connection. The default port is <b>1204</b> .
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).  <i>i</i> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.

### HL7 Message Specific

#### HL7 Message Specific

**Message Header** *i*

**HL7 Message** *i*




Default message header

Override message header

*ORM\_01\_MEDICO.hl7*


HL7 Message Specific

Setting	Description
Message Header	Define if you want to use the default message header (MSH) as defined in the selected .hl7 message file or if you want to override certain headers: <ul style="list-style-type: none"> <li>Default message header: Send the MSH as defined in the .hl7 message file.</li> <li>Override message header: Define a custom MSH below that overrides the MSH in the .hl7 message file.</li> </ul>
Sending Application	<b>This setting is only visible if you select <a href="#">Override message header</a> above.</b>  Enter the name of the sending application, for example, <b>PRTG</b> . It overrides the default value in the message. Enter a string.
Sending Facility	<b>This setting is only visible if you select <a href="#">Override message header</a> above.</b>  Enter the name of the sending facility. It overrides the default value in the message. Enter a string.
Receiving Application	<b>This setting is only visible if you select <a href="#">Override message header</a> above.</b>  Enter the name of the receiving application. It overrides the default value in the message. Enter a string.


Setting	Description
Receiving Facility	<p>This setting is only visible if you select <a href="#">Override message header</a> above.</p> <p>Enter the name of the receiving facility. It overrides the default value in the message. Enter a string.</p>
HL7 Message	<p>Select an .hl7 file from the list. This sensor sends it to the target device with every scanning interval.</p> <p>The list shows all files that are available in the \Custom Sensors\hl7 subfolder of the PRTG program directory on the probe system. For files to appear in this list, store them in this subfolder with the extension <a href="#">.hl7</a>.</p> <ul style="list-style-type: none"> <li> To be accepted by the HL7 interface, your files must have the expected HL7 message format. PRTG comes with two sample .hl7 message files that you can use to test your HL7 monitoring and to have a look at the expected format. These files are in the \Custom Sensors\hl7 subfolder.</li> <li> You can override certain headers using the Message Header sensor setting.</li> <li> You cannot change this value after sensor creation.</li> </ul>

## Debug Options

**Debug Options**

**Result Handling** 
  
 Discard result (default)
   
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime


---

Graph Type **i**
 Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>+</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
ACK Status	The acknowledgment (ACK) status <ul style="list-style-type: none"> <li>▪ Up status: Accept</li> <li>▪ Down status: Error, Reject</li> </ul>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Message Control ID OK	The message control ID status <ul style="list-style-type: none"> <li>▪ Up status: Yes</li> <li>▪ Down status: No</li> </ul>
Response Time	The response time <p>ⓘ This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

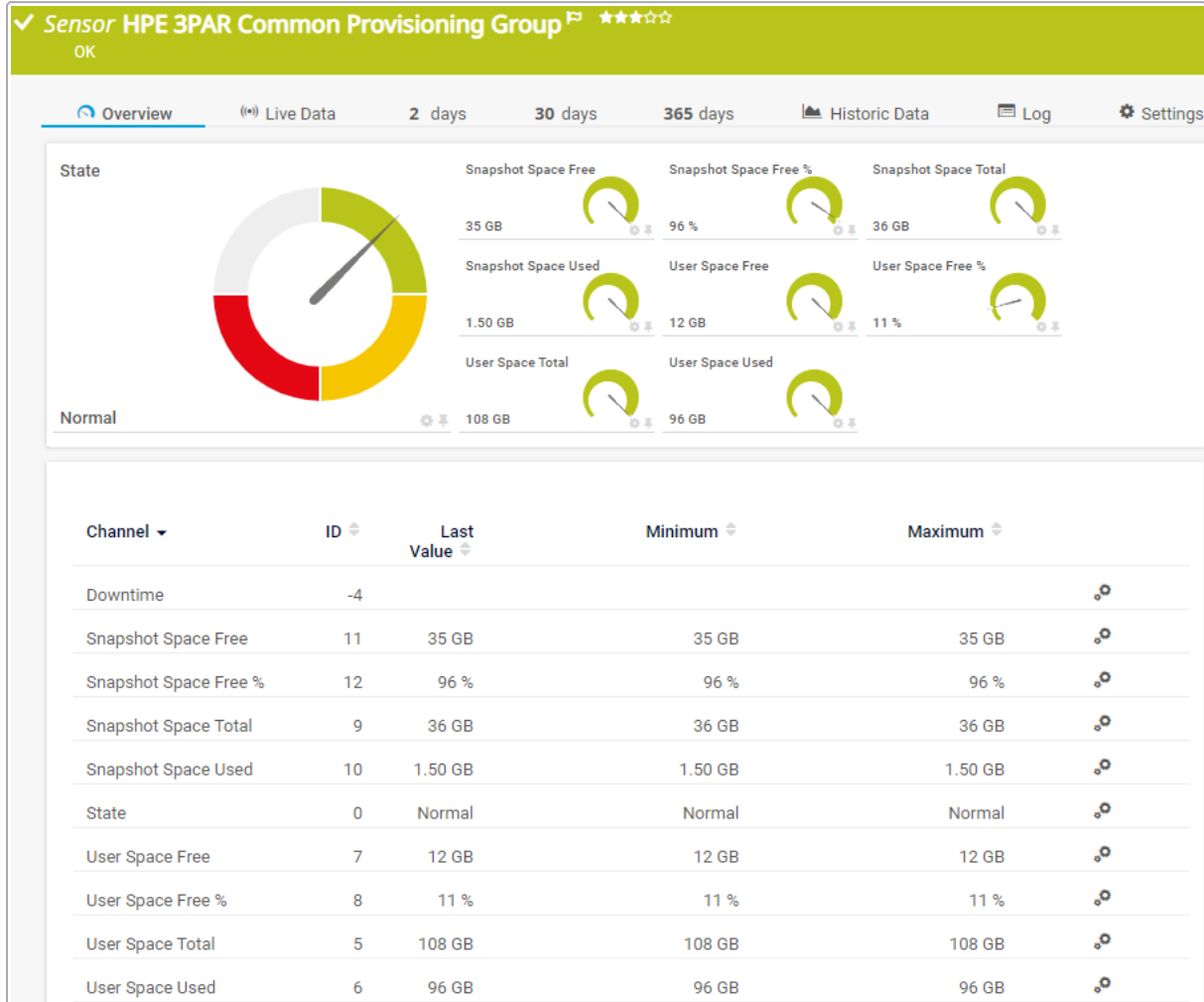
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>



## 7.8.56 HPE 3PAR Common Provisioning Group Sensor

The HPE 3PAR Common Provisioning Group sensor monitors the capacity of a Common Provisioning Group (CPG) on an HPE 3PAR storage system.



HPE 3PAR Common Provisioning Group Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1023]</sup>.

### Sensor in Other Languages

- Dutch: HPE 3PAR Common Provisioning Group
- French: HPE 3PAR groupe de provisionnement commun
- German: HPE 3PAR Common Provisioning-Gruppe
- Japanese: HPE 3PAR 共通プロビジョニンググループ
- Portuguese: Grupo de provisionamento comum do HPE 3PAR
- Russian: Общая группа подготовки HPE 3PAR
- Simplified Chinese: HPE 3PAR 通用配置群组

- Spanish: Grupo de suministro común HPE 3PAR

## Remarks

Consider the following [remarks](#) <sup>1020</sup> and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for HPE 3PAR.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <b>1 minute</b>.</li> <li>▪ The recommended scanning interval of this sensor is <b>5 minutes</b>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.
Knowledge Base	Knowledge Base: <a href="#">Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

**Tags** ⓘ exampletag ✕ ⊕

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cpg
- hpe
- hpe3par
- rest

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### HPE 3PAR Specific

**HPE 3PAR Specific**

Name ⓘ *example*

ID ⓘ *7*

Virtual Domain ⓘ *n/a*

HPE 3PAR Specific

Setting	Description
Name	The name of the CPG that this sensor monitors.
ID	The ID of the CPG that this sensor monitors.
Virtual Domain	The virtual domain to which the CPG that this sensor monitors belongs.

### Sensor Display


**Sensor Display**

Primary Channel ⓘ *Downtime*

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>



## Debug Options

**Debug Options**


Result Handling 

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Logical Space Free	The free logical space
Logical Space Free %	The free logical space (%)
Logical Space Total	The allocated logical space
Logical Space Used	The space that is already in use
Snapshot Space Free	The free snapshot space
Snapshot Space Free %	The free snapshot space (%)
Snapshot Space Total	The allocated snapshot space
Snapshot Space Used	The snapshot space that is already in use
State	<p>The CPG status</p> <ul style="list-style-type: none"> <li>▪ Up status: Normal</li> <li>▪ Warning status: Degraded</li> <li>▪ Down status: Failed</li> <li>▪ Unknown status: Unknown</li> </ul> <p>ⓘ This channel is the primary channel by default.</p>
User Space Free	The free user space
User Space Free %	The free user space (%)
User Space Total	The allocated user space

Channel	Description
User Space Used	The user space that is already in use

## More

### KNOWLEDGE BASE

Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?

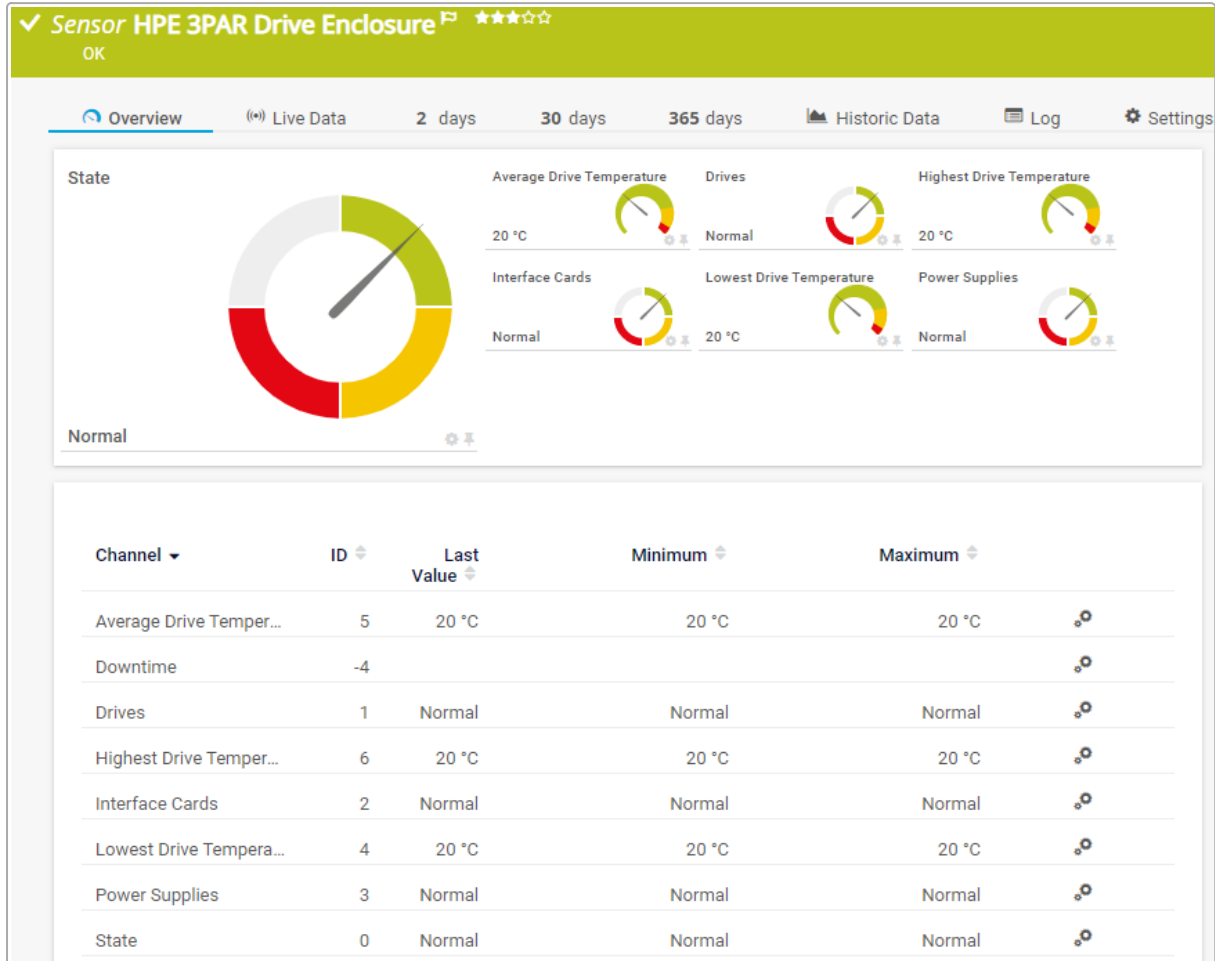
- <https://kb.paessler.com/en/topic/89717>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.57 HPE 3PAR Drive Enclosure Sensor

The HPE 3PAR Drive Enclosure sensor monitors a drive enclosure of an HPE 3PAR storage system.



HPE 3PAR Drive Enclosure Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: HPE 3PAR Schijfbehuizing
- French: HPE 3PAR boîtier de lecteurs
- German: HPE 3PAR Laufwerksgehäuse
- Japanese: HPE 3PAR ドライブエンクロージャ
- Portuguese: Gabinete de unidades do HPE 3PAR
- Russian: Дисковая полка HPE 3PAR
- Simplified Chinese: HPE 3PAR 驱动器机箱
- Spanish: Gabinete de una unidad de disco HPE 3PAR

## Remarks

Consider the following [remarks](#)<sup>[1026]</sup> and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for HPE 3PAR.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Scanning interval	<ul style="list-style-type: none"> <li>The minimum scanning interval of this sensor is <b>1 minute</b>.</li> <li>The recommended scanning interval of this sensor is <b>5 minutes</b>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.
Knowledge Base	Knowledge Base: <a href="#">Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  X +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- enclosure
- hpe
- hpe3par
- ssh

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.



## HPE 3PAR Specific

**HPE 3PAR Specific**

**ID** ⓘ 0

**Enclosure Name** ⓘ Example

**Drive Count** ⓘ 24

**Model** ⓘ DCS8

**Form Factor** ⓘ SFF

HPE 3PAR Specific

Setting	Description
ID	The ID of the drive enclosure that this sensor monitors.
Enclosure Name	The name of the drive enclosure that this sensor monitors.
Drive Count	The number of drives in the enclosure that this sensor monitors.
Model	The model of the drive enclosure that this sensor monitors.
Form Factor	The form factor of the drive bays of the enclosure that this sensor monitors.

## Sensor Display


**Sensor Display**

**Primary Channel** ⓘ Downtime

**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.


Setting	Description
	<p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.           <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

**Result Handling** 
  
 Discard result (default)
   
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Average Drive Temperature	The average temperature of all drives in the drive bay  This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: 60°C</li> <li>▪ Upper warning limit: 50°C</li> </ul>
Drives	The drives status <ul style="list-style-type: none"> <li>▪ Up status: Normal</li> <li>▪ Warning status: Degraded</li> <li>▪ Down status: Failed</li> <li>▪ Unknown status: Unknown</li> </ul>
Highest Drive Temperature	The highest temperature of all drives in the drive bay  This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: 60°C</li> <li>▪ Upper warning limit: 50°C</li> </ul>
Interface Cards	The interface cards status <ul style="list-style-type: none"> <li>▪ Up status: Normal</li> <li>▪ Warning status: Degraded</li> <li>▪ Down status: Failed</li> </ul>

Channel	Description
	<ul style="list-style-type: none"> <li>Unknown status: Unknown</li> </ul>
Lowest Drive Temperature	<p>The lowest temperature of all drives in the drive bay</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>Upper error limit: 60°C</li> <li>Upper warning limit: 50°C</li> </ul>
Power Supplies	<p>The power supplies status</p> <ul style="list-style-type: none"> <li>Up status: Normal</li> <li>Warning status: Degraded</li> <li>Down status: Failed</li> <li>Unknown status: Unknown</li> </ul>
State	<p>The drive enclosure status</p> <ul style="list-style-type: none"> <li>Up status: Normal</li> <li>Warning status: Degraded</li> <li>Down status: Failed</li> <li>Unknown status: Unknown</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?

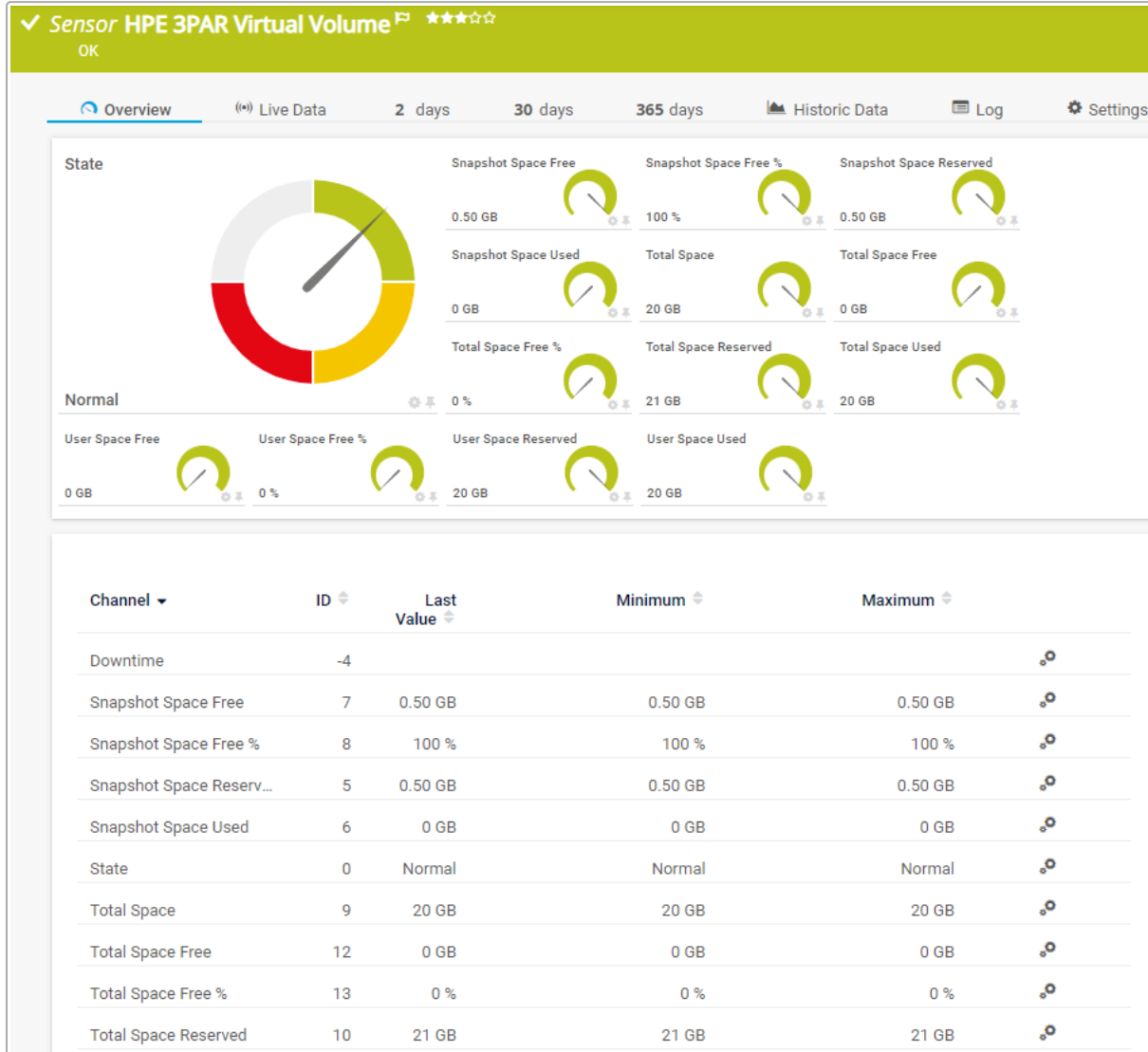
- <https://kb.paessler.com/en/topic/89717>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.58 HPE 3PAR Virtual Volume Sensor

The HPE 3PAR Virtual Volume sensor monitors the capacity of a virtual volume on an HPE 3PAR storage system.



HPE 3PAR Virtual Volume Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1035]</sup>.

### Sensor in Other Languages

- Dutch: HPE 3PAR Virtueel Volume
- French: HPE 3PAR volume virtuel
- German: HPE 3PAR Virtual Volume
- Japanese: HPE 3PAR 仮想ボリューム
- Portuguese: Volume virtual HPE 3PAR
- Russian: Виртуальный том HPE 3PAR

- Simplified Chinese: HPE 3PAR 虚拟卷
- Spanish: Volumen virtual HPE 3PAR

## Remarks

Consider the following [remarks](#)<sup>1032</sup> and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for HPE 3PAR.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <b>1 minute</b>.</li> <li>▪ The recommended scanning interval of this sensor is <b>5 minutes</b>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.
Knowledge Base	Knowledge Base: <a href="#">Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- hpe
- hpe3par
- rest
- virtualvolume

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## HPE 3PAR Specific

**HPE 3PAR Specific**

Name ⓘ *Example*

Provisioning Type ⓘ *Full*

Volume Type ⓘ *Base*

HPE 3PAR Specific

Setting	Description
Name	The name of the virtual volume that this sensor monitors.
Provisioning Type	The provisioning type of the virtual volume that this sensor monitors.
Volume Type	The volume type of the virtual volume that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ *Downtime*

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>

Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**

Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><span style="font-size: 0.8em;">☁</span> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><span style="font-size: 0.8em;">ⓘ</span> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).



## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Snapshot Space Free	The free snapshot space
Snapshot Space Free %	The free snapshot space (%)
Snapshot Space Reserved	The reserved snapshot space
Snapshot Space Used	The snapshot space that is already in use
State	<p>The overall virtual volume status</p> <ul style="list-style-type: none"> <li>▪ Up status: Normal</li> <li>▪ Warning status: Degraded</li> <li>▪ Down status: Failed</li> <li>▪ Unknown status: Unknown</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Total Space	The total space
Total Space Free	The total free space
Total Space Free %	The total free space (%)
Total Space Reserved	The total reserved space
Total Space Used	The total space that is in use
User Space Free	The free user space
User Space Free %	The free user space (%)

Channel	Description
User Space Reserved	The reserved user space
User Space Used	The user space that is already in use

## More

### ■ KNOWLEDGE BASE

Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?

- <https://kb.paessler.com/en/topic/89717>

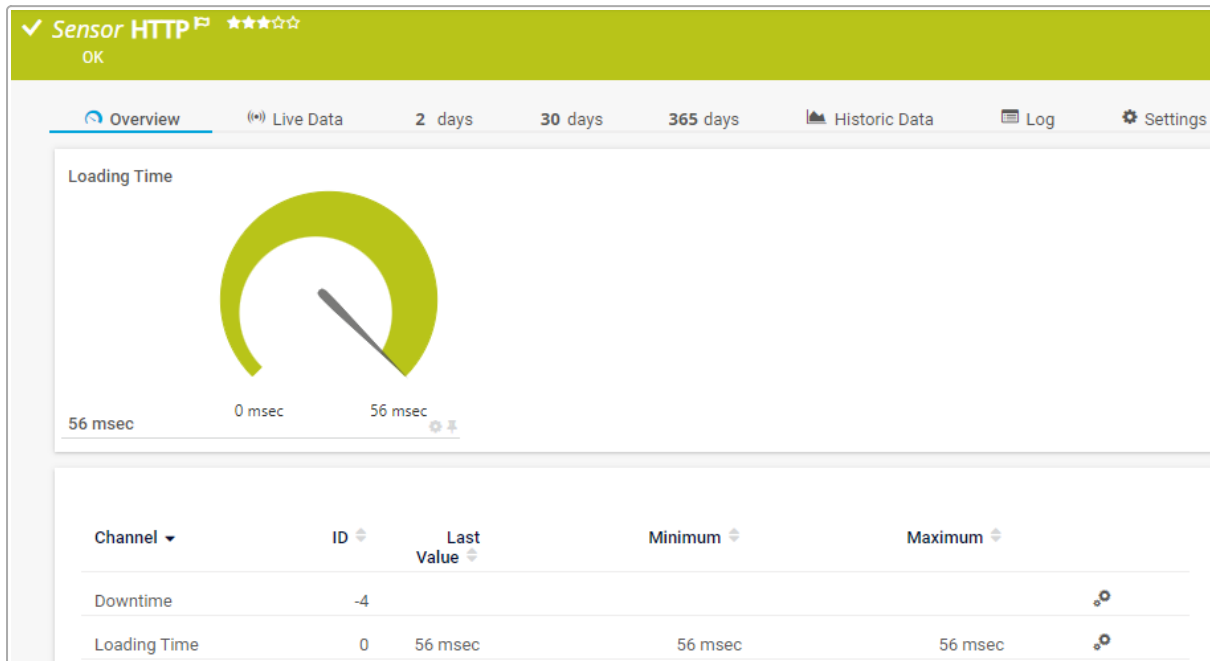
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.59 HTTP Sensor

The HTTP sensor monitors a web server using HTTP.

**i** You can use this sensor to monitor if a website or a specific website element is reachable.



HTTP Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1042]</sup>.

### Sensor in Other Languages

- Dutch: HTTP
- French: HTTP
- German: HTTP
- Japanese: HTTP
- Portuguese: HTTP
- Russian: HTTP
- Simplified Chinese: HTTP
- Spanish: HTTP

### Remarks

Consider the following [remarks](#)<sup>[1037]</sup> and requirements for this sensor:

Remark	Description
SRP ciphers	This sensor does not support Secure Remote Password (SRP) ciphers.
Smart URL replacement	This sensor supports <a href="#">smart URL replacement</a> <sup>[1042]</sup> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">My HTTP sensors fail to monitor websites which use SNI. What can I do?</a></li> <li>Knowledge Base: <a href="#">Which HTTP status code leads to which HTTP sensor status?</a></li> </ul>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- httpsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## HTTP Specific

**HTTP Specific**

Timeout (Sec.) ⓘ 60

---

URL ⓘ https://example.com

---

Request Method ⓘ  GET (default)  
 POST  
 HEAD

Server Name Indication ⓘ example.com

SNI Inheritance ⓘ  Inherit SNI from parent device (default)  
 Do not inherit SNI from parent device

HTTP Specific

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is 900 seconds (15 minutes).</p> <p> ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
URL	<p>Enter the URL that the sensor connects to.</p> <p>If you enter an absolute URL, the sensor uses this address independently of the IP Address/DNS Name setting of the parent device. You can enter the URL of a web page (to measure the loading time of the page's source code), or enter the URL of an image or of a page asset to measure this element's availability and loading time.</p> <p> ⓘ The URL must be <a href="#">URL encoded</a>.</p> <p> ⓘ If you monitor an image or a page asset, this can create a high amount of memory load. We recommend that the size of the elements that you want to monitor does not exceed 200 MB.</p> <p> ■ PRTG uses a smart URL replacement with which you can use the parent device's IP address or Domain Name System (DNS) name setting as part of the URL. For more information, see section <a href="#">Smart URL Replacement</a><sup>[1042]</sup>.</p>
Request Method	<p>Select an HTTP request method to determine how the sensor requests the URL:</p> <ul style="list-style-type: none"> <li>▪ GET (default): Directly request the website. <ul style="list-style-type: none"> <li> ⓘ We recommend that you use this setting for a simple check of the web page.</li> </ul> </li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ POST: Send post form data to the URL. <ul style="list-style-type: none"> <li>❗ If you select this setting, you must enter the data in the Postdata field below.</li> <li>❗ If a POST request is redirected, all further requests are GET (default) requests.</li> </ul> </li> <li>▪ HEAD: Only request the HTTP header from the server without the actual web page. <ul style="list-style-type: none"> <li>❗ Although this saves bandwidth because it transfers less data, we do not recommend that you use this. This is because the measured request time is not the one that your users experience and you might not be notified of slow results or timeouts.</li> </ul> </li> </ul>
Postdata	<p>This setting is only visible if you select POST above.</p> <p>Enter the data part for the POST request.</p> <ul style="list-style-type: none"> <li>❗ No Extensible Markup Language (XML) is allowed here.</li> </ul>
Content Type	<p>This setting is only visible if you select POST above.</p> <p>Define the content type of the POST request:</p> <ul style="list-style-type: none"> <li>▪ Default (application/x-www-form-urlencoded): Use the default content type to encode the form data set for submission to the server.</li> <li>▪ Custom: Use a custom content type. Enter the content type below.</li> </ul>
Custom Content Type	<p>This setting is only visible if you select Custom above.</p> <p>Define the custom content type, for example, XML, JavaScript Object Notation (JSON), or HTTP.</p>
Server Name Indication	<p>The Server Name Indication (SNI) that the sensor automatically determines from the host address of the <a href="#">parent device</a> or from the target URL of the sensor.</p> <ul style="list-style-type: none"> <li>❗ The SNI must be a fully qualified domain name (FQDN). Make sure that it matches the configuration of the target server.</li> </ul> <p>■ For more information, see the Knowledge Base: <a href="#">My HTTP sensors fail to monitor websites which use SNI. What can I do?</a></p> <ul style="list-style-type: none"> <li>❗ This sensor implicitly supports SNI, an extension to the Transport Layer Security (TLS) protocol.</li> </ul>
SNI Inheritance	<p>Define if you want to inherit the SNI from the parent device:</p> <ul style="list-style-type: none"> <li>▪ Inherit SNI from parent device: Determine the SNI from the host address of the parent device.</li> <li>▪ Do not inherit SNI from parent device: Determine the SNI from the target URL as defined in the settings of this sensor.</li> </ul>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can only enter the protocol followed by a colon and three forward slashes (this means that you can enter either <http://> or <https://>, or even a simple forward slash / as the equivalent for <http://>). PRTG automatically fills in the parent device's IP Address/DNS Name in front of the third forward slash.


Whether this results in a valid URL or not depends on the IP address or Domain Name System (DNS) name of the parent device. In combination with cloning devices, you can use smart URL replacement to create many similar devices.


For example, if you create a device with the DNS name [www.example.com](http://www.example.com) and you add an HTTP sensor to it, you can provide values in the following ways:

- If you enter <https://> in the URL field, PRTG automatically creates the URL <https://www.example.com/>
- If you enter [/help](http://www.example.com/help) in the URL field, PRTG automatically creates and monitor the URL <http://www.example.com/help>
- It is also possible to provide a port number in the URL field. It is taken over by the device's DNS name and is internally added, for example, <http://:8080/>

 Smart URL replacement does not work for sensors that run on the probe device.

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Loading Time	The web page or element loading time  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

My HTTP sensors fail to monitor websites which use SNI. What can I do?

- <https://kb.paessler.com/en/topic/67398>

Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

What security features does PRTG include?



- <https://kb.paessler.com/en/topic/61108>

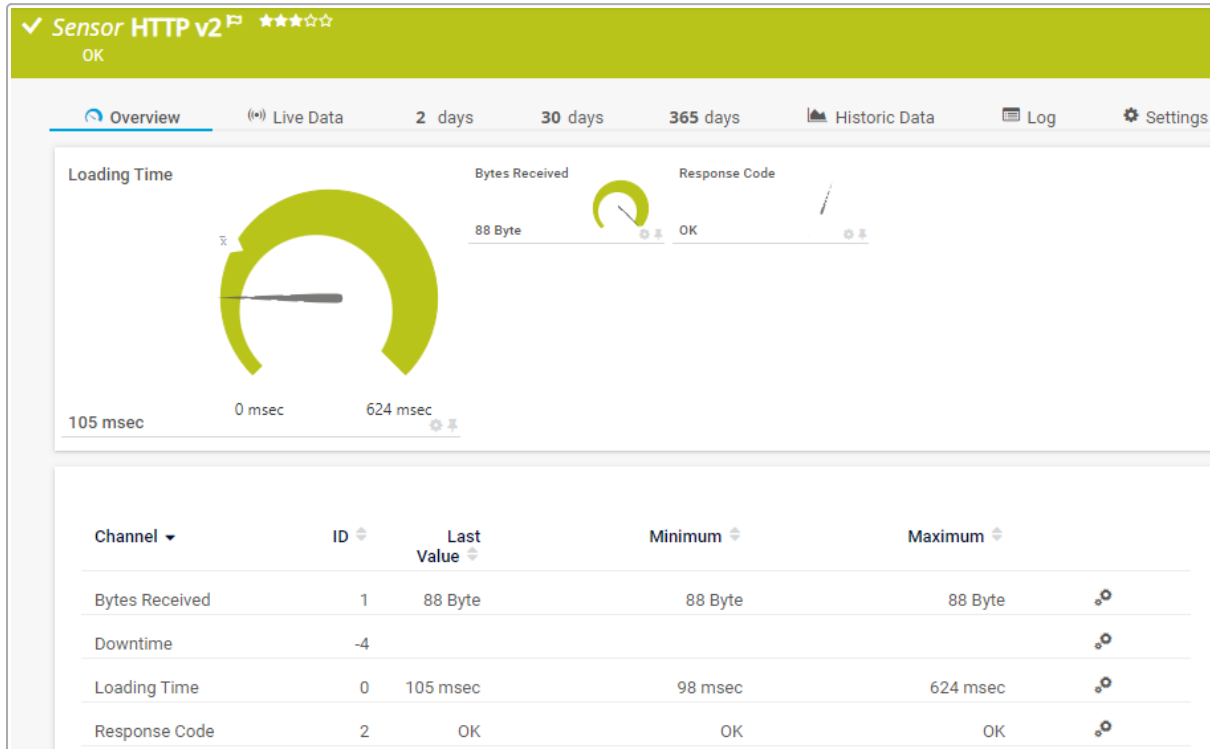
My HTTP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/85284>

## 7.8.60 HTTP v2 Sensor

The HTTP v2 sensor monitors a web server using the Hypertext Transfer Protocol (HTTP).

**i** You can use this sensor to monitor if a website or a specific website element is reachable.



HTTP v2 Sensor

**■** For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1050]</sup>.

### Sensor in Other Languages

- Dutch: HTTP v2
- French: HTTP v2
- German: HTTP v2
- Japanese: HTTP v2
- Portuguese: HTTP v2
- Russian: HTTP v2
- Simplified Chinese: HTTP v2
- Spanish: HTTP v2

### Remarks

Consider the following [remarks](#)<sup>[1044]</sup> and requirements for this sensor:

Remark	Description
Smart URL replacement	This sensor supports <a href="#">smart URL replacement</a> <sup>11049</sup> .
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Credentials	You can define credentials for HTTP in the settings of an object that is higher in the <a href="#">object hierarchy</a> .
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">1 minute</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.
Knowledge Base	Knowledge Base: <a href="#">Which HTTP status code leads to which HTTP sensor status?</a>

## Basic Sensor Settings

### Basic Sensor Settings

Sensor Name ⓘ

Example Name

Tags ⓘ

exampletag ✕ +

Priority ⓘ

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- http
- httpsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

HTTP Specific

### HTTP Specific

**Timeout per Request (Sec.)** ⓘ 30

---

**Maximum Number of Redirects** ⓘ 16

---

**URL** ⓘ https://%host/

---

**Request Method** ⓘ

GET (default)

POST

HEAD

---

**Custom Headers** ⓘ

HTTP Specific

Setting	Description
Timeout per Request (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is 900 seconds (15 minutes).</p> <p>ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p> <p>ⓘ The timeout is per request, not per sensor scan. If a request is redirected, the timeout begins again.</p>
Maximum Number of Redirects	<p>Enter the maximum number of times the sensor scan will follow an HTTP redirect request. The sensor will display the status of the last page before the number of redirects is exhausted. The default number of redirects the sensor will follow is 16. The maximum number of redirects the sensor will follow is 100. Enter 0 if you do not want the sensor to follow any redirects.</p>
URL	<p>Enter the URL that the sensor connects to.</p>

Setting	Description
	<p>If you enter an absolute URL, the sensor uses this address independently of the IP Address/DNS Name setting of the parent device. You can enter the URL of a web page (to measure the loading time of the page's source code), or enter the URL of an image or of a page asset to measure this element's availability and loading time.</p> <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> The URL must be <a href="#">URL encoded</a>.</li> <li><span style="color: red;">❗</span> If you monitor an image or a page asset, this can create a high amount of memory load. We recommend that the size of the elements that you want to monitor does not exceed 200 MB.</li> <li><span style="color: red;">❗</span> The default URL is <a href="https://%host/">https://%host/</a>. PRTG replaces <a href="#">%host</a> with the IP address or DNS name of the parent device. PRTG does not display the value in the sensor log or the sensor's settings.</li> </ul>
Request Method	<p>Select an HTTP request method to determine how the sensor requests the URL:</p> <ul style="list-style-type: none"> <li>▪ GET (default): Directly request the website. <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> We recommend that you use this setting for a simple check of the web page.</li> </ul> </li> <li>▪ POST: Send post form data to the URL. <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> If you select this setting, you must enter the data in the POST Body field below.</li> <li><span style="color: red;">❗</span> If a POST request is redirected, all further requests are GET (default) requests.</li> </ul> </li> <li>▪ HEAD: Only request the HTTP header from the server without the actual web page. <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> Although this saves bandwidth because it transfers less data, we do not recommend that you use this. This is because the measured request time is not the one that your users experience and you might not be notified of slow results or timeouts.</li> </ul> </li> </ul>
Content Type	<p><a href="#">This setting is only visible if you select POST above.</a></p> <p>Define the content type of the POST request. The default content type is <a href="#">application/x-www-form-urlencoded</a>.</p>
POST Body	<p><a href="#">This setting is only visible if you select POST above.</a></p> <p>Enter the data part for the POST request.</p> <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> No Extensible Markup Language (XML) is allowed here.</li> </ul>
Custom Headers	<p>Enter a list of custom headers with their respective values that the HTTP request of the sensor contains. The syntax of a header-value pair is <a href="#">header1:value1</a>.</p>

Setting	Description
	<p><b>i</b> If you enter more than one header-value pair, enter each pair in one line: header1:value1 header2:value2 header3:value3</p> <p><b>i</b> Make sure that the HTTP header statement is valid. Otherwise, the sensor request cannot be successful.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⚙</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

## Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can only enter the protocol followed by a colon and three forward slashes (this means that you can enter either [http://](#) or [https://](#), or even a simple forward slash / as the equivalent for [http://](#)). PRTG automatically fills in the parent device's IP Address/DNS Name in front of the third forward slash.

Whether this results in a valid URL or not depends on the IP address or Domain Name System (DNS) name of the parent device. In combination with cloning devices, you can use smart URL replacement to create many similar devices.

For example, if you create a device with the DNS name [www.example.com](#) and you add an HTTP sensor to it, you can provide values in the following ways:

- If you enter [https://](#) in the URL field, PRTG automatically creates the URL [https://www.example.com/](#)
- If you enter [/help](#) in the URL field, PRTG automatically creates and monitor the URL [http://www.example.com/help](#)

- It is also possible to provide a port number in the URL field. It is taken over by the device's DNS name and is internally added, for example, <http://:8080/>

**i** Smart URL replacement does not work for sensors that run on the probe device.

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Bytes Received	The number of bytes received
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Loading Time	The web page or element loading time <b>i</b> This channel is the primary channel by default.
Response Code	The response code of the target server

## More

### ■ KNOWLEDGE BASE

Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

What security features does PRTG include?

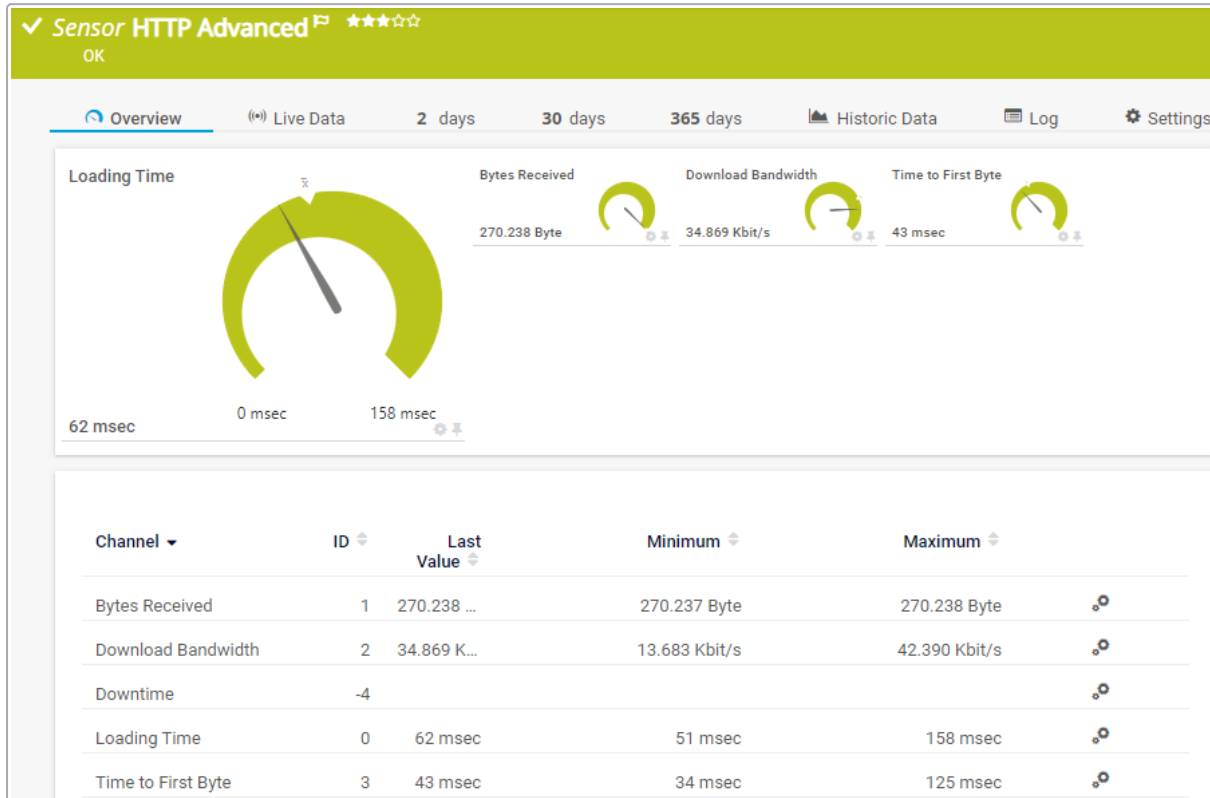
- <https://kb.paessler.com/en/topic/61108>



## 7.8.61 HTTP Advanced Sensor

The HTTP Advanced sensor monitors the source code of a web page using HTTP. It supports authentication, content checks, and other advanced parameters.

**i** The monitored content size is uncompressed.



HTTP Advanced Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: HTTP Geavanceerd
- French: HTTP avancé
- German: HTTP (Erweitert)
- Japanese: HTTP アドバンスト
- Portuguese: HTTP (avançado)
- Russian: HTTP (расширенный)
- Simplified Chinese: HTTP 高级
- Spanish: HTTP (avanzado)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
SRP ciphers	This sensor does not support Secure Remote Password (SRP) ciphers. If you need to use SRP ciphers, use the Compatibility engine.
HTTP compression	This sensor does not support HTTP compression. If you need to use it anyway, select Compatibility engine in the sensor settings.
Smart URL replacement	This sensor supports <a href="#">smart URL replacement</a> <sup>110621</sup> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
Fast internet connections	Bandwidth monitoring of fast internet connections might be inaccurate.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">Which user agent should I use in the HTTP Advanced sensor's settings?</a></li> <li>Knowledge Base: <a href="#">My HTTP sensors fail to monitor websites which use SNI. What can I do?</a></li> <li>Knowledge Base: <a href="#">Which HTTP status code leads to which HTTP sensor status?</a></li> </ul>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- httpsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>6671</sup>.

## HTTP Specific

**HTTP Specific**

Timeout (Sec.) ⓘ 60

---

URL ⓘ https://example.com

---

Request Method ⓘ  GET (default)  
 POST  
 HEAD

---

Server Name Indication ⓘ example.com

---

SNI Inheritance ⓘ  Inherit SNI from parent device (default)  
 Do not inherit SNI from parent device

HTTP Specific

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p>ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
URL	<p>Enter the URL that the sensor connects to.</p> <p>If you enter an absolute URL, the sensor uses this address independently of the IP Address/DNS Name setting of the parent device. You can enter the URL of a web page (to measure the loading time of the page's source code), or enter the URL of an image or of a page asset to measure this element's availability and loading time.</p> <p>ⓘ The URL must be <a href="#">URL encoded</a>.</p> <p>ⓘ If you monitor an image or a page asset, this can create a high amount of memory load. We recommend that the size of the elements that you want to monitor does not exceed 200 MB.</p> <p>■ PRTG uses a smart URL replacement with which you can use the parent device's IP address or Domain Name System (DNS) name setting as part of the URL. For more information, see section <a href="#">Smart URL Replacement</a> <sup>1062</sup>.</p>
Request Method	<p>Select an HTTP request method to determine how the sensor requests the URL:</p> <ul style="list-style-type: none"> <li>▪ GET (default): Directly request the website.</li> </ul> <p>ⓘ We recommend that you use this setting for a simple check of the web page.</p>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ <b>POST:</b> Send post form data to the URL.               <ul style="list-style-type: none"> <li>❗ If you select this setting, you must enter the data in the Postdata field below.</li> <li>❗ If a POST request is redirected, all further requests are GET (default) requests.</li> </ul> </li> <li>▪ <b>HEAD:</b> Only request the HTTP header from the server without the actual web page.               <ul style="list-style-type: none"> <li>❗ Although this saves bandwidth because it transfers less data, we do not recommended that you use this. This is because the measured request time is not the one that your users experience and you might not be notified of slow results or timeouts.</li> </ul> </li> </ul>
Postdata	<p>This setting is only visible if you select <b>POST</b> above.</p> <p>Enter the data part for the POST request.</p> <p>❗ No Extensible Markup Language (XML) is allowed here.</p>
Content Type	<p>This setting is only visible if you select <b>POST</b> above.</p> <p>Define the content type of the POST request:</p> <ul style="list-style-type: none"> <li>▪ <b>Default (application/x-www-form-urlencoded):</b> Use the default content type to encode the form data set for submission to the server.</li> <li>▪ <b>Custom:</b> Use a custom content type. Enter the content type below.</li> </ul>
Custom Content Type	<p>This setting is only visible if you select <b>Custom</b> above.</p> <p>Define the custom content type, for example, XML, JavaScript Object Notation (JSON), or HTTP.</p>
Server Name Indication	<p>The Server Name Indication (SNI) that the sensor automatically determines from the host address of the <a href="#">parent device</a> or from the target URL of the sensor.</p> <p>❗ The SNI must be a fully qualified domain name (FQDN). Make sure that it matches the configuration of the target server.</p> <p>■ For more information, see the Knowledge Base: <a href="#">My HTTP sensors fail to monitor websites which use SNI. What can I do?</a></p> <p>❗ This sensor implicitly supports SNI, an extension to the Transport Layer Security (TLS) protocol.</p>
SNI Inheritance	<p>Define if you want to inherit the SNI from the parent device:</p> <ul style="list-style-type: none"> <li>▪ <b>Inherit SNI from parent device:</b> Determine the SNI from the host address of the parent device.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Do not inherit SNI from parent device: Determine the SNI from the target URL as defined in the settings of this sensor.</li> </ul>

## Monitoring Engine

**Monitoring Engine** Monitoring Engine ⓘ

Default  
 Compatibility engine

Monitoring Engine

Setting	Description
Monitoring Engine	<p>Choose the monitoring engine that the sensor uses:</p> <ul style="list-style-type: none"> <li>Default: Use the default monitoring engine.</li> <li>Compatibility engine: Execute an external executable program. Use this method as an alternative for websites that do not work with the default monitoring engine.               <ul style="list-style-type: none"> <li> ⓘ This method needs more resources but it can be helpful in some cases.</li> <li> ⓘ If you select the compatibility mode, the options for the SSL method are different. You can also check for trusted certificates. See below.</li> <li> ⓘ Smart URL Replacement does not work with the compatibility mode, so this sensor does <b>not</b> automatically use the IP Address/DNS Name of the parent device.</li> </ul> </li> </ul>
SSL/TLS Method	<p><b>This setting is only visible if you select Compatibility engine above.</b></p> <p>Select the SSL/TLS method:</p> <ul style="list-style-type: none"> <li>SSLv3</li> <li>TLS 1.0, TLS 1.1, TLS 1.2</li> <li>SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 (default)</li> </ul>
Check SSL Certificates	<p><b>This setting is only visible if you select Compatibility engine above.</b></p> <p>Specify if the sensor checks the certificate of the URL:</p> <ul style="list-style-type: none"> <li>Do not check certificates (default): Do not check the certificates of the web pages.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Check if certificates are trusted: Check the certificates of the web pages. If the certificate of the server is not trusted, the sensor shows the Down <a href="#">status</a> and displays a corresponding message.</li> </ul>

## Advanced Sensor Data

**Advanced Sensor Data**

**HTTP Version** ?  HTTP 1.0  
 HTTP 1.1 (default)

**User Agent** ?  Use the default string (default)  
 Use a custom string

**HTTP Headers** ?  Do not use custom HTTP headers (default)  
 Use custom HTTP headers

**If Content Changes** ?  Ignore (default)  
 Trigger 'change' notification

**Require Keyword** ?  Do not check for keyword (default)  
 Set sensor to warning status if keyword is missing  
 Set sensor to down status if keyword is missing

**Exclude Keyword** ?  Do not check for keyword (default)  
 Set sensor to warning status if keyword is found  
 Set sensor to down status if keyword is found

**Download Limit (KB)** ?

---

**Result Handling** ?  Discard result (default)  
 Store result








Advanced Sensor Data




Setting	Description
HTTP Version	Define the HTTP version that the sensor uses when it connects to the target URL: <ul style="list-style-type: none"> <li>HTTP 1.0: Use HTTP version 1.0.</li> <li>HTTP 1.1: Use HTTP version 1.1.</li> </ul>

Setting	Description
User Agent	<p>Choose which user agent string the sensor sends when it connects to the target URL:</p> <ul style="list-style-type: none"> <li>▪ Use the default string: Do not enter a specific user agent and use the default string. Usually, this is <a href="#">Mozilla/5.0 (compatible; PRTG Network Monitor (www.paessler.com); Windows)</a>.</li> <li>▪ Use a custom string: Use a custom user agent. Define the custom user agent below.</li> </ul>
Custom User Agent	<p><a href="#">This setting is only visible if you select Use a custom string above.</a></p> <p>Enter the string that the sensor uses as the user agent when it connects to the target URL.</p>
HTTP Headers	<p>Define if you want to send custom HTTP headers to the target URL:</p> <ul style="list-style-type: none"> <li>▪ Do not use custom HTTP headers: Do not use custom HTTP headers.</li> <li>▪ Use custom HTTP headers: Use custom headers. Define below.</li> </ul>
Custom HTTP Headers	<p><a href="#">This setting is only visible if you select Use custom HTTP headers above.</a></p> <p>Enter a list of custom HTTP headers and values that you want to transmit to the URL, each pair in one line. The syntax of a header-value pair is <a href="#">header1:value1</a></p> <ul style="list-style-type: none"> <li>❗ The sensor does not support the header field names <a href="#">user-agent</a>, <a href="#">content-length</a>, and <a href="#">host</a>.</li> <li>❗ Make sure that the HTTP header statement is valid. Otherwise, the sensor request cannot be successful.</li> </ul>
If Content Changes	<p>Define what the sensor does if the content of the web page changes:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> <li>▪ Trigger 'change' notification: Send an internal message that indicates a change. <ul style="list-style-type: none"> <li>❗ In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</li> </ul> </li> </ul>
Require Keyword	<p>Define if the sensor checks the result at the URL for keywords:</p> <ul style="list-style-type: none"> <li>▪ Do not check for keyword (default): Do not search for keywords in the result.</li> <li>▪ Set sensor to warning status if keyword is missing: Check if a keyword exists in the result. If it exists, set the sensor to the Warning status.</li> <li>▪ Set sensor to down status if keyword is missing: Check if a keyword exists in the result. If it exists, set the sensor to the Down status.</li> </ul>


Setting	Description
	<p><b>i</b> The content check is only intended for HTML websites and might not work with other target URLs. For example, binary files are not supported.</p> <p><b>i</b> This sensor loads the source code at the URL. If you set up a content check, only this source code is checked for the keywords. The code is not necessarily identical to the code used to display the page when opening the same URL in a web browser. This is because a reload might be configured or certain information might be inserted after loading, for example, via JavaScript.</p> <p><b>i</b> PRTG does not follow links to embedded objects nor does it execute scripts. Only the first page at the URL is loaded and checked against the expressions configured.</p>
Response Must Include	<p><a href="#">This setting is only visible if you select Set sensor to warning status if keyword is missing</a> or <a href="#">Set sensor to down status if keyword is missing above</a>.</p> <p>Define the search string that must be part of the source code at the URL. You can enter a simple string in plain text or a <a href="#">regular expression (regex)</a>.</p> <p><b>i</b> If the source code does <b>not</b> include the search pattern, the sensor shows the status defined above.</p> <p><b>i</b> The search string must be case-sensitive.</p>
Search Method	<p>Define the method with which you want to provide the search string:</p> <ul style="list-style-type: none"> <li>▪ Simple string search (default): Search for a simple string in plain text.</li> </ul> <p><b>i</b> The characters <b>*</b> and <b>?</b> work as placeholders. <b>*</b> stands for no number or any number of characters and <b>?</b> stands for exactly one character. You cannot change this behavior. The literal search for these characters is only possible with a regex.</p> <p><b>i</b> You can also search for HTML tags.</p> <ul style="list-style-type: none"> <li>▪ Regular expression: Search with a regex.</li> </ul> <p><b>i</b> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</p>
Exclude Keyword	<p>Define if the sensor checks the result at the URL for keywords:</p> <ul style="list-style-type: none"> <li>▪ Do not check for keyword (default): Do not search for keywords in the result.</li> <li>▪ Set sensor to warning status if keyword is found: Check if a keyword exists in the result. If it exists, set the sensor to the Warning status.</li> <li>▪ Set sensor to down status if keyword is found: Check if a keyword exists in the result. If it exists, set the sensor to the Warning status.</li> </ul>



Setting	Description
	<p> The content check is only intended for HTML websites and might not work with other target URLs. For example, binary files are not supported.</p>
Response Must Not Include	<p><a href="#">This setting is only visible if you select</a> Set sensor to warning status if keyword is found <a href="#">or</a> Set sensor to down status if keyword is found <a href="#">above</a>.</p> <p>Define the search string that must <b>not</b> be part of the source code at the specified URL. You can enter a simple string in plain text or a regular expression.</p> <p> The search string must be case-sensitive.</p> <p> If the data <b>does</b> include this string, the sensor shows the status defined above.</p>
Search Method	<p>Define the method with which you want to provide the search string:</p> <ul style="list-style-type: none"> <li>▪ Simple string search (default): Search for a simple string in plain text.</li> </ul> <p> The characters <b>*</b> and <b>?</b> work as placeholders. <b>*</b> stands for no number or any number of characters and <b>?</b> stands for exactly one character. You cannot change this behavior. The literal search for these characters is only possible with a regex.</p> <p> You can also search for HTML tags.</p> <ul style="list-style-type: none"> <li>▪ Regular expression: Search with a regex.</li> </ul> <p> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</p>
Download Limit (KB)	<p>Enter the maximum amount of data (in kilobytes) that the sensor transfers per request.</p> <p> If you set content checks, be aware that they might be incomplete because only the content downloaded up to this limit is checked for search expressions.</p>
Result Handling	<p>Define what the sensor does with the data loaded at the URL:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last result of the requested data in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID]-A.txt, and Result of Sensor [ID].Data.txt. This setting is for debugging purposes, especially in combination with content checks. PRTG overwrites these files with each scanning interval.</li> </ul>


Setting	Description
	<p> For debugging, select Store result to write the source code file to disk and to look up what exactly PRTG gets when it calls the URL. If the URL does not point to a web page but to a binary file, for example, to an image, you usually do not check for content.</p> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Authentication

**Authentication** Authentication 

Web page does not need authentication (default)  
 Web page needs authentication

Authentication

Setting	Description
Authentication	<p>Define if authentication is necessary on the web page:</p> <ul style="list-style-type: none"> <li>▪ Web page does not need authentication (default)</li> <li>▪ Web page needs authentication</li> </ul>
User Name	<p><b>This setting is only visible if you select Web page needs authentication above.</b></p> <p>If the proxy requires authentication, enter the user name for the proxy login. Enter a string.</p>
Password	<p><b>This setting is only visible if you select Web page needs authentication above.</b></p> <p>Enter a password.</p>
Authentication Method	<p><b>This setting is only visible if you select Web page needs authentication above.</b></p> <p>Select the authentication method that the URL uses:</p> <ul style="list-style-type: none"> <li>▪ HTTP authentication (default): Use simple HTTP authentication.             <ul style="list-style-type: none"> <li> This authentication method transmits credentials as plain text.</li> </ul> </li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>NT LAN Manager authentication: Use the Microsoft NT LAN Manager (NTLM) protocol for authentication.</li> <li>Digest access authentication: Use digest access authentication. This applies a hash function to the password, which is safer than HTTP authentication (default).</li> </ul>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can only enter the protocol followed by a colon and three forward slashes (this means that you can enter either [http://](#) or [https://](#), or even a simple forward slash / as the equivalent for [http://](#)). PRTG automatically fills in the parent device's IP Address/DNS Name in front of the third forward slash.

Whether this results in a valid URL or not depends on the IP address or Domain Name System (DNS) name of the parent device. In combination with cloning devices, you can use smart URL replacement to create many similar devices.

For example, if you create a device with the DNS name [www.example.com](#) and you add an HTTP sensor to it, you can provide values in the following ways:

- If you enter [https://](#) in the URL field, PRTG automatically creates the URL [https://www.example.com/](#)
- If you enter [/help](#) in the URL field, PRTG automatically creates and monitor the URL [http://www.example.com/help](#)
- It is also possible to provide a port number in the URL field. It is taken over by the device's DNS name and is internally added, for example, [http://:8080/](#)

 Smart URL replacement does not work for sensors that run on the probe device.

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Bytes Received	The number of bytes received
Download Bandwidth	The download speed
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Loading Time	The loading time

Channel	Description
	 This channel is the primary channel by default.
Time To First Byte	The time to the first byte

## More

### KNOWLEDGE BASE

Which user agent should I use in the HTTP Advanced sensor's settings?

- <https://kb.paessler.com/en/topic/30593>

My HTTP sensors fail to monitor websites which use SNI. What can I do?

- <https://kb.paessler.com/en/topic/67398>

Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Why do my HTTP Advanced sensors differ in the bytes received value?

- <https://kb.paessler.com/en/topic/78778>

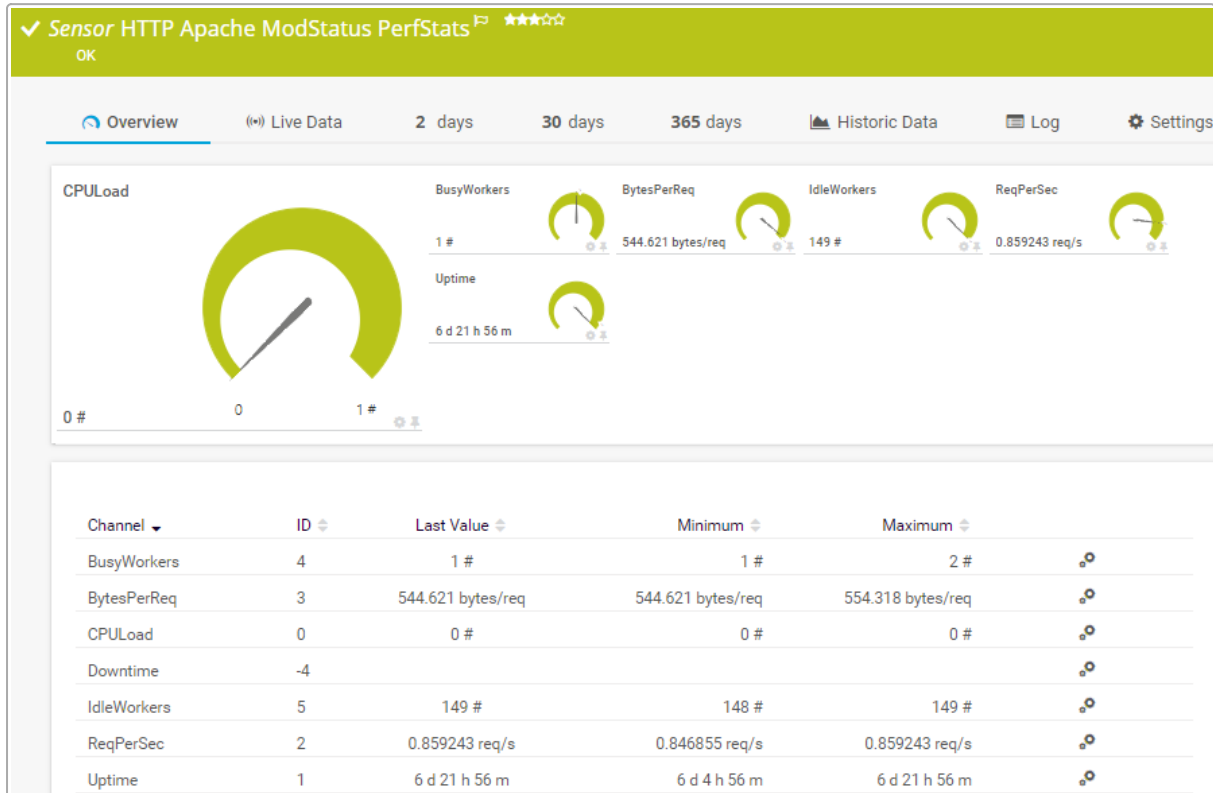
My HTTP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/85284>

## 7.8.62 HTTP Apache ModStatus PerfStats Sensor

The HTTP Apache ModStatus PerfStats sensor monitors performance statistics of an Apache web server via [mod\\_status](#) over HTTP.

**i** This sensor implicitly supports SNI, an extension to the Transport Layer Security (TLS) protocol.



HTTP Apache ModStatus PerfStats Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1068</sup>.

### Sensor in Other Languages

- Dutch: HTTP Apache ModStatus PerfStats
- French: Apache ModStatus PerfStats (HTTP)
- German: HTTP Apache ModStatus PerfStats
- Japanese: HTTP Apache ModStatus 性能統計
- Portuguese: PerfStats Apache ModStatus (HTTP)
- Russian: HTTP Apache ModStatus — стат. произв-сти
- Simplified Chinese: HTTP Apache ModStatus PerfStats
- Spanish: PerfStats Apache ModStatus (HTTP)

### Remarks

Consider the following [remarks](#)<sup>1064</sup> and requirements for this sensor:

Remark	Description
SRP ciphers	This sensor does not support Secure Remote Password (SRP) ciphers.
Smart URL replacement	This sensor supports <a href="#">smart URL replacement</a> <sup>10681</sup> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Knowledge Base	Knowledge Base: <a href="#">Which HTTP status code leads to which HTTP sensor status?</a>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- apache
- httpsensor
- httpapachemodstatusperfstatssensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>6671</sup>.

### HTTP Specific

#### HTTP Specific

**Timeout (Sec.)** ⓘ 60

---

**URL** ⓘ http(s)://www.example.com

HTTP Specific

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
URL	<p>Enter the URL to the <a href="#">mod_status</a> module on your Apache server. PRTG automatically appends <a href="#">/server-status?auto</a> to it. If you enter an absolute URL, the sensor uses this address independently of the IP Address/DNS Name setting of the parent device.</p> <p><b>■</b> PRTG uses a smart URL replacement with which you can use the parent device's IP address or Domain Name System (DNS) name setting as part of the URL. For more information, see section <a href="#">Smart URL Replacement</a> <sup>1068</sup>.</p>

## Authentication

**Authentication**

Authentication **i**
  
  Web page does not need authentication (default)
  
  Web page needs authentication

Authentication

Setting	Description
Authentication	<p>Define if authentication is necessary on the web page:</p> <ul style="list-style-type: none"> <li>▪ Web page does not need authentication (default)</li> <li>▪ Web page needs authentication</li> </ul>
User Name	<p><b>This setting is only visible if you select</b> Web page needs authentication above.</p> <p>If the proxy requires authentication, enter the user name for the proxy login. Enter a string.</p>
Password	<p><b>This setting is only visible if you select</b> Web page needs authentication above.</p> <p>Enter a password.</p>
Authentication Method	<p><b>This setting is only visible if you select</b> Web page needs authentication above.</p> <p>Select the authentication method that the URL uses:</p>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ HTTP authentication (default): Use simple HTTP authentication. <ul style="list-style-type: none"> <li>ⓘ This authentication method transmits credentials as plain text.</li> </ul> </li> <li>▪ NT LAN Manager authentication: Use the Microsoft NT LAN Manager (NTLM) protocol for authentication.</li> <li>▪ Digest access authentication: Use digest access authentication. This applies a hash function to the password, which is safer than HTTP authentication (default).</li> </ul>

## Sensor Display

**Sensor Display**


Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can only enter the protocol followed by a colon and three forward slashes (this means that you can enter either [http://](#) or [https://](#), or even a simple forward slash / as the equivalent for [http://](#)). PRTG automatically fills in the parent device's IP Address/DNS Name in front of the third forward slash.

Whether this results in a valid URL or not depends on the IP address or Domain Name System (DNS) name of the parent device. In combination with cloning devices, you can use smart URL replacement to create many similar devices.


For example, if you create a device with the DNS name [www.example.com](#) and you add an HTTP sensor to it, you can provide values in the following ways:

- If you enter [https://](#) in the URL field, PRTG automatically creates the URL [https://www.example.com/](#)
- If you enter [/help](#) in the URL field, PRTG automatically creates and monitor the URL [http://www.example.com/help](#)
- It is also possible to provide a port number in the URL field. It is taken over by the device's DNS name and is internally added, for example, [http://:8080/](#)

 Smart URL replacement does not work for sensors that run on the probe device.

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
BusyWorkers	The number of busy worker threads
BytesPerReq	The number of bytes per request
CPUload	The CPU load  This channel is the primary channel by default.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
IdleWorkers	The number of idle worker threads
ReqPerSec	The number of requests
Uptime	The uptime

## More

### KNOWLEDGE BASE

Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

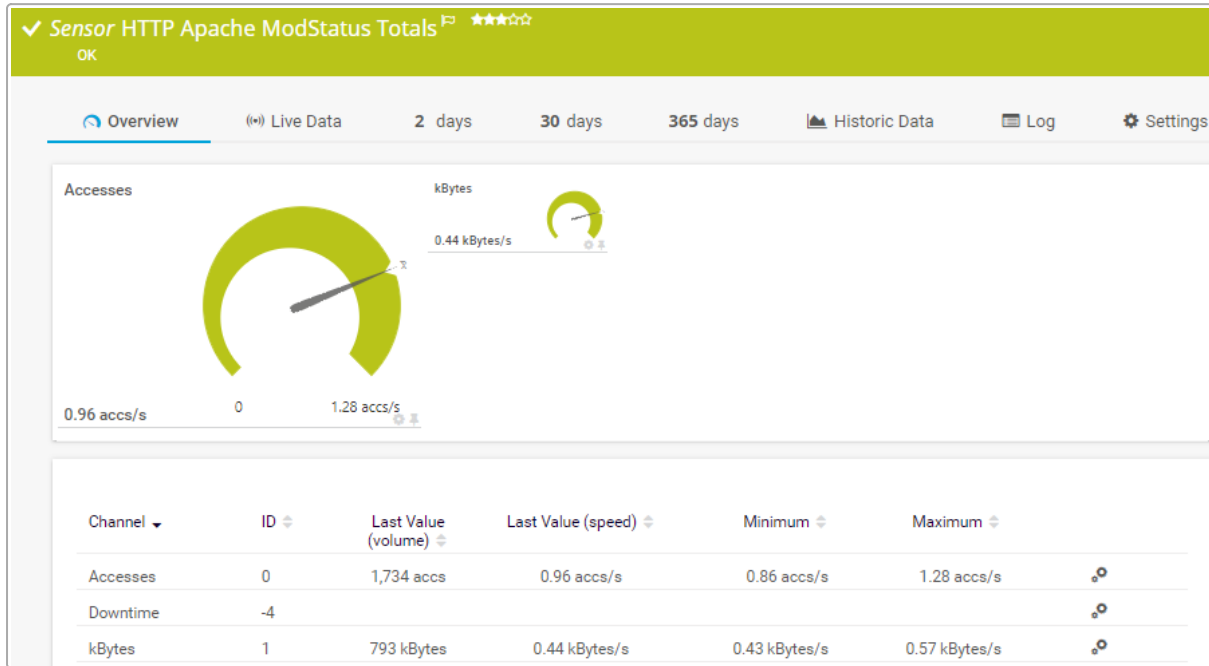
My HTTP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/85284>

## 7.8.63 HTTP Apache ModStatus Totals Sensor

The HTTP Apache ModStatus Totals sensor monitors the activity of an Apache web server using [mod\\_status](#) over HTTP.

**i** This sensor implicitly supports SNI, an extension to the Transport Layer Security (TLS) protocol.



HTTP Apache ModStatus Totals Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1074</sup>.

### Sensor in Other Languages

- Dutch: HTTP Apache ModStatus Totalen
- French: Apache ModStatus totaux (HTTP)
- German: HTTP Apache ModStatus Gesamt
- Japanese: HTTP Apache ModStatus 合計
- Portuguese: Totais Apache ModStatus (HTTP)
- Russian: HTTP Apache ModStatus — итоги
- Simplified Chinese: HTTP Apache ModStatus 合计
- Spanish: Totales Apache ModStatus (HTTP)

### Remarks

Consider the following [remarks](#)<sup>1070</sup> and requirements for this sensor:

Remark	Description
SRP ciphers	This sensor does not support Secure Remote Password (SRP) ciphers.
Smart URL replacement	This sensor supports <a href="#">smart URL replacement</a> <sup>11074</sup> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Knowledge Base	Knowledge Base: <a href="#">Which HTTP status code leads to which HTTP sensor status?</a>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- apache
- httpsensor
- httpapachemodstatustotalssensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>1667</sup>.

### HTTP Specific

#### HTTP Specific

**Timeout (Sec.)** ⓘ 60

---

**URL** ⓘ http(s)://www.example.com

HTTP Specific

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
URL	<p>Enter the URL to the <a href="#">mod_status</a> module on your Apache server. PRTG automatically appends <a href="#">/server-status?auto</a> to it. If you enter an absolute URL, the sensor uses this address independently of the IP Address/DNS Name setting of the parent device.</p> <p><b>■</b> PRTG uses a smart URL replacement with which you can use the parent device's IP address or Domain Name System (DNS) name setting as part of the URL. For more information, see section <a href="#">Smart URL Replacement</a><sup>1074</sup>.</p>

## Authentication

**Authentication**

Authentication ⓘ  Web page does not need authentication (default)  Web page needs authentication

Authentication

Setting	Description
Authentication	<p>Define if authentication is necessary on the web page:</p> <ul style="list-style-type: none"> <li>▪ Web page does not need authentication (default)</li> <li>▪ Web page needs authentication</li> </ul>
User Name	<p><b>This setting is only visible if you select</b> Web page needs authentication <b>above.</b></p> <p>If the proxy requires authentication, enter the user name for the proxy login. Enter a string.</p>
Password	<p><b>This setting is only visible if you select</b> Web page needs authentication <b>above.</b></p> <p>Enter a password.</p>
Authentication Method	<p><b>This setting is only visible if you select</b> Web page needs authentication <b>above.</b></p> <p>Select the authentication method that the URL uses:</p>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ HTTP authentication (default): Use simple HTTP authentication. <ul style="list-style-type: none"> <li>ⓘ This authentication method transmits credentials as plain text.</li> </ul> </li> <li>▪ NT LAN Manager authentication: Use the Microsoft NT LAN Manager (NTLM) protocol for authentication.</li> <li>▪ Digest access authentication: Use digest access authentication. This applies a hash function to the password, which is safer than HTTP authentication (default).</li> </ul>

## Sensor Display

**Sensor Display**


Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can only enter the protocol followed by a colon and three forward slashes (this means that you can enter either [http://](#) or [https://](#), or even a simple forward slash / as the equivalent for [http://](#)). PRTG automatically fills in the parent device's IP Address/DNS Name in front of the third forward slash.


Whether this results in a valid URL or not depends on the IP address or Domain Name System (DNS) name of the parent device. In combination with cloning devices, you can use smart URL replacement to create many similar devices.


For example, if you create a device with the DNS name [www.example.com](#) and you add an HTTP sensor to it, you can provide values in the following ways:

- If you enter [https://](#) in the URL field, PRTG automatically creates the URL [https://www.example.com/](#)
- If you enter [/help](#) in the URL field, PRTG automatically creates and monitor the URL [http://www.example.com/help](#)
- It is also possible to provide a port number in the URL field. It is taken over by the device's DNS name and is internally added, for example, [http://:8080/](#)

 Smart URL replacement does not work for sensors that run on the probe device.

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Accesses	The number of accesses
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
KBytes	The data transferred  This channel is the primary channel by default.



## More

### ■ KNOWLEDGE BASE

Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My HTTP sensors don't work. What can I do?

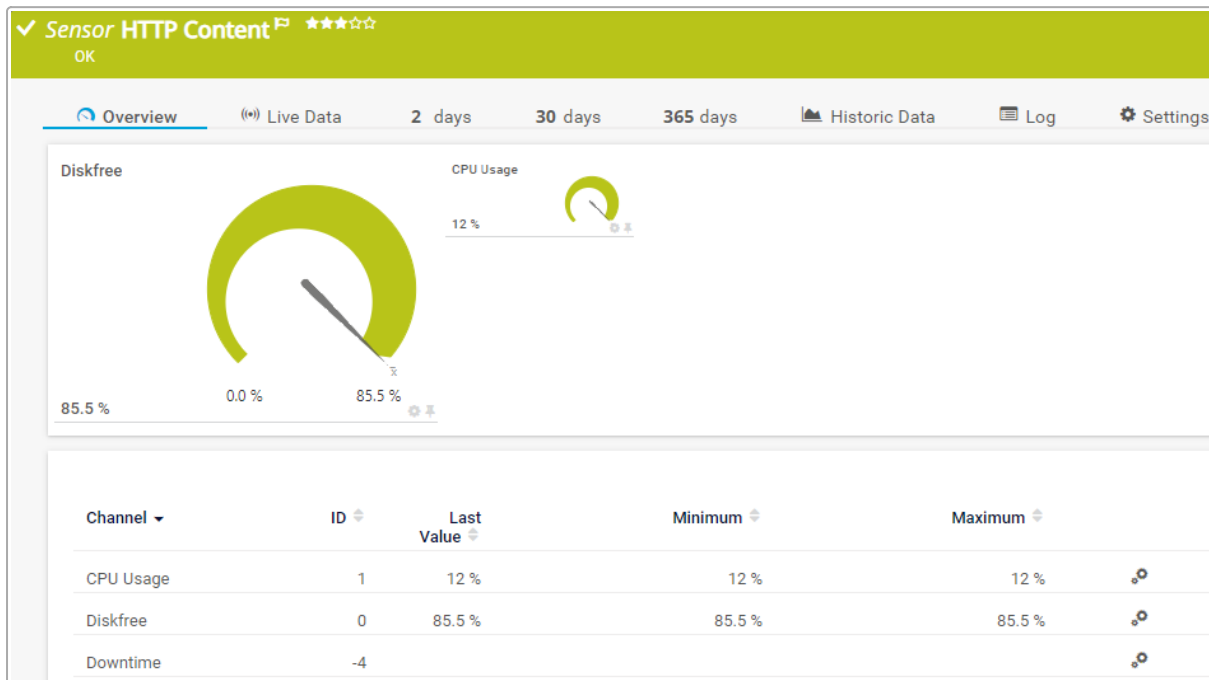
- <https://kb.paessler.com/en/topic/85284>

## 7.8.64 HTTP Content Sensor

The HTTP Content sensor monitors numeric values returned by an HTTP request.

**i** In the returned HTML page, each value must be placed between brackets [ ]. See section [Example](#)<sup>[1081]</sup>.

**i** This sensor implicitly supports SNI, an extension to the Transport Layer Security (TLS) protocol.



HTTP Content Sensor

**■** For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1082]</sup>.

### Sensor in Other Languages


- Dutch: HTTP (Inhoud)
- French: Contenu (HTTP)
- German: HTTP (Inhalt)
- Japanese: HTTP コンテンツ
- Portuguese: Conteúdo HTTP
- Russian: HTTP: Содержимое
- Simplified Chinese: HTTP 内容
- Spanish: Contenido HTTP

### Remarks

Consider the following [remarks](#)<sup>[1076]</sup> and requirements for this sensor:

Remark	Description
Channels	This sensor does not officially support more than <a href="#">50 channels</a> .
SRP ciphers	This sensor does not support Secure Remote Password (SRP) ciphers.
Smart URL replacement	This sensor supports <a href="#">smart URL replacement</a> <sup>110821</sup> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">How can I monitor internal values of a web application with PRTG?</a></li> <li>Knowledge Base: <a href="#">Which HTTP status code leads to which HTTP sensor status?</a></li> </ul>

### Add Sensor

Setting	Description
Number of Channels	<p>Define how many values the .html file returns. The sensor handles each value in its own <a href="#">channel</a>. Each value must be placed between brackets [ ]. Enter the number of bracket-value pairs that the URL returns. Enter an integer.</p> <p> Do not enter a number that is greater than the number of values that the HTTP request returns. Otherwise, you get an error message.</p>

### Basic Sensor Settings

#### Basic Sensor Settings

Sensor Name ⓘ

Tags ⓘ

Priority ⓘ

Example Name

---

exampletag ✕ +

★★★★☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- httpsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>1667</sup>.

## HTTP Specific

<b>HTTP Specific</b>	Timeout (Sec.) ⓘ <input type="text" value="60"/>
	Script URL ⓘ <input type="text" value="https://"/>
	Value Type ⓘ <input type="text" value="Integer"/>
<i>You can modify channel names and units in the sensor's channel settings.</i>	

HTTP Specific

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p>ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
Script URL	<p>Enter the URL that the sensor connects to. If you enter an absolute URL, the sensor uses this address independently of the IP Address/DNS Name setting of the parent device.</p> <p>ⓘ The URL must be <a href="#">URL encoded</a>.</p> <p>■ PRTG uses a smart URL replacement with which you can use the parent device's IP address or Domain Name System (DNS) name setting as part of the URL. For more information, see section <a href="#">Smart URL Replacement</a><sup>1082</sup>.</p>
Value Type	<p>Define what kind of values the .html file returns:</p> <ul style="list-style-type: none"> <li>▪ Integer: Returns integers.</li> <li>▪ Float: Returns floats with a dot . between the predecimal position and the decimal places. The sensor also displays integers unless they do not produce a buffer overflow.</li> </ul> <p>ⓘ The sensor cannot handle string values.</p> <p>ⓘ You cannot change this value after sensor creation.</p>

## Advanced Sensor Data

**Advanced Sensor Data**

**If Content Changes** ⓘ  Ignore (default)  
 Trigger 'change' notification

**Result Handling** ⓘ  Discard result (default)  
 Store result

Advanced Sensor Data


Setting	Description
If Content Changes	<p>Define what the sensor does if the content of the web page changes:</p> <ul style="list-style-type: none"> <li>Ignore (default): Do nothing.</li> <li>Trigger 'change' notification: Send an internal message that indicates a change. <ul style="list-style-type: none"> <li> ⓘ In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</li> </ul> </li> </ul>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Authentication

**Authentication**

**Authentication** ⓘ  Web page does not need authentication (default)  
 Web page needs authentication

Authentication

Setting	Description
Authentication	<p>Define if authentication is necessary on the web page:</p> <ul style="list-style-type: none"> <li>▪ Web page does not need authentication (default)</li> <li>▪ Web page needs authentication</li> </ul>
User Name	<p><b>This setting is only visible if you select</b> Web page needs authentication above.</p> <p>If the proxy requires authentication, enter the user name for the proxy login. Enter a string.</p>
Password	<p><b>This setting is only visible if you select</b> Web page needs authentication above.</p> <p>Enter a password.</p>
Authentication Method	<p><b>This setting is only visible if you select</b> Web page needs authentication above.</p> <p>Select the authentication method that the URL uses:</p> <ul style="list-style-type: none"> <li>▪ HTTP authentication (default): Use simple HTTP authentication. <ul style="list-style-type: none"> <li> This authentication method transmits credentials as plain text.</li> </ul> </li> <li>▪ NT LAN Manager authentication: Use the Microsoft NT LAN Manager (NTLM) protocol for authentication.</li> <li>▪ Digest access authentication: Use digest access authentication. This applies a hash function to the password, which is safer than HTTP authentication (default).</li> </ul>

## Sensor Display

**Sensor Display**


Primary Channel ⓘ Downtime

---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p>

Setting	Description
	<p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Example

 For example, consider the URL <http://www.example.com/status.html> that returns a PHP script with the current system status in a simple HTML page as follows:

```
<html>
  <body>
    Description: Script gives back current status of disk free (%) and CPU usage (%).
    [85.5][12.0]
  </body>
</html>
```

You would configure the HTTP Content sensor using

- the Script URL from above,
- the value type Float,

- and the number of channels 2.

The sensor calls the URL with every scanning interval and only regards the two values in brackets [ ] and handles each of them in one channel. The additional description text and HTML tags are not necessary. In this example, they are added in case a human calls the URL.

- ❗ If you define the number of channels as 1, the sensor only reads the first value. The second value is ignored. Using 3 as the number of channels results in a sensor error message.

## Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can only enter the protocol followed by a colon and three forward slashes (this means that you can enter either <http://> or <https://>, or even a simple forward slash / as the equivalent for <http://>). PRTG automatically fills in the parent device's IP Address/DNS Name in front of the third forward slash.

Whether this results in a valid URL or not depends on the IP address or Domain Name System (DNS) name of the parent device. In combination with cloning devices, you can use smart URL replacement to create many similar devices.

For example, if you create a device with the DNS name [www.example.com](http://www.example.com) and you add an HTTP sensor to it, you can provide values in the following ways:

- If you enter <https://> in the URL field, PRTG automatically creates the URL <https://www.example.com/>
- If you enter [/help](http://www.example.com/help) in the URL field, PRTG automatically creates and monitor the URL <http://www.example.com/help>
- It is also possible to provide a port number in the URL field. It is taken over by the device's DNS name and is internally added, for example, <http://:8080/>

- ❗ Smart URL replacement does not work for sensors that run on the probe device.

## Channel List

- ❗ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	The numeric values that an HTTP request returns in several channels

## More

### ■ KNOWLEDGE BASE

How can I monitor internal values of a web application with PRTG?



- <https://kb.paessler.com/en/topic/4>

Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

What security features does PRTG include?

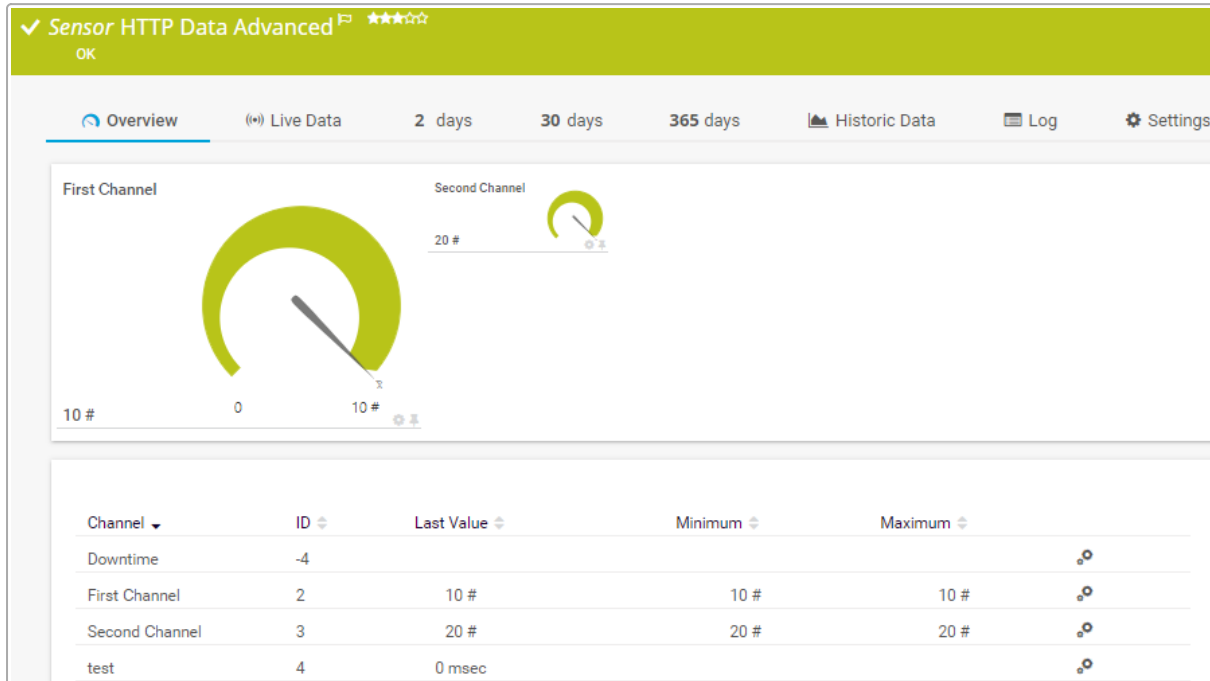
- <https://kb.paessler.com/en/topic/61108>

My HTTP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/85284>

## 7.8.65 HTTP Data Advanced Sensor

The HTTP Data Advanced sensor accesses a web server and retrieves Extensible Markup Language (XML) encoded or JavaScript Object Notation (JSON) encoded data.



HTTP Data Advanced Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: HTTP Data Geavanceerd
- French: Données avancé (HTTP)
- German: HTTP Daten (Erweitert)
- Japanese: HTTP データアドバンスト
- Portuguese: Dados HTTP (avanzado)
- Russian: HTTP: Данные (расширенный)
- Simplified Chinese: HTTP 数据高级
- Spanish: Datos HTTP (avanzado)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Return data	The requested web server must return XML-encoded or JSON-encoded data that matches the format as defined in the PRTG Manual: <a href="#">Custom Sensors</a> .
SRP ciphers	This sensor does not support Secure Remote Password (SRP) ciphers.
Smart URL replacement	This sensor supports <a href="#">smart URL replacement</a> <sup>11091</sup> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
Performance	For best sensor performance, we recommend that you specify the content type on the target system, which is <a href="#">application/xml</a> or <a href="#">application/json</a> .
Knowledge Base	Knowledge Base: <a href="#">Which HTTP status code leads to which HTTP sensor status?</a>

## Basic Sensor Settings

### Basic Sensor Settings

Sensor Name ⓘ

Tags ⓘ

Priority ⓘ

Example Name

---

exampletag ✕ +

---

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- httpsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## HTTP Specific

**HTTP Specific**

Timeout (Sec.) ⓘ 60

---

URL ⓘ https://example.com

---

Request Method ⓘ  GET (default)  
 POST  
 HEAD

---

Server Name Indication ⓘ example.com

---

SNI Inheritance ⓘ  Inherit SNI from parent device (default)  
 Do not inherit SNI from parent device

HTTP Specific

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p>ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
URL	<p>Enter the URL that the sensor connects to.</p> <p>If you enter an absolute URL, the sensor uses this address independently of the IP Address/DNS Name setting of the parent device. You can enter the URL of a web page (to measure the loading time of the page's source code), or enter the URL of an image or of a page asset to measure this element's availability and loading time.</p> <p>ⓘ The URL must be <a href="#">URL encoded</a>.</p> <p>ⓘ If you monitor an image or a page asset, this can create a high amount of memory load. We recommend that the size of the elements that you want to monitor does not exceed 200 MB.</p> <p>■ PRTG uses a smart URL replacement with which you can use the parent device's IP address or Domain Name System (DNS) name setting as part of the URL. For more information, see section <a href="#">Smart URL Replacement</a> <sup>1091</sup>.</p>
Request Method	<p>Select an HTTP request method to determine how the sensor requests the URL:</p> <ul style="list-style-type: none"> <li>▪ GET (default): Directly request the website.</li> </ul> <p>ⓘ We recommend that you use this setting for a simple check of the web page.</p>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ POST: Send post form data to the URL.               <ul style="list-style-type: none"> <li>❗ If you select this setting, you must enter the data in the Postdata field below.</li> <li>❗ If a POST request is redirected, all further requests are GET (default) requests.</li> </ul> </li> <li>▪ HEAD: Only request the HTTP header from the server without the actual web page.               <ul style="list-style-type: none"> <li>❗ Although this saves bandwidth because it transfers less data, we do not recommended that you use this. This is because the measured request time is not the one that your users experience and you might not be notified of slow results or timeouts.</li> </ul> </li> </ul>
Postdata	<p>This setting is only visible if you select POST above.</p> <p>Enter the data part for the POST request.</p> <p>❗ No Extensible Markup Language (XML) is allowed here.</p>
Content Type	<p>This setting is only visible if you select POST above.</p> <p>Define the content type of the POST request:</p> <ul style="list-style-type: none"> <li>▪ Default (application/x-www-form-urlencoded): Use the default content type to encode the form data set for submission to the server.</li> <li>▪ Custom: Use a custom content type. Enter the content type below.</li> </ul>
Custom Content Type	<p>This setting is only visible if you select Custom above.</p> <p>Define the custom content type, for example, XML, JavaScript Object Notation (JSON), or HTTP.</p>
Server Name Indication	<p>The Server Name Indication (SNI) that the sensor automatically determines from the host address of the <a href="#">parent device</a> or from the target URL of the sensor.</p> <p>❗ The SNI must be a fully qualified domain name (FQDN). Make sure that it matches the configuration of the target server.</p> <p>■ For more information, see the Knowledge Base: <a href="#">My HTTP sensors fail to monitor websites which use SNI. What can I do?</a></p> <p>❗ You cannot change this value after sensor creation.</p>
SNI Inheritance	<p>Define if you want to inherit the SNI from the parent device:</p> <ul style="list-style-type: none"> <li>▪ Inherit SNI from parent device: Determine the SNI from the host address of the parent device.</li> <li>▪ Do not inherit SNI from parent device: Determine the SNI from the target URL as defined in the settings of this sensor.</li> </ul>

Setting	Description
Result Handling	<p>Define what the sensor does with the data loaded at the URL:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last result of the requested data in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID]-A.txt, and Result of Sensor [ID].Data.txt. This setting is for debugging purposes, especially in combination with content checks. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### Advanced Sensor Data

**Advanced Sensor Data**



HTTP Version ⓘ  HTTP 1.0  
 HTTP 1.1

User Agent ⓘ  Use the default string  
 Use a custom string

Use Custom HTTP Headers ⓘ  Do not use custom HTTP headers  
 Use custom HTTP headers


Advanced Sensor Data

Setting	Description
HTTP Version	<p>Define the HTTP version that the sensor uses when it connects to the target URL:</p> <ul style="list-style-type: none"> <li>▪ HTTP 1.0: Use HTTP version 1.0.</li> <li>▪ HTTP 1.1: Use HTTP version 1.1.</li> </ul>
User Agent	<p>Choose which user agent string the sensor sends when it connects to the target URL:</p> <ul style="list-style-type: none"> <li>▪ Use the default string: Do not enter a specific user agent and use the default string. Usually, this is <a href="#">Mozilla/5.0 (compatible; PRTG Network Monitor (www.paessler.com); Windows)</a>.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Use a custom string: Use a custom user agent. Define the custom user agent below.</li> </ul>
Custom User Agent	<p>This setting is only visible if you select Use a custom string above.</p> <p>Enter the string that the sensor uses as the user agent when it connects to the target URL.</p>
HTTP Headers	<p>Define if you want to send custom HTTP headers to the target URL:</p> <ul style="list-style-type: none"> <li>Do not use custom HTTP headers: Do not use custom HTTP headers.</li> <li>Use custom HTTP headers: Use custom headers. Define below.</li> </ul>
Custom HTTP Headers	<p>This setting is only visible if you select Use custom HTTP headers above.</p> <p>Enter a list of custom HTTP headers and values that you want to transmit to the URL, each pair in one line. The syntax of a header-value pair is <code>header1:value1</code></p> <ul style="list-style-type: none"> <li> The sensor does not support the header field names <code>user-agent</code>, <code>content-length</code>, and <code>host</code>.</li> <li> Make sure that the HTTP header statement is valid. Otherwise, the sensor request cannot be successful.</li> </ul>

## Authentication

**Authentication**

Authentication   Web page does not need authentication (default)  Web page needs authentication

Authentication

Setting	Description
Authentication	<p>Define if authentication is necessary on the web page:</p> <ul style="list-style-type: none"> <li>Web page does not need authentication (default)</li> <li>Web page needs authentication</li> </ul>
User Name	<p>This setting is only visible if you select Web page needs authentication above.</p> <p>If the proxy requires authentication, enter the user name for the proxy login. Enter a string.</p>

Setting	Description
Password	<p>This setting is only visible if you select <a href="#">Web page needs authentication above</a>.</p> <p>Enter a password.</p>
Authentication Method	<p>This setting is only visible if you select <a href="#">Web page needs authentication above</a>.</p> <p>Select the authentication method that the URL uses:</p> <ul style="list-style-type: none"> <li>▪ HTTP authentication (default): Use simple HTTP authentication. <ul style="list-style-type: none"> <li>ⓘ This authentication method transmits credentials as plain text.</li> </ul> </li> <li>▪ NT LAN Manager authentication: Use the Microsoft NT LAN Manager (NTLM) protocol for authentication.</li> <li>▪ Digest access authentication: Use digest access authentication. This applies a hash function to the password, which is safer than HTTP authentication (default).</li> </ul>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>



Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can only enter the protocol followed by a colon and three forward slashes (this means that you can enter either [http://](#) or [https://](#), or even a simple forward slash / as the equivalent for [http://](#)). PRTG automatically fills in the parent device's IP Address/DNS Name in front of the third forward slash.


Whether this results in a valid URL or not depends on the IP address or Domain Name System (DNS) name of the parent device. In combination with cloning devices, you can use smart URL replacement to create many similar devices.



For example, if you create a device with the DNS name [www.example.com](#) and you add an HTTP sensor to it, you can provide values in the following ways:

- If you enter [https://](#) in the URL field, PRTG automatically creates the URL [https://www.example.com/](#)
- If you enter [/help](#) in the URL field, PRTG automatically creates and monitor the URL [http://www.example.com/help](#)
- It is also possible to provide a port number in the URL field. It is taken over by the device's DNS name and is internally added, for example, [http://:8080/](#)

 Smart URL replacement does not work for sensors that run on the probe device.

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	<p>The values that the web server returns in several channels</p> <p> This channel is the primary channel by default.</p> <p> For more information about the return value format, see section <a href="#">Custom Sensors</a>.</p>

## More

### KNOWLEDGE BASE

Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My HTTP sensors fail to monitor websites which use SNI. What can I do?

- <https://kb.paessler.com/en/topic/67398>

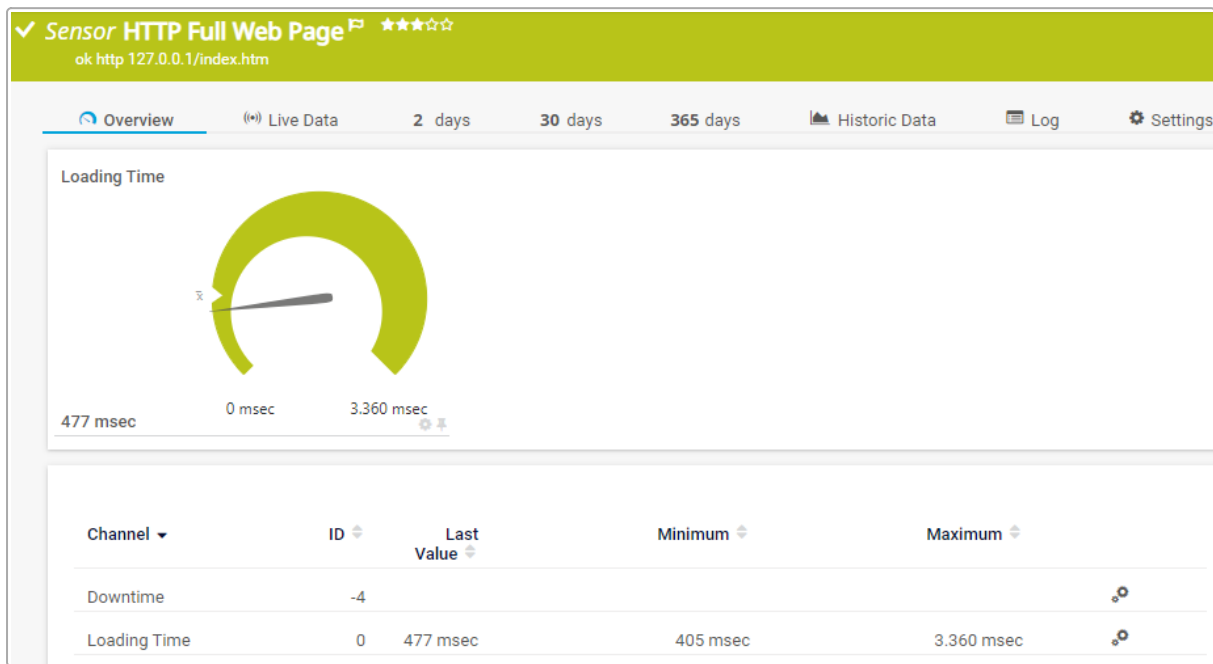
My HTTP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/85284>

## 7.8.66 HTTP Full Web Page Sensor

The HTTP Full Web Page sensor monitors the full download time of a web page including assets such as images. In the background, it opens the web page in a browser instance to perform the measurement. It does not follow links.

**i** Be careful with this sensor because it can generate a considerable amount of internet traffic if you use it with a short scanning interval.



HTTP Full Web Page Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1093]</sup>.

### Sensor in Other Languages

- Dutch: HTTP Volledige Webpagina
- French: Page web complète (HTTP)
- German: HTTP (Komplette Webseite)
- Japanese: HTTP 完全ウェブページ監視
- Portuguese: Página completa HTTP
- Russian: HTTP: Полное время загрузки веб-страницы
- Simplified Chinese: HTTP 完整网页
- Spanish: Página web completa HTTP

### Remarks

Consider the following [remarks](#)<sup>[1093]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
SRP ciphers	This sensor does not support Secure Remote Password (SRP) ciphers.
Smart URL replacement	This sensor supports <a href="#">smart URL replacement</a> <sup>110991</sup> .
IPv6	This sensor supports IPv6.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">What to do when I see a CreateUniqueTempDir() error message for my HTTP Full Web Page sensor?</a></li> <li>▪ Knowledge Base: <a href="#">HTTP Full Web Page sensor is unable to navigate. What can I do?</a></li> <li>▪ Knowledge Base: <a href="#">How can I change the size of PhantomJS full web page screenshots?</a></li> <li>▪ Knowledge Base: <a href="#">Why is my HTTP Full Web Page sensor generating so many temporary files?</a></li> <li>▪ Knowledge Base: <a href="#">Which HTTP status code leads to which HTTP sensor status?</a></li> </ul>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- httpfullsensor

 For more information about basic sensor settings, see section [Sensor Settings](#)<sup>6671</sup>.

## Full Web Page Download Settings

**Full Web Page Download Settings**

Timeout (Sec.) ⓘ 20

---

URL ⓘ https://

---

Browser Engine ⓘ  Chromium (default)  
 PhantomJS (Headless WebKit)  
 Internet Explorer

---

Security Context ⓘ  Use security context of PRTG probe service (default)  
 Use Windows credentials from parent device

Full Web Page Download Settings

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p> ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
URL	<p>Enter the address of the web page that the sensor loads. If you enter an absolute URL, the sensor uses this address independently of the IP Address/DNS Name setting of the parent device.</p> <p> ⓘ The URL must be <a href="#">URL encoded</a>.</p> <p> ■ PRTG uses a smart URL replacement with which you can use the parent device's IP address or Domain Name System (DNS) name setting as part of the URL. For more information, see section <a href="#">Smart URL Replacement</a><sup>[1095]</sup>.</p>
Browser Engine	<p>Define which browser engine this sensor uses to load the web page:</p> <ul style="list-style-type: none"> <li>▪ Chromium (default): Use the WebKit engine that is delivered with PRTG to measure the loading time. With each scanning interval, PRTG loads the URL in an instance of Chromium and measures the time it takes to fully load the page. This is the recommended setting. <ul style="list-style-type: none"> <li> ⓘ Chromium does not support TLS 1.2-only connections. In this case, we recommend that you use the PhantomJS engine or Internet Explorer instead.</li> </ul> </li> <li>▪ PhantomJS (Headless Webkit): Use the PhantomJS engine. This engine can have a high impact on the probe system's CPU and memory load but additional options for <a href="#">result handling</a><sup>[1096]</sup> are available.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Internet Explorer: With each scanning interval, the URL is loaded in the background in an instance of Internet Explorer. PRTG uses the Internet Explorer of the probe system.               <ul style="list-style-type: none"> <li>❗ For full functionality, we strongly recommend that you install at least Internet Explorer 11 on the probe system.</li> <li>❗ If you select Internet Explorer as browser engine, you might face issues with the creation of temporary files. In this case, we recommend that you use the Chromium or the PhantomJS browser engines. For more information, see the Knowledge Base: <a href="#">Why is my HTTP Full Web Page sensor generating so many temporary files?</a></li> </ul> </li> <li>❗ All browser engines use the proxy settings from the Windows user account that the probe runs under (this is usually the local Windows "system" user account). To use a proxy, adjust the settings accordingly on the probe system (on all cluster nodes, if in a cluster). For more information, see the Knowledge Base: <a href="#">How can I access proxy settings for the HTTP Full Web Page sensor?</a></li> </ul>
Security Context	<p>Define the Windows user account that this sensor uses to run the browser engine:</p> <ul style="list-style-type: none"> <li>▪ Use security context of PRTG probe service (default): Run the browser engine under the same Windows user account that the probe system runs under. By default, this is the local Windows "system" user account.</li> <li>▪ Use Windows credentials from parent device: Use the Windows user account from the parent <a href="#">device settings</a>.               <ul style="list-style-type: none"> <li>❗ We recommend that you use this setting if you use Chromium (default) as your browser engine.</li> </ul> </li> </ul>
Result Handling	<p><a href="#">This setting is only visible if you select PhantomJS (Headless Webkit) above.</a></p> <p>Specify how the browser engine handles the web page result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Render and store a screenshot of most recent result as JPG: Render and store the web page result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Fullpage of Sensor (ID).jpg. This setting is for debugging purposes. PRTG overwrites the file with each scanning interval.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Render and store screenshots of all results as JPGs (requires lots of disk space): Render and store one new screenshot of the web page with each sensor scan, and store the screenshots in the \Screenshots (Fullpage Sensor) subfolder of the PRTG data directory on the probe system. You can use this option to create a visual history of the web page.               <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> Depending on the monitored website and the scanning interval of the sensor, this option can create a very high amount of data. Use this option with care and make sure you set appropriate data purging limits in the <a href="#">Core &amp; Probes</a> settings.</li> <li><span style="color: blue;">■</span> If necessary, you can change the window size of the rendered screenshots. For more information, see the Knowledge Base: <a href="#">How can I change the size of PhantomJS full web page screenshots?</a></li> <li><span style="color: red;">❗</span> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</li> </ul> </li> </ul>
Authentication	<p><span style="color: blue;">This setting is only visible if you select PhantomJS (Headless Webkit) above.</span></p> <p>Define if the monitored web page needs authentication for access:</p> <ul style="list-style-type: none"> <li>▪ Web page does not need authentication: Access to the web page is granted without authentication.</li> <li>▪ Web page needs authentication: PRTG automatically tries to use HTTP basic authentication (BA) or Windows NT LAN Manager (NTLM) to access the web page with authentication. Enter the credentials below.               <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> Basic access authentication forwards the credentials in plain text.</li> </ul> </li> </ul>
User Name	<p><span style="color: blue;">This setting is only visible if you select PhantomJS (Headless Webkit) above.</span></p> <p>Enter the user name for the web page.</p>
Password	<p><span style="color: blue;">This setting is only visible if you select PhantomJS (Headless Webkit) above.</span></p> <p>Enter the password for the web page.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).



## Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can only enter the protocol followed by a colon and three forward slashes (this means that you can enter either <http://> or <https://>, or even a simple forward slash / as the equivalent for <http://>). PRTG automatically fills in the parent device's IP Address/DNS Name in front of the third forward slash.

Whether this results in a valid URL or not depends on the IP address or Domain Name System (DNS) name of the parent device. In combination with cloning devices, you can use smart URL replacement to create many similar devices.


For example, if you create a device with the DNS name [www.example.com](http://www.example.com) and you add an HTTP sensor to it, you can provide values in the following ways:

- If you enter <https://> in the URL field, PRTG automatically creates the URL <https://www.example.com/>
- If you enter [/help](http://www.example.com/help) in the URL field, PRTG automatically creates and monitor the URL <http://www.example.com/help>
- It is also possible to provide a port number in the URL field. It is taken over by the device's DNS name and is internally added, for example, <http://:8080/>

 Smart URL replacement does not work for sensors that run on the probe device.

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Loading Time	The loading time of the full web page  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

What to do when I see a CreateUniqueTempDir() error message for my HTTP Full Web Page sensor?

- <https://kb.paessler.com/en/topic/40783>

HTTP Full Web Page sensor is unable to navigate. What can I do?

- <https://kb.paessler.com/en/topic/59999>

How can I change the size of PhantomJS full web page screenshots?

- <https://kb.paessler.com/en/topic/60247>

Why is my HTTP Full Web Page sensor generating so many temporary files?

- <https://kb.paessler.com/en/topic/65758>

Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

What is the difference between "HTTP" and "HTTP Full Web Page" web server sensors?

- <https://kb.paessler.com/en/topic/943>

How can I access proxy settings for the HTTP Full Web Page sensor?

- <https://kb.paessler.com/en/topic/81408>

My HTTP sensors don't work. What can I do?

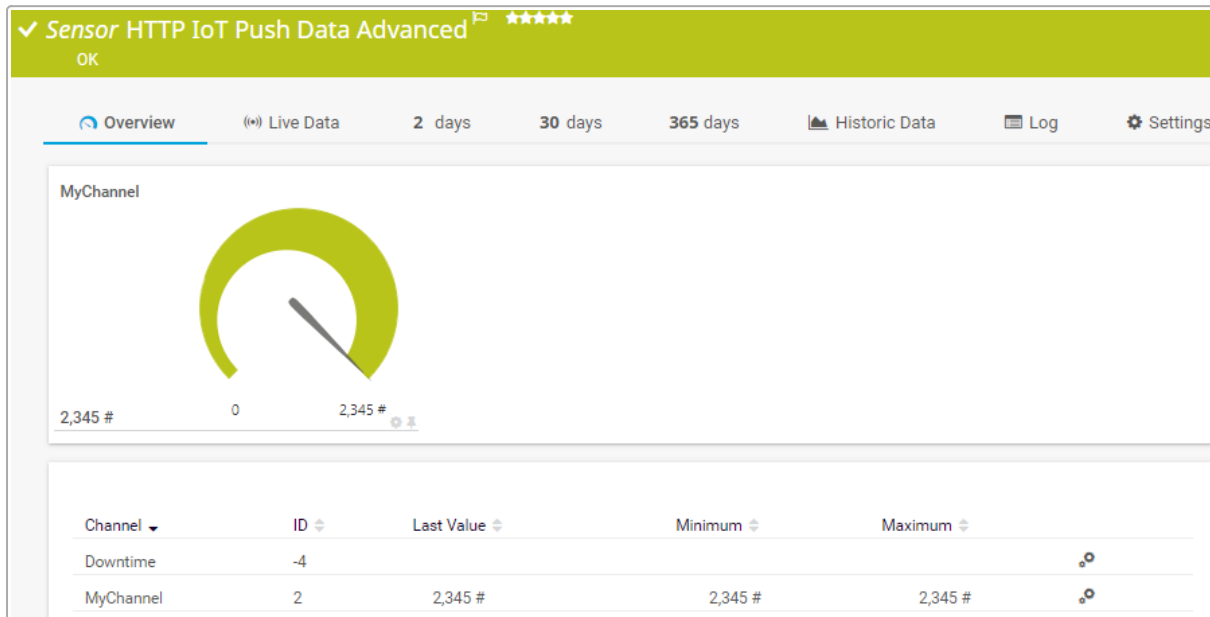
- <https://kb.paessler.com/en/topic/85284>

## 7.8.67 HTTP IoT Push Data Advanced Sensor

The HTTP IoT Push Data Advanced sensor displays data from messages that are received from Internet of Things (IoT) capable devices (for example, Sigfox devices) and that are pushed via an HTTPS request to PRTG. It provides a URL that you can use to push messages to the probe system via HTTPS (secured with TLS 1.3 and weak ciphers).

☁ This sensor is especially useful when you want to push data to a PRTG Hosted Monitor instance.

📘 For more information about the sensor usage, see section [How to Use](#)<sup>[1105]</sup>.



HTTP IoT Push Data Advanced Sensor

■ For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1106]</sup>.

### Sensor in Other Languages

- Dutch: HTTP IoT Push Data Geavanceerd
- French: Données IoT avancé (HTTP Push)
- German: HTTP IoT Push-Daten (Erweitert)
- Japanese: HTTP IoT プッシュデータ(アドバンスト)
- Portuguese: Dados de push IoT (avançado) (HTTP)
- Russian: Дополнительные данные push-объекта HTTP IoT
- Simplified Chinese: HTTP IoT 高级推送数据
- Spanish: Datos push IoT (avanzado) (HTTP)

### Remarks

Consider the following [remarks](#)<sup>[1107]</sup> and requirements for this sensor:

Remark	Description
Fixed port	This sensor has a fixed port (5051). You cannot change it.
Fixed SSL/TLS version	This sensor has a fixed SSL/TLS version (HTTPS (secured with TLS 1.3 and weak ciphers)). You cannot change it.
Remote probe	If you want to add this sensor to a remote probe and use an HTTPS connection to send push notifications, you must import a Secure Sockets Layer (SSL) certificate into the \cert subfolder of the <a href="#">PRTG program directory</a> on the remote probe. However, this certificate does not have to match the certificate that you use on the PRTG core server. For more information about SSL certificates, see the Paessler website: <a href="#">How to use your own SSL certificate with the PRTG web server</a>
Cluster probe	This sensor does not support cluster probes. You can only set it up on local probes or remote probes.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
Multiple channels	If you use this sensor with multiple channels, we recommend that you <b>simultaneously</b> push the data for <b>all</b> your channels to PRTG. You can push data to only one of your channels. However, all other channels record the value of <b>0</b> for this push message.
False alerts	This sensor might result in false alerts if the parent probe disconnects from the PRTG core server. In this case, the sensor shows the error message: <b>The latest push message that the sensor received is older than the specified time threshold allows. (code: PE222).</b>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- HttpPushSensor
- IoT
- PushData
- PushSensor
- Sigfox

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## TLS Settings

**TLS Settings** TLS Port ⓘ 5051

TLS Settings

Setting	Description
TLS Port	The number of the port on which this sensor listens for incoming HTTPS requests. This is always <a href="#">5051</a> .

## HTTP Push Authentication

**HTTP Push Authentication** Identification Token ⓘ 12345678-ABCD-EFGH-87654321

HTTP Push Authentication

Setting	Description
Identification Token	<p>This is the token that PRTG uses to find the matching sensor for the incoming message. When you create the sensor, this token is <code>{_guid_}</code>.</p> <p>PRTG replaces this token with an automatically generated token after sensor creation. If you want to use a different identification token, you can edit it during or after sensor creation.</p> <p>ⓘ PRTG does not automatically replace the token if you change it already during sensor creation.</p>

## HTTP Push Data

**HTTP Push Data**

No Incoming Data ⓘ

Ignore and keep last status (default)  
 Switch to unknown status  
 Switch to down status after x minutes

HTTP Push Data

Setting	Description
No Incoming Data	<p>Define which <a href="#">status</a> the sensor shows if it does not receive a push message for at least two scanning intervals:</p> <ul style="list-style-type: none"> <li>▪ Ignore and keep last status (default): Keep the status as defined by the last message that the sensor received.               <ul style="list-style-type: none"> <li>ⓘ The parent probe must be connected to keep the last status. If the parent probe disconnects, the sensor shows the Unknown status. If the parent probe connects again, the sensor does not automatically switch from the Unknown status to the last status before the parent probe disconnects.</li> </ul> </li> <li>▪ Switch to unknown status: Show the Unknown status if the sensor does not receive a message for at least two scanning intervals.</li> <li>▪ Switch to down status after x minutes: Show the Down status if the sensor does not receive a message within a specific time span. Define the time threshold below.</li> </ul>
Time Threshold (Minutes)	<p><b>This setting is only visible if you select</b> Switch to down status after x minutes <b>above.</b></p> <p>Enter a time threshold in minutes. If this time elapses, the sensor shows the Down status if it does not receive a push message within this time span. Enter an integer. The maximum threshold is <b>1440</b> minutes.</p>

## Sensor Display

**Sensor Display**




Primary Channel ⓘ Downtime

---


Graph Type ⓘ

Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## How to Use

This function is known as a [webhook](#). Basically, a webhook works like a push notification. Webhooks are usually triggered by an event (for example, a new comment on a blog post) and send according information to a specified URL. The HTTP IoT Push Data Advanced sensor then displays the data of pushed and received messages.

 The data that is pushed to this sensor must be valid XML or JSON.

 For more information about the return value format, see section [Custom Sensors](#).

The HTTP IoT Push Data Advanced sensor uses the following URLs depending on the type of HTTPS request:

- GET (default) requests: `https://<probe_ip>:5051/<token>?content=<valid XML_or_JSON>`

The XML-encoded value of the content parameter has to match the format defined in section [Custom Sensors](#).

- POST requests: `https://<probe_ip>:5051/<token>`

This HTTPS request method sends the XML-encoded or JSON-encoded HTTPS body as POST data. The body has to match the format defined in section [Custom Sensors](#). We strongly recommend the HTTPS content type `application/xml` or `application/json`.

Replace the parameters `<probe_ip>`, `<token>`, and `<valid XML_or_JSON>` (for GET requests) with the corresponding values:

- For PRTG Network Monitor, the probe IP is the IP address of the probe system.

☁ For PRTG Hosted Monitor instances, the probe IP is the Domain Name System (DNS) name of the instance.

- The port number is always `5051`. You cannot change this.
- You can define identification token in the sensor settings.
- The content of GET requests has to be valid XML or JSON in the PRTG API format.
  - ⓘ The content has to be URL encoded (for example, the whitespaces in the sample URL below). Most browsers do the URL-encoding automatically.

Minimum example for the GET method that returns one static channel value:

```
https://127.0.0.1:5051/XYZ123?
content=<prtg><result><channel>MyChannel</channel><value>10</value></result><text>this
%20is%20a%20message</text></prtg>
```

- ⓘ By default, values within the `<value>` tags in the returned XML or JSON must be `integers` for them to be processed. If `float` values are returned, you must explicitly define this value type as defined in section [Custom Sensors](#) with `<float>` tags, otherwise the sensor shows 0 values in affected channels. Example:



```
https://127.0.0.1:5051/XYZ123?
content=<prtg><result><channel>MyChannel</channel><value>10.45</value><float>1</float>
</result><text>this%20is%20a%20message</text></prtg>
```

- ⓘ You can use several sensors with the same port and identification token. In this case, push message data is shown in each of these sensors.

## Channel List

- ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.



Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	<p>The data received from the message encoded in valid XML or JSON in several channels</p> <p> This channel is the primary channel by default.</p> <p> For more information about the return value format, see section <a href="#">Custom Sensors</a>.</p>

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How can I monitor Sigfox geolocation with PRTG?

- <https://kb.paessler.com/en/topic/80157>

How can I monitor the Sigfox API with PRTG?

- <https://kb.paessler.com/en/topic/80346>

How can I monitor Sigfox callbacks with PRTG?

- <https://kb.paessler.com/en/topic/80232>

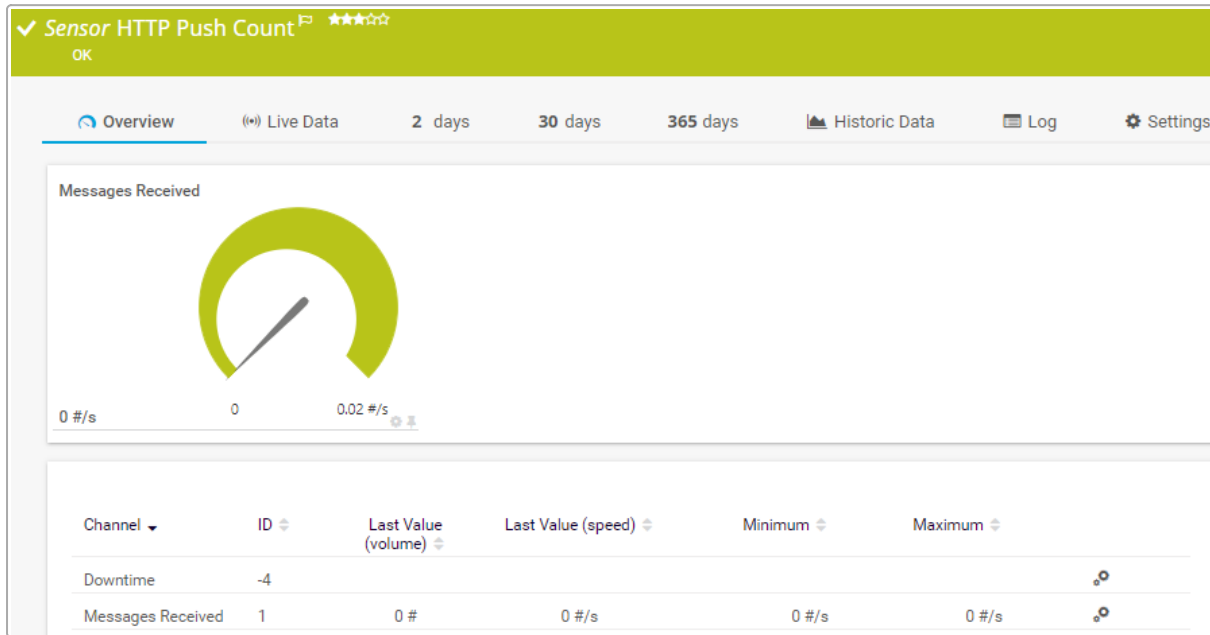
My HTTP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/85284>

## 7.8.68 HTTP Push Count Sensor

The HTTP Push Count sensor counts received messages that are pushed via an HTTP request to PRTG. It provides a URL that you can use to push messages to the probe system via HTTP (secured with TLS 1.2 or not secure).

**i** For more information about the sensor usage, see section [How to Use](#)<sup>[1112]</sup>.



HTTP Push Count Sensor


**■** For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1113]</sup>.

### Sensor in Other Languages

- Dutch: HTTP Push Aantal
- French: Compteur (HTTP Push)
- German: HTTP Push-Anzahl
- Japanese: HTTP プッシュ数
- Portuguese: Contagem de push (HTTP)
- Russian: HTTP: Количество push-объектов
- Simplified Chinese: HTTP 推送计数
- Spanish: Recuento Push (HTTP)

### Remarks

Consider the following [remarks](#)<sup>[1108]</sup> and requirements for this sensor:

Remark	Description
Remote probe	If you want to add this sensor to a remote probe and use an HTTPS connection to send push notifications, you must import a Secure Sockets Layer (SSL) certificate into the \cert subfolder of the <a href="#">PRTG program directory</a> on the remote probe. However, this certificate does not have to match the certificate that you use on the PRTG core server. For more information about SSL certificates, see the Paessler website: <a href="#">How to use your own SSL certificate with the PRTG web server</a>
Cluster probe	This sensor does not support cluster probes. You can only set it up on local probes or remote probes.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- HttpPushSensor
- PushCount
- PushSensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) .

## HTTP Push

**HTTP Push**

TLS Settings ⓘ *HTTP (unsecure)*

Port ⓘ 5050

Request Method ⓘ  ANY  
 GET (default)  
 POST

Identification Token ⓘ 12345678-ABCD-EFGH-87654321

---

Request Handling ⓘ  Discard request  
 Store request

HTTP Push

Setting	Description
TLS Settings	<p>Define the security of the incoming HTTP push requests:</p> <ul style="list-style-type: none"> <li>▪ HTTP (unsecure): Send push messages to the probe system via HTTP (not secure).</li> <li>▪ HTTPS low security (TLS 1.0 to 1.3 and weak ciphers): Send push messages to the probe system via HTTPS. The sensor supports connections secured with TLS 1.0 to TLS 1.3 and weak ciphers. It uses the SSL certificate that is delivered with PRTG or <a href="#">your own trusted SSL certificate</a> that you imported for the PRTG web server. <ul style="list-style-type: none"> <li>ⓘ If you install the sensor on a remote probe, make sure that you import the same SSL certificates to the remote probe that you use on the PRTG core server.</li> </ul> </li> <li>▪ HTTPS high security (TLS 1.2 to 1.3 and strong ciphers): Send push messages to the probe system via HTTPS. The sensor supports connections secured with TLS 1.2 to TLS 1.3 and strong ciphers. It uses the SSL certificate that is delivered with PRTG or <a href="#">your own trusted SSL certificate</a> that you imported for the PRTG web server. <ul style="list-style-type: none"> <li>ⓘ If you install the sensor on a remote probe, make sure that you import the same SSL certificates to the remote probe that you use on the PRTG core server.</li> </ul> </li> </ul> <p>ⓘ You cannot change this value after sensor creation.</p>
Port	<p><b>This setting is only visible if you select HTTP (unsecure) above.</b></p> <p>Enter the number of the port on which this sensor listens for incoming HTTP requests. The default port is <b>5050</b>.</p> <p>ⓘ You cannot change this value after sensor creation.</p>

Setting	Description
TLS Port	<p>This setting is only visible if you select <a href="#">HTTPS low security (TLS 1.0 to 1.3 and weak ciphers)</a> or <a href="#">HTTPS high security (TLS 1.2 to 1.3 and strong ciphers)</a> <a href="#">above</a>.</p> <p>Enter the number of the port on which this sensor listens for incoming HTTPS requests. The default port is <b>5051</b>.</p> <p><b>i</b> You cannot change this value after sensor creation.</p>
Request Method	<p>Select the request method of the webhook:</p> <ul style="list-style-type: none"> <li>any: Do not use any filter for the request method.</li> <li>GET (default): Select this method if the webhook uses GET.</li> <li>POST: Select this method if the webhook sends POST data. <ul style="list-style-type: none"> <li><b>i</b> POST data must be form-encoded request bodies with the same parameters as for GET requests.</li> </ul> </li> </ul>
Identification Token	<p>This is the token that PRTG uses to find the matching sensor for the incoming message. When you create the sensor, this token is <code>{_guid_}</code>.</p> <p>PRTG replaces this token with an automatically generated token after sensor creation. If you want to use a different identification token, you can edit it during or after sensor creation.</p> <p><b>i</b> PRTG does not automatically replace the token if you change it already during sensor creation.</p>
Request Handling	<p>Define what PRTG does with the incoming messages:</p> <ul style="list-style-type: none"> <li>Discard request: Do not store the pushed messages.</li> <li>Store result: Store the last message received from the sensor in the <code>\Logs\sensors</code> subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Request for Sensor [ID].txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul>

## Sensor Display




**Sensor Display**

Primary Channel **i** Downtime


---


Graph Type **i** 
 Show channels independently (default)
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## How to Use

This function is known as [webhook](#). Basically, a webhook works like a push notification. Webhooks are usually triggered by an event (for example, a new comment on a blog post) and send according information to a specified URL. The HTTP Push Count sensor then displays the number of pushed and received messages.

The HTTP Push Count sensor uses the following URL:

[http://<probe\\_ip>:<port\\_number>/<token>](http://<probe_ip>:<port_number>/<token>)

Replace the parameters [<probe\\_ip>](#), [<port\\_number>](#), and [<token>](#) with the corresponding values.

- The [<probe\\_ip>](#) is the IP address of the probe system with the sensor.

- The `<port_number>` is where the sensor listens for incoming HTTP calls.
- The `<token>` is used to define the matching sensor.

Example:

```
http://192.0.2.0:5050/XYZ123
```

- ⓘ You can use several sensors with the same port and identification token. In this case, the number of push messages is shown in each of these sensors.

## Channel List

- ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Messages Received	The number of messages received ⓘ This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

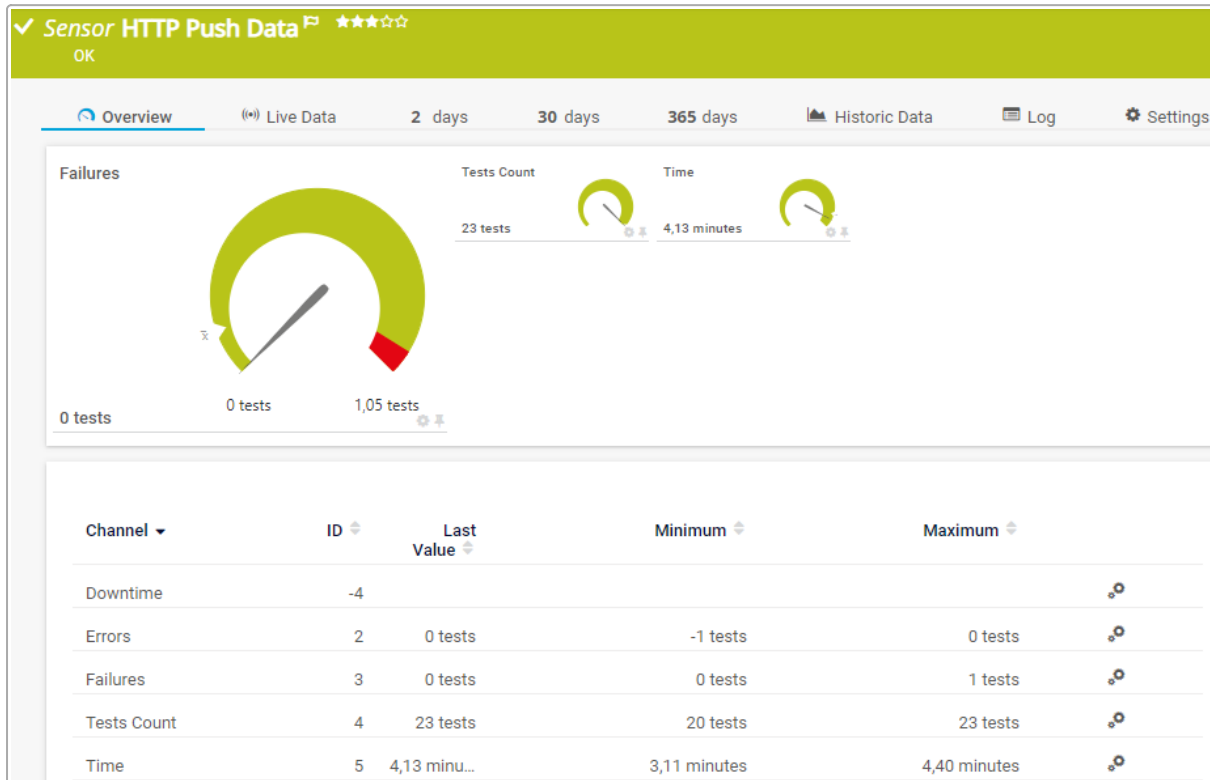
My HTTP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/85284>

## 7.8.69 HTTP Push Data Sensor

The HTTP Push Data sensor displays numeric values from received messages that are pushed via an HTTP request to PRTG. It provides a URL that you can use to push messages to the probe system via HTTP (secured with TLS 1.2 or not secure).

**i** For more information about the sensor usage, see section [How to Use](#)<sup>[1120]</sup>.



HTTP Push Data Sensor

**■** For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1120]</sup>.


### Sensor in Other Languages

- Dutch: HTTP Push Data
- French: Données (HTTP Push)
- German: HTTP Push-Daten
- Japanese: HTTP プッシュデータ
- Portuguese: Dados de push HTTP
- Russian: Данные push-объекта HTTP
- Simplified Chinese: HTTP 推送数据
- Spanish: Datos push (HTTP)



## Remarks

Consider the following [remarks](#)<sup>1115</sup> and requirements for this sensor:

Remark	Description
Remote probe	If you want to add this sensor to a remote probe and use an HTTPS connection to send push notifications, you must import a Secure Sockets Layer (SSL) certificate into the \cert subfolder of the <a href="#">PRTG program directory</a> on the remote probe. However, this certificate does not have to match the certificate that you use on the PRTG core server. For more information about SSL certificates, see the Paessler website: <a href="#">How to use your own SSL certificate with the PRTG web server</a>
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
False alerts	This sensor might result in false alerts if the parent probe disconnects from the PRTG core server. In this case, the sensor shows the error message: <a href="#">The latest push message that the sensor received is older than the specified time threshold allows.</a> (code: PE222).
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag × +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- HttpPushSensor
- PushData
- PushSensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## HTTP Push

**HTTP Push**

TLS Settings ⓘ *HTTP (unsecure)*

Port ⓘ 5050

Request Method ⓘ  ANY  
 GET (default)  
 POST




Identification Token ⓘ 12345678-ABCD-EFGH-87654321

---

Request Handling ⓘ  Discard request  
 Store request

HTTP Push

Setting	Description
TLS Settings	<p>Define the security of the incoming HTTP push requests:</p> <ul style="list-style-type: none"> <li>▪ HTTP (unsecure): Send push messages to the probe system via HTTP (not secure).</li> <li>▪ HTTPS low security (TLS 1.0 to 1.3 and weak ciphers): Send push messages to the probe system via HTTPS. The sensor supports connections secured with TLS 1.0 to TLS 1.3 and weak ciphers. It uses the SSL certificate that is delivered with PRTG or <a href="#">your own trusted SSL certificate</a> that you imported for the PRTG web server. <ul style="list-style-type: none"> <li>ⓘ If you install the sensor on a remote probe, make sure that you import the same SSL certificates to the remote probe that you use on the PRTG core server.</li> </ul> </li> <li>▪ HTTPS high security (TLS 1.2 to 1.3 and strong ciphers): Send push messages to the probe system via HTTPS. The sensor supports connections secured with TLS 1.2 to TLS 1.3 and strong ciphers. It uses the SSL certificate that is delivered with PRTG or <a href="#">your own trusted SSL certificate</a> that you imported for the PRTG web server. <ul style="list-style-type: none"> <li>ⓘ If you install the sensor on a remote probe, make sure that you import the same SSL certificates to the remote probe that you use on the PRTG core server.</li> </ul> </li> </ul> <p>ⓘ You cannot change this value after sensor creation.</p>
Port	<p><b>This setting is only visible if you select HTTP (unsecure) above.</b></p> <p>Enter the number of the port on which this sensor listens for incoming HTTP requests. The default port is <b>5050</b>.</p> <p>ⓘ You cannot change this value after sensor creation.</p>

Setting	Description
<p>TLS Port</p>	<p>This setting is only visible if you select <a href="#">HTTPS low security</a> (TLS 1.0 to 1.3 and weak ciphers) or <a href="#">HTTPS high security</a> (TLS 1.2 to 1.3 and strong ciphers) <a href="#">above</a>.</p> <p>Enter the number of the port on which this sensor listens for incoming HTTPS requests. The default port is <a href="#">5051</a>.</p> <p> You cannot change this value after sensor creation.</p>
<p>Request Method</p>	<p>Select the request method of the webhook:</p> <ul style="list-style-type: none"> <li>▪ any: Do not use any filter for the request method.</li> <li>▪ GET (default): Select this method if the webhook uses GET.</li> <li>▪ POST: Select this method if the webhook sends POST data.</li> </ul> <p> POST data must be form-encoded request bodies with the same parameters as for GET requests.</p>
<p>Identification Token</p>	<p>This is the token that PRTG uses to find the matching sensor for the incoming message. When you create the sensor, this token is <a href="#">{__guid__}</a>.</p> <p>PRTG replaces this token with an automatically generated token after sensor creation. If you want to use a different identification token, you can edit it during or after sensor creation.</p> <p> PRTG does not automatically replace the token if you change it already during sensor creation.</p>
<p>Request Handling</p>	<p>Define what PRTG does with the incoming messages:</p> <ul style="list-style-type: none"> <li>▪ Discard request: Do not store the pushed messages.</li> <li>▪ Store result: Store the last message received from the sensor in the <code>\Logs\sensors</code> subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Request for Sensor [ID].txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul>

## HTTP Push Data

**HTTP Push Data**

**No Incoming Data** ⓘ

Ignore and keep last status (default)

Switch to unknown status

Switch to down status after x minutes

**Value Type** ⓘ

Integer

Float

HTTP Push Data

Setting	Description
No Incoming Data	<p>Define which <a href="#">status</a> the sensor shows if it does not receive a push message for at least two scanning intervals:</p> <ul style="list-style-type: none"> <li>Ignore and keep last status (default): Keep the status as defined by the last message that the sensor received. <ul style="list-style-type: none"> <li>ⓘ The parent probe must be connected to keep the last status. If the parent probe disconnects, the sensor shows the Unknown status. If the parent probe connects again, the sensor does not automatically switch from the Unknown status to the last status before the parent probe disconnected.</li> </ul> </li> <li>Switch to unknown status: Show the Unknown status if the sensor does not receive a message for at least two scanning intervals.</li> <li>Switch to down status after x minutes: Show the Down status if the sensor does not receive a message within a specific time span. Define the time threshold below.</li> </ul>
Time Threshold (Minutes)	<p><b>This setting is only visible if you select</b> Switch to down status after x minutes <b>above.</b></p> <p>Enter a time threshold in minutes. If this time elapses, the sensor shows the Down status if it does not receive a push message within this time span. Enter an integer. The maximum threshold is <b>1440</b> minutes.</p>
Value Type	<p>Define the type of the value of the received data:</p> <ul style="list-style-type: none"> <li>Integer</li> <li>Float (with a dot . between the predecimal position and the decimal places)</li> </ul> <p>ⓘ If this setting does not match, the sensor shows the Down status.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## How to Use

This function is known as [webhook](#). Basically, a webhook works like a push notification. Webhooks are usually triggered by an event (for example, a new comment on a blog post) and send according information to a specified URL. The HTTP Push Data sensor then displays the data of pushed and received messages.

The HTTP Push Data sensor uses the following URL:

`http://<probe_ip>:<port_number>/<token>?value=<integer_or_float>&text=<text message>`

Replace the parameters `<probe_ip>`, `<port_number>`, `<token>`, and `<integer_or_float>` with the corresponding values. The `&text` parameter is optional: You can omit it.

- You can define the [port number](#) and [identification token](#) in the sensor settings.
- The [probe IP](#) is the IP address of the probe system with this sensor.
- The [value](#) can be an integer or a float value depending on the data of your application. You must set the value type accordingly in the sensor settings. This parameter is the sensor value.
  - ❶ If this parameter is missing, the sensor shows a [Down status](#).
- You can optionally add a custom text message by replacing the parameter `<text message>` with your custom text. The text is shown as the sensor message. If there is no value but only a text, the text is shown as an error message.
  - ❶ This text message has to be URL encoded (for example, the whitespaces in the sample URL below). Most browsers do URL-encoding automatically.

Example:

`http://192.0.2.0:5050/XYZ123?value=0&text=this%20is%20a%20message`

- ❶ You can use several sensors with the same port and identification token. In this case, the data of push messages is shown in each of these sensors.

## Channel List

- ❶ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	The received value and an optional message in one channel ❶ This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

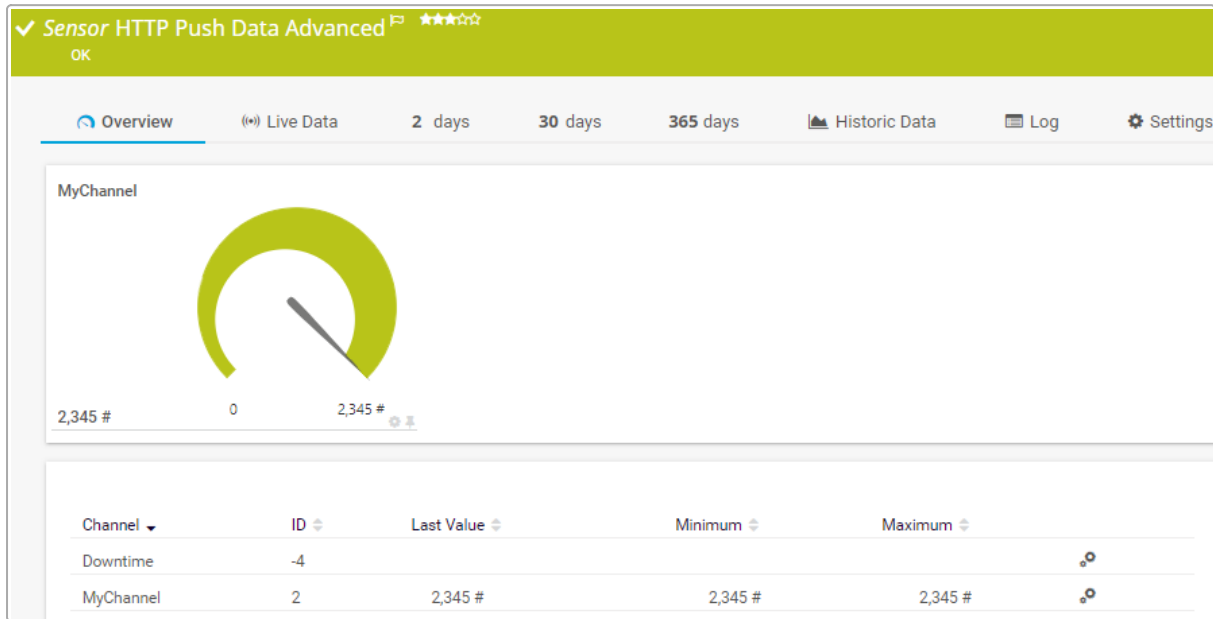
My HTTP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/85284>

## 7.8.70 HTTP Push Data Advanced Sensor

The HTTP Push Data Advanced sensor displays data from received messages that are pushed via an HTTP request to PRTG. It provides a URL that you can use to push messages to the probe system via HTTP (secured with TLS 1.2 or not secure).

**i** For more information about the sensor usage, see section [How to Use](#)<sup>[1127]</sup>.



HTTP Push Data Advanced Sensor

**■** For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1128]</sup>.


### Sensor in Other Languages

- Dutch: HTTP Push Data geavanceerd
- French: Données avancé (HTTP Push)
- German: HTTP Push-Daten (Erweitert)
- Japanese: HTTP プッシュデータ(アドバンスト)
- Portuguese: Dados de push HTTP avançado
- Russian: HTTP: Данные push-объекта (расширенный)
- Simplified Chinese: HTTP 高级推送数据
- Spanish: Datos push (avanzado) (HTTP)

### Remarks

Consider the following [remarks](#)<sup>[1122]</sup> and requirements for this sensor:



Remark	Description
Remote probe	If you want to add this sensor to a remote probe and use an HTTPS connection to send push notifications, you must import a Secure Sockets Layer (SSL) certificate into the \cert subfolder of the <a href="#">PRTG program directory</a> on the remote probe. However, this certificate does not have to match the certificate that you use on the PRTG core server. For more information about SSL certificates, see the Paessler website: <a href="#">How to use your own SSL certificate with the PRTG web server</a>
Cluster probe	This sensor does not support cluster probes. You can only set it up on local probes or remote probes.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
Multiple channels	If you use this sensor with multiple channels, we recommend that you <b>simultaneously</b> push the data for <b>all</b> your channels to PRTG. You can push data to only one of your channels. However, all other channels record the value of <b>0</b> for this push message.
False alerts	This sensor might result in false alerts if the parent probe disconnects from the PRTG core server. In this case, the sensor shows the error message: <a href="#">The latest push message that the sensor received is older than the specified time threshold allows. (code: PE222)</a> .
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- HttpPushSensor

- PushData
- PushSensor

For more information about basic sensor settings, see section [Sensor Settings](#) [667].

## HTTP Push

**HTTP Push**

TLS Settings ⓘ *HTTP (unsecure)*

Port ⓘ 5050

Request Method ⓘ  ANY  
 GET (default)  
 POST

Identification Token ⓘ 12345678-ABCD-EFGH-87654321

Request Handling ⓘ  Discard request  
 Store request

HTTP Push

Setting	Description
TLS Settings	<p>Define the security of the incoming HTTP push requests:</p> <ul style="list-style-type: none"> <li>▪ HTTP (unsecure): Send push messages to the probe system via HTTP (not secure).</li> <li>▪ HTTPS low security (TLS 1.0 to 1.3 and weak ciphers): Send push messages to the probe system via HTTPS. The sensor supports connections secured with TLS 1.0 to TLS 1.3 and weak ciphers. It uses the SSL certificate that is delivered with PRTG or <a href="#">your own trusted SSL certificate</a> that you imported for the PRTG web server. <ul style="list-style-type: none"> <li>ⓘ If you install the sensor on a remote probe, make sure that you import the same SSL certificates to the remote probe that you use on the PRTG core server.</li> </ul> </li> <li>▪ HTTPS high security (TLS 1.2 to 1.3 and strong ciphers): Send push messages to the probe system via HTTPS. The sensor supports connections secured with TLS 1.2 to TLS 1.3 and strong ciphers. It uses the SSL certificate that is delivered with PRTG or <a href="#">your own trusted SSL certificate</a> that you imported for the PRTG web server. <ul style="list-style-type: none"> <li>ⓘ If you install the sensor on a remote probe, make sure that you import the same SSL certificates to the remote probe that you use on the PRTG core server.</li> </ul> </li> </ul> <p>ⓘ You cannot change this value after sensor creation.</p>

Setting	Description
Port	<p>This setting is only visible if you select HTTP (unsecure) <a href="#">above</a>.</p> <p>Enter the number of the port on which this sensor listens for incoming HTTP requests. The default port is <b>5050</b>.</p> <p><b>i</b> You cannot change this value after sensor creation.</p>
TLS Port	<p>This setting is only visible if you select HTTPS low security (TLS 1.0 to 1.3 and weak ciphers) or HTTPS high security (TLS 1.2 to 1.3 and strong ciphers) <a href="#">above</a>.</p> <p>Enter the number of the port on which this sensor listens for incoming HTTPS requests. The default port is <b>5051</b>.</p> <p><b>i</b> You cannot change this value after sensor creation.</p>
Request Method	<p>Select the request method of the webhook:</p> <ul style="list-style-type: none"> <li>▪ any: Do not use any filter for the request method.</li> <li>▪ GET (default): Select this method if the webhook uses GET.</li> <li>▪ POST: Select this method if the webhook sends POST data.</li> </ul> <p><b>i</b> POST data must be form-encoded request bodies with the same parameters as for GET requests.</p>
Identification Token	<p>This is the token that PRTG uses to find the matching sensor for the incoming message. When you create the sensor, this token is <code>{_guid_}</code>.</p> <p>PRTG replaces this token with an automatically generated token after sensor creation. If you want to use a different identification token, you can edit it during or after sensor creation.</p> <p><b>i</b> PRTG does not automatically replace the token if you change it already during sensor creation.</p>
Request Handling	<p>Define what PRTG does with the incoming messages:</p> <ul style="list-style-type: none"> <li>▪ Discard request: Do not store the pushed messages.</li> <li>▪ Store result: Store the last message received from the sensor in the <code>\Logs\sensors</code> subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Request for Sensor [ID].txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul>

## HTTP Push Data

**HTTP Push Data**

**No Incoming Data** ⓘ  Ignore and keep last status (default)  
 Switch to unknown status  
 Switch to down status after x minutes

HTTP Push Data

Setting	Description
No Incoming Data	<p>Define which <a href="#">status</a> the sensor shows if it does not receive a push message for at least two scanning intervals:</p> <ul style="list-style-type: none"> <li>▪ Ignore and keep last status (default): Keep the status as defined by the last message that the sensor received.               <ul style="list-style-type: none"> <li>ⓘ The parent probe must be connected to keep the last status. If the parent probe disconnects, the sensor shows the Unknown status. If the parent probe connects again, the sensor does not automatically switch from the Unknown status to the last status before the parent probe disconnects.</li> </ul> </li> <li>▪ Switch to unknown status: Show the Unknown status if the sensor does not receive a message for at least two scanning intervals.</li> <li>▪ Switch to down status after x minutes: Show the Down status if the sensor does not receive a message within a specific time span. Define the time threshold below.</li> </ul>
Time Threshold (Minutes)	<p><b>This setting is only visible if you select</b> Switch to down status after x minutes <b>above.</b></p> <p>Enter a time threshold in minutes. If this time elapses, the sensor shows the Down status if it does not receive a push message within this time span. Enter an integer. The maximum threshold is <b>1440</b> minutes.</p>

## Sensor Display




**Sensor Display**

**Primary Channel** ⓘ Downtime


---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## How to Use

This function is known as [webhook](#). Basically, a webhook works like a [push notification](#). Webhooks are usually triggered by some event (for example, a new comment on a blog post) and send according information to a specified URL. The HTTP Push Data Advanced sensor then displays the data of pushed and received messages.

The data that is pushed to this sensor must be valid XML or JSON.

 For more information about the return value format, see section [Custom Sensors](#).

The HTTP Push Data Advanced sensor uses the following URLs depending on the type of HTTP request:

- GET (default) requests: `http://<probe_ip>:<port_number>/<token>?content=<valid XML_or_JSON>`

The XML encoded value of the content parameter has to match the format as defined in section [Custom Sensors](#).

- POST requests: `http://<probe_ip>:<port_number>/<token>`

This HTTP request method sends the XML or JSON encoded HTTP body as POST data. The body has to match the format as defined in section [Custom Sensors](#). For POST requests, use an HTTP content type other than `application/x-www-form-urlencoded`. We strongly recommend the HTTP content type `application/xml` or `application/json`.

Replace the parameters `<probe_ip>`, `<port_number>`, `<token>`, and `<valid XML_or_JSON>` (for GET requests) with the corresponding values:

- You can define [port number](#) and [identification token](#) in the sensor settings.
- The [probe IP](#) is the IP address of the probe system with this sensor.
- The content of GET requests has to be valid XML or JSON in the PRTG API format.
  - ❶ The content has to be URL encoded (for example, the whitespaces in the sample URL below). Most browsers do URL-encoding automatically.

Minimum example for the GET method that returns one static channel value:

```
http://127.0.0.1:5050/XYZ123?
content=<prtg><result><channel>MyChannel</channel><value>10</value></result><text>this%20is%20a%20message</text></prtg>
```

- ❶ By default, values within the `<value>` tags in the returned XML or JSON must be [integers](#) to be processed. If [float](#) values are returned, you must explicitly define this value type as defined in section [Custom Sensors](#) with `<float>` tags, otherwise the sensor shows **0** values in affected channels. Example:



```
http://127.0.0.1:5050/XYZ123?
content=<prtg><result><channel>MyChannel</channel><value>10.45</value><float>1</float></result><text>this%20is%20a%20message</text></prtg>
```

- ❶ You can use several sensors with the same port and identification token. In this case, the data of push messages is shown in each of these sensors.

## Channel List

- ❶ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
[Value]	<p>The data received from the message encoded in valid XML or JSON in several channels</p> <p> This channel is the primary channel by default.</p> <p> For more information about the return value format, see section <a href="#">Custom Sensors</a>.</p>

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

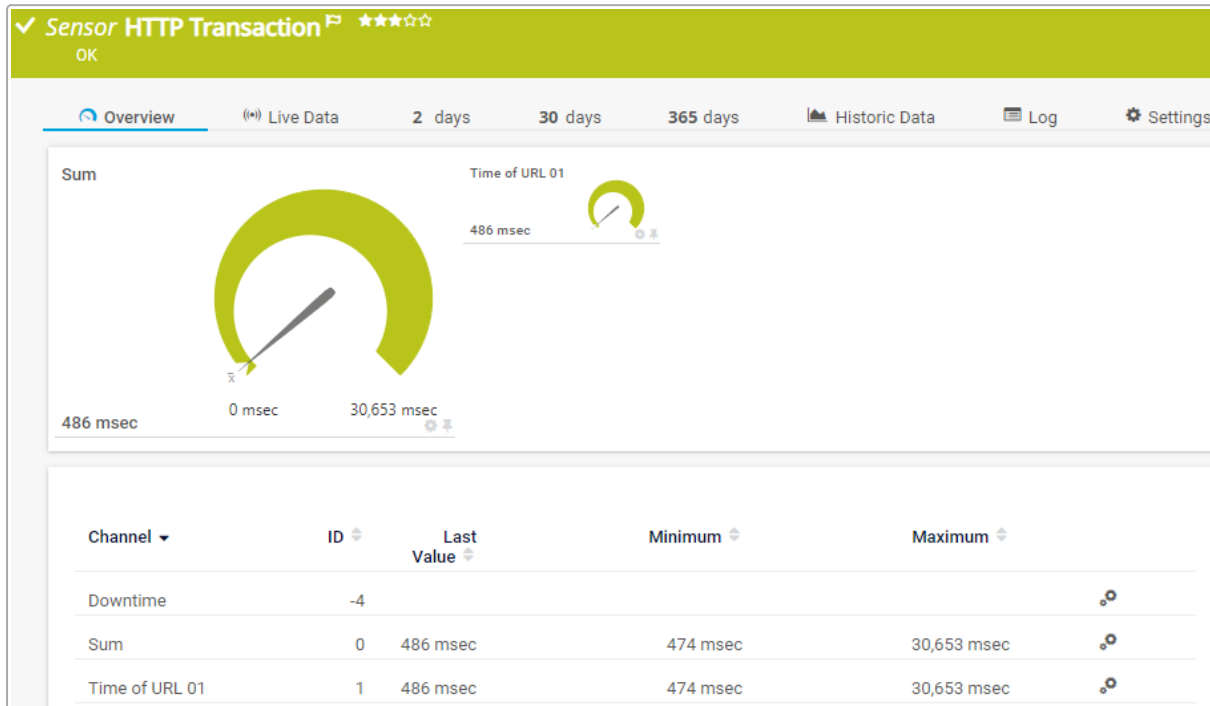
My HTTP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/85284>

## 7.8.71 HTTP Transaction Sensor

The HTTP Transaction sensor monitors an interactive website, such as a web shop, by performing a transaction using a set of HTTP URLs. The sensor monitors whether logins or shopping carts work properly.

**i** This sensor implicitly supports SNI, an extension to the Transport Layer Security (TLS) protocol.



HTTP Transaction Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1140]</sup>.

### Sensor in Other Languages

- Dutch: HTTP (Transactie)
- French: Transaction (HTTP)
- German: HTTP (Transaktion)
- Japanese: HTTP トランザクション
- Portuguese: Transação HTTP
- Russian: Транзакция HTTP
- Simplified Chinese: HTTP 处理
- Spanish: Transacción HTTP

### Remarks

Consider the following [remarks](#)<sup>[1130]</sup> and requirements for this sensor:



Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
SRP ciphers	This sensor does not support Secure Remote Password (SRP) ciphers. If you need to use SRP ciphers, use the Compatibility engine.
Smart URL replacement	This sensor supports <a href="#">smart URL replacement</a> <sup>[1139]</sup> .
IPv6	This sensor supports IPv6.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">Configuration tips for HTTP Transaction sensors needed</a></li> <li>Knowledge Base: <a href="#">Which user agent should I use in the HTTP Advanced sensor's settings?</a></li> </ul>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- httptransactionsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## HTTP Specific

### HTTP Specific

**Timeout (Sec.)** ⓘ

---

**Single URL Timeout (Sec.)** ⓘ

HTTP Specific

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for all HTTP requests. Enter an integer. The maximum value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the complete transaction takes longer than this value, the sensor cancels the request and shows an according error message. If two consecutive requests are unsuccessful (for whatever reason), the sensor shows the Down <a href="#">status</a>.</p>
Single URL Timeout (Sec.)	<p>Enter a timeout in seconds for one single HTTP request. Enter an integer. The maximum value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply of any single request takes longer than this value, the sensor cancels the transaction and shows an according error message.</p>

## Monitoring Engine

**Monitoring Engine** Monitoring Engine **i**

Default  
 Compatibility engine

Monitoring Engine

Setting	Description
Monitoring Engine	<p>Choose the monitoring engine that the sensor uses:</p> <ul style="list-style-type: none"> <li>▪ Default: Use the default monitoring engine.</li> <li>▪ Compatibility engine: Execute an external executable program. Use this method as an alternative for websites that do not work with the default monitoring engine.             <ul style="list-style-type: none"> <li><b>i</b> This method needs more resources but it can be helpful in some cases.</li> <li><b>i</b> If you select the compatibility mode, the options for the SSL method are different. You can also check for trusted certificates. See below.</li> <li><b>i</b> Smart URL Replacement does not work with the compatibility mode, so this sensor does <b>not</b> automatically use the IP Address/DNS Name of the parent device.</li> </ul> </li> </ul>
SSL/TLS Method	<p><b>This setting is only visible if you select Compatibility engine above.</b></p> <p>Select the SSL/TLS method:</p> <ul style="list-style-type: none"> <li>▪ SSLv3</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ TLS 1.0, TLS 1.1, TLS 1.2</li> <li>▪ SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 (default)</li> </ul>
Check SSL Certificates	<p>This setting is only visible if you select Compatibility engine <a href="#">above</a>.</p> <p>Specify if the sensor checks the certificate of the URL:</p> <ul style="list-style-type: none"> <li>▪ Do not check certificates (default): Do not check the certificates of the web pages.</li> <li>▪ Check if certificates are trusted: Check the certificates of the web pages. If the certificate of the server is not trusted, the sensor shows the Down <a href="#">status</a> and displays a corresponding message.</li> </ul>

### Advanced Sensor Data

**Advanced Sensor Data**

Download Limit (KB) ⓘ 0

---

Cookie Management ⓘ  Use cookies (default)  
 Ignore

User Agent ⓘ  Use the default string  
 Use a custom string

Result Handling ⓘ  Discard result (default)  
 Store result

Advanced Sensor Data

Setting	Description
Download Limit (KB)	<p>Enter a number that defines the maximum amount of data (in kilobytes) that the sensor transfers per request.</p> <p><b>i</b> If you set content checks, be aware that they might be incomplete. This is because the sensor only checks the content that is downloaded up to this limit for search expressions.</p>
Cookie Management	<p>Select if you want to allow cookies for the transaction:</p> <ul style="list-style-type: none"> <li>▪ Use cookies (default): Allow cookies to be set and read during the transaction cycle. We recommend that you use this option.</li> <li>▪ Ignore: Do not allow cookies. Use this option if you want to test the transaction without the use of cookies.</li> </ul>

Setting	Description
User Agent	<p>Choose which user agent string the sensor sends when it connects to the target URL:</p> <ul style="list-style-type: none"> <li>▪ Use the default string: Do not enter a specific user agent and use the default string. Usually, this is <a href="#">Mozilla/5.0 (compatible; PRTG Network Monitor (www.paessler.com); Windows)</a>.</li> <li>▪ Use a custom string: Use a custom user agent. Define the custom user agent below.</li> </ul>
Custom User Agent	<p><a href="#">This setting is only visible if you select Use a custom string above.</a></p> <p>Enter the string that the sensor uses as the user agent when it connects to the target URL.</p>
Result Handling	<p>Define what PRTG does with the web page that is loaded at the URL:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last result of the web page in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID]-1.txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes, especially in combination with content checks. PRTG overwrites the files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>


## Authentication

**Authentication**

Authentication ⓘ  Web page does not need authentication (default)  
 Web page needs authentication

Authentication

Setting	Description
Authentication	<p>Define if authentication is necessary on the web page:</p> <ul style="list-style-type: none"> <li>▪ Web page does not need authentication (default)</li> <li>▪ Web page needs authentication</li> </ul>

Setting	Description
User Name	<p>This setting is only visible if you select Web page needs authentication above.</p> <p>If the proxy requires authentication, enter the user name for the proxy login. Enter a string.</p>
Password	<p>This setting is only visible if you select Web page needs authentication above.</p> <p>Enter a password.</p>
Authentication Method	<p>This setting is only visible if you select Web page needs authentication above.</p> <p>Select the authentication method that the URL uses:</p> <ul style="list-style-type: none"> <li>▪ HTTP authentication (default): Use simple HTTP authentication. <ul style="list-style-type: none"> <li> This authentication method transmits credentials as plain text.</li> </ul> </li> <li>▪ NT LAN Manager authentication: Use the Microsoft NT LAN Manager (NTLM) protocol for authentication.</li> <li>▪ Digest access authentication: Use digest access authentication. This applies a hash function to the password, which is safer than HTTP authentication (default).</li> </ul>

## Transaction URL

You can define up to 10 different transaction URLs, which are all called in a row. If the transaction can be completed, the sensor shows the Up status. Using this mechanism, you can set up extended monitoring with multiple URLs.

Enter settings for at least one transaction URL. You can use as many steps as necessary and disable the other steps.

**Transaction URL #1**

URL ⓘ

Request Method ⓘ  GET (default)  
 POST  
 HEAD

Require Keyword ⓘ  Do not check for keyword (default)  
 Set sensor to warning status if keyword is missing  
 Set sensor to down status if keyword is missing

Exclude Keyword ⓘ  Do not check for keyword (default)  
 Set sensor to warning status if keyword is found  
 Set sensor to down status if keyword is found

**Transaction URL #2**

Transaction Step #2 ⓘ  Disable step #2 (default)  
 Enable step #2

Transaction URL #x

Setting	Description
Transaction Step #x	<p>This setting is available for URL #2 through #10. Define if you want to use this step for the transaction check:</p> <ul style="list-style-type: none"> <li>▪ Disable step #x (default): Do not use this step. Choose this option if you do not need all 10 steps for the transaction check.</li> <li>▪ Enable step #x: Enable this step. Further options are available.</li> </ul>
URL	<p>Enter the URL that the sensor connects to. If you enter an absolute URL, the sensor uses this address independently of the IP Address/DNS Name setting of the parent device.</p> <p><b>ⓘ</b> The URL must not be <a href="#">URL encoded</a>.</p> <p><b>■</b> PRTG uses a smart URL replacement with which you can use the parent device's IP address or Domain Name System (DNS) name setting as part of the URL. For more information, see section <a href="#">Smart URL Replacement</a> [1139].</p>
Request Method	<p>Select an HTTP request method to determine how the sensor requests the URL:</p> <ul style="list-style-type: none"> <li>▪ GET (default): Directly request the website.</li> </ul> <p><b>ⓘ</b> We recommend that you use this setting for a simple check of the web page.</p>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ <b>POST:</b> Send post form data to the URL.               <ul style="list-style-type: none"> <li>❗ If you select this setting, you must enter the data in the Postdata field below.</li> <li>❗ If a POST request is redirected, all further requests are GET (default) requests.</li> </ul> </li> <li>▪ <b>HEAD:</b> Only request the HTTP header from the server without the actual web page.               <ul style="list-style-type: none"> <li>❗ Although this saves bandwidth because it transfers less data, we do not recommended that you use this. This is because the measured request time is not the one that your users experience and you might not be notified of slow results or timeouts.</li> </ul> </li> </ul>
Postdata	<p><a href="#">This setting is only visible if you select POST above.</a></p> <p>Enter the data part for the POST request.</p> <ul style="list-style-type: none"> <li>❗ No Extensible Markup Language (XML) is allowed here.</li> </ul>
Require Keyword	<p>Define if the sensor checks the result at the URL for keywords:</p> <ul style="list-style-type: none"> <li>▪ Do not check for keyword (default): Do not search for keywords in the result.</li> <li>▪ Set sensor to warning status if keyword is missing: Check if a keyword exists in the result. If it exists, set the sensor to the Warning status.</li> <li>▪ Set sensor to down status if keyword is missing: Check if a keyword exists in the result. If it exists, set the sensor to the Down status.</li> </ul> <ul style="list-style-type: none"> <li>❗ The content check is only intended for HTML websites and might not work with other target URLs.</li> </ul>
Response Must Include	<p><a href="#">This setting is only visible if you select Set sensor to warning status if keyword is missing or Set sensor to down status if keyword is missing above.</a></p> <p>Define the search string that must be part of the result at the URL.</p> <ul style="list-style-type: none"> <li>❗ If the result at the URL does <b>not</b> include the search pattern, the sensor shows the status defined above and displays this string along with the affected URL in the sensor message.</li> <li>❗ Only simple text search is available here.</li> <li>❗ The characters <b>*</b> and <b>?</b> work as placeholders. <b>*</b> stands for no number or any number of characters and <b>?</b> stands for exactly one character. You cannot change this behavior. The literal search for these characters is not possible.</li> </ul>
Exclude Keyword	<p>Define if the sensor checks the result at the URL for keywords:</p>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Do not check for keyword (default): Do not search for keywords in the result.</li> <li>▪ Set sensor to warning status if keyword is found: Check if a keyword exists in the result. If it exists, set the sensor to the Warning status.</li> <li>▪ Set sensor to down status if keyword is found: Check if a keyword exists in the result. If it exists, set the sensor to the Warning status.</li> </ul> <p><b>i</b> The content check is only intended for HTML websites and might not work with other target URLs.</p>
Response Must Not Include	<p>Define a string that must not be part of the result at the URL. If the data includes this string, the sensor shows the Down status and displays this string along with the affected URL in the sensor message. Enter a string.</p> <p><b>i</b> Only simple text search is available here.</p> <p><b>i</b> The characters * and ? work as placeholders. * stands for no number or any number of characters and ? stands for exactly one character. You cannot change this behavior. The literal search for these characters is not possible.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime


---

Graph Type **i** 
 Show channels independently (default)
   
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can only enter the protocol followed by a colon and three forward slashes (this means that you can enter either [http://](#) or [https://](#), or even a simple forward slash / as the equivalent for [http://](#)). PRTG automatically fills in the parent device's IP Address/DNS Name in front of the third forward slash.

Whether this results in a valid URL or not depends on the IP address or Domain Name System (DNS) name of the parent device. In combination with cloning devices, you can use smart URL replacement to create many similar devices.

For example, if you create a device with the DNS name [www.example.com](#) and you add an HTTP sensor to it, you can provide values in the following ways:

- If you enter [https://](#) in the URL field, PRTG automatically creates the URL [https://www.example.com/](#)
- If you enter [/help](#) in the URL field, PRTG automatically creates and monitor the URL [http://www.example.com/help](#)
- It is also possible to provide a port number in the URL field. It is taken over by the device's DNS name and is internally added, for example, [http://:8080/](#)

 Smart URL replacement does not work for sensors that run on the probe device.

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Sum	The loading time of the complete transaction <b>i</b> This channel is the primary channel by default.
Time of URL [#]	The loading time of single URLs

## More

### ■ KNOWLEDGE BASE

Configuration tips for HTTP Transaction sensors needed

- <https://kb.paessler.com/en/topic/443>

Which user agent should I use in the HTTP Advanced sensor's settings?

- <https://kb.paessler.com/en/topic/30593>

What security features does PRTG include?

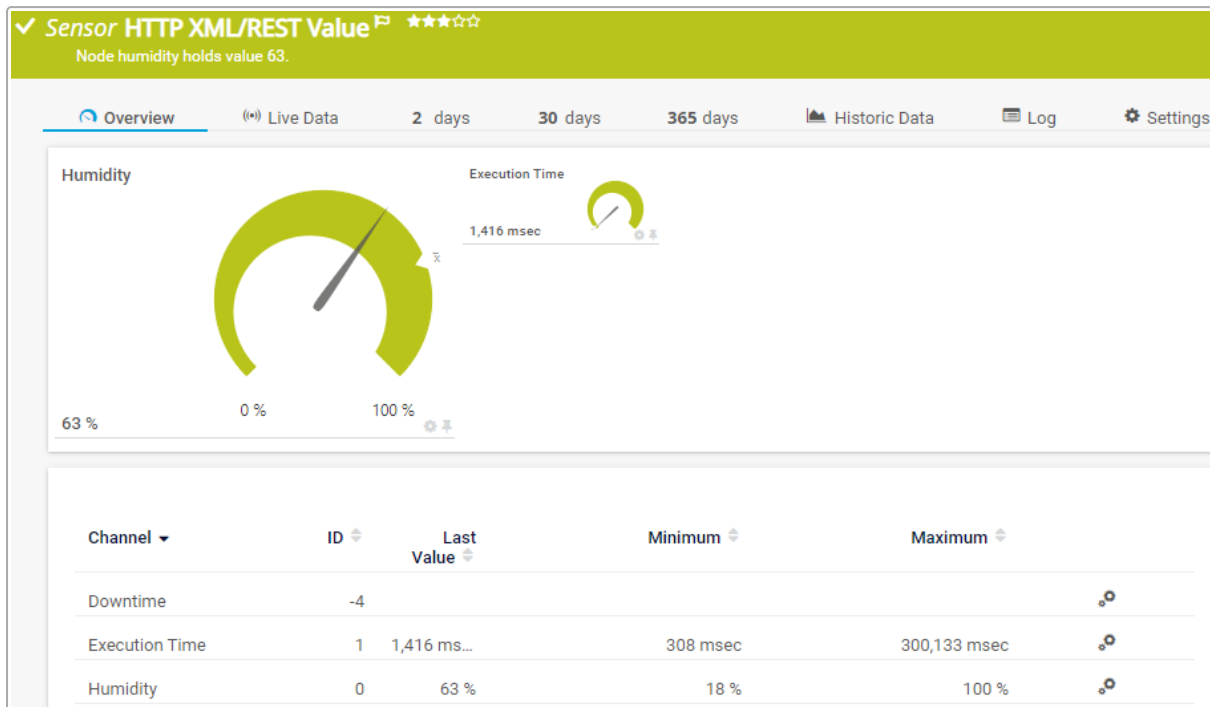
- <https://kb.paessler.com/en/topic/61108>

My HTTP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/85284>

## 7.8.72 HTTP XML/REST Value Sensor

The HTTP XML/REST Value sensor retrieves an .xml file from a URL and parses it.



HTTP XML/REST Value Sensor



For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1150]</sup>.

### Sensor in Other Languages


- Dutch: HTTP XML/REST Waarde
- French: Valeur XML/REST (HTTP)
- German: HTTP XML-/REST-Wert
- Japanese: HTTP XML/REST 値
- Portuguese: Valor HTTP XML/REST
- Russian: Значение HTTP XML/REST
- Simplified Chinese: HTTP XML/REST 值
- Spanish: Valor HTTP XML/REST

### Remarks

Consider the following [remarks](#)<sup>[1147]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node. If the sensor shows the error PE087, additionally install .NET 3.5 on the probe system.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Windows Server	We recommend Windows Server 2016 on the probe system for best performance of this sensor.
SRP ciphers	This sensor does not support Secure Remote Password (SRP) ciphers.
Smart URL replacement	This sensor supports <a href="#">smart URL replacement</a> <sup>[1150]</sup> .
IPv6	This sensor supports IPv6.
Single node	This sensor can monitor only one single node in an .xml file and shows the value in one channel. To monitor more than one node of an .xml document, add one sensor for each target node.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">Where can I find more information about the HTTP XML/REST Value sensor?</a></li> <li>▪ Knowledge Base: <a href="#">Which HTTP status code leads to which HTTP sensor status?</a></li> </ul>

## Add Sensor

Setting	Description
Channel Name	<p>Enter a name for the channel that displays the value at the URL.</p> <p> You can change this value later in the <a href="#">channel settings</a> of this sensor.</p>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- ptfensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Settings

### Sensor Settings

**URL** ⓘ

---

**XML Node (and optional property)** ⓘ

---

**HTTP User Name** ⓘ

---

**HTTP Password** ⓘ

---

**Sensor Value** ⓘ  Use the value of the selected XML node (default)  
 Use the number of occurrences of the selected XML node or its children/siblings

---

**Name Space Handling** ⓘ  Use name spaces  
 Remove name spaces

---

**Content Type** ⓘ  Enable (default)  
 Disable  
 Custom

---

**Remove Characters** ⓘ

---

**HTTP Headers** ⓘ

---

**Decimal Delimiter** ⓘ

---

**Custom Message** ⓘ





---





**If Channel Value Changes** ⓘ  Ignore (default)  
 Trigger 'change' notification

---

**Unit String** ⓘ

Sensor Settings

Setting	Description
URL	<p>Enter the URL that returns the .xml file. If you enter an absolute URL, the sensor uses this address independently of the IP Address/DNS Name setting of the parent device.</p> <p> The URL must be <a href="#">URL encoded</a>.</p> <p> PRTG uses a smart URL replacement with which you can use the parent device's IP address or Domain Name System (DNS) name setting as part of the URL. For more information, see section <a href="#">Smart URL Replacement</a> <sup>[1150]</sup>.</p>
XML Node (and optional property)	<p>Enter the name of the node that this sensor checks, or enter a node name and a property name to check a property value. To obtain a value from nested tags, enter the tag names and separate them with a forward slash (/). For example, use <a href="#">myTag/myTagInside</a> as XML node value.</p> <p> You can also check values in JavaScript Object Notation (JSON). See section <a href="#">Checking JSON</a> <sup>[1148]</sup>.</p> <p> You can try to use XPath syntax here but it does not work in all cases and we do not provide any technical support for XPath issues. For more information about XPath, see the Knowledge Base: <a href="#">How can I use XPath with the HTTP XML/REST Value sensor?</a></p>
HTTP User Name	<p>If the URL requires authentication, enter the user name. Enter a string or leave the field empty.</p>
HTTP Password	<p>If the URL requires authentication, enter the password. Enter a string or leave the field empty.</p>
Sensor Value	<p>Define what value the sensor shows:</p> <ul style="list-style-type: none"> <li>▪ Use the value of the selected XML node: Return the value that the sensor finds at the XML node. If this is a non-numeric value, the sensor shows 0.</li> <li>▪ Use the number of occurrences of the selected XML node or its children/siblings: Return the number of occurrences found. Define further settings below.</li> </ul>
Count XML Nodes	<p><a href="#">This setting is only visible if you select Use the number of occurrences of the selected XML node or its children/siblings</a> <a href="#">above</a>.</p> <p>Define which count the sensor shows:</p> <ul style="list-style-type: none"> <li>▪ Occurrences of the selected XML node: Return how often the defined XML node occurs at the URL.</li> <li>▪ Child nodes of the selected XML node: Return the number of child nodes that exist below the node at the URL.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Sibling nodes of the selected XML node: Return the number of sibling nodes that exist next to the node at the URL.</li> </ul>
Name Space Handling	<p>Define whether to use namespaces in the .xml document or not:</p> <ul style="list-style-type: none"> <li>▪ Use name spaces: Process the value you enter in the XML Node (and optional property) field, possibly including namespace information.</li> <li>▪ Remove name spaces: Ignore namespace information in the .xml document and process the value you enter in the XML Node (and optional property) field as node names only.</li> </ul> <p> For more information see section <a href="#">About Namespaces</a> .</p>
Content Type	<p>Define what to include in the header of the request that the sensor sends to the URL:</p> <ul style="list-style-type: none"> <li>▪ Enable (default): This works for most web servers and is the recommended setting.</li> <li>▪ Disable: Only very few web servers cannot handle this content type and need this setting. Try this if you get an error message with the enabled option.</li> <li>▪ Custom: You can use a custom content type.</li> </ul>
Custom Content Type	<p><a href="#">This setting is only visible if you select Custom above.</a></p> <p>Enter a custom content type like <a href="#">text/xml</a> or <a href="#">text/html</a>.</p>
HTTP Headers	<p>Optionally enter a list of custom HTTP headers with their respective values that you want to transmit to the URL. The syntax of a list with header-value pairs is <a href="#">header1:value1 header2:value2 ... headerx:valuex</a></p> <p> The sensor does not accept header field names that include a dash (–) character. If you want to use such an HTTP header, leave out the dash in the name. For example, enter <a href="#">ContentType:value</a> instead of <a href="#">Content-Type:value</a>. Example: <a href="#">From:johnqpublic@example.com AcceptLanguage:en-us</a></p> <p> Make sure that the HTTP header statement is valid. Otherwise, the sensor request cannot be successful.</p>
Remove Characters	<p><a href="#">This setting is only visible if you select Use the value of the selected XML node above.</a></p> <p>Optionally enter a string that the sensor removes from the returned XML value.</p>

Setting	Description
	Use this to remove any unwanted characters from the result, for example to remove a thousands separator from numeric values. Enter a string or leave the field empty.
Decimal Delimiter	<p><b>This setting is only visible if you select</b> Use the value of the selected XML node <a href="#">above</a>.</p> <p>If the sensor value of the returned XML node is of the type <b>float</b>, you can define any character as the decimal delimiter. Enter one character or leave the field empty.</p>
Custom Message	Optionally enter a custom sensor message. Use <b>%1</b> as a placeholder to automatically fill in the returned XML value. Enter a string or leave the field empty.
If Channel Value Changes	<p>Define what the sensor does if the channel value changes:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> <li>▪ Trigger 'change' notification: Send an internal message that indicates a change. <ul style="list-style-type: none"> <li>ⓘ In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</li> </ul> </li> </ul> <p>ⓘ The notification for this sensor can only be triggered if the returned value is a numeric value. This option does not support strings.</p>
Unit String	<p>Enter the unit for the values that this sensor returns. Enter a string.</p> <ul style="list-style-type: none"> <li>ⓘ PRTG uses the unit string for display purposes and shows it in graphs, data tables, and gauges.</li> <li>ⓘ You can change this value later in the <a href="#">channel settings</a> of this sensor.</li> </ul>

## Debug Options

**Debug Options**

Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	Define what PRTG does with the sensor result:



Setting	Description
	<ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other above.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Checking JSON

With the XML Node (and optional property) field, you can also check values that are returned in JSON notation under the defined URL.

**Example**

A JSON notated section might look like the following:

```
{
  "test": "Hello World",
  "object": {
    "value": "content",
    "AnotherValue": "AnotherContent"
  },
  "arraytest": [
    "one",
    "two"
  ]
}
```

Depending on your entries in the XML Node (and optional property) field, the sensor processes the respective values:

Entry in Sensor's "XML Node (and optional property)" Field (from Example Above)	Processed Value (from Example Above)
test	Hello World
object/value	content
object/AnotherValue	AnotherContent
object	contentAnotherContent
arraytest[1]	one
arraytest[2]	two

**i** The sensor converts whitespaces in JSON keys into underscores (\_). So, for example, if you look for the node `some node` in the JSON, you need to enter `some_node` into the node field. If you count the number of nodes (for example, `some_node`), both `some node` and `some_node` would be counted if they appear in the JSON.

**i** If a key exists more than once in the JSON, the value of the first appearance is returned (no difference between whitespace and underscore).

### About Namespaces

In an .xml document, tags might use namespaces.

 Example

A namespace notated section might look like the following:

```
<myNamespace:myNode>
  some information
</myNamespace:myNode>
```

If you set this sensor to Use name spaces (this is the default setting), it expects the full node name, including the namespace information, in the XML Node (and optional property) field. In the example above, this is [myNamespace:myNode](#).

If your node names are unique even without the namespace information, you can simplify the settings by setting this sensor to Remove name spaces. The sensor then expects the node name only in the XML Node (and optional property) field. In the example above, this is [myNode](#).

## Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can only enter the protocol followed by a colon and three forward slashes (this means that you can enter either [http://](#) or [https://](#), or even a simple forward slash [/](#) as the equivalent for [http://](#)). PRTG automatically fills in the parent device's IP Address/DNS Name in front of the third forward slash.

Whether this results in a valid URL or not depends on the IP address or Domain Name System (DNS) name of the parent device. In combination with cloning devices, you can use smart URL replacement to create many similar devices.


For example, if you create a device with the DNS name [www.example.com](#) and you add an HTTP sensor to it, you can provide values in the following ways:

- If you enter [https://](#) in the URL field, PRTG automatically creates the URL [https://www.example.com/](#)
- If you enter [/help](#) in the URL field, PRTG automatically creates and monitor the URL [http://www.example.com/help](#)
- It is also possible to provide a port number in the URL field. It is taken over by the device's DNS name and is internally added, for example, [http://:8080/](#)

 Smart URL replacement does not work for sensors that run on the probe device.

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Execution Time	The execution time
[Value]	The value of one defined XML node  This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

Where can I find more information about the HTTP XML/REST Value sensor?

- <https://kb.paessler.com/en/topic/62463>

Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How can I use XPath with the HTTP XML/REST Value sensor?

- <https://kb.paessler.com/en/topic/26393>

How do I extract values from XML nodes (with nested tags) using the HTTP XML/REST Value sensor?

- <https://kb.paessler.com/en/topic/43223>

Why does my HTTP XML/REST Value sensor return a 404 error?

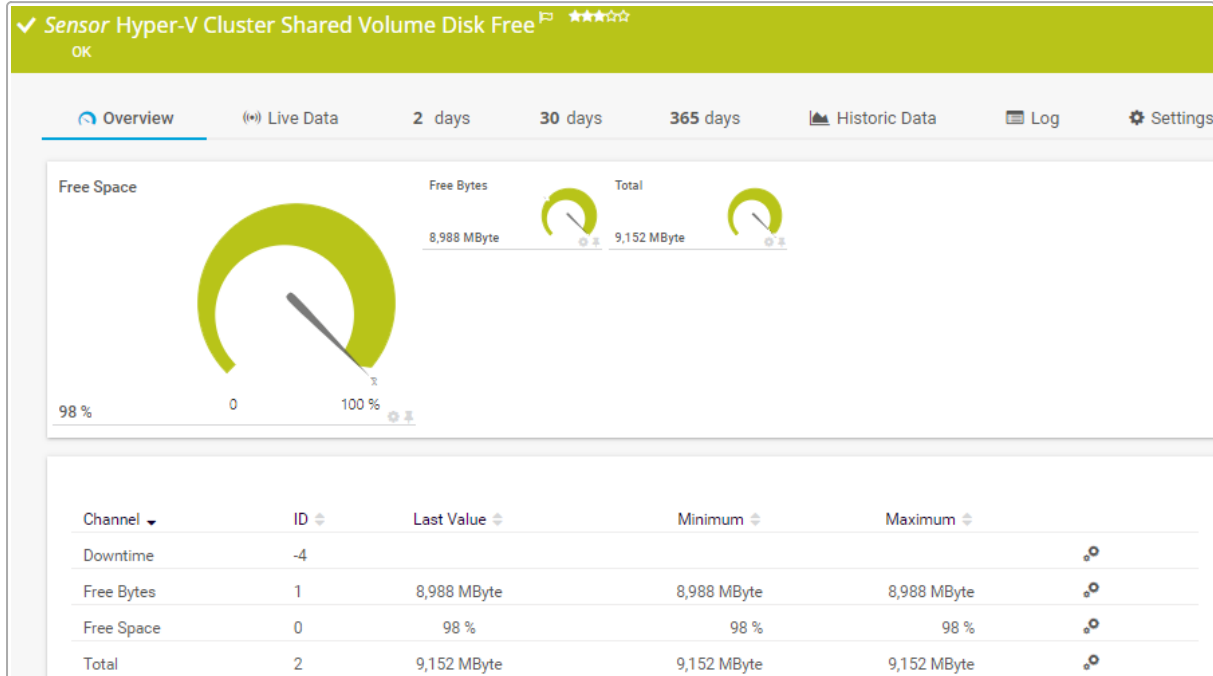
- <https://kb.paessler.com/en/topic/46503>

My HTTP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/85284>

## 7.8.73 Hyper-V Cluster Shared Volume Disk Free Sensor

The Hyper-V Cluster Shared Volume Disk Free sensor monitors free space on the disks of a Microsoft Hyper-V cluster shared volume via PowerShell.



Hyper-V Cluster Shared Volume Disk Free Sensor







For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Hyper-V Cluster Shared Volume Disk Free
- French: Hyper-V cluster espace disponible du volume partagé
- German: Hyper-V Freigegebenes Clustervolume Freier Speicher
- Japanese: Hyper-V クラスタ共有ボリュームディスク空き容量
- Portuguese: Disco de volume compartilhado do cluster Hyper-V livre
- Russian: Свободное дисковое пространство общего тома кластера Hyper-V
- Simplified Chinese: Hyper-V 群集共享卷磁盘可用空间
- Spanish: Espacio libre en disco de volumen compartido en clúster Hyper-V

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Remote PowerShell	<p>This sensor requires <a href="#">Remote PowerShell</a> on the target system.</p> <p> In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message <a href="#">The WSMAN provider host process did not return a proper response</a>. In this case, increase the memory limit for Remote PowerShell.</p> <p> For more information, see the Knowledge Base: <a href="#">How do I enable and use remote commands in Windows PowerShell?</a> and <a href="#">How can I increase memory for Remote PowerShell?</a></p>
WSFC PowerShell Interface	<p>This sensor requires <a href="#">WSFC PowerShell Interface</a> on the target system.</p> <p> You can list all modules in the PowerShell console with the command <a href="#">Get-Module -ListAvailable</a>. Here, <a href="#">FailoverClusters</a> must appear. Under Windows Server 2008 (not officially supported) and Windows Server 2012 (not officially supported), the interface is part of the VMM Administrator Console, or the VMM 2012 Management Console.</p> <p> The interface is available everywhere the WSFC feature is installed: Windows Server 2008 R2 (SP1) Full and Core (not installed by default), Microsoft Hyper-V Server 2008 R2 (SP1), and Remote Server Administration Tools (RSAT) for Windows 10, Windows 8.1, Windows 8, and Windows 7 (SP1).</p>
Parent device	<p>This sensor requires that the parent device is a Windows server that runs Hyper-V.</p>
Credentials	<p>This sensor requires credentials for Windows systems.</p>
Unsupported characters	<p>Make sure that the resource names of your disks do not contain unsupported characters, especially avoid the number sign (#). In general, the sensor supports UTF-8 characters. We recommend that you do not rename resource disk names once you have set up monitoring. For more information, see the Knowledge Base: <a href="#">Why don't my Hyper-V sensors work after changing names?</a></p>
IPv6	<p>This sensor supports IPv6.</p>
Performance impact	<p>This sensor has a <a href="#">medium</a> performance impact.</p>

Remark	Description
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">Why don't my Hyper-V sensors work after changing names?</a></li> <li>Knowledge Base: <a href="#">Where can I find more information about PowerShell sensors?</a></li> </ul>
Hosted probe	<p>☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.</p>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- diskfree
- hyperv
- powershell

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>[667]</sup>.

### Disk Free Settings

#### Disk Free Settings

**Disks** ⓘ C:\ClusterStorage\Volume1

---

**Result Handling** ⓘ  Discard result (default)  
 Store result

Disk Free Settings



Setting	Description
Disks	The name of the disk that this sensor monitors.
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---


Graph Type **i**  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>+</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other above.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Bytes	The free space
Free Space	The free space (%)  This channel is the primary channel by default.
Total	The total space

## More

### ■ KNOWLEDGE BASE

Why don't my Hyper-V sensors work after changing names?

- <https://kb.paessler.com/en/topic/15533>

Where can I find more information about PowerShell sensors?

- <https://kb.paessler.com/en/topic/62451>

How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

How can I increase memory for Remote PowerShell?

- <https://kb.paessler.com/en/topic/61922>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My PowerShell sensor returns an error message. What can I do?

- <https://kb.paessler.com/en/topic/59473>

I get the error "WinRM cannot process the request" when I try to use a PowerShell sensor

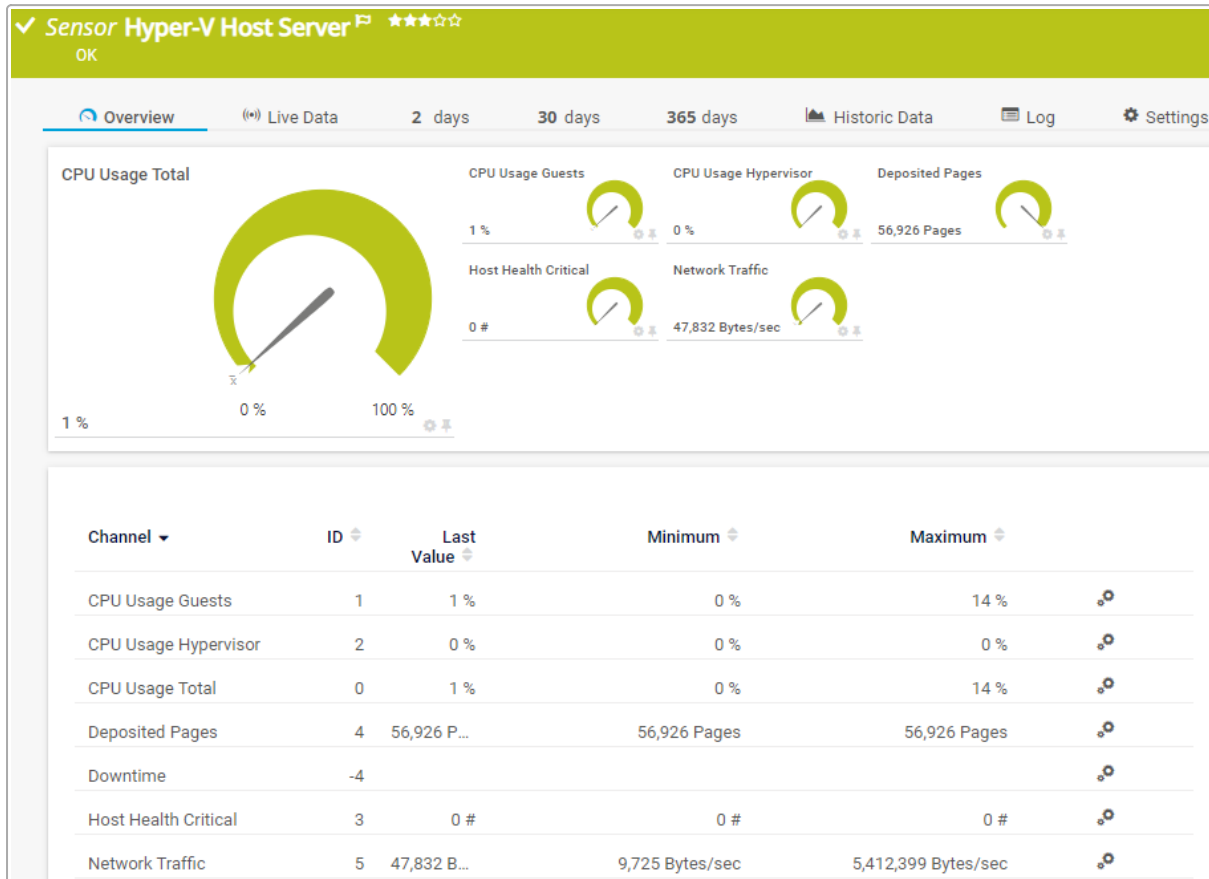
- <https://kb.paessler.com/en/topic/59745>

I have problems with the PowerShell Exchange sensors, what can I do?

- <https://kb.paessler.com/en/topic/54353>

## 7.8.74 Hyper-V Host Server Sensor

The Hyper-V Host Server sensor monitors a Microsoft Hyper-V host server via Windows Management Instrumentation (WMI) or Windows performance counters, as configured in the [Windows Compatibility Options](#) of the parent device.



Hyper-V Host Server Sensor






For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Hyper-V Host Server
- French: Hyper-V serveur hôte
- German: Hyper-V Host Server
- Japanese: Hyper-V ホストサーバー
- Portuguese: Servidor host Hyper-V
- Russian: Сервер узла Hyper-V
- Simplified Chinese: Hyper-V 主机服务器
- Spanish: Servidor host Hyper-V

## Remarks

Consider the following [remarks](#) <sup>1159</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <b>high</b> performance impact. We recommend that you use no more than <b>200</b> of this sensor on each probe.
Windows version	This sensor requires <b>at least Windows Server 2008 R2</b> on the probe system (on every cluster node, if on a cluster probe).   <b>WoW64</b> must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the PRTG probe service only runs with 32-bit support. Without it, WMI sensors do not work.
Remote Registry Windows service	This sensor requires that the <b>Remote Registry</b> Windows service runs on the target system.   If this service does not run, a connection via performance counters is not possible. However, WMI connections might still work.   To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.
Parent device	This sensor requires that the parent device is a Windows server that runs Hyper-V.
Credentials	This sensor requires credentials for Windows systems.   We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system.  Otherwise, a connection via performance counters is not possible. However, WMI connections might still work.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Hybrid Approach: Performance Counters and WMI

**i** By default, this sensor uses WMI to request monitoring data. You can change the default behavior to a [hybrid approach](#) in the Windows Compatibility Options of the parent [device's settings](#) on which you create this sensor: if you choose this option, the sensor first tries to query data via [Windows performance counters](#) and uses WMI as a fallback if performance counters are not available. When running in fallback mode, the sensor tries to connect via performance counters again after 24 hours.

**i** Sensors that use the WMI protocol have a high impact on the system performance. Try to stay below 200 WMI sensors per [probe](#). Above this number, consider using multiple [remote probes](#) for load balancing.

**i** For a general introduction to the technology behind WMI, see section [Monitoring via WMI](#).

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- hypervserversensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Debug Options

### Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **ⓘ** Downtime

---


Graph Type **ⓘ**  Show channels independently (default)

Stack channels on top of each other

Sensor Display


Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CPU Usage Guests	The CPU usage of the guests (%)
CPU Usage Hypervisor	The CPU usage of the hypervisor (%)
CPU Usage Total	The total CPU usage  This channel is the primary channel by default.
Deposited Pages	The number of deposited pages
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Host Health Critical	The number of host health-critical values
Network Traffic	The sum of the total bytes (received and sent) on all ports of the virtual switch

## More

### ■ KNOWLEDGE BASE

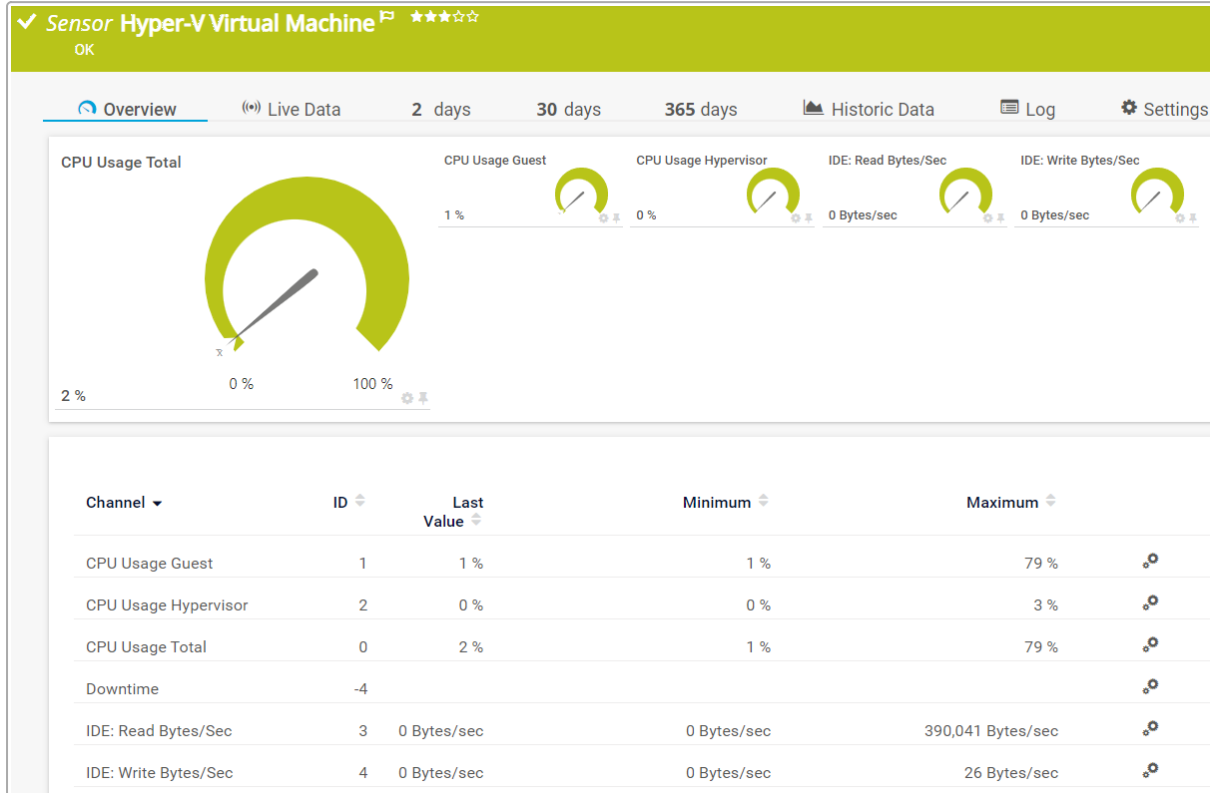
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>



## 7.8.75 Hyper-V Virtual Machine Sensor

The Hyper-V Virtual Machine sensor monitors a virtual machine (VM) that runs on a Microsoft Hyper-V host server via Windows Management Instrumentation (WMI) or Windows performance counters, as configured in the [Windows Compatibility Options](#) of the parent device.



Hyper-V Virtual Machine Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1167</sup>.

### Sensor in Other Languages

- Dutch: Virtuele Hyper-V-Machine
- French: Hyper-V machine virtuelle
- German: Hyper-V Virtuelle Maschine
- Japanese: Hyper-V 仮想マシン
- Portuguese: Máquina virtual Hyper-V
- Russian: Виртуальная машина Hyper-V
- Simplified Chinese: Hyper-V 虚拟机
- Spanish: Máquina virtual Hyper-V

### Remarks

Consider the following [remarks](#)<sup>1163</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Windows version	<p>This sensor requires <a href="#">at least Windows Server 2008 R2</a> on the probe system (on every cluster node, if on a cluster probe).</p> <p><b>i</b> WoW64 must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the PRTG probe service only runs with 32-bit support. Without it, WMI sensors do not work.</p>
Remote Registry Windows service	<p>This sensor requires that the <a href="#">Remote Registry</a> Windows service runs on the target system.</p> <p><b>i</b> If this service does not run, a connection via performance counters is not possible. However, WMI connections might still work.</p> <p><b>i</b> To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.</p>
Parent device	This sensor requires that the parent device is a Windows server that runs Hyper-V.
Credentials	<p>This sensor requires credentials for Windows systems.</p> <p><b>i</b> We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system.</p> <p>Otherwise, a connection via performance counters is not possible. However, WMI connections might still work.</p>
Live migration	This sensor does not support <a href="#">Live Migration</a> .
IPv6	This sensor supports IPv6.
VM monitoring	To monitor a VM with this sensor, disable User Account Control (UAC) in the control panel of the Windows operating system that runs on this VM. Otherwise, the sensor might change to the Down status and show the error message <a href="#">The virtual machine is not running or is powered off</a> .
Unsupported characters	Make sure that the names of your VMs do not contain unsupported characters, especially avoid the number sign (#). We recommend that you not rename VMs once you have set up monitoring. For more information, see the Knowledge Base: <a href="#">Why don't my Hyper-V sensors work after changing names?</a>

Remark	Description
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Hybrid Approach: Performance Counters and WMI

**i** By default, this sensor uses WMI to request monitoring data. You can change the default behavior to a [hybrid approach](#) in the Windows Compatibility Options of the parent [device's settings](#) on which you create this sensor: if you choose this option, the sensor first tries to query data via [Windows performance counters](#) and uses WMI as a fallback if performance counters are not available. When running in fallback mode, the sensor tries to connect via performance counters again after 24 hours.

**i** Sensors that use the WMI protocol have a high impact on the system performance. Try to stay below 200 WMI sensors per [probe](#). Above this number, consider using multiple [remote probes](#) for load balancing.

**i** For a general introduction to the technology behind WMI, see section [Monitoring via WMI](#).

## Basic Sensor Settings

**Basic Sensor Settings**

Sensor Name ⓘ Example Name

Tags ⓘ  X +

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmihypersensor

**■** For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Virtual Machine Settings

**Virtual Machine Settings**

**GUID** ⓘ 1111aaaa-22bb-cc33-dd44-555555eeeeeee

**Virtual Machine Name** ⓘ Ubuntu - Docker 2

**Description** ⓘ Microsoft Virtual Machine

**Powered-Off VM Handling** ⓘ  Alarm when VM is powered off (default)  
 Ignore powered-off state

**Result Handling** ⓘ  Discard result (default)  
 Store result

Virtual Machine Settings

Setting	Description
GUID	The globally unique identifier (GUID) of the VM that this sensor monitors.
Virtual Machine Name	The name of the VM that this sensor monitors.
Description	The description of the VM that this sensor monitors.
Powered-Off VM Handling	<p>Define how the sensor reacts to VMs that are powered off:</p> <ul style="list-style-type: none"> <li>▪ Alarm when VM is powered off (default): Change to the Down <a href="#">status</a> if the VM is powered off.</li> </ul> <p>ⓘ If the sensor is in the Down status, it does not record any data in any of its channels.</p> <ul style="list-style-type: none"> <li>▪ Ignore powered off state: Do not change to the Down status if the VM is powered off. The sensor reports zero values instead.</li> </ul>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CPU Usage Guest	The CPU usage of the guests (%)
CPU Usage Hypervisor	The CPU usage of the hypervisor (%)
CPU Usage Total	The total CPU usage  This channel is the primary channel by default.
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
IDE: Read Bytes/Sec	The disk read speed of the IDE
IDE: Write Bytes/Sec	The disk write speed of the IDE

## More

### ■ KNOWLEDGE BASE

Why don't my Hyper-V sensors work after changing names?

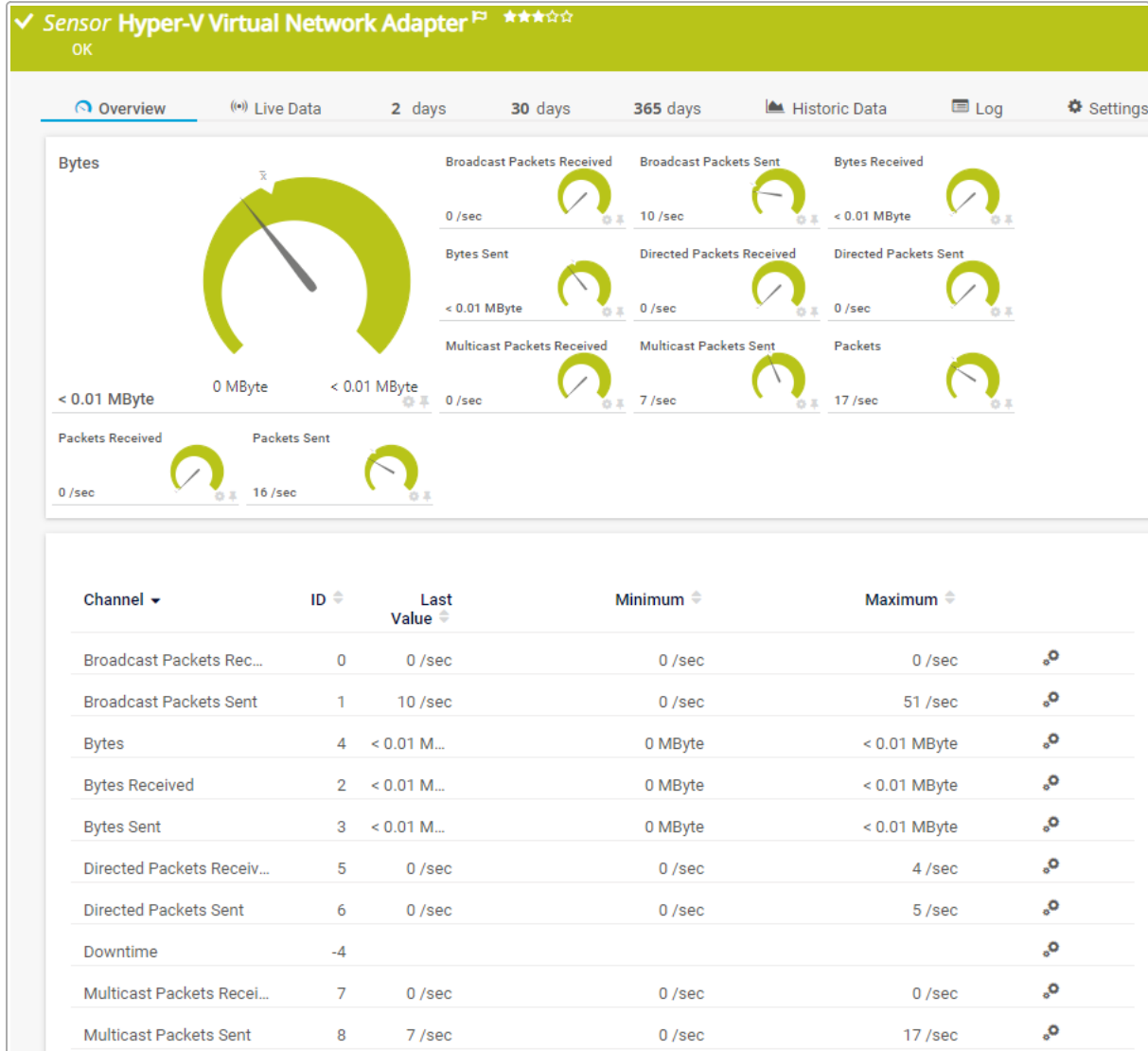
- <https://kb.paessler.com/en/topic/15533>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.76 Hyper-V Virtual Network Adapter Sensor

The Hyper-V Virtual Network Adapter sensor monitors virtual network adapters that run on a Microsoft Hyper-V host server via Windows Management Instrumentation (WMI) or Windows performance counters, as configured in the [Windows Compatibility Options](#) of the parent device.



Hyper-V Virtual Network Adapter Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1173</sup>.

### Sensor in Other Languages

- Dutch: Hyper-V Virtuele Netwerk Adapter
- French: Hyper-V carte réseau virtuelle
- German: Hyper-V Virtueller Netzwerkadapter
- Japanese: Hyper-V 仮想ネットワークアダプター
- Portuguese: Adaptador de rede virtual Hyper-V

- Russian: Виртуальный сетевой адаптер Hyper-V
- Simplified Chinese: Hyper-V 虚拟网络适配器
- Spanish: Adaptador de red virtual Hyper-V

## Remarks

Consider the following [remarks](#)<sup>1170</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Windows version	<p>This sensor requires <a href="#">at least Windows Server 2008 R2</a> on the probe system (on every cluster node, if on a cluster probe).</p> <p><b>i</b> WoW64 must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the PRTG probe service only runs with 32-bit support. Without it, WMI sensors do not work.</p>
Remote Registry Windows service	<p>This sensor requires that the <a href="#">Remote Registry</a> Windows service runs on the target system.</p> <p><b>i</b> If this service does not run, a connection via performance counters is not possible. However, WMI connections might still work.</p> <p><b>i</b> To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.</p>
Parent device	This sensor requires that the parent device is a Windows server that runs Hyper-V.
Credentials	<p>This sensor requires credentials for Windows systems.</p> <p><b>i</b> We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system.</p> <p>Otherwise, a connection via performance counters is not possible. However, WMI connections might still work.</p>
IPv6	This sensor supports IPv6.
Renaming VMs	We recommend that you do not rename virtual machines (VM) once you have set up monitoring. Renaming VMs also changes the internal virtual network adapter names, so monitoring might be interrupted. For more information about VM naming, see the Knowledge Base: <a href="#">Why don't my Hyper-V sensors work after changing names?</a>



Remark	Description
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Hybrid Approach: Performance Counters and WMI

**i** By default, this sensor uses WMI to request monitoring data. You can change the default behavior to a [hybrid approach](#) in the Windows Compatibility Options of the parent [device's settings](#) on which you create this sensor: if you choose this option, the sensor first tries to query data via [Windows performance counters](#) and uses WMI as a fallback if performance counters are not available. When running in fallback mode, the sensor tries to connect via performance counters again after 24 hours.

**i** Sensors that use the WMI protocol have a high impact on the system performance. Try to stay below 200 WMI sensors per [probe](#). Above this number, consider using multiple [remote probes](#) for load balancing.

**i** For a general introduction to the technology behind WMI, see section [Monitoring via WMI](#).

## Basic Sensor Settings

**Basic Sensor Settings**

Sensor Name ⓘ Example Name

Tags ⓘ  X +

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmihypervirtualnetworkadapter

**■** For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Hyper-V Virtual Network Adapter Settings

Hyper-V Virtual Network Adapter Settings

Virtual Network Adapter ⓘ *Fujitsu DynamicLoM Emulex*

Result Handling ⓘ  Discard result (default)  
 Store result

Hyper-V Virtual Network Adapter Settings

Setting	Description
Virtual Network Adapter	The name of the virtual network adapter that this sensor monitors.
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

Sensor Display

Primary Channel ⓘ Downtime


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor. <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	Define how this sensor shows different channels:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li>❗ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

❗ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Broadcast Packets Received	The number of broadcast packets received
Broadcast Packets Sent	The number of broadcast packets sent
Bytes	The number of bytes transferred in total ❗ This channel is the primary channel by default.
Bytes Received	The number of received bytes
Bytes Sent	The number of sent bytes

Channel	Description
Directed Packets Received	The number of directed packets received
Directed Packets Sent	The number of directed packets sent
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Multicast Packets Received	The number of multicast packets received
Multicast Packets Sent	The number of multicast packets sent
Packets	The number of packets transferred in total
Packets Received	The number of packets received
Packets Sent	The number of packets sent

## More

### ■ KNOWLEDGE BASE

Why don't my Hyper-V sensors work after changing names?

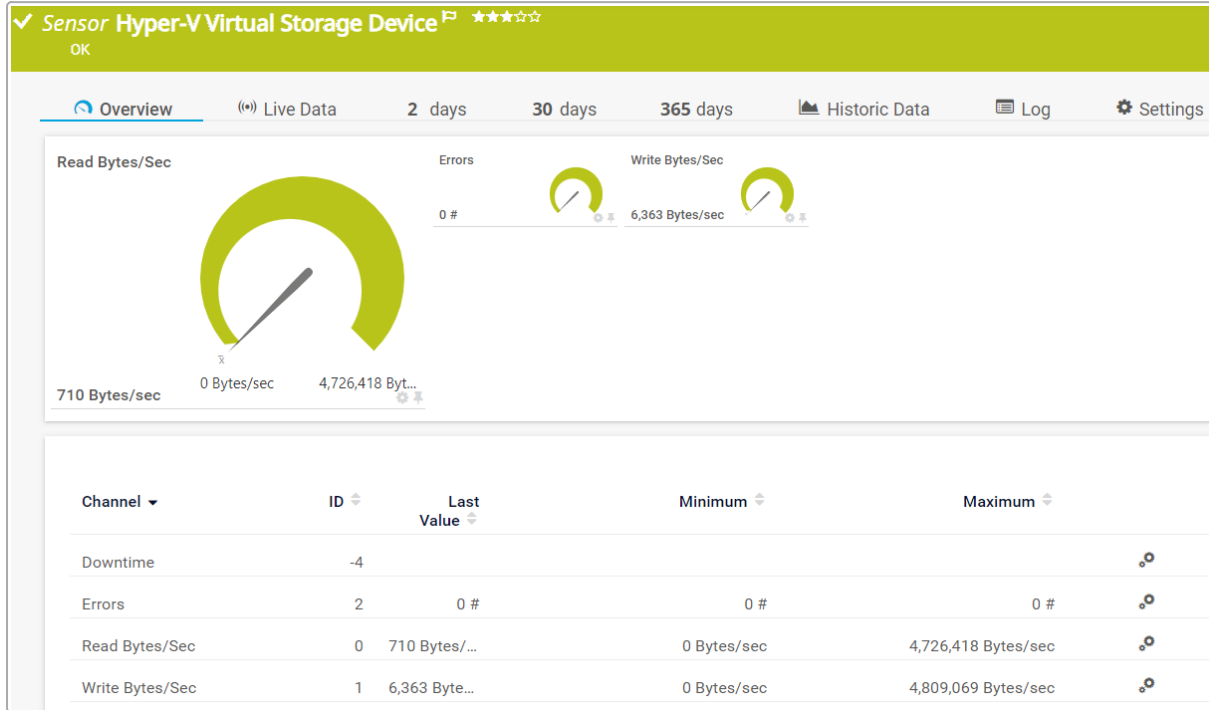
- <https://kb.paessler.com/en/topic/15533>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.77 Hyper-V Virtual Storage Device Sensor

The Hyper-V Virtual Storage Device sensor monitors a virtual storage device that runs on a Microsoft Hyper-V host server via Windows Management Instrumentation (WMI) or Windows performance counters, as configured in the [Windows Compatibility Options](#) of the parent device.



Hyper-V Virtual Storage Device Sensor






For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Hyper-V Virtueel Opslag Apparaat
- French: Hyper-V équipement de stockage virtuel
- German: Hyper-V Virtuelles Speichergerät
- Japanese: Hyper-V 仮想ストレージデバイス
- Portuguese: Dispositivo de armazenamento virtual Hyper-V
- Russian: Виртуальное устройство хранения Hyper-V
- Simplified Chinese: Hyper-V 虚拟存储设备
- Spanish: Dispositivo de almacenamiento virtual Hyper-V

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Windows version	This sensor requires <a href="#">at least Windows Server 2008 R2</a> on the probe system (on every cluster node, if on a cluster probe).   WoW64 must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the PRTG probe service only runs with 32-bit support. Without it, WMI sensors do not work.
Remote Registry Windows service	This sensor requires that the <a href="#">Remote Registry</a> Windows service runs on the target system.   If this service does not run, a connection via performance counters is not possible. However, WMI connections might still work.   To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.
Parent device	This sensor requires that the parent device is a Windows server that runs Hyper-V.
Credentials	This sensor requires credentials for Windows systems.   We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system.  Otherwise, a connection via performance counters is not possible. However, WMI connections might still work.
Live migration	This sensor does not support <a href="#">Live Migration</a> .
IPv6	This sensor supports IPv6.
Knowledge Base	Knowledge Base: <a href="#">Why don't my Hyper-V sensors work after changing names?</a>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Hybrid Approach: Performance Counters and WMI

**i** By default, this sensor uses WMI to request monitoring data. You can change the default behavior to a [hybrid approach](#) in the Windows Compatibility Options of the parent [device's settings](#) on which you create this sensor: if you choose this option, the sensor first tries to query data via [Windows performance counters](#) and uses WMI as a fallback if performance counters are not available. When running in fallback mode, the sensor tries to connect via performance counters again after 24 hours.

**i** Sensors that use the WMI protocol have a high impact on the system performance. Try to stay below 200 WMI sensors per [probe](#). Above this number, consider using multiple [remote probes](#) for load balancing.

**i** For a general introduction to the technology behind WMI, see section [Monitoring via WMI](#).

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmihypervirtualstoragesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Hyper-V Virtual Storage Device Settings

### Hyper-V Virtual Storage Device Settings

**Virtual Storage Device** ⓘ C:-ProgramData-Microsoft-Windows-Hyper-V-Ubuntu

---

**Host Operating System** *Windows Server 2012 and later*

---

**Result Handling** ⓘ  Discard result (default)  
 Store result

Hyper-V Virtual Storage Device Settings

Setting	Description
Virtual Storage Device	The unique identifier of the virtual storage device that this sensor monitors.
Host Operating System	The host operating system of the virtual storage device that this sensor monitors.
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⚙</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>




Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Errors	The number of errors
Read Bytes/Sec	The read speed  This channel is the primary channel by default.
Write Bytes/Sec	The write speed

## More

### KNOWLEDGE BASE

Why don't my Hyper-V sensors work after changing names?

- <https://kb.paessler.com/en/topic/15533>

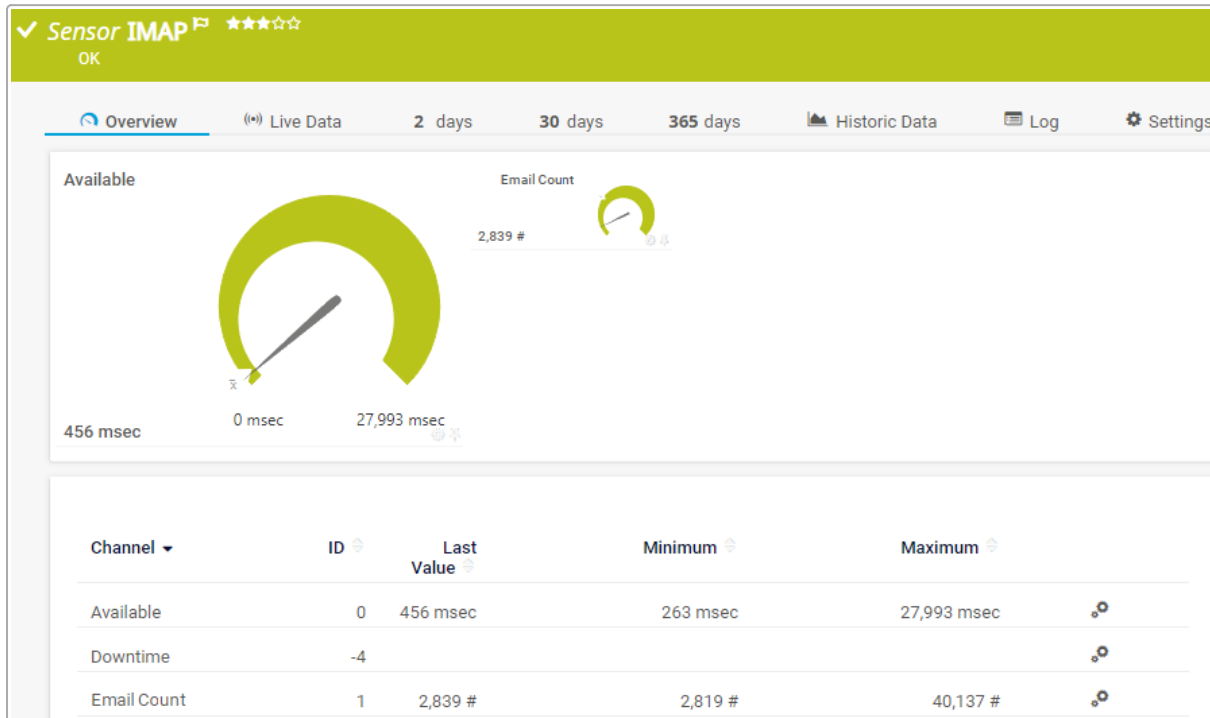
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.78 IMAP Sensor

The IMAP sensor monitors an email server via the Internet Message Access Protocol (IMAP).

**i** The sensor can check the content of emails for certain keywords. This way, you can use the sensor to monitor backup solutions via emails that are sent by these solutions. For more information, see the Knowledge Base: [How can I monitor my backup software to be sure backup succeeded last night?](#)



IMAP Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: IMAP
- French: IMAP
- German: IMAP
- Japanese: IMAP
- Portuguese: IMAP
- Russian: IMAP
- Simplified Chinese: IMAP
- Spanish: IMAP

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
SRP ciphers	This sensor does not support Secure Remote Password (SRP) ciphers.
Microsoft 365 mailboxes	This sensor does not support Microsoft 365 mailboxes. If you want to monitor a Microsoft 365 mailbox, use the <a href="#">Microsoft 365 Mailbox</a> <sup>12521</sup> sensor.
IPv4	This sensor only supports IPv4.
Performance impact	This sensor has a <b>medium</b> performance impact.
Content checks	If you use content checks, we recommend that you use a dedicated IMAP account that is only checked by PRTG. Editing mails in the mailbox of the monitored IMAP account can lead to false alarms or malfunctions of this sensor.
Subfolder monitoring	This sensor might not work properly when monitoring subfolders of mailboxes. If it has to check subsequent emails with identical subjects, it might not recognize emails that come in later.
Daylight Saving Time	Emails that arrive during the Daylight Saving Time (winter time to summer time) change might not be processed properly. If you experience this issue, delete the respective emails.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">My IMAP sensor does not process HTML emails correctly using regex. What can I do?</a></li> <li>▪ Knowledge Base: <a href="#">How can I monitor my backup software to be sure backup succeeded last night?</a></li> <li>▪ Knowledge Base: <a href="#">Can I analyze multipart emails using the IMAP sensor?</a></li> <li>▪ Knowledge Base: <a href="#">My IMAP sensor does not find emails when I check for message date. What can I do?</a></li> </ul>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- imapsensor
- mailsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Connectivity

**Connectivity**

Timeout (Sec.) ⓘ 60

---

Port ⓘ 993

---

Transport-Level Security ⓘ

- Use transport-level security if available using StartTLS
- Use transport-level security if available
- Enforce transport-level security using StartTLS
- Enforce transport-level security (default)

Connectivity

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p> ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
Port	<p>Specify the port that the sensor uses for the IMAP connection. The default port for unsecure connections is <b>143</b> and the default port for secure connections is <b>993</b>. The actual setting depends on the server you connect to. Enter an integer.</p> <p> ⓘ We recommend that you use the default value.</p> <p> ⓘ If the connection is unsuccessful, try a different port number.</p>
Transport-Level Security	<p>Define how the sensor handles the security of the connection:</p> <ul style="list-style-type: none"> <li>▪ Use transport-level security if available using StartTLS: Try to connect to the server via a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection and StartTLS. If the server does not support this, the sensor tries to connect without connection security.</li> <li>▪ Use transport-level security if available: Try to connect to the server via an SSL/TLS-secured connection. If the server does not support this, the sensor tries to connect without connection security.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Enforce transport-level security using StartTLS: Try to connect to the server via an SSL/TLS-secured connection and StartTLS. If the server does not support this, the sensor shows the Down <a href="#">status</a>.</li> <li>▪ Enforce transport-level security (default): Try to connect to the server via an SSL/TLS-secured connection. If the server does not support this, the sensor shows the Down status.</li> </ul> <p><b>i</b> If the sensor connects to a server via StartTLS, the connection is first established without connection security. After the connection has been established, the sensor sends a certain command (<a href="#">StartTLS</a>) over the unsecured connection to negotiate a secure connection via SSL/TLS.</p> <p><b>i</b> If the sensor does <b>not</b> use StartTLS, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If no secure connection is possible, no communication takes place.</p>

## Sensor Behavior

### Sensor Behavior

**Email Processing** **i**

Do not process emails (default)

Count emails in the mailbox

Process emails in the mailbox

**Result Handling** **i**

Discard result (default)

Store result

Sensor Behavior

Setting	Description
Email Processing	<p>Define if the sensor additionally checks the content of all incoming emails:</p> <ul style="list-style-type: none"> <li>▪ Do not process emails (default): Only check the availability of the IMAP server and check if a login is successful. Do not process any emails in the IMAP email account.</li> <li>▪ Count emails in the mailbox: Count the emails in the mailbox.</li> <li>▪ Process emails in the mailbox: Log in to the IMAP email account and check the emails that it contains. Define further options below.</li> </ul>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Authentication

### Authentication

**User Name** ⓘ

**Password** ⓘ

**Folder Name** ⓘ

Authentication

Setting	Description
User Name	Enter a user name for IMAP authentication. Enter a string.
Password	Enter a password for IMAP authentication. Enter a string. ⓘ The password must <b>not</b> contain spaces, percent signs (%), or the character combination !*.
Folder Name	Enter the name of a folder in the mailbox (for example, the IMAP folder) that the sensor checks. The default value is <a href="#">Inbox</a> . Unless you set a last message date check below, the sensor always looks at <a href="#">all</a> emails contained in the mailbox. ⓘ Make sure that you do not manually edit emails in this mailbox with a different email client because this can result in malfunctions of this sensor's email identification.

## Filter Emails in Inbox

ⓘ This settings section is only visible if you select Process emails in the mailbox.

### Filter Emails in Inbox

Only Include Emails with Matching "From" ⓘ  Do not check (default)  
 Check using simple string search  
 Check using regular expression

Only Include Emails with Matching "Subject" ⓘ  Do not check (default)  
 Check using simple string search  
 Check using regular expression

Only Include Emails with Matching Email Body ⓘ  Do not check (default)  
 Check using simple string search  
 Check using regular expression

Only Include Recent Emails ⓘ  Do not check message age (default)  
 Emails must be younger than

If No Email Matches the Above Filters ⓘ  Set sensor to up status (default)  
 Set sensor to warning status  
 Set sensor to down status

Filter Emails in Inbox

Setting	Description
Only Include Emails with Matching "From"	<p>Define if you want to check the "From" field of the emails:</p> <ul style="list-style-type: none"> <li>▪ Do not check (default): Do not process this field in emails.</li> <li>▪ Check using simple string search: Process this field in emails using a simple string in plain text.</li> <li>▪ Check using regular expression: Process this field in emails using a regular expression (regex).</li> </ul> <p> ⓘ In the search, the sensor scans all emails from the newest to the oldest.</p> <p> ⓘ PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</p> <p> ⓘ The sensor finishes the scan with the first match. This means that after it finds a match in one email, the sensor does not perform any further checks in older emails.</p>
Search for	<p><b>This setting is only visible if you select</b> Check using simple string search <b>or</b> Check using regular expression <b>above</b>.</p> <p>Enter the email address or the <a href="#">regular expression</a> that the "From" field of the email must contain or match.</p>



Setting	Description
Only Include Emails with Matching "Subject"	<p>Define if you want to check the "Subject" field of the emails:</p> <ul style="list-style-type: none"> <li>▪ Do not check (default): Do not process this field in emails.</li> <li>▪ Check using simple string search: Process this field in emails using a simple string in plain text.</li> <li>▪ Check using regular expression: Process this field in emails using a regular expression (regex).</li> </ul> <p><b>i</b> In the search, the sensor scans all emails from the newest to the oldest.</p> <p><b>i</b> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</p> <p><b>i</b> The sensor finishes the scan with the first match. This means that after it finds a match in one email, the sensor does not perform any further checks in older emails.</p>
Search for	<p><b>This setting is only visible if you select</b> Check using simple string search <b>or</b> Check using regular expression <b>above</b>.</p> <p>Enter the simple string in plain text or the regex that the "Subject" field of the email must contain or match.</p>
Only Include Emails with Matching Email Body	<p>Define if you want to check the body of the emails:</p> <ul style="list-style-type: none"> <li>▪ Do not check (default): Do not process the email body.</li> <li>▪ Check using simple string search: Process the email body using a simple string in plain text.</li> <li>▪ Check using regular expression: Process the email body using a regex.</li> </ul> <p><b>i</b> In the search, the sensor scans all emails from the newest to the oldest.</p> <p><b>i</b> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</p> <p><b>i</b> The sensor finishes the scan with the first match. This means that after it finds a match in one email, the sensor does not perform any further checks in older emails.</p>
Search for	<p><b>This setting is only visible if you select</b> Check using simple string search <b>or</b> Check using regular expression <b>above</b>.</p> <p>Enter the simple string in plain text or the regex that the body of the email must contain or match.</p>


Setting	Description
Only Include Recent Emails	<p>Define if you want to check all emails in the mailbox or only mails that were received during the last few hours:</p> <ul style="list-style-type: none"> <li>▪ Do not check message age (default): Check all emails that the mailbox contains.</li> <li>▪ Emails must be younger than: Only check emails that were received during the last few hours. Define below.</li> </ul>
Maximum Age (Hours)	<p><b>This setting is only visible if you select</b> Emails must be younger than <b>above</b>.</p> <p>Enter the maximum age in hours. The sensor only processes emails that are younger. Enter an integer.</p>
If No Email Matches the Above Filters	<p>Define which <b>status</b> the sensor shows if it does not find any email in the mailbox that matches the above filters:</p> <ul style="list-style-type: none"> <li>▪ Set sensor to up status (default): Show the Up status if the sensor does not find any email in the mailbox that matches the filters.</li> <li>▪ Set sensor to warning status: Show the Warning status if the sensor does not find any email in the mailbox that matches the filters.</li> <li>▪ Set sensor to down status: Show the Down status if the sensor does not find any email in the mailbox that matches the filters.</li> </ul>
Message	<p><b>This setting is only visible if you select</b> Set sensor to warning status <b>or</b> Set sensor to down status <b>above</b>.</p> <p>Define the message that the sensor shows if it does not find any matching emails.</p>

### Validate Latest Email

- i** This settings section is only visible if you select Process emails in the mailbox.
- i** The sensor only validates the latest email that matches the above filters. If the sensor does not find a matching email, it does not perform any email validation.

**Validate Latest Email**

The sensor only validates the latest email that matches the above filters. If the sensor does not find a matching email, it does not perform any email validation.

Set Sensor to Warning Status 

Never (default)


Always

If subject contains

If subject does not contain

If email body contains

If email body does not contain

Set Sensor to Down Status 

Never (default)

Always


If subject contains

If subject does not contain

If email body contains

If email body does not contain

Make sure that the sensor has dedicated access to the mailbox. External logins can distort message age recognition.

Based on Message Age, Set Sensor to Warning Status 

Never (default)

If email is older than

Validate Latest Email

Setting	Description
Set Sensor to Warning Status	<p>Define in which cases the sensor shows the Warning status:</p> <ul style="list-style-type: none"> <li>▪ <b>Never (default):</b> Never show the Warning status because of email content.</li> <li>▪ <b>Always:</b> Always show the Warning status if it could identify any emails.</li> <li>▪ <b>If subject contains:</b> Show the Warning status if the subject of the email contains the Search String you define below.</li> <li>▪ <b>If subject does not contain:</b> Show the Warning status if the subject of the email does not contain the Search String you define below.</li> <li>▪ <b>If email body contains:</b> Show the Warning status if the body of the email contains the Search String you define below.</li> <li>▪ <b>If email body does not contain:</b> Show the Warning status if the body of the email does not contain the Search String you define below.</li> </ul>
Search Method	<p><b>This setting is only visible if you select</b> If subject contains, If subject does not contain, If email body contains, <b>or</b> If email body does not contain <b>above.</b></p> <p>Define the method with which you want to search for the respective condition:</p> <ul style="list-style-type: none"> <li>▪ <b>Simple string search (default):</b> Search the email subject or body with a simple string in plain text.</li> </ul>

Setting	Description
	<p><b>i</b> The characters * and ? work as placeholders. * stands for no number or any number of characters and ? stands for exactly one character. You cannot change this behavior. The literal search for these characters is only possible with a regex.</p> <ul style="list-style-type: none"> <li>▪ Regular expression: Search the email subject or body with a regex.</li> </ul> <p><b>i</b> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</p>
Search String	<p><b>This setting is only visible if you select</b> If subject contains, If subject does not contain, If email body contains, <b>or</b> If email body does not contain <b>above</b>.</p> <p>Define the string that you want to search the email subject or body for. You can enter a simple string in plain text or a regex.</p>
Warning Message	<p><b>This setting is only visible if you select a "warning" condition above</b>.</p> <p>Define the message that the sensor shows for the Warning status.</p>
Set Sensor to Down Status	<p>Define in which cases the sensor shows the Down status:</p> <ul style="list-style-type: none"> <li>▪ Never (default): Never show the Down status based on email content.</li> <li>▪ Always: Always show the Down status if any emails could be identified.</li> <li>▪ If subject contains: Show the Down status if the subject of the found email contains the Search String you define below.</li> <li>▪ If subject does not contain: Show the Down status if the subject of the found email does not contain the Search String you define below.</li> <li>▪ If email body contains: Show the Down status if the body of the found email contains the Search String you define below.</li> <li>▪ If email body does not contain: Show the Down status if the body of the found email does not contain the Search String you define below.</li> </ul>
Search Method	<p><b>This setting is only visible if you select</b> If subject contains, If subject does not contain, If email body contains, <b>or</b> If email body does not contain <b>above</b>.</p> <p>Define the method with which you want to search for the respective condition:</p> <ul style="list-style-type: none"> <li>▪ Simple string search (default): Search the email subject or body with a simple string in plain text.</li> </ul>

Setting	Description
	<p><b>i</b> The characters * and ? work as placeholders. * stands for no number or any number of characters and ? stands for exactly one character. You cannot change this behavior. The literal search for these characters is only possible with a regex.</p> <ul style="list-style-type: none"> <li>▪ Regular expression: Search the email subject or body with a regex.</li> </ul> <p><b>i</b> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</p>
Search String	<p>This setting is only visible if you select <a href="#">If subject contains</a>, <a href="#">If subject does not contain</a>, <a href="#">If email body contains</a>, or <a href="#">If email body does not contain above</a>.</p> <p>Define the string that you want to search the email subject or body for. You can enter a simple string in plain text or a regex.</p>
Error Message	<p>This setting is only visible if you select <a href="#">Always</a>, <a href="#">If subject contains</a>, <a href="#">If subject does not contain</a>, <a href="#">If email body contains</a>, or <a href="#">If email body does not contain above</a>.</p> <p>Define the message that the sensor shows for the Down status.</p>
Based on Message Age, Set Sensor to Warning Status	<p>Define if you want to check the age of the latest matching email in the mailbox:</p> <ul style="list-style-type: none"> <li>▪ Never (default): Do not check the age of the email.</li> <li>▪ If email is older than: Set the sensor to the Warning status if the found email is older than you define below.</li> </ul>
Message Age (Hours)	<p>This setting is only visible if you select the <a href="#">message age check above</a>.</p> <p>Enter the maximum age in hours. If the processed email is older, the sensor shows the Warning status. Enter an integer.</p> <p><b>i</b> Make sure you do not manually edit emails in this mailbox with a different email client because this can result in malfunctions of the message age check.</p>

## Sensor Display


**Sensor Display**

Primary Channel **i** Downtime


---


Graph Type **i** 
 Show channels independently (default)
   
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Available	<p>The response time</p> <p><b>i</b> This channel is the primary channel by default.</p>

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Email Count	The number of emails in the defined mailbox

## More

### ■ KNOWLEDGE BASE

How can I monitor my backup software to be sure backup succeeded last night?

- <https://kb.paessler.com/en/topic/47023>

My IMAP sensor does not process HTML emails correctly using regex. What can I do?

- <https://kb.paessler.com/en/topic/61019>

Can I analyze multipart emails using the IMAP sensor?

- <https://kb.paessler.com/en/topic/63532>

My IMAP sensor does not find emails when I check for message date. What can I do?

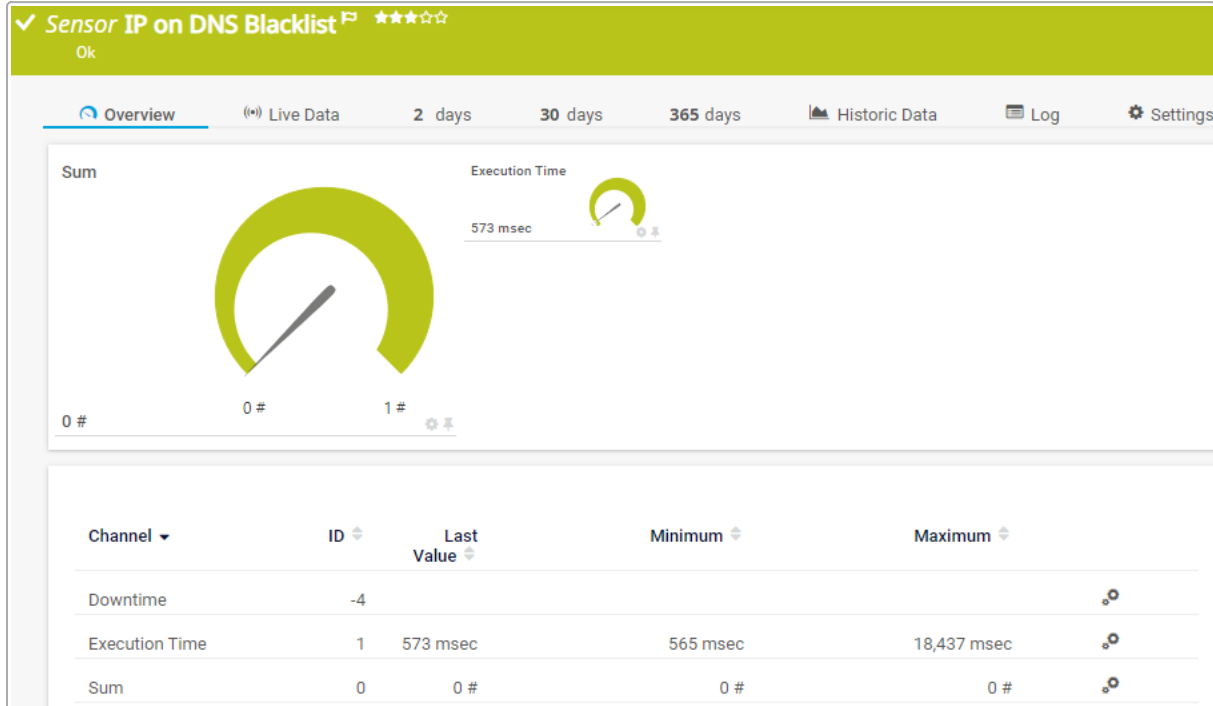
- <https://kb.paessler.com/en/topic/69811>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.79 IP on DNS Blacklist Sensor

The IP on DNS Blacklist sensor checks if the IP address of its parent device is listed on specific blacklist servers.



IP on DNS Blacklist Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1197]</sup>.



### Sensor in Other Languages

- Dutch: IP op DNS Blacklist
- French: IP sur liste noire du DNS
- German: IP auf Schwarzer Liste des DNS
- Japanese: DNS ブラックリスト記載の IP
- Portuguese: IP em Blacklist DNS
- Russian: Черный список IP-адресов на DNS
- Simplified Chinese: DNS 黑名单 IP
- Spanish: IP en lista negra de DNS

### Remarks

Consider the following [remarks](#)<sup>[1194]</sup> and requirements for this sensor:



Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node. If the sensor shows the error PE087, additionally install .NET 3.5 on the probe system.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Windows Server	We recommend Windows Server 2016 on the probe system for best performance of this sensor.
IPv6	This sensor supports IPv6.
Parent device	If a Domain Name System (DNS) name is used as the host name of the parent device, PRTG resolves it to an IP address before querying blacklist servers.
Additional thresholds	During normal operation, there should be 0 hits and the sensor should show the Up <a href="#">status</a> . If the sensor can find the IP address on at least one of the blacklist servers, it shows the Warning status by default. You can set additional thresholds in the <a href="#">channel settings</a> .
Knowledge Base	Knowledge Base: <a href="#">Is there a list of anti spam black list servers?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- ptfsensor

 For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Settings

Sensor Settings
Blacklist Servers ⓘ

Sensor Settings

Setting	Description
Blacklist Servers	<p>Define the blacklist servers that the sensor uses for the check. You can enter a comma-separated list. The default is <a href="#">bl.spamcop.net</a>.</p> <ul style="list-style-type: none"> <li><span style="color: #0070C0;">■</span> For a list of servers, see the Knowledge Base: <a href="#">Is there a list of anti spam black list servers?</a></li> <li><span style="color: #C00000;">ⓘ</span> With each scanning interval, PRTG queries all servers in the list. We recommend that you do not enter more than 10 servers to make sure that the check can be completed within the scanning interval of this sensor. If you use too many blacklist servers, the sensor shows the error message <a href="#">Timeout (code: PE018)</a>.</li> </ul>

## Debug Options

Debug Options
Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><span style="color: #C00000;">☁</span> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><span style="color: #C00000;">ⓘ</span> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Execution Time	The execution time
Sum	The number of blacklist hits found  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

Is there a list of anti spam black list servers?

- <https://kb.paessler.com/en/topic/37633>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

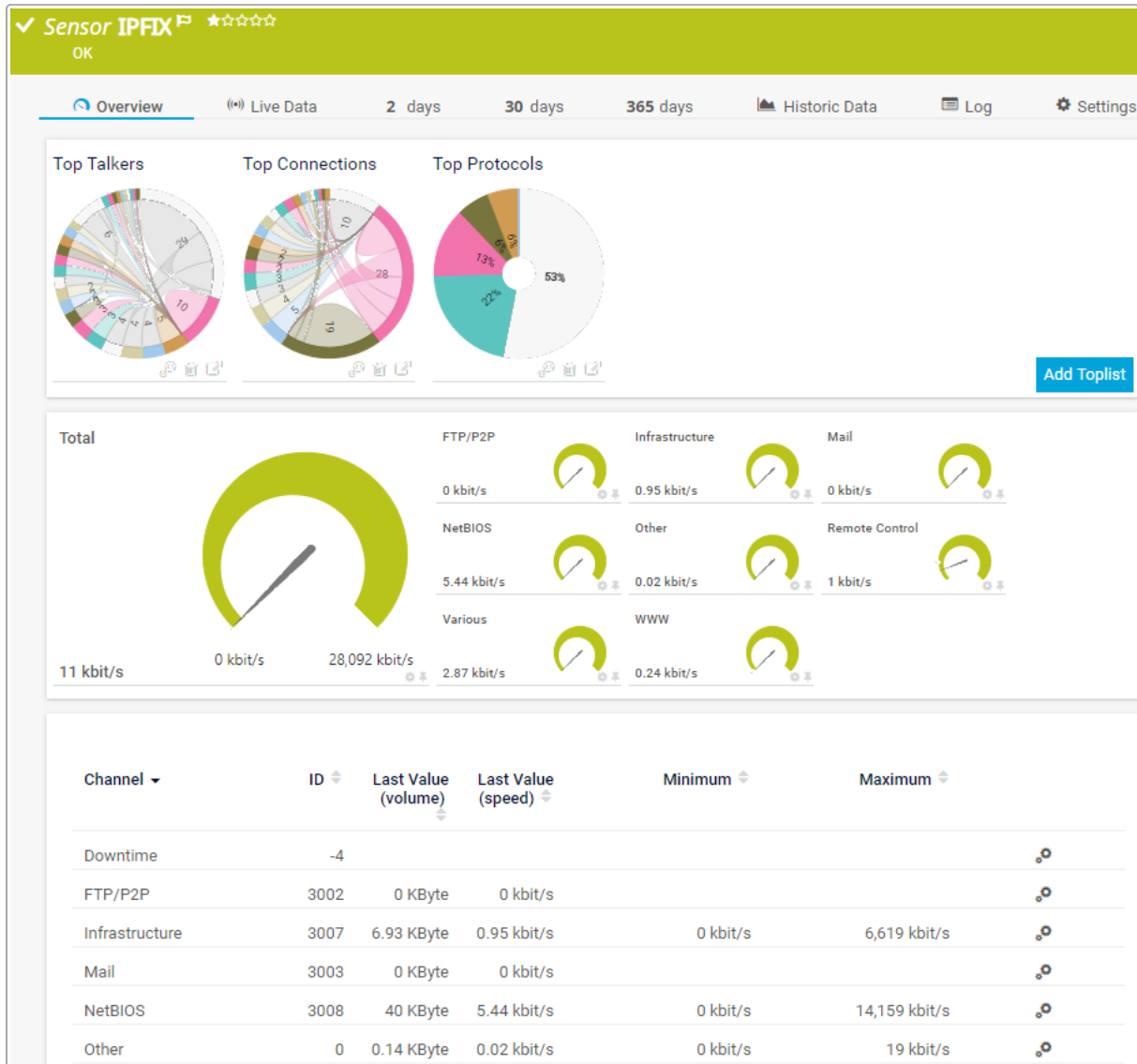
For which sensor types do you recommend at least Windows Server 2016 and why?

- <https://kb.paessler.com/en/topic/64331>

## 7.8.80 IPFIX Sensor

The IPFIX sensor receives traffic data from an Internet Protocol Flow Information Export (IPFIX) compatible device and shows traffic by type. This sensor has several filter options to divide traffic into different channels.

**i** Make sure that the target device supports IPFIX if you want to use this sensor.



IPFIX Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: IPFIX
- French: IPFIX
- German: IPFIX

- Japanese: IPFIX
- Portuguese: IPFIX
- Russian: IPFIX
- Simplified Chinese: IPFIX
- Spanish: IPFIX

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
IPFIX	This sensor requires that the IPFIX export is enabled on the target system. The target system must send the flow data stream to the IP address of the probe system.
Channels	This sensor does not officially support more than <b>50 channels</b> .
Cluster probe	This sensor does not support cluster probes. You can only set it up on local probes or remote probes.
IPv4	This sensor only supports IPv4.
Knowledge Base	Knowledge Base: <a href="#">What is the Active Flow Timeout in flow sensors?</a>
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ

**Priority** ⓘ

Example Name

exampletag
✕
+

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- bandwidthsensor
- netflowsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## IPFIX Specific Settings

**IPFIX Specific Settings**

Receive Packets on UDP Port ⓘ 9997

---

Sender IP Address ⓘ

---

Receive Packets on IP Address ⓘ

Probe's Local IP Addresses

---

192.0.2.0

---

Active Flow Timeout (Minutes) ⓘ 10

---






Sampling Mode ⓘ  Disable (default)  
 Enable

---

Stream Data Handling ⓘ  Discard stream data (default)  
 Store stream data only for the 'Other' channel  
 Store all stream data

IPFIX Specific Settings

Setting	Description
Receive Packets on UDP Port	Enter the UDP port number on which PRTG receives the flow packets. It must match the UDP port number in the IPFIX export options of the hardware router device. Enter an integer.
Sender IP Address	Enter the IP address of the sending device that you want to receive the IPFIX data from. Enter an IP address to only receive data from a specific device or leave the field empty to receive data from any device on the specified port.
Receive Packets on IP Address	Select the IP addresses on which PRTG listens to IPFIX packets. The list of IP addresses is specific to your setup. To select an IP address, enable a check box in front of the respective line. The IP address that you select must match the IP address in the IPFIX export options of the hardware router device.

Setting	Description
Active Flow Timeout (Minutes)	<p>Enter a time span in minutes after which the sensor must receive new flow data. If the timeout elapses and the sensor receives no new data during this time, it shows the Unknown <a href="#">status</a>. Enter an integer. The maximum timeout is 60 minutes.</p> <p> We recommend that you set the timeout one minute longer than the timeout in the hardware router device.</p> <p> If you set this value too low, flow information might be lost.</p> <p> For more information, see the Knowledge Base: <a href="#">What is the Active Flow Timeout in flow sensors?</a></p>
Sampling Mode	<p>Define if you want to use the sampling mode:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Use the standard flow.</li> <li>▪ Enable: Use the sampling mode and specify the Sampling Rate below.</li> </ul> <p> This setting must match the setting in the xFlow exporter.</p>
Sampling Rate	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Enter a number that matches the sampling rate in the exporting device. If the number is different, monitoring results will be incorrect. Enter an integer.</p>
Stream Data Handling	<p>Define what PRTG does with the stream and packet data:</p> <ul style="list-style-type: none"> <li>▪ Discard stream data (default): Do not store the stream and packet data.</li> <li>▪ Store stream data only for the 'Other' channel: Only store stream and packet data that is not otherwise filtered and is therefore accounted to the default Other channel. PRTG stores this data in the \StreamLog subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Streams Sensor [ID] (1).csv. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> <li>▪ Store all stream data: Store all stream and packet data. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> Use with caution. It can create huge data files. We recommend that you only use this setting for a short time.</p>



## Channel Configuration

**Channel Configuration**

Channel Selection ⓘ

Group	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Content
Web	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	WWW Traffic: HTTP, HTTPS
File Transfer	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	File Transfer: FTP (Control)
Mail	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Mail Traffic: IMAP, POP3, SMTP
Chat	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Chat, Instant Messaging: IRC, AIM
Remote Control	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Remote Control: RDP, SSH, Telnet, VNC
Infrastructure	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Network Services: DHCP, DNS, Ident, ICMP, SNMP
NetBIOS	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	NetBIOS: NETBIOS
Citrix	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Citrix: Citrix
Other Protocols	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Various: Other UDP, Other TCP

**Note** You can change the default configuration for groups and channels. This way, you do not have to customize this setting each time that you add this sensor type. For details, see the Knowledge Base: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)

Channel Configuration

Setting	Description
Channel Selection	<p>Define the categories that the sensor accounts the traffic to:</p> <ul style="list-style-type: none"> <li>▪ Web: Internet web traffic.</li> <li>▪ File Transfer: Traffic from FTP.</li> <li>▪ Mail: Internet mail traffic.</li> <li>▪ Chat: Traffic from chat and instant messaging.</li> <li>▪ Remote Control: Traffic from remote control applications such as RDP, SSH, Telnet, and Virtual Network Computing (VNC).</li> <li>▪ Infrastructure: Traffic from network services such as DHCP, DNS, Ident, ICMP, and SNMP.</li> <li>▪ NetBIOS: Traffic from NetBIOS communication.</li> <li>▪ Citrix: Traffic from Citrix applications.</li> <li>▪ Other Protocols: Traffic from various other protocols via UDP and TCP.</li> </ul> <p>For each group, you can select how many channels the sensor uses, that is, how detailed the sensor divides the traffic:</p> <ul style="list-style-type: none"> <li>▪ No (✘): Do not account traffic of this group in its own channel. The sensor accounts all traffic of this group to the default channel named Other.</li> <li>▪ Yes (✔): Count all traffic of this group and summarize it in one channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Detail (🔍): Count all traffic of this group and further divide it into different channels. The traffic appears in several channels that you can see in the Content column. <ul style="list-style-type: none"> <li>ⓘ Extensive use of this option can cause load problems on the probe system. We recommend that you set specific, well-chosen filters for the data that you really want to analyze.</li> </ul> </li> </ul> <p>■ You can change the default configuration for groups and channels. For more information, see the Knowledge Base: <a href="#">How can I change the default groups and channels for flow and Packet Sniffer sensors?</a></p>

## Filtering

■ For more information, see section [Filter Rules](#) <sup>1206</sup>.

**Filtering**

**Filters** To include and exclude specific traffic, you can define filter rules based on the following format guidelines:

- field[filter]

**Fields:**

IP, Port, SourceIP, SourcePort, DestinationIP, DestinationPort, Protocol (values TCP, UDP, ICMP, OSPFIGP or any number), ToS, DSCP

**Additional IPFIX fields:**

Interface, ASI, InboundInterface, OutboundInterface, SourceASI, DestinationASI, MAC, SourceMAC, DestinationMAC, Mask, SourceMask, DestinationMask ('Masks' represent subnet masks in the form of a single number ('number of contiguous bits')), NextHop (IP Address), VLAN, SourceVLAN, DestinationVLAN ('VLANs' represent a VLAN identifier)

Include Filter ⓘ

Exclude Filter ⓘ

Filtering

Setting	Description
Include Filter	Define if you want to filter any traffic. If you leave this field empty, the sensor includes all traffic. To include specific traffic only, define filters using a special <a href="#">syntax</a> .
Exclude Filter	First, the sensor considers the filters in Include Filter. From this subset, you can explicitly exclude traffic, using the same syntax.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Primary Toplist

**Primary Toplist**


Primary Toplist ⓘ Top Connections

Primary Toplist

Setting	Description
Primary Toplist	Define which Toplist is the primary Toplist of the sensor:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Top Talkers</li> <li>▪ Top Connections</li> <li>▪ Top Protocols</li> <li>▪ <a href="#">[Any custom Toplists you add]</a></li> </ul> <p><b>i</b> PRTG shows the primary Toplist in maps when you add a Toplist object.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Toplists

For all Flow (NetFlow, jFlow, sFlow, IPFIX) and Packet Sniffer sensors, Toplists are available on the sensor's Overview tab. Using Toplists, you can review traffic data for small time periods in great detail.

 For more information, see section [Toplists](#).


## Filter Rules

 For more information, see section [Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Chat	The traffic from chat and instant messaging (IRC, AIM)
Citrix	The traffic from Citrix applications
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
FTP/P2P	The traffic from file transfer (FTP/P2P)
Infrastructure	The traffic from network services (DHCP, DNS, Ident, ICMP, SNMP)
Mail	The internet mail traffic (IMAP, POP3, SMTP)
NetBIOS	The traffic from NetBIOS communication
Other	The traffic from various other protocols (UDP, TCP)
Remote Control	The traffic from remote control applications (RDP, SSH, Telnet, Virtual Network Computing (VNC))
Total	The total traffic  This channel is the primary channel by default.
Various	The traffic from various other sources
WWW	The traffic from the web (HTTP, HTTPS)

## More

### KNOWLEDGE BASE

What is the Active Flow Timeout in flow sensors?

- <https://kb.paessler.com/en/topic/66485>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How can I change the default groups and channels for flow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

### PAESSLER TOOLS

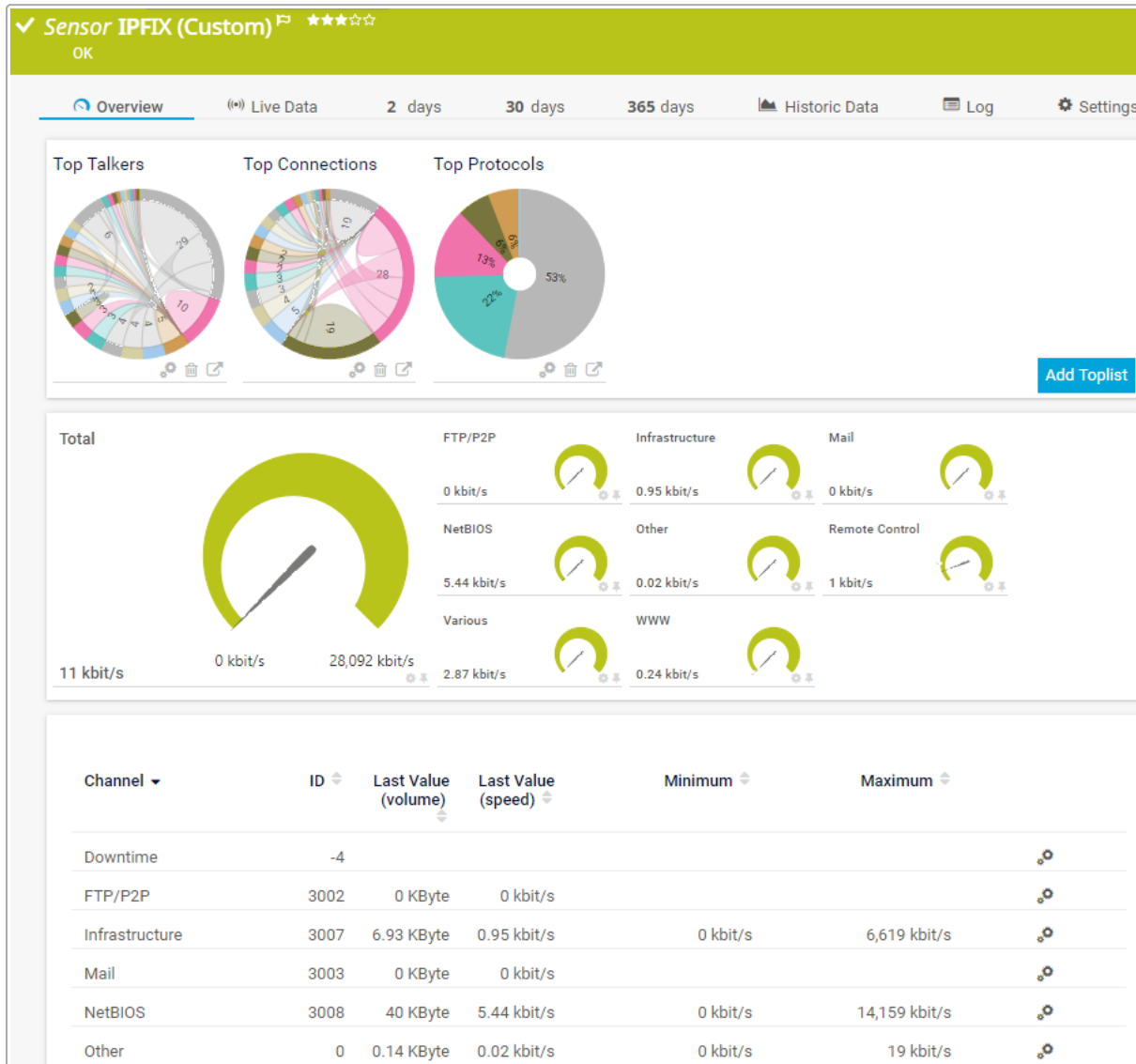
NetFlow Tester

- <https://www.paessler.com/tools/netflowtester>

## 7.8.81 IPFIX (Custom) Sensor

The IPFIX (Custom) sensor receives traffic data from an Internet Protocol Flow Information Export (IPFIX) compatible device and shows the traffic by type. With this sensor, you can define your own channel definitions to divide traffic into different channels.

**i** Make sure that the target device supports IPFIX if you want to use this sensor.



IPFIX (Custom) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: IPFIX (aangepast)
- French: IPFIX personnalisé
- German: IPFIX (Benutzerdef.)

- Japanese: IPFIX( カスタム)
- Portuguese: IPFIX (customizado)
- Russian: IPFIX (нестандартный)
- Simplified Chinese: IPFIX (自定义)
- Spanish: IPFIX (personalizado)

## Remarks

Consider the following [remarks](#) <sup>1209</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
IPFIX	This sensor requires that the IPFIX export is enabled on the target system. The target system must send the flow data stream to the IP address of the probe system.
Channels	This sensor does not officially support more than <a href="#">50 channels</a> .
Cluster probe	This sensor does not support cluster probes. You can only set it up on local probes or remote probes.
IPv4	This sensor only supports IPv4.
Knowledge Base	Knowledge Base: <a href="#">What is the Active Flow Timeout in flow sensors?</a>
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ

**Priority** ⓘ

Example Name

---

exampletag ✕ +

---

★★★★☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- bandwidthsensor
- netflowsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### IPFIX Specific Settings

#### IPFIX Specific Settings

Receive Packets on UDP Port ⓘ

---

Sender IP Address ⓘ

---

Receive Packets on IP Address ⓘ

Probe's Local IP Addresses

---

192.0.2.0

---

Active Flow Timeout (Minutes) ⓘ

---

Sampling Mode ⓘ

Disable (default)

Enable

---

Channel Definition ⓘ

---

Stream Data Handling ⓘ

Discard stream data (default)







Store stream data only for the 'Other' channel

Store all stream data

IPFIX Specific Settings

Setting	Description
Receive Packets on UDP Port	Enter the UDP port number on which PRTG receives the flow packets. It must match the UDP port number in the IPFIX export options of the hardware router device. Enter an integer.
Sender IP Address	Enter the IP address of the sending device that you want to receive the IPFIX data from. Enter an IP address to only receive data from a specific device or leave the field empty to receive data from any device on the specified port.



Setting	Description
Receive Packets on IP Address	<p>Select the IP addresses on which PRTG listens to IPFIX packets. The list of IP addresses is specific to your setup. To select an IP address, enable a check box in front of the respective line. The IP address that you select must match the IP address in the IPFIX export options of the hardware router device.</p>
Active Flow Timeout (Minutes)	<p>Enter a time span in minutes after which the sensor must receive new flow data. If the timeout elapses and the sensor receives no new data during this time, it shows the Unknown <a href="#">status</a>. Enter an integer. The maximum timeout is 60 minutes.</p> <p> We recommend that you set the timeout one minute longer than the timeout in the hardware router device.</p> <p> If you set this value too low, flow information might be lost.</p> <p> For more information, see the Knowledge Base: <a href="#">What is the Active Flow Timeout in flow sensors?</a></p>
Sampling Mode	<p>Define if you want to use the sampling mode:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Use the standard flow.</li> <li>▪ Enable: Use the sampling mode and specify the Sampling Rate below.</li> </ul> <p> This setting must match the setting in the xFlow exporter.</p>
Sampling Rate	<p><b>This setting is only visible if you select Enable above.</b></p> <p>Enter a number that matches the sampling rate in your device that exports the flows. If the number is different, monitoring results will be incorrect. Enter an integer.</p>
Channel Definition	<p>Enter a channel definition to divide the traffic into different channels. Enter each definition in one line. The sensor accounts all traffic that you do not define a channel for to the default channel Other.</p> <p> For more information, see section <a href="#">Channel Definitions for Flow, IPFIX and Packet Sniffer Sensors</a>.</p> <p> Extensive use of many filters can cause load problems on the probe system. We recommend that you define specific, well-chosen filters for the data that you really want to analyze. We recommend that you do not use more than 20 channels in graphs and tables, and not more than 100 channels in total. For performance reasons, we recommend that you add several sensors with fewer channels each.</p>
Stream Data Handling	<p>Define what PRTG does with the stream and packet data:</p> <ul style="list-style-type: none"> <li>▪ Discard stream data (default): Do not store the stream and packet data.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Store stream data only for the 'Other' channel: Only store stream and packet data that is not otherwise filtered and is therefore accounted to the default Other channel. PRTG stores this data in the \StreamLog subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Streams Sensor [ID] (1).csv. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> <li>▪ Store all stream data: Store all stream and packet data. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><b>i</b> Use with caution. It can create huge data files. We recommend that you only use this setting for a short time.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

## Filtering

For more information, see section [Filter Rules](#) <sup>1214</sup>.

**Filtering**

**Filters** *To include and exclude specific traffic, you can define filter rules based on the following format guidelines:*

- field[filter]

*Fields:*

IP, Port, SourceIP, SourcePort, DestinationIP, DestinationPort, Protocol (values TCP, UDP, ICMP, OSPF/IGP or any number), ToS, DSCP

*Additional IPFIX fields:*

Interface, ASI, InboundInterface, OutboundInterface, SourceASI, DestinationASI, MAC, SourceMAC, DestinationMAC, Mask, SourceMask, DestinationMask ('Masks' represent subnet masks in the form of a single number ('number of contiguous bits')), NextHop (IP Address), VLAN, SourceVLAN, DestinationVLAN ('VLANs' represent a VLAN identifier)

Include Filter ⓘ

Exclude Filter ⓘ

Filtering

Setting	Description
Include Filter	Define if you want to filter any traffic. If you leave this field empty, the sensor includes all traffic. To include specific traffic only, define filters using a special <a href="#">syntax</a> .
Exclude Filter	First, the sensor considers the filters in Include Filter. From this subset, you can explicitly exclude traffic, using the same syntax.


## Primary Toplist

**Primary Toplist**
Primary Toplist ⓘ
Top Connections

Primary Toplist

Setting	Description
Primary Toplist	<p>Define which Toplist is the primary Toplist of the sensor:</p> <ul style="list-style-type: none"> <li>▪ Top Talkers</li> <li>▪ Top Connections</li> <li>▪ Top Protocols</li> <li>▪ <a href="#">[Any custom Toplists you add]</a></li> </ul> <p><b>i</b> PRTG shows the primary Toplist in maps when you add a Toplist object.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Toplists

For all Flow (NetFlow, jFlow, sFlow, IPFIX) and Packet Sniffer sensors, Toplists are available on the sensor's Overview tab. Using Toplists, you can review traffic data for small time periods in great detail.

 For more information, see section [Toplists](#).


## Filter Rules

 For more information, see section [Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
<a href="#">[Custom]</a>	The traffic by type according to the channel definition
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Other	All traffic for which no channel is defined
Total	The total traffic  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

What is the Active Flow Timeout in flow sensors?

- <https://kb.paessler.com/en/topic/66485>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

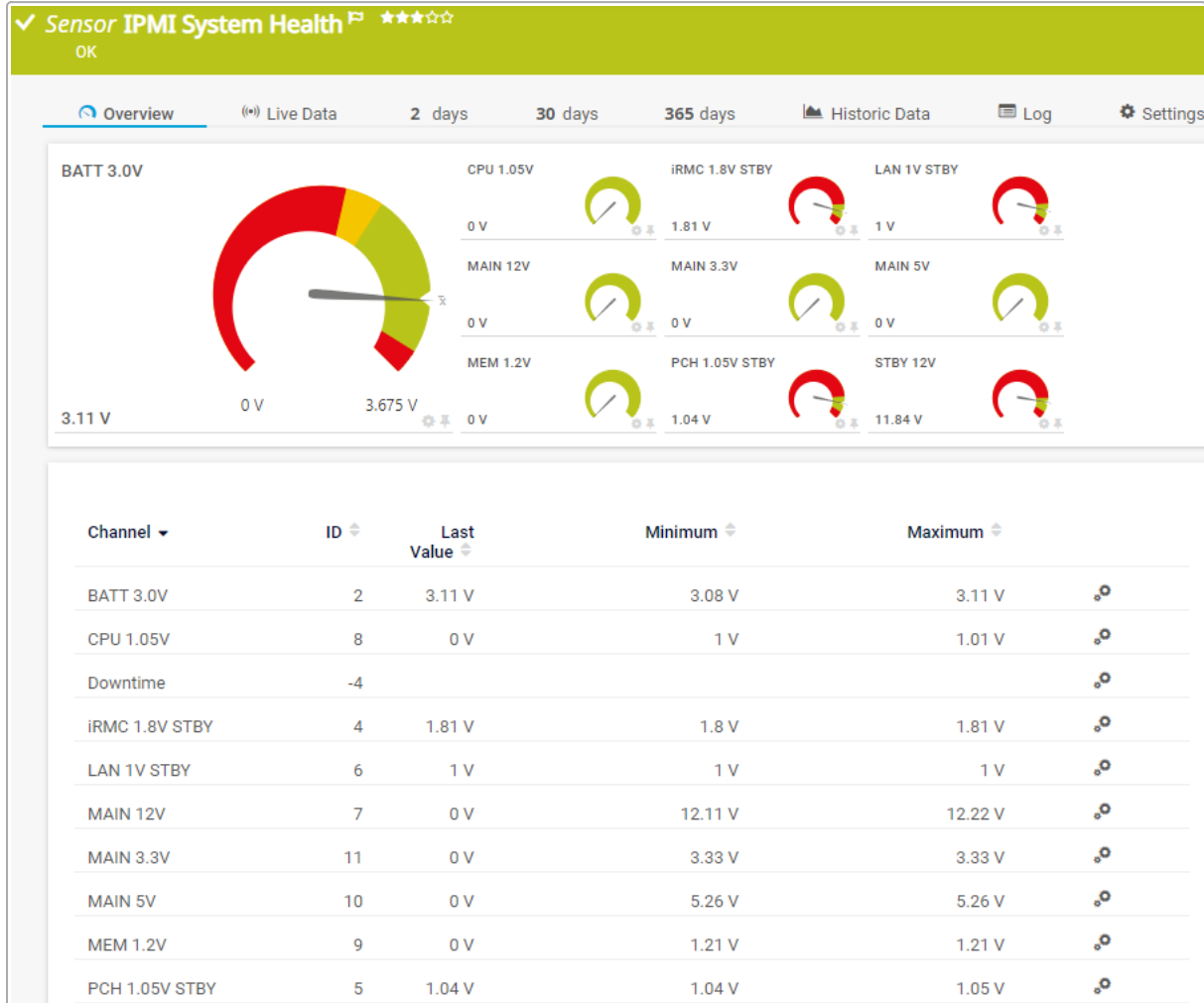
### PAESSLER TOOLS

NetFlow Tester

- <https://www.paessler.com/tools/netflowtester>

## 7.8.82 IPMI System Health Sensor

The IPMI System Health sensor monitors the status of a system via the Intelligent Platform Management Interface (IPMI).



IPMI System Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).




### Sensor in Other Languages

- Dutch: IPMI Systeemstatus
- French: IPMI état du système
- German: IPMI Systemzustand
- Japanese: IPMI システム正常性
- Portuguese: Saúde do sistema IPMI
- Russian: Работоспособность системы IPMI
- Simplified Chinese: IPMI 系统健康状况

- Spanish: Salud de sistema IPMI

## Remarks

Consider the following [remarks](#)<sup>1217</sup> and requirements for this sensor:

Remark	Description
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Credentials	This sensor requires that you explicitly specify the credentials of the IPMI in the sensor settings.
IPMI v1.0	This sensor only supports IPMI v1.0. If the target system uses IPMI v2.0, try the <a href="#">Redfish System Health</a> <sup>1695</sup> sensor.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- ipmi

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### IPMI Credentials

## IPMI Credentials

**User Name** ⓘ

**Password** ⓘ

IPMI Credentials

Setting	Description
User Name	Enter the user name for the IPMI.
Password	Enter the password for the IPMI. ⓘ This sensor only supports passwords with a maximum of <b>16</b> characters.

### IPMI Specific

## IPMI Specific

**Group** ⓘ

**Result Handling** ⓘ

Discard result (default)

Store result

IPMI Specific

Setting	Description
Group	The metric that this sensor monitors.
Result Handling	Define what PRTG does with the log file results: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **ⓘ** Downtime

---


Graph Type **ⓘ**  Show channels independently (default)

Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	The value status, for example <ul style="list-style-type: none"> <li>▪ Fan RPM</li> <li>▪ Status of a power supply</li> <li>▪ Temperatures, for example, the system temperature or the peripheral temperature</li> <li>▪ Voltages</li> </ul>

## More

### ■ KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

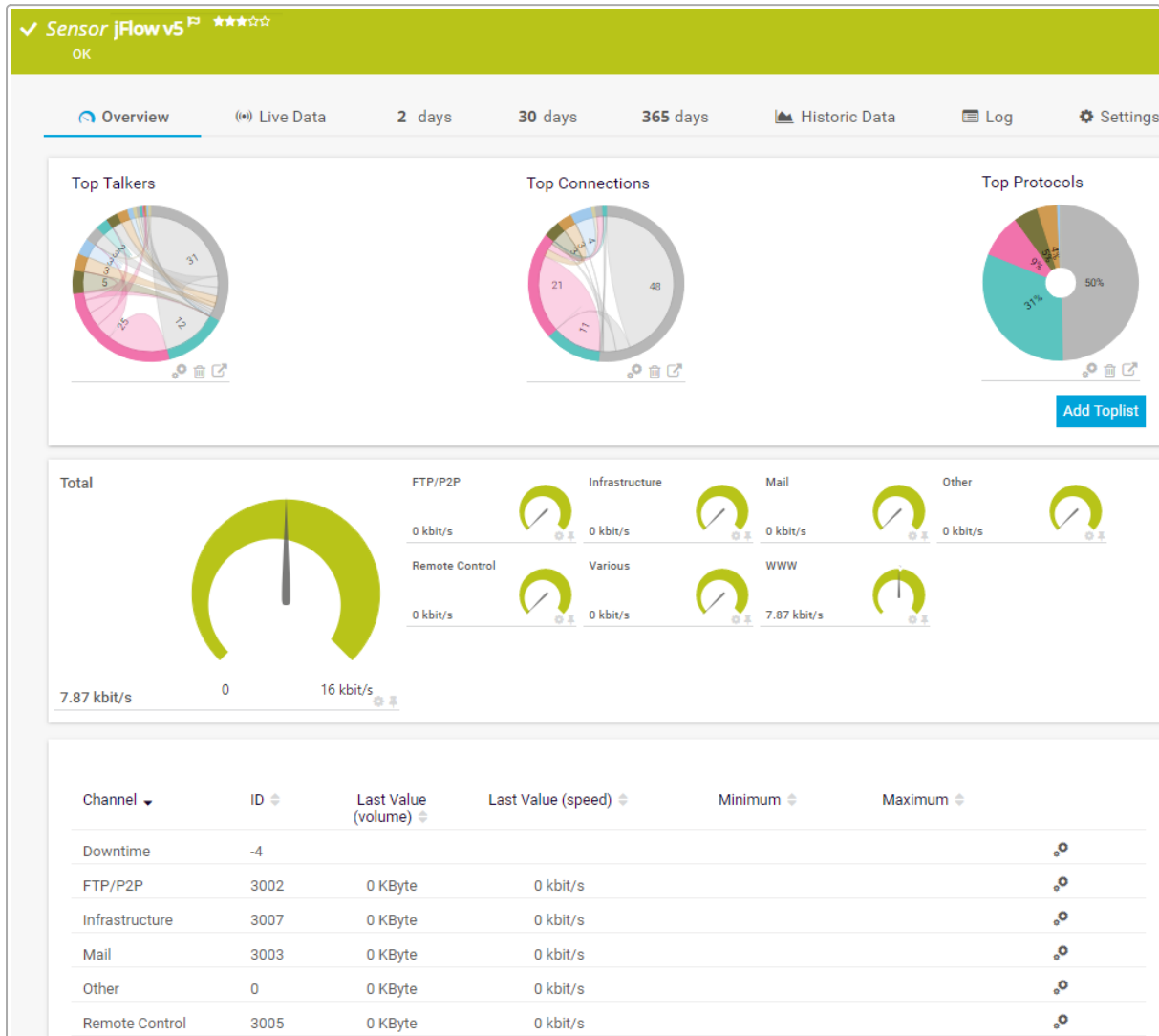
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

### 7.8.83 jFlow v5 Sensor

The jFlow v5 sensor receives traffic data from a jFlow v5-compatible device and shows the traffic by type. This sensor has several filter options to divide traffic into different channels.

**i** Make sure that the sensor matches the jFlow version that your device exports.



jFlow v5 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1223]</sup>.


#### Sensor in Other Languages

- Dutch: jFlow v5
- French: jFlow v5
- German: jFlow v5
- Japanese: jFlow v5
- Portuguese: jFlow v5

- Russian: jFlow v5
- Simplified Chinese: jFlow v5
- Spanish: jFlow v5

## Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
jFlow	This sensor requires that the jFlow export of the respective version is enabled on the target system. The target system must send the flow data stream to the IP address of the probe system.
Cluster probe	This sensor does not support cluster probes. You can only set it up on local probes or remote probes.
IPv4	This sensor only supports IPv4.
Clone sensor	If you clone this sensor to the <b>same</b> probe, PRTG keeps the <a href="#">selected IP addresses</a> on which it listens for Flow (NetFlow, jFlow, sFlow, IPFIX) packets. If you clone this sensor to a <b>different</b> probe, PRTG selects <b>all</b> available IP addresses by default.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">What is the Active Flow Timeout in flow sensors?</a></li> <li>▪ Knowledge Base: <a href="#">How can I change the default groups and channels for flow and Packet Sniffer sensors?</a></li> </ul>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- bandwidthsensor
- jflowsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### jFlow v5 Specific Settings

**jFlow v5 Specific Settings**

Receive Packets on UDP Port ⓘ 9997

---

Sender IP Address ⓘ

---

Receive Packets on IP Address ⓘ

Probe's Local IP Addresses

---

192.0.2.0

---

Active Flow Timeout (Minutes) ⓘ 10

---

Sampling Mode ⓘ

Disable (default)

Enable

---

Stream Data Handling ⓘ







Discard stream data (default)

Store stream data only for the 'Other' channel

Store all stream data

jFlow v5 Specific Settings

Setting	Description
Receive Packets on UDP Port	<p>Enter the UDP port number on which PRTG receives the flow packets. It must match the UDP port number that in the jFlow export options of the hardware router device. Enter an integer.</p> <p><b>i</b> When you configure the export, make sure that you select the appropriate jFlow version for this sensor.</p>
Sender IP Address	<p>Enter the IP address of the sending device that you want to receive the jFlow data from. Enter an IP address to only receive data from a specific device or leave the field empty to receive data from any device on the specified port.</p>

Setting	Description
Receive Packets on IP Address	<p>Select the IP addresses on which PRTG listens to jFlow packets. The list of IP addresses is specific to your setup. To select an IP address, enable a check box in front of the respective line. The IP address that you select must match the IP address in the jFlow export options of the hardware router device.</p> <p> When you configure the export, make sure that you select the appropriate jFlow version for this sensor.</p>
Active Flow Timeout (Minutes)	<p>Enter a time span in minutes after which the sensor must receive new flow data. If the timeout elapses and the sensor receives no new data during this time, it shows the Unknown <a href="#">status</a>. Enter an integer. The maximum timeout is 60 minutes.</p> <p> We recommend that you set the timeout one minute longer than the timeout in the hardware router device.</p> <p> If you set this value too low, flow information might be lost.</p> <p> For more information, see the Knowledge Base: <a href="#">What is the Active Flow Timeout in flow sensors?</a></p>
Sampling Mode	<p>Define if you want to use the sampling mode:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Use the standard flow.</li> <li>▪ Enable: Use the sampling mode and specify the Sampling Rate below.</li> </ul> <p> This setting must match the setting in the xFlow exporter.</p>
Sampling Rate	<p><b>This setting is only visible if you select Enable above.</b></p> <p>Enter a number that matches the sampling rate in the exporting device. If the number is different, monitoring results will be incorrect. Enter an integer.</p>
Stream Data Handling	<p>Define what PRTG does with the stream and packet data:</p> <ul style="list-style-type: none"> <li>▪ Discard stream data (default): Do not store the stream and packet data.</li> <li>▪ Store stream data only for the 'Other' channel: Only store stream and packet data that is not otherwise filtered and is therefore accounted to the default Other channel. PRTG stores this data in the \StreamLog subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Streams Sensor [ID] (1).csv. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> <li>▪ Store all stream data: Store all stream and packet data. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> Use with caution. It can create huge data files. We recommend that you only use this setting for a short time.</p>

## Channel Configuration

**Channel Configuration**

Channel Selection ⓘ

Group	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Content
Web	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	WWW Traffic: HTTP, HTTPS
File Transfer	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	File Transfer: FTP (Control)
Mail	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Mail Traffic: IMAP, POP3, SMTP
Chat	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Chat, Instant Messaging: IRC, AIM
Remote Control	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Remote Control: RDP, SSH, Telnet, VNC
Infrastructure	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Network Services: DHCP, DNS, Ident, ICMP, SNMP
NetBIOS	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	NetBIOS: NETBIOS
Citrix	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Citrix: Citrix
Other Protocols	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Various: Other UDP, Other TCP

**Note** You can change the default configuration for groups and channels. This way, you do not have to customize this setting each time that you add this sensor type. For details, see the Knowledge Base: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)

Channel Configuration

Setting	Description
Channel Selection	<p>Define the categories that the sensor accounts the traffic to:</p> <ul style="list-style-type: none"> <li>▪ Web: Internet web traffic.</li> <li>▪ File Transfer: Traffic from FTP.</li> <li>▪ Mail: Internet mail traffic.</li> <li>▪ Chat: Traffic from chat and instant messaging.</li> <li>▪ Remote Control: Traffic from remote control applications such as RDP, SSH, Telnet, and Virtual Network Computing (VNC).</li> <li>▪ Infrastructure: Traffic from network services such as DHCP, DNS, Ident, ICMP, and SNMP.</li> <li>▪ NetBIOS: Traffic from NetBIOS communication.</li> <li>▪ Citrix: Traffic from Citrix applications.</li> <li>▪ Other Protocols: Traffic from various other protocols via UDP and TCP.</li> </ul> <p>For each group, you can select how many channels the sensor uses, that is, how detailed the sensor divides the traffic:</p> <ul style="list-style-type: none"> <li>▪ No (✘): Do not account traffic of this group in its own channel. The sensor accounts all traffic of this group to the default channel named Other.</li> <li>▪ Yes (✔): Count all traffic of this group and summarize it in one channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Detail (🔍): Count all traffic of this group and further divide it into different channels. The traffic appears in several channels that you can see in the Content column. <ul style="list-style-type: none"> <li>ⓘ Extensive use of this option can cause load problems on the probe system. We recommend that you set specific, well-chosen filters for the data that you really want to analyze.</li> </ul> </li> </ul> <p>■ You can change the default configuration for groups and channels. For more information, see the Knowledge Base: <a href="#">How can I change the default groups and channels for flow and Packet Sniffer sensors?</a></p>

## Filtering

■ For more information, see section [Filter Rules](#) <sup>1226</sup>.

**Filtering**

**Filters** To include and exclude specific traffic, you can define filter rules based on the following format guidelines:

- field[filter]

**Fields:**

IP, Port, SourceIP, SourcePort, DestinationIP, DestinationPort, Protocol (values TCP, UDP, ICMP, OSPFIGP or any number), ToS, DSCP

**Additional IPFIX fields:**

Interface, ASI, InboundInterface, OutboundInterface, SourceASI, DestinationASI, MAC, SourceMAC, DestinationMAC, Mask, SourceMask, DestinationMask ('Masks' represent subnet masks in the form of a single number ('number of contiguous bits')), NextHop (IP Address), VLAN, SourceVLAN, DestinationVLAN ('VLANs' represent a VLAN identifier)

Include Filter ⓘ

Exclude Filter ⓘ

Filtering

Setting	Description
Include Filter	Define if you want to filter any traffic. If you leave this field empty, the sensor includes all traffic. To include specific traffic only, define filters using a special <a href="#">syntax</a> .
Exclude Filter	First, the sensor considers the filters in Include Filter. From this subset, you can explicitly exclude traffic, using the same syntax.



## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Primary Toplist

**Primary Toplist**


Primary Toplist ⓘ Top Connections

Primary Toplist

Setting	Description
Primary Toplist	Define which Toplist is the primary Toplist of the sensor:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Top Talkers</li> <li>▪ Top Connections</li> <li>▪ Top Protocols</li> <li>▪ <a href="#">[Any custom Toplists you add]</a></li> </ul> <p><b>i</b> PRTG shows the primary Toplist in maps when you add a Toplist object.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Toplists

For all Flow (NetFlow, jFlow, sFlow, IPFIX) and Packet Sniffer sensors, Toplists are available on the sensor's Overview tab. Using Toplists, you can review traffic data for small time periods in great detail.

■ For more information, see section [Toplists](#).

## Filter Rules

The following filter rules apply to all Flow (NetFlow, jFlow, sFlow, IPFIX) and Packet Sniffer sensors.

■ For more information, see section [Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors](#).

Field	Possible Filter Values
IP	IP address or DNS name
Port	Any number
SourceIP	IP address or DNS name
SourcePort	Any number
DestinationIP	IP address or DNS name

Field	Possible Filter Values
DestinationPort	Any number
Protocol	Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Open Shortest Path First (OSPF), any number
ToS	Type of Service (ToS): any number
DSCP	Differentiated Services Code Point (DSCP): any number

The following filter rules apply to jFlow v5 sensors only.

Field	Possible Filter Values
Interface	Any number
ASI	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP address of the sending device. Use this if you have several devices that send flow data on the same port, and you want to divide the traffic of each device into a different channel.  Possible values: IP address or DNS name
SourceASI	Any number
DestinationASI	Any number

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Chat	The traffic from chat and instant messaging (IRC, AIM)

Channel	Description
Citrix	The traffic from Citrix applications
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
FTP/P2P	The traffic from file transfer (FTP/P2P)
Infrastructure	The traffic from network services (DHCP, DNS, Ident, ICMP, SNMP)
Mail	The internet mail traffic (IMAP, POP3, SMTP)
NetBIOS	The traffic from NetBIOS communication
Other	The traffic from various other protocols (UDP, TCP)
Remote Control	The traffic from remote control applications (RDP, SSH, Telnet, Virtual Network Computing (VNC))
Total	The total traffic <span>ⓘ</span> This channel is the primary channel by default.
Various	The traffic from various other sources
WWW	The traffic from the web (HTTP, HTTPS)

## More

### ■ KNOWLEDGE BASE

What is the Active Flow Timeout in flow sensors?

- <https://kb.paessler.com/en/topic/66485>

How can I change the default groups and channels for flow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

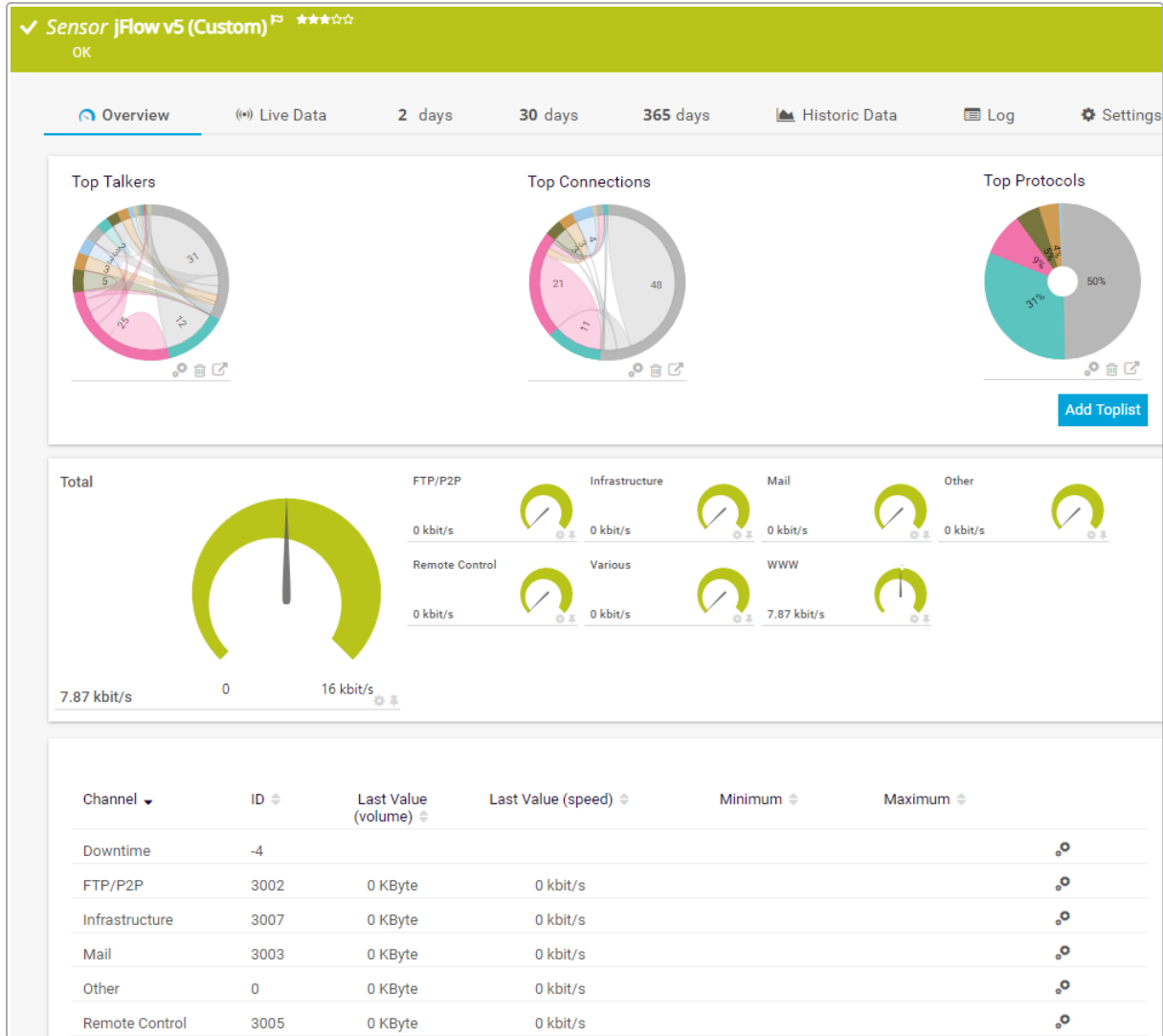
Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

## 7.8.84 jFlow v5 (Custom) Sensor

The jFlow v5 (Custom) sensor receives traffic data from a jFlow v5-compatible device and shows the traffic by type. With this sensor, you can define your own channel definitions to divide traffic into different channels.

**i** Make sure that the sensor matches the jFlow version that your device exports.



jFlow v5 (Custom) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).


### Sensor in Other Languages

- Dutch: jFlow v5 (Klant specifiek)
- French: jFlow v5 personnalisé
- German: jFlow v5 (Benutzerdefiniert)
- Japanese: jFlow v5( カスタム)
- Portuguese: jFlow v5 (customizado)

- Russian: jFlow v5 (нестандартный)
- Simplified Chinese: jFlow v5 (自定义)
- Spanish: jFlow v5 (personalizado)

## Remarks

Consider the following [remarks](#)<sup>1232</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
jFlow	This sensor requires that the jFlow export of the respective version is enabled on the target system. The target system must send the flow data stream to the IP address of the probe system.
Channels	This sensor does not officially support more than <a href="#">50 channels</a> .
Cluster probe	This sensor does not support cluster probes. You can only set it up on local probes or remote probes.
IPv4	This sensor only supports IPv4.
Knowledge Base	Knowledge Base: <a href="#">What is the Active Flow Timeout in flow sensors?</a>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- bandwidthsensor

- jflowsensor

For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### jFlow v5 Specific Settings

**jFlow v5 Specific Settings**

Receive Packets on UDP Port ⓘ 9997

---

Sender IP Address ⓘ

---

Receive Packets on IP Address ⓘ

Probe's Local IP Addresses

---

192.0.2.0

---

Active Flow Timeout (Minutes) ⓘ 10

---

Sampling Mode ⓘ  Disable (default)  
 Enable

---








Channel Definition ⓘ

---


Stream Data Handling ⓘ  Discard stream data (default)  
 Store stream data only for the 'Other' channel  
 Store all stream data

jFlow v5 Specific Settings

Setting	Description
Receive Packets on UDP Port	Enter the UDP port number on which PRTG receives the flow packets. It must match the UDP port number that in the jFlow export options of the hardware router device. Enter an integer.  <b>i</b> When you configure the export, make sure that you select the appropriate jFlow version for this sensor.
Sender IP Address	Enter the IP address of the sending device that you want to receive the jFlow data from. Enter an IP address to only receive data from a specific device or leave the field empty to receive data from any device on the specified port.

Setting	Description
Receive Packets on IP Address	<p>Select the IP addresses on which PRTG listens to jFlow packets. The list of IP addresses is specific to your setup. To select an IP address, enable a check box in front of the respective line. The IP address that you select must match the IP address in the jFlow export options of the hardware router device.</p> <p> When you configure the export, make sure that you select the appropriate jFlow version for this sensor.</p>
Active Flow Timeout (Minutes)	<p>Enter a time span in minutes after which the sensor must receive new flow data. If the timeout elapses and the sensor receives no new data during this time, it shows the Unknown <a href="#">status</a>. Enter an integer. The maximum timeout is 60 minutes.</p> <p> We recommend that you set the timeout one minute longer than the timeout in the hardware router device.</p> <p> If you set this value too low, flow information might be lost.</p> <p> For more information, see the Knowledge Base: <a href="#">What is the Active Flow Timeout in flow sensors?</a></p>
Sampling Mode	<p>Define if you want to use the sampling mode:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Use the standard flow.</li> <li>▪ Enable: Use the sampling mode and specify the Sampling Rate below.</li> </ul> <p> This setting must match the setting in the xFlow exporter.</p>
Sampling Rate	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Enter a number that matches the sampling rate in your device that exports the flows. If the number is different, monitoring results will be incorrect. Enter an integer.</p>
Channel Definition	<p>Enter a channel definition to divide the traffic into different channels. Enter each definition in one line. The sensor accounts all traffic that you do not define a channel for to the default channel Other.</p> <p> For more information, see section <a href="#">Channel Definitions for Flow, IPFIX and Packet Sniffer Sensors</a>.</p> <p> Extensive use of many filters can cause load problems on the probe system. We recommend that you define specific, well-chosen filters for the data that you really want to analyze. We recommend that you do not use more than 20 channels in graphs and tables, and not more than 100 channels in total. For performance reasons, we recommend that you add several sensors with fewer channels each.</p>
Stream Data Handling	<p>Define what PRTG does with the stream and packet data:</p>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ Discard stream data (default): Do not store the stream and packet data.</li> <li>▪ Store stream data only for the 'Other' channel: Only store stream and packet data that is not otherwise filtered and is therefore accounted to the default Other channel. PRTG stores this data in the \StreamLog subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Streams Sensor [ID] (1).csv. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> <li>▪ Store all stream data: Store all stream and packet data. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> Use with caution. It can create huge data files. We recommend that you only use this setting for a short time.</p>

## Filtering

For more information, see section [Filter Rules](#)<sup>1237</sup>.

**Filtering**

**Filters** To include and exclude specific traffic, you can define filter rules based on the following format guidelines:

- field[filter]

**Fields:**

IP, Port, SourceIP, SourcePort, DestinationIP, DestinationPort, Protocol (values TCP, UDP, ICMP, OSPFIGP or any number), ToS, DSCP

**Additional IPFIX fields:**

Interface, ASI, InboundInterface, OutboundInterface, SourceASI, DestinationASI, MAC, SourceMAC, DestinationMAC, Mask, SourceMask, DestinationMask ('Masks' represent subnet masks in the form of a single number ('number of contiguous bits')), NextHop (IP Address), VLAN, SourceVLAN, DestinationVLAN ('VLANs' represent a VLAN identifier)

Include Filter 

Exclude Filter 

Filtering

Setting	Description
Include Filter	Define if you want to filter any traffic. If you leave this field empty, the sensor includes all traffic. To include specific traffic only, define filters using a special <a href="#">syntax</a> .
Exclude Filter	First, the sensor considers the filters in Include Filter. From this subset, you can explicitly exclude traffic, using the same syntax.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Primary Toplist

**Primary Toplist**


Primary Toplist ⓘ Top Connections

Primary Toplist

Setting	Description
Primary Toplist	Define which Toplist is the primary Toplist of the sensor:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Top Talkers</li> <li>▪ Top Connections</li> <li>▪ Top Protocols</li> <li>▪ <a href="#">[Any custom Toplists you add]</a></li> </ul> <p><b>i</b> PRTG shows the primary Toplist in maps when you add a Toplist object.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Toplists

For all Flow (NetFlow, jFlow, sFlow, IPFIX) and Packet Sniffer sensors, Toplists are available on the sensor's Overview tab. Using Toplists, you can review traffic data for small time periods in great detail.

 For more information, see section [Toplists](#).

## Filter Rules

The following filter rules apply to all Flow (NetFlow, jFlow, sFlow, IPFIX) and Packet Sniffer sensors.

 For more information, see section [Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors](#).

Field	Possible Filter Values
IP	IP address or DNS name
Port	Any number
SourceIP	IP address or DNS name
SourcePort	Any number
DestinationIP	IP address or DNS name

Field	Possible Filter Values
DestinationPort	Any number
Protocol	Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Open Shortest Path First (OSPF), any number
ToS	Type of Service (ToS): any number
DSCP	Differentiated Services Code Point (DSCP): any number


The following filter rules apply to jFlow v5 sensors only.

Field	Possible Filter Values
Interface	Any number
ASI	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP address of the sending device. Use this if you have several devices that send flow data on the same port, and you want to divide the traffic of each device into a different channel.  Possible values: IP address or DNS name
SourceASI	Any number
DestinationASI	Any number

## Channel List

- i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
[Custom]	The traffic by type according to the channel definition

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Other	All traffic for which no channel is defined
Total	The total traffic  This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

What is the Active Flow Timeout in flow sensors?

- <https://kb.paessler.com/en/topic/66485>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

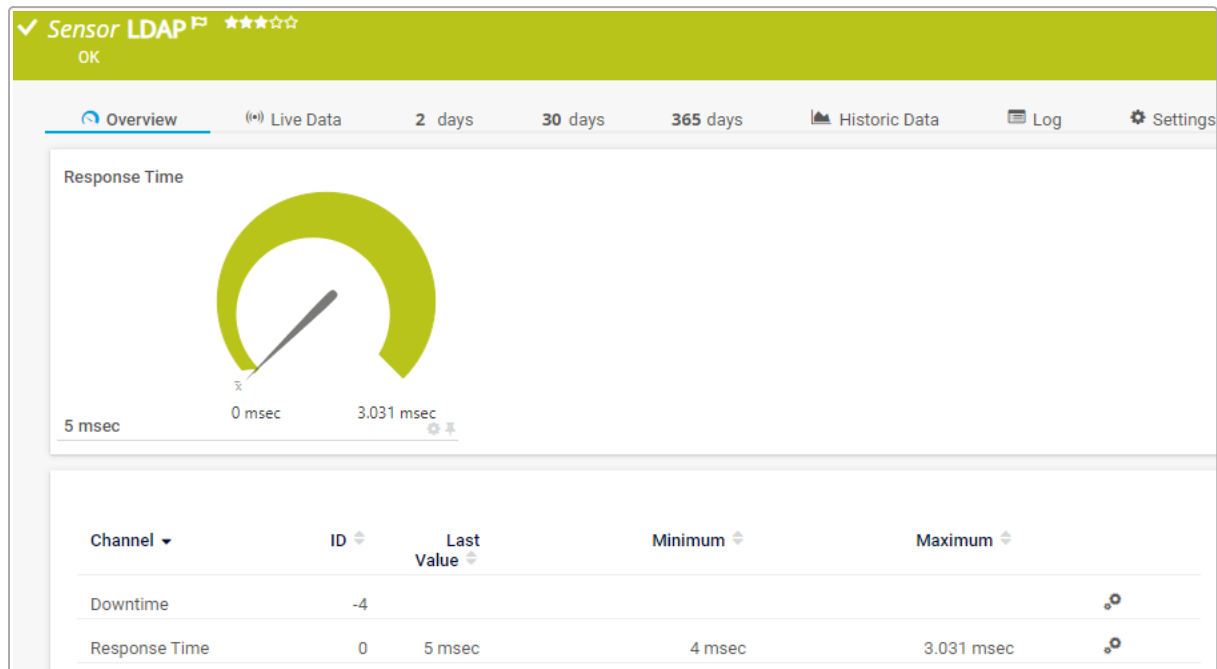
Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

## 7.8.85 LDAP Sensor

The LDAP sensor monitors directory services via the Lightweight Directory Access Protocol (LDAP). It connects to the server by trying a "bind".

**i** If the server does not respond or authentication fails, the sensor shows the Down status.



LDAP Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1243</sup>.

### Sensor in Other Languages

- Dutch: LDAP
- French: LDAP
- German: LDAP
- Japanese: LDAP
- Portuguese: LDAP
- Russian: LDAP
- Simplified Chinese: LDAP
- Spanish: LDAP

### Remarks

Consider the following [remarks](#)<sup>1240</sup> and requirements for this sensor:

Remark	Description
LDAP	This sensor officially supports Microsoft implementations of LDAP. Other third-party LDAP implementations might work but are not officially supported.
DNS name	This sensor requires a DNS name in the <a href="#">settings of the parent device</a> if you use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection to the LDAP server.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
IPv4	This sensor only supports IPv4.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- Idapsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### LDAP Specific

#### LDAP Specific

**Connection Security** ⓘ  Use LDAP without connection security (default)  
 Use LDAP over SSL

**Port Selection** ⓘ  Use default port (default)  
 Use custom port

**Distinguished Name** ⓘ

**Password** ⓘ

LDAP Specific

Setting	Description
Connection Security	<p>Define if the sensor uses an SSL/TLS-secured connection to the LDAP server:</p> <ul style="list-style-type: none"> <li>Use LDAP without connection security (default)</li> <li>Use LDAP over SSL</li> </ul> <p><b>i</b> If you select Use LDAP over SSL, you need to enter a DNS name in the <a href="#">settings of the parent device</a>. The sensor does not work with an IP address.</p>
Port Selection	<p>Define if you want to use a default port or a custom port for the connection to the LDAP server:</p> <ul style="list-style-type: none"> <li>Use default port (default): Use the default port. This is port <b>389</b> for unsecure connections and port <b>636</b> for secure connections.</li> <li>Use custom port: Use a custom port. Specify the Port below.</li> </ul>
Port	<p>This setting is only visible if you select Use custom port above.</p> <p>Enter a custom port for the connection to the LDAP server. Enter an integer.</p>
Distinguished Name	<p>Enter the distinguished name (DN) that you want to authenticate against the LDAP server. Usually, this is the information for the user that you want to authenticate with. For example, use the format <a href="#">cn=Manager,dc=my-domain,dc=com</a> for a DN on an OpenLDAP server.</p>
Password	<p>Enter the password for the Distinguished Name.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p>



Setting	Description
	<p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.           <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Response Time	<p>The response time</p> <p><b>i</b> This channel is the primary channel by default.</p>

## More

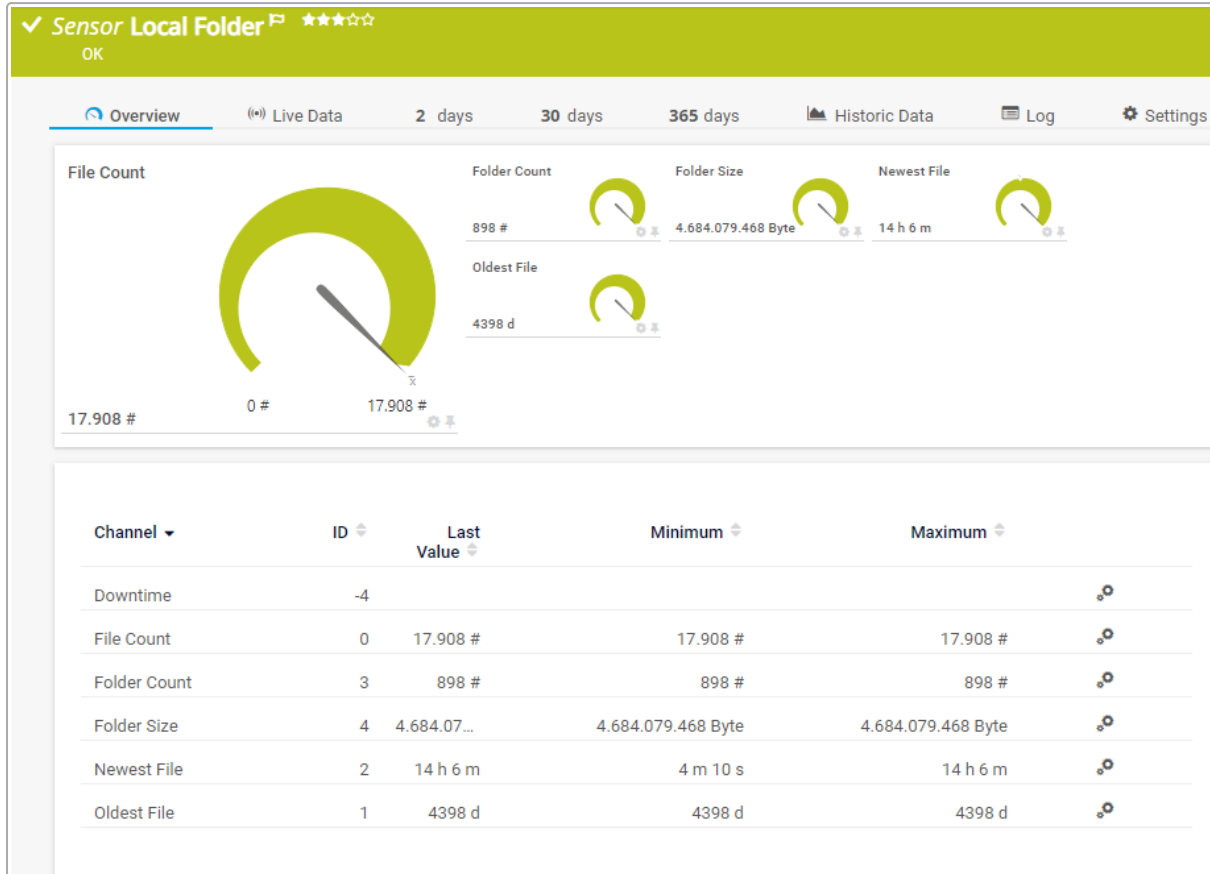
### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.86 Local Folder Sensor

The Local Folder sensor monitors a local folder on a probe system.



Local Folder Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Lokale Map
- French: Dossier local
- German: Lokaler Ordner
- Japanese: ローカルフォルダー
- Portuguese: Pasta local
- Russian: Локальная папка
- Simplified Chinese: 本地文件夹
- Spanish: Carpeta local

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Sensor creation	You can create this sensor only on a <a href="#">probe device</a> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Scanning interval	<ul style="list-style-type: none"> <li>The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>The recommended scanning interval of this sensor is <a href="#">5 minutes</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- filesystem
- folder

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Local Folder Specific

**Local Folder Specific**

Path ⓘ C:\

---

Timeout (Sec.) ⓘ 300

---

Recurse Subfolders ⓘ  Do not recurse subfolders (default)  
 Monitor the folder and its subfolders (recursive)

Filter by File Name ⓘ  Disable (default)  
 Include filter  
 Exclude filter

Filter by File Age ⓘ  Disable (default)  
 Enable

Local Folder Specific

Setting	Setting
Path	<p>Enter the path of the folder that you want to monitor. For example, enter <a href="#">C:\Windows</a>. The folder must exist on the probe system.</p> <p> ⓘ The sensor only supports local paths.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds. If the scan of the folder takes longer, the sensor cancels the request and shows an error message. If two consecutive scans fail, the sensor shows the Down status. The default value is <a href="#">300</a> seconds (5 minutes). The maximum value is <a href="#">1079</a> seconds (17 minutes and 59 seconds).</p>
Recurse Subfolders	<p>Specify if the sensor includes subfolders in the folder monitoring:</p> <ul style="list-style-type: none"> <li>▪ Do not recurse subfolders (default): Only monitor the folder. Do not monitor its subfolders.</li> <li>▪ Monitor the folder and its subfolders (recursive): Monitor the folder and all of its subfolders.</li> </ul> <p> ⓘ If you recurse subfolders in large directories that have a high number of branches, this might cause timeout errors or performance issues.</p>
Filter by File Name	<p>Select if you want to filter by file name:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not filter by file name.</li> <li>▪ Include filter: The sensor counts files that match the File Filter.</li> <li>▪ Exclude filter: The sensor counts files that do not match the File Filter.</li> </ul>

Setting	Setting
File Filter	<p>This setting is only visible if you select <a href="#">Include filter</a> or <a href="#">Exclude filter</a> above.</p> <p>Enter a comma-separated list of file names, file formats, or patterns you want to filter for. For example, '*.pdf, *.docx' includes or excludes files with the file formats .pdf or .docx.</p> <p><b>i</b> The file filter is not case-sensitive and supports wildcards (*).</p>
Filter by File Age	<p>Select if you want to filter by file age:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not filter by file age.</li> <li>▪ Enable: Filter by file age.</li> </ul>
Newer Than	<p>This setting is only visible if you select <a href="#">Enable</a> above.</p> <p>Enter a file age. The sensor only counts files that are younger than this age.</p> <p><b>i</b> Leave this field empty if you only want to filter for files with the Older Than setting.</p>
Older Than	<p>This setting is only visible if you select <a href="#">Enable</a> above.</p> <p>Enter a file age. The sensor only counts files that are older than this age.</p> <p><b>i</b> Leave this field empty if you only want to filter for files with the Newer Than setting.</p>
File Age Filter Unit	<p>This setting is only visible if you select <a href="#">Enable</a> above.</p> <p>Select the time unit that you want to use for Filter by File Age:</p> <ul style="list-style-type: none"> <li>▪ Days (default)</li> <li>▪ Hours</li> <li>▪ Minutes</li> </ul>

## Sensor Display


**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i** 
 Show channels independently (default)
   
 Stack channels on top of each other

Sensor Display


Setting	Setting
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

### Debug Options


**Result Handling** **i**
 Discard result (default)
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
File Count	<p>The number of files in the folder</p> <p><b>i</b> The sensor counts all files in a folder, including <a href="#">hidden files</a>.</p> <p><b>i</b> This channel is the primary channel by default.</p>
Folder Count	The number of folders
Folder Size	The folder size
Newest File	<p>The time since the newest modification of a file in the folder (newest file)</p> <p><b>i</b> The sensor shows a negative value if the date of a modified file is in the future.</p>
Oldest File	The time since the oldest modification of a file in the folder (oldest file)

## More

 KNOWLEDGE BASE

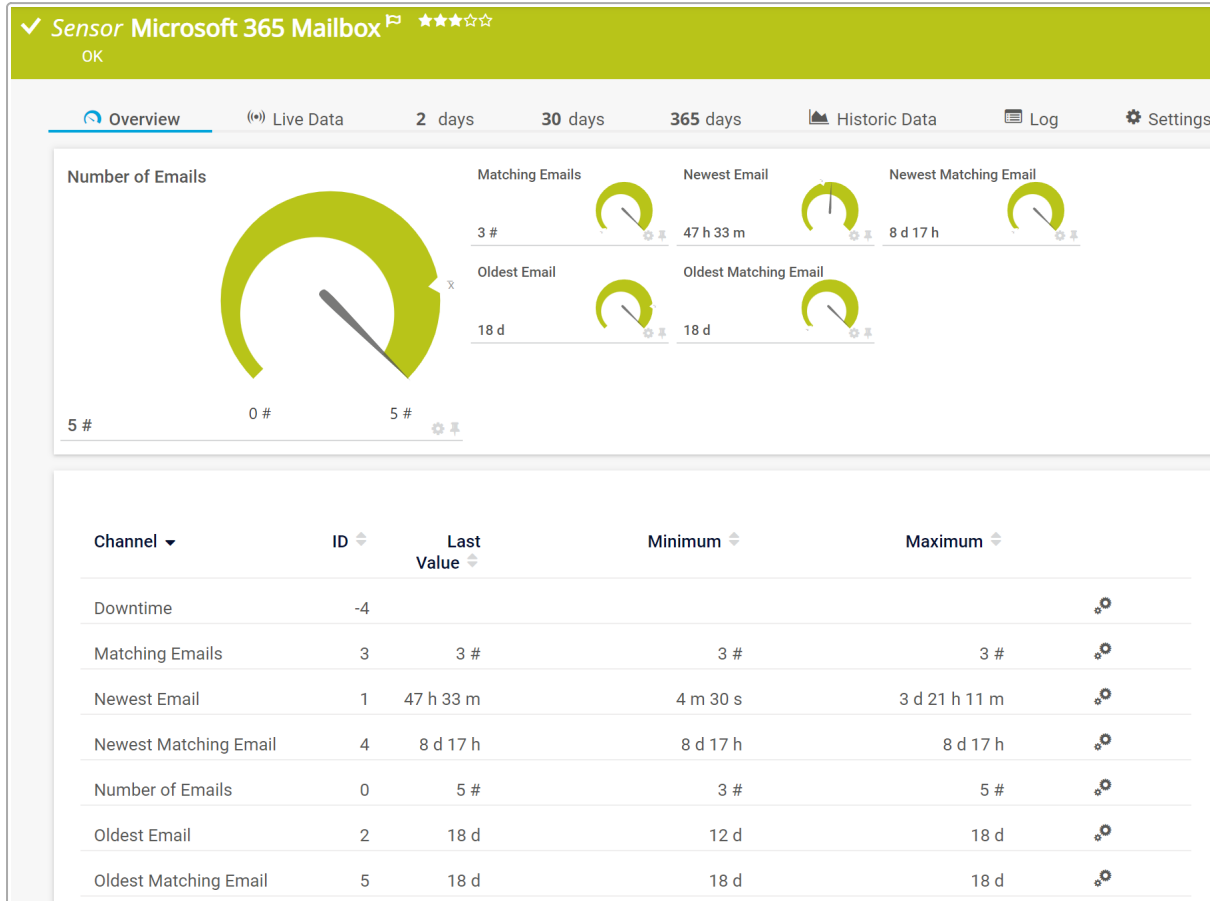


What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.87 Microsoft 365 Mailbox Sensor

The Microsoft 365 Mailbox sensor monitors a folder of a Microsoft 365 mailbox via Microsoft Graph.



Microsoft 365 Mailbox Sensor






For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Microsoft 365 Mailbox
- French: Microsoft 365 boîte aux lettres
- German: Microsoft 365 Postfach
- Japanese: Microsoft 365 メールボックス
- Portuguese: Caixa de correio do Microsoft 365
- Russian: Почтовый ящик Microsoft 365
- Simplified Chinese: Microsoft 365 邮箱
- Spanish: Buzón de Microsoft 365

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Permission for the APIs	<p>This sensor requires permissions for <a href="#">Microsoft Graph</a>.</p> <p> This sensor requires the following delegated permissions to query data from <a href="#">Microsoft Graph</a>:</p> <ul style="list-style-type: none"> <li>▫ Microsoft Graph / User.Read</li> <li>▫ Microsoft Graph / Mail.Read</li> <li>▫ Microsoft Graph / Mail.Read.Shared (optional)</li> <li>▫ Microsoft Graph / offline_access</li> </ul> <p> For more information, see the Knowledge Base: <a href="#">How do I obtain credentials and set permissions for the Microsoft 365 Mailbox sensor?</a></p>
Redirect URIs	<p>This sensor requires that you provide a redirect URI in the Microsoft Azure Portal. You must provide the DNS name or an IP address of your PRTG web server as redirect URI in the Microsoft Azure Portal according the following pattern: <a href="https://&lt;yourprtgserver&gt;/ms365.htm">https://&lt;yourprtgserver&gt;/ms365.htm</a></p> <p> Microsoft Azure only accepts redirect URIs that start with <a href="#">HTTPS</a>.</p> <p> For more information, see the Knowledge Base: <a href="#">How do I obtain credentials and set permissions for the Microsoft 365 Mailbox sensor?</a></p>
Secure HTTPS server	<p>This sensor requires that the PRTG web server accepts incoming HTTPS requests.</p> <p> For more information, see section PRTG Web Server in chapter <a href="#">User Interface</a>.</p>
Credentials	<p>This sensor requires credentials for Microsoft 365.</p>
IPv6	<p>This sensor supports IPv6.</p>
Performance impact	<p>This sensor has a <a href="#">low</a> performance impact.</p>
Scanning interval	<ul style="list-style-type: none"> <li>▫ The minimum scanning interval of this sensor is <a href="#">30 seconds</a>.</li> <li>▫ The recommended scanning interval of this sensor is <a href="#">10 minutes</a>.</li> </ul>
Knowledge Base	<p>Knowledge Base: <a href="#">How do I obtain credentials and set permissions for the Microsoft 365 Mailbox sensor?</a></p>

## Basic Sensor Settings

Basic Sensor Settings

Sensor Name ⓘ Example Name

---

Tags ⓘ exampletag ✕ +

---

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- mailsensor
- microsoft365
- microsoft365sensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Microsoft 365 Specific

Microsoft 365 Specific

Folder Name ⓘ *Junk Email*

---

Folder Path ⓘ /

Microsoft 365 Specific

Setting	Description
Folder Name	The name of the target folder that this sensor monitors.
Folder Path	The path of the target folder that this sensor monitors.

## Microsoft OAuth 2.0 Specific

Microsoft OAuth 2.0 Specific

Authorization Renew

Microsoft OAuth 2.0 Specific

Setting	Description
Authorization	Click Renew to start the Microsoft Azure authorization process.

### Microsoft 365 Mailbox

**Microsoft 365 Mailbox**

**Shared Mailbox User Principal Name (optional)**  ⓘ
*SharedMailbox@example.com*

Microsoft 365 Mailbox

Setting	Description
Shared Mailbox User Principal Name (optional)	<p>The user principal name of a shared mailbox to which the authenticated user account has access.</p> <p><span style="font-size: 1.2em;"> ⓘ</span> In most cases, the user principal name is the email address of the shared mailbox.</p>

## Microsoft 365 Settings

**Microsoft 365 Settings**

**Filter by 'Subject'** ⓘ  Disable (default)  
 'Subject' matches exact string  
 'Subject' contains all strings  
 'Subject' contains one or more strings  
 'Subject' matches regular expression

**Filter by 'From'** ⓘ  Disable (default)  
 'From' matches exact string  
 'From' contains all strings  
 'From' contains one or more strings  
 'From' matches regular expression

**Filter by 'Body'** ⓘ  Disable (default)  
 'Body' matches exact string  
 'Body' contains all strings  
 'Body' contains one or more strings  
 'Body' matches regular expression

**Filter by 'Age'** ⓘ  Disable (default)  
 Enable

Microsoft 365 Settings

Setting	Description
Filter by 'Subject'	<p>Select if you want to filter the emails by the 'Subject' field:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not use Filter by 'Subject'.</li> <li>▪ 'Subject' matches exact string: Filter emails whose 'Subject' field matches the defined string exactly.</li> <li>▪ 'Subject' contains all strings: Filter emails whose 'Subject' field contains all defined strings.</li> <li>▪ 'Subject' contains one or more strings: Filter emails whose 'Subject' field contains at least one of the defined strings.</li> <li>▪ 'Subject' matches regular expression: Filter emails whose 'Subject' field matches the defined regular expression.</li> </ul>

Setting	Description
	<p><b>i</b> The regular expressions filter will result in the Down status if there are more than 10,000 emails in the mailbox folder you want to monitor. This is because the regular expression filter is applied after the emails are retrieved from the API. The larger the volume of emails, the greater the impact on performance. Enable the Filter by 'Age' setting or use a non-regular expression filter in addition to the regular expression filter to reduce the number of emails.</p> <p><b>i</b> If you enable Filter by 'Subject', Filter by 'From', or Filter by 'Body', the sensor creates up to three additional channels that monitor the emails that match your filters.</p> <p><b>i</b> If you disable the filters, the additional channels remain, but do not receive data anymore.</p>
Search for	<p>This setting is only visible if you choose to filter by the 'Subject' field above.</p> <p>Enter a string or regular expression that you want to use for Filter by 'Subject'.</p> <p><b>i</b> If you select 'Subject' contains all strings or 'Subject' contains one or more strings above, you can also enter a comma-separated list of strings to search for more than one string. For example, if you select 'Subject' contains all strings and enter <b>backup</b> and <b>failed</b>, the sensor counts all items that contain both strings. If you select 'Subject' contains one or more strings and enter <b>backup</b> and <b>failed</b>, the sensor counts all items that contain at least one of the strings.</p>
Filter by 'From'	<p>Select if you want to filter the emails by the 'From' field:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not use Filter by 'From'.</li> <li>▪ 'From' matches exact string: Filter emails whose 'From' field matches the defined string exactly.</li> <li>▪ 'From' contains all strings: Filter emails whose 'From' field contains all defined strings.</li> <li>▪ 'From' contains one or more strings: Filter emails whose 'From' field contains at least one of the defined strings.</li> <li>▪ 'From' matches regular expression: Filter emails whose 'From' field matches the defined regular expression.</li> </ul> <p><b>i</b> The regular expressions filter will result in the Down status if there are more than 10,000 emails in the mailbox folder you want to monitor. This is because the regular expression filter is applied after the emails are retrieved from the API. The larger the volume of emails, the greater the impact on performance. Enable the Filter by 'Age' setting or use a non-regular expression filter in addition to the regular expression filter to reduce the number of emails.</p>

Setting	Description
	<p><b>i</b> If you enable Filter by 'Subject', Filter by 'From', or Filter by 'Body', the sensor creates up to three additional channels that monitor the emails that match your filters.</p> <p><b>i</b> If you disable the filters, the additional channels remain, but do not receive data anymore.</p>
Search for	<p><b>This setting is only visible if you choose to filter by the 'From' field above.</b></p> <p>Enter a string or regular expression that you want to use for Filter by 'From'.</p> <p><b>i</b> If you select 'From' contains all strings or 'From' contains one or more strings above, you can also enter a comma-separated list of strings to search for more than one string. For example, if you select 'From' contains all strings and enter <b>backup</b> and <b>failed</b>, the sensor counts all items that contain both strings. If you select 'From' contains one or more strings and enter <b>backup</b> and <b>failed</b>, the sensor counts all items that contain at least one of the strings.</p>
Filter by 'Body'	<p>Select if you want to filter the emails by the text in the 'Body' field:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not use Filter by 'Body'.</li> <li>▪ 'Body' matches exact string: Filter emails whose body matches the defined string exactly.</li> <li>▪ 'Body' contains all strings: Filter emails whose body contains all defined strings.</li> <li>▪ 'Body' contains one or more strings: Filter emails whose body contains at least one of the defined strings.</li> <li>▪ 'Body' matches regular expression: Filter emails whose body matches the defined regular expression.</li> </ul> <p><b>i</b> The regular expressions filter will result in the Down status if there are more than 10,000 emails in the mailbox folder you want to monitor. This is because the regular expression filter is applied after the emails are retrieved from the API. The larger the volume of emails, the greater the impact on performance. Enable the Filter by 'Age' setting or use a non-regular expression filter in addition to the regular expression filter to reduce the number of emails.</p> <p><b>i</b> If you enable Filter by 'Subject', Filter by 'From', or Filter by 'Body', the sensor creates up to three additional channels that monitor the emails that match your filters.</p> <p><b>i</b> If you disable the filters, the additional channels remain, but do not receive data anymore.</p>
Search for	<p><b>This setting is only visible if you choose to filter by the 'Body' field above.</b></p>



Setting	Description
	<p>Enter a string or regular expression that you want to use for Filter by 'Body'.</p> <p><b>i</b> If you select 'Body' contains all strings or 'Body' contains one or more strings above, you can also enter a comma-separated list of strings to search for more than one string. For example, if you select 'Body' contains all strings and enter <a href="#">backup</a> and <a href="#">failed</a>, the sensor counts all items that contain both strings. If you select 'Body' contains one or more strings and enter <a href="#">backup</a> and <a href="#">failed</a>, the sensor counts all items that contain at least one of the strings.</p>
Filter by 'Age'	Select if you want to filter the emails by their age. The filter will be applied to all channels of the sensor.
Maximum Age (Minutes)	<p><a href="#">This setting is only visible if you enable Filter by 'Age' above.</a></p> <p>Enter the maximum age in minutes. The sensor only processes emails that are younger. Enter an integer.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⚙</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>

Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**

Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><span style="font-size: 0.8em;">☁</span> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><span style="font-size: 0.8em;">ⓘ</span> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

- i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Matching Emails	The number of emails that match the defined filters <b>i</b> This channel is only created if you enable Filter by 'Subject', Filter by 'From', or Filter by 'Body'.
Newest Email	The age of the newest email
Newest Matching Email	The age of the newest email that matches the defined filters <b>i</b> This channel is only created if you enable Filter by 'Subject', Filter by 'From', or Filter by 'Body'.
Number of Emails	The number of emails <b>i</b> This channel is the primary channel by default.
Oldest Email	The age of the oldest email
Oldest Matching Email	The age of the oldest email that matches the defined filters <b>i</b> This channel is only created if you enable Filter by 'Subject', Filter by 'From', or Filter by 'Body'.

## More

### ■ KNOWLEDGE BASE

How can I provide feedback about PRTG and contribute to the PRTG development?

- <https://kb.paessler.com/en/topic/91332>

How do I obtain credentials and set permissions for the Microsoft 365 Mailbox sensor?

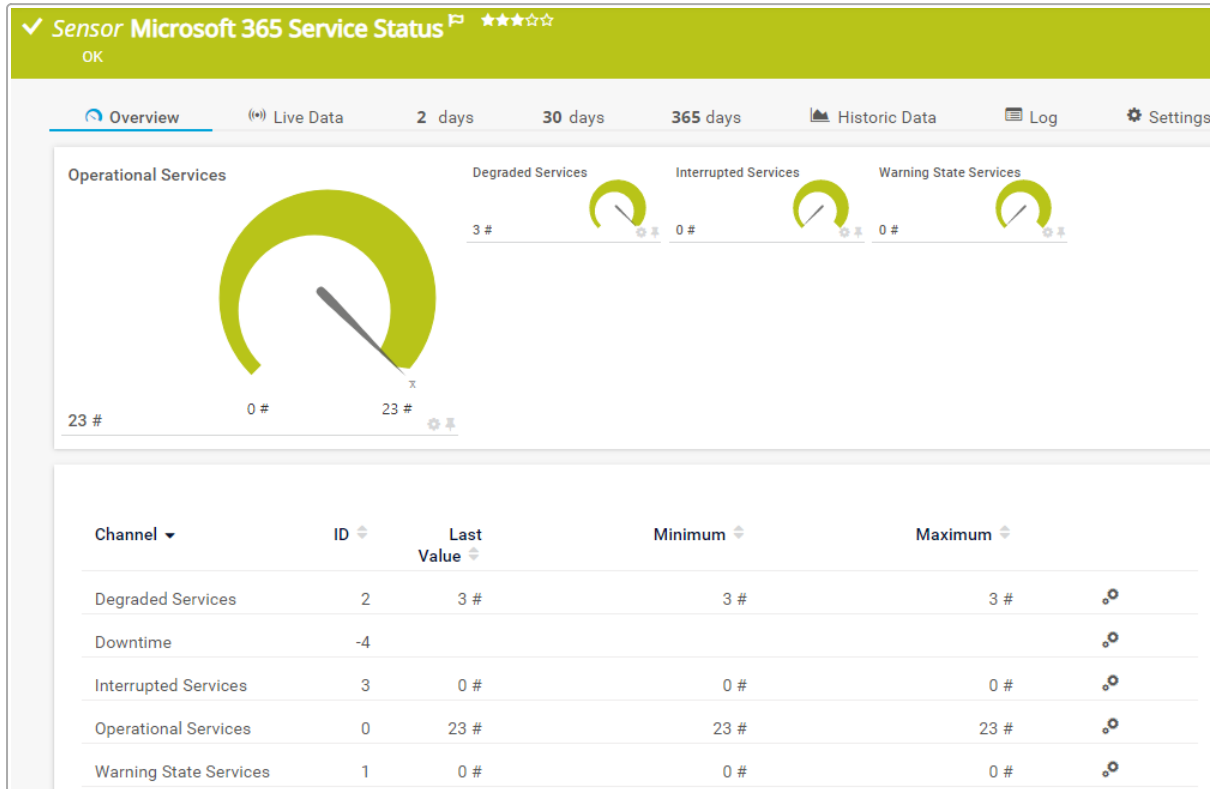
- <https://kb.paessler.com/en/topic/90778>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.88 Microsoft 365 Service Status Sensor

The Microsoft 365 Service Status sensor monitors the overall status of all services of a Microsoft 365 subscription.



Microsoft 365 Service Status Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Microsoft 365 Service Status
- French: Microsoft 365 statut de service
- German: Microsoft 365 Dienststatus
- Japanese: Microsoft 365 サービスステータス
- Portuguese: Status do serviço do Microsoft 365
- Russian: Состояние подписки Microsoft 365
- Simplified Chinese: Microsoft 365 服务状态
- Spanish: Estado del servicio Microsoft 365

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Permission for the APIs	<p>This sensor requires permissions for <a href="#">Microsoft Graph</a>.</p> <ul style="list-style-type: none"> <li>API / Permissions name: Microsoft Graph / ServiceHealth.Read.All</li> </ul> <p>■ For more information, see the Knowledge Base: <a href="#">How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?</a></p>
Credentials	This sensor requires credentials for Microsoft 365.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
Scanning interval	<ul style="list-style-type: none"> <li>The minimum scanning interval of this sensor is <b>1 minute</b>.</li> <li>The recommended scanning interval of this sensor is <b>5 minutes</b>.</li> </ul>
Knowledge Base	Knowledge Base: <a href="#">How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- microsoft365
- microsoft365sensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Microsoft 365 Settings

**Microsoft 365 Specific**

Service ⓘ *Microsoft 365 suite*

Workload ID ⓘ *OSDPPlatform*

Microsoft 365 Settings

Setting	Description
API Request Retry	Enter a number how often the sensor queries the Microsoft Graph if an API query returns no result before the sensor shows the Down status. Enter an integer. The default value is <b>3</b> . The maximum value is <b>10</b> . If you enter <b>0</b> , the sensor does not retry to query the APIs.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ *Downtime*

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking <b>⚙</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>

Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**

Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><span style="font-size: 0.8em;">☁</span> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><span style="font-size: 0.8em;">ⓘ</span> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Degraded Services	The number of degraded services
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Interrupted Services	The number of interrupted services
Operational Services	The number of operation services <b>i</b> This channel is the primary channel by default.
Warning State Services	The number of services in the warning status

## More

### ■ KNOWLEDGE BASE

How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?

- <https://kb.paessler.com/en/topic/88462>

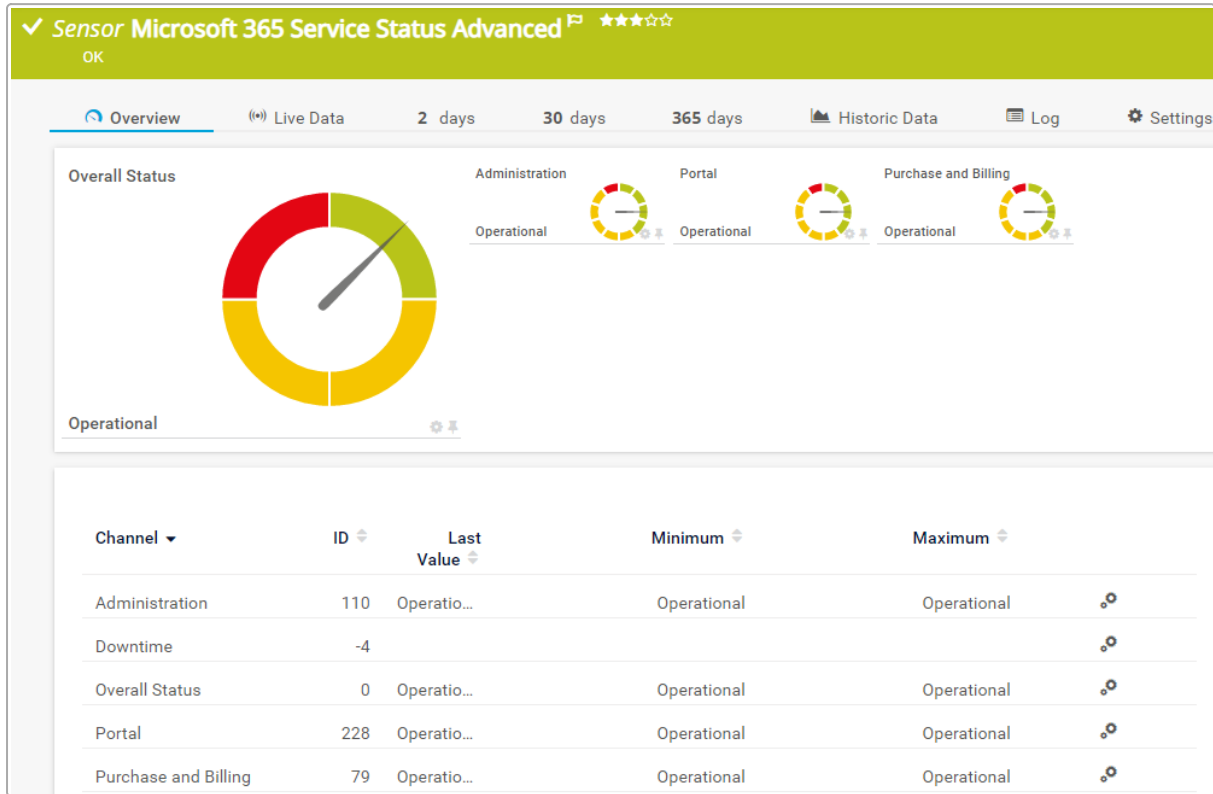
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>



## 7.8.89 Microsoft 365 Service Status Advanced Sensor

The Microsoft 365 Service Status Advanced sensor monitors the detailed status of a service of a Microsoft 365 subscription.



Microsoft 365 Service Status Advanced Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1271]</sup>.

### Sensor in Other Languages

- Dutch: Microsoft 365 Servicestatus Geavanceerd
- French: Microsoft 365 statut de service avancé
- German: Microsoft 365 Dienststatus (Erweitert)
- Japanese: Microsoft 365 サービスステータス詳細
- Portuguese: Status do serviço do Microsoft 365 (Avançado)
- Russian: Подробные данные о состоянии службы Microsoft 365
- Simplified Chinese: Microsoft 365 服务状态高级
- Spanish: Estado del servicio de Microsoft 365 (avanzado)

### Remarks

Consider the following [remarks](#)<sup>[1267]</sup> and requirements for this sensor:

Remark	Description
Permission for the APIs	<p>This sensor requires permissions for <a href="#">Microsoft Graph</a>.</p> <ul style="list-style-type: none"> <li>API / Permissions name: Microsoft Graph / ServiceHealth.Read.All</li> </ul> <p>■ For more information, see the Knowledge Base: <a href="#">How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?</a></p>
Credentials	This sensor requires credentials for Microsoft 365.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Scanning interval	<ul style="list-style-type: none"> <li>The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>The recommended scanning interval of this sensor is <a href="#">20 minutes</a>.</li> </ul>
Knowledge Base	Knowledge Base: <a href="#">How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- microsoft365
- microsoft365sensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Microsoft 365 Specific

**Microsoft 365 Specific**

**Service** ⓘ *Microsoft 365 suite*

**Workload ID** ⓘ *OSDPPlatform*

Microsoft 365 Specific

Setting	Description
Service	The name of the Microsoft 365 service that this sensor monitors.
Workload ID	The Microsoft 365 Workload ID of the service that this sensor monitors.

### Microsoft 365 Settings

**Microsoft 365 Settings**

**API Request Retry** ⓘ 3

Microsoft 365 Settings

Setting	Description
API Request Retry	Enter a number how often the sensor queries the Microsoft Graph if an API query returns no result before the sensor shows the Down status. Enter an integer. The default value is 3. The maximum value is 10. If you enter 0, the sensor does not retry to query the APIs.

### Sensor Display




**Sensor Display**

**Primary Channel** ⓘ Downtime

**Graph Type** ⓘ


Show channels independently (default)  
 Stack channels on top of each other

Sensor Display


Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><a href="#">This setting is only visible if you select</a> Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**


**Result Handling** 
 Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Overall Status	<p>The overall services status</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded, Warning</li> <li>▪ Down status: Interrupted</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
[Service]	<p><b>i</b> Due to changes in the Microsoft 365 Management APIs, this sensor cannot create service channels anymore.</p>

## More

### KNOWLEDGE BASE

How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?

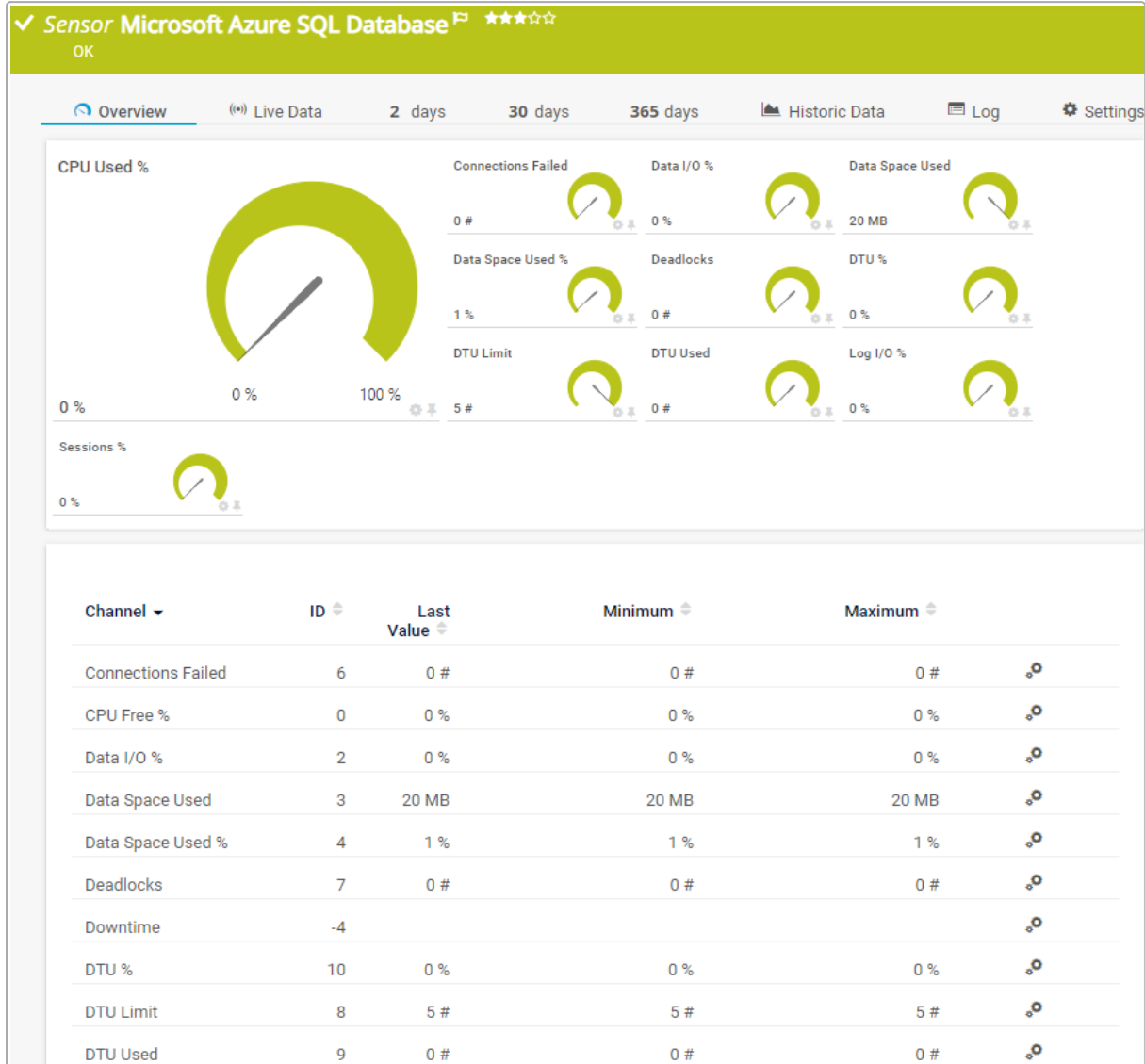
- <https://kb.paessler.com/en/topic/88462>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.90 Microsoft Azure SQL Database Sensor

The Microsoft Azure SQL Database sensor monitors the metrics of an Azure SQL Database (single database or elastic pool) in a Microsoft Azure subscription.



Microsoft Azure SQL Database Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1277</sup>.

### Sensor in Other Languages

- Dutch: Microsoft Azure SQL database
- French: Microsoft Azure base de données SQL
- German: Microsoft Azure SQL-Datenbank
- Japanese: Microsoft Azure SQL Database
- Portuguese: Banco de dados SQL do Microsoft Azure

- Russian: База данных Microsoft Azure SQL
- Simplified Chinese: Microsoft Azure SQL 数据库
- Spanish: Base de datos SQL de Microsoft Azure

## Remarks

Consider the following [remarks<sup>1273</sup>](#) and requirements for this sensor:

Remark	Description
Permissions for the Azure custom role	<p>This sensor requires an Azure custom role with permissions for specific actions.</p> <p><b>i</b> Create an Azure custom role and add permissions for the following actions:</p> <ul style="list-style-type: none"> <li>▪ "Microsoft.Sql/servers/*/read",</li> <li>▪ "Microsoft.Insights/Metrics/providers/Metrics/Read",</li> <li>▪ "Microsoft.Insights/Metrics/Microsoft.Insights/Read",</li> <li>▪ "Microsoft.Insights/Metrics/Read",</li> <li>▪ "Microsoft.Insights/Metricnamespaces/Read",</li> <li>▪ "Microsoft.Insights/MetricDefinitions/providers/Microsoft.Insights/Read",</li> <li>▪ "Microsoft.Insights/Components/providers/Microsoft.Insights/MetricDefinitions/Read"</li> </ul> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">How do I obtain credentials and create custom roles for the Microsoft Azure sensors?</a></p>
Credentials	This sensor requires credentials for Microsoft Azure.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <b>1 minute</b>.</li> <li>▪ The recommended scanning interval of this sensor is <b>5 minutes</b>.</li> </ul>
Knowledge Base	Knowledge Base: <a href="#">How do I obtain credentials and create custom roles for the Microsoft Azure sensors?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- azure
- microsoftazure
- microsoftazuresqldatabase

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Microsoft Azure Specific

### Microsoft Azure Specific

**Azure SQL Database Name** ⓘ *Example*

**Azure SQL Database ID** ⓘ */subscriptions/1111aaaa-22bb-33cc-dd44-eeee5555/examplegroup/example*

**Azure SQL Server Name** ⓘ *example-server*

**Resource Type** ⓘ *Elastic pool*

**Region** ⓘ *West Europe*

**Purchasing Model** ⓘ *DTU*

**Elastic Pool** ⓘ *example-pool*

Microsoft Azure Specific

Setting	Description
Azure SQL Database Name	The name of the Azure SQL Database that this sensor monitors.  ⓘ If you change the database name in your Microsoft Azure subscription, you must add the sensor anew.
Azure SQL Database ID	The ID of the Azure SQL Database that this sensor monitors.
Azure SQL Server Name	The name of the Azure SQL server that hosts the Azure SQL Database.



Setting	Description
Resource Type	The resource type of the Azure SQL Database that this sensor monitors. This can be a single database or an elastic pool in a virtual core (vCore) based purchasing model or a DTU-based purchasing model.  <b>i</b> If you change the resource type in your Microsoft Azure subscription, you must add the sensor anew.
Region	The Azure region of the Azure SQL Database that this sensor monitors.
Purchasing Model	The purchasing model of the Azure SQL Database. This can be vCore based or DTU based.
Elastic Pool	The name of the elastic pool if the resource type of the Azure SQL Database is an elastic pool. If the resource type is not an elastic pool, the field shows <a href="#">n/a</a> .

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.  <b>i</b> You can set a different primary channel later by clicking <b>+</b> below a channel gauge on the sensor's Overview tab.
Graph Type	Define how this sensor shows different channels: <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a> ).

Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**

Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><span style="font-size: 0.8em;">☁</span> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><span style="font-size: 0.8em;">ⓘ</span> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Connections Failed	The number of failed connections
CPU Used %	The CPU usage (%) <b>i</b> This channel is the primary channel by default.
Data I/O %	The data I/O operations (%)
Data Space Used	The data space usage
Data Space Used %	The data space usage (%)
Deadlocks	The number of deadlocks
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
DTU %	The DTUs (%)
DTU Limit	The DTU limit
DTU Used	The used DTU
eDTU Limit	The eDTU limit
eDTU Used	The used eDTU
Log I/O	The log I/O operations
Sessions %	The sessions (%)

## More

### ■ KNOWLEDGE BASE

How do I obtain credentials and create custom roles for the Microsoft Azure sensors?

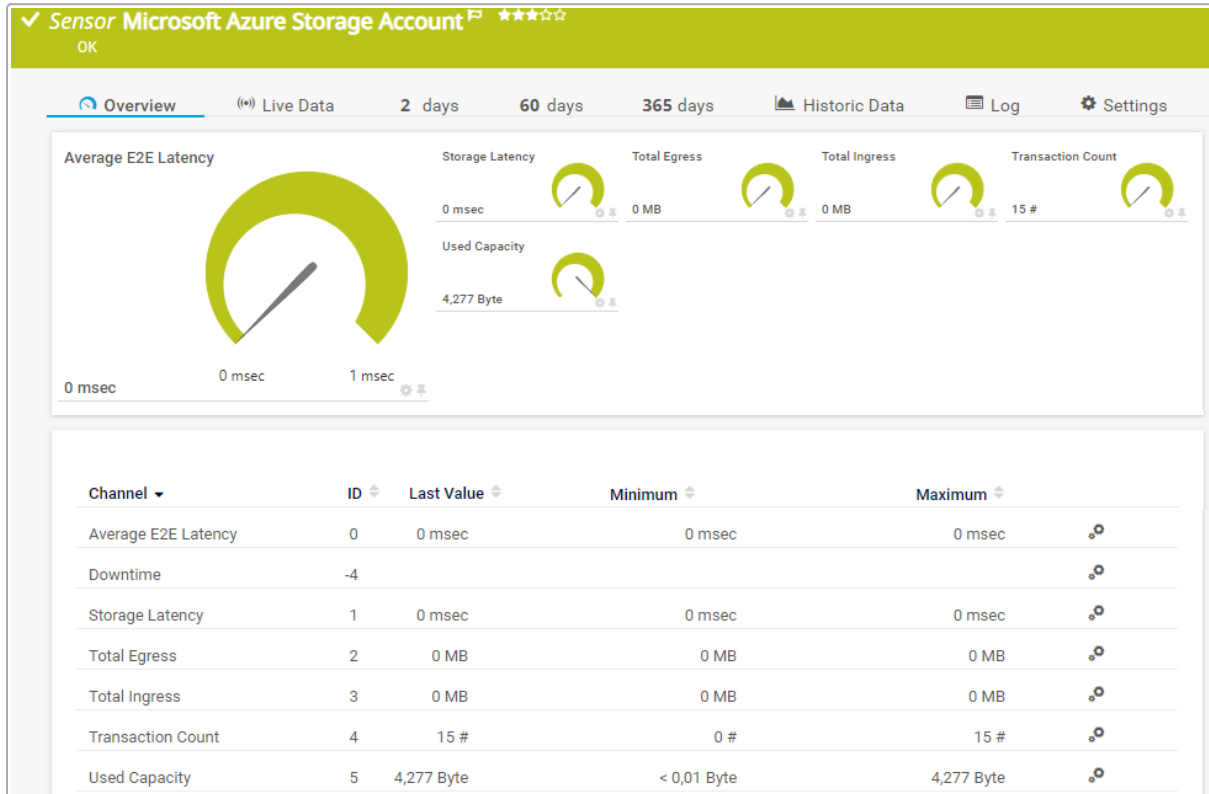
- <https://kb.paessler.com/en/topic/88625>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.91 Microsoft Azure Storage Account Sensor

The Microsoft Azure Storage Account sensor monitors the storage account in a Microsoft Azure subscription.



Microsoft Azure Storage Account Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Microsoft Azure Storage Account
- French: Microsoft Azure compte de stockage
- German: Microsoft Azure Speicherkonto
- Japanese: Microsoft Azure ストレージアカウント
- Portuguese: Conta de armazenamento do Microsoft Azure
- Russian: Учетная запись хранилища данных Microsoft Azure
- Simplified Chinese: Microsoft Azure 存储帐户
- Spanish: Cuenta de almacenamiento de Microsoft Azure

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Permissions for the Azure custom role	<p>This sensor requires an Azure custom role with permissions for specific actions.</p> <p><b>i</b> Create an Azure custom role and add permissions for the following actions:</p> <ul style="list-style-type: none"> <li>▫ "Microsoft.Storage/storageAccounts/read",</li> <li>▫ "Microsoft.Insights/Metrics/Read"</li> </ul> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">How do I obtain credentials and create custom roles for the Microsoft Azure sensors?</a></p>
Credentials	This sensor requires credentials for Microsoft Azure.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <b>1 minute</b>.</li> <li>▪ The recommended scanning interval of this sensor is <b>5 minutes</b>.</li> </ul>
Knowledge Base	Knowledge Base: <a href="#">How do I obtain credentials and create custom roles for the Microsoft Azure sensors?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  X +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- azure
- microsoftazure

- microsoftazurestorageaccount

For more information about basic sensor settings, see section [Sensor Settings](#).

## Microsoft Azure Specific

**Microsoft Azure Specific**

**Storage Account Name**  ⓘ  *Example*

**Storage Account ID**  ⓘ  */subscriptions/1111aaaa-22bb-33cc-dd44-eeee5555/examplegroup/example*

**Account Kind**  ⓘ  *StorageV2*

**Region**  ⓘ  *Germany West Central*

**Resource Group**  ⓘ  *Example Group*

Microsoft Azure Specific

Setting	Description
Storage Account Name	The name of the storage account that this sensor monitors.
Storage Account ID	The ID of the storage account that this sensor monitors.
Account Kind	The kind of the storage account that this sensor monitors.
Region	The Azure region of the storage account that this sensor monitors.
Resource Group	The Microsoft Azure resource group of the storage account that this sensor monitors.

## Sensor Display

**Sensor Display**

**Primary Channel**  ⓘ  *Downtime*


**Graph Type**  ⓘ

Show channels independently (default)

Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.


Setting	Description
	<p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**


**Result Handling** 
  
 Discard result (default)
  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>




## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Average E2E Latency	The average E2E latency  This channel is the primary channel by default.
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Transaction Count	The total number of requests made to the storage service
Storage Latency	The latency of the storage
Total Egress	The total egress
Total Ingress	The total ingress
Used Capacity	The used capacity

## More

### ■ KNOWLEDGE BASE

How do I obtain credentials and create custom roles for the Microsoft Azure sensors?

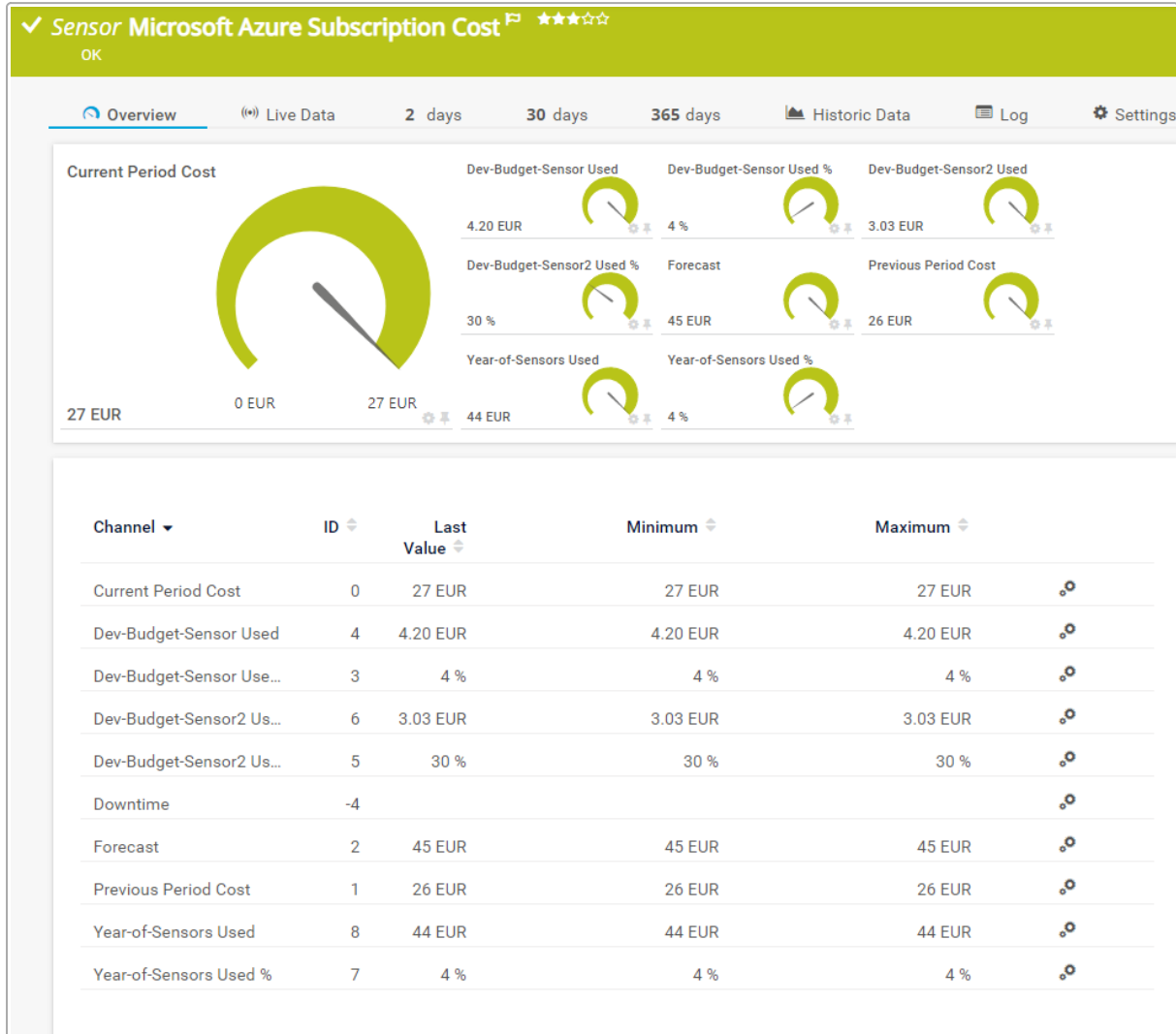
- <https://kb.paessler.com/en/topic/88625>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.92 Microsoft Azure Subscription Cost Sensor

The Microsoft Azure Subscription Cost sensor monitors the cost in a Microsoft Azure subscription.



Microsoft Azure Subscription Cost Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).



### Sensor in Other Languages

- Dutch: Microsoft Azure Abonnementskosten
- French: Microsoft Azure coût de l'abonnement
- German: Microsoft Azure Abonnementkosten
- Japanese: Microsoft Azure サブスクリプションコスト
- Portuguese: Custo da assinatura do Microsoft Azure
- Russian: Затраты подписки Microsoft Azure
- Simplified Chinese: Microsoft Azure 订阅成本

- Spanish: Coste de la suscripción a Microsoft Azure

## Remarks

Consider the following [remarks](#) <sup>1285</sup> and requirements for this sensor:

Remark	Description
Permissions for the Azure custom role	<p>This sensor requires an Azure custom role with permissions for specific actions.</p> <p> Create an Azure custom role and add permissions for the following actions:</p> <ul style="list-style-type: none"> <li>▪ "Microsoft.Consumption/*/read",</li> <li>▪ "Microsoft.Consumption/*/action",</li> <li>▪ "Microsoft.CostManagement/query/read",</li> <li>▪ "Microsoft.Billing/*/read"</li> </ul> <p> For more information, see the Knowledge Base: <a href="#">How do I obtain credentials and create custom roles for the Microsoft Azure sensors?</a></p>
Credentials	This sensor requires credentials for Microsoft Azure.
CSP subscriptions	This sensor does not support cloud solution provider (CSP) subscriptions.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <b>1 minute</b>.</li> <li>▪ The recommended scanning interval of this sensor is <b>4 hours</b>.</li> </ul>
Knowledge Base	Knowledge Base: <a href="#">How do I obtain credentials and create custom roles for the Microsoft Azure sensors?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- azure
- microsoftazure
- microsoftazuresubscriptioncost

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Microsoft Azure Specific

### Microsoft Azure Specific

**Budgets** ⓘ *Disable (default)*

**Cost Forecast** ⓘ *Disable (default)*

**Most Expensive Service** ⓘ  *Disable (default)*  
 *Enable*

Microsoft Azure Specific

Setting	Description
Budgets	If additional channels for the budget usage in your Microsoft Azure subscription are enabled or disabled.
Cost Forecast	If the additional channel with a cost forecast for your Microsoft Azure subscription is enabled or disabled.
Most Expensive Service	Select if you want to show the most expensive service of your Microsoft Azure subscription in the sensor message: <ul style="list-style-type: none"> <li>▪ Disable (default)</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Enable</li> </ul>
Most Expensive Service Category	<p>This setting is only visible if you select <a href="#">Enable</a> above.</p> <p>Select the category for which you want to show the most expensive service in the sensor message:</p> <ul style="list-style-type: none"> <li>▪ Resource group</li> <li>▪ Resource type</li> <li>▪ Resource ID</li> <li>▪ Location</li> <li>▪ Service name</li> </ul>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)

Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select <a href="#">Stack channels on top of each other</a> above.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

## Debug Options


**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Current Period Cost	The current period cost
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Forecast	The cost forecast
[Budget] Used	The used budget <b>i</b> This channel is the primary channel by default.
[Budget] Used %	The used budget (%)
Previous Period Cost	The previous period cost

## More

### ■ KNOWLEDGE BASE

How do I obtain credentials and create custom roles for the Microsoft Azure sensors?

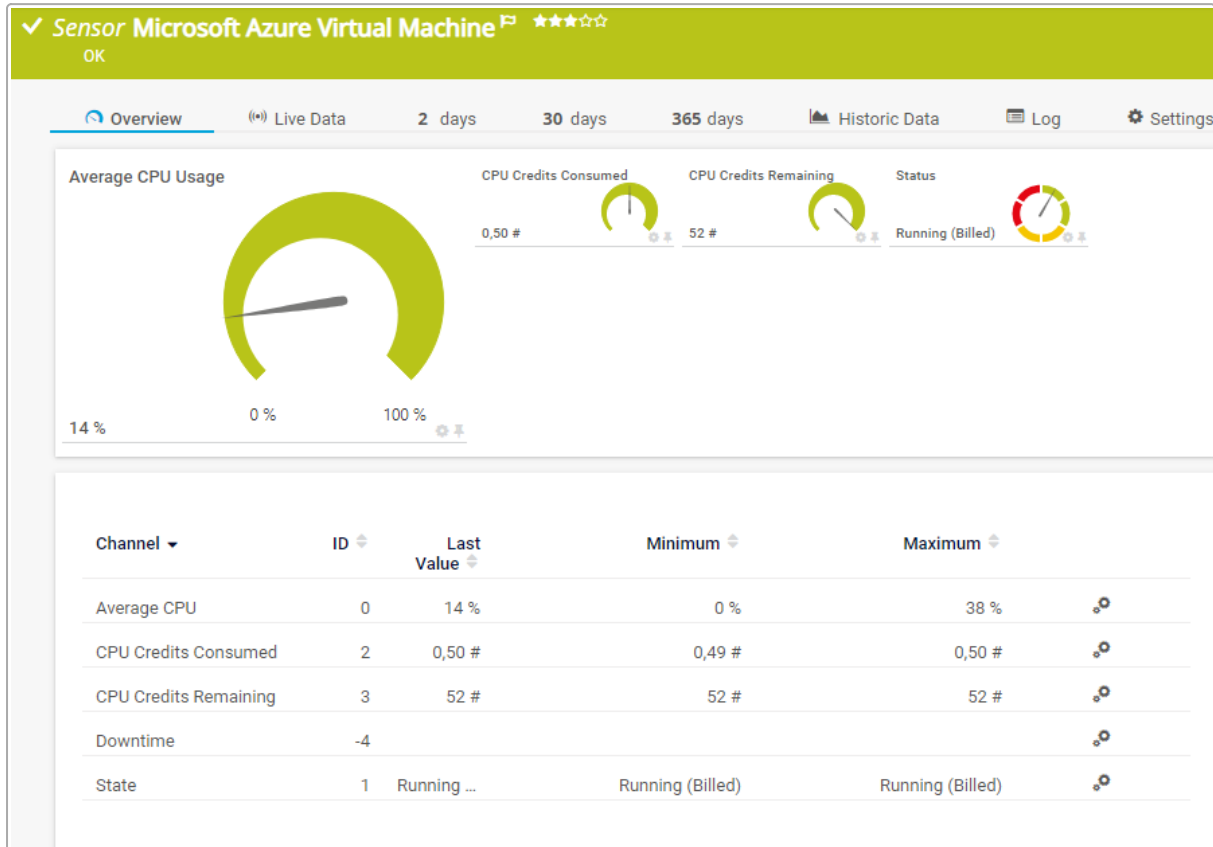
- <https://kb.paessler.com/en/topic/88625>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.93 Microsoft Azure Virtual Machine Sensor

The Microsoft Azure Virtual Machine sensor monitors the status of a virtual machine (VM) in a Microsoft Azure subscription.



Microsoft Azure Virtual Machine Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).



### Sensor in Other Languages

- Dutch: Microsoft Azure Virtuele Machine
- French: Microsoft Azure machine virtuelle
- German: Microsoft Azure Virtueller Computer
- Japanese: Microsoft Azure 仮想マシン
- Portuguese: Máquina virtual do Microsoft Azure
- Russian: Виртуальная машина Microsoft Azure
- Simplified Chinese: Microsoft Azure 虚拟机
- Spanish: Máquina virtual Microsoft Azure

### Remarks

Consider the following [remarks](#) and requirements for this sensor:



Remark	Description
Permissions for the Azure custom role	<p>This sensor requires an Azure custom role with permissions for specific actions.</p> <p> Create an Azure custom role and add permissions for the following actions:</p> <ul style="list-style-type: none"> <li>▫ "Microsoft.Network/publicIPAddresses/read"</li> <li>▫ "Microsoft.Network/virtualNetworks/read"</li> <li>▫ "Microsoft.Network/loadBalancers/read"</li> <li>▫ "Microsoft.Network/networkInterfaces/read"</li> <li>▫ "Microsoft.Compute/virtualMachines/*/read"</li> <li>▫ "Microsoft.Insights/Metrics/providers/Metrics/Read"</li> <li>▫ "Microsoft.Insights/Metrics/Microsoft.Insights/Read"</li> <li>▫ "Microsoft.Insights/Metrics/Read"</li> <li>▫ "Microsoft.Insights/Metricnamespaces/Read"</li> <li>▫ "Microsoft.Insights/MetricDefinitions/providers/Microsoft.Insights/Read"</li> <li>▫ "Microsoft.Insights/Components/providers/Microsoft.Insights/MetricDefinitions/Read"</li> </ul> <p> For more information, see the Knowledge Base: <a href="#">How do I obtain credentials and create custom roles for the Microsoft Azure sensors?</a></p>
Credentials	This sensor requires credentials for Microsoft Azure.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <b>1 minute</b>.</li> <li>▪ The recommended scanning interval of this sensor is <b>5 minutes</b>.</li> </ul>
Knowledge Base	Knowledge Base: <a href="#">How do I obtain credentials and create custom roles for the Microsoft Azure sensors?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- azure
- microsoftazure
- microsoftazurevirtualmachine

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Microsoft Azure Specific

### Microsoft Azure Specific

**Virtual Machine Name** ⓘ *MicrosoftVM*

**Virtual Machine ID** ⓘ 1234

**Operating System** ⓘ *Windows*

**Resource Group** ⓘ *Example Group*

**Region** ⓘ *East US*

Microsoft Azure Specific

Setting	Description
Virtual Machine Name	The name of the VM that this sensor monitors.
Virtual Machine ID	The ID of the VM that this sensor monitors.
Operating System	The operating system of the server on which the VM runs.

Setting	Description
Resource Group	The Microsoft Azure resource group of the VM that this sensor monitors.
Region	The Azure region of the VM that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Average CPU Usage	<p>The average CPU load</p> <p>ⓘ This channel is the primary channel by default.</p>
CPU Credits Consumed	The number of consumed CPU credits

Channel	Description
CPU Credits Remaining	The number of remaining CPU credits
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Status	<p>The VM status</p> <ul style="list-style-type: none"> <li>▪ Up status: Running (Billed), Starting (Not Billed)</li> <li>▪ Warning status: Stopped (Billed), Stopping (Billed)</li> <li>▪ Down status: Deallocated (Not Billed), Deallocating (Not Billed)</li> </ul>

## More

### ■ KNOWLEDGE BASE

How do I obtain credentials and create custom roles for the Microsoft Azure sensors?

- <https://kb.paessler.com/en/topic/88625>

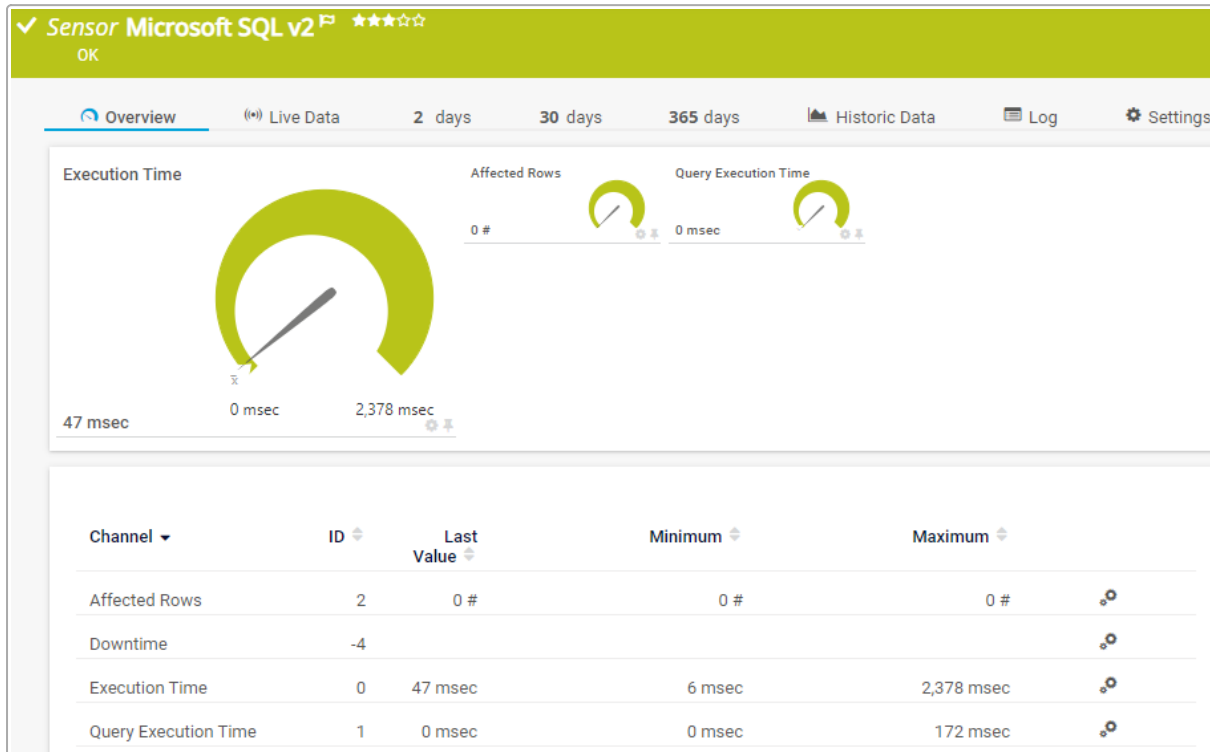
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.94 Microsoft SQL v2 Sensor

The Microsoft SQL v2 sensor monitors a database on a Microsoft SQL server and executes a query.

- i** The sensor can also process the data table and show the values that you define in individual channels.



Microsoft SQL v2 Sensor

- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Microsoft SQL v2
- French: Microsoft SQL v2
- German: Microsoft SQL v2
- Japanese: Microsoft SQL v2
- Portuguese: Microsoft SQL v2
- Russian: Microsoft SQL v2
- Simplified Chinese: Microsoft SQL v2
- Spanish: Microsoft SQL v2

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
SQL query storage	This sensor requires that you store the SQL query in a file on the probe system. In a cluster, copy the file to every cluster node.  ■ For more information, see the Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a>
.NET 4.7.2 or later	This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.  ❗ If the framework is missing, you cannot create this sensor.  ■ For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a>
Microsoft SQL server	This sensor supports Microsoft SQL server as of version 2005.
IPv6	This sensor supports IPv6.
Lookups	This sensor can use <a href="#">lookups</a> <sup>[1303]</sup> . Select Lookup as Channel #x Unit and define the lookup file in Channel #x Lookup.
Credentials	Define the credentials for database management systems in settings that are higher in the object hierarchy.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">How to set up the SQL v2 sensors in PRTG? Is there a guide?</a></li> <li>▪ Knowledge Base: <a href="#">How can I monitor strings from an SQL database and show a sensor status depending on it?</a></li> <li>▪ Knowledge Base: <a href="#">How can I monitor error tables in SQL databases?</a></li> <li>▪ Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a></li> </ul>
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- sqlsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Database Specific

### Database Specific

**Database** ⓘ MyDatabase

---

**SQL Server Instance** ⓘ  No instance name required (default)  
 Use instance name

**Instance Name** ⓘ SQLEXPRESS


---

**Encryption** ⓘ  Use server defaults (default)  
 Enforce encryption but do not validate server certificate  
 Enforce encryption and validate server certificate

Database Specific

Setting	Description
Database	Enter the name of the SQL database to which the sensor connects, for example, <a href="#">MyDatabase</a> . This is a logical entity on the database server where database objects exist.
SQL Server Instance	Define if you want to use an instance name for the database connection: <ul style="list-style-type: none"> <li>▪ No instance name required (default): Use the default instance for the connection.</li> <li>▪ Use instance name: Use a named instance. Specify the Instance Name below.</li> </ul>



Setting	Description
Instance Name	<p>This setting is only visible if you select Use instance name above.</p> <p>Enter the name of the instance that you want to monitor.</p>
Encryption	<p>Define the encryption usage for the database connection:</p> <ul style="list-style-type: none"> <li>Use server defaults (default): Only encrypt the database connection if the database server enforces encryption.</li> <li>Enforce encryption but do not validate server certificate: Make sure that the database connection is encrypted.</li> <li>Enforce encryption and validate server certificate: Force encryption and validate the database server certificate. This approach provides the highest level of security and can help prevent man-in-the-middle attacks, for example. <ul style="list-style-type: none"> <li> The sensor only validates the certificate if the database server enforces encryption.</li> </ul> </li> </ul>

## Data

**Data**

SQL Query File ⓘ *Demo Serveruptime.sql*

Input Parameter Handling ⓘ  Do not use input parameter (default)  
 Use input parameter






Transaction Handling ⓘ  Do not use transaction (default)  
 Use transaction and always roll back  
 Use transaction and commit on success

Data Processing ⓘ *Only execute query (default)*

Result Handling ⓘ  Discard result (default)  
 Store result

Data





Setting	Description
SQL Query File	<p>Select the SQL query file that includes a valid SQL statement that the sensor executes on the server with every scanning interval. The list contains SQL scripts from the \Custom Sensors\sql subfolder of the <a href="#">PRTG program directory</a> on the probe system. Store your script there. If you use the script on a cluster probe, you must store the script on all cluster nodes.</p>

Setting	Description
	<p>A correct expression in the file could be: <a href="#">SELECT AVG(UnitPrice) FROM Products</a>. If you want to use transactions, separate the individual steps with semicolons ";".</p> <ul style="list-style-type: none"> <li> Note that with each request, PRTG transfers the full result set, so use filters and limits in your query.</li> <li> The demo script Demo Serveruptime.sql is available by default. You can use it to monitor the uptime of the target server.</li> <li> See also the Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a></li> <li> You cannot change this value after sensor creation.</li> </ul>
Input Parameter Handling	<p>Define if you want to pass a parameter to the SQL query file:</p> <ul style="list-style-type: none"> <li>▪ Do not use input parameter (default): Execute the SQL query file without using variables.</li> <li>▪ Use input parameter: Execute an SQL query file that contains a variable. Provide the parameter that you want to use in the query below.</li> </ul>
Input Parameter	<p><a href="#">This setting is only visible if you select Use input parameter above.</a></p> <p>Enter the parameter that you want to pass to the SQL query file. This parameter replaces the variables <a href="#">@prtg</a>, <a href="#">:prtg</a>, or <a href="#">?</a> in the SQL query, considering the general rules for SQL variables.</p> <p>You can also use PRTG placeholders for custom sensors (command-line parameters) as input parameters, for example, <a href="#">%sensorid</a> or <a href="#">%deviceid</a>. For more information, see section <a href="#">Custom Sensors</a>.</p> <ul style="list-style-type: none"> <li> Provide strings as they are and do not surround them with quotation marks. PRTG automatically and correctly inserts string parameters into the query.</li> </ul>
Transaction Handling	<p>Define if you want to use transactions and if they affect the database content:</p> <ul style="list-style-type: none"> <li>▪ Do not use transaction (default): Do not execute transactions.</li> <li>▪ Use transaction and always roll back: The query does not change data in the database. In the SQL query file, separate the single steps of the transaction with semicolons.</li> <li>▪ Use transaction and commit on success: The query changes data in the database. The changes only apply if all execution steps succeed without any errors. In the SQL query file, separate the single steps of the transaction with semicolons.</li> </ul>
Data Processing	<p>Define whether the sensor processes data from the database:</p>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Only execute query (default): Only show information about the number of affected rows and the execution time of the query. Affected rows are rows that were changed by the query (for example, created, deleted, or edited).</li> <li>▪ Count table rows: Execute a <b>SELECT</b> statement and monitor how many rows of the data table this statement returns.</li> <li>▪ Process data table: Read and analyze the data table. If you select this option, the sensor counts rows with <b>SELECT</b> statements as well.</li> </ul> <p><b>i</b> You cannot change this value after sensor creation.</p>
DBNull Handling	<p><b>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</b></p> <p>Define the sensor behavior if the query returns <b>DBNull</b>:</p> <ul style="list-style-type: none"> <li>▪ Error: Show the Down status if the query returns <b>DBNull</b>.</li> <li>▪ Number 0: Recognize the result <b>DBNull</b> as a valid value and interpret it as the number <b>0</b>.</li> </ul>
Select Channel Value by	<p><b>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</b></p> <p>Define how to select the desired cell in the database table:</p> <ul style="list-style-type: none"> <li>▪ Column number: Determine the channel value by using the value in row 0 of the column whose number you specify in Channel #x Column Number.</li> <li>▪ Column name: Determine the channel value by using the value in row 0 of the column whose name you specify in Channel #x Column Name.</li> <li>▪ Row number: Determine the channel value by using the value in column 0 of the row whose number you specify in Channel #x Row Number.</li> <li>▪ Key value pair: Determine the channel value by searching in column 0 for the key you specify in Channel #x Key and by returning the value in column 1 of the same row where the key value was found.</li> </ul> <p><b>i</b> Defining how the desired cell in the database table is selected is necessary to configure the cells that are used in the channels.</p> <p><b>i</b> The option you select here also defines the method of how to optionally determine a value for the sensor message. For more information, see setting Use Data Table Value in Message.</p> <p><b>■</b> For an example for channel value selection, see section <a href="#">Monitoring Databases</a>.</p>

Setting	Description
Channel #2 - #10	<p>This setting is only visible if you select <a href="#">Process data table</a> <a href="#">above</a>.</p> <p>You can define up to 10 channels. You must define at least one channel, so you see all available settings for <a href="#">Channel #1</a>. Specify how to handle all other possible channels:</p> <ul style="list-style-type: none"> <li>▪ Disable: Do not create this channel.</li> <li>▪ Enable: Create this channel.</li> </ul> <p><b>i</b> It is not possible to enable or disable channels after sensor creation.</p>
Channel #x Name	<p>This setting is only visible if you select <a href="#">Process data table</a> <a href="#">for the setting</a> <a href="#">Data Processing during sensor creation</a>.</p> <p>Enter a name for the channel. Enter a string. The sensor dynamically generates channels with this name as identifier.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({}), for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Channel #x Column Number	<p>This setting is only visible if you select <a href="#">Process data table</a> <a href="#">for the setting</a> <a href="#">Data Processing during sensor creation</a> <a href="#">and if you select</a> <a href="#">Column number for the setting</a> <a href="#">Select Channel Value by</a>.</p> <p>Provide the number of the column to use to determine the channel value in row 0. Enter an integer.</p>
Channel #x Column Name	<p>This setting is only visible if you select <a href="#">Process data table</a> <a href="#">for the setting</a> <a href="#">Data Processing during sensor creation</a> <a href="#">and if you select</a> <a href="#">Column name for the setting</a> <a href="#">Select Channel Value by</a>.</p> <p>Provide the name of the column to use to determine the channel value in row 0. Enter an integer.</p>
Channel #x Row Number	<p>This setting is only visible if you select <a href="#">Process data table</a> <a href="#">for the setting</a> <a href="#">Data Processing during sensor creation</a> <a href="#">and if you select</a> <a href="#">Row number for the setting</a> <a href="#">Select Channel Value by</a>.</p> <p>Provide the number of the column to use to determine the channel value in row 0. Enter an integer.</p>
Channel #x Key	<p>This setting is only visible if you select <a href="#">Process data table</a> <a href="#">for the setting</a> <a href="#">Data Processing during sensor creation</a> <a href="#">and if you select</a> <a href="#">Key value pair for the setting</a> <a href="#">Select Channel Value by</a>.</p>

Setting	Description
	<p>Provide the key to search for in column 0 of the data table. The value in column 1 of the same row where the key value was found to use to determine the channel value. Enter a string.</p>
<p>Channel #x Mode</p>	<p><b>This setting is only visible if you select Process data table above.</b></p> <p>Define how to display the determined value in the channel:</p> <ul style="list-style-type: none"> <li>▪ Absolute (default): Show the value as the sensor retrieves it from the data table.</li> <li>▪ Difference: The sensor calculates and shows the difference between the last and the current value returned from the data table. <ul style="list-style-type: none"> <li>ⓘ This mode is not compatible with the unit Lookup.</li> <li>ⓘ This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative and decreasing values.</li> </ul> </li> <li>▪ Absolute (recommended): Show the value as the sensor retrieves it from the data table.</li> <li>▪ Difference: The sensor calculates and shows the difference between the last and the current value returned from the data table. <ul style="list-style-type: none"> <li>ⓘ This mode is not compatible with the unit Lookup.</li> <li>ⓘ This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative and decreasing values.</li> </ul> </li> </ul>
<p>Channel #x Unit</p>	<p><b>This setting is only visible if you select Process data table above.</b></p> <p>Define the unit of the channel value:</p> <ul style="list-style-type: none"> <li>▪ BytesBandwidth</li> <li>▪ BytesMemory</li> <li>▪ BytesDisk</li> <li>▪ Temperature</li> <li>▪ Percent</li> <li>▪ TimeResponse</li> <li>▪ TimeSeconds</li> <li>▪ TimeHours</li> <li>▪ Count</li> <li>▪ CPU</li> <li>▪ BytesFile</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ SpeedDisk</li> <li>▪ SpeedNet</li> <li>▪ Custom</li> <li>▪ Lookup</li> </ul> <p> For more information about the available units, see section <a href="#">Custom Sensors</a>.</p> <p> To use <a href="#">lookups</a> with this channel, select Lookup and define the lookup file in Channel #x Lookup. Do not use Custom if you use lookups with this sensor.</p> <p> It is not possible to use the unit Lookup in combination with the Difference mode. You are not able to create the sensor in this case.</p>
Channel #x Custom Unit	<p>This setting is only visible if you select <a href="#">Custom</a> above.</p> <p>Define a unit for the channel value. Enter a string.</p>
Channel #x Lookup	<p>This setting is only visible if you select <a href="#">Lookup</a> above.</p> <p>Select a <a href="#">lookup</a> file that you want to use with this channel.</p>
Use Data Table Value in Message	<p>This setting is only visible if you select <a href="#">Process data table</a> for the setting <a href="#">Data Processing during sensor creation</a>.</p> <p>Define if the sensor message shows a value from the data table:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Disable</a>: Do not use a custom sensor message.</li> <li>▪ <a href="#">Enable</a>: Define a custom sensor message with a defined value of the data table. Define the value selection below.</li> </ul> <p> The method of how to determine a value for the sensor message is defined in the setting <a href="#">Select Channel Value by</a> above.</p>
Message Column Number	<p>This setting is only visible if you select <a href="#">Process data table</a> for the setting <a href="#">Data Processing during sensor creation</a>, if you select <a href="#">Column name for the setting</a> <a href="#">Select Channel Value by</a>, and if you select <a href="#">Enable</a> above.</p> <p>Enter the number of a column. The sensor message shows the value in row 0 of this column. Enter an integer.</p>
Message Column Name	<p>This setting is only visible if you select <a href="#">Process data table</a> for the setting <a href="#">Data Processing during sensor creation</a>, if you select <a href="#">Column name for the setting</a> <a href="#">Select Channel Value by</a>, and if you select <a href="#">Enable</a> above.</p>

Setting	Description
	<p>Enter the name of a column. The sensor message shows the value in row 0 of this column. Enter a string.</p> <p><b>i</b> Columns start with index 0.</p>
Message Row Number	<p><a href="#">This setting is only visible if you select Process data table for the setting Data Processing during sensor creation, if you select Row number for the setting Select Channel Value by, and if you select Enable above.</a></p> <p>Enter the name of a column. The sensor message shows the value in row 0 of this column. Enter the number of a row. The sensor message shows the value in column 0 of this row. Enter an integer.</p> <p><b>i</b> Rows start with index 0.</p>
Message Key	<p><a href="#">This setting is only visible if you select Process data table for the setting Data Processing during sensor creation, if you select Key value pair for the setting Select Channel Value by, and if you select Enable above.</a></p> <p>Enter a key to search for in column 0 of the data table. The sensor message shows the value in column 1 of the row where the key was found. Enter a string.</p>
Message	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Define the sensor message. Enter a string. Use the placeholder <code>{0}</code> at the position where you want to display the value.</p> <p>Example: <a href="#">The message is {0}</a></p> <p><b>i</b> PRTG does not support the number sign (#) in sensor messages. If a message contains a number sign, PRTG clips the message at this point.</p>
If Message Changes	<p><a href="#">This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</a></p> <p>Define what the sensor does when its message changes:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> <li>▪ Trigger 'change' notification: Send an internal message that indicates a change.</li> </ul> <p><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⚙</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>



## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Affected Rows	The number of rows that were addressed by the query (including <a href="#">SELECT</a> statements if you process data tables)
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Execution Time	The execution time of the entire request (including connection buildup, query execution, transaction handling, disconnection)  <b>i</b> This channel is the primary channel by default.
Query Execution Time	The execution time of the specified query

## SQL Variables

You can use the following variables in the SQL query file to be replaced by an input parameter. This is useful if you have various SQL sensors with queries that differ in only one parameter.

- Microsoft SQL, MySQL, PostgreSQL: [@prtg](#)
- Oracle SQL: [:prtg](#)
- ADO SQL: [?](#) (question mark)

**i** [@prtg](#), [:prtg](#), and [?](#) are common SQL query parameters and they are used in a parameterized SQL query. This means that the query and the parameter are forwarded without any changes to the database. This leads to some restrictions on the database side. For example, you cannot use variables as placeholders for table names or as lists in IN operators.

Examples for variables usage:

```
SELECT * FROM Table WHERE name = @prtg
SELECT @prtg FROM Table
```

## More

### ■ KNOWLEDGE BASE

How to set up the SQL v2 sensors in PRTG? Is there a guide?

- <https://kb.paessler.com/en/topic/70618>

How can I monitor strings from an SQL database and show a sensor status depending on it?

- <https://kb.paessler.com/en/topic/63259>

How can I monitor error tables in SQL databases?

- <https://kb.paessler.com/en/topic/70774>

Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

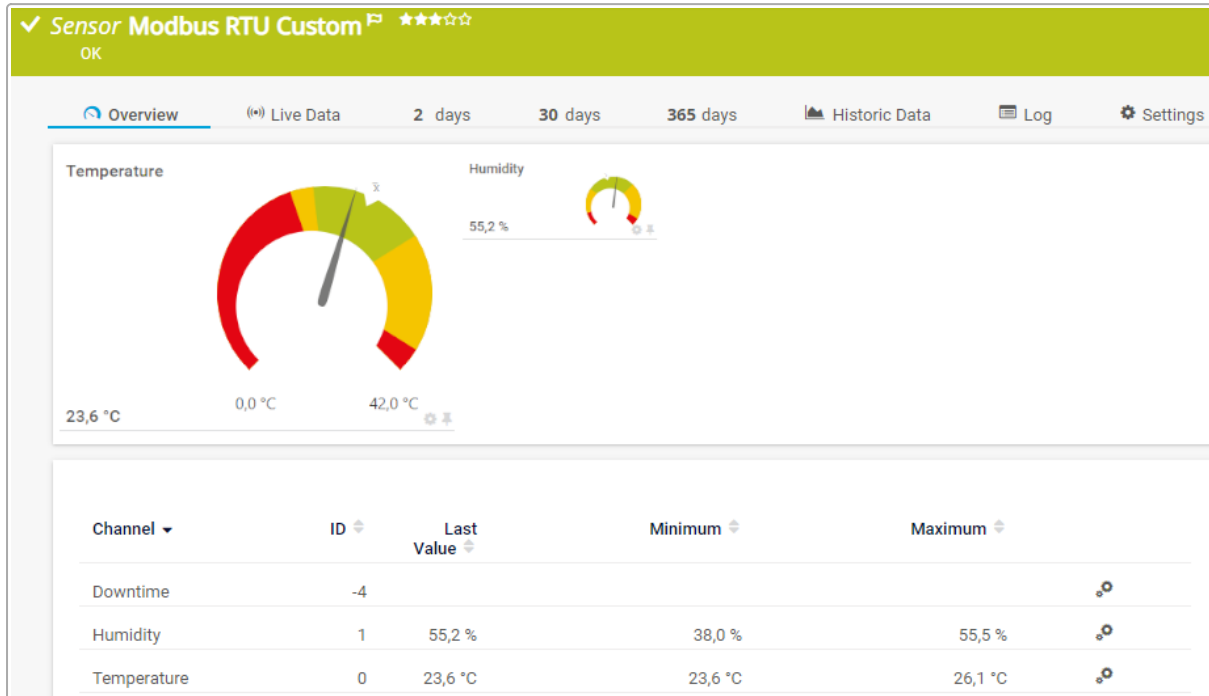
- <https://kb.paessler.com/en/topic/61108>

How do I monitor the size of a Microsoft SQL Server database?

- <https://kb.paessler.com/en/topic/18183>

## 7.8.95 Modbus RTU Custom Sensor

The Modbus RTU Custom sensor connects to a Modbus Remote Terminal Unit (RTU) server and monitors up to ten returned numeric values.



Modbus RTU Custom Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1316]</sup>.

### Sensor in Other Languages




- Dutch: Modbus RTU Aangepast
- French: Modbus RTU personnalisé
- German: Modbus RTU (Benutzerdefiniert)
- Japanese: Modbus RTU カスタム
- Portuguese: Modbus RTU customizado
- Russian: Пользовательский Modbus RTU
- Simplified Chinese: Modbus RTU 自定义
- Spanish: Modbus RTU (personalizado)

### Remarks

Consider the following [remarks](#)<sup>[1309]</sup> and requirements for this sensor:

Remark	Description
Sensor creation	You can create this sensor only on a <a href="#">probe device</a> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Serial port	This sensor always uses the serial port of the probe device.
Knowledge Base	Knowledge Base: <a href="#">How can I apply Zoom Service Status sensors and Modbus sensors via device templates?</a>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Add Sensor

Setting	Description
Channel #1 - #10 Name	Enter a name for the channel.  You can change this value later in the <a href="#">channel settings</a> of this sensor.
Channel #1 - #10 Unit	Enter a unit for the channel.  You can change this value later in the <a href="#">channel settings</a> of this sensor.
Channel #2 - #10	You can define up to 10 channels. You must define at least one channel, so you see all available settings for <a href="#">Channel #1</a> . Specify how to handle all other possible channels: <ul style="list-style-type: none"> <li>▪ Disable (default): Do not create this channel.</li> <li>▪ Enable: Create this channel. Specify at least the name, type, and register number for this channel below.</li> </ul>  It is not possible to enable or disable channels after sensor creation.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- modbus

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Modbus RTU Specific

### Modbus RTU Specific

**Device COM Port** ⓘ COM1

---

**Baud Rate** ⓘ 9600

---

**Parity** ⓘ None (default)

---

**Data Bits** ⓘ 8 (default)

---

**Stop Bits** ⓘ 1 (default)

---

**Retry Attempts** ⓘ 3

---

**Receive Timeout (msec)** ⓘ 500

---

**Unit ID** ⓘ 1

---

**Byte Order** ⓘ  Big-endian (AB CD)  
 Little-endian (DC BA)  
 Big-endian byte swap (BA DC)  
 Little-endian byte swap (CD AB)

Modbus RTU Specific

Setting	Description
Device COM Port	<p>Enter the component object model (COM) port of the serial port device.</p> <p><b>i</b> On Windows systems, the COM port of the device looks like this, for example: <a href="#">COM3</a>.</p>
Baud Rate	<p>Enter the speed of the serial connection in baud. The default baud rate is <a href="#">9600</a>.</p>
Parity	<p>Select the parity of the serial connection:</p> <ul style="list-style-type: none"> <li>▪ None (default)</li> <li>▪ Even</li> <li>▪ Odd</li> </ul>
Data Bits	<p>Select the number of the data bits of the serial connection:</p> <ul style="list-style-type: none"> <li>▪ 8 (default)</li> <li>▪ 7</li> <li>▪ 6</li> <li>▪ 5</li> </ul>
Stop Bits	<p>Select the number of stop bits of the serial connection:</p> <ul style="list-style-type: none"> <li>▪ 1 (default)</li> <li>▪ 2</li> </ul>
Retry Attempts	<p>Enter the number of retries until a timeout occurs. If you enter <b>0</b>, the sensor does not retry the communication attempt. The default value is <b>3</b>. Enter an integer.</p>
Receive Timeout (msec)	<p>Enter a receive timeout in milliseconds (msec). If the reply from the device takes longer than this value, the request is aborted and triggers an error message. The default value is <a href="#">500 msec (0.5 seconds)</a>.</p>
Unit ID	<p>Enter the Modbus unit ID that you want to monitor.</p> <p><b>i</b> In a standard Modbus network, there are up to <a href="#">247</a> unit IDs, each with a unique assigned identifier from <a href="#">1</a> to <a href="#">247</a>.</p>
Byte Order	<p>Select the sequence of the transmitted information:</p> <ul style="list-style-type: none"> <li>▪ Big-endian (AB CD)</li> <li>▪ Little-endian (DC BA)</li> <li>▪ Big-endian byte swap (BA DC)</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Little-endian byte swap (CD AB)</li> </ul>

### Modbus Channel Specific

#### Modbus Channel Specific

**Channel #1 Register Type** ⓘ *Holding register bit*

**Channel #1 Register Number** ⓘ 0

**Channel #1 Register Width** ⓘ

16 bits wide (default)
   
 32 bits wide
   
 64 bits wide

**Channel #1 Bit Index** ⓘ 0

Modbus Channel Specific

Setting	Description
Channel #1 - #10 Register Type	<p>Select the type of the register:</p> <ul style="list-style-type: none"> <li>Coil (default): Coil numbers start with 0 and range from 00001 to 09999.</li> <li>Discrete input: Discrete input numbers start with 1 and range from 10001 to 19999.</li> <li>Input register: Input register numbers start with 3 and range from 30001 to 39999.</li> <li>Holding register: Holding register numbers start with 4 and range from 40001 to 49999.</li> <li>Input register bit: Select Input register bit to monitor a specific bit of the received value. Input register numbers start with 3 and range from 30001 to 39999.</li> <li>Holding register bit: Select Holding register bit to monitor a specific bit of the received value. Holding register numbers start with 4 and range from 40001 to 49999.</li> </ul> <p> ⓘ After sensor creation, this setting shows the register type of the channel value.</p>
Channel #1 - #10 Register Number	Enter the register number from which you want to retrieve information.

Setting	Description
	<p><b>i</b> The register number must be a number that contains one to five digits. The sensor supports numbers between 0 and 65534.</p> <p><b>i</b> Depending on your Modbus device, you might need to remove the register type prefix. For example, you need to enter 60 for the input register 30060 or 316 for the holding register 40316.</p>
<p>Channel #1 - #10 Value Type</p>	<p>This setting is only visible if you select Input register or Holding register above.</p> <p>Select the value type that the channel displays:</p> <ul style="list-style-type: none"> <li>▪ Absolute (default): Integer64 values with or without an operational sign, such as 10 or 120 or -12 or 120.</li> <li>▪ Delta (counter): The sensor calculates the difference between the last value and the current value. The sensor additionally divides the delta value by a time period to indicate a speed value. The sensor ignores this setting if you select Double or Float as Channel #x Data Type.</li> </ul> <p><b>i</b> This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative values and decreasing values.</p>
<p>Channel #1 - #10 Data Type</p>	<p>This setting is only visible if you select Input register or Holding register above.</p> <p>Select the data type of the register:</p> <ul style="list-style-type: none"> <li>▪ 16-bit integer (default)</li> <li>▪ Unsigned 16-bit integer</li> <li>▪ 32-bit integer</li> <li>▪ Unsigned 32-bit integer</li> <li>▪ 64-bit integer</li> <li>▪ Float</li> <li>▪ Double</li> </ul> <p><b>i</b> You cannot change this value after sensor creation.</p>
<p>Channel #1 - #10 Register Width</p>	<p>This setting is only visible if you select Input register or Holding register above.</p> <p>Select the width of the value in the register:</p> <ul style="list-style-type: none"> <li>▪ 16 bits wide (default)</li> <li>▪ 32 bits wide</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>64 bits wide</li> </ul>
Channel #1 - #10 Bit Index	<p>This setting is only visible if you select <a href="#">Input register</a> or <a href="#">Holding register</a> above.</p> <p>Enter the index of the bit that you want to monitor.</p> <p><b>i</b> Enter a value between 0 and 15, 31, or 63, depending on the Channel #1 - #10 Register Width. 0 monitors the least significant bit. To monitor the most significant bit, enter 15 for a 16-bit register, 31 for a 32-bit register, or 63 for a 64-bit register.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i** 
 Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select <a href="#">Stack channels on top of each other</a> above.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

## Debug Options


**Debug Options**

**Result Handling** ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	The returned numeric values in up to ten channels

## More

### ■ KNOWLEDGE BASE

How can I apply Zoom Service Status sensors and Modbus sensors via device templates?

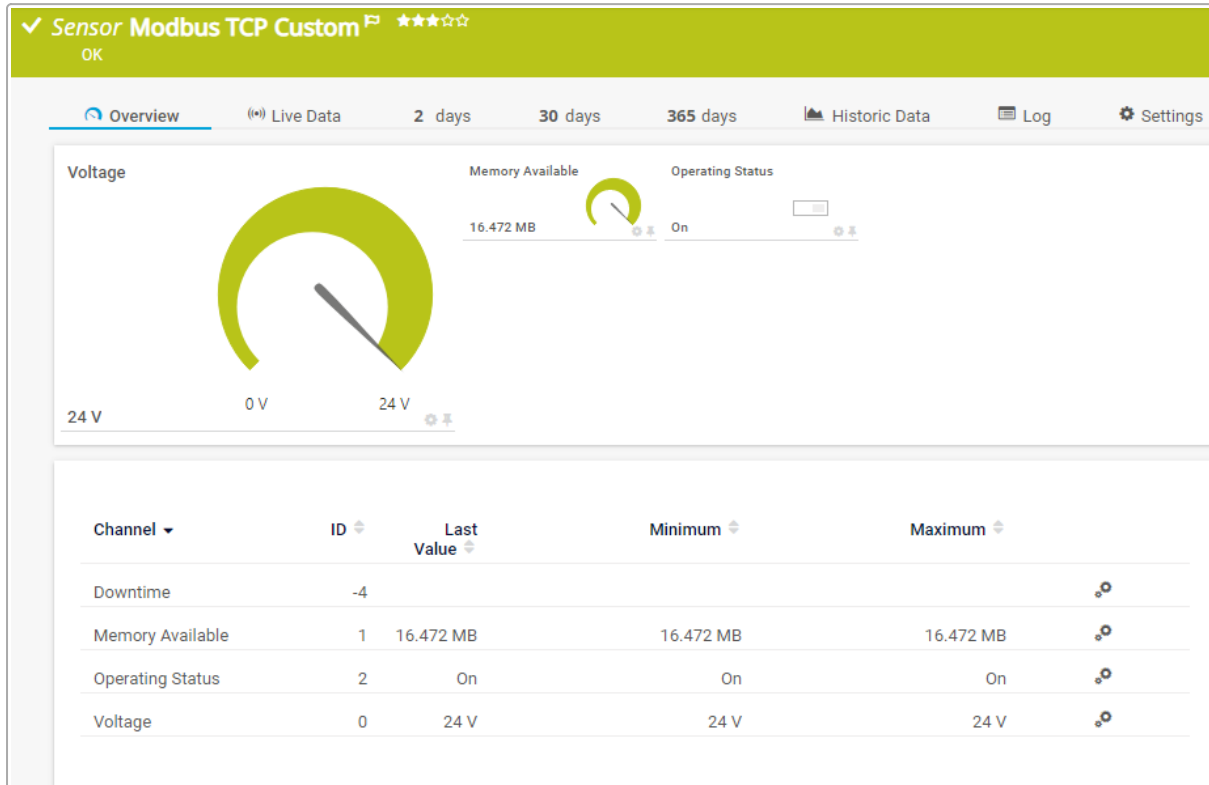
- <https://kb.paessler.com/en/topic/89684>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.96 Modbus TCP Custom Sensor

The Modbus TCP Custom sensor connects to a Modbus Transmission Control Protocol (TCP) server and monitors up to ten returned numeric values.



Modbus TCP Custom Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1323</sup>.

### Sensor in Other Languages

- Dutch: Modbus TCP Aangepast
- French: Modbus TCP personnalisé
- German: Modbus TCP (Benutzerdefiniert)
- Japanese: Modbus TCP カスタム
- Portuguese: Modbus TCP customizado
- Russian: Пользовательский Modbus TCP
- Simplified Chinese: Modbus TCP 自定义
- Spanish: Modbus TCP (personalizado)

### Remarks

Consider the following [remarks](#)<sup>1318</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Multi-platform probe	You can add this sensor to a multi-platform probe.
Knowledge Base	Knowledge Base: <a href="#">How can I apply Zoom Service Status sensors and Modbus sensors via device templates?</a>

### Add Sensor

Setting	Description
Channel #1 - #10 Name	<p>Enter a name for the channel.</p> <p><b>i</b> You can change this value later in the <a href="#">channel settings</a> of this sensor.</p>
Channel #1 - #10 Unit	<p>Enter a unit for the channel.</p> <p><b>i</b> You can change this value later in the <a href="#">channel settings</a> of this sensor.</p>
Channel #2 - #10	<p>You can define up to 10 channels. You must define at least one channel, so you see all available settings for <a href="#">Channel #1</a>. Specify how to handle all other possible channels:</p> <ul style="list-style-type: none"> <li>▪ <b>Disable (default):</b> Do not create this channel.</li> <li>▪ <b>Enable:</b> Create this channel. Specify at least the name, type, and register number for this channel below.</li> </ul> <p><b>i</b> It is not possible to enable or disable channels after sensor creation.</p>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- modbus

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Modbus TCP Specific

### Modbus TCP Specific

**Port** ⓘ

**Receive Timeout (msec)** ⓘ

**Unit ID** ⓘ

**Byte Order** ⓘ

Big-endian (AB CD)

Little-endian (DC BA)

Big-endian byte swap (BA DC)

Little-endian byte swap (CD AB)

Modbus TCP Specific

Setting	Description
Port	Enter the port for the connection to the Modbus TCP server. The default port is <a href="#">502</a> .
Receive Timeout (msec)	Enter a receive timeout in milliseconds (msec). If the reply from the device takes longer than this value, the request is aborted and triggers an error message. The default value is <a href="#">500 msec</a> ( <a href="#">0.5 seconds</a> ).
Unit ID	Enter the Modbus unit ID that you want to monitor.

Setting	Description
	<p><b>i</b> In a standard Modbus network, there are up to 255 unit IDs, each with a unique assigned identifier from 1 to 255.</p>
Byte Order	<p>Select the sequence of the transmitted information:</p> <ul style="list-style-type: none"> <li>▪ Big-endian (AB CD)</li> <li>▪ Little-endian (DC BA)</li> <li>▪ Big-endian byte swap (BA DC)</li> <li>▪ Little-endian byte swap (CD AB)</li> </ul>

### Modbus Channel Specific

#### Modbus Channel Specific

Channel #1 Register Type ⓘ *Holding register bit*

Channel #1 Register Number ⓘ 0

---

Channel #1 Register Width ⓘ

- 16 bits wide (default)
- 32 bits wide
- 64 bits wide

Channel #1 Bit Index ⓘ 0

Modbus Channel Specific

Setting	Description
Channel #1 - #10 Register Type	<p>Select the type of the register:</p> <ul style="list-style-type: none"> <li>▪ Coil (default): Coil numbers start with 0 and range from 00001 to 09999.</li> <li>▪ Discrete input: Discrete input numbers start with 1 and range from 10001 to 19999.</li> <li>▪ Input register: Input register numbers start with 3 and range from 30001 to 39999.</li> <li>▪ Holding register: Holding register numbers start with 4 and range from 40001 to 49999.</li> <li>▪ Input register bit: Select Input register bit to monitor a specific bit of the received value. Input register numbers start with 3 and range from 30001 to 39999.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Holding register bit: Select Holding register bit to monitor a specific bit of the received value. Holding register numbers start with 4 and range from 40001 to 49999.</li> </ul> <p><b>i</b> You cannot change this value after sensor creation.</p>
<p>Channel #1 - #10 Register Number</p>	<p>Enter the register number from which you want to retrieve information.</p> <p><b>i</b> The register number must be a number that contains one to five digits. The sensor supports numbers between 0 and 65534.</p> <p><b>i</b> Depending on your Modbus device, you might need to remove the register type prefix. For example, you need to enter 60 for the input register 30060 or 316 for the holding register 40316.</p>
<p>Channel #1 - #10 Value Type</p>	<p>This setting is only visible if you select Input register or Holding register above.</p> <p>Select the value type that the channel displays:</p> <ul style="list-style-type: none"> <li>▪ Absolute (default): Integer64 values with or without an operational sign, such as 10 or 120 or -12 or 120.</li> <li>▪ Delta (counter): The sensor calculates the difference between the last value and the current value. The sensor additionally divides the delta value by a time period to indicate a speed value. The sensor ignores this setting if you select Double or Float as Channel #x Data Type.</li> </ul> <p><b>i</b> This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative values and decreasing values.</p>
<p>Channel #1 - #10 Data Type</p>	<p>This setting is only visible if you select Input register or Holding register above.</p> <p>Select the data type of the register:</p> <ul style="list-style-type: none"> <li>▪ 16-bit integer (default)</li> <li>▪ Unsigned 16-bit integer</li> <li>▪ 32-bit integer</li> <li>▪ Unsigned 32-bit integer</li> <li>▪ 64-bit integer</li> <li>▪ Float</li> <li>▪ Double</li> </ul> <p><b>i</b> You cannot change this value after sensor creation.</p>



Setting	Description
Channel #1 - #10 Register Width	<p>This setting is only visible if you select Input register or Holding register above.</p> <p>Select the width of the value in the register:</p> <ul style="list-style-type: none"> <li>16 bits wide (default)</li> <li>32 bits wide</li> <li>64 bits wide</li> </ul>
Channel #1 - #10 Bit Index	<p>This setting is only visible if you select Input register or Holding register above.</p> <p>Enter the index of the bit that you want to monitor.</p> <p><b>i</b> Enter a value between 0 and 15, 31, or 63, depending on the Channel #1 - #10 Register Width. 0 monitors the least significant bit. To monitor the most significant bit, enter 15 for a 16-bit register, 31 for a 32-bit register, or 63 for a 64-bit register.</p>

## Sensor Display

**Sensor Display**


Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>



## Debug Options

**Debug Options**


Result Handling 

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	The returned numeric values in up to ten channels

## More

### ■ KNOWLEDGE BASE

How can I apply Zoom Service Status sensors and Modbus sensors via device templates?

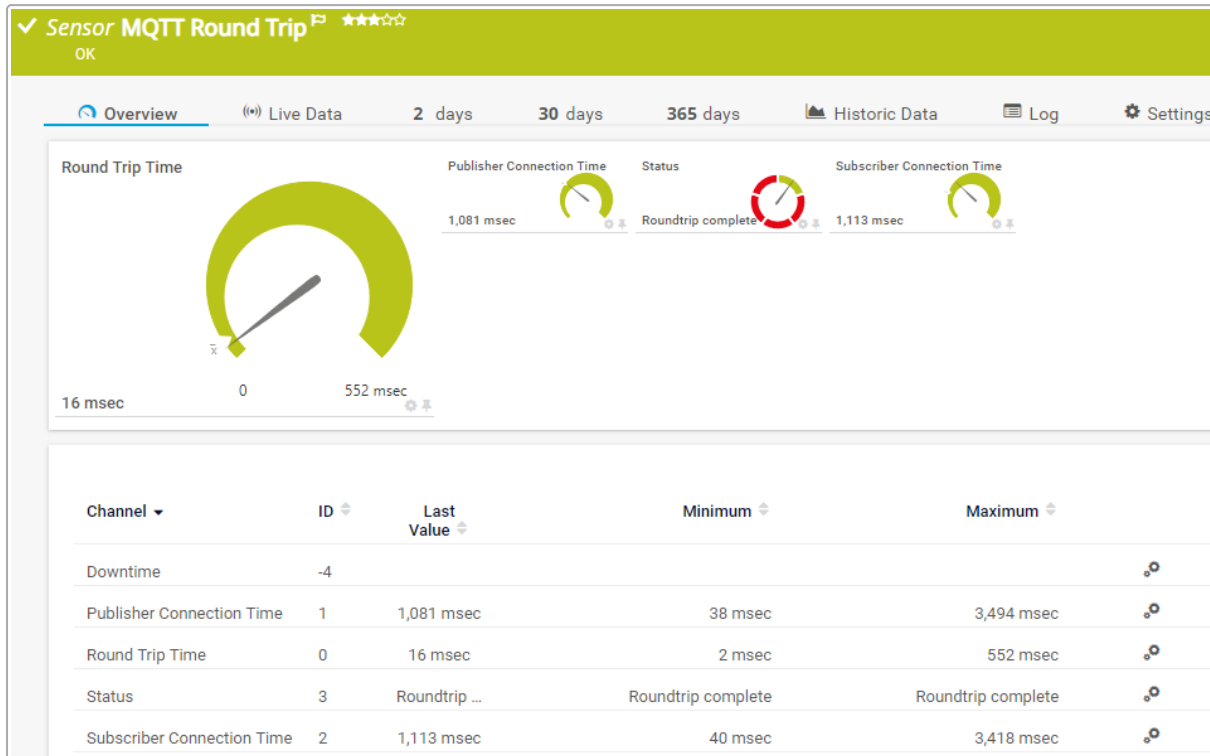
- <https://kb.paessler.com/en/topic/89684>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.97 MQTT Round Trip Sensor

The MQTT Round Trip sensor monitors the availability of a Message Queue Telemetry Transport (MQTT) broker (server), connects to the broker as a publishing and subscribing client, and sends the data packets using a predefined topic.



MQTT Round Trip Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1330</sup>.

### Sensor in Other Languages

- Dutch: MQTT Heen en Terug
- French: MQTT aller-retour
- German: MQTT Round Trip
- Japanese: MQTT ラウンドトリップ
- Portuguese: Ida e volta MQTT
- Russian: Цикл MQTT
- Simplified Chinese: MQTT 往返
- Spanish: Ida y vuelta MQTT

### Remarks

Consider the following [remarks](#)<sup>1326</sup> and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for MQTT.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
New framework	This sensor was converted to a new framework. MQTT Round Trip sensors that were added before PRTG 20.2.59 do not work anymore. We recommend that you pause existing sensors to keep their historic data. To continue monitoring, please add a new MQTT Round Trip sensor.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- mqtt
- mqttroundtrip
- roundtrip

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## MQTT Specific

**MQTT Specific**

Topic ⓘ PRTG/roundtrip/%sensorid

---

Connection Settings ⓘ  Use default settings  
 Use custom settings

MQTT Specific

Setting	Description
Topic	<p>Enter the topic for the round trip. The default is <a href="#">PRTG/roundtrip/%sensorid</a>.</p> <p> ⓘ PRTG replaces <a href="#">%sensorid</a> with the sensor's ID.</p>
Connection Settings	<p>Define the connection settings for the connection to the MQTT broker:</p> <ul style="list-style-type: none"> <li>▪ Use default settings: Use the default connection settings.</li> <li>▪ Use custom settings: Use a ClientID that you can specify below.</li> </ul>
ClientID	<p><a href="#">This setting is only visible if you select Use custom settings above.</a></p> <p>Enter the ClientID for the connection to the MQTT broker. The default is <a href="#">PRTG_%sensorid</a>.</p> <p> ⓘ PRTG replaces <a href="#">%sensorid</a> with the sensor's ID. For the subscribing client, PRTG automatically adds <a href="#">_subscriber</a> to the ClientID. For the publishing client, PRTG automatically adds <a href="#">_publisher</a> to the ClientID.</p>

## Sensor Display

**Sensor Display**


Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p>


Setting	Description
	<p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                     <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

**Result Handling** 
 Discard result (default)  
 Store result

Debug Options


Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result: Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Publisher Connection Time	The time it takes the publisher to connect
Round Trip Time	The RTT of the message (after both publisher and subscriber connect)  This channel is the primary channel by default.
Status	The round trip status <ul style="list-style-type: none"> <li>▪ Up status: Roundtrip Complete</li> <li>▪ Down status: Message Not Received, Message Not Sent, Publisher Could Not Connect, Subscriber Could Not Connect</li> </ul>
Subscriber Connection Time	The time it takes the subscriber to connect

## More

### ■ KNOWLEDGE BASE

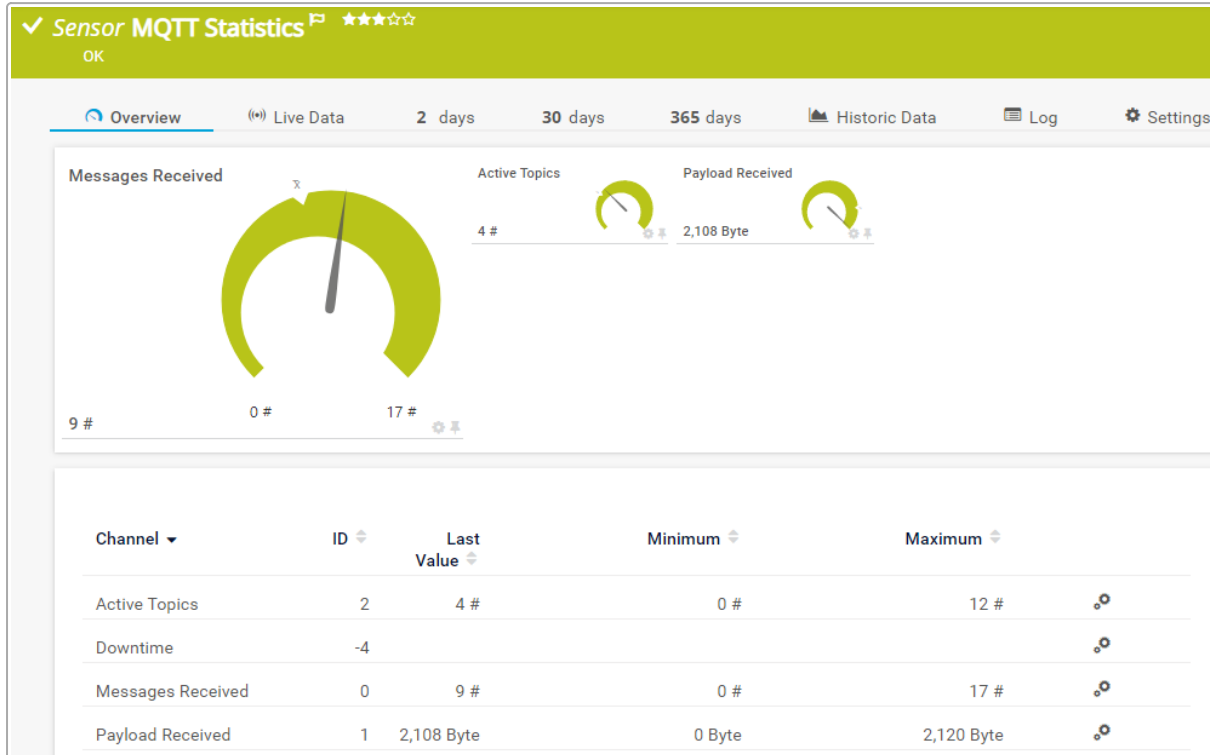
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>



## 7.8.98 MQTT Statistics Sensor

The MQTT Statistics sensor monitors a Message Queue Telemetry Transport (MQTT) topic.



MQTT Statistics Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1334]</sup>.

### Sensor in Other Languages

- Dutch: MQTT Statistieken
- French: MQTT statistiques
- German: MQTT Statistik
- Japanese: MQTT 統計
- Portuguese: Estatísticas MQTT
- Russian: Статистика MQTT
- Simplified Chinese: MQTT 统计
- Spanish: Estadísticas MQTT

### Remarks

Consider the following [remarks](#)<sup>[1331]</sup> and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for MQTT.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>medium</b> performance impact.
Multi-platform probe	You can add this sensor to a multi-platform probe.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- mqtt
- mqttstatistics

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### MQTT Specific

#### MQTT Specific

**Topic** ⓘ PRTG/roundtrip/%sensorid

---

MQTT Specific

Setting	Description
Topic	Enter the topic that you want to monitor. ⓘ The sensor supports single-level (+) and multi-level (#) wildcards.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Active Topics	The number of active MQTT topics
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Messages Received	<p>The number of messages received since the last scan</p> <p>ⓘ This channel is the primary channel by default.</p>
Payload Received	The payload received

## More

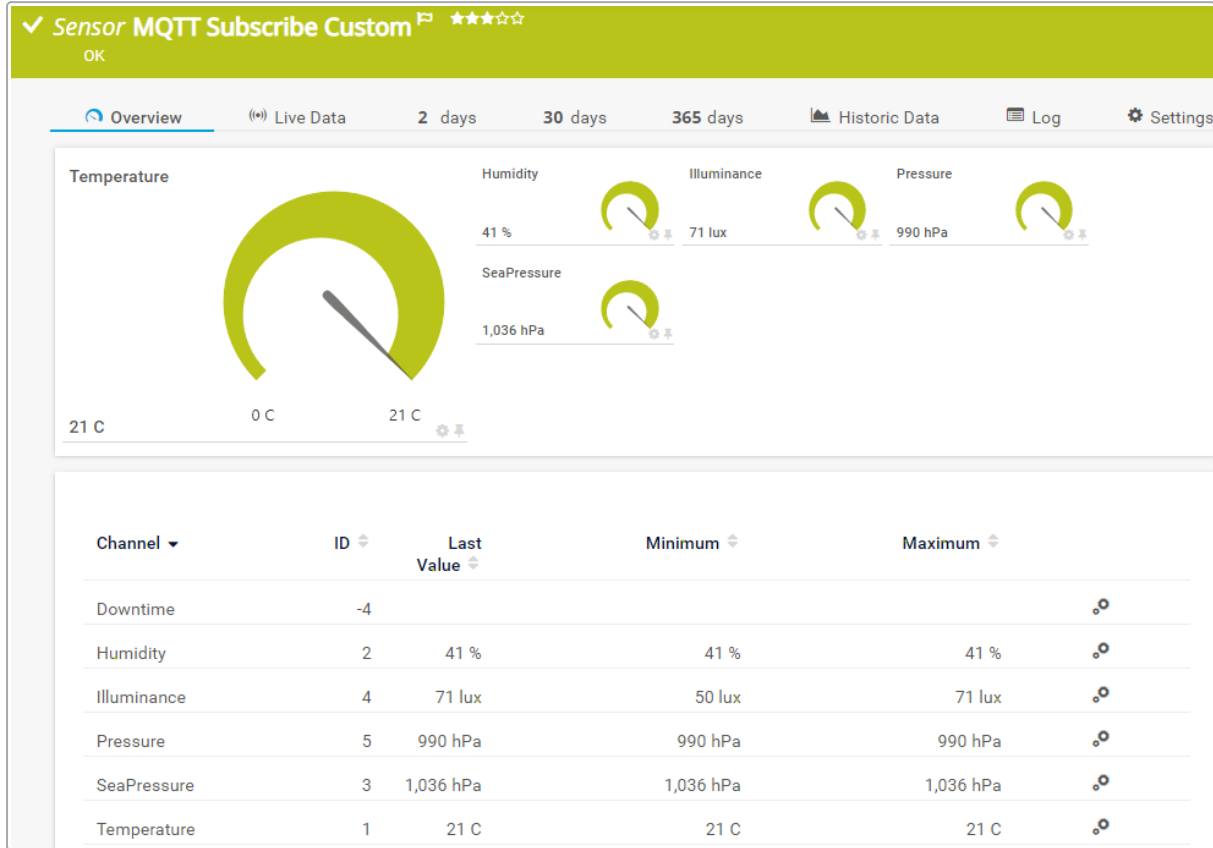
### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.99 MQTT Subscribe Custom Sensor

The MQTT Subscribe Custom sensor subscribes to a Message Queue Telemetry Transport (MQTT) topic and monitors up to ten numeric values from the received JavaScript Object Notation (JSON) data.



MQTT Subscribe Custom Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1341</sup>.

### Sensor in Other Languages

- Dutch: MQTT Abonneren Aangepast
- French: MQTT abonnement personnalisé
- German: MQTT Subscribe (Benutzerdefiniert)
- Japanese: MQTT サブスクライブカスタム
- Portuguese: Assinatura customizada MQTT
- Russian: Пользовательская подписка MQTT
- Simplified Chinese: MQTT 订阅自定义
- Spanish: Suscriptor MQTT personalizado

### Remarks

Consider the following [remarks](#)<sup>1336</sup> and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for MQTT.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
Multi-platform probe	You can add this sensor to a multi-platform probe.

### Add Sensor

Setting	Description
Channel #1 Name	Enter a name for the channel.  ⓘ You can change this value later in the <a href="#">channel settings</a> of this sensor.
Channel #1 Unit	Enter the unit for the numeric value that this sensor monitors.  ⓘ You can change this value later in the <a href="#">channel settings</a> of this sensor.

### Basic Sensor Settings

**Basic Sensor Settings**

Sensor Name ⓘ Example Name

---

Tags ⓘ  X +

---

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- mqtt
- mqttsubscribecustom

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## MQTT Specific

**MQTT Specific**

**Topic** ⓘ

---

**Time Since Last Message** ⓘ  Disable (default)  
 Enable

**Last Message Handling** ⓘ  Dismiss (default)  
 Retain

**Sensor Message JSONPath** ⓘ

---

**Channel #1 JSONPath** ⓘ

---

**Channel #1 Value Type** ⓘ

MQTT Specific

Setting	Description
Topic	<p>Enter the topic that you want to monitor.</p> <p> ⓘ The sensor supports single-level (+) and multi-level (#) wildcards.</p>
Time Since Last Message	<p>Select if you want to add a channel that shows the time in seconds since the last message was received:</p> <ul style="list-style-type: none"> <li>▪ <b>Disable (default):</b> Do not create this channel.</li> <li>▪ <b>Enable:</b> Create this channel. The sensor remains in the Up status even if it received no messages during the last scan interval.</li> </ul> <p> ⓘ You can define a threshold notification trigger to receive notifications if no data is received for a certain amount of time.</p>
Last Message Handling	<p>Define what PRTG does with the last message received if there are no new messages in the following scanning interval:</p> <ul style="list-style-type: none"> <li>▪ <b>Dismiss (default):</b> The sensor dismisses the last message received after a new scan.</li> <li>▪ <b>Retain:</b> The sensor saves the last message received until a new message is received.</li> </ul>
Sensor Message JSONPath	<p>Optionally enter the path to the value in the JSON data. The sensor shows the received value as the sensor message.</p>



Setting	Description
	<p><b>i</b> The data must be in valid JSON format. For details about the format, see Channel #x JSONPath below.</p> <p><b>i</b> The sensor only shows the received value if the sensor is in the Up status. If the sensor changes to the Down status, the sensor message shows the error message instead.</p>
<p>Channel #x JSONPath</p>	<p>Enter the path to the numeric value in the received JSON structure that you want to monitor.</p> <p><b>i</b> The data must be in valid JSON format, for example like this:</p> <pre data-bbox="485 797 1347 974"> {   "Sensor1": {"Temp":25,"Unit":"°C"},   "Sensor2": {"Humidity":36,"Unit":"%"} } </pre> <p>To query temperature, enter the following JSONPath:</p> <pre data-bbox="485 1016 1347 1066">\$.Sensor1.Temp</pre> <p>To query humidity, enter the following JSONPath:</p> <pre data-bbox="485 1108 1347 1158">\$.Sensor2.Humidity</pre>
<p>Channel #x Value Type</p>	<p>Select the value type that the channel displays:</p> <ul style="list-style-type: none"> <li>▪ Absolute (integer): Integer64 values with or without an operational sign, such as 10 or 120 or -12 or 120.</li> <li>▪ Absolute (float): Double values, such as -5.80 or 8.23. <ul style="list-style-type: none"> <li><b>i</b> If you select Absolute (float), the sensor automatically shows all decimal places of the received value in the channel. You can define how many decimal places of the channel's data that you want to display in graphs and tables in the <a href="#">channel settings</a>.</li> </ul> </li> <li>▪ Delta (counter): Counter values. The sensor calculates the difference between the last and the current value. Enter an integer. The sensor additionally divides the delta value by a time period to indicate a speed value. <ul style="list-style-type: none"> <li><b>i</b> This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative values and decreasing values.</li> </ul> </li> <li><b>i</b> Absolute (integer) and Absolute (float) support the extraction of numerical values from a received string. The sensor parses the numerical value from the beginning of the string until it encounters the first element that is not part of a numerical value, for example a letter. The sensor ignores whitespace characters.</li> <li><b>i</b> You cannot change this value after sensor creation.</li> </ul>

Setting	Description
Channel #2 - #10	<p>You can define up to 10 channels. You must define at least one channel, so you see all available settings for <a href="#">Channel #1</a>. Specify how to handle all other possible channels:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not create this channel.</li> <li>▪ Enable: Create this channel.</li> </ul> <p><b>i</b> If you select Disable (default), you can still see the channels, but they do not receive data anymore.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)

Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	The returned numeric values in up to ten channels

## More

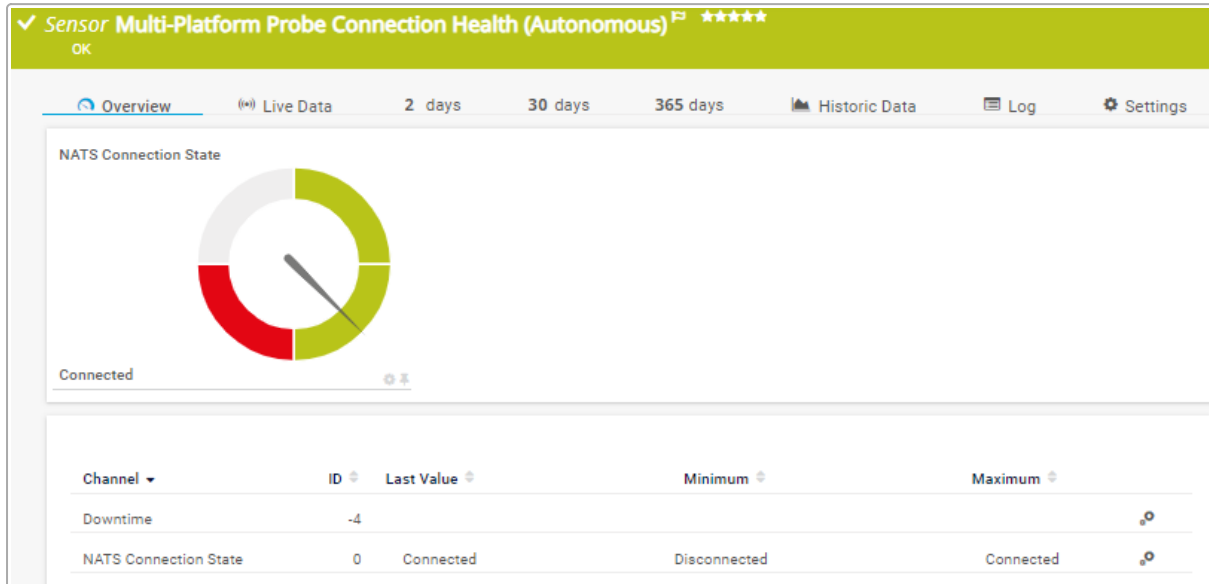
### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.100 Multi-Platform Probe Connection Health (Autonomous) Sensor

The Multi-Platform Probe Connection Health (Autonomous) sensor monitors the state of the connection between the PRTG core and multi-platform probes.



Multi-Platform Probe Connection Health (Autonomous) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Multi-Platform Probe Verbindings Status (Autonom)
- French: État de la connexion de la sonde multi plate-forme (autonome)
- German: Zustand der Verbindungen mit Multi-Plattform Probes (Autonom)
- Japanese: マルチプラットフォームプローブの接続の正常性(自律)
- Portuguese: Saúde da conexão da sonda multiplataforma (autônoma)
- Russian: Работоспособность подключения многоплатформенного зонда (автономно)
- Simplified Chinese: 多平台探针连接运行状况(自主)
- Spanish: Salud de conexión de sonda multiplataforma (autónomo)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <b>very low</b> performance impact.

Remark	Description
Sensor creation	PRTG automatically creates this sensor on the PRTG core server when you enable <a href="#">multi-platform probe</a> connections under Setup   System Administration   Core & Probes.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Knowledge Base	Knowledge Base: <a href="#">What is the multi-platform probe and how can I use it?</a>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- multiplatformprobeconnectionhealthsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Display

#### Sensor Display


**Primary Channel** ⓘ Downtime

---

**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.


Setting	Description
	<p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.           <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

**Result Handling** 
  
 Discard result (default)
   
 Store result

Debug Options


Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>



## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
NATS Connection State	<p>The state of the connection to the NATS server</p> <ul style="list-style-type: none"> <li>• Up: Connected, Disabled</li> <li>• Down: Disconnected</li> <li>• Unknown: Unknown</li> </ul> <p> If this sensor remains in the Down or Unknown state, check your configuration in Setup   System Administration   Core &amp; Probes.</p> <p> This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

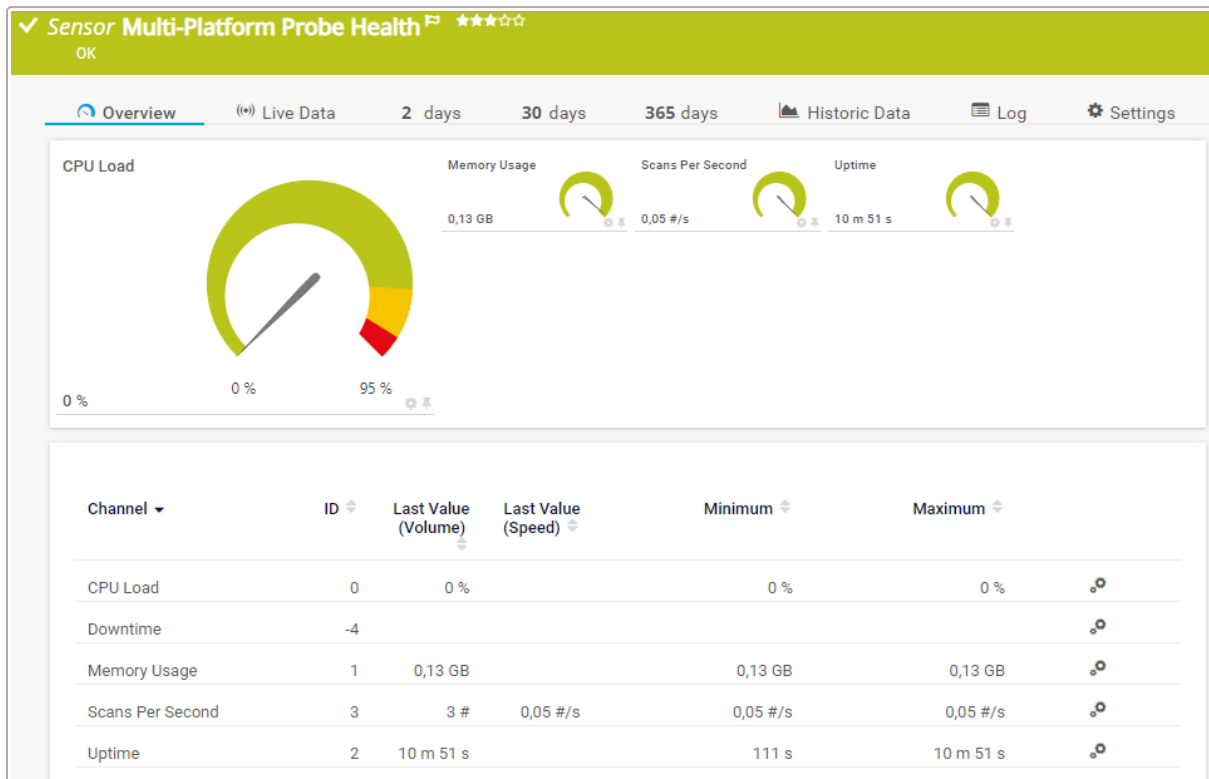
What is the multi-platform probe and how can I use it?

- <https://kb.paessler.com/en/topic/90140>



## 7.8.101 Multi-Platform Probe Health Sensor

The Multi-Platform Probe Health Sensor monitors the status of a multi-platform probe device.



Multi-Platform Probe Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1350</sup>.

### Sensor in Other Languages

- Dutch: Multi-Platform Probe Status
- French: État de la sonde multiplateforme
- German: Zustand der Multi-Plattform Probe
- Japanese: マルチプラットフォームプローブの正常性
- Portuguese: Saúde da sonda multiplataforma
- Russian: Работоспособность многоплатформенного зонда
- Simplified Chinese: 多平台探针健康状况
- Spanish: Salud de la sonda multiplataforma

### Remarks

Consider the following [remarks](#)<sup>1347</sup> and requirements for this sensor:

Remark	Description
Sensor creation	PRTG automatically creates this sensor. You cannot delete it. If you manually create the sensor, you can delete it.
Windows	This sensor does not support Windows operating systems.
Probe device	You can create this sensor only on a <a href="#">probe device</a> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Scanning interval	The recommended scanning interval of this sensor is <a href="#">1 minute</a> .
Multi-platform probe	You can add this sensor to a multi-platform probe.
Knowledge Base	Knowledge Base: <a href="#">What is the multi-platform probe and how can I use it?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- multiplatformprobehealthsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Multi-Platform Probe Health Specific

Multi-Platform Probe Health Specific
Port ? 23562

Multi-Platform Probe Health Specific

Setting	Description
Port	Enter the port number (between 1 and 65535) that this sensor uses to connect to the multi-platform probe. The default port is <a href="#">23562</a> .

## Sensor Display

Sensor Display

Primary Channel ? Downtime

Graph Type ?

- Show channels independently (default)
- Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><span style="font-size: 1.2em;">?</span> You can set a different primary channel later by clicking <span style="font-size: 0.8em;">?</span> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><span style="font-size: 1.2em;">?</span> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

## Debug Options


**Debug Options**

**Result Handling** ⓘ  Discard result (default)   
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CPU Load	<p>The CPU load (%) of the multi-platform probe. Extensive CPU load can lead to false, incomplete, and incorrect monitoring results. This value should usually stay below 50%.</p> <p><b>i</b> This channel is the primary channel by default.</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: 90%</li> <li>▪ Upper warning limit: 80%</li> </ul>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Memory Usage	The memory usage
Scans per Second	The number of scans per second
Uptime	The uptime

## More

### ■ KNOWLEDGE BASE

What is the multi-platform probe and how can I use it?

- <https://kb.paessler.com/en/topic/90140>

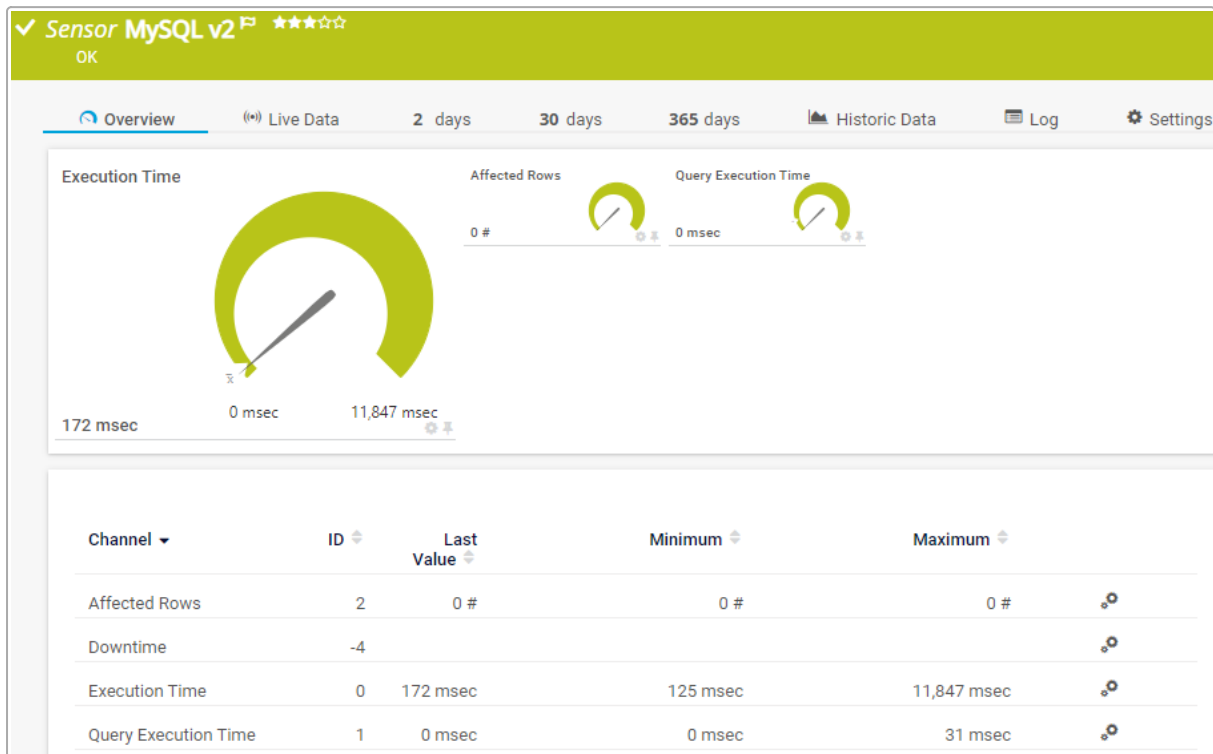
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.102 MySQL v2 Sensor

The MySQL v2 sensor monitors a database on a MySQL server and executes a query.

- ❶ The sensor can also process the data table and show the values that you define in individual channels.



MySQL v2 Sensor

- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1362</sup>.

### Sensor in Other Languages

- Dutch: MySQL v2
- French: MySQL v2
- German: MySQL v2
- Japanese: MySQL v2
- Portuguese: MySQL v2
- Russian: MySQL v2
- Simplified Chinese: MySQL v2
- Spanish: MySQL v2

### Remarks

Consider the following [remarks](#)<sup>1352</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
SQL query storage	This sensor requires that you store the SQL query in a file on the probe system. In a cluster, copy the file to every cluster node.  ■ For more information, see the Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a>
.NET 4.7.2 or later	This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.  ❗ If the framework is missing, you cannot create this sensor.  ■ For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a>
MySQL server	This sensor supports MySQL server versions as of 5.7.
IPv6	This sensor supports IPv6.
Lookups	This sensor can use <a href="#">lookups</a> <sup>[1359]</sup> . Select Lookup as Channel #x Unit and define the lookup file in Channel #x Lookup.
Credentials	Define the credentials for database management systems in settings that are higher in the object hierarchy.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">How to set up the SQL v2 sensors in PRTG? Is there a guide?</a></li> <li>▪ Knowledge Base: <a href="#">How can I monitor strings from an SQL database and show a sensor status depending on it?</a></li> <li>▪ Knowledge Base: <a href="#">How can I monitor error tables in SQL databases?</a></li> <li>▪ Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a></li> </ul>
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- sqlsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Database Specific

### Database Specific

**Database** ⓘ

**SSL Mode** ⓘ

None

Preferred (default)

Required

Database Specific

Setting	Description
Database	<p>Enter the name of the MySQL database to which the sensor connects, for example, <a href="#">MyDatabase</a>. This is a logical entity on the database server where database objects exist.</p> <p>The database name of a MySQL server also reflects a physical directory structure where your database objects are stored. Enter the appropriate string, which is the same as you would supply when you invoke the <a href="#">mysql.exe</a> admin tool (with the command-line switch <code>-p</code>) or after you log in with <a href="#">mysql.exe</a> with the command <code>use</code>.</p>
SSL Mode	<p>Select the MySQL Secure Sockets Layer (SSL) mode for the connection:</p> <ul style="list-style-type: none"> <li>▪ None: Do not use SSL.</li> <li>▪ Preferred (default): Use SSL if the server supports it.</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>Required: Always use SSL and deny the connection if the server does not support it. Do not perform a server certificate validation.</li> </ul> <p>The SSL mode options that you can choose are the same as the values of the MySQL <code>sslmode</code> parameter. PRTG sends it with the sensor requests.</p> <p><b>i</b> For more information about the MySQL SSL modes, refer to the MySQL documentation.</p>

## Data

**Data**

**SQL Query File** ⓘ *Demo Serveruptime.sql*

**Input Parameter Handling** ⓘ  Do not use input parameter (default)  
 Use input parameter

**Transaction Handling** ⓘ  Do not use transaction (default)  
 Use transaction and always roll back  
 Use transaction and commit on success






**Data Processing** ⓘ *Only execute query (default)*

**Result Handling** ⓘ  Discard result (default)  
 Store result

Data

Setting	Description
SQL Query File	<p>Select the SQL query file that includes a valid SQL statement that the sensor executes on the server with every scanning interval. The list contains SQL scripts from the \Custom Sensors\sql subfolder of the <a href="#">PRTG program directory</a> on the probe system. Store your script there. If you use the script on a cluster probe, you must store the script on all cluster nodes.</p> <p>A correct expression in the file could be: <code>SELECT AVG(UnitPrice) FROM Products</code>. If you want to use transactions, separate the individual steps with semicolons ";".</p> <p><b>i</b> Note that with each request, PRTG transfers the full result set, so use filters and limits in your query.</p> <p><b>i</b> The demo script Demo Serveruptime.sql is available by default. You can use it to monitor the uptime of the target server.</p>

Setting	Description
	<p>■ See also the Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a></p> <p>ⓘ You cannot change this value after sensor creation.</p>
Input Parameter Handling	<p>Define if you want to pass a parameter to the SQL query file:</p> <ul style="list-style-type: none"> <li>▪ Do not use input parameter (default): Execute the SQL query file without using variables.</li> <li>▪ Use input parameter: Execute an SQL query file that contains a variable. Provide the parameter that you want to use in the query below.</li> </ul>
Input Parameter	<p><b>This setting is only visible if you select Use input parameter above.</b></p> <p>Enter the parameter that you want to pass to the SQL query file. This parameter replaces the variables <code>@prtg</code>, <code>:prtg</code>, or <code>?</code> in the SQL query, considering the general rules for SQL variables.</p> <p>You can also use PRTG placeholders for custom sensors (command-line parameters) as input parameters, for example, <code>%sensorid</code> or <code>%deviceid</code>. For more information, see section <a href="#">Custom Sensors</a>.</p> <p>ⓘ Provide strings as they are and do not surround them with quotation marks. PRTG automatically and correctly inserts string parameters into the query.</p>
Transaction Handling	<p>Define if you want to use transactions and if they affect the database content:</p> <ul style="list-style-type: none"> <li>▪ Do not use transaction (default): Do not execute transactions.</li> <li>▪ Use transaction and always roll back: The query does not change data in the database. In the SQL query file, separate the single steps of the transaction with semicolons.</li> <li>▪ Use transaction and commit on success: The query changes data in the database. The changes only apply if all execution steps succeed without any errors. In the SQL query file, separate the single steps of the transaction with semicolons.</li> </ul>
Data Processing	<p>Define whether the sensor processes data from the database:</p> <ul style="list-style-type: none"> <li>▪ Only execute query (default): Only show information about the number of affected rows and the execution time of the query. Affected rows are rows that were changed by the query (for example, created, deleted, or edited).</li> <li>▪ Count table rows: Execute a <b>SELECT</b> statement and monitor how many rows of the data table this statement returns.</li> <li>▪ Process data table: Read and analyze the data table. If you select this option, the sensor counts rows with <b>SELECT</b> statements as well.</li> </ul>

Setting	Description
	<p> You cannot change this value after sensor creation.</p>
DBNull Handling	<p><a href="#">This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</a></p> <p>Define the sensor behavior if the query returns <b>DBNull</b>:</p> <ul style="list-style-type: none"> <li>▪ Error: Show the Down status if the query returns <b>DBNull</b>.</li> <li>▪ Number 0: Recognize the result <b>DBNull</b> as a valid value and interpret it as the number <b>0</b>.</li> </ul>
Select Channel Value by	<p><a href="#">This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</a></p> <p>Define how to select the desired cell in the database table:</p> <ul style="list-style-type: none"> <li>▪ Column number: Determine the channel value by using the value in row 0 of the column whose number you specify in Channel #x Column Number.</li> <li>▪ Column name: Determine the channel value by using the value in row 0 of the column whose name you specify in Channel #x Column Name.</li> <li>▪ Row number: Determine the channel value by using the value in column 0 of the row whose number you specify in Channel #x Row Number.</li> <li>▪ Key value pair: Determine the channel value by searching in column 0 for the key you specify in Channel #x Key and by returning the value in column 1 of the same row where the key value was found.</li> </ul> <p> Defining how the desired cell in the database table is selected is necessary to configure the cells that are used in the channels.</p> <p> The option you select here also defines the method of how to optionally determine a value for the sensor message. For more information, see setting Use Data Table Value in Message.</p> <p> For an example for channel value selection, see section <a href="#">Monitoring Databases</a>.</p>
Channel #2 - #10	<p><a href="#">This setting is only visible if you select Process data table above.</a></p> <p>You can define up to 10 channels. You must define at least one channel, so you see all available settings for <b>Channel #1</b>. Specify how to handle all other possible channels:</p> <ul style="list-style-type: none"> <li>▪ Disable: Do not create this channel.</li> <li>▪ Enable: Create this channel.</li> </ul> <p> It is not possible to enable or disable channels after sensor creation.</p>

Setting	Description
Channel #x Name	<p>This setting is only visible if you select <a href="#">Process data table for the setting Data Processing during sensor creation</a>.</p> <p>Enter a name for the channel. Enter a string. The sensor dynamically generates channels with this name as identifier.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Channel #x Column Number	<p>This setting is only visible if you select <a href="#">Process data table for the setting Data Processing during sensor creation</a> and if you select <a href="#">Column number for the setting Select Channel Value by</a>.</p> <p>Provide the number of the column to use to determine the channel value in row 0. Enter an integer.</p>
Channel #x Column Name	<p>This setting is only visible if you select <a href="#">Process data table for the setting Data Processing during sensor creation</a> and if you select <a href="#">Column name for the setting Select Channel Value by</a>.</p> <p>Provide the name of the column to use to determine the channel value in row 0. Enter an integer.</p>
Channel #x Row Number	<p>This setting is only visible if you select <a href="#">Process data table for the setting Data Processing during sensor creation</a> and if you select <a href="#">Row number for the setting Select Channel Value by</a>.</p> <p>Provide the number of the column to use to determine the channel value in row 0. Enter an integer.</p>
Channel #x Key	<p>This setting is only visible if you select <a href="#">Process data table for the setting Data Processing during sensor creation</a> and if you select <a href="#">Key value pair for the setting Select Channel Value by</a>.</p> <p>Provide the key to search for in column 0 of the data table. The value in column 1 of the same row where the key value was found to use to determine the channel value. Enter a string.</p>
Channel #x Mode	<p>This setting is only visible if you select <a href="#">Process data table above</a>.</p> <p>Define how to display the determined value in the channel:</p> <ul style="list-style-type: none"> <li>▪ Absolute (default): Show the value as the sensor retrieves it from the data table.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Difference: The sensor calculates and shows the difference between the last and the current value returned from the data table.               <ul style="list-style-type: none"> <li>ⓘ This mode is not compatible with the unit Lookup.</li> <li>ⓘ This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative and decreasing values.</li> </ul> </li> <li>▪ Absolute (recommended): Show the value as the sensor retrieves it from the data table.</li> <li>▪ Difference: The sensor calculates and shows the difference between the last and the current value returned from the data table.               <ul style="list-style-type: none"> <li>ⓘ This mode is not compatible with the unit Lookup.</li> <li>ⓘ This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative and decreasing values.</li> </ul> </li> <li>ⓘ You cannot change this value after sensor creation.</li> </ul>
Channel #x Unit	<p>This setting is only visible if you select <a href="#">Process data table</a> above.</p> <p>Define the unit of the channel value:</p> <ul style="list-style-type: none"> <li>▪ BytesBandwidth</li> <li>▪ BytesMemory</li> <li>▪ BytesDisk</li> <li>▪ Temperature</li> <li>▪ Percent</li> <li>▪ TimeResponse</li> <li>▪ TimeSeconds</li> <li>▪ TimeHours</li> <li>▪ Count</li> <li>▪ CPU</li> <li>▪ BytesFile</li> <li>▪ SpeedDisk</li> <li>▪ SpeedNet</li> <li>▪ Custom</li> <li>▪ Lookup</li> </ul> <p>■ For more information about the available units, see section <a href="#">Custom Sensors</a>.</p>

Setting	Description
	<p><b>i</b> To use <a href="#">lookups</a> with this channel, select Lookup and define the lookup file in Channel #x Lookup. Do not use Custom if you use lookups with this sensor.</p> <p><b>i</b> It is not possible to use the unit Lookup in combination with the Difference mode. You are not able to create the sensor in this case.</p>
Channel #x Custom Unit	<p>This setting is only visible if you select Custom above.</p> <p>Define a unit for the channel value. Enter a string.</p>
Channel #x Lookup	<p>This setting is only visible if you select Lookup above.</p> <p>Select a <a href="#">lookup</a> file that you want to use with this channel.</p>
Use Data Table Value in Message	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</p> <p>Define if the sensor message shows a value from the data table:</p> <ul style="list-style-type: none"> <li>▪ Disable: Do not use a custom sensor message.</li> <li>▪ Enable: Define a custom sensor message with a defined value of the data table. Define the value selection below.</li> </ul> <p><b>i</b> The method of how to determine a value for the sensor message is defined in the setting Select Channel Value by above.</p>
Message Column Number	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation, if you select Column name for the setting Select Channel Value by, and if you select Enable above.</p> <p>Enter the number of a column. The sensor message shows the value in row 0 of this column. Enter an integer.</p>
Message Column Name	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation, if you select Column name for the setting Select Channel Value by, and if you select Enable above.</p> <p>Enter the name of a column. The sensor message shows the value in row 0 of this column. Enter a string.</p> <p><b>i</b> Columns start with index 0.</p>
Message Row Number	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation, if you select Row number for the setting Select Channel Value by, and if you select Enable above.</p>

Setting	Description
	<p>Enter the name of a column. The sensor message shows the value in row 0 of this column. Enter the number of a row. The sensor message shows the value in column 0 of this row. Enter an integer.</p> <p><b>i</b> Rows start with index 0.</p>
<p>Message Key</p>	<p><b>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation, if you select Key value pair for the setting Select Channel Value by, and if you select Enable above.</b></p> <p>Enter a key to search for in column 0 of the data table. The sensor message shows the value in column 1 of the row where the key was found. Enter a string.</p>
<p>Message</p>	<p><b>This setting is only visible if you select Enable above.</b></p> <p>Define the sensor message. Enter a string. Use the placeholder <code>{0}</code> at the position where you want to display the value.</p> <p>Example: <code>The message is {0}</code></p> <p><b>i</b> PRTG does not support the number sign (<code>#</code>) in sensor messages. If a message contains a number sign, PRTG clips the message at this point.</p>
<p>If Message Changes</p>	<p><b>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</b></p> <p>Define what the sensor does when its message changes:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> <li>▪ Trigger 'change' notification: Send an internal message that indicates a change.</li> </ul> <p><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</p>
<p>Result Handling</p>	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the <code>\Logs\sensors</code> subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are <code>Result of Sensor [ID].txt</code>, <code>Result of Sensor [ID].Data.txt</code>, and <code>Result of Sensor [ID].log</code>. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.



Channel	Description
Affected Rows	The number of rows that were addressed by the query (including <b>SELECT</b> statements if you process data tables)
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Execution Time	The execution time of the entire request (including connection buildup, query execution, transaction handling, disconnection)  <span>ⓘ</span> This channel is the primary channel by default.
Query Execution Time	The execution time of the specified query

## SQL Variables

You can use the following variables in the SQL query file to be replaced by an input parameter. This is useful if you have various SQL sensors with queries that differ in only one parameter.

- Microsoft SQL, MySQL, PostgreSQL: [@prtg](#)
- Oracle SQL: [:prtg](#)
- ADO SQL: [?](#) (question mark)

ⓘ [@prtg](#), [:prtg](#), and [?](#) are common SQL query parameters and they are used in a parameterized SQL query. This means that the query and the parameter are forwarded without any changes to the database. This leads to some restrictions on the database side. For example, you cannot use variables as placeholders for table names or as lists in IN operators.

Examples for variables usage:

```
SELECT * FROM Table WHERE name = @prtg
SELECT @prtg FROM Table
```

## More

### ■ KNOWLEDGE BASE

How to set up the SQL v2 sensors in PRTG? Is there a guide?

- <https://kb.paessler.com/en/topic/70618>

How can I monitor strings from an SQL database and show a sensor status depending on it?

- <https://kb.paessler.com/en/topic/63259>

How can I monitor error tables in SQL databases?

- <https://kb.paessler.com/en/topic/70774>

Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

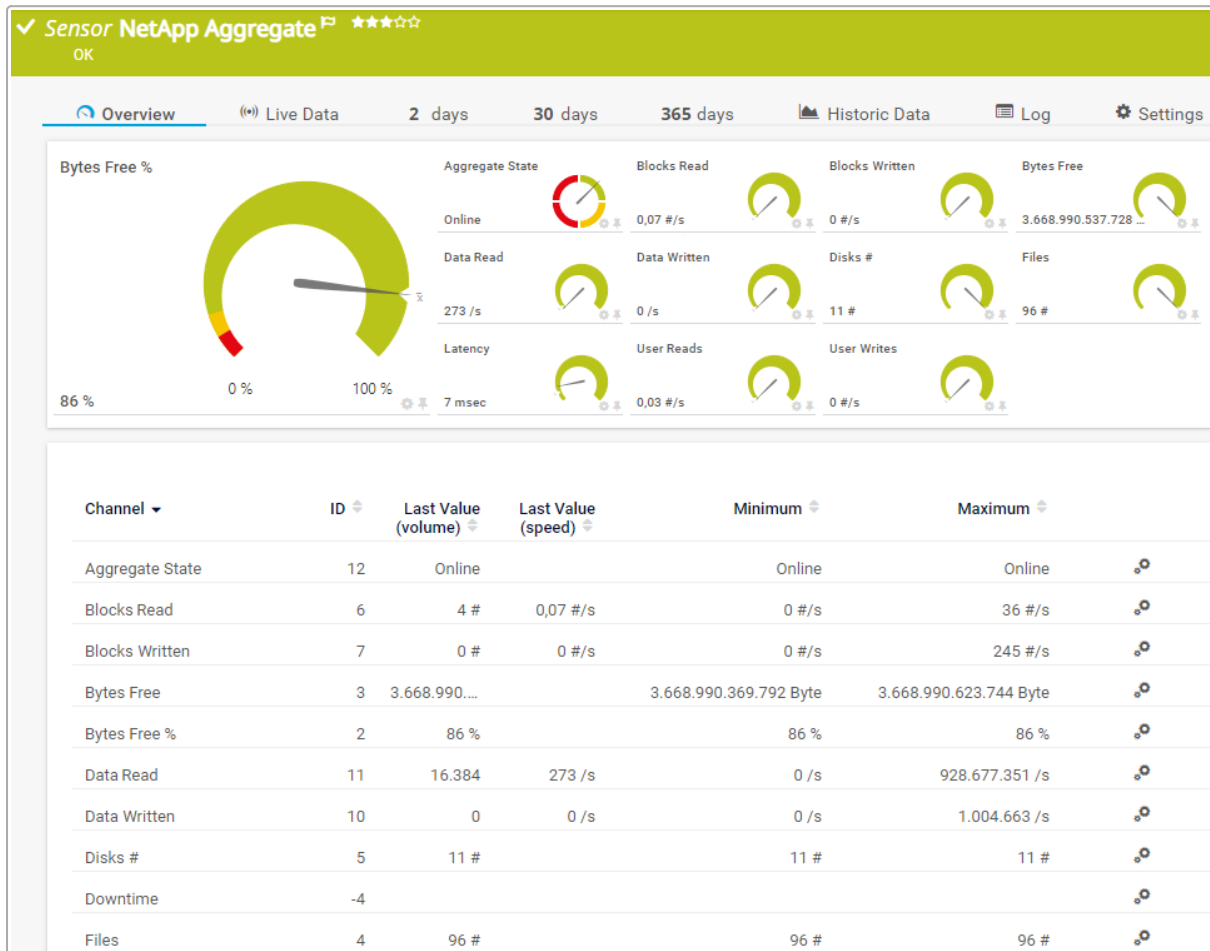
- <https://kb.paessler.com/en/topic/61108>

## 7.8.103 NetApp Aggregate Sensor

### IMPORTANT INFORMATION

This sensor supports NetApp cDOT as of version 8.3 or ONTAP from versions 9.0 to 9.12. If you use ONTAP as of version 9.6, we recommend that you use the [NetApp Aggregate v2](#) <sup>[1372]</sup> sensor.

The NetApp Aggregate sensor monitors the status of a NetApp cDOT or ONTAP storage aggregate accessing the application programming interface (API) via the Simple Object Access Protocol (SOAP).



NetApp Aggregate Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) <sup>[1370]</sup>.

### Sensor in Other Languages

- Dutch: NetApp Aggregate
- French: NetApp agrégat de stockage
- German: NetApp Aggregat
- Japanese: NetApp の合計

- Portuguese: Agregado NetApp
- Russian: Статистическое выражение NetApp
- Simplified Chinese: NetApp 聚合
- Spanish: Agregado NetApp

## Remarks

Consider the following [remarks](#) <sup>11366</sup> and requirements for this sensor:

Remark	Description
Enabled ONTAPI access	<p>The ONTAPI user account that you use with this sensor requires access to the <a href="#">DATA ONTAP API (ONTAPI)</a> so that the sensor can request data from it. The access is enabled by default.</p> <p><b>i</b> If access is disabled, locally use the following command on the cluster console to enable ONTAPI access for the user:</p> <pre>services web&gt; modify -vserver clusterd -name ontapi -enabled true</pre> <p>For this sensor, read-only user rights are sufficient for the ONTAPI user account that you use to access ONTAPI. Modify or add this user with a suitable role in the console under Cluster   ClusterX   Configuration   Security   Users</p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p><b>i</b> If the framework is missing, you cannot create this sensor.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
NetApp versions	<p>This sensor supports NetApp cDOT as of version 8.3 and NetApp ONTAP as of version 9.0.</p>
IPv6	<p>This sensor supports IPv6.</p>
Performance impact	<p>This sensor has a <a href="#">very low</a> performance impact.</p>
Credentials	<p>You can define NetApp API credentials (User Name and Password) in the <a href="#">credentials for Windows systems</a> settings of the parent device. This way, you do not need to individually enter credentials for each NetApp sensor that you add to the same device.</p>
Lookups	<p>This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.</p>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cdot
- netapp
- ontap
- soap

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## NetApp Connection

### NetApp Connection

**NetApp Credentials** ⓘ

**Port** ⓘ

**Connection Security** ⓘ

**Timeout (Sec.)** ⓘ

Use explicit credentials

Use Windows credentials from parent device

HTTP

HTTPS

NetApp Connection

Setting	Description
NetApp Credentials	Specify which credentials you want to use to connect to the NetApp API: <ul style="list-style-type: none"> <li>▪ Use explicit credentials: Use individual NetApp API credentials.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Use Windows credentials from parent device: Use the credentials (User Name and Password) in the <a href="#">parent device settings</a> in section Credentials for Windows Systems.</li> </ul> <p><b>i</b> Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you do not need to individually enter credentials for each NetApp sensor.</p>
User Name	<p>This setting is only visible if you select Use explicit credentials <a href="#">above</a>.</p> <p>Enter a user name for access to the NetApp API. Enter a string.</p> <p><b>i</b> Read-only rights for this ONTAP user account are sufficient.</p>
Password	<p>This setting is only visible if you select Use explicit credentials <a href="#">above</a>.</p> <p>Enter the password of the user for access to the NetApp API. Enter a string.</p>
Port	<p>Enter a port number on which you can access the NetApp API. Enter an integer. The default port is <a href="#">443</a>.</p>
Connection Security	<p>Define if the connection to the NetApp API is Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured:</p> <ul style="list-style-type: none"> <li>HTTP: Use an unsecured HTTP connection.</li> <li>HTTPS: Use a secure connection to the defined port to send the query.</li> </ul>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <a href="#">900</a> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

### NetApp Specific

NetApp Specific
Aggregates **i**
AGGR\_00

NetApp Specific

Setting	Description
Aggregates	The identifier of the aggregate that this sensor monitors.

## Debug Options

**Debug Options**

**Result Handling** ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

**Primary Channel** ⓘ

Downtime


---

**Graph Type** ⓘ


Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.


 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Aggregate State	<p>The aggregate status</p> <ul style="list-style-type: none"> <li>Up status: Online</li> <li>Warning status: Restrict</li> <li>Down status: Offline, Other Error</li> </ul>
Blocks Read	The number of blocks read
Blocks Written	The number of blocks written
Bytes Free	The free bytes in total
Bytes Free %	The free bytes (%)



Channel	Description
	 This channel is the primary channel by default.
Data Read	The data read speed
Data Written	The data write speed
Disks #	The number of disks on the aggregate
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Files	The number of files on the aggregate
Latency	The latency
User Reads	The number of user reads
User Writes	The number of user writes

## More

### KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

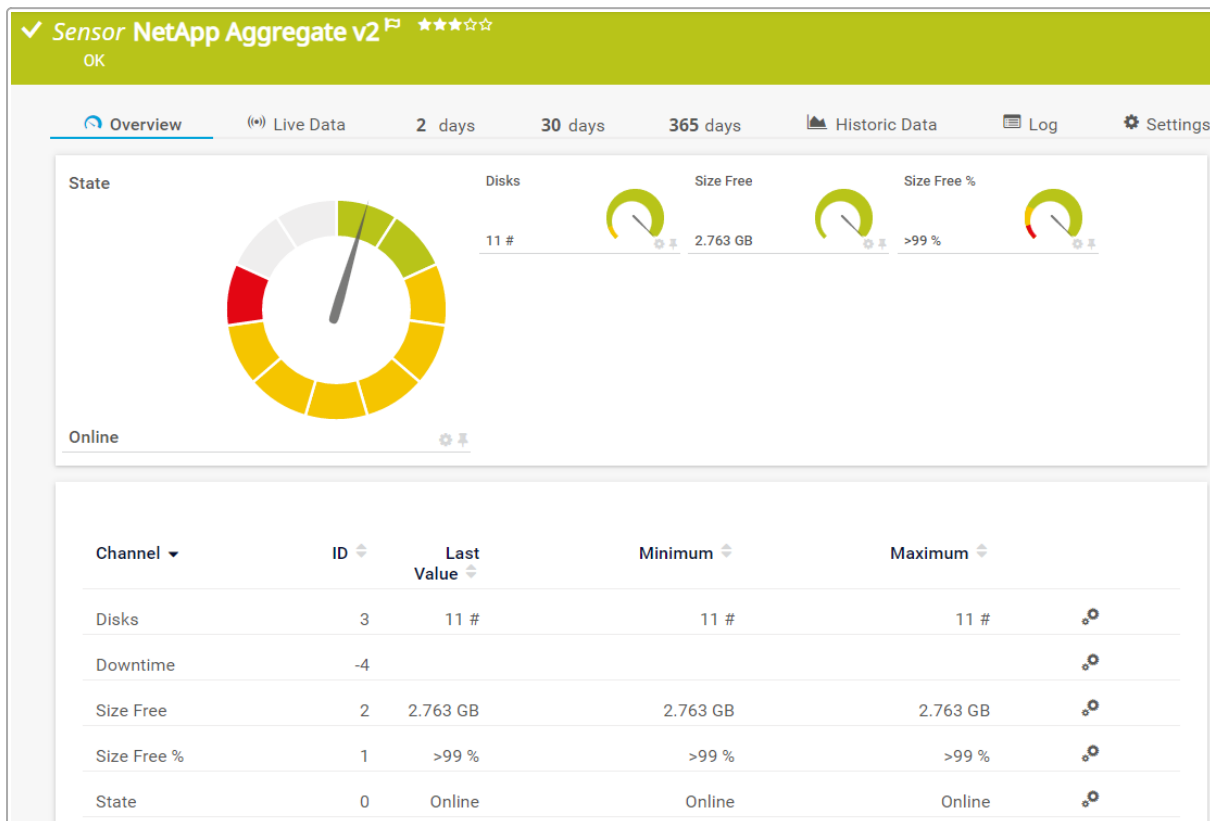
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.104 NetApp Aggregate v2 Sensor

The NetApp Aggregate v2 sensor monitors the status of a NetApp storage aggregate via the Representational State Transfer (REST) application programming interface (API) using ONTAP as of version 9.6.

**i** This sensor was converted to a new framework so that it will continue to function after the changes of the ONTAP REST API.



NetApp Aggregate v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1372</sup>.

### Sensor in Other Languages

- Dutch: NetApp Aggregaat v2
- French: NetApp agrégat de stockage v2
- German: NetApp Aggregat v2
- Japanese: NetApp 合計 v2
- Portuguese: Agregado NetApp v2
- Russian: Статистическое выражение NetApp v2
- Simplified Chinese: NetApp 聚合 v2
- Spanish: Agregado NetApp v2

## Remarks

Consider the following [remarks](#)<sup>[1373]</sup> and requirements for this sensor:

Remark	Description
Credentials for NetApp	This sensor requires an <a href="#">ONTAP System Manager</a> user account with the role <a href="#">readonly</a> and with access to the <a href="#">HTTP</a> application with <a href="#">Password</a> authentication.
Permissions for the ONTAP REST API	<p>This sensor requires permissions for the <a href="#">ONTAP REST API</a>.</p> <p><b>i</b> This sensor requires the role <a href="#">readonly</a> with the following permissions for the <a href="#">ONTAP REST API</a>:</p> <p>Access level <a href="#">Read-Only</a>:</p> <ul style="list-style-type: none"> <li>▫ /api</li> <li>▫ /api/security/audit/destinations</li> </ul> <p>Access level <a href="#">Read/Write</a>:</p> <ul style="list-style-type: none"> <li>▫ /api/security/authentication/password</li> </ul> <p>Access level <a href="#">None</a>:</p> <ul style="list-style-type: none"> <li>▫ /api/security</li> </ul>
Credentials	This sensor requires credentials for NetApp.
Output	This sensor does not include system-owned root aggregates in the output.
NetApp versions	This sensor supports ONTAP as of version 9.6. If you want to use NetApp cDOT as of version 8.3 or ONTAP from version 9.0 to version 9.5, use the <a href="#">NetApp Aggregate</a> <sup>[1365]</sup> sensor. <sup>[1472]</sup>
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Scanning interval	The recommended scanning interval of this sensor is <a href="#">1 minute</a> .
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- aggregate
- netapp
- ontap
- rest

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## NetApp Specific

### NetApp Specific

**Aggregate Name** ⓘ AGGR\_01\_NET\_AFF220\_01\_SSD

---

**Node Name** ⓘ net-aff220-01

NetApp Specific

Setting	Description
Aggregate Name	The name of the aggregate that this sensor monitors.
Node Name	The name of the node that contains the aggregate that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Disks	<p>The number of disks on the aggregate</p> <p>ⓘ This channel has a default limit:</p> <ul style="list-style-type: none"> <li>▪ Lower warning limit: <b>1</b></li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Size Free	The free size
Size Free %	<p>The free size (%)</p> <p>ⓘ This channel has default limits:</p>

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Lower error limit: 10%</li> <li>▪ Lower warning limit: 25%</li> </ul>
State	<p>The aggregate status</p> <ul style="list-style-type: none"> <li>▪ Up status: Online, Onlining</li> <li>▪ Warning status: Offline, Offlining, Relocating, Unmounted, Restricted, Inconsistent</li> <li>▪ Down status: Failed</li> <li>▪ Unknown status: Channel Value Not Set, Unknown</li> </ul> <p> This channel is the primary channel by default.</p>

## More

### KNOWLEDGE BASE

What security features does PRTG include?

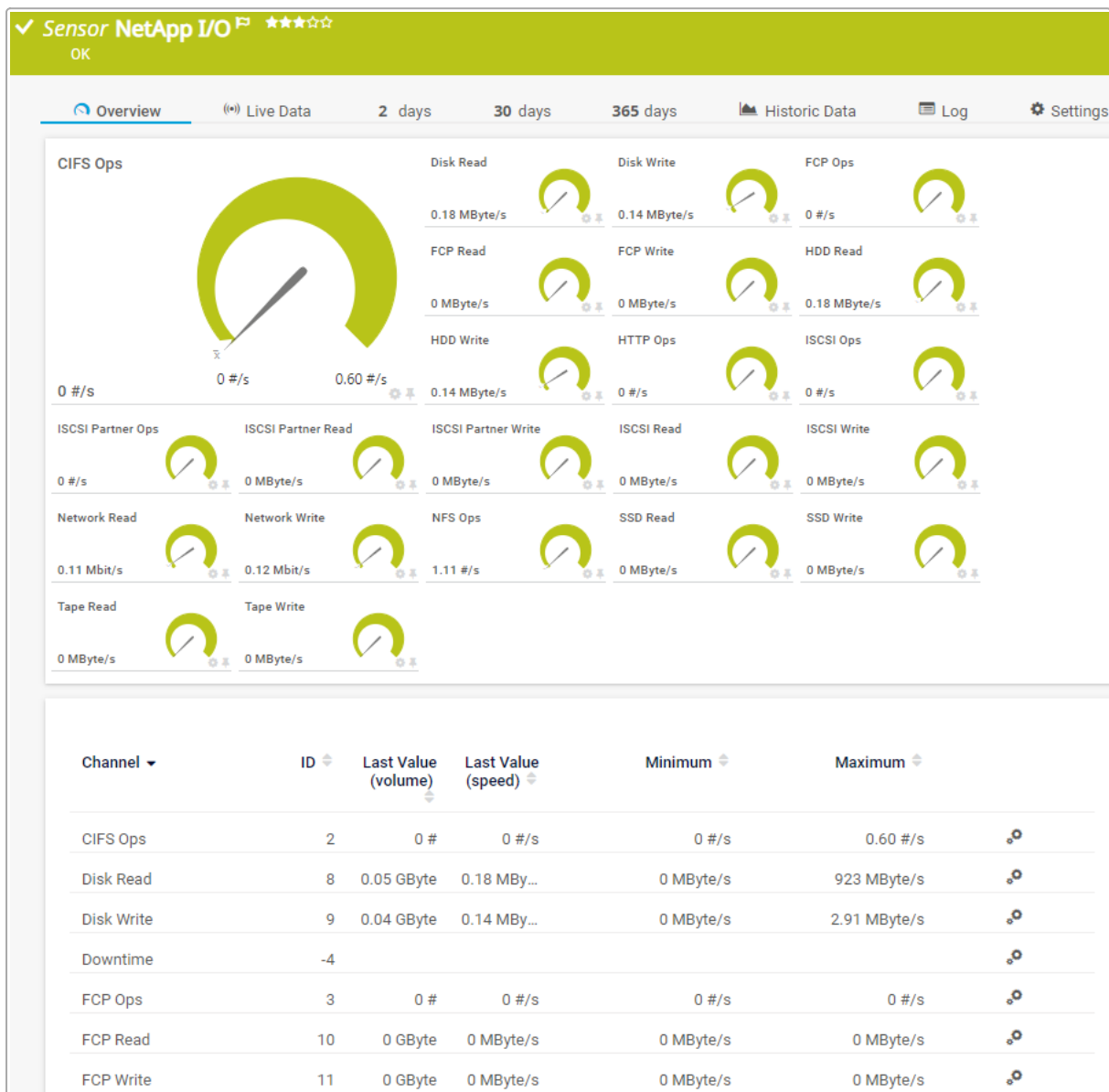
- <https://kb.paessler.com/en/topic/61108>

## 7.8.105 NetApp I/O Sensor

### IMPORTANT INFORMATION

This sensor supports NetApp cDOT as of version 8.3 or ONTAP from versions 9.0 to 9.12. If you use ONTAP as of version 9.11, we recommend that you use the [NetApp I/O v2](#) <sup>[1386]</sup> sensor. <sup>[1372]</sup>

The NetApp I/O sensor monitors input and output operations of a NetApp cDOT or ONTAP storage system accessing the application programming interface (API) via the Simple Object Access Protocol (SOAP).



NetApp I/O Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) <sup>[1383]</sup>.



## Sensor in Other Languages

- Dutch: NetApp I/O
- French: NetApp E/S
- German: NetApp I/O
- Japanese: NetApp I/O
- Portuguese: E/S NetApp
- Russian: Ввод-вывод NetApp
- Simplified Chinese: NetApp I/O
- Spanish: E/S NetApp

## Remarks

Consider the following [remarks](#) <sup>1379</sup> and requirements for this sensor:

Remark	Description
Enabled ONTAPI access	<p>The ONTAPI user account that you use with this sensor requires access to the <a href="#">DATA ONTAP API (ONTAPI)</a> so that the sensor can request data from it. The access is enabled by default.</p> <p><b>i</b> If access is disabled, locally use the following command on the cluster console to enable ONTAPI access for the user:</p> <pre>services web&gt; modify -vserver clusterd -name ontapi -enabled true</pre> <p>For this sensor, read-only user rights are sufficient for the ONTAPI user account that you use to access ONTAPI. Modify or add this user with a suitable role in the console under Cluster   ClusterX   Configuration   Security   Users</p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p><b>i</b> If the framework is missing, you cannot create this sensor.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
NetApp versions	<p>This sensor supports NetApp cDOT as of version 8.3 and NetApp ONTAP as of version 9.0.</p>
IPv6	<p>This sensor supports IPv6.</p>
Performance impact	<p>This sensor has a <a href="#">very low</a> performance impact.</p>

Remark	Description
Credentials	You can define NetApp API credentials (User Name and Password) in the <a href="#">credentials for Windows systems</a> settings of the parent device. This way, you do not need to individually enter credentials for each NetApp sensor that you add to the same device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cdot
- netapp
- ontap
- soap

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### NetApp Connection

#### NetApp Connection

**NetApp Credentials** ⓘ

Use explicit credentials

Use Windows credentials from parent device

---

**Port** ⓘ 443

---

**Connection Security** ⓘ

HTTP

HTTPS

---

**Timeout (Sec.)** ⓘ 60

NetApp Connection

Setting	Description
NetApp Credentials	<p>Specify which credentials you want to use to connect to the NetApp API:</p> <ul style="list-style-type: none"> <li>▪ Use explicit credentials: Use individual NetApp API credentials.</li> <li>▪ Use Windows credentials from parent device: Use the credentials (User Name and Password) in the <a href="#">parent device settings</a> in section Credentials for Windows Systems.</li> </ul> <p><b>i</b> Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you do not need to individually enter credentials for each NetApp sensor.</p>
User Name	<p><b>This setting is only visible if you select Use explicit credentials above.</b></p> <p>Enter a user name for access to the NetApp API. Enter a string.</p> <p><b>i</b> Read-only rights for this ONTAP user account are sufficient.</p>
Password	<p><b>This setting is only visible if you select Use explicit credentials above.</b></p> <p>Enter the password of the user for access to the NetApp API. Enter a string.</p>
Port	<p>Enter a port number on which you can access the NetApp API. Enter an integer. The default port is <b>443</b>.</p>
Connection Security	<p>Define if the connection to the NetApp API is Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured:</p> <ul style="list-style-type: none"> <li>▪ HTTP: Use an unsecured HTTP connection.</li> <li>▪ HTTPS: Use a secure connection to the defined port to send the query.</li> </ul>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

### NetApp Specific

**NetApp Specific** System Nodes **i** *mycompany000-01*

NetApp Specific

Setting	Description
System Nodes	The ID of the system node that this sensor monitors.

### Debug Options

**Debug Options**

**Result Handling** ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### Sensor Display

**Sensor Display**

**Primary Channel** ⓘ

Downtime


---

**Graph Type** ⓘ


Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are

Setting	Description
	<p>available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CIFS Ops	<p>The number of CIFS operations</p> <p><b>i</b> This channel is the primary channel by default.</p>
Disk Read	The disk read speed

Channel	Description
Disk Write	The disk write speed
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
FCP Ops	The number of FCP operations
FCP Read	The FCP read speed
FCP Write	The FCP write speed
HDD Read	The HDD read speed
HDD Write	The HDD write speed
HTTP Ops	The number of HTTP operations
ISCSI Ops	The number of iSCSI operations
ISCSI Partner Ops	The number of iSCSI partner operations
ISCSI Partner Read	The iSCSI partner read speed
ISCSI Partner Write	The iSCSI partner write speed
ISCSI Read	The iSCSI read speed
ISCSI Write	The iSCSI write speed
Network Read	The network read speed
Network Write	The network write speed
NFS Ops	The number of NFS operations
SSD Read	The SSD read speed
SSD Write	The SSD write speed
Tape Read	The tape read speed

Channel	Description
Tape Write	The tape write speed

## More

### KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

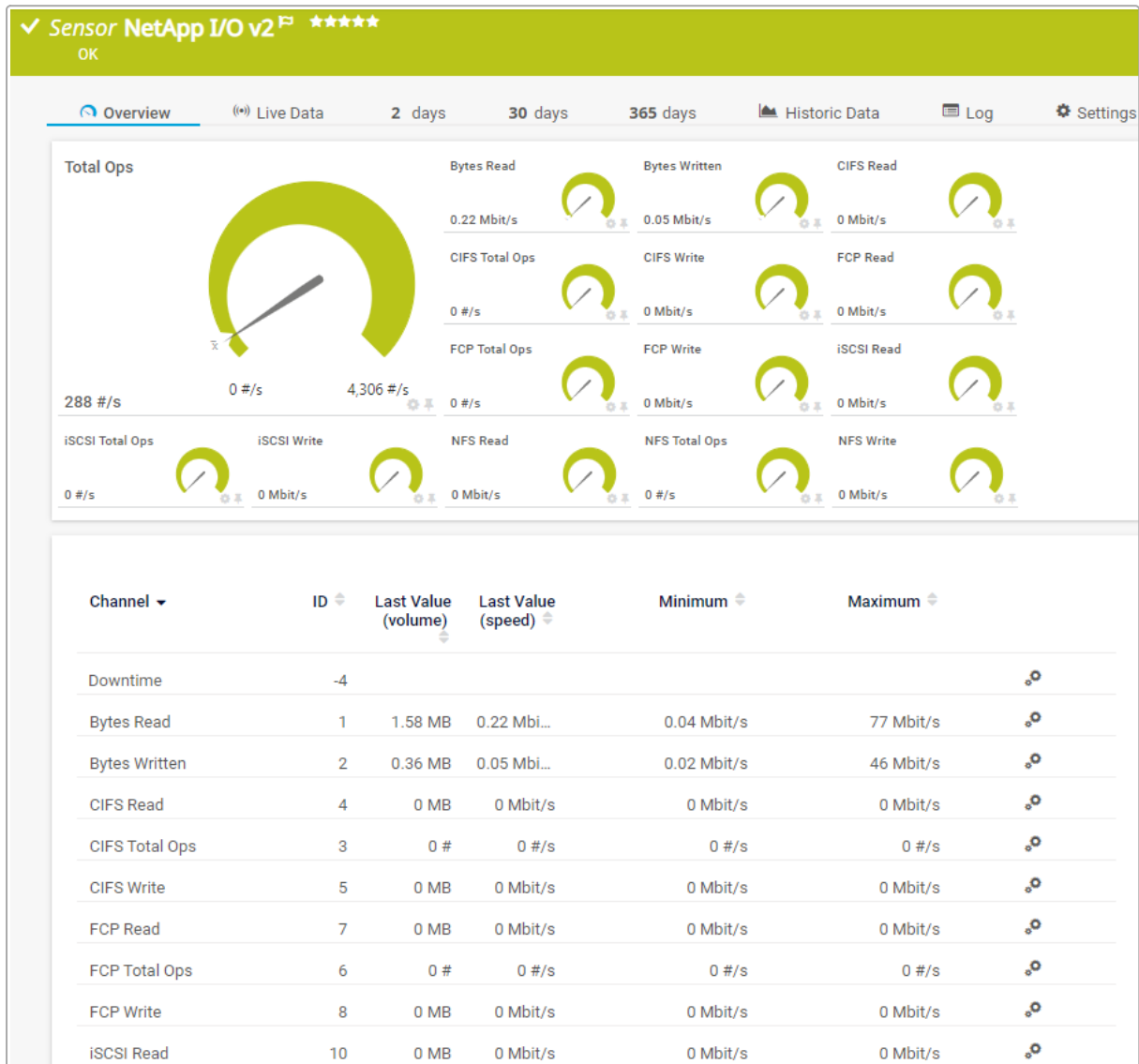
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.106 NetApp I/O v2 Sensor

The NetApp I/O v2 sensor monitors input and output operations of a NetApp storage system via the Representational State Transfer (REST) application programming interface (API) using ONTAP as of version 9.11.

**i** This sensor was converted to a new framework so that it will continue to function after the changes of the ONTAP REST API.



NetApp I/O v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1390]</sup>.

### Sensor in Other Languages

- Dutch: NetApp I/O v2
- French: NetApp E/S v2
- German: NetApp I/O v2



- Japanese: NetApp I/O v2
- Portuguese: E/S NetApp v2
- Russian: Ввод-вывод NetApp v2
- Simplified Chinese: NetApp 输入/输出 v2
- Spanish: E/S NetApp v2

## Remarks

Consider the following [remarks](#)<sup>[1387]</sup> and requirements for this sensor:

Remark	Description
Credentials for NetApp	This sensor requires an <a href="#">ONTAP System Manager</a> user account with the role <a href="#">readonly</a> and with access to the <a href="#">HTTP</a> application with <a href="#">Password</a> authentication.
Permissions for the ONTAP REST API	<p>This sensor requires permissions for the <a href="#">ONTAP REST API</a>.</p> <p><b>i</b> This sensor requires the role <a href="#">readonly</a> with the following permissions for the <a href="#">ONTAP REST API</a>:</p> <p>Access level <a href="#">Read-Only</a>:</p> <ul style="list-style-type: none"> <li>▪ /api</li> <li>▪ /api/security/audit/destinations</li> </ul> <p>Access level <a href="#">Read/Write</a>:</p> <ul style="list-style-type: none"> <li>▪ /api/security/authentication/password</li> </ul> <p>Access level <a href="#">None</a>:</p> <ul style="list-style-type: none"> <li>▪ /api/security</li> </ul>
NetApp versions	This sensor requires ONTAP as of version 9.11. If you want to use NetApp cDOT as of version 8.3 or ONTAP from version 9.0 to version 9.10, use the <a href="#">NetApp I/O</a> <sup>[1378]</sup> sensor.
Credentials	This sensor requires credentials for NetApp.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">1 minute</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- netapp
- ontap
- rest

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## NetApp Specific

### NetApp Specific

**Node Name** ⓘ mycompany000-01

NetApp Specific

Setting	Description
Node Name	The name of the node that this sensor monitors.

## Sensor Display




### Sensor Display

**Primary Channel** ⓘ Downtime

---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display


Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><a href="#">This setting is only visible if you select</a> Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**


**Result Handling** 
 Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Bytes Read	The number of bytes read
Bytes Written	The number of bytes written
CIFS Read	The CIFS read speed
CIFS Total Ops	<p>The number of CIFS operations</p> <p><b>i</b> This channel is the primary channel by default.</p>
CIFS Write	The CIFS write speed
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
FCP Read	The FCP read speed
FCP Total Ops	The number of FCP operations
FCP Write	The FCP write speed

Channel	Description
iSCSI Read	The iSCSI read speed
iSCSI Total Ops	The number of iSCSI operations
iSCSI Write	The iSCSI read speed
NFS Read	The NFS read speed
NFS Total Ops	The number of NFS operations
NFS Write	The NFS write speed
Total Ops	The number of operations

## More

### KNOWLEDGE BASE

What security features does PRTG include?

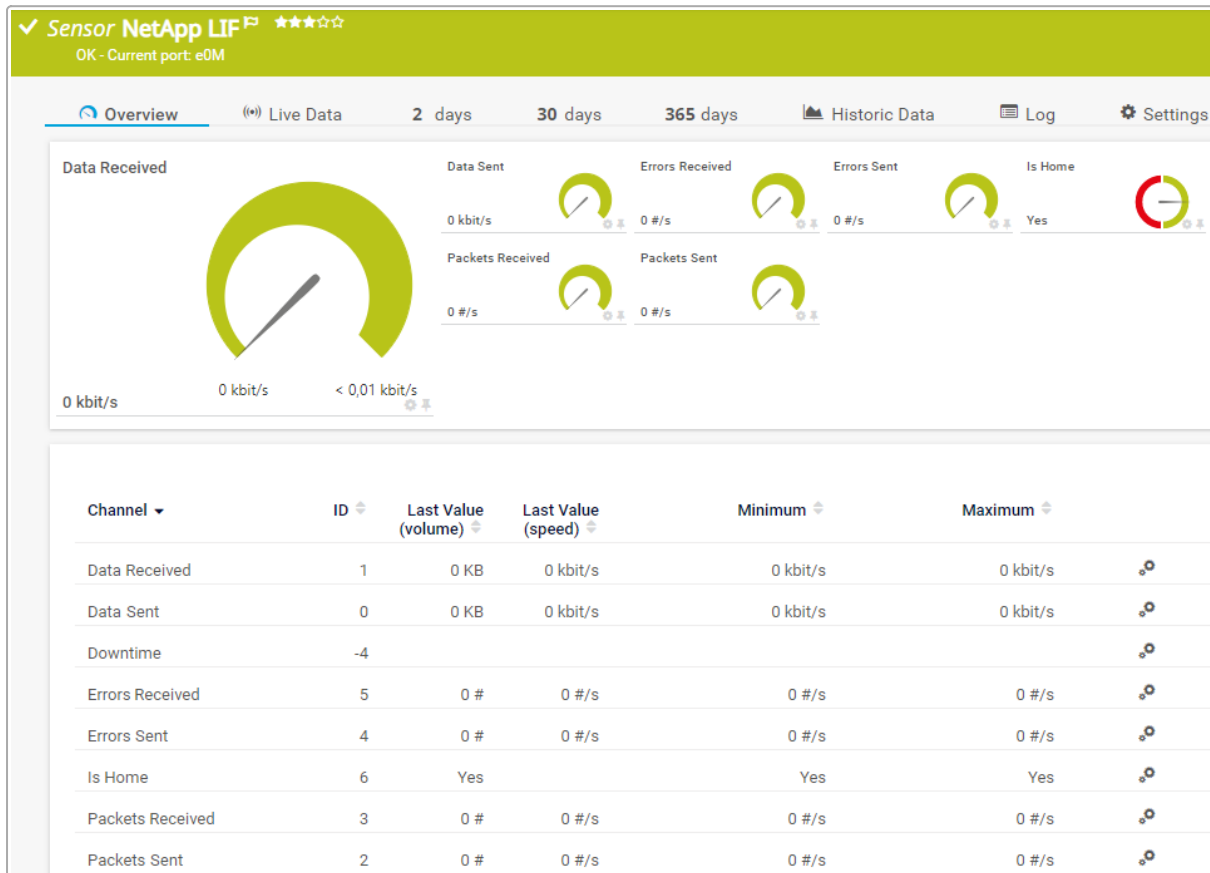
- <https://kb.paessler.com/en/topic/61108>

## 7.8.107 NetApp LIF Sensor

### IMPORTANT INFORMATION

This sensor supports NetApp cDOT as of version 8.3 or ONTAP from versions 9.0 to 9.12. If you use ONTAP as of version 9.10, we recommend that you use the [NetApp LIF v2<sup>\[1372\]</sup>](#) sensor.

The NetApp LIF sensor monitors logical interfaces of a NetApp cDOT or ONTAP cluster accessing the application programming interface (API) via the Simple Object Access Protocol (SOAP).



NetApp LIF Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List<sup>\[1397\]</sup>](#).

### Sensor in Other Languages

- Dutch: NetApp LIF
- French: NetApp LIF
- German: NetApp LIF
- Japanese: NetApp LIF
- Portuguese: LIF NetApp

- Russian: LIF NetApp
- Simplified Chinese: NetApp LIF
- Spanish: LIF NetApp

## Remarks

Consider the following [remarks](#)<sup>1393</sup> and requirements for this sensor:

Remark	Description
Enabled ONTAPI access	<p>The ONTAPI user account that you use with this sensor requires access to the <a href="#">DATA ONTAP API (ONTAPI)</a> so that the sensor can request data from it. The access is enabled by default.</p> <p><b>i</b> If access is disabled, locally use the following command on the cluster console to enable ONTAPI access for the user:</p> <pre>services web&gt; modify -vserver clusterd -name ontapi -enabled true</pre> <p>For this sensor, read-only user rights are sufficient for the ONTAPI user account that you use to access ONTAPI. Modify or add this user with a suitable role in the console under Cluster   ClusterX   Configuration   Security   Users</p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p><b>i</b> If the framework is missing, you cannot create this sensor.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
NetApp versions	<p>This sensor supports NetApp cDOT as of version 8.3 and NetApp ONTAP as of version 9.0.</p>
IPv6	<p>This sensor supports IPv6.</p>
Performance impact	<p>This sensor has a <a href="#">very low</a> performance impact.</p>
Credentials	<p>You can define NetApp API credentials (User Name and Password) in the <a href="#">credentials for Windows systems</a> settings of the parent device. This way, you do not need to individually enter credentials for each NetApp sensor that you add to the same device.</p>
Lookups	<p>This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.</p>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cdot
- netapp
- ontap
- soap

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## NetApp Connection

### NetApp Connection

**NetApp Credentials** ⓘ  Use explicit credentials  
 Use Windows credentials from parent device

**Port** ⓘ

**Connection Security** ⓘ  HTTP  
 HTTPS

**Timeout (Sec.)** ⓘ

NetApp Connection

Setting	Description
NetApp Credentials	Specify which credentials you want to use to connect to the NetApp API: <ul style="list-style-type: none"> <li>▪ Use explicit credentials: Use individual NetApp API credentials.</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>Use Windows credentials from parent device: Use the credentials (User Name and Password) in the <a href="#">parent device settings</a> in section Credentials for Windows Systems.</li> <li><b>i</b> Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you do not need to individually enter credentials for each NetApp sensor.</li> </ul>
User Name	<p>This setting is only visible if you select Use explicit credentials <a href="#">above</a>.</p> <p>Enter a user name for access to the NetApp API. Enter a string.</p> <p><b>i</b> Read-only rights for this ONTAP user account are sufficient.</p>
Password	<p>This setting is only visible if you select Use explicit credentials <a href="#">above</a>.</p> <p>Enter the password of the user for access to the NetApp API. Enter a string.</p>
Port	<p>Enter a port number on which you can access the NetApp API. Enter an integer. The default port is <b>443</b>.</p>
Connection Security	<p>Define if the connection to the NetApp API is Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured:</p> <ul style="list-style-type: none"> <li>HTTP: Use an unsecured HTTP connection.</li> <li>HTTPS: Use a secure connection to the defined port to send the query.</li> </ul>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

### NetApp Specific

**NetApp Specific** LIFs **i** *LIF NetApp-Cluster-01*

NetApp Specific

Setting	Description
LIFs	The ID of the LIF that this sensor monitors.

## Debug Options

**Debug Options**

**Result Handling** ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].Data.txt and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**


**Primary Channel** ⓘ Downtime

---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Data Received	<p>The data received</p> <p> This channel is the primary channel by default.</p>
Data Sent	The data sent
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Errors Received	The number of errors received
Errors Sent	The number of errors sent

Channel	Description
Is Home	If the LIF is on the home port <ul style="list-style-type: none"><li>▪ Up status: Yes</li><li>▪ Down status: No</li></ul>
Packets Received	The number of packets received
Packets Sent	The number of packets sent

## More

### KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

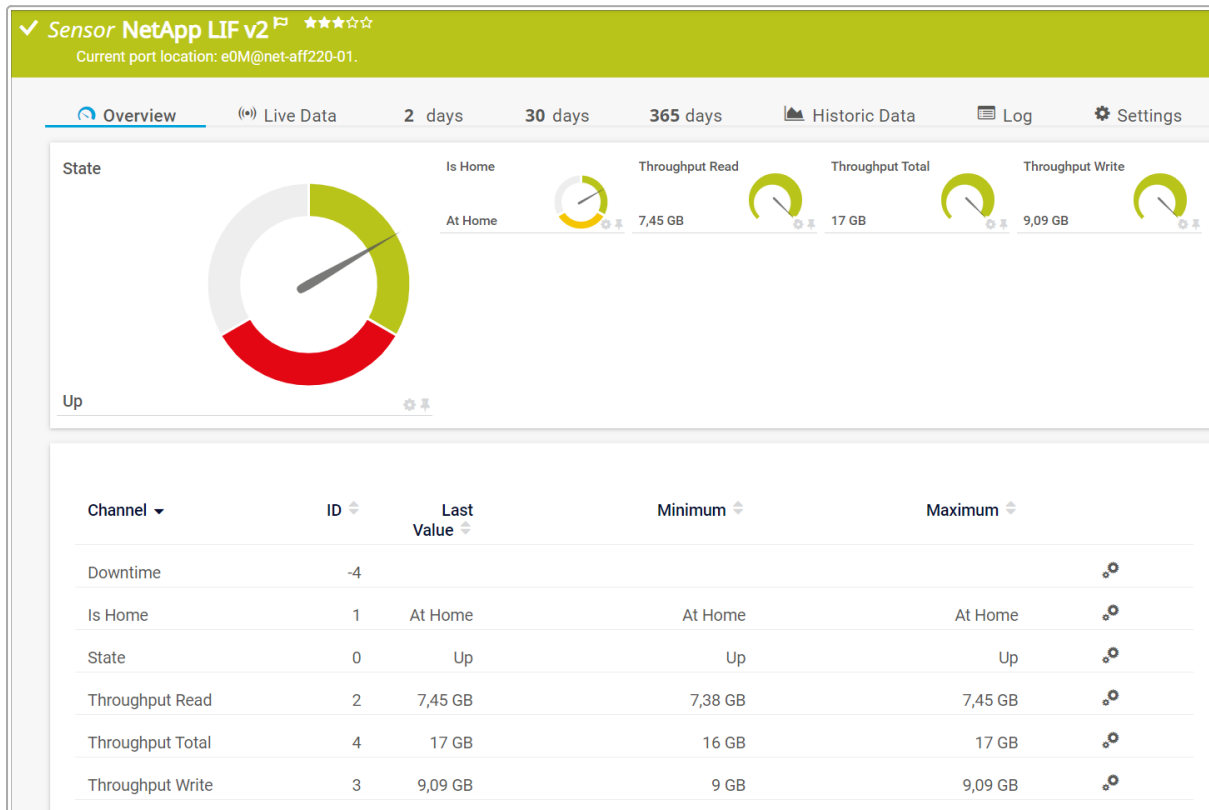
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.108 NetApp LIF v2 Sensor

The NetApp LIF v2 sensor monitors a logical interface (LIF) of a NetApp storage system via the Representational State Transfer (REST) application programming interface (API) using ONTAP as of version 9.10.

**i** This sensor was converted to a new framework so that it will continue to function after the changes of the ONTAP REST API.



NetApp LIF v2 Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1403]</sup>.

### Sensor in Other Languages

- Dutch: NetApp LIF v2
- French: NetApp LIF v2
- German: NetApp LIF v2
- Japanese: NetApp LIF v2
- Portuguese: LIF NetApp v2
- Russian: LIF NetApp v2
- Simplified Chinese: NetApp LIF v2
- Spanish: LIF NetApp v2

## Remarks

Consider the following [remarks](#)<sup>[1400]</sup> and requirements for this sensor:

Remark	Description
Credentials for NetApp	This sensor requires an <a href="#">ONTAP System Manager</a> user account with the role <a href="#">readonly</a> and with access to the <a href="#">HTTP</a> application with <a href="#">Password</a> authentication.
Permissions for the ONTAP REST API	<p>This sensor requires permissions for the <a href="#">ONTAP REST API</a>.</p> <p> This sensor requires the role <a href="#">readonly</a> with the following permissions for the <a href="#">ONTAP REST API</a>:</p> <p>Access level <a href="#">Read-Only</a>:</p> <ul style="list-style-type: none"> <li>▫ /api</li> <li>▫ /api/security/audit/destinations</li> </ul> <p>Access level <a href="#">Read/Write</a>:</p> <ul style="list-style-type: none"> <li>▫ /api/security/authentication/password</li> </ul> <p>Access level <a href="#">None</a>:</p> <ul style="list-style-type: none"> <li>▫ /api/security</li> </ul>
NetApp versions	This sensor requires ONTAP as of version 9.10. If you want to use NetApp cDOT as of version 8.3 or ONTAP from version 9.0 to version 9.9, use the <a href="#">NetApp LIF</a> <sup>[1392]</sup> sensor.
Credentials	This sensor requires credentials for NetApp.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">1 minute</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- lif
- netapp
- ontap
- rest

■ For more information about basic sensor settings, see section [Sensor Settings](#) 667.

## NetApp Specific

### NetApp Specific

**Name** ⓘ *cluster\_mgmt*

**Home Node Name** ⓘ *net-aff220-01*

**Scope** ⓘ *cluster*

NetApp Specific

Setting	Description
Name	The name of the LIF that this sensor monitors.

Setting	Description
Home Node Name	The home node name of the LIF that this sensor monitors.
Scope	The scope of the LIF that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>



## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Is Home	If the LIF is on the home port

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Up status: At Home</li> <li>▪ Down status: Not At Home</li> <li>▪ Unknown status: Channel Value Not Set</li> </ul>
State	<p>The LIF status</p> <ul style="list-style-type: none"> <li>▪ Up status: Up</li> <li>▪ Down status: Down</li> <li>▪ Unknown status: Channel Value Not Set</li> </ul> <p> This channel is the primary channel by default.</p>
Throughput Read	The number of bytes read
Throughput Total	The total number of bytes read and written
Throughput Write	The number of bytes written

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

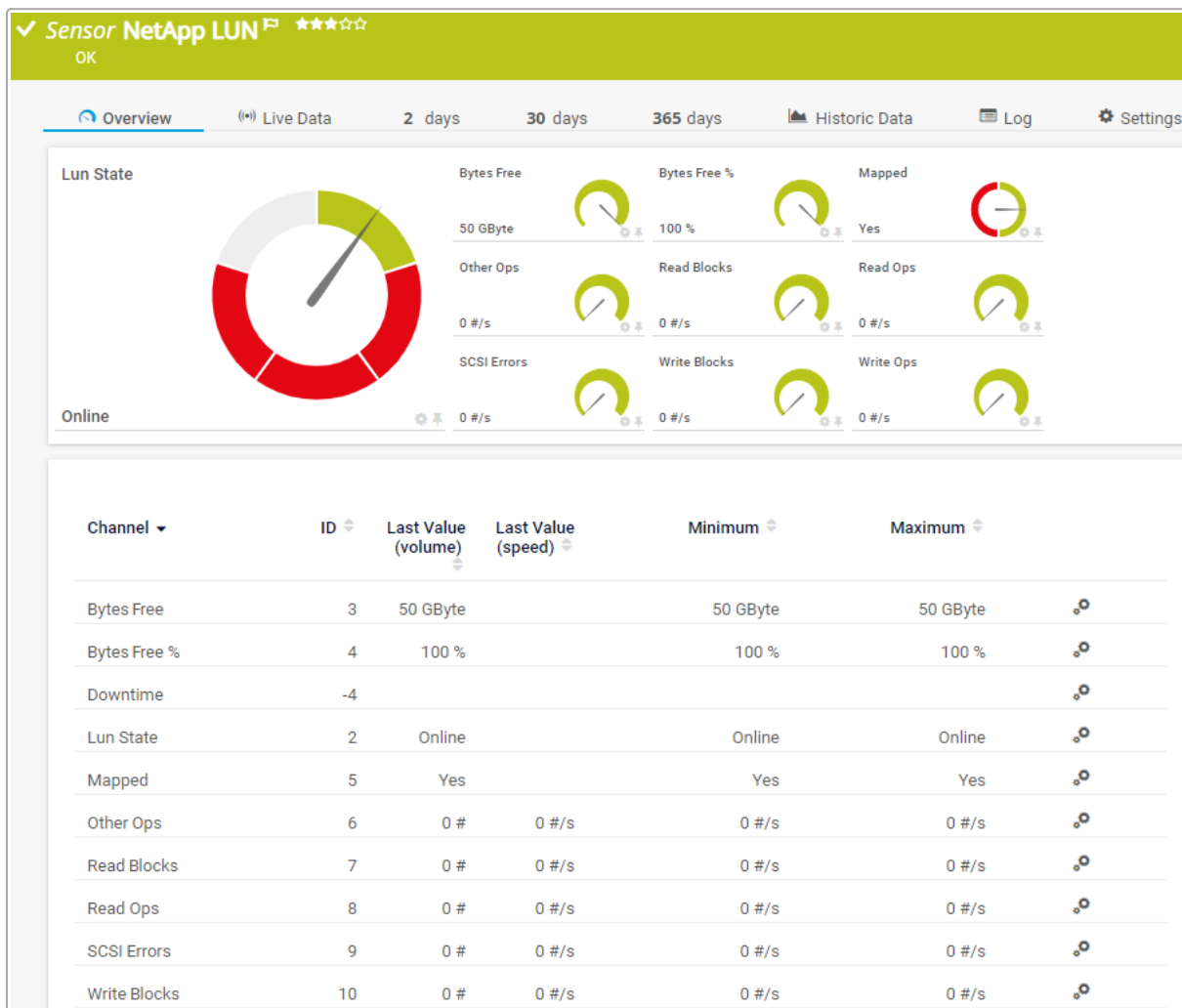
- <https://kb.paessler.com/en/topic/61108>

## 7.8.109 NetApp LUN Sensor

### IMPORTANT INFORMATION

This sensor supports NetApp cDOT as of version 8.3 or ONTAP from versions 9.0 to 9.12. If you use ONTAP as of version 9.6, we recommend that you use the [NetApp LUN v2](#) sensor.

The NetApp LUN sensor monitors the logical unit number (LUN) of a NetApp cDOT or ONTAP storage system accessing the application programming interface (API) via the Simple Object Access Protocol (SOAP).



NetApp LUN Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: NetApp LUN
- French: NetApp LUN

- German: NetApp LUN
- Japanese: NetApp LUN
- Portuguese: LUN NetApp
- Russian: LUN NetApp
- Simplified Chinese: NetApp LUN
- Spanish: LUN NetApp

## Remarks

Consider the following [remarks](#) <sup>[1406]</sup> and requirements for this sensor:

Remark	Description
Enabled ONTAPI access	<p>The ONTAPI user account that you use with this sensor requires access to the <a href="#">DATA ONTAP API (ONTAPI)</a> so that the sensor can request data from it. The access is enabled by default.</p> <p><b>i</b> If access is disabled, locally use the following command on the cluster console to enable ONTAPI access for the user:</p> <pre>services web&gt; modify -vserver clusterd -name ontapi -enabled true</pre> <p>For this sensor, read-only user rights are sufficient for the ONTAPI user account that you use to access ONTAPI. Modify or add this user with a suitable role in the console under Cluster   ClusterX   Configuration   Security   Users</p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p><b>i</b> If the framework is missing, you cannot create this sensor.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
NetApp versions	<p>This sensor supports NetApp cDOT as of version 8.3 and NetApp ONTAP as of version 9.0.</p>
IPv6	<p>This sensor supports IPv6.</p>
Performance impact	<p>This sensor has a <a href="#">very low</a> performance impact.</p>
Credentials	<p>You can define NetApp API credentials (User Name and Password) in the <a href="#">credentials for Windows systems</a> settings of the parent device. This way, you do not need to individually enter credentials for each NetApp sensor that you add to the same device.</p>

Remark	Description
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cdot
- netapp
- ontap
- soap

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### NetApp Connection

#### NetApp Connection

**NetApp Credentials** ⓘ  Use explicit credentials  
 Use Windows credentials from parent device

**Port** ⓘ

**Connection Security** ⓘ  HTTP  
 HTTPS

**Timeout (Sec.)** ⓘ

NetApp Connection

Setting	Description
NetApp Credentials	<p>Specify which credentials you want to use to connect to the NetApp API:</p> <ul style="list-style-type: none"> <li>▪ Use explicit credentials: Use individual NetApp API credentials.</li> <li>▪ Use Windows credentials from parent device: Use the credentials (User Name and Password) in the <a href="#">parent device settings</a> in section Credentials for Windows Systems.</li> </ul> <p><b>i</b> Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you do not need to individually enter credentials for each NetApp sensor.</p>
User Name	<p><b>This setting is only visible if you select Use explicit credentials above.</b></p> <p>Enter a user name for access to the NetApp API. Enter a string.</p> <p><b>i</b> Read-only rights for this ONTAP user account are sufficient.</p>
Password	<p><b>This setting is only visible if you select Use explicit credentials above.</b></p> <p>Enter the password of the user for access to the NetApp API. Enter a string.</p>
Port	<p>Enter a port number on which you can access the NetApp API. Enter an integer. The default port is <b>443</b>.</p>
Connection Security	<p>Define if the connection to the NetApp API is Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured:</p> <ul style="list-style-type: none"> <li>▪ HTTP: Use an unsecured HTTP connection.</li> <li>▪ HTTPS: Use a secure connection to the defined port to send the query.</li> </ul>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

### NetApp Specific

**NetApp Specific** LUNs **i** LUN /vol/LUN\_vol/LUN

NetApp Specific

Setting	Description
LUNs	The ID of the LUN that this sensor monitors.

### Debug Options

**Debug Options**

**Result Handling** ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].Data.txt and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### Sensor Display

**Sensor Display**

**Primary Channel** ⓘ Downtime


---

**Graph Type** ⓘ


Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are

Setting	Description
	<p>available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.


 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Bytes Free	The free space
Bytes Free %	The free bytes (%)



Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
LUN State	<p>The LUN status</p> <ul style="list-style-type: none"> <li>▪ Up status: Online</li> <li>▪ Down status: LUN has been automatically taken offline due to a media error on the associated foreign LUN, LUN has been automatically taken offline due to an NVRAM failure, LUN has been automatically taken offline due to insufficient space</li> <li>▪ Unknown status: LUN is administratively offline or a more detailed offline reason is not available</li> </ul> <p> This channel is the primary channel by default.</p>
Mapped	<p>If the LUN is mapped</p> <ul style="list-style-type: none"> <li>▪ Up status: Yes</li> <li>▪ Down status: No</li> </ul>
Other Ops	The other operations
Read Blocks	The number of read blocks
Read Ops	The number of disk read operations
SCSI Errors	The number of SCSI errors
Write Blocks	The number of write blocks
Write Ops	The number of disk write operations

## More

### KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

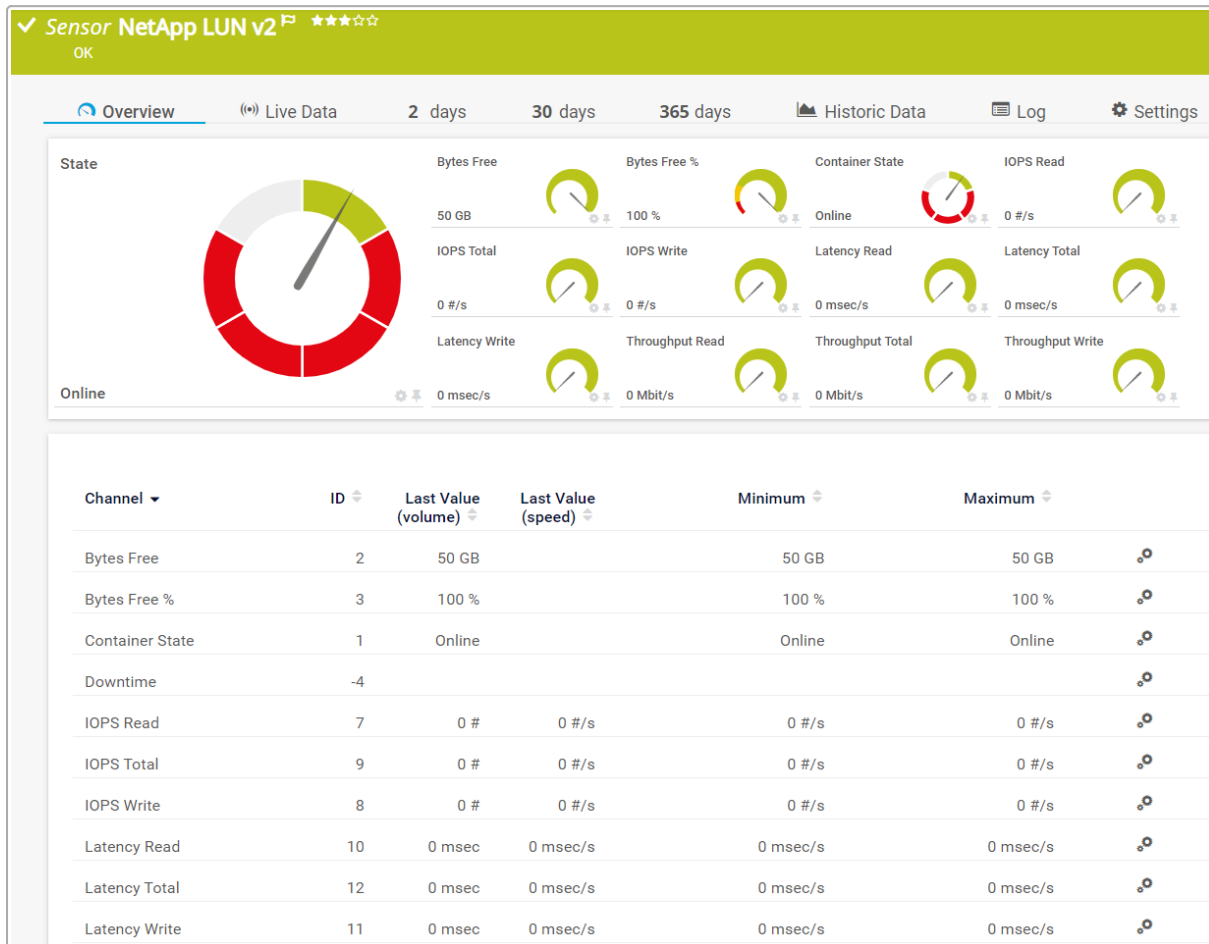
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.110 NetApp LUN v2 Sensor

The NetApp LUN v2 sensor monitors the logical unit number (LUN) of a NetApp storage system via the Representational State Transfer (REST) application programming interface (API) using ONTAP as of version 9.6.

**i** This sensor was converted to a new framework so that it will continue to function after the changes of the ONTAP REST API.



NetApp LUN v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1416</sup>.

### Sensor in Other Languages

- Dutch: NetApp LUN v2
- French: NetApp LUN v2
- German: NetApp LUN v2
- Japanese: NetApp LUN v2
- Portuguese: LUN NetApp v2
- Russian: LUN NetApp v2
- Simplified Chinese: NetApp LUN v2

- Spanish: LUN NetApp v2

## Remarks

Consider the following [remarks](#)<sup>[1413]</sup> and requirements for this sensor:

Remark	Description
Credentials for NetApp	This sensor requires an <a href="#">ONTAP System Manager</a> user account with the role <a href="#">readonly</a> and with access to the <a href="#">HTTP</a> application with <a href="#">Password</a> authentication.
Permissions for the ONTAP REST API	<p>This sensor requires permissions for the <a href="#">ONTAP REST API</a>.</p> <p> This sensor requires the role <a href="#">readonly</a> with the following permissions for the <a href="#">ONTAP REST API</a>:</p> <p>Access level <a href="#">Read-Only</a>:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">/api</a></li> <li>▪ <a href="#">/api/security/audit/destinations</a></li> </ul> <p>Access level <a href="#">Read/Write</a>:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">/api/security/authentication/password</a></li> </ul> <p>Access level <a href="#">None</a>:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">/api/security</a></li> </ul>
NetApp versions	This sensor requires ONTAP as of version 9.6. If you want to use NetApp cDOT as of version 8.3 or ONTAP from version 9.0 to version 9.5, use the <a href="#">NetApp LUN</a> <sup>[1405]</sup> sensor.
Credentials	This sensor requires credentials for NetApp.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">1 minute</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- lun
- netapp
- ontap
- rest

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## NetApp Specific

### NetApp Specific

**LUN Path Name** ⓘ /vol/LUN/LUN

---

**Operating System Type** ⓘ windows\_2008

---

**Description** ⓘ LUN

NetApp Specific

Setting	Description
LUN Path Name	The path name of the LUN that this sensor monitors.
Operating System Type	The operating system type of the LUN that this sensor monitors.
Description	The description of the LUN that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Bytes Free	<p>The free space</p> <p>ⓘ This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: <a href="#">10%</a></li> <li>▪ Lower warning limit: <a href="#">25%</a></li> </ul>
Bytes Free %	The free space (%)
Container State	<p>The container status</p> <ul style="list-style-type: none"> <li>▪ Up status: Online</li> <li>▪ Down status: Aggregate Offline, Volume Offline, Error</li> <li>▪ Unknown status: Channel Value Not Set</li> </ul>

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
IOPS Read	The number of IOPS read
IOPS Total	The total number of IOPS
IOPS Write	The number of IOPS written
Latency Read	The read latency
Latency Total	The total latency
Latency Write	The write latency
State	<p>The LUN status</p> <ul style="list-style-type: none"> <li>▪ Up status: Online</li> <li>▪ Down status: Offline, NVRAM Failure, Space Error, Foreign LUN Error</li> <li>▪ Unknown status: Channel Value Not Set</li> </ul> <p> This channel is the primary channel by default.</p>
Throughput Read	The number of bytes read
Throughput Total	The total number of bytes read and written
Throughput Write	The number of bytes written

## More

### KNOWLEDGE BASE

What security features does PRTG include?

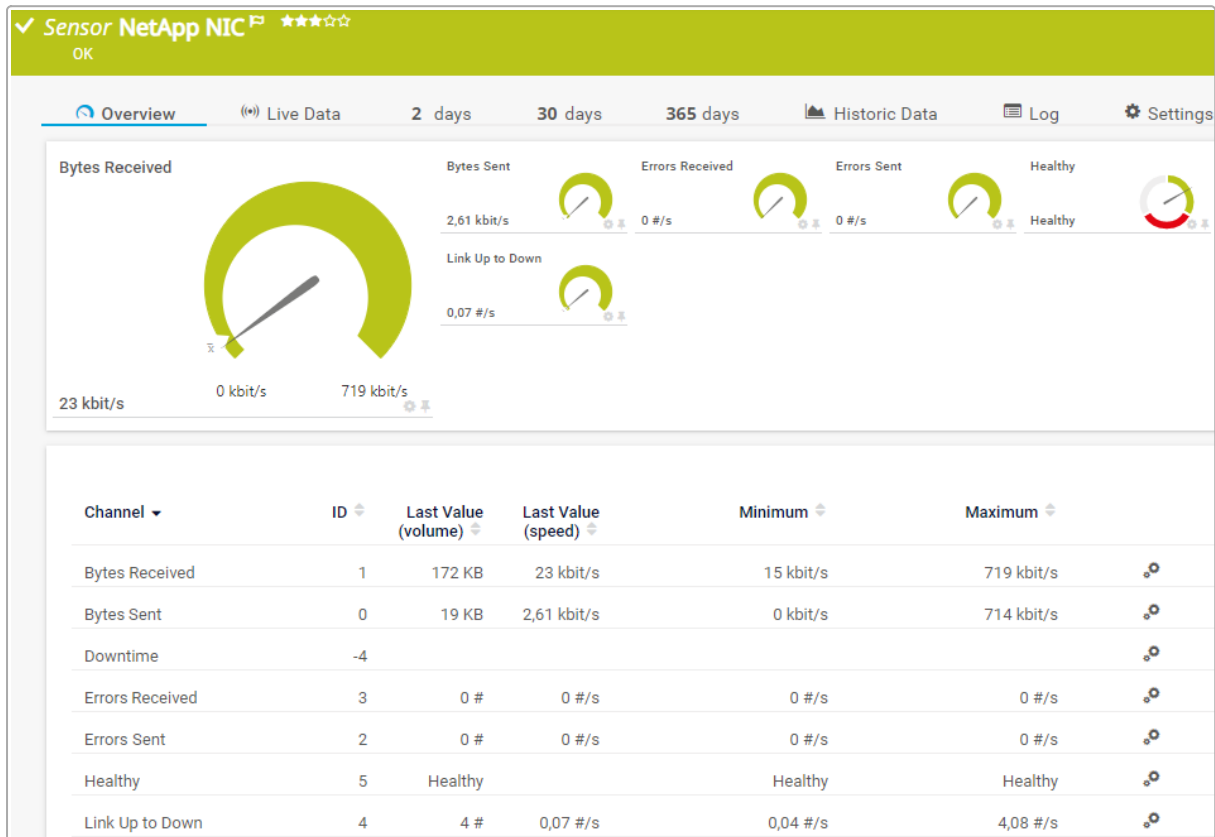
- <https://kb.paessler.com/en/topic/61108>

## 7.8.111 NetApp NIC Sensor

### IMPORTANT INFORMATION

This sensor supports NetApp cDOT as of version 8.3 or ONTAP from versions 9.0 to 9.12. If you use ONTAP as of version 9.10, we recommend that you use the [NetApp NIC v2](#) <sup>[1425]</sup> sensor.

The NetApp NIC sensor monitors the network interface card (NIC) of a NetApp cDOT or ONTAP cluster accessing the application programming interface (API) via the Simple Object Access Protocol (SOAP).



NetApp NIC Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) <sup>[1423]</sup>.

### Sensor in Other Languages

- Dutch: NetApp NIC
- French: NetApp NIC
- German: NetApp NIC
- Japanese: NetApp NIC
- Portuguese: NIC NetApp
- Russian: NIC NetApp



- Simplified Chinese: NetApp NIC
- Spanish: NIC NetApp

## Remarks

Consider the following [remarks](#)<sup>1419</sup> and requirements for this sensor:

Remark	Description
Enabled ONTAPI access	<p>The ONTAPI user account that you use with this sensor requires access to the <a href="#">DATA ONTAP API (ONTAPI)</a> so that the sensor can request data from it. The access is enabled by default.</p> <p><b>i</b> If access is disabled, locally use the following command on the cluster console to enable ONTAPI access for the user:</p> <pre>services web&gt; modify -vserver clusterd -name ontapi -enabled true</pre> <p>For this sensor, read-only user rights are sufficient for the ONTAPI user account that you use to access ONTAPI. Modify or add this user with a suitable role in the console under Cluster   ClusterX   Configuration   Security   Users</p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p><b>i</b> If the framework is missing, you cannot create this sensor.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
NetApp versions	<p>This sensor supports NetApp cDOT as of version 8.3 and NetApp ONTAP as of version 9.0.</p>
IPv6	<p>This sensor supports IPv6.</p>
Performance impact	<p>This sensor has a <a href="#">very low</a> performance impact.</p>
Credentials	<p>You can define NetApp API credentials (User Name and Password) in the <a href="#">credentials for Windows systems</a> settings of the parent device. This way, you do not need to individually enter credentials for each NetApp sensor that you add to the same device.</p>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cdot
- netapp
- ontap
- soap

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## NetApp Connection

### NetApp Connection

**NetApp Credentials** ⓘ  Use explicit credentials  
 Use Windows credentials from parent device

**Port** ⓘ

**Connection Security** ⓘ  HTTP  
 HTTPS

**Timeout (Sec.)** ⓘ

NetApp Connection

Setting	Description
NetApp Credentials	Specify which credentials you want to use to connect to the NetApp API: <ul style="list-style-type: none"> <li>▪ Use explicit credentials: Use individual NetApp API credentials.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Use Windows credentials from parent device: Use the credentials (User Name and Password) in the <a href="#">parent device settings</a> in section Credentials for Windows Systems.</li> </ul> <p><b>i</b> Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you do not need to individually enter credentials for each NetApp sensor.</p>
User Name	<p>This setting is only visible if you select Use explicit credentials <a href="#">above</a>.</p> <p>Enter a user name for access to the NetApp API. Enter a string.</p> <p><b>i</b> Read-only rights for this ONTAP user account are sufficient.</p>
Password	<p>This setting is only visible if you select Use explicit credentials <a href="#">above</a>.</p> <p>Enter the password of the user for access to the NetApp API. Enter a string.</p>
Port	<p>Enter a port number on which you can access the NetApp API. Enter an integer. The default port is <a href="#">443</a>.</p>
Connection Security	<p>Define if the connection to the NetApp API is Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured:</p> <ul style="list-style-type: none"> <li>HTTP: Use an unsecured HTTP connection.</li> <li>HTTPS: Use a secure connection to the defined port to send the query.</li> </ul>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <a href="#">900</a> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

### NetApp Specific

NetApp Specific
NICs **i** NIC NetApp01

NetApp Specific

Setting	Description
NICs	The ID of the NIC that this sensor monitors.

## Debug Options

**Debug Options**

**Result Handling** ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].Data.txt and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**


**Primary Channel** ⓘ Downtime

---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>


Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Bytes Received	The number of bytes received  This channel is the primary channel by default.
Bytes Sent	The number of bytes sent
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Errors Received	The number of errors received
Errors Sent	The number of errors sent

Channel	Description
Healthy	If the system is healthy <ul style="list-style-type: none"><li>▪ Up status: Healthy</li><li>▪ Down status: Unhealthy</li><li>▪ Unknown status: Not Available</li></ul>
Link Up to Down	The number of up to down links

## More

### ■ KNOWLEDGE BASE

What are beta sensors and how can I use them?

- <https://kb.paessler.com/en/topic/88697>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

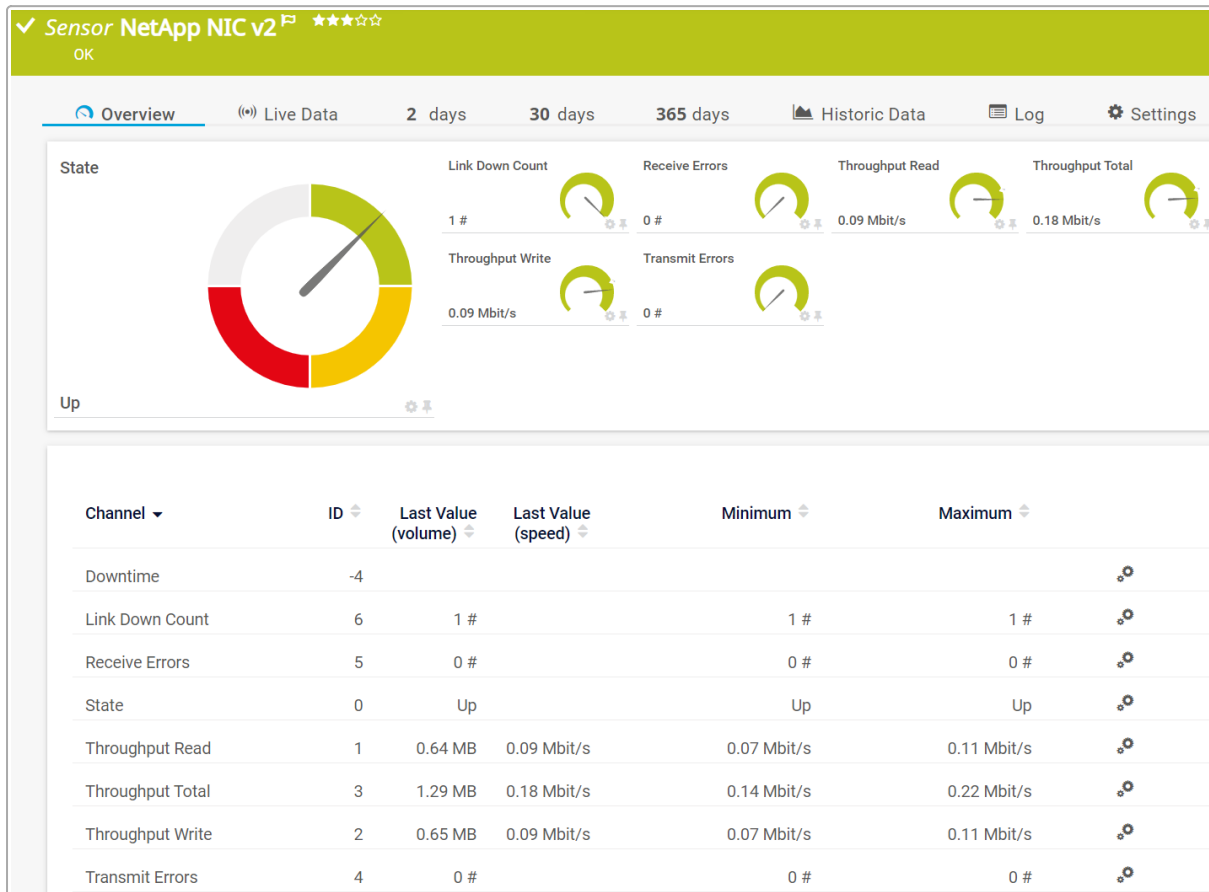
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.112 NetApp NIC v2 Sensor

The NetApp NIC v2 sensor monitors a network interface card (NIC) of a NetApp storage system via the Representational State Transfer (REST) application programming interface (API) using ONTAP as of version 9.10.

**i** This sensor was converted to a new framework so that it will continue to function after the changes of the ONTAP REST API.



NetApp NIC v2 Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) <sup>[1429]</sup>.

### Sensor in Other Languages

- Dutch: NetApp NIC v2
- French: NetApp NIC v2
- German: NetApp NIC v2
- Japanese: NetApp NIC v2
- Portuguese: NIC NetApp v2
- Russian: NIC NetApp v2
- Simplified Chinese: NetApp NIC v2
- Spanish: NIC NetApp v2

## Remarks

Consider the following [remarks](#)<sup>[1426]</sup> and requirements for this sensor:

Remark	Description
Credentials for NetApp	This sensor requires an <a href="#">ONTAP System Manager</a> user account with the role <a href="#">readonly</a> and with access to the <a href="#">HTTP</a> application with <a href="#">Password</a> authentication.
Permissions for the ONTAP REST API	<p>This sensor requires permissions for the <a href="#">ONTAP REST API</a>.</p> <p> This sensor requires the role <a href="#">readonly</a> with the following permissions for the <a href="#">ONTAP REST API</a>:</p> <p>Access level <a href="#">Read-Only</a>:</p> <ul style="list-style-type: none"> <li>▫ /api</li> <li>▫ /api/security/audit/destinations</li> </ul> <p>Access level <a href="#">Read/Write</a>:</p> <ul style="list-style-type: none"> <li>▫ /api/security/authentication/password</li> </ul> <p>Access level <a href="#">None</a>:</p> <ul style="list-style-type: none"> <li>▫ /api/security</li> </ul>
Credentials	This sensor requires credentials for NetApp.
NetApp versions	This sensor supports ONTAP as of version 9.10. If you want to use NetApp cDOT as of version 8.3 or ONTAP from version 9.0 to version 9.9, use the <a href="#">NetApp NIC</a> <sup>[1418]</sup> sensor.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Scanning interval	<ul style="list-style-type: none"> <li>▫ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▫ The recommended scanning interval of this sensor is <a href="#">1 minute</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.



## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- netapp
- nic
- ontap
- rest

■ For more information about basic sensor settings, see section [Sensor Settings](#) 667.

## NetApp Specific

### NetApp Specific

**Name** ⓘ *e0M*

**Home Node Name** ⓘ *net-app01*

**Type** ⓘ *physical*

NetApp Specific

Setting	Description
Name	The name of the NIC that this sensor monitors.
Home Node Name	The home node name of the NIC that this sensor monitors.

Setting	Description
Type	The type of the NIC that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Link Down Count	The number of link status changes from up to down

Channel	Description
	<p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper error limit: 0</li> </ul>
Receive Errors	<p>The number of errors received</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper error limit: 0</li> </ul>
State	<p>The NIC status</p> <ul style="list-style-type: none"> <li>Up status: Up</li> <li>Down status: Down</li> <li>Warning status: Degraded</li> <li>Unknown status: Channel Value Not Set</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Throughput Read	The number of bytes read
Throughput Total	The total number of bytes read and written
Throughput Write	The number of bytes written
Transmit Errors	<p>The number of errors sent</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper error limit: 0</li> </ul>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

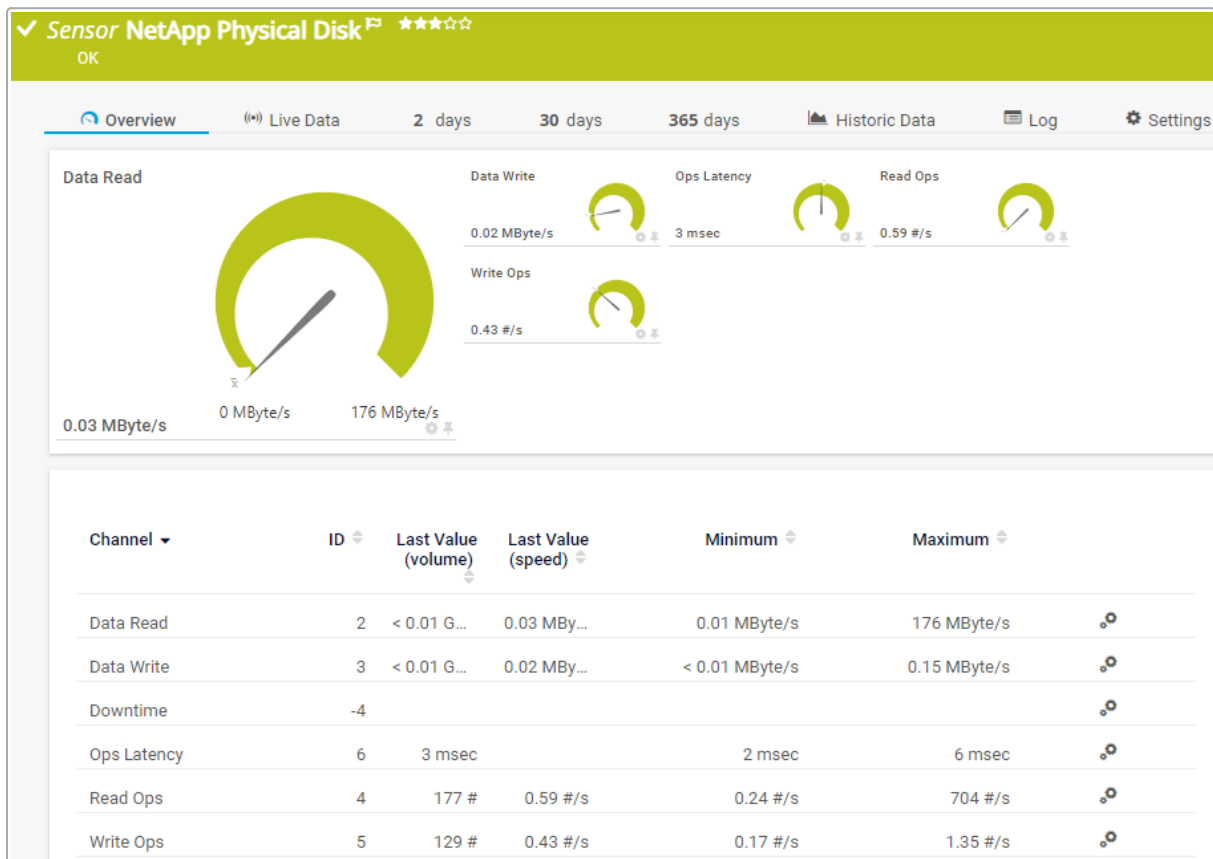
- <https://kb.paessler.com/en/topic/61108>

## 7.8.113 NetApp Physical Disk Sensor

### IMPORTANT INFORMATION

This sensor supports NetApp cDOT as of version 8.3 or ONTAP from versions 9.0 to 9.12. If you use ONTAP as of version 9.9, we recommend that you use the [NetApp Physical Disk v2<sup>\[1438\]</sup>](#) sensor.

The NetApp Physical Disk sensor monitors disks of a NetApp cDOT or ONTAP storage system accessing the application programming interface (API) via the Simple Object Access Protocol (SOAP).



NetApp Physical Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List<sup>\[1438\]</sup>](#).

### Sensor in Other Languages

- Dutch: NetApp Fysieke Schijf
- French: NetApp disque physique
- German: NetApp Physikal. Laufwerk
- Japanese: NetApp 物理ディスク
- Portuguese: Disco físico NetApp

- Russian: Физический диск NetApp
- Simplified Chinese: NetApp 物理磁盘
- Spanish: Disco físico NetApp

## Remarks

Consider the following [remarks](#)<sup>1432</sup> and requirements for this sensor:

Remark	Description
Enabled ONTAPI access	<p>The ONTAPI user account that you use with this sensor requires access to the <a href="#">DATA ONTAP API (ONTAPI)</a> so that the sensor can request data from it. The access is enabled by default.</p> <p><b>i</b> If access is disabled, locally use the following command on the cluster console to enable ONTAPI access for the user:</p> <pre>services web&gt; modify -vserver clusterd -name ontapi -enabled true</pre> <p>For this sensor, read-only user rights are sufficient for the ONTAPI user account that you use to access ONTAPI. Modify or add this user with a suitable role in the console under Cluster   ClusterX   Configuration   Security   Users</p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p><b>i</b> If the framework is missing, you cannot create this sensor.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
NetApp versions	<p>This sensor supports NetApp cDOT as of version 8.3 and NetApp ONTAP as of version 9.0.</p>
IPv6	<p>This sensor supports IPv6.</p>
Performance impact	<p>This sensor has a <a href="#">very low</a> performance impact.</p>
Credentials	<p>You can define NetApp API credentials (User Name and Password) in the <a href="#">credentials for Windows systems</a> settings of the parent device. This way, you do not need to individually enter credentials for each NetApp sensor that you add to the same device.</p>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cdot
- netapp
- ontap
- soap

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## NetApp Connection

### NetApp Connection

**NetApp Credentials** ⓘ  Use explicit credentials  
 Use Windows credentials from parent device

**Port** ⓘ

**Connection Security** ⓘ  HTTP  
 HTTPS

**Timeout (Sec.)** ⓘ

NetApp Connection

Setting	Description
NetApp Credentials	Specify which credentials you want to use to connect to the NetApp API: <ul style="list-style-type: none"> <li>▪ Use explicit credentials: Use individual NetApp API credentials.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Use Windows credentials from parent device: Use the credentials (User Name and Password) in the <a href="#">parent device settings</a> in section Credentials for Windows Systems.</li> </ul> <p><b>i</b> Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you do not need to individually enter credentials for each NetApp sensor.</p>
User Name	<p>This setting is only visible if you select Use explicit credentials <a href="#">above</a>.</p> <p>Enter a user name for access to the NetApp API. Enter a string.</p> <p><b>i</b> Read-only rights for this ONTAP user account are sufficient.</p>
Password	<p>This setting is only visible if you select Use explicit credentials <a href="#">above</a>.</p> <p>Enter the password of the user for access to the NetApp API. Enter a string.</p>
Port	<p>Enter a port number on which you can access the NetApp API. Enter an integer. The default port is <a href="#">443</a>.</p>
Connection Security	<p>Define if the connection to the NetApp API is Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured:</p> <ul style="list-style-type: none"> <li>HTTP: Use an unsecured HTTP connection.</li> <li>HTTPS: Use a secure connection to the defined port to send the query.</li> </ul>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <a href="#">900</a> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

### NetApp Specific

NetApp Specific
Disk **i** Disk 1.21.0

NetApp Specific

Setting	Description
Disk	The physical disk that this sensor monitors.



## Debug Options

**Debug Options**

**Result Handling** ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

**Primary Channel** ⓘ

Downtime


---

**Graph Type** ⓘ


Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Data Read	<p>The data read speed</p> <p> This channel is the primary channel by default.</p>
Data Write	The data write speed
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Ops Latency	The latency of operations
Read Ops	The number of disk read operations

Channel	Description
Write Ops	The number of disk write operations

## More

### KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

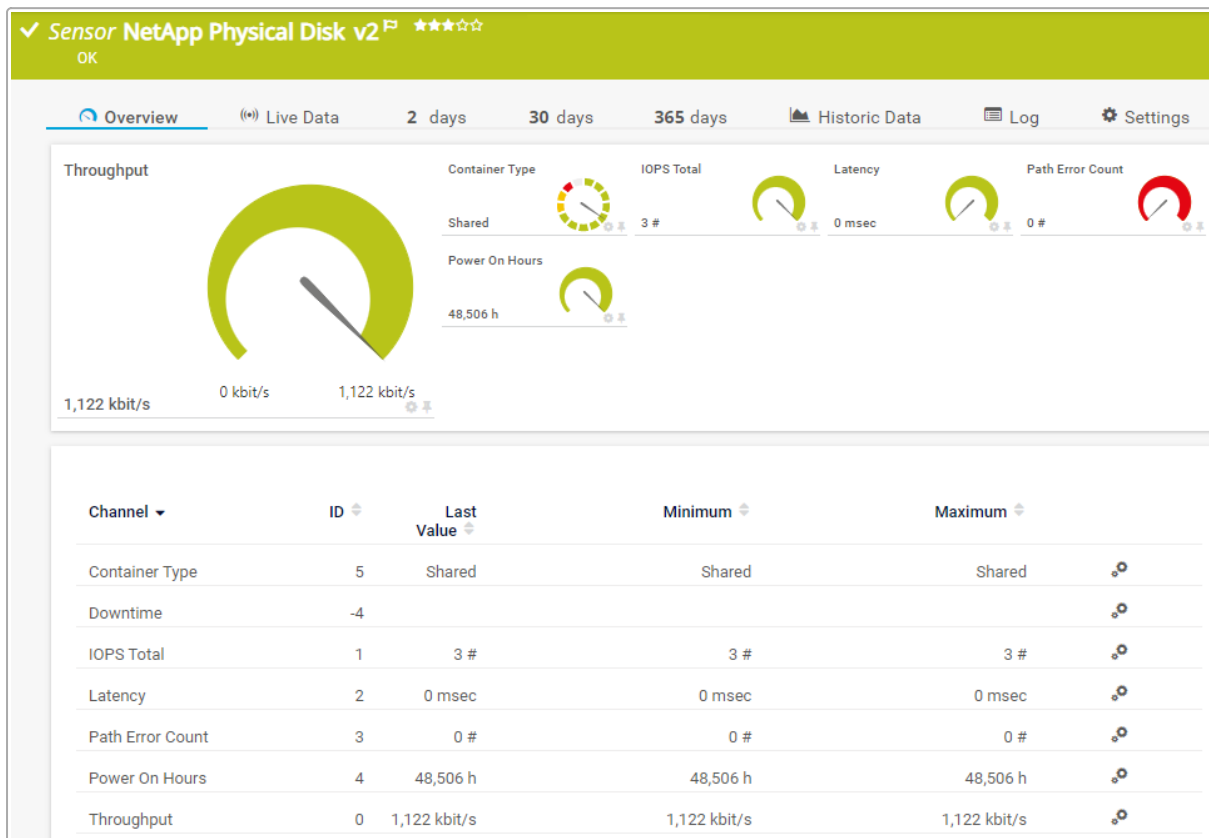
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.114 NetApp Physical Disk v2 Sensor

The NetApp Physical Disk v2 sensor monitors physical disks of a NetApp storage system via the Representational State Transfer (REST) application programming interface (API) using ONTAP as of version 9.9.

**i** This sensor was converted to a new framework so that it will continue to function after the changes of the ONTAP REST API.



NetApp Physical Disk v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1442</sup>.

### Sensor in Other Languages

- Dutch: NetApp Fysieke Schijf v2
- French: NetApp disque physique v2
- German: NetApp Physikalischer Datenträger v2
- Japanese: NetApp 物理ディスク v2
- Portuguese: Disco físico NetApp v2
- Russian: Физический диск NetApp v2
- Simplified Chinese: NetApp 物理磁盘 v2
- Spanish: Disco físico NetApp v2

## Remarks

Consider the following [remarks](#)<sup>[1439]</sup> and requirements for this sensor:

Remark	Description
Credentials for NetApp	This sensor requires an <a href="#">ONTAP System Manager</a> user account with the role <a href="#">readonly</a> and with access to the <a href="#">HTTP</a> application with <a href="#">Password</a> authentication.
Permissions for the ONTAP REST API	<p>This sensor requires permissions for the <a href="#">ONTAP REST API</a>.</p> <p> This sensor requires the role <a href="#">readonly</a> with the following permissions for the <a href="#">ONTAP REST API</a>:</p> <p>Access level <a href="#">Read-Only</a>:</p> <ul style="list-style-type: none"> <li>▫ /api</li> <li>▫ /api/security/audit/destinations</li> </ul> <p>Access level <a href="#">Read/Write</a>:</p> <ul style="list-style-type: none"> <li>▫ /api/security/authentication/password</li> </ul> <p>Access level <a href="#">None</a>:</p> <ul style="list-style-type: none"> <li>▫ /api/security</li> </ul>
Credentials	This sensor requires credentials for NetApp.
Channels	This sensor requires ONTAP 9.10 for some channels.
NetApp versions	This sensor supports ONTAP as of version 9.9. If you want to use NetApp cDOT as of version 8.3 or ONTAP from version 9.0 to version 9.8, use the <a href="#">NetApp Physical Disk</a> <sup>[1431]</sup> sensor.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">1 minute</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- netapp
- ontap
- physicaldisk
- rest

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## NetApp Specific

### NetApp Specific

**Disk Name** ⓘ 1.1.3

**Home Node Name** ⓘ *homenode02*

NetApp Specific

Setting	Description
Disk Name	The name of the physical disk that this sensor monitors.
Home Node Name	The home node name of the physical disk that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Container Type	<p>The container type</p> <ul style="list-style-type: none"> <li>▪ Up status: Aggregate, Foreign, Labelmaint, Maintenance, Shared, Spare, Unsupported, Remote, Mediator</li> <li>▪ Warning status: Unassigned, Unknown</li> <li>▪ Down status: Broken</li> <li>▪ Unknown status: Channel Value Not Set</li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
IOPS Total	<p>The number of IOPS</p>



Channel	Description
Latency	The latency
Path Error Count	<p>The number of path errors</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper error limit: 0</li> </ul>
Power On Hours	The total time that the disk has been spinning
Throughput	<p>The throughput</p> <p><b>i</b> This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

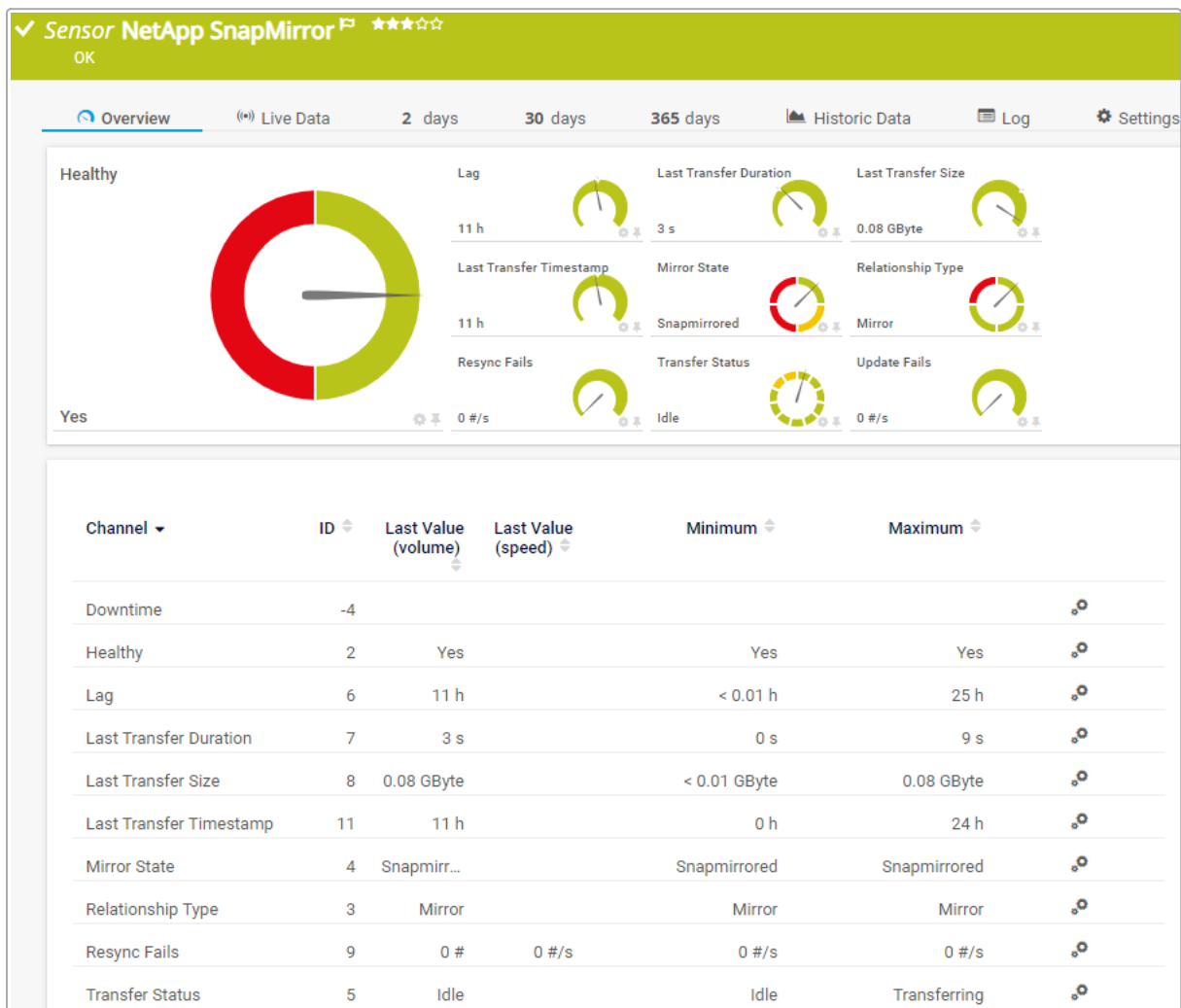
- <https://kb.paessler.com/en/topic/61108>

## 7.8.115 NetApp SnapMirror Sensor

### IMPORTANT INFORMATION

This sensor supports NetApp cDOT as of version 8.3 or ONTAP from versions 9.0 to 9.12. If you use ONTAP as of version 9.6, we recommend that you use the [NetApp SnapMirror v2<sup>\[1451\]</sup>](#) sensor.

The NetApp SnapMirror sensor monitors SnapMirror relationships of a NetApp cDOT or ONTAP storage system accessing the application programming interface (API) via the Simple Object Access Protocol (SOAP).



NetApp SnapMirror Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List<sup>\[1449\]</sup>](#).

### Sensor in Other Languages

- Dutch: NetApp SnapMirror

- French: NetApp SnapMirror
- German: NetApp SnapMirror
- Japanese: NetApp SnapMirror
- Portuguese: NetApp SnapMirror
- Russian: NetApp SnapMirror
- Simplified Chinese: NetApp SnapMirror
- Spanish: NetApp SnapMirror

## Remarks

Consider the following [remarks](#)<sup>1445</sup> and requirements for this sensor:

Remark	Description
Enabled ONTAPI access	<p>The ONTAPI user account that you use with this sensor requires access to the <a href="#">DATA ONTAP API (ONTAPI)</a> so that the sensor can request data from it. The access is enabled by default.</p> <p><b>i</b> If access is disabled, locally use the following command on the cluster console to enable ONTAPI access for the user:</p> <pre>services web&gt; modify -vserver clusterd -name ontapi -enabled true</pre> <p>For this sensor, read-only user rights are sufficient for the ONTAPI user account that you use to access ONTAPI. Modify or add this user with a suitable role in the console under Cluster   ClusterX   Configuration   Security   Users</p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p><b>i</b> If the framework is missing, you cannot create this sensor.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
NetApp versions	<p>This sensor supports NetApp cDOT as of version 8.3 and NetApp ONTAP as of version 9.0.</p>
IPv6	<p>This sensor supports IPv6.</p>
Performance impact	<p>This sensor has a <a href="#">very low</a> performance impact.</p>
Credentials	<p>You can define NetApp API credentials (User Name and Password) in the <a href="#">credentials for Windows systems</a> settings of the parent device. This way, you do not need to individually enter credentials for each NetApp sensor that you add to the same device.</p>

Remark	Description
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cdot
- netapp
- ontap
- soap

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### NetApp Connection

#### NetApp Connection

**NetApp Credentials** ⓘ  Use explicit credentials  
 Use Windows credentials from parent device

**Port** ⓘ

**Connection Security** ⓘ  HTTP  
 HTTPS

**Timeout (Sec.)** ⓘ

NetApp Connection

Setting	Description
NetApp Credentials	<p>Specify which credentials you want to use to connect to the NetApp API:</p> <ul style="list-style-type: none"> <li>▪ Use explicit credentials: Use individual NetApp API credentials.</li> <li>▪ Use Windows credentials from parent device: Use the credentials (User Name and Password) in the <a href="#">parent device settings</a> in section Credentials for Windows Systems.</li> </ul> <p><b>i</b> Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you do not need to individually enter credentials for each NetApp sensor.</p>
User Name	<p><b>This setting is only visible if you select Use explicit credentials above.</b></p> <p>Enter a user name for access to the NetApp API. Enter a string.</p> <p><b>i</b> Read-only rights for this ONTAP user account are sufficient.</p>
Password	<p><b>This setting is only visible if you select Use explicit credentials above.</b></p> <p>Enter the password of the user for access to the NetApp API. Enter a string.</p>
Port	<p>Enter a port number on which you can access the NetApp API. Enter an integer. The default port is <b>443</b>.</p>
Connection Security	<p>Define if the connection to the NetApp API is Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured:</p> <ul style="list-style-type: none"> <li>▪ HTTP: Use an unsecured HTTP connection.</li> <li>▪ HTTPS: Use a secure connection to the defined port to send the query.</li> </ul>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

### NetApp Specific

**NetApp Specific** SnapMirrors **i** cDOT\_SnapMirror\_0

NetApp Specific

Setting	Description
SnapMirrors	The SnapMirror that this sensor monitors.

### Debug Options

**Debug Options**

**Result Handling** ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### Sensor Display

**Sensor Display**


**Primary Channel** ⓘ Downtime

---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are

Setting	Description
	<p>available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Healthy	<p>If the system is healthy</p> <ul style="list-style-type: none"> <li>▪ Up status: Yes</li> </ul>

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Down status: No</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Lag	The lag transfer duration
Last Transfer Duration	The last transfer duration
Last Transfer Size	The last transfer size
Last Transfer Timestamp	The time stamp of the last transfer
Mirror State	<p>The mirror status</p> <ul style="list-style-type: none"> <li>▪ Up status: Snapmirrored</li> <li>▪ Warning status: Uninitialized</li> <li>▪ Down status: Broken-Off, Unknown</li> </ul>
Relationship Type	<p>The relationship type</p> <ul style="list-style-type: none"> <li>▪ Up status: Mirror, Mirror and Vault, Vault</li> <li>▪ Down status: Unknown</li> </ul>
Resync Fails	The number of resynchronization fails
Transfer Status	<p>The transfer status (relationship status returned from the API)</p> <ul style="list-style-type: none"> <li>▪ Up status: Aborting, Checking, Finalizing, Idle, Preparing, Queued, Quiesced, Quiescing, Transferring</li> <li>▪ Warning status: Breaking, Unknown</li> </ul>
Update Fails	The number of update fails

## More

### ■ KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

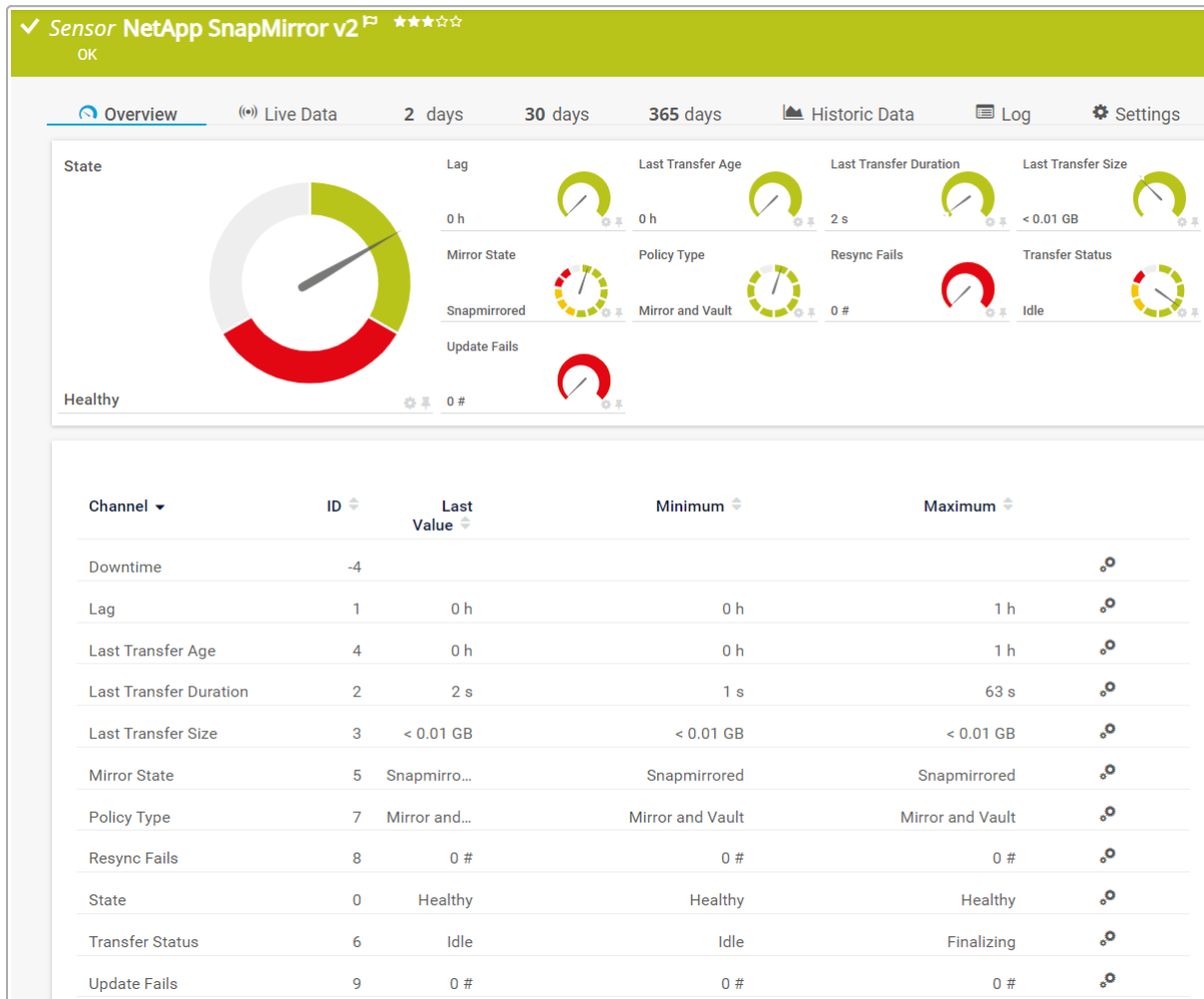
- <https://kb.paessler.com/en/topic/61108>



## 7.8.116 NetApp SnapMirror v2 Sensor

The NetApp SnapMirror v2 sensor monitors SnapMirror relationships of an ONTAP storage system the Representational State Transfer (REST) application programming interface (API) using ONTAP as of version 9.6.

**i** This sensor was converted to a new framework so that it will continue to function after the changes of the ONTAP REST API.



NetApp SnapMirror v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) <sup>1451</sup>.

### Sensor in Other Languages

- Dutch: NetApp SnapMirror v2
- French: NetApp SnapMirror v2
- German: NetApp SnapMirror v2
- Japanese: NetApp SnapMirror v2
- Portuguese: NetApp SnapMirror v2

- Russian: NetApp SnapMirror v2
- Simplified Chinese: NetApp SnapMirror v2
- Spanish: NetApp SnapMirror v2

## Remarks

Consider the following [remarks](#)<sup>1452</sup> and requirements for this sensor:

Remark	Description
Credentials for NetApp	This sensor requires an <a href="#">ONTAP System Manager</a> user account with the role <a href="#">readonly</a> and with access to the <a href="#">HTTP</a> application with <a href="#">Password</a> authentication.
Permissions for the ONTAP REST API	<p>This sensor requires permissions for the <a href="#">ONTAP REST API</a>.</p> <p><b>i</b> This sensor requires the role <a href="#">readonly</a> with the following permissions for the <a href="#">ONTAP REST API</a>:</p> <p>Access level <a href="#">Read-Only</a>:</p> <ul style="list-style-type: none"> <li>▪ /api</li> <li>▪ /api/security/audit/destinations</li> </ul> <p>Access level <a href="#">Read/Write</a>:</p> <ul style="list-style-type: none"> <li>▪ /api/security/authentication/password</li> </ul> <p>Access level <a href="#">None</a>:</p> <ul style="list-style-type: none"> <li>▪ /api/security</li> </ul>
Credentials	This sensor requires credentials for NetApp.
NetApp versions	This sensor supports ONTAP as of version 9.6. If you want to use NetApp cDOT as of version 8.3 or ONTAP from version 9.0 to 9.5, use the <a href="#">NetApp SnapMirror</a> <sup>1444</sup> sensor.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">1 minute</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- netapp
- ontap
- rest
- snapmirror

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## NetApp Specific

### NetApp Specific

**Source Path** ⓘ *paessler:netapp*

NetApp Specific

Setting	Description
Source Path	The source path of the SnapMirror relationship that this sensor monitors.

## Sensor Display

### Sensor Display

**Primary Channel** ⓘ Downtime




---

**Graph Type** ⓘ

Show channels independently (default)


Stack channels on top of each other

Sensor Display


Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><a href="#">This setting is only visible if you select</a> Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**


**Result Handling** 
 Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
State	<p>The system status</p> <ul style="list-style-type: none"> <li>▪ Up status: Healthy</li> <li>▪ Down status: Unhealthy</li> <li>▪ Unknown status: Channel Value Not Set</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Lag	The lag transfer duration
Last Transfer Duration	The last transfer duration
Last Transfer Size	The last transfer size
Last Transfer Age	The age of the last transfer
Mirror State	The mirror status

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Up status: Aborting, Checking, Expanding, In Sync, Quiesced, Quiescing, Snapmirrored</li> <li>▪ Warning status: Paused, Synchronizing, Uninitialized</li> <li>▪ Down status: Broken Off, Out Of Sync</li> <li>▪ Unknown status: Channel Value Not Set</li> </ul>
Policy Type	<p>The policy type of the relationship</p> <ul style="list-style-type: none"> <li>▪ Up status: Async, Async Mirror, Automated Failover, Continuous, Mirror and Vault, Strict Sync Mirror, Sync, Sync Mirror, Vault</li> <li>▪ Unknown status: Channel Value Not Set</li> </ul>
Resync Fails	<p>The number of resynchronization fails</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: 0</li> </ul>
Transfer Status	<p>The transfer status (relationship status returned from the API)</p> <ul style="list-style-type: none"> <li>▪ Up status: Finalizing, Idle, In Sync, Preparing, Queued, Success, Transferring</li> <li>▪ Warning status: Aborted, Hard Aborted</li> <li>▪ Down status: Failed</li> <li>▪ Unknown status: Channel Value Not Set</li> </ul>
Update Fails	<p>The number of update fails</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: 0</li> </ul>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.117 NetApp System Health Sensor

### IMPORTANT INFORMATION

This sensor supports NetApp cDOT as of version 8.3 or ONTAP from versions 9.0 to 9.12. If you use ONTAP as of version 9.6, we recommend that you use the [NetApp System Health v2](#)<sup>[1465]</sup> sensor.

The NetApp System Health sensor monitors the health of a NetApp cDOT or ONTAP storage system accessing the application programming interface (API) via the Simple Object Access Protocol (SOAP).



NetApp System Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1462]</sup>.

### Sensor in Other Languages

- Dutch: NetApp Systeemstatus
- French: NetApp état du système
- German: NetApp Systemzustand
- Japanese: NetApp システム正常性

- Portuguese: Saúde do sistema NetApp
- Russian: Работоспособность системы NetApp
- Simplified Chinese: NetApp 系统健康状况
- Spanish: Salud de sistema NetApp

## Remarks

Consider the following [remarks](#)<sup>[1458]</sup> and requirements for this sensor:

Remark	Description
Enabled ONTAPI access	<p>The ONTAPI user account that you use with this sensor requires access to the <a href="#">DATA ONTAP API (ONTAPI)</a> so that the sensor can request data from it. The access is enabled by default.</p> <p><b>i</b> If access is disabled, locally use the following command on the cluster console to enable ONTAPI access for the user:</p> <pre>services web&gt; modify -vserver clusterd -name ontapi -enabled true</pre> <p><b>i</b> This sensor requires administrator rights for the ONTAPI user account that you use to access ONTAPI. Modify or add this user with a suitable role in the console under Cluster   ClusterX   Configuration   Security   Users</p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p><b>i</b> If the framework is missing, you cannot create this sensor.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
NetApp versions	<p>This sensor supports NetApp cDOT as of version 8.3 and NetApp ONTAP as of version 9.0.</p>
IPv6	<p>This sensor supports IPv6.</p>
Performance impact	<p>This sensor has a <a href="#">very low</a> performance impact.</p>
Read-only	<p>As an <a href="#">alternative to administrator rights</a><sup>[1462]</sup>, you can add a specific Role Attribute and use read-only rights.</p>
Credentials	<p>You can define NetApp API credentials (User Name and Password) in the <a href="#">credentials for Windows systems</a> settings of the parent device. This way, you do not need to individually enter credentials for each NetApp sensor that you add to the same device.</p>



Remark	Description
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cdot
- netapp
- ontap
- soap

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## NetApp Connection

### NetApp Connection

**NetApp Credentials** ⓘ

Use explicit credentials

Use Windows credentials from parent device

---

**Port** ⓘ 443

---

**Connection Security** ⓘ

HTTP

HTTPS

---

**Timeout (Sec.)** ⓘ 60

NetApp Connection

Setting	Description
NetApp Credentials	<p>Specify which credentials you want to use to connect to the NetApp API:</p> <ul style="list-style-type: none"> <li>▪ Use explicit credentials: Use individual NetApp API credentials.</li> <li>▪ Use Windows credentials from parent device: Use the credentials (User Name and Password) in the <a href="#">parent device settings</a> in section Credentials for Windows Systems.</li> </ul> <p><b>i</b> Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you do not need to individually enter credentials for each NetApp sensor.</p>
User Name	<p><b>This setting is only visible if you select Use explicit credentials above.</b></p> <p>Enter a user name for access to the NetApp API. Enter a string.</p> <p><b>i</b> Read-only rights for this ONTAP user account are sufficient.</p>
Password	<p><b>This setting is only visible if you select Use explicit credentials above.</b></p> <p>Enter the password of the user for access to the NetApp API. Enter a string.</p>
Port	<p>Enter a port number on which you can access the NetApp API. Enter an integer. The default port is <b>443</b>.</p>
Connection Security	<p>Define if the connection to the NetApp API is Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured:</p> <ul style="list-style-type: none"> <li>▪ HTTP: Use an unsecured HTTP connection.</li> <li>▪ HTTPS: Use a secure connection to the defined port to send the query.</li> </ul>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

### NetApp Specific

NetApp Specific
System Nodes **3** node001

NetApp Specific

Setting	Description
System Nodes	The ID of the system node that this sensor monitors.

### Debug Options

**Debug Options**

**Result Handling** ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### Sensor Display

**Sensor Display**

**Primary Channel** ⓘ

Downtime


---

**Graph Type** ⓘ


Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are

Setting	Description
	<p>available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Permissions: Alternative to Administrator Rights

If you do not want to provide administrator rights for the ONTAPI user account that you use with the NetApp System Health sensor, you can add a new command to the selected role of the user that makes read-only rights sufficient.

- Edit the Role of this user in the console under Cluster | ClusterX | Configuration | Security | Users.
- Add the command storage aggregate check\_spare\_low with access control list (ACL) all to the Role Attributes.

With this role attribute, read-only rights are sufficient for the NetApp System Health sensor.

## Channel List

- i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CPU	<p>The CPU load (%)</p> <ul style="list-style-type: none"> <li>ⓘ This channel is the primary channel by default.</li> <li>ⓘ This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: 90%</li> <li>▪ Upper warning limit: 80%</li> </ul> </li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Failed Fans	<p>The number of failed fans</p> <ul style="list-style-type: none"> <li>ⓘ This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: 2</li> <li>▪ Upper warning limit: 1</li> </ul> </li> </ul>
Failed PSU	<p>The number of failed power supplies</p> <ul style="list-style-type: none"> <li>ⓘ This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: 2</li> <li>▪ Upper warning limit: 1</li> </ul> </li> </ul>
Memory	<p>The memory usage</p>
Node Health	<p>The node health</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Down status: Error</li> </ul>
NVRAM Battery	<p>The NVRAM battery status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Down status: Error</li> </ul>
Spare Disks #	<p>The number of spare disks</p>
Spare Disks Low	<p>If spare disks are low as reported by the NetApp</p> <ul style="list-style-type: none"> <li>▪ Up status: No</li> <li>▪ Down status: Yes</li> </ul>

Channel	Description
Spare Size Usable	The usable spare size
Storage Configuration Path	<p>The storage configuration path that describes the connection of a node</p> <ul style="list-style-type: none"> <li>▪ Up status: multi_path, multi_path_ha, quad_path, quad_path_ha, N/A</li> <li>▪ Warning status: single_path, single_path_ha, mixed_path, mixed_path_ha</li> <li>▪ Down status: unknown</li> </ul> <p><b>i</b> If no storage configuration path is returned, the sensor shows the Up status (N/A) because the availability of the configuration path depends on the NetApp version.</p>
Temperature	<p>The temperature status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Down status: Error</li> </ul>
Uptime	The uptime

## More

### ■ KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.118 NetApp System Health v2 Sensor

The NetApp System Health v2 sensor monitors the health of a node of a NetApp storage cluster via the Representational State Transfer (REST) application programming interface (API) using ONTAP as of version 9.6.

**i** This sensor was converted to a new framework so that it will continue to function after the changes of the ONTAP REST API.



NetApp System Health v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sub>1469</sub>.

### Sensor in Other Languages

- Dutch: NetApp Systeemstatus v2
- French: NetApp état du système v2
- German: NetApp Systemzustand v2
- Japanese: NetApp システム正常性 v2
- Portuguese: Saúde do sistema NetApp v2
- Russian: Работоспособность системы NetApp v2
- Simplified Chinese: NetApp 系统健康状况 v2

- Spanish: Salud del sistema NetApp v2

## Remarks

Consider the following [remarks](#) <sup>[1466]</sup> and requirements for this sensor:

Remark	Description
Credentials for NetApp	This sensor requires an <a href="#">ONTAP System Manager</a> user account with the role <a href="#">readonly</a> and with access to the <a href="#">HTTP</a> application with <a href="#">Password</a> authentication.
Permissions for the ONTAP REST API	<p>This sensor requires permissions for the <a href="#">ONTAP REST API</a>.</p> <p><b>i</b> This sensor requires the role <a href="#">readonly</a> with the following permissions for the <a href="#">ONTAP REST API</a>:</p> <p>Access level <a href="#">Read-Only</a>:</p> <ul style="list-style-type: none"> <li>▪ /api</li> <li>▪ /api/security/audit/destinations</li> </ul> <p>Access level <a href="#">Read/Write</a>:</p> <ul style="list-style-type: none"> <li>▪ /api/security/authentication/password</li> </ul> <p>Access level <a href="#">None</a>:</p> <ul style="list-style-type: none"> <li>▪ /api/security</li> </ul>
Credentials	This sensor requires credentials for NetApp.
Channels	This sensor requires ONTAP 9.11 for some <a href="#">channels</a> <sup>[1469]</sup> .
NetApp versions	This sensor supports ONTAP as of version 9.6. If you want to use NetApp cDOT as of version 8.3 or ONTAP from version 9.0 to version 9.5, use the <a href="#">NetApp System Health</a> <sup>[1457]</sup> sensor.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">1 minute</a>.</li> </ul>



Remark	Description
Multi-platform probe	You can add this sensor to a multi-platform probe.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- netapp
- ontap
- rest

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### NetApp Specific

#### NetApp Specific

**Node Name** ⓘ *netapp01*

NetApp Specific

Setting	Description
Node Name	The name of the node that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Failed PSUs	<p>The number of failed power supplies</p> <p>ⓘ This channel has a default limit:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: 0</li> </ul>
Node Health	<p>The node health</p> <ul style="list-style-type: none"> <li>▪ Up status: Up</li> <li>▪ Warning status: Booting, Taken Over, Waiting for Giveback</li> <li>▪ Down status: Down, Degraded, Unknown</li> </ul>

Channel	Description
	<ul style="list-style-type: none"> <li>Unknown status: Channel Value Not Set</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
NVRAM Battery	<p>The NVRAM battery status</p> <ul style="list-style-type: none"> <li>Up status: OK, Fully Charged</li> <li>Warning status: Near End-of-life, Over-charged, Partially Discharged</li> <li>Down status: Fully Discharged, Not Present, At End-of-life</li> <li>Unknown status: Channel Value Not Set, Unknown</li> </ul> <p><b>i</b> This channel requires ONTAP 9.11.</p>
Storage Configuration Path	<p>The storage configuration path that describes the connection of a node</p> <ul style="list-style-type: none"> <li>Up status: Multi Path, Multi Path HA, Mixed Path, Single Path HA, Mixed Path HA, Quad Path, Quad Path HA, Tri Path, Tri Path HA, Virtual</li> <li>Warning status: Unknown, Single Path</li> <li>Unknown status: Channel Value Not Set</li> </ul> <p><b>i</b> This channel requires ONTAP 9.11.</p>
Spare Disks Available	<p>The number of spare disks</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>Lower error limit: 1</li> <li>Lower warning limit: 2</li> </ul>
Spare Size Usable	<p>The usable spare size</p>
Temperature State	<p>The temperature status</p> <ul style="list-style-type: none"> <li>Up status: Normal</li> <li>Down status: Over</li> <li>Unknown status: Channel Value Not Set</li> </ul>
Uptime	<p>The uptime</p>

More

 KNOWLEDGE BASE

What security features does PRTG include?

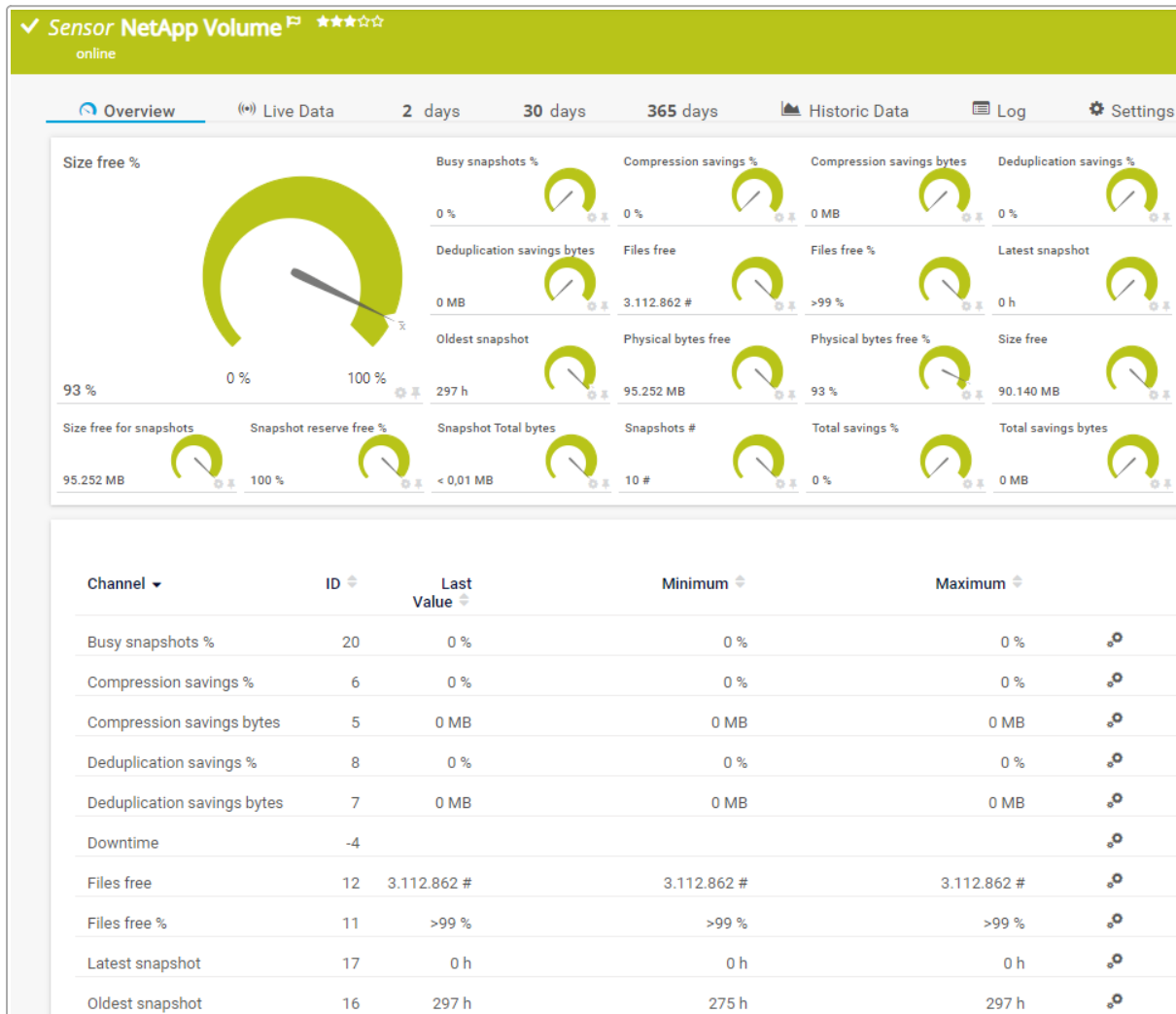
- <https://kb.paessler.com/en/topic/61108>

## 7.8.119 NetApp Volume Sensor

### IMPORTANT INFORMATION

This sensor supports NetApp cDOT as of version 8.3 or ONTAP from versions 9.0 to 9.12. If you use ONTAP as of version 9.6, we recommend that you use the [NetApp Volume v2](#) sensor.

The NetApp Volume sensor monitors volumes on a NetApp cDOT or ONTAP storage system accessing the application programming interface (API) via the Simple Object Access Protocol (SOAP).



NetApp Volume Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: NetApp Volume
- French: NetApp volume de stockage

- German: NetApp Volume
- Japanese: NetApp ボリューム
- Portuguese: Volume NetApp
- Russian: Том NetApp
- Simplified Chinese: NetApp 卷
- Spanish: Volumen NetApp

## Remarks

Consider the following [remarks](#)<sup>[1473]</sup> and requirements for this sensor:

Remark	Description
Enabled ONTAPI access	<p>The ONTAPI user account that you use with this sensor requires access to the <a href="#">DATA ONTAP API (ONTAPI)</a> so that the sensor can request data from it. The access is enabled by default.</p> <p><b>i</b> If access is disabled, locally use the following command on the cluster console to enable ONTAPI access for the user:</p> <pre>services web&gt; modify -vserver clusterd -name ontapi -enabled true</pre> <p>For this sensor, read-only user rights are sufficient for the ONTAPI user account that you use to access ONTAPI. Modify or add this user with a suitable role in the console under Cluster   ClusterX   Configuration   Security   Users</p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p><b>i</b> If the framework is missing, you cannot create this sensor.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
NetApp versions	<p>This sensor supports NetApp cDOT as of version 8.3 and NetApp ONTAP as of version 9.0.</p>
IPv6	<p>This sensor supports IPv6.</p>
Performance impact	<p>This sensor has a <a href="#">very low</a> performance impact.</p>
Credentials	<p>You can define NetApp API credentials (User Name and Password) in the <a href="#">credentials for Windows systems</a> settings of the parent device. This way, you do not need to individually enter credentials for each NetApp sensor that you add to the same device.</p>
Add Sensor dialog	<p>Volumes that are offline do not appear in the Add Sensor dialog.</p>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cdot
- netapp
- ontap
- soap

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## NetApp Connection

### NetApp Connection

**NetApp Credentials** ⓘ  Use explicit credentials  
 Use Windows credentials from parent device

**Port** ⓘ

**Connection Security** ⓘ  HTTP  
 HTTPS

**Timeout (Sec.)** ⓘ

NetApp Connection

Setting	Description
NetApp Credentials	Specify which credentials you want to use to connect to the NetApp API: <ul style="list-style-type: none"> <li>▪ Use explicit credentials: Use individual NetApp API credentials.</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>Use Windows credentials from parent device: Use the credentials (User Name and Password) in the <a href="#">parent device settings</a> in section Credentials for Windows Systems.</li> </ul> <p><b>i</b> Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you do not need to individually enter credentials for each NetApp sensor.</p>
User Name	<p>This setting is only visible if you select Use explicit credentials <a href="#">above</a>.</p> <p>Enter a user name for access to the NetApp API. Enter a string.</p> <p><b>i</b> Read-only rights for this ONTAP user account are sufficient.</p>
Password	<p>This setting is only visible if you select Use explicit credentials <a href="#">above</a>.</p> <p>Enter the password of the user for access to the NetApp API. Enter a string.</p>
Port	<p>Enter a port number on which you can access the NetApp API. Enter an integer. The default port is <b>443</b>.</p>
Connection Security	<p>Define if the connection to the NetApp API is Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured:</p> <ul style="list-style-type: none"> <li>HTTP: Use an unsecured HTTP connection.</li> <li>HTTPS: Use a secure connection to the defined port to send the query.</li> </ul>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

### NetApp Specific

NetApp Specific
Volumes **i** *Volume volume000-01:vol0*

NetApp Specific

Setting	Description
Volumes	The volume that this sensor monitors.

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].Data.txt and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

Sensor Display

**Primary Channel** ⓘ

Downtime

---


**Graph Type** ⓘ

Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Busy Snapshots %	The number of busy snapshots (%)
Compression Savings %	The compression savings (%)
Compression Savings Bytes	The compression savings
Deduplication Savings %	The deduplication savings (%)
Deduplication Savings Bytes	The deduplication savings

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Files Free	The free files in total
Files Free %	The free files (%)
Latest Snapshot	The age of the last snapshot
Oldest Snapshot	The oldest snapshot age
Physical Bytes Free	The free physical bytes in total
Physical Bytes Free %	The free physical bytes (%)
Size Free	The free size in total
Size Free %	The free size (%) <b>i</b> This channel is the primary channel by default.
Size Free For Snapshots	The free size for snapshots
Snapshot Reserve Free %	The free snapshot reserve (%)
Snapshots #	The number of snapshots
Total Savings %	The total savings (%)
Total Savings Bytes	The total savings

## More

### ■ KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

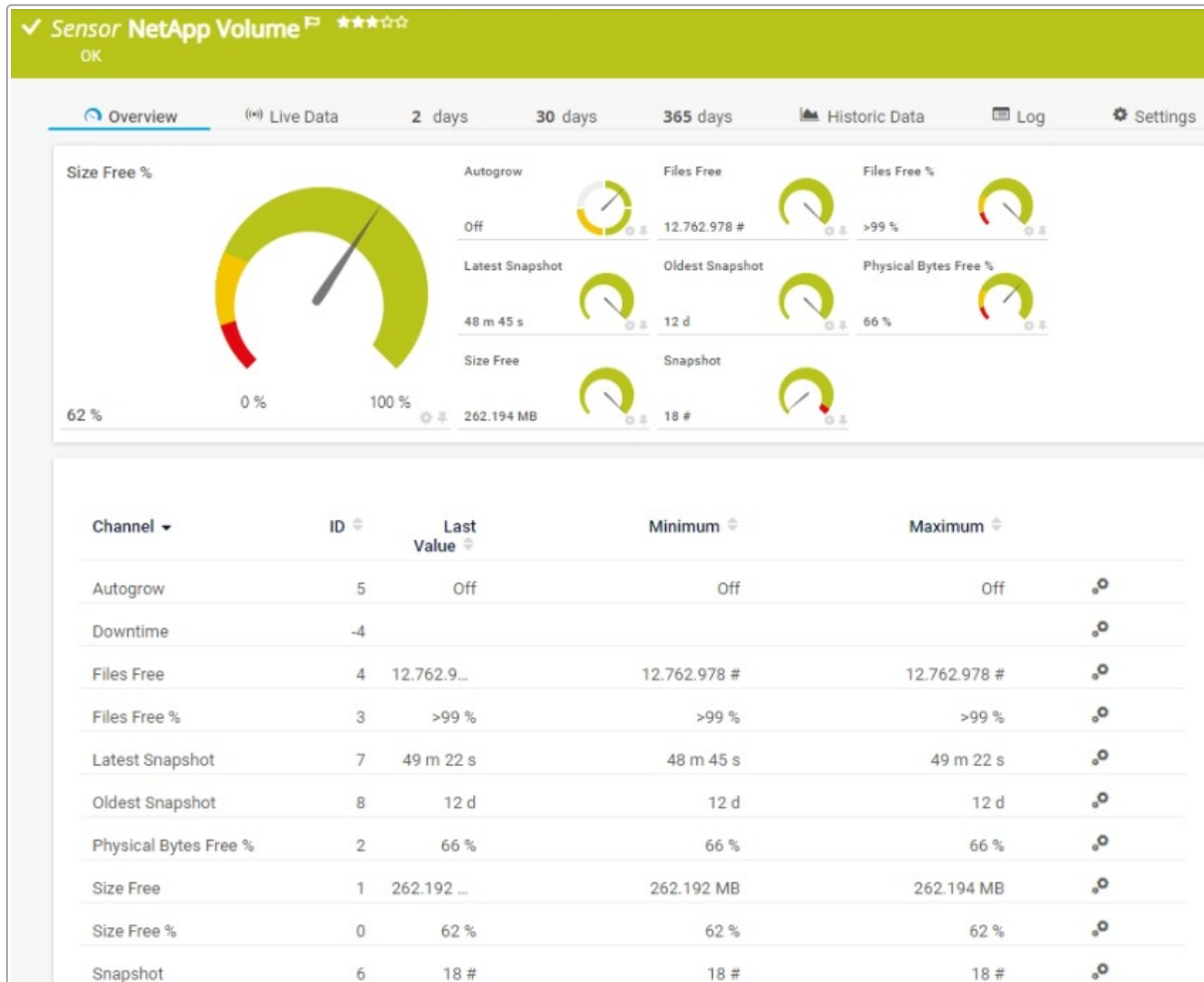
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.120 NetApp Volume v2 Sensor

The NetApp Volume v2 sensor monitors a volume of a NetApp storage system via the Representational State Transfer (REST) application programming interface (API) using ONTAP as of version 9.6.

**i** This sensor was converted to a new framework so that it will continue to function after the changes of the ONTAP REST API.



NetApp Volume Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1483]</sup>.

### Sensor in Other Languages

- Dutch: NetApp Volume v2
- French: NetApp volume de stockage v2
- German: NetApp Volume v2
- Japanese: NetApp ボリューム v2
- Portuguese: Volume NetApp v2
- Russian: Tom NetApp v2

- Simplified Chinese: NetApp 卷 v2
- Spanish: Volumen NetApp v2

## Remarks

Consider the following [remarks](#)<sup>[1480]</sup> and requirements for this sensor:

Remark	Description
Credentials for NetApp	This sensor requires an <a href="#">ONTAP System Manager</a> user account with the role <a href="#">readonly</a> and with access to the <a href="#">HTTP</a> application with <a href="#">Password</a> authentication.
Permissions for the ONTAP REST API	<p>This sensor requires permissions for the <a href="#">ONTAP REST API</a>.</p> <p><b>i</b> This sensor requires the role <a href="#">readonly</a> with the following permissions for the <a href="#">ONTAP REST API</a>:</p> <p>Access level <a href="#">Read-Only</a>:</p> <ul style="list-style-type: none"> <li>▪ /api</li> <li>▪ /api/security/audit/destinations</li> </ul> <p>Access level <a href="#">Read/Write</a>:</p> <ul style="list-style-type: none"> <li>▪ /api/security/authentication/password</li> </ul> <p>Access level <a href="#">None</a>:</p> <ul style="list-style-type: none"> <li>▪ /api/security</li> </ul>
Credentials	This sensor requires credentials for NetApp.
NetApp versions	This sensor supports ONTAP as of version 9.6. If you want to use NetApp cDOT as of version 8.3 or ONTAP from version 9.0 to version 9.5, use the <a href="#">NetApp Volume</a> <sup>[1472]</sup> sensor.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">1 minute</a>.</li> </ul>

Remark	Description
Multi-platform probe	You can add this sensor to a multi-platform probe.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- netapp
- ontap
- rest

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### NetApp Specific

#### NetApp Specific

**Volume Name** ⓘ Example1

---

**Aggregate Names** ⓘ Example Aggregate

NetApp Specific

Setting	Description
Volume Name	The name of the volume that this sensor monitors.
Aggregate Names	The names of the aggregates that contain the volume that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**


Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options



Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Autogrow	<p>The autogrow status</p> <ul style="list-style-type: none"> <li>▪ Up status: Off, Can Grow</li> <li>▪ Warning status: Grow Limit Reached</li> <li>▪ Unknown status: Channel Value Not Set</li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Files Free	<p>The number of files that can be created on the volume</p>
Files Free %	<p>The number of files that can be created on the volume</p>

Channel	Description
	<p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: <a href="#">10%</a></li> <li>▪ Lower warning limit: <a href="#">25%</a></li> </ul>
Latest Snapshot	The time since the latest snapshot
Oldest Snapshot	The oldest snapshot age
Physical Bytes Free %	<p>The free physical bytes</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: <a href="#">10%</a></li> <li>▪ Lower warning limit: <a href="#">25%</a></li> </ul>
Size Free	<p>The free size</p> <p><b>i</b> This channel also takes the snapshot reserve space (if set in the ONTAP System Manager) on the volume into account.</p>
Size Free %	<p>The free size (%)</p> <p><b>i</b> This channel is the primary channel by default.</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: <a href="#">10%</a></li> <li>▪ Lower warning limit: <a href="#">25%</a></li> </ul> <p><b>i</b> This channel also takes the snapshot reserve space (if set in the ONTAP System Manager) on the volume into account.</p>
Snapshot	<p>The number of snapshots</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: <a href="#">1024</a></li> </ul> <p><b>i</b> Volumes can contain up to 1023 snapshot copies. The limit of this channel is set to define a fixed size of the <a href="#">gauge</a> that reflects the maximum number of snapshot copies that the volume can contain.</p>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.121 NetFlow v5 Sensor

The NetFlow v5 sensor receives traffic data from a NetFlow v5-compatible device and shows the traffic by type. This sensor has several filter options to divide traffic into different channels.

**i** Make sure that the sensor matches the NetFlow version that your device exports.

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum
Chat	3004	0.01 MByte	< 0.01 Mbit/s	0 Mbit/s	< 0.01 Mbit/s
Citrix	3010	0 MByte	0 Mbit/s	0 Mbit/s	< 0.01 Mbit/s
Downtime	-4				
FTP/P2P	3002	0.04 MByte	< 0.01 Mbit/s	0 Mbit/s	< 0.01 Mbit/s
Infrastructure	3007	0 MByte	0 Mbit/s	0 Mbit/s	< 0.01 Mbit/s

NetFlow v5 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1494]</sup>.


### Sensor in Other Languages

- Dutch: NetFlow v5
- French: NetFlow v5

- German: NetFlow v5
- Japanese: NetFlow v5
- Portuguese: NetFlow v5
- Russian: NetFlow v5
- Simplified Chinese: NetFlow v5
- Spanish: NetFlow v5

## Remarks

Consider the following [remarks](#)<sup>[1487]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
NetFlow	This sensor requires that the NetFlow export of the respective version is enabled on the target system. The target system must send the flow data stream to the IP address of the probe system.
Cluster probe	This sensor does not support cluster probes. You can only set it up on local probes or remote probes.
IPv6	This sensor supports IPv6.
Clone sensor	If you clone this sensor to the <b>same</b> probe, PRTG keeps the <a href="#">selected IP addresses</a> <sup>[1489]</sup> on which it listens for Flow (NetFlow, jFlow, sFlow, IPFIX) packets. If you clone this sensor to a <b>different</b> probe, PRTG selects <b>all</b> available IP addresses by default.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">What is the Active Flow Timeout in flow sensors?</a></li> <li>▪ Knowledge Base: <a href="#">How can I change the default groups and channels for flow and Packet Sniffer sensors?</a></li> </ul>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- bandwidthsensor
- netflowsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## NetFlow v5 Specific Settings

### NetFlow v5 Specific Settings

**Receive Packets on UDP Port** ⓘ 9997

---

**Sender IP Address** ⓘ

---

**Receive Packets on IP Address** ⓘ

▾ Probe's Local IP Addresses

---

192.0.2.0

---

**Active Flow Timeout (Minutes)** ⓘ 10

---

**Sampling Mode** ⓘ

Disable (default)

Enable

---

**Stream Data Handling** ⓘ

Discard stream data (default)

Store stream data only for the 'Other' channel

Store all stream data

NetFlow v5 Specific Settings

Setting	Description
Receive Packets on UDP Port	<p>Enter the User Datagram Protocol (UDP) port number on which PRTG receives the flow packets. It must match the UDP port number in the NetFlow export options of the hardware router device. Enter an integer.</p> <p> When you configure the export, make sure that you select the appropriate NetFlow version for this sensor.</p>
Sender IP Address	<p>Enter the IP address of the sending device that you want to receive the NetFlow from. Enter an IP address to only receive data from a specific device or leave the field empty to receive data from any device on the specified port.</p>
Receive Packets on IP Address	<p>Select the IP addresses on which PRTG listens to NetFlow packets. The list of IP addresses is specific to your setup. To select an IP address, enable a check box in front of the respective line. The IP address that you select must match the IP address in the NetFlow export options of the hardware router device.</p> <p> When you configure the export, make sure that you select the appropriate NetFlow version for this sensor.</p> <p> You can also select all items or cancel the selection by using the check box in the table header.</p>
Active Flow Timeout (Minutes)	<p>Enter a time span in minutes after which the sensor must receive new flow data. If the timeout elapses and the sensor receives no new data during this time, it shows the Unknown <a href="#">status</a>. Enter an integer. The maximum timeout is 60 minutes.</p> <p> We recommend that you set the timeout one minute longer than the timeout in the hardware router device.</p> <p> If you set this value too low, flow information might be lost.</p> <p> For more information, see the Knowledge Base: <a href="#">What is the Active Flow Timeout in flow sensors?</a></p> <p> If the target device sends incorrect time information that results in wrong monitoring data, try to use 0 as the active flow timeout. This ignores the start and stop information of a flow as provided by the device and accounts all data to the current point in time. It might result in spikes but the sensor captures all data.</p>
Sampling Mode	<p>Define if you want to use the sampling mode:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Use the standard flow.</li> <li>▪ Enable: Use the sampling mode and specify the Sampling Rate below.</li> </ul> <p> This setting must match the setting in the xFlow exporter.</p>

Setting	Description
Sampling Rate	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Enter a number that matches the sampling rate in the exporting device. If the number is different, monitoring results will be incorrect. Enter an integer.</p>
Stream Data Handling	<p>Define what PRTG does with the stream and packet data:</p> <ul style="list-style-type: none"> <li>▪ Discard stream data (default): Do not store the stream and packet data.</li> <li>▪ Store stream data only for the 'Other' channel: Only store stream and packet data that is not otherwise filtered and is therefore accounted to the default Other channel. PRTG stores this data in the \StreamLog subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Streams Sensor [ID] (1).csv. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> <li>▪ Store all stream data: Store all stream and packet data. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><b>i</b> Use with caution. It can create huge data files. We recommend that you only use this setting for a short time.</p>

## Channel Configuration

Channel Configuration

Channel Selection ⓘ

Group	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Content
Web	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WWW Traffic: HTTP, HTTPS
File Transfer	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	File Transfer: FTP (Control)
Mail	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Mail Traffic: IMAP, POP3, SMTP
Chat	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Chat, Instant Messaging: IRC, AIM
Remote Control	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Remote Control: RDP, SSH, Telnet, VNC
Infrastructure	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Network Services: DHCP, DNS, Ident, ICMP, SNMP
NetBIOS	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	NetBIOS: NETBIOS
Citrix	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Citrix: Citrix
Other Protocols	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Various: Other UDP, Other TCP

**Note** You can change the default configuration for groups and channels. This way, you do not have to customize this setting each time that you add this sensor type. For details, see the Knowledge Base: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)

Channel Configuration

Setting	Description
Channel Selection	<p>Define the categories that the sensor accounts the traffic to:</p> <ul style="list-style-type: none"> <li>▪ Web: Internet web traffic.</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ File Transfer: Traffic from FTP.</li> <li>▪ Mail: Internet mail traffic.</li> <li>▪ Chat: Traffic from chat and instant messaging.</li> <li>▪ Remote Control: Traffic from remote control applications such as RDP, SSH, Telnet, and Virtual Network Computing (VNC).</li> <li>▪ Infrastructure: Traffic from network services such as DHCP, DNS, Ident, ICMP, and SNMP.</li> <li>▪ NetBIOS: Traffic from NetBIOS communication.</li> <li>▪ Citrix: Traffic from Citrix applications.</li> <li>▪ Other Protocols: Traffic from various other protocols via UDP and TCP.</li> </ul> <p>For each group, you can select how many channels the sensor uses, that is, how detailed the sensor divides the traffic:</p> <ul style="list-style-type: none"> <li>▪ No (✘): Do not account traffic of this group in its own channel. The sensor accounts all traffic of this group to the default channel named Other.</li> <li>▪ Yes (✔): Count all traffic of this group and summarize it in one channel.</li> <li>▪ Detail (🗨): Count all traffic of this group and further divide it into different channels. The traffic appears in several channels that you can see in the Content column.</li> </ul> <p><b>i</b> Extensive use of this option can cause load problems on the probe system. We recommend that you set specific, well-chosen filters for the data that you really want to analyze.</p> <p><b>■</b> You can change the default configuration for groups and channels. For more information, see the Knowledge Base: <a href="#">How can I change the default groups and channels for flow and Packet Sniffer sensors?</a></p>

## Filtering

**■** For more information, see section [Filter Rules](#)<sup>[1494]</sup>.

**Filtering**

**Filters** To include and exclude specific traffic, you can define filter rules based on the following format guidelines:

- field[filter]

**Fields:**  
IP, Port, SourceIP, SourcePort, DestinationIP, DestinationPort, Protocol (values TCP, UDP, ICMP, OSPFIGP or any number), ToS, DSCP

**Additional IPFIX fields:**  
Interface, ASI, InboundInterface, OutboundInterface, SourceASI, DestinationASI, MAC, SourceMAC, DestinationMAC, Mask, SourceMask, DestinationMask ('Masks' represent subnet masks in the form of a single number ('number of contiguous bits')), NextHop (IP Address), VLAN, SourceVLAN, DestinationVLAN ('VLANs' represent a VLAN identifier)

Include Filter ⓘ

Exclude Filter ⓘ

Filtering

Setting	Description
Include Filter	Define if you want to filter any traffic. If you leave this field empty, the sensor includes all traffic. To include specific traffic only, define filters using a special <a href="#">syntax</a> .
Exclude Filter	First, the sensor considers the filters in Include Filter. From this subset, you can explicitly exclude traffic, using the same syntax.

## Sensor Display


**Sensor Display**

Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display


Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.  ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.
Graph Type	Define how this sensor shows different channels:

Setting	Description
	<ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Primary Toplist


**Primary Toplist** Primary Toplist ⓘ Top Connections

Primary Toplist

Setting	Description
Primary Toplist	<p>Define which Toplist is the primary Toplist of the sensor:</p> <ul style="list-style-type: none"> <li>Top Talkers</li> <li>Top Connections</li> <li>Top Protocols</li> <li><a href="#">[Any custom Toplists you add]</a></li> </ul> <p> PRTG shows the primary Toplist in maps when you add a Toplist object.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Toplists

For all Flow (NetFlow, jFlow, sFlow, IPFIX) and Packet Sniffer sensors, Toplists are available on the sensor's Overview tab. Using Toplists, you can review traffic data for small time periods in great detail.

■ For more information, see section [Toplists](#).

## Filter Rules

■ For more information, see section [Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Chat	The traffic from chat and instant messaging (IRC, AIM)
Citrix	The traffic from Citrix applications
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
FTP/P2P	The traffic from file transfer (FTP/P2P)
Infrastructure	The traffic from network services (DHCP, DNS, Ident, ICMP, SNMP)
Mail	The internet mail traffic (IMAP, POP3, SMTP)
NetBIOS	The traffic from NetBIOS communication
Other	The traffic from various other protocols (UDP, TCP)
Remote Control	The traffic from remote control applications (RDP, SSH, Telnet, Virtual Network Computing (VNC))
Total	The total traffic <b>i</b> This channel is the primary channel by default.
Various	The traffic from various other sources

Channel	Description
WWW	The traffic from the web (HTTP, HTTPS)

## More

### KNOWLEDGE BASE

What is the Active Flow Timeout in flow sensors?

- <https://kb.paessler.com/en/topic/66485>

How can I change the default groups and channels for flow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

### PAESSLER TOOLS

NetFlow Tester

- <https://www.paessler.com/tools/netflowtester>

## 7.8.122 NetFlow v5 (Custom) Sensor

The NetFlow v5 (Custom) sensor receives traffic data from a NetFlow v5-compatible device and shows the traffic by type. With this sensor, you can define your own channel definitions to divide traffic into different channels.

**i** Make sure that the sensor matches the NetFlow version that your device exports.

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum
Chat	3004	0.01 MBy...	< 0.01 M...	0 Mbit/s	< 0.01 Mbit/s
Citrix	3010	0 MByte	0 Mbit/s	0 Mbit/s	< 0.01 Mbit/s
Downtime	-4				
FTP/P2P	3002	0.04 MBy...	< 0.01 M...	0 Mbit/s	< 0.01 Mbit/s
Infrastructure	3007	0 MByte	0 Mbit/s	0 Mbit/s	< 0.01 Mbit/s

NetFlow v5 (Custom) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1503]</sup>.


### Sensor in Other Languages

- Dutch: NetFlow v5 (aangepast)

- French: NetFlow v5 personnalisé
- German: NetFlow v5 (Benutzerdefiniert)
- Japanese: NetFlow v5(カスタム)
- Portuguese: NetFlow v5 (customizado)
- Russian: NetFlow v5 (настраиваемый)
- Simplified Chinese: NetFlow v5 (自定义)
- Spanish: NetFlow v5 (personalizado)

## Remarks

Consider the following [remarks](#)<sup>1497</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
NetFlow	This sensor requires that the NetFlow export of the respective version is enabled on the target system. The target system must send the flow data stream to the IP address of the probe system.
Channels	This sensor does not officially support more than <a href="#">50 channels</a> .
Cluster probe	This sensor does not support cluster probes. You can only set it up on local probes or remote probes.
IPv6	This sensor supports IPv6.
Knowledge Base	Knowledge Base: <a href="#">What is the Active Flow Timeout in flow sensors?</a>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ

**Priority** ⓘ

Example Name

---

exampletag ✕ +

---

★★★★☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- bandwidthsensor
- netflowsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## NetFlow v5 Specific Settings

### NetFlow v5 Specific Settings

**Receive Packets on UDP Port** ⓘ 9997

---

**Sender IP Address** ⓘ

---

**Receive Packets on IP Address** ⓘ

⇅ Probe's Local IP Addresses

---

192.0.2.0

---

**Active Flow Timeout (Minutes)** ⓘ 10

---

**Sampling Mode** ⓘ

Disable (default)
 

Enable

---

**Channel Definition** ⓘ

---

**Stream Data Handling** ⓘ









Discard stream data (default)
 




Store stream data only for the 'Other' channel

Store all stream data


NetFlow v5 Specific Settings



Setting	Description
Receive Packets on UDP Port	<p>Enter the User Datagram Protocol (UDP) port number on which PRTG receives the flow packets. It must match the UDP port number in the NetFlow export options of the hardware router device. Enter an integer.</p> <p> When you configure the export, make sure that you select the appropriate NetFlow version for this sensor.</p>
Sender IP Address	<p>Enter the IP address of the sending device that you want to receive the NetFlow from. Enter an IP address to only receive data from a specific device or leave the field empty to receive data from any device on the specified port.</p>
Receive Packets on IP Address	<p>Select the IP addresses on which PRTG listens to NetFlow packets. The list of IP addresses is specific to your setup. To select an IP address, enable a check box in front of the respective line. The IP address that you select must match the IP address in the NetFlow export options of the hardware router device.</p> <p> When you configure the export, make sure that you select the appropriate NetFlow version for this sensor.</p> <p> You can also select all items or cancel the selection by using the check box in the table header.</p>
Active Flow Timeout (Minutes)	<p>Enter a time span in minutes after which the sensor must receive new flow data. If the timeout elapses and the sensor receives no new data during this time, it shows the Unknown <a href="#">status</a>. Enter an integer. The maximum timeout is 60 minutes.</p> <p> We recommend that you set the timeout one minute longer than the timeout in the hardware router device.</p> <p> If you set this value too low, flow information might be lost.</p> <p> For more information, see the Knowledge Base: <a href="#">What is the Active Flow Timeout in flow sensors?</a></p> <p> If the target device sends incorrect time information that results in wrong monitoring data, try to use 0 as the active flow timeout. This ignores the start and stop information of a flow as provided by the device and accounts all data to the current point in time. It might result in spikes but the sensor captures all data.</p>
Sampling Mode	<p>Define if you want to use the sampling mode:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Use the standard flow.</li> <li>▪ Enable: Use the sampling mode and specify the Sampling Rate below.</li> </ul> <p> This setting must match the setting in the xFlow exporter.</p>

Setting	Description
Sampling Rate	<p>This setting is only visible if you select <a href="#">Enable</a> above.</p> <p>Enter a number that matches the sampling rate in your device that exports the flows. If the number is different, monitoring results will be incorrect. Enter an integer.</p>
Channel Definition	<p>Enter a channel definition to divide the traffic into different channels. Enter each definition in one line. The sensor accounts all traffic that you do not define a channel for to the default channel Other.</p> <p> For more information, see section <a href="#">Channel Definitions for Flow, IPFIX and Packet Sniffer Sensors</a>.</p> <p> Extensive use of many filters can cause load problems on the probe system. We recommend that you define specific, well-chosen filters for the data that you really want to analyze. We recommend that you do not use more than 20 channels in graphs and tables, and not more than 100 channels in total. For performance reasons, we recommend that you add several sensors with fewer channels each.</p>
Stream Data Handling	<p>Define what PRTG does with the stream and packet data:</p> <ul style="list-style-type: none"> <li>▪ Discard stream data (default): Do not store the stream and packet data.</li> <li>▪ Store stream data only for the 'Other' channel: Only store stream and packet data that is not otherwise filtered and is therefore accounted to the default Other channel. PRTG stores this data in the \StreamLog subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Streams Sensor [ID] (1).csv. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> <li>▪ Store all stream data: Store all stream and packet data. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> Use with caution. It can create huge data files. We recommend that you only use this setting for a short time.</p>

## Filtering

 For more information, see section [Filter Rules](#) 1503.

**Filtering**

**Filters** To include and exclude specific traffic, you can define filter rules based on the following format guidelines:

- field[filter]

**Fields:**

IP, Port, SourceIP, SourcePort, DestinationIP, DestinationPort, Protocol (values TCP, UDP, ICMP, OSPFIGP or any number), ToS, DSCP

**Additional IPFIX fields:**

Interface, ASI, InboundInterface, OutboundInterface, SourceASI, DestinationASI, MAC, SourceMAC, DestinationMAC, Mask, SourceMask, DestinationMask ('Masks' represent subnet masks in the form of a single number ('number of contiguous bits')), NextHop (IP Address), VLAN, SourceVLAN, DestinationVLAN ('VLANs' represent a VLAN identifier)

Include Filter ⓘ

Exclude Filter ⓘ

Filtering

Setting	Description
Include Filter	Define if you want to filter any traffic. If you leave this field empty, the sensor includes all traffic. To include specific traffic only, define filters using a special <a href="#">syntax</a> .
Exclude Filter	First, the sensor considers the filters in Include Filter. From this subset, you can explicitly exclude traffic, using the same syntax.

## Sensor Display


**Sensor Display**

Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display


Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.  ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.
Graph Type	Define how this sensor shows different channels:

Setting	Description
	<ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Primary Toplist

**Primary Toplist** Primary Toplist ⓘ Top Connections

Primary Toplist

Setting	Description
Primary Toplist	<p>Define which Toplist is the primary Toplist of the sensor:</p> <ul style="list-style-type: none"> <li>Top Talkers</li> <li>Top Connections</li> <li>Top Protocols</li> <li><a href="#">[Any custom Toplists you add]</a></li> </ul> <p> PRTG shows the primary Toplist in maps when you add a Toplist object.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Toplists

For all Flow (NetFlow, jFlow, sFlow, IPFIX) and Packet Sniffer sensors, Toplists are available on the sensor's Overview tab. Using Toplists, you can review traffic data for small time periods in great detail.

■ For more information, see section [Toplists](#).

## Filter Rules

■ For more information, see section [Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
[Custom]	The traffic by type according to the channel definition
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Other	All traffic for which no channel is defined
Total	The total traffic ⓘ This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

What is the Active Flow Timeout in flow sensors?

- <https://kb.paessler.com/en/topic/66485>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

### ✂ PAESSLER TOOLS

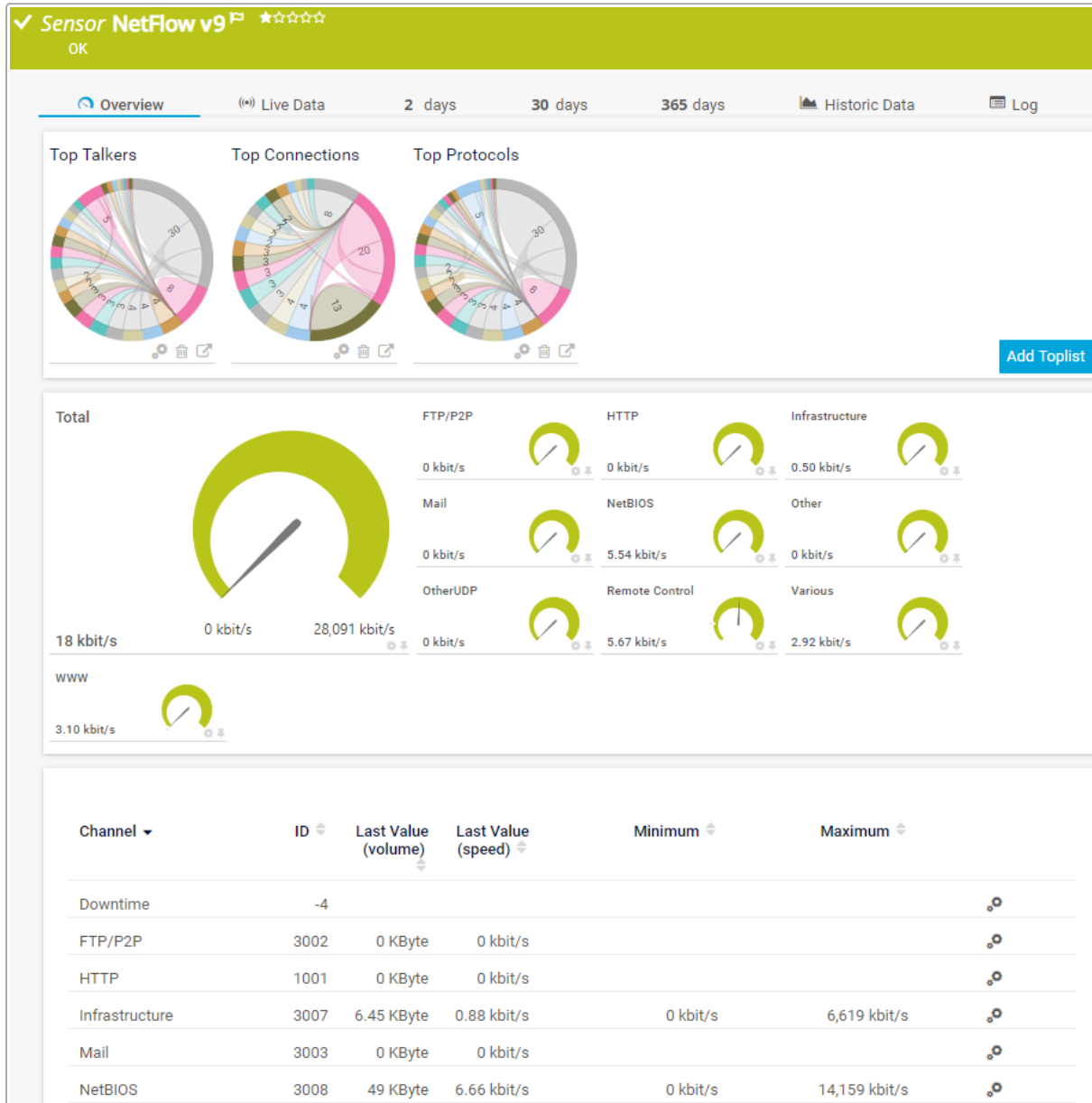
NetFlow Tester

- <https://www.paessler.com/tools/netflowtester>

## 7.8.123 NetFlow v9 Sensor

The NetFlow v9 sensor receives traffic data from a NetFlow v9-compatible device and shows the traffic by type. This sensor has several filter options to divide traffic into different channels.

**i** Make sure that the sensor matches the NetFlow version that your device exports.



NetFlow v9 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).


### Sensor in Other Languages

- Dutch: NetFlow v9
- French: NetFlow v9

- German: NetFlow v9
- Japanese: NetFlow v9
- Portuguese: NetFlow v9
- Russian: NetFlow v9
- Simplified Chinese: NetFlow v9
- Spanish: NetFlow v9

## Remarks

Consider the following [remarks](#) <sup>[1506]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
NetFlow	This sensor requires that the NetFlow export of the respective version is enabled on the target system. The target system must send the flow data stream to the IP address of the probe system.
Cluster probe	This sensor does not support cluster probes. You can only set it up on local probes or remote probes.
IPv6	This sensor supports IPv6.
Clone sensor	If you clone this sensor to the <b>same</b> probe, PRTG keeps the <a href="#">selected IP addresses</a> <sup>[1508]</sup> on which it listens for Flow (NetFlow, jFlow, sFlow, IPFIX) packets. If you clone this sensor to a <b>different</b> probe, PRTG selects <b>all</b> available IP addresses by default.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">What is the Active Flow Timeout in flow sensors?</a></li> <li>▪ Knowledge Base: <a href="#">How can I change the default groups and channels for flow and Packet Sniffer sensors?</a></li> </ul>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.



## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- bandwidthsensor
- netflowsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## NetFlow v9 Specific Settings

### NetFlow v9 Specific Settings

**Receive Packets on UDP Port** ⓘ 9997

---

**Sender IP Address** ⓘ

---

**Receive Packets on IP Address** ⓘ

▾ Probe's Local IP Addresses

---

192.0.2.0

---

**Active Flow Timeout (Minutes)** ⓘ 10

---

**Sampling Mode** ⓘ  Disable (default)  
 Enable

---

**Stream Data Handling** ⓘ  Discard stream data (default)  
 Store stream data only for the 'Other' channel  
 Store all stream data

NetFlow v9 Specific Settings

Setting	Description
Receive Packets on UDP Port	<p>Enter the User Datagram Protocol (UDP) port number on which PRTG receives the flow packets. It must match the UDP port number in the NetFlow export options of the hardware router device. Enter an integer.</p> <p> When you configure the export, make sure that you select the appropriate NetFlow version for this sensor.</p>
Sender IP Address	<p>Enter the IP address of the sending device that you want to receive the NetFlow from. Enter an IP address to only receive data from a specific device or leave the field empty to receive data from any device on the specified port.</p>
Receive Packets on IP Address	<p>Select the IP addresses on which PRTG listens to NetFlow packets. The list of IP addresses is specific to your setup. To select an IP address, enable a check box in front of the respective line. The IP address that you select must match the IP address in the NetFlow export options of the hardware router device.</p> <p> When you configure the export, make sure that you select the appropriate NetFlow version for this sensor.</p> <p> You can also select all items or cancel the selection by using the check box in the table header.</p>
Active Flow Timeout (Minutes)	<p>Enter a time span in minutes after which the sensor must receive new flow data. If the timeout elapses and the sensor receives no new data during this time, it shows the Unknown <a href="#">status</a>. Enter an integer. The maximum timeout is 60 minutes.</p> <p> We recommend that you set the timeout one minute longer than the timeout in the hardware router device.</p> <p> If you set this value too low, flow information might be lost.</p> <p> For more information, see the Knowledge Base: <a href="#">What is the Active Flow Timeout in flow sensors?</a></p> <p> If the target device sends incorrect time information that results in wrong monitoring data, try to use 0 as the active flow timeout. This ignores the start and stop information of a flow as provided by the device and accounts all data to the current point in time. It might result in spikes but the sensor captures all data.</p>
Sampling Mode	<p>Define if you want to use the sampling mode:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Use the standard flow.</li> <li>▪ Enable: Use the sampling mode and specify the Sampling Rate below.</li> </ul> <p> This setting must match the setting in the xFlow exporter.</p>

Setting	Description
Sampling Rate	<p>This setting is only visible if you select Enable above.</p> <p>Enter a number that matches the sampling rate in the exporting device. If the number is different, monitoring results will be incorrect. Enter an integer.</p>
Stream Data Handling	<p>Define what PRTG does with the stream and packet data:</p> <ul style="list-style-type: none"> <li>Discard stream data (default): Do not store the stream and packet data.</li> <li>Store stream data only for the 'Other' channel: Only store stream and packet data that is not otherwise filtered and is therefore accounted to the default Other channel. PRTG stores this data in the \StreamLog subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Streams Sensor [ID] (1).csv. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> <li>Store all stream data: Store all stream and packet data. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><b>i</b> Use with caution. It can create huge data files. We recommend that you only use this setting for a short time.</p>

## Channel Configuration

Channel Configuration

Channel Selection ⓘ

Group	✕	✓	🔍	Content
Web	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	WWW Traffic: HTTP, HTTPS
File Transfer	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	File Transfer: FTP (Control)
Mail	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Mail Traffic: IMAP, POP3, SMTP
Chat	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Chat, Instant Messaging: IRC, AIM
Remote Control	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Remote Control: RDP, SSH, Telnet, VNC
Infrastructure	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Network Services: DHCP, DNS, Ident, ICMP, SNMP
NetBIOS	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	NetBIOS: NETBIOS
Citrix	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Citrix: Citrix
Other Protocols	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Various: Other UDP, Other TCP

**Note** You can change the default configuration for groups and channels. This way, you do not have to customize this setting each time that you add this sensor type. For details, see the Knowledge Base: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)

Channel Configuration

Setting	Description
Channel Selection	<p>Define the categories that the sensor accounts the traffic to:</p> <ul style="list-style-type: none"> <li>Web: Internet web traffic.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ File Transfer: Traffic from FTP.</li> <li>▪ Mail: Internet mail traffic.</li> <li>▪ Chat: Traffic from chat and instant messaging.</li> <li>▪ Remote Control: Traffic from remote control applications such as RDP, SSH, Telnet, and Virtual Network Computing (VNC).</li> <li>▪ Infrastructure: Traffic from network services such as DHCP, DNS, Ident, ICMP, and SNMP.</li> <li>▪ NetBIOS: Traffic from NetBIOS communication.</li> <li>▪ Citrix: Traffic from Citrix applications.</li> <li>▪ Other Protocols: Traffic from various other protocols via UDP and TCP.</li> </ul> <p>For each group, you can select how many channels the sensor uses, that is, how detailed the sensor divides the traffic:</p> <ul style="list-style-type: none"> <li>▪ No (✘): Do not account traffic of this group in its own channel. The sensor accounts all traffic of this group to the default channel named Other.</li> <li>▪ Yes (✔): Count all traffic of this group and summarize it in one channel.</li> <li>▪ Detail (🔍): Count all traffic of this group and further divide it into different channels. The traffic appears in several channels that you can see in the Content column.</li> </ul> <p><b>i</b> Extensive use of this option can cause load problems on the probe system. We recommend that you set specific, well-chosen filters for the data that you really want to analyze.</p> <p><b>■</b> You can change the default configuration for groups and channels. For more information, see the Knowledge Base: <a href="#">How can I change the default groups and channels for flow and Packet Sniffer sensors?</a></p>

## Filtering

**■** For more information, see section [Filter Rules](#)<sup>[1513]</sup>.

**Filtering**

**Filters** To include and exclude specific traffic, you can define filter rules based on the following format guidelines:

- field[filter]

**Fields:**

IP, Port, SourceIP, SourcePort, DestinationIP, DestinationPort, Protocol (values TCP, UDP, ICMP, OSPFIGP or any number), ToS, DSCP

**Additional IPFIX fields:**

Interface, ASI, InboundInterface, OutboundInterface, SourceASI, DestinationASI, MAC, SourceMAC, DestinationMAC, Mask, SourceMask, DestinationMask ('Masks' represent subnet masks in the form of a single number ('number of contiguous bits')), NextHop (IP Address), VLAN, SourceVLAN, DestinationVLAN ('VLANs' represent a VLAN identifier)

Include Filter ⓘ

Exclude Filter ⓘ

Filtering

Setting	Description
Include Filter	Define if you want to filter any traffic. If you leave this field empty, the sensor includes all traffic. To include specific traffic only, define filters using a special <a href="#">syntax</a> .
Exclude Filter	First, the sensor considers the filters in Include Filter. From this subset, you can explicitly exclude traffic, using the same syntax.

## Sensor Display


**Sensor Display**

Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display


Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.  ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.
Graph Type	Define how this sensor shows different channels:

Setting	Description
	<ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Primary Toplist

**Primary Toplist** Primary Toplist ⓘ Top Connections

Primary Toplist

Setting	Description
Primary Toplist	<p>Define which Toplist is the primary Toplist of the sensor:</p> <ul style="list-style-type: none"> <li>Top Talkers</li> <li>Top Connections</li> <li>Top Protocols</li> <li><a href="#">[Any custom Toplists you add]</a></li> </ul> <p> PRTG shows the primary Toplist in maps when you add a Toplist object.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Toplists

For all Flow (NetFlow, jFlow, sFlow, IPFIX) and Packet Sniffer sensors, Toplists are available on the sensor's Overview tab. Using Toplists, you can review traffic data for small time periods in great detail.

■ For more information, see section [Toplists](#).

## Filter Rules

■ For more information, see section [Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Chat	The traffic from chat and instant messaging (IRC, AIM)
Citrix	The traffic from Citrix applications
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
FTP/P2P	The traffic from file transfer (FTP/P2P)
Infrastructure	The traffic from network services (DHCP, DNS, Ident, ICMP, SNMP)
Mail	The internet mail traffic (IMAP, POP3, SMTP)
NetBIOS	The traffic from NetBIOS communication
Other	The traffic from various other protocols (UDP, TCP)
Remote Control	The traffic from remote control applications (RDP, SSH, Telnet, Virtual Network Computing (VNC))
Total	The total traffic ⓘ This channel is the primary channel by default.
Various	The traffic from various other sources

Channel	Description
WWW	The traffic from the web (HTTP, HTTPS)

## More

### KNOWLEDGE BASE

What is the Active Flow Timeout in flow sensors?

- <https://kb.paessler.com/en/topic/66485>

How can I change the default groups and channels for flow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

### PAESSLER TOOLS

NetFlow Tester

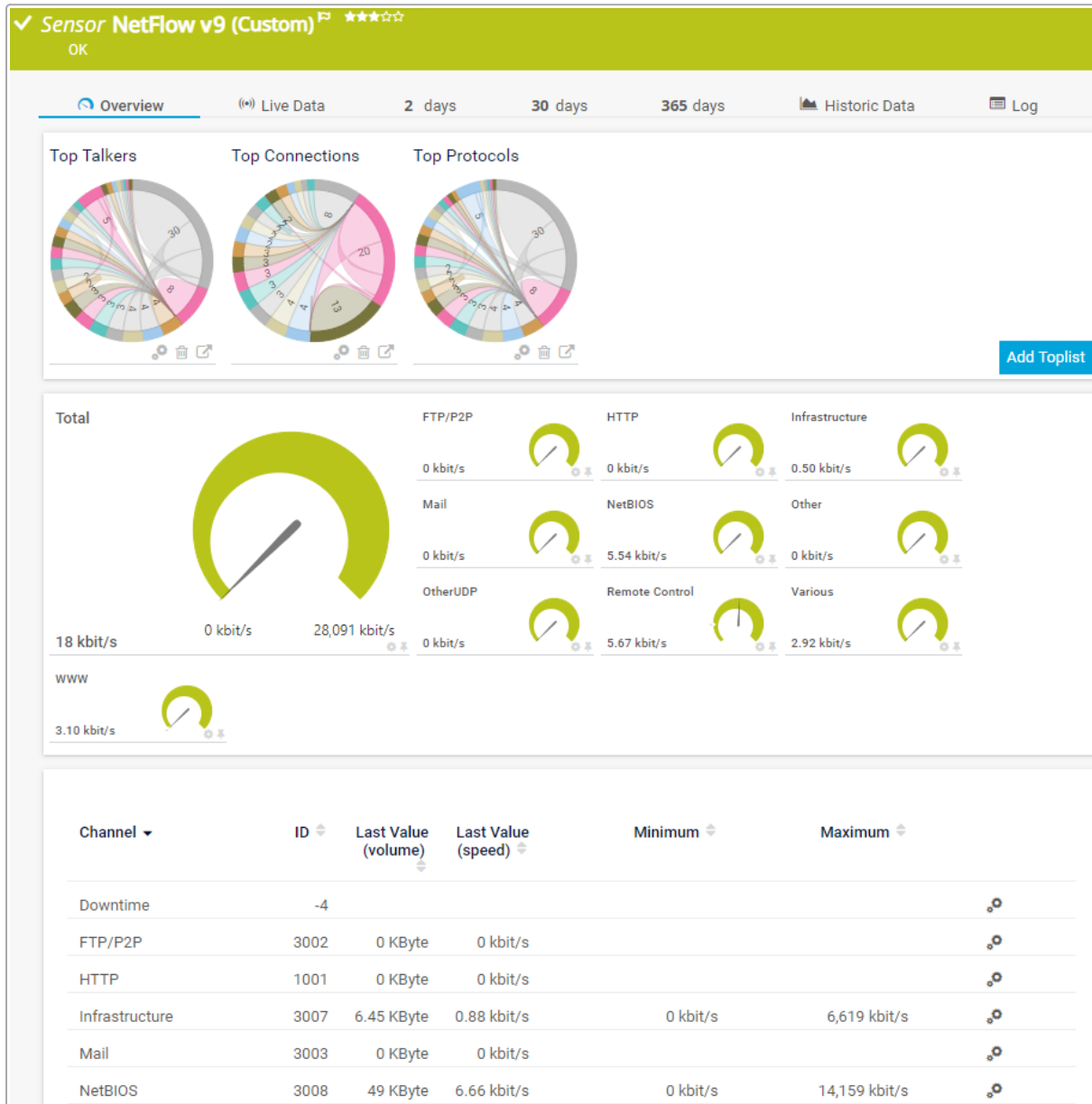
- <https://www.paessler.com/tools/netflowtester>



## 7.8.124 NetFlow v9 (Custom) Sensor

The NetFlow v9 (Custom) sensor receives traffic data from a NetFlow v9-compatible device and shows the traffic by type. With this sensor, you can define your own channel definitions to divide traffic into different channels.

**i** Make sure that the sensor matches the NetFlow version that your device exports.



NetFlow v9 (Custom) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) <sup>(1522)</sup>.


### Sensor in Other Languages

- Dutch: NetFlow v9 (aangepast)

- French: NetFlow v9 personnalisé
- German: NetFlow v9 (Benutzerdefiniert)
- Japanese: NetFlow v9(カスタム)
- Portuguese: NetFlow v9 (customizado)
- Russian: NetFlow v9 (настраиваемый)
- Simplified Chinese: NetFlow v9 (自定义)
- Spanish: NetFlow v9 (personalizado)

## Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
NetFlow	This sensor requires that the NetFlow export of the respective version is enabled on the target system. The target system must send the flow data stream to the IP address of the probe system.
Channels	This sensor does not officially support more than <a href="#">50 channels</a> .
Cluster probe	This sensor does not support cluster probes. You can only set it up on local probes or remote probes.
IPv6	This sensor supports IPv6.
Knowledge Base	Knowledge Base: <a href="#">What is the Active Flow Timeout in flow sensors?</a>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- bandwidthsensor
- netflowsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## NetFlow v9 Specific Settings

### NetFlow v9 Specific Settings

**Receive Packets on UDP Port** ⓘ

---

**Sender IP Address** ⓘ

---

**Receive Packets on IP Address** ⓘ

▾ Probe's Local IP Addresses

---

---

**Active Flow Timeout (Minutes)** ⓘ

---

**Sampling Mode** ⓘ

Disable (default)

Enable

---

**Channel Definition** ⓘ

---









**Stream Data Handling** ⓘ

Discard stream data (default)

Store stream data only for the 'Other' channel

Store all stream data

NetFlow v9 Specific Settings

Setting	Description
Receive Packets on UDP Port	<p>Enter the User Datagram Protocol (UDP) port number on which PRTG receives the flow packets. It must match the UDP port number in the NetFlow export options of the hardware router device. Enter an integer.</p> <p> When you configure the export, make sure that you select the appropriate NetFlow version for this sensor.</p>
Sender IP Address	<p>Enter the IP address of the sending device that you want to receive the NetFlow from. Enter an IP address to only receive data from a specific device or leave the field empty to receive data from any device on the specified port.</p>
Receive Packets on IP Address	<p>Select the IP addresses on which PRTG listens to NetFlow packets. The list of IP addresses is specific to your setup. To select an IP address, enable a check box in front of the respective line. The IP address that you select must match the IP address in the NetFlow export options of the hardware router device.</p> <p> When you configure the export, make sure that you select the appropriate NetFlow version for this sensor.</p> <p> You can also select all items or cancel the selection by using the check box in the table header.</p>
Active Flow Timeout (Minutes)	<p>Enter a time span in minutes after which the sensor must receive new flow data. If the timeout elapses and the sensor receives no new data during this time, it shows the Unknown <a href="#">status</a>. Enter an integer. The maximum timeout is 60 minutes.</p> <p> We recommend that you set the timeout one minute longer than the timeout in the hardware router device.</p> <p> If you set this value too low, flow information might be lost.</p> <p> For more information, see the Knowledge Base: <a href="#">What is the Active Flow Timeout in flow sensors?</a></p> <p> If the target device sends incorrect time information that results in wrong monitoring data, try to use 0 as the active flow timeout. This ignores the start and stop information of a flow as provided by the device and accounts all data to the current point in time. It might result in spikes but the sensor captures all data.</p>
Sampling Mode	<p>Define if you want to use the sampling mode:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Use the standard flow.</li> <li>▪ Enable: Use the sampling mode and specify the Sampling Rate below.</li> </ul> <p> This setting must match the setting in the xFlow exporter.</p>

Setting	Description
Sampling Rate	<p>This setting is only visible if you select <a href="#">Enable</a> above.</p> <p>Enter a number that matches the sampling rate in your device that exports the flows. If the number is different, monitoring results will be incorrect. Enter an integer.</p>
Channel Definition	<p>Enter a channel definition to divide the traffic into different channels. Enter each definition in one line. The sensor accounts all traffic that you do not define a channel for to the default channel Other.</p> <p>■ For more information, see section <a href="#">Channel Definitions for Flow, IPFIX and Packet Sniffer Sensors</a>.</p> <p>ⓘ Extensive use of many filters can cause load problems on the probe system. We recommend that you define specific, well-chosen filters for the data that you really want to analyze. We recommend that you do not use more than 20 channels in graphs and tables, and not more than 100 channels in total. For performance reasons, we recommend that you add several sensors with fewer channels each.</p>
Stream Data Handling	<p>Define what PRTG does with the stream and packet data:</p> <ul style="list-style-type: none"> <li>▪ Discard stream data (default): Do not store the stream and packet data.</li> <li>▪ Store stream data only for the 'Other' channel: Only store stream and packet data that is not otherwise filtered and is therefore accounted to the default Other channel. PRTG stores this data in the \StreamLog subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Streams Sensor [ID] (1).csv. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> <li>▪ Store all stream data: Store all stream and packet data. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>ⓘ Use with caution. It can create huge data files. We recommend that you only use this setting for a short time.</p>

## Filtering

■ For more information, see section [Filter Rules](#) <sup>[1522]</sup>.

**Filtering**

**Filters** To include and exclude specific traffic, you can define filter rules based on the following format guidelines:

- field[filter]

**Fields:**

IP, Port, SourceIP, SourcePort, DestinationIP, DestinationPort, Protocol (values TCP, UDP, ICMP, OSPFIGP or any number), ToS, DSCP

**Additional IPFIX fields:**

Interface, ASI, InboundInterface, OutboundInterface, SourceASI, DestinationASI, MAC, SourceMAC, DestinationMAC, Mask, SourceMask, DestinationMask ('Masks' represent subnet masks in the form of a single number ('number of contiguous bits')), NextHop (IP Address), VLAN, SourceVLAN, DestinationVLAN ('VLANs' represent a VLAN identifier)

Include Filter ⓘ

Exclude Filter ⓘ

Filtering

Setting	Description
Include Filter	Define if you want to filter any traffic. If you leave this field empty, the sensor includes all traffic. To include specific traffic only, define filters using a special <a href="#">syntax</a> .
Exclude Filter	First, the sensor considers the filters in Include Filter. From this subset, you can explicitly exclude traffic, using the same syntax.

## Sensor Display


**Sensor Display**

Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display


Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.  ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.
Graph Type	Define how this sensor shows different channels:

Setting	Description
	<ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Primary Toplist

**Primary Toplist** Primary Toplist ⓘ Top Connections

Primary Toplist

Setting	Description
Primary Toplist	<p>Define which Toplist is the primary Toplist of the sensor:</p> <ul style="list-style-type: none"> <li>Top Talkers</li> <li>Top Connections</li> <li>Top Protocols</li> <li><a href="#">[Any custom Toplists you add]</a></li> </ul> <p> PRTG shows the primary Toplist in maps when you add a Toplist object.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Toplists

For all Flow (NetFlow, jFlow, sFlow, IPFIX) and Packet Sniffer sensors, Toplists are available on the sensor's Overview tab. Using Toplists, you can review traffic data for small time periods in great detail.

■ For more information, see section [Toplists](#).

## Filter Rules

■ For more information, see section [Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
[Custom]	The traffic by type according to the channel definition
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Other	All traffic for which no channel is defined
Total	The total traffic ⓘ This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

What is the Active Flow Timeout in flow sensors?

- <https://kb.paessler.com/en/topic/66485>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

### ✂ PAESSLER TOOLS

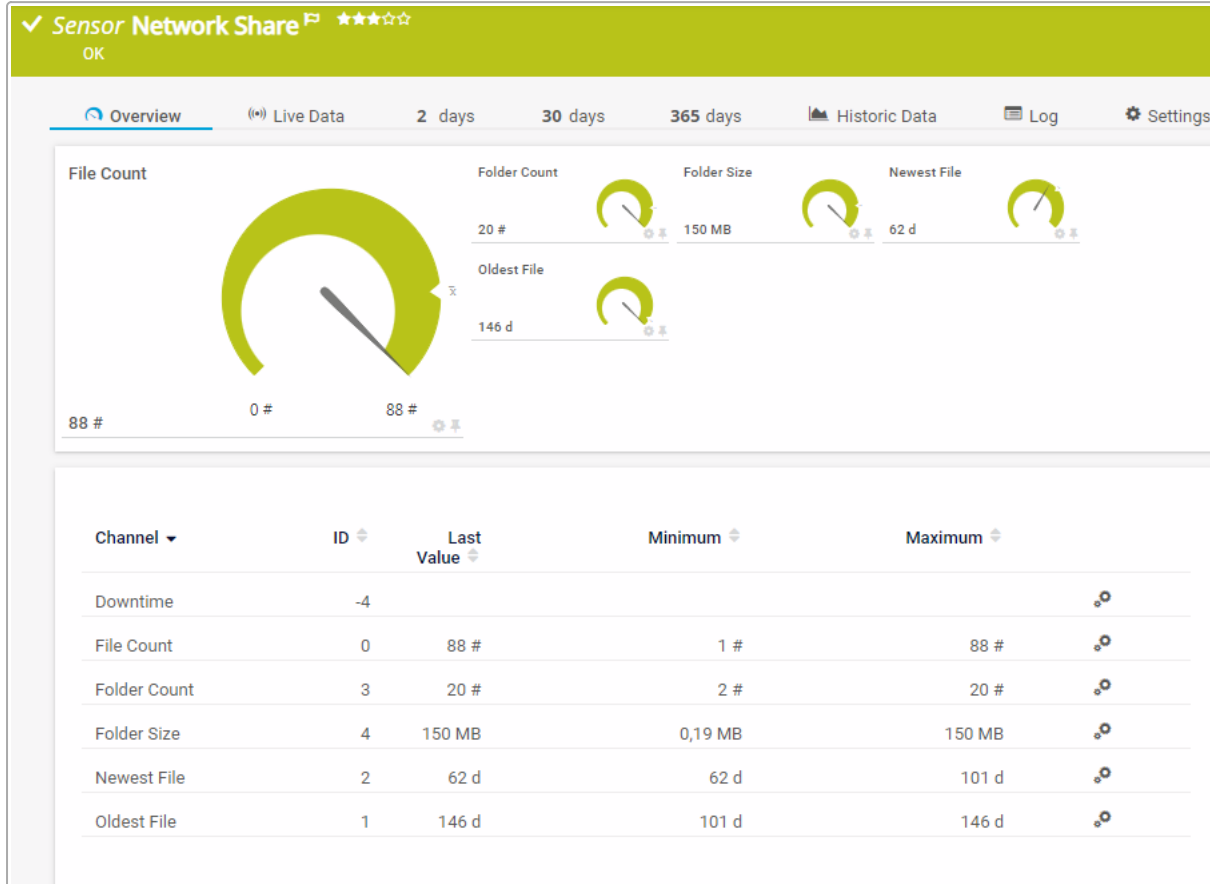
NetFlow Tester



- <https://www.paessler.com/tools/netflowtester>

## 7.8.125 Network Share Sensor

The Network Share sensor monitors a Server Message Block (SMB) or Common Internet File System (CIFS) network share.



Network Share Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1529]</sup>.

### Sensor in Other Languages

- Dutch: Netwerkshare
- French: Partage réseau
- German: Netzwerkfreigabe
- Japanese: ネットワーク共有
- Portuguese: Compartilhamento de rede
- Russian: Сетевая папка
- Simplified Chinese: 网络共享
- Spanish: Recurso compartido de red

## Remarks

Consider the following [remarks](#)<sup>[1525]</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
Scanning interval	<ul style="list-style-type: none"> <li>The minimum scanning interval of this sensor is <b>1 minute</b>.</li> <li>The recommended scanning interval of this sensor is <b>5 minutes</b>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★★★★☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cifs
- folder
- networkshare
- smb

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Network Share Specific

**Network Share Specific**

Path ⓘ \_\_\_\_\_

---

Timeout (Sec.) ⓘ 300

---

Recurse Subfolders ⓘ  Do not recurse subfolders (default)  
 Monitor the folder and its subfolders (recursive)

Filter by File Name ⓘ  Disable (default)  
 Include filter  
 Exclude filter

Filter by File Age ⓘ  Disable (default)  
 Enable

Network Share Specific

Setting	Setting
Path	Enter the path of the network share that you want to monitor. For example, <code>folder\subfolder</code> .
Timeout (Sec.)	Enter a timeout in seconds. If the scan of the folder takes longer, the sensor cancels the request and shows an error message. If two consecutive scans fail, the sensor shows the Down status. The default value is 300 seconds (5 minutes).
Recurse Subfolders	Specify if the sensor includes subfolders in the folder monitoring: <ul style="list-style-type: none"> <li>Do not recurse subfolders (default): Only monitor the folder. Do not monitor its subfolders.</li> <li>Monitor the folder and its subfolders (recursive): Monitor the folder and all of its subfolders. <ul style="list-style-type: none"> <li><b>i</b> If you recurse subfolders in large directories that have a high number of branches, this might cause timeout errors or performance issues.</li> </ul> </li> </ul>
Filter by File Name	Select if you want to filter by file name: <ul style="list-style-type: none"> <li>Disable (default): Do not filter by file name.</li> <li>Include filter: The sensor counts files that match the File Filter.</li> <li>Exclude filter: The sensor counts files that do not match the File Filter.</li> </ul>
File Filter	This setting is only visible if you select Include filter or Exclude filter above.

Setting	Setting
	<p>Enter a comma-separated list of file names, file formats, or patterns you want to filter for. For example, '*.pdf, *.docx' includes or excludes files with the file formats .pdf or .docx.</p> <p><b>i</b> The file filter is not case-sensitive and supports wildcards (*).</p>
Filter by File Age	<p>Select if you want to filter by file age:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not filter by file age.</li> <li>▪ Enable: Filter by file age.</li> </ul>
Newer Than	<p><b>This setting is only visible if you select Enable above.</b></p> <p>Enter a file age. The sensor only counts files that are younger than this age.</p> <p><b>i</b> Leave this field empty if you only want to filter for files with the Older Than setting.</p>
Older Than	<p><b>This setting is only visible if you select Enable above.</b></p> <p>Enter a file age. The sensor only counts files that are older than this age.</p> <p><b>i</b> Leave this field empty if you only want to filter for files with the Newer Than setting.</p>
File Age Filter Unit	<p><b>This setting is only visible if you select Enable above.</b></p> <p>Select the time unit that you want to use for Filter by File Age:</p> <ul style="list-style-type: none"> <li>▪ Days (default)</li> <li>▪ Hours</li> <li>▪ Minutes</li> </ul>

## Sensor Display


**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i** 
 Show channels independently (default)
   
 Stack channels on top of each other

Sensor Display


Setting	Setting
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**


**Result Handling** **i**
 Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
File Count	<p>The number of files in the folder</p> <p><b>i</b> The sensor counts all files in a folder, including <a href="#">hidden files</a>.</p> <p><b>i</b> This channel is the primary channel by default.</p>
Folder Count	The number of folders
Folder Size	The folder size
Newest File	<p>The time since the newest modification of a file in the folder (newest file)</p> <p><b>i</b> The sensor shows a negative value if the date of a modified file is in the future.</p>
Oldest File	The time since the oldest modification of a file in the folder (oldest file)

## More

 KNOWLEDGE BASE

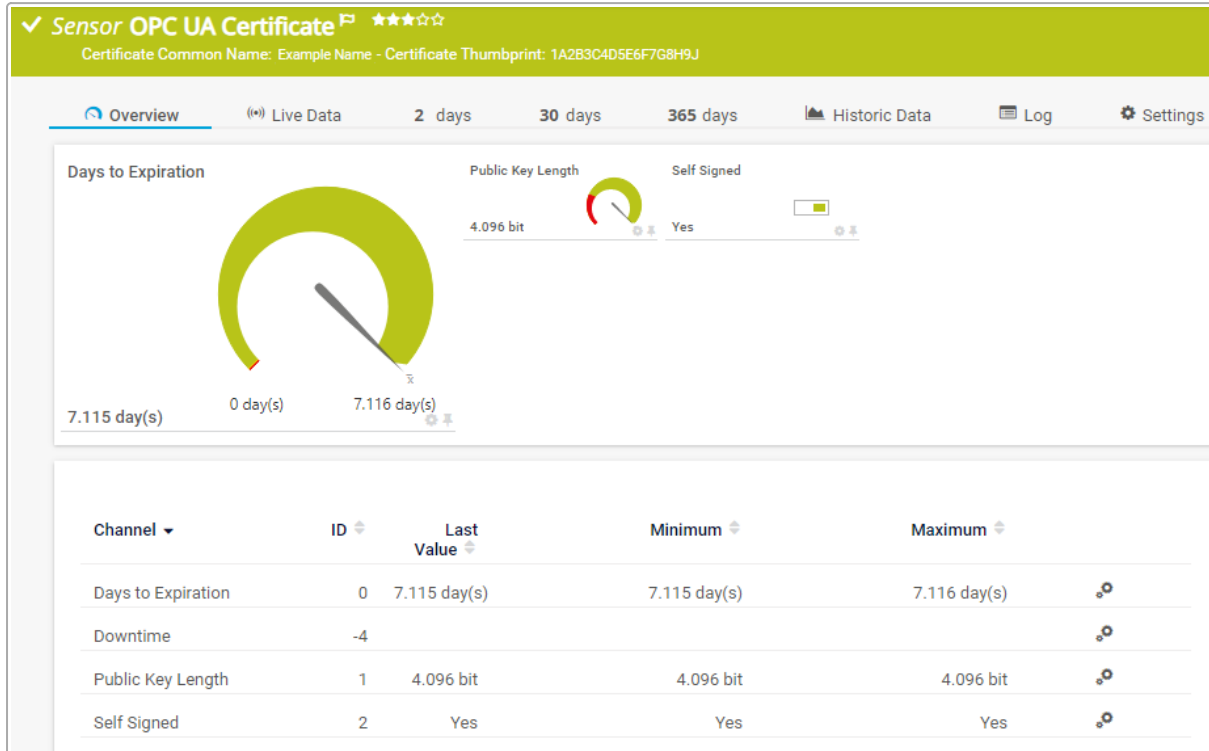
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>



## 7.8.126 OPC UA Certificate Sensor

The OPC UA Certificate sensor monitors the certificate of an OPC Unified Architecture (OPC UA) server.



OPC UA Certificate Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1534</sup>.

### Sensor in Other Languages

- Dutch: OPC UA Certificaat
- French: Certificat OPC UA
- German: OPC UA Zertifikat
- Japanese: OPC UA 証明書
- Portuguese: Certificado OPC UA
- Russian: Сертификат OPC UA
- Simplified Chinese: OPC UA 证书
- Spanish: Certificado OPC UA

### Remarks

Consider the following [remarks](#)<sup>1531</sup> and requirements for this sensor:

Remark	Description
Valid port	This sensor requires a <a href="#">valid port</a> for the connection to the OPC UA server.
Credentials	This sensor requires credentials for OPC UA in the settings of the parent device.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">12 hours</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  X +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- certificate
- opcua
- opcuacertificate

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Days to Expiration	<p>The number of days to expiration</p> <p>ⓘ This channel is the primary channel by default.</p> <p>ⓘ This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: <a href="#">7 days</a></li> <li>▪ Lower warning limit: <a href="#">28 days</a></li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Public Key Length	<p>The public key length</p>

Channel	Description
	<p> This channel has default limits:</p> <ul style="list-style-type: none"><li>▪ Lower error limit: <a href="#">1024 bits</a></li><li>▪ Lower warning limit: <a href="#">1025 bits</a></li></ul>
Self Signed	If a self-signed certificate is used

## More

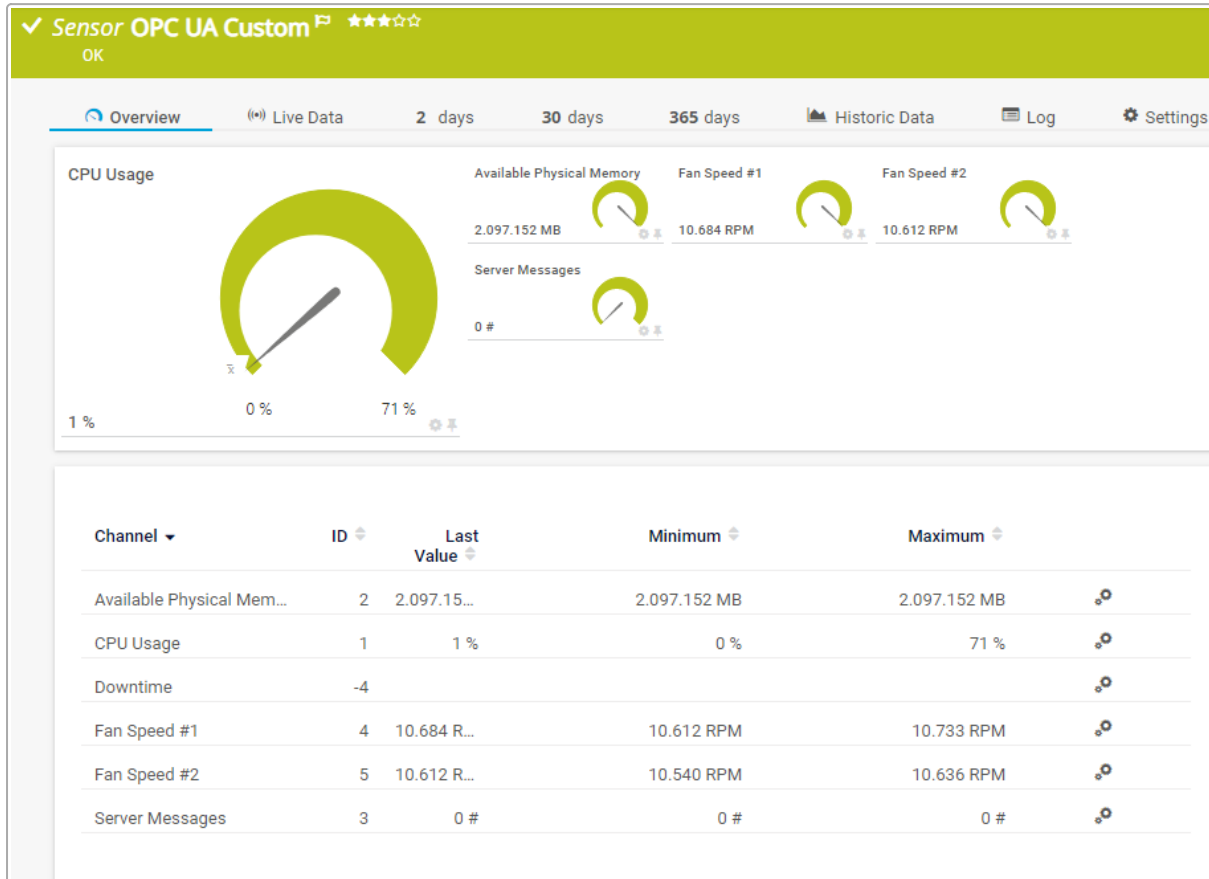
### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.127 OPC UA Custom Sensor

The OPC UA Custom sensor monitors up to ten numeric values returned by specific OPC Unified Architecture (OPC UA) NodeIDs.



OPC UA Custom Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[154]</sup>.

### Sensor in Other Languages




- Dutch: OPC UA Aangepast
- French: OPC UA personnalisé
- German: OPC UA (Benutzerdefiniert)
- Japanese: OPC UA カスタム
- Portuguese: OPC UA customizado
- Russian: Пользовательский OPC UA
- Simplified Chinese: OPC UA 自定义
- Spanish: OPC UA (personalizado)

## Remarks

Consider the following [remarks](#)<sup>1537</sup> and requirements for this sensor:

Remark	Description
Valid port	This sensor requires a <a href="#">valid port</a> for the connection to the OPC UA server.
Credentials	This sensor requires credentials for OPC UA in the settings of the parent device.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Scanning interval	The minimum scanning interval of this sensor is <a href="#">30 seconds</a> .
Multi-platform probe	You can add this sensor to a multi-platform probe.
Knowledge Base	Knowledge Base: <a href="#">Which OPC UA data types does the OPC UA Custom sensor support?</a>

## Add Sensor

Setting	Description
Channel #1 – #10 Naming Method	<p>Select the naming method for the channels of the sensor:</p> <ul style="list-style-type: none"> <li>▪ Use automatic naming (default): The sensor uses the name provided by the OPC UA node. <ul style="list-style-type: none"> <li> You cannot use automatic naming after sensor creation.</li> </ul> </li> <li>▪ Enter custom name: Enter a custom name in field Channel #1 - #10 Name. <ul style="list-style-type: none"> <li> You can change this value later in the <a href="#">channel settings</a> of this sensor.</li> </ul> </li> </ul>
Channel #1 - #10 Unit	<p>Enter the unit for the numeric value that this sensor monitors.</p> <ul style="list-style-type: none"> <li> You can change this value later in the <a href="#">channel settings</a> of this sensor.</li> </ul>

Setting	Description
Channel #1 – #10 NodeID	<p>Enter the NodeID from which you want to receive numeric data.</p> <p><b>i</b> A NodeID looks like this, for example: <code>ns=1;i=1234</code>, <code>ns=2;s=test_one</code>, or <code>'ns=1;s=test_one'[4]</code>. The sensor supports string identifiers, numeric identifiers, and array syntaxes.</p>
Channel #2 - #10	<p>You can define up to 10 channels. You must define at least one channel, so you see all available settings for Channel #1. Specify how to handle all other possible channels:</p> <ul style="list-style-type: none"> <li>▪ Disable: Do not create this channel.</li> <li>▪ Enable: Create this channel.</li> </ul> <p><b>i</b> It is not possible to enable or disable channels after sensor creation.</p>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** i

**Tags** i  x +

**Priority** i ★★★★★

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- opcua
- opcuacustom

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### OPC UA Specific

#### OPC UA Specific

**Sensor Message Node ID** i

**Channel #1 Node ID** i

OPC UA Specific



Setting	Description
Sensor Message NodeID	<p>Optionally enter the NodeID from which you want to receive a string that the sensor shows as sensor message.</p> <p><b>i</b> A NodeID looks like this, for example: <code>ns=1;i=1234</code>, <code>ns=2;s=test_one</code>, or <code>'ns=1;s=test_one'[4]</code>. The sensor supports string identifiers, numeric identifiers, and array syntaxes.</p> <p><b>i</b> The sensor only shows the received string if the sensor is in the Up status. If the sensor enters the Down status, the sensor message shows the error message instead.</p>
Channel #x NodeID	<p>The NodeID from which the sensor receives numeric data.</p> <p><b>i</b> A NodeID looks like this, for example: <code>ns=1;i=1234</code>, <code>ns=2;s=test_one</code>, or <code>'ns=1;s=test_one'[4]</code>. The sensor supports string identifiers, numeric identifiers, and array syntaxes.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>

Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**

Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><span style="font-size: 0.8em;">☁</span> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><span style="font-size: 0.8em;">ⓘ</span> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	The returned numeric values in up to ten channels

## More

### KNOWLEDGE BASE

Which OPC UA data types does the OPC UA Custom sensor support?

- <https://kb.paessler.com/en/topic/89236>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.128 OPC UA Server Status Sensor

The OPC UA Server Status sensor monitors the server status, uptime, and diagnostic information of an OPC Unified Architecture (OPC UA) server.



OPC UA Server Status Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: OPC UA Serverstatus
- French: OPC UA statut du serveur
- German: OPC UA Serverzustand
- Japanese: OPC UA サーバーステータス
- Portuguese: Status de servidor OPC UA

- Russian: Состояние сервера OPC UA
- Simplified Chinese: OPC UA 服务器状态
- Spanish: Estado del servidor OPC UA

## Remarks

Consider the following [remarks](#)<sup>1543</sup> and requirements for this sensor:

Remark	Description
Activated server diagnostics on your OPC UA server	This sensor requires activated diagnostic summary information settings on your OPC UA server to create all diagnostic channels. Without activated diagnostic summary information settings, the sensor can only show the server status and the uptime.  <b>i</b> Note that not all vendors support diagnostic summary information.
Valid port	This sensor requires a <a href="#">valid port</a> for the connection to the OPC UA server.
Credentials	This sensor requires credentials for OPC UA in the settings of the parent device.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- opcua
- opcuaserverstatus
- serverstatus

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ

Show channels independently (default)

Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Rejected Requests Count	The number of rejected requests
Rejected Session Count	The number of rejected sessions
Security Rejected Requests Count	The number of security rejected requests
Security Rejected Session Count	The number of security rejected sessions
Server Status	<p>The server status</p> <ul style="list-style-type: none"> <li>▪ Up status: Running, Test</li> <li>▪ Warning status: No Configuration, Shut Down, Suspended</li> <li>▪ Down status: Communication Fault, Failed, Unknown</li> </ul> <p> This channel is the primary channel by default.</p>
Session Abort Count	The number of session aborts
Session Count	The number of sessions
Session Timeout Count	The number of session timeouts
Subscription Count	The number of subscriptions
Uptime	The uptime

## More

### KNOWLEDGE BASE

What security features does PRTG include?

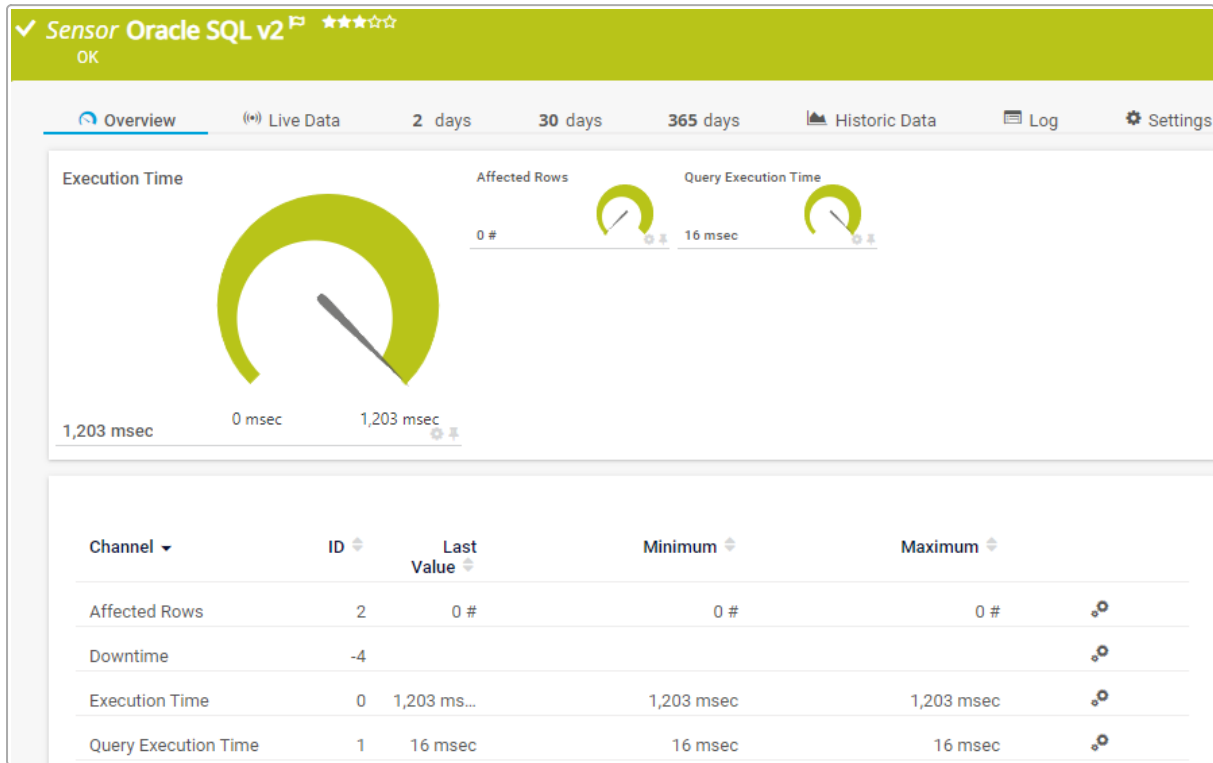
- <https://kb.paessler.com/en/topic/61108>



## 7.8.129 Oracle SQL v2 Sensor

The Oracle SQL v2 sensor monitors a database on an Oracle server and executes a query.

- i** The sensor can also process the data table and show the values that you define in individual channels.



Oracle SQL v2 Sensor

- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Oracle SQL v2
- French: Oracle SQL v2
- German: Oracle SQL v2
- Japanese: Oracle SQL v2
- Portuguese: Oracle SQL v2
- Russian: Oracle SQL v2
- Simplified Chinese: Oracle SQL v2
- Spanish: Oracle SQL v2

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
SQL query storage	This sensor requires that you store the SQL query in a file on the probe system. In a cluster, copy the file to every cluster node.  ■ For more information, see the Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a>
.NET 4.7.2 or later	This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.  ❗ If the framework is missing, you cannot create this sensor.  ■ For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a>
Oracle version	This sensor supports Oracle database servers as of version 10.2
IPv6	This sensor supports IPv6.
Lookups	This sensor can use <a href="#">lookups</a> <sup>[1554]</sup> . Select Lookup as Channel #x Unit and define the lookup file in Channel #x Lookup.
Credentials	Define the credentials for database management systems in settings that are higher in the object hierarchy.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">How to set up the SQL v2 sensors in PRTG? Is there a guide?</a></li> <li>▪ Knowledge Base: <a href="#">How can I monitor strings from an SQL database and show a sensor status depending on it?</a></li> <li>▪ Knowledge Base: <a href="#">How can I monitor error tables in SQL databases?</a></li> <li>▪ Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a></li> </ul>
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- sqlsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Database Specific

### Database Specific

**Identifier** ⓘ orcl

---

**Identification Parameter** ⓘ

SID (default)

SERVICE\_NAME

Database Specific

Setting	Description
Identifier	<p>Enter the <a href="#">Oracle System ID (SID)</a> or the <a href="#">SERVICE_NAME</a> of the database that the sensor connects to. Specify the Identification Parameter below. By default, the sensor uses the SID as the connection string.</p> <p> ⓘ You can find the SID or SERVICE_NAME in the <a href="#">CONNECT_DATA</a> part of the <a href="#">TNSNames.ora</a> file on the Oracle server. For example, a SID can look like this: <code>orcl</code></p>
Identification Parameter	<p>Define the type of identifier that you want to use to connect to the database:</p> <ul style="list-style-type: none"> <li>▪ <b>SID (default):</b> Connect to the database instance using the SID as the connection string.</li> <li>▪ <b>SERVICE NAME:</b> Connect to the database instance using the <a href="#">SERVICE_NAME</a> as the connection string.</li> </ul>

Setting	Description
	<p><b>i</b> The type of identifier that you need to use depends on the configuration of the Oracle server.</p>

## Data

**Data**

**SQL Query File** ⓘ *Demo Serveruptime.sql*

**Input Parameter Handling** ⓘ

Do not use input parameter (default)

Use input parameter

**Transaction Handling** ⓘ

Do not use transaction (default)

Use transaction and always roll back

Use transaction and commit on success

**Data Processing** ⓘ *Only execute query (default)*

**Result Handling** ⓘ

Discard result (default)

Store result


Data

Setting	Description
SQL Query File	<p>Select the SQL query file that includes a valid SQL statement that the sensor executes on the server with every scanning interval. The list contains SQL scripts from the \Custom Sensors\sql subfolder of the <a href="#">PRTG program directory</a> on the probe system. Store your script there. If you use the script on a cluster probe, you must store the script on all cluster nodes.</p> <p>A correct expression in the file could be: <code>SELECT AVG(UnitPrice) FROM Products</code>. If you want to use transactions, separate the individual steps with semicolons ";".</p> <p><b>i</b> Note that with each request, PRTG transfers the full result set, so use filters and limits in your query.</p> <p><b>i</b> The demo script Demo Serveruptime.sql is available by default. You can use it to monitor the uptime of the target server.</p> <p><b>■</b> See also the Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a></p> <p><b>i</b> You cannot change this value after sensor creation.</p>

Setting	Description
Input Parameter Handling	<p>Define if you want to pass a parameter to the SQL query file:</p> <ul style="list-style-type: none"> <li>▪ Do not use input parameter (default): Execute the SQL query file without using variables.</li> <li>▪ Use input parameter: Execute an SQL query file that contains a variable. Provide the parameter that you want to use in the query below.</li> </ul>
Input Parameter	<p><b>This setting is only visible if you select Use input parameter above.</b></p> <p>Enter the parameter that you want to pass to the SQL query file. This parameter replaces the variables <code>@prtg</code>, <code>:prtg</code>, or <code>?</code> in the SQL query, considering the general rules for SQL variables.</p> <p>You can also use PRTG placeholders for custom sensors (command-line parameters) as input parameters, for example, <code>%sensorid</code> or <code>%deviceid</code>. For more information, see section <a href="#">Custom Sensors</a>.</p> <p><b>i</b> Provide strings as they are and do not surround them with quotation marks. PRTG automatically and correctly inserts string parameters into the query.</p>
Transaction Handling	<p>Define if you want to use transactions and if they affect the database content:</p> <ul style="list-style-type: none"> <li>▪ Do not use transaction (default): Do not execute transactions.</li> <li>▪ Use transaction and always roll back: The query does not change data in the database. In the SQL query file, separate the single steps of the transaction with semicolons.</li> <li>▪ Use transaction and commit on success: The query changes data in the database. The changes only apply if all execution steps succeed without any errors. In the SQL query file, separate the single steps of the transaction with semicolons.</li> </ul>
Data Processing	<p>Define whether the sensor processes data from the database:</p> <ul style="list-style-type: none"> <li>▪ Only execute query (default): Only show information about the number of affected rows and the execution time of the query. Affected rows are rows that were changed by the query (for example, created, deleted, or edited).</li> <li>▪ Count table rows: Execute a <code>SELECT</code> statement and monitor how many rows of the data table this statement returns.</li> <li>▪ Process data table: Read and analyze the data table. If you select this option, the sensor counts rows with <code>SELECT</code> statements as well.</li> </ul> <p><b>i</b> You cannot change this value after sensor creation.</p>

Setting	Description
DBNull Handling	<p><b>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</b></p> <p>Define the sensor behavior if the query returns <b>DBNull</b>:</p> <ul style="list-style-type: none"> <li>▪ Error: Show the Down status if the query returns <b>DBNull</b>.</li> <li>▪ Number 0: Recognize the result <b>DBNull</b> as a valid value and interpret it as the number <b>0</b>.</li> </ul>
Select Channel Value by	<p><b>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</b></p> <p>Define how to select the desired cell in the database table:</p> <ul style="list-style-type: none"> <li>▪ Column number: Determine the channel value by using the value in row 0 of the column whose number you specify in Channel #x Column Number.</li> <li>▪ Column name: Determine the channel value by using the value in row 0 of the column whose name you specify in Channel #x Column Name.</li> <li>▪ Row number: Determine the channel value by using the value in column 0 of the row whose number you specify in Channel #x Row Number.</li> <li>▪ Key value pair: Determine the channel value by searching in column 0 for the key you specify in Channel #x Key and by returning the value in column 1 of the same row where the key value was found.</li> </ul> <p><b>i</b> Defining how the desired cell in the database table is selected is necessary to configure the cells that are used in the channels.</p> <p><b>i</b> The option you select here also defines the method of how to optionally determine a value for the sensor message. For more information, see setting Use Data Table Value in Message.</p> <p><b>■</b> For an example for channel value selection, see section <a href="#">Monitoring Databases</a>.</p>
Channel #2 - #10	<p><b>This setting is only visible if you select Process data table above.</b></p> <p>You can define up to 10 channels. You must define at least one channel, so you see all available settings for <b>Channel #1</b>. Specify how to handle all other possible channels:</p> <ul style="list-style-type: none"> <li>▪ Disable: Do not create this channel.</li> <li>▪ Enable: Create this channel.</li> </ul> <p><b>i</b> It is not possible to enable or disable channels after sensor creation.</p>

Setting	Description
Channel #x Name	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</p> <p>Enter a name for the channel. Enter a string. The sensor dynamically generates channels with this name as identifier.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Channel #x Column Number	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation and if you select Column number for the setting Select Channel Value by.</p> <p>Provide the number of the column to use to determine the channel value in row 0. Enter an integer.</p>
Channel #x Column Name	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation and if you select Column name for the setting Select Channel Value by.</p> <p>Provide the name of the column to use to determine the channel value in row 0. Enter an integer.</p>
Channel #x Row Number	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation and if you select Row number for the setting Select Channel Value by.</p> <p>Provide the number of the column to use to determine the channel value in row 0. Enter an integer.</p>
Channel #x Key	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation and if you select Key value pair for the setting Select Channel Value by.</p> <p>Provide the key to search for in column 0 of the data table. The value in column 1 of the same row where the key value was found to use to determine the channel value. Enter a string.</p>
Channel #x Mode	<p>This setting is only visible if you select Process data table above.</p> <p>Define how to display the determined value in the channel:</p> <ul style="list-style-type: none"> <li>▪ Absolute (default): Show the value as the sensor retrieves it from the data table.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Difference: The sensor calculates and shows the difference between the last and the current value returned from the data table.               <ul style="list-style-type: none"> <li>ⓘ This mode is not compatible with the unit Lookup.</li> <li>ⓘ This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative and decreasing values.</li> </ul> </li> <li>▪ Absolute (recommended): Show the value as the sensor retrieves it from the data table.</li> <li>▪ Difference: The sensor calculates and shows the difference between the last and the current value returned from the data table.               <ul style="list-style-type: none"> <li>ⓘ This mode is not compatible with the unit Lookup.</li> <li>ⓘ This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative and decreasing values.</li> </ul> </li> <li>ⓘ You cannot change this value after sensor creation.</li> </ul>
<p>Channel #x Unit</p>	<p><a href="#">This setting is only visible if you select Process data table above.</a></p> <p>Define the unit of the channel value:</p> <ul style="list-style-type: none"> <li>▪ BytesBandwidth</li> <li>▪ BytesMemory</li> <li>▪ BytesDisk</li> <li>▪ Temperature</li> <li>▪ Percent</li> <li>▪ TimeResponse</li> <li>▪ TimeSeconds</li> <li>▪ TimeHours</li> <li>▪ Count</li> <li>▪ CPU</li> <li>▪ BytesFile</li> <li>▪ SpeedDisk</li> <li>▪ SpeedNet</li> <li>▪ Custom</li> <li>▪ Lookup</li> </ul> <p> For more information about the available units, see section <a href="#">Custom Sensors</a>.</p>



Setting	Description
	<p><b>i</b> To use <a href="#">lookups</a> with this channel, select Lookup and define the lookup file in Channel #x Lookup. Do not use Custom if you use lookups with this sensor.</p> <p><b>i</b> It is not possible to use the unit Lookup in combination with the Difference mode. You are not able to create the sensor in this case.</p>
Channel #x Custom Unit	<p>This setting is only visible if you select Custom above.</p> <p>Define a unit for the channel value. Enter a string.</p>
Channel #x Lookup	<p>This setting is only visible if you select Lookup above.</p> <p>Select a <a href="#">lookup</a> file that you want to use with this channel.</p>
Use Data Table Value in Message	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</p> <p>Define if the sensor message shows a value from the data table:</p> <ul style="list-style-type: none"> <li>▪ Disable: Do not use a custom sensor message.</li> <li>▪ Enable: Define a custom sensor message with a defined value of the data table. Define the value selection below.</li> </ul> <p><b>i</b> The method of how to determine a value for the sensor message is defined in the setting Select Channel Value by above.</p>
Message Column Number	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation, if you select Column name for the setting Select Channel Value by, and if you select Enable above.</p> <p>Enter the number of a column. The sensor message shows the value in row 0 of this column. Enter an integer.</p>
Message Column Name	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation, if you select Column name for the setting Select Channel Value by, and if you select Enable above.</p> <p>Enter the name of a column. The sensor message shows the value in row 0 of this column. Enter a string.</p> <p><b>i</b> Columns start with index 0.</p>
Message Row Number	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation, if you select Row number for the setting Select Channel Value by, and if you select Enable above.</p>

Setting	Description
	<p>Enter the name of a column. The sensor message shows the value in row 0 of this column. Enter the number of a row. The sensor message shows the value in column 0 of this row. Enter an integer.</p> <p><b>i</b> Rows start with index 0.</p>
<p>Message Key</p>	<p><b>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation, if you select Key value pair for the setting Select Channel Value by, and if you select Enable above.</b></p> <p>Enter a key to search for in column 0 of the data table. The sensor message shows the value in column 1 of the row where the key was found. Enter a string.</p>
<p>Message</p>	<p><b>This setting is only visible if you select Enable above.</b></p> <p>Define the sensor message. Enter a string. Use the placeholder <code>{0}</code> at the position where you want to display the value.</p> <p>Example: <code>The message is {0}</code></p> <p><b>i</b> PRTG does not support the number sign (#) in sensor messages. If a message contains a number sign, PRTG clips the message at this point.</p>
<p>If Message Changes</p>	<p><b>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</b></p> <p>Define what the sensor does when its message changes:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> <li>▪ Trigger 'change' notification: Send an internal message that indicates a change.</li> </ul> <p><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</p>
<p>Result Handling</p>	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the <code>\Logs\sensors</code> subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are <code>Result of Sensor [ID].txt</code>, <code>Result of Sensor [ID].Data.txt</code>, and <code>Result of Sensor [ID].log</code>. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Affected Rows	The number of rows that were addressed by the query (including <b>SELECT</b> statements if you process data tables)
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Execution Time	The execution time of the entire request (including connection buildup, query execution, transaction handling, disconnection)  <span>ⓘ</span> This channel is the primary channel by default.
Query Execution Time	The execution time of the specified query

## SQL Variables

You can use the following variables in the SQL query file to be replaced by an input parameter. This is useful if you have various SQL sensors with queries that differ in only one parameter.

- Microsoft SQL, MySQL, PostgreSQL: [@prtg](#)
- Oracle SQL: [:prtg](#)
- ADO SQL: [?](#) (question mark)

ⓘ [@prtg](#), [:prtg](#), and [?](#) are common SQL query parameters and they are used in a parameterized SQL query. This means that the query and the parameter are forwarded without any changes to the database. This leads to some restrictions on the database side. For example, you cannot use variables as placeholders for table names or as lists in IN operators.

Examples for variables usage:

```
SELECT * FROM Table WHERE name = @prtg
SELECT @prtg FROM Table
```

## More

### ■ KNOWLEDGE BASE

How to set up the SQL v2 sensors in PRTG? Is there a guide?

- <https://kb.paessler.com/en/topic/70618>

How can I monitor strings from an SQL database and show a sensor status depending on it?

- <https://kb.paessler.com/en/topic/63259>

How can I monitor error tables in SQL databases?

- <https://kb.paessler.com/en/topic/70774>

Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

Which .NET version does PRTG require?

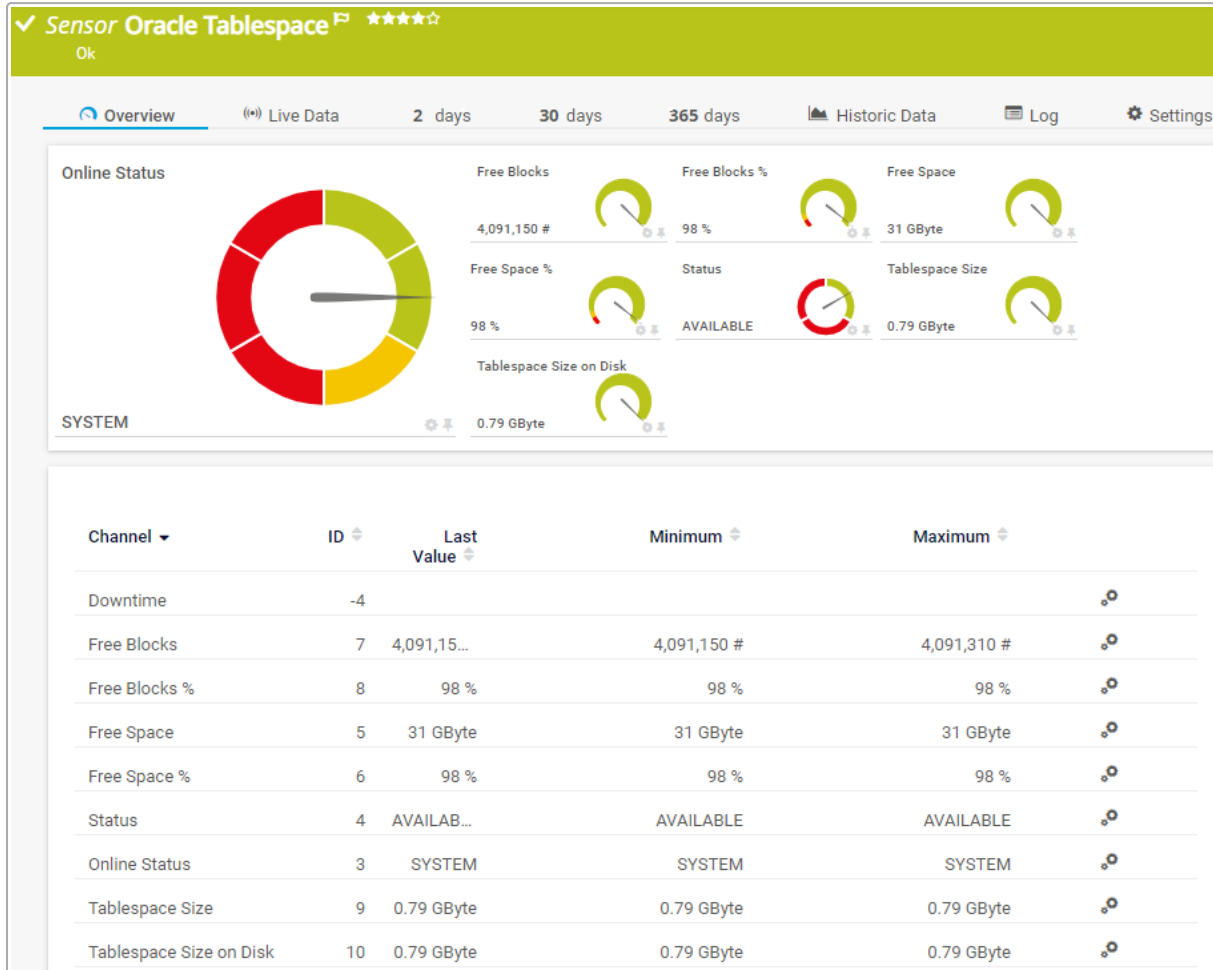
- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.130 Oracle Tablespace Sensor

The Oracle Tablespace sensor monitors a tablespace on an Oracle server.



Oracle Tablespace Sensor





For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1564</sup>.

### Sensor in Other Languages

- Dutch: Oracle Tablespace
- French: Tablespace Oracle
- German: Oracle Tablespace
- Japanese: Oracle テーブルスペース
- Portuguese: Oracle Tablespace
- Russian: Tablespace Oracle
- Simplified Chinese: Oracle 表空间
- Spanish: Oracle Tablespace

## Remarks

Consider the following [remarks](#) <sup>(1561)</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Sufficient account privileges	This sensor requires sufficient privileges for the account that you use for the connection.   Use an account for the connection that has the privileges to see all (or specific) views. We recommend that you use the <a href="#">SYSTEM</a> account if possible, otherwise grant your database administrator the <a href="#">SELECT_CATALOG_ROLE</a> to the account that you use. Without sufficient privileges, you might see the error message <a href="#">ORA-00942: table or view does not exist</a> .
.NET 4.7.2 or later	This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.   If the framework is missing, you cannot create this sensor.   For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a>
Overprovisioning	This sensor does not support overprovisioning.
Oracle version	This sensor supports Oracle database servers as of version 10.2
IPv6	This sensor supports IPv6.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Credentials	Define the credentials for database management systems in settings that are higher in the object hierarchy.
Knowledge Base	Knowledge Base: <a href="#">Why is my Oracle Tablespace sensor showing negative values?</a>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★★★★☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- sqlsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Oracle Specific

### Oracle Specific

**Identifier** ⓘ

**Identification Parameter** ⓘ  SID (default)  
 SERVICE\_NAME

**Sensor Name Prefix** ⓘ  Do not use a prefix for the sensor name (default)  
 Use SERVICE\_NAME as prefix for the sensor name

Oracle Specific

Setting	Description
Identifier	<p>Enter the <a href="#">Oracle System ID (SID)</a> or the <a href="#">SERVICE_NAME</a> of the database that the sensor connects to. Specify the Identification Parameter below. By default, the sensor uses the SID as the connection string.</p> <p><span style="font-size: 1.2em;">ⓘ</span> You can find the SID or SERVICE_NAME in the <a href="#">CONNECT_DATA</a> part of the <a href="#">TNSNames.ora</a> file on the Oracle server. For example, a SID can look like this: <code>orcl</code></p>
Identification Parameter	<p>Define the type of identifier that you want to use to connect to the database:</p> <ul style="list-style-type: none"> <li>▪ <b>SID (default):</b> Connect to the database instance using the SID as the connection string.</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ <b>SERVICE NAME:</b> Connect to the database instance using the <b>SERVICE_NAME</b> as the connection string.</li> </ul> <p><b>i</b> The type of identifier that you need to use depends on the configuration of the Oracle server.</p>
Sensor Name Prefix	<p>Define if you want to use the <b>SERVICE_NAME</b> as the prefix for the sensor name:</p> <ul style="list-style-type: none"> <li>▪ Do not use a prefix for the sensor name (default): Only show the name of the tablespace that this sensor monitors.</li> <li>▪ Use <b>SERVICE_NAME</b> as prefix for the sensor name: Add the <b>SERVICE_NAME</b> to the beginning of the sensor name.</li> </ul> <p><b>i</b> If you have multiple databases on your Oracle server, use the <b>SERVICE_NAME</b> as the prefix to distinguish the tablespaces that you monitor.</p>

### Tablespace Specific

Tablespace Specific
Tablespaces **i** SYSAUX

Tablespace Specific

Setting	Description
Tablespaces	The tablespace that this sensor monitors.


### Sensor Display

Sensor Display


Primary Channel **i** Downtime


Graph Type **i**
 Show channels independently (default)
   
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Free Blocks	The number of free blocks
Free Blocks %	<p>The number of free blocks (%)</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: 5%</li> <li>▪ Lower warning limit: 10%</li> </ul>
Free Space	The free space
Free Space %	<p>The free space (%)</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: 5%</li> <li>▪ Lower warning limit: 10%</li> </ul>
Online Status	<p>The online status</p> <ul style="list-style-type: none"> <li>▪ Up status: Online, System</li> <li>▪ Warning status: Recover</li> <li>▪ Down status: Offline, Sysoff, Unknown</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Status	<p>The status</p> <ul style="list-style-type: none"> <li>▪ Up status: Available</li> <li>▪ Down status: Invalid, Unknown</li> </ul>
Tablespace Size	The size of the tablespace
Tablespace Size on Disk	The size of the tablespace on disk

## More

### ■ KNOWLEDGE BASE

Why is my Oracle Tablespace sensor showing negative values?

- <https://kb.paessler.com/en/topic/79066>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

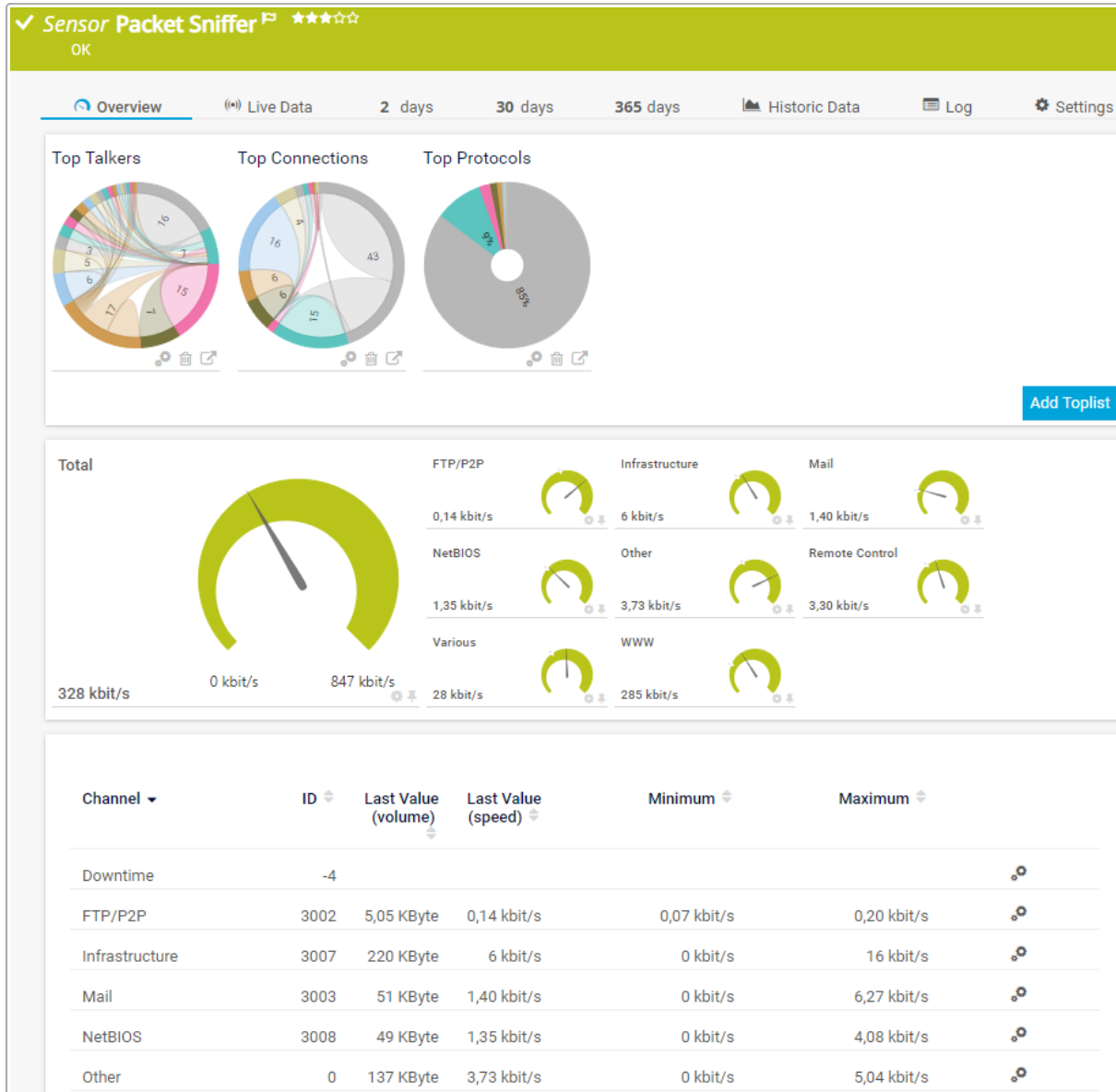
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.131 Packet Sniffer Sensor

The Packet Sniffer sensor monitors the headers of data packets that pass a local network card using a built-in packet sniffer. You can choose from predefined channels.

**i** This sensor analyzes only header traffic.



Packet Sniffer Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1573]</sup>.


### Sensor in Other Languages

- Dutch: Packet Sniffer
- French: Reniflage de paquets
- German: Packet Sniffer

- Japanese: パケットスニファー
- Portuguese: Sniffer de pacotes
- Russian: Анализатор пакетов
- Simplified Chinese: 数据包嗅探程序
- Spanish: Analizador de paquetes

## Remarks

Consider the following [remarks](#)  and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
Probe device	By default, this sensor works only on a probe device.
IPv6	This sensor supports IPv6.
Network Mapper	Using Network Mapper (Nmap) on the parent probe system might cause high CPU load. If you have this issue, restarting the PRTG probe service might help.
Knowledge Base	Knowledge Base: <a href="#">How can I change the default groups and channels for flow and Packet Sniffer sensors?</a>
Traffic	By default, you can only monitor traffic passing the probe system where the probe device with the sensor is set up. To monitor other traffic in your network, you can configure a monitoring port (if available) that the switch sends a copy of all traffic to. You can then physically connect this port to a network card of the probe system (either local probe or remote probe system). This way, PRTG can analyze the complete traffic that passes through the switch. This feature of your hardware might be called Switched Port Analyzer (SPAN), port mirroring, or port monitoring.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Known Issues

- The sensor does not support the Simulate Error Status option in the Context Menu. If you trigger this action, the sensor does not show a simulated Down status.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ

exampletag
✕
+

**Priority** ⓘ

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- bandwidthsensor
- sniffersensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sniffer Specific

■ For more information on filters, see section [Filter Rules](#) <sup>1573</sup>.

### Sniffer Specific

**Filters** To include and exclude specific traffic, you can define filter rules based on the following format guidelines:

- field[filter]

Fields are:

IP, Port, SourceIP, SourcePort, DestinationIP, DestinationPort, Protocol (values TCP, UDP, ICMP, OSPFIGP, or any number), ToS, DSCP

Additional Sniffer Fields:

MAC, SourceMAC, DestinationMAC, EtherType (values IPV4, ARP, RARP, APPLE, AARP, IPV6, IPXold, IPX, or any number)

**Include Filter** ⓘ

---

**Exclude Filter** ⓘ

**Network Adapters** ⓘ Search...

- Network Adapter**
- NdisWan Adapter ()
- Intel(R) Ethernet Connection I2...
- Adapter for loopback traffic ca...





**Stream Data Handling** ⓘ

Discard stream data (default)

Store stream data only for the 'Other' channel

Store all stream data

Sniffer Specific

Setting	Description
Include Filter	Define if you want to filter any traffic. If you leave this field empty, the sensor includes all traffic. To include specific traffic only, define filters using a special <a href="#">syntax</a> .
Exclude Filter	First, the sensor considers the filters in Include Filter. From this subset, you can explicitly exclude traffic, using the same syntax.
Network Adapters	<p>Select the network adapters that this sensor monitors. You see a list of all adapters that are available on the probe system. To select an adapter, enable the check box in front of the respective name.</p> <ul style="list-style-type: none"> <li> You can also select all items or cancel the selection by using the check box in the table header.</li> <li> You cannot change this setting if the probe is not connected.</li> </ul>
Stream Data Handling	<p>Define what PRTG does with the stream and packet data:</p> <ul style="list-style-type: none"> <li>▪ Discard stream data (default): Do not store the stream and packet data.</li> <li>▪ Store stream data only for the 'Other' channel: Only store stream and packet data that is not otherwise filtered and is therefore accounted to the default Other channel. PRTG stores this data in the \StreamLog subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Streams Sensor [ID] (1).csv. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> <li>▪ Store all stream data: Store all stream and packet data. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <ul style="list-style-type: none"> <li> Use with caution. It can create huge data files. We recommend that you only use this setting for a short time.</li> <li> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</li> </ul>



## Channel Configuration

**Channel Configuration**

Channel Selection ⓘ

Group	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Content
Web	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	WWW Traffic: HTTP, HTTPS
File Transfer	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	File Transfer: FTP (Control)
Mail	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Mail Traffic: IMAP, POP3, SMTP
Chat	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Chat, Instant Messaging: IRC, AIM
Remote Control	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Remote Control: RDP, SSH, Telnet, VNC
Infrastructure	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Network Services: DHCP, DNS, Ident, ICMP, SNMP
NetBIOS	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	NetBIOS: NETBIOS
Citrix	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Citrix: Citrix
Other Protocols	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Various: Other UDP, Other TCP

**Note** You can change the default configuration for groups and channels. This way, you do not have to customize this setting each time that you add this sensor type. For details, see the Knowledge Base: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)

Channel Configuration

Setting	Description
Channel Selection	<p>Define the categories that the sensor accounts the traffic to:</p> <ul style="list-style-type: none"> <li>▪ Web: Internet web traffic.</li> <li>▪ File Transfer: Traffic from FTP.</li> <li>▪ Mail: Internet mail traffic.</li> <li>▪ Chat: Traffic from chat and instant messaging.</li> <li>▪ Remote Control: Traffic from remote control applications such as RDP, SSH, Telnet, and Virtual Network Computing (VNC).</li> <li>▪ Infrastructure: Traffic from network services such as DHCP, DNS, Ident, ICMP, and SNMP.</li> <li>▪ NetBIOS: Traffic from NetBIOS communication.</li> <li>▪ Citrix: Traffic from Citrix applications.</li> <li>▪ Other Protocols: Traffic from various other protocols via UDP and TCP.</li> </ul> <p>For each group, you can select how many channels the sensor uses, that is, how detailed the sensor divides the traffic:</p> <ul style="list-style-type: none"> <li>▪ No (✘): Do not account traffic of this group in its own channel. The sensor accounts all traffic of this group to the default channel named Other.</li> <li>▪ Yes (✔): Count all traffic of this group and summarize it in one channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Detail (🔍): Count all traffic of this group and further divide it into different channels. The traffic appears in several channels that you can see in the Content column. <ul style="list-style-type: none"> <li>ⓘ Extensive use of this option can cause load problems on the probe system. We recommend that you set specific, well-chosen filters for the data that you really want to analyze.</li> </ul> </li> </ul> <p>■ You can change the default configuration for groups and channels. For more information, see the Knowledge Base: <a href="#">How can I change the default groups and channels for flow and Packet Sniffer sensors?</a></p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Primary Toplist

Primary Toplist

Primary Toplist ⓘ
Top Connections

Primary Toplist

Setting	Description
Primary Toplist	<p>Define which Toplist is the primary Toplist of the sensor:</p> <ul style="list-style-type: none"> <li>▪ Top Talkers</li> <li>▪ Top Connections</li> <li>▪ Top Protocols</li> <li>▪ <a href="#">[Any custom Toplists you add]</a></li> </ul> <p>ⓘ PRTG shows the primary Toplist in maps when you add a Toplist object.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Toplists

For all Flow (NetFlow, jFlow, sFlow, IPFIX) and Packet Sniffer sensors, Toplists are available on the sensor's Overview tab. Using Toplists, you can review traffic data for small time periods in great detail.

■ For more information, see section [Toplists](#).

## Filter Rules

■ For more information, see section [Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Chat	The traffic from chat and instant messaging (IRC, AIM)
Citrix	The traffic from Citrix applications
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
FTP/P2P	The traffic from file transfer (FTP/P2P)
Infrastructure	The traffic from network services (DHCP, DNS, Ident, ICMP, SNMP)
Mail	The internet mail traffic (IMAP, POP3, SMTP)
NetBIOS	The traffic from NetBIOS communication
Other	The traffic from various other protocols (UDP, TCP)
Remote Control	The traffic from remote control applications (RDP, SSH, Telnet, Virtual Network Computing (VNC))
Total	The total traffic <span>ⓘ</span> This channel is the primary channel by default.
Various	The traffic from various other sources
WWW	The traffic from the web (HTTP, HTTPS)

## More

### ■ KNOWLEDGE BASE

How can I change the default groups and channels for flow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

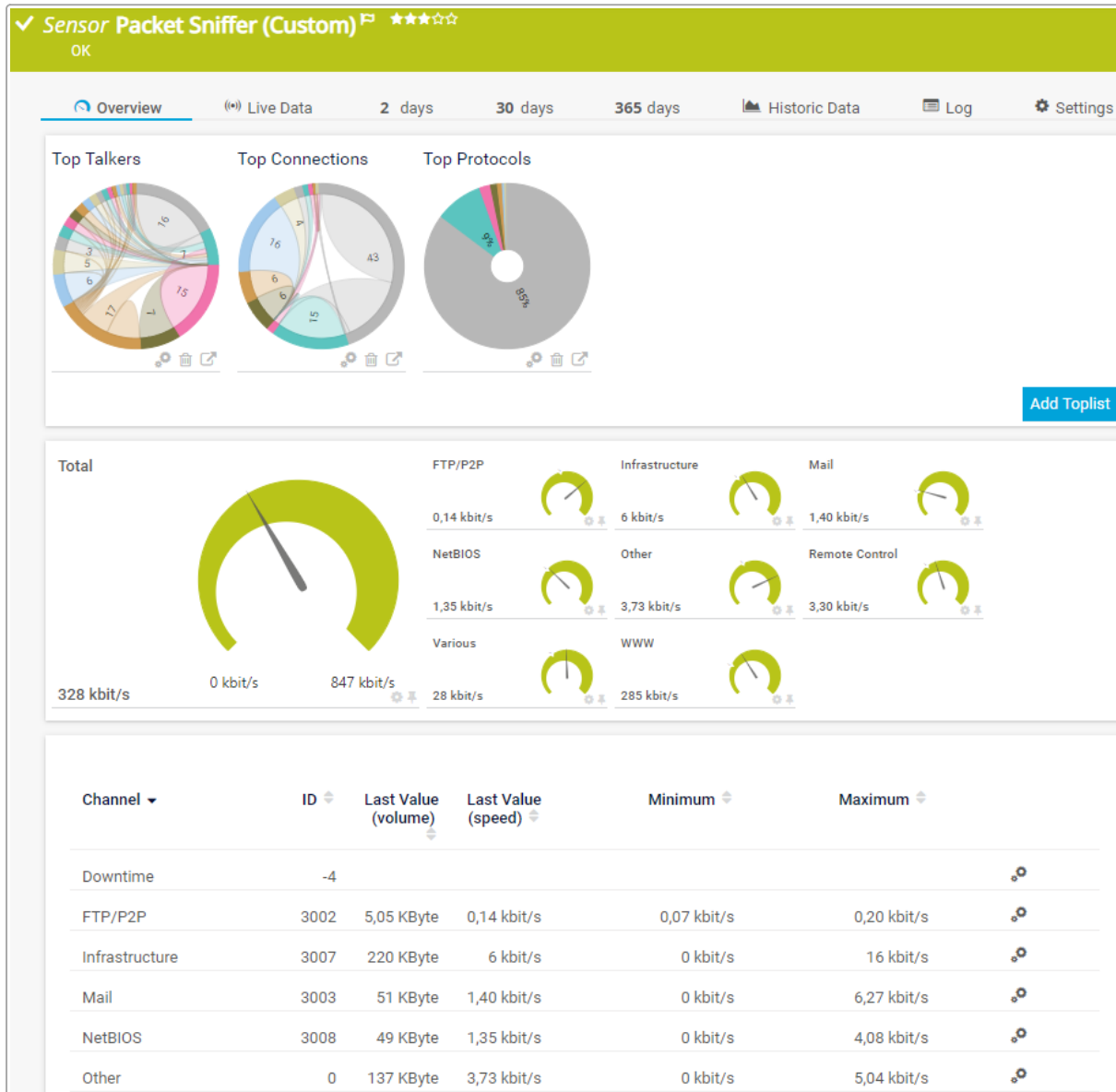
Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

## 7.8.132 Packet Sniffer (Custom) Sensor

The Packet Sniffer (Custom) sensor monitors the headers of data packets that pass a local network card using a built-in packet sniffer. With this sensor, you can define your own channel definitions to divide traffic into different channels.

- ❗ This sensor analyzes only header traffic.
- ❗ This sensor does not have any predefined channels.



Packet Sniffer (Custom) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).


### Sensor in Other Languages

- Dutch: Packet Sniffer (Aangepast)

- French: Reniflage de paquets personnalisé
- German: Packet Sniffer (Benutzerdef.)
- Japanese: パケットスニフアー(カスタム)
- Portuguese: Sniffer de pacotes (customizado)
- Russian: Анализатор пакетов (нестандартный)
- Simplified Chinese: 数据包嗅探程序 (自定义)
- Spanish: Analizador de paquetes (personalizado)

## Remarks

Consider the following [remarks](#)<sup>1576</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
Probe device	By default, this sensor works only on a probe device.
Channels	This sensor does not officially support more than <b>50 channels</b> .
IPv6	This sensor supports IPv6.
Traffic	By default, you can only monitor traffic passing the probe system where the probe device with the sensor is set up. To monitor other traffic in your network, you can configure a monitoring port (if available) that the switch sends a copy of all traffic to. You can then physically connect this port to a network card of the probe system (either local probe or remote probe system). This way, PRTG can analyze the complete traffic that passes through the switch. This feature of your hardware might be called Switched Port Analyzer (SPAN), port mirroring, or port monitoring.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Known Issues

- The sensor does not support the Simulate Error Status option in the Context Menu. If you trigger this action, the sensor does not show a simulated Down status.

## Basic Sensor Settings

### Basic Sensor Settings

Sensor Name ⓘ Example Name

Tags ⓘ  X +

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- bandwidthsensor
- sniffersensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Sniffer Specific

■ For more information on filters, see section [Filter Rules](#)<sup>1581</sup>.

**Sniffer Specific**

**Filters** To include and exclude specific traffic, you can define filter rules based on the following format guidelines:

- field[filter]

Fields are:  
IP, Port, SourceIP, SourcePort, DestinationIP, DestinationPort, Protocol (values TCP, UDP, ICMP, OSPFIGP, or any number), ToS, DSCP

Additional Sniffer Fields:  
MAC, SourceMAC, DestinationMAC, EtherType (values IPV4, ARP, RARP, APPLE, AARP, IPV6, IPXold, IPX, or any number)

Include Filter

Exclude Filter

Channel Definition

Network Adapters Search...

- Network Adapter
- NdisWan Adapter ()
- Intel(R) Ethernet Connection I2...
- Adapter for loopback traffic ca...





Stream Data Handling

- Discard stream data (default)
- Store stream data only for the 'Other' channel
- Store all stream data

Sniffer Specific


Setting	Description
Include Filter	Define if you want to filter any traffic. If you leave this field empty, the sensor includes all traffic. To include specific traffic only, define filters using a special <a href="#">syntax</a> .
Exclude Filter	First, the sensor considers the filters in Include Filter. From this subset, you can explicitly exclude traffic, using the same syntax.
Channel Definition	<p>Enter a channel definition to divide the traffic into different channels. Enter each definition in one line. The sensor accounts all traffic that you do not define a channel for to the default channel Other.</p> <p> For more information, see section <a href="#">Channel Definitions for Flow, IPFIX and Packet Sniffer Sensors</a>.</p> <p> Extensive use of many filters can cause load problems on the probe system. We recommend that you define specific, well-chosen filters for the data that you really want to analyze. We recommend that you do not use more than 20 channels in graphs and tables, and not more than 100 channels in total. For performance reasons, we recommend that you add several sensors with fewer channels each.</p>




Setting	Description
Network Adapters	<p>Select the network adapters that this sensor monitors. You see a list of all adapters that are available on the probe system. To select an adapter, enable the check box in front of the respective name.</p> <ul style="list-style-type: none"> <li> You can also select all items or cancel the selection by using the check box in the table header.</li> <li> You cannot change this setting if the probe is not connected.</li> </ul>
Stream Data Handling	<p>Define what PRTG does with the stream and packet data:</p> <ul style="list-style-type: none"> <li>▪ Discard stream data (default): Do not store the stream and packet data.</li> <li>▪ Store stream data only for the 'Other' channel: Only store stream and packet data that is not otherwise filtered and is therefore accounted to the default Other channel. PRTG stores this data in the \StreamLog subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Streams Sensor [ID] (1).csv. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> <li>▪ Store all stream data: Store all stream and packet data. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <ul style="list-style-type: none"> <li> Use with caution. It can create huge data files. We recommend that you only use this setting for a short time.</li> <li> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</li> </ul>

## Sensor Display



**Sensor Display**


Primary Channel  Downtime

---

Graph Type 
 Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <ul style="list-style-type: none"> <li> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</li> </ul>


Setting	Description
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

### Primary Toplist


Primary Toplist

Primary Toplist 
Top Connections

Primary Toplist

Setting	Description
Primary Toplist	<p>Define which Toplist is the primary Toplist of the sensor:</p> <ul style="list-style-type: none"> <li>Top Talkers</li> <li>Top Connections</li> <li>Top Protocols</li> <li><a href="#">[Any custom Toplists you add]</a></li> </ul> <p> PRTG shows the primary Toplist in maps when you add a Toplist object.</p>

### Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Toplists

For all Flow (NetFlow, jFlow, sFlow, IPFIX) and Packet Sniffer sensors, Toplists are available on the sensor's Overview tab. Using Toplists, you can review traffic data for small time periods in great detail.

■ For more information, see section [Toplists](#).

## Filter Rules

The following filter rules apply to all Flow (NetFlow, jFlow, sFlow, IPFIX) and Packet Sniffer sensors.

■ For more information, see section [Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors](#).

Field	Possible Filter Values
IP	IP address or DNS name
Port	Any number
SourceIP	IP address or DNS name
SourcePort	Any number
DestinationIP	IP address or DNS name
DestinationPort	Any number
Protocol	<a href="#">Transmission Control Protocol (TCP)</a> , <a href="#">User Datagram Protocol (UDP)</a> , <a href="#">Internet Control Message Protocol (ICMP)</a> , <a href="#">Open Shortest Path First (OSPF)</a> , any number
ToS	<a href="#">Type of Service (ToS)</a> : any number
DSCP	<a href="#">Differentiated Services Code Point (DSCP)</a> : any number

The following filter rules apply to Packet Sniffer sensors only.

Field	Possible Filter Values
MAC	Physical address
SourceMAC	Physical address

Field	Possible Filter Values
DestinationMAC	Physical address
EtherType	IPV4, ARP, RARP, APPLE, AARP, IPV6, IPXold, IPX, any number
VlanPCP	IEEE 802.1Q VLAN Priority Code Point
VlanID	IEEE 802.1Q VLAN Identifier
TrafficClass	IPv6 Traffic Class: corresponds to TOS used with IPv4
FlowLabel	IPv6 Flow Label

## Channel List

- i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
[Custom]	The traffic by type according to the channel definition
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Other	All traffic for which no channel is defined
Total	The total traffic <b>i</b> This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

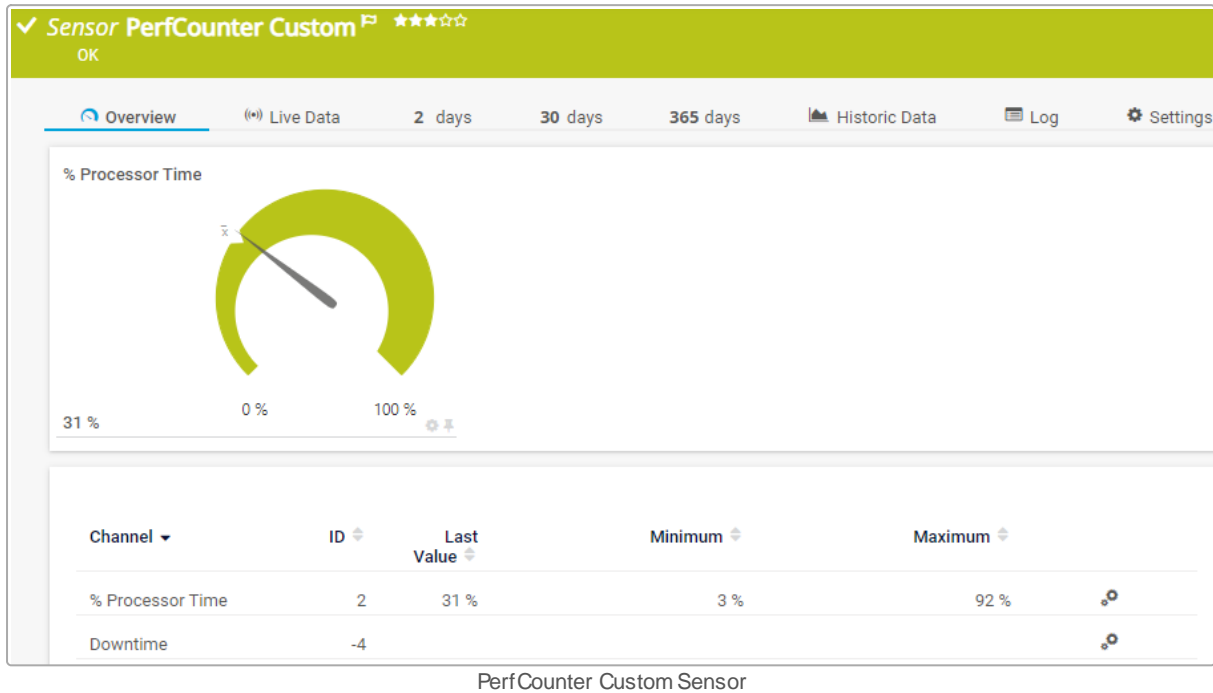
Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

## 7.8.133 PerfCounter Custom Sensor

The PerfCounter Custom sensor monitors a configured set of Windows performance counters. You can define your own channels.

**i** This sensor does not have any predefined channels.




For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1587</sup>.

### Sensor in Other Languages

- Dutch: Prestatie Meters Klantspecifiek
- French: Windows PerfCounter personnalisé
- German: Leistungsindikator (benutzerdef.)
- Japanese: パフォーマンスカウンターカスタム
- Portuguese: PerfCounter (customizado)
- Russian: Специальные настройки PerfCounter
- Simplified Chinese: 性能计数器自定义
- Spanish: PerfCounter (personalizado)

### Remarks

Consider the following [remarks](#)<sup>1583</sup> and requirements for this sensor:

Remark	Description
Windows version	This sensor requires <a href="#">at least Windows Server 2008 R2</a> on the probe system (on every cluster node, if on a cluster probe).
Remote Registry Windows service	<p>This sensor requires that the <a href="#">Remote Registry</a> Windows service runs on the target system.</p> <p><b>i</b> If this service does not run, a connection via performance counters is not possible.</p> <p><b>i</b> To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.</p>
Credentials	<p>This sensor requires credentials for Windows systems.</p> <p><b>i</b> We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system.</p> <p>Otherwise, a connection via performance counters is not possible. However, WMI connections might still work.</p> <p><b>i</b> The user account must be a member of the <a href="#">Performance Monitor Users</a> user group on the target system.</p>
Same name	You cannot add different performance counters with the same name to one sensor.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Angle brackets	If a performance counter contains angle brackets (< or >), do not edit the channel settings because this might cause an error.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">How can I find out the names of available performance counters?</a></li> <li>▪ Knowledge Base: <a href="#">My performance counter sensor does not work. What can I do?</a></li> </ul>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

Basic Sensor Settings

Sensor Name ⓘ

Tags ⓘ

exampletag ✕ +

Priority ⓘ

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- performancecounter
- performancecountercustom

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Performance Counter Settings

Performance Counter Settings

Performance Counters ⓘ

Value Display Mode ⓘ

Performance Counter Settings

Setting	Description
Performance Counters	<p>Enter the performance counters that you want to query. Enter each counter in one line. PRTG creates one channel for each performance counter that you select. Use the following syntax: the name of the counter, followed by two colons (:), and the unit.</p> <p>Example: <code>\Processor(_Total)\% Processor Time::%</code></p> <p> ⓘ You cannot monitor different performance counters with the same name in one sensor. The sensor uses the performance counter as the channel name, so this would create duplicate channels, which PRTG does not support. If you want to monitor different performance counters with the same name, add one sensor for each counter. You can also create a <a href="#">custom sensor</a>. For example, you can write a PowerShell query that connects to the target device, retrieves the desired counters with the <a href="#">Get-Counter</a> cmdlet, and reports them to PRTG as individual channels.</p>

Setting	Description
	<p><b>i</b> If a custom performance counter includes angle brackets (&lt; or &gt;), do not edit the <a href="#">channel settings</a> (for example, limits) after sensor creation. This might lead to a malfunctioning sensor.</p> <p><b>i</b> You cannot change this value after sensor creation.</p>
Value Display Mode	<p>Determine if the sensor displays the returned value as an absolute value or if it displays the difference between the last and the current value:</p> <ul style="list-style-type: none"> <li>Absolute (default): Display the returned value as an absolute value.</li> <li>Difference: Display the difference between last and current value. <ul style="list-style-type: none"> <li><b>i</b> Make sure that all performance counters that you monitor are capable of this mode.</li> </ul> </li> </ul> <p><b>i</b> You cannot change this value after sensor creation.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>



Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other above.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
[Custom]	<p>The Windows performance counters in different channels</p> <p>■ To find available performance counters and their names on the target system, see the Knowledge Base: <a href="#">How can I find out the names of available performance counters?</a></p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>

## More

### ■ KNOWLEDGE BASE

How can I find out the names of available performance counters?

- <https://kb.paessler.com/en/topic/50673>

My performance counter sensor does not work. What can I do?

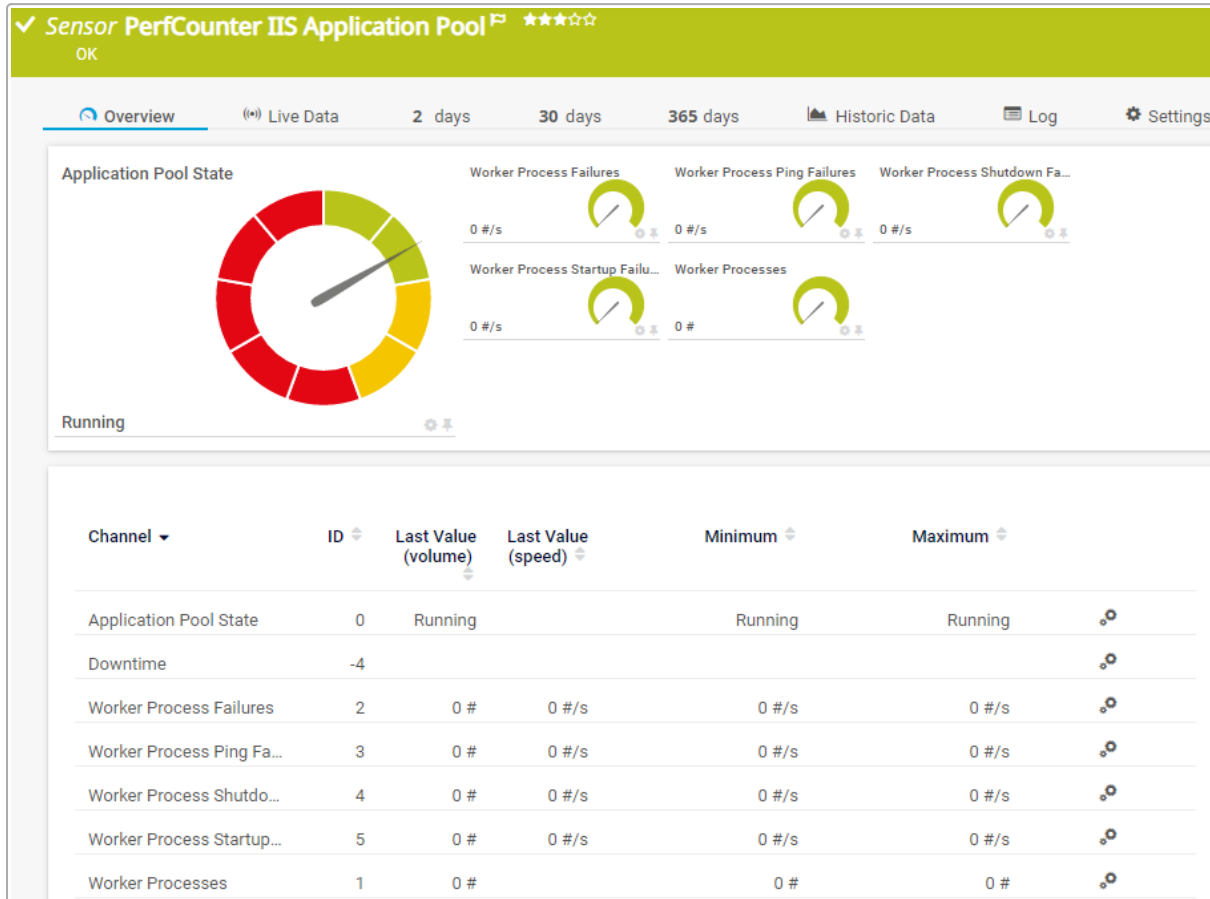
- <https://kb.paessler.com/en/topic/59804>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.134 PerfCounter IIS Application Pool Sensor

The PerfCounter IIS Application Pool sensor monitors a Microsoft Internet Information Services (IIS) application pool via Windows performance counters.



PerfCounter IIS Application Pool Sensor






For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: PerfCounter IIS Application Pool
- French: Windows IIS Pool d'applications (PerfCounter)
- German: Leistungsindikator IIS-Anwendungspool
- Japanese: パフォーマンスカウンター IIS アプリケーションプール
- Portuguese: Pool de aplicativos IIS (PerfCounter)
- Russian: Пул приложений IIS (PerfCounter)
- Simplified Chinese: 性能计数器 IIS 应用程序池
- Spanish: Grupo de aplicaciones IIS (PerfCounter)

## Remarks

Consider the following [remarks](#) <sup>11590</sup> and requirements for this sensor:

Remark	Description
Windows version	This sensor requires <a href="#">at least Windows Server 2008 R2</a> on the probe system (on every cluster node, if on a cluster probe).
IIS version 7.5	This sensor requires as of Microsoft IIS 7.5 on the target system.
Remote Registry Windows service	<p>This sensor requires that the <a href="#">Remote Registry</a> Windows service runs on the target system.</p> <ul style="list-style-type: none"> <li> If this service does not run, a connection via performance counters is not possible.</li> <li> To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.</li> </ul>
Credentials	<p>This sensor requires credentials for Windows systems.</p> <ul style="list-style-type: none"> <li> We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system.</li> </ul> <p>Otherwise, a connection via performance counters is not possible. However, WMI connections might still work.</p> <ul style="list-style-type: none"> <li> The user account must be a member of the <a href="#">Performance Monitor Users</a> user group on the target system.</li> </ul>
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

Basic Sensor Settings

Sensor Name ⓘ

Tags ⓘ

✕ +

Priority ⓘ

★  ★  ★  ☆  ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- pciisappool
- performancecounter

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## IIS Application Pool Specific

IIS Application Pool Specific

Application Pools ⓘ

IIS Application Pool Specific

Setting	Description
Application Pools	The name of the application pool that this sensor monitors.

## Sensor Display


Sensor Display

Primary Channel ⓘ


Graph Type ⓘ


Show channels independently (default)
   
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Application Pool State	<p>The overall application pool status</p> <ul style="list-style-type: none"> <li>▪ Up status: Running, Unavailable for Total</li> <li>▪ Warning status: Initialized, Shutdown Pending</li> </ul>

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Down status: Delete Pending, Stopped, Stopping, Unavailable, Uninitialized</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Worker Process Failures	The number of failures in worker processes
Worker Process Ping Failures	The number of failures in worker process pings
Worker Process Shutdown Failures	The number of failures in worker process shutdowns
Worker Process Startup Failures	The number of failures in worker process startups
Worker Processes	The number of worker processes

## More

### ■ KNOWLEDGE BASE

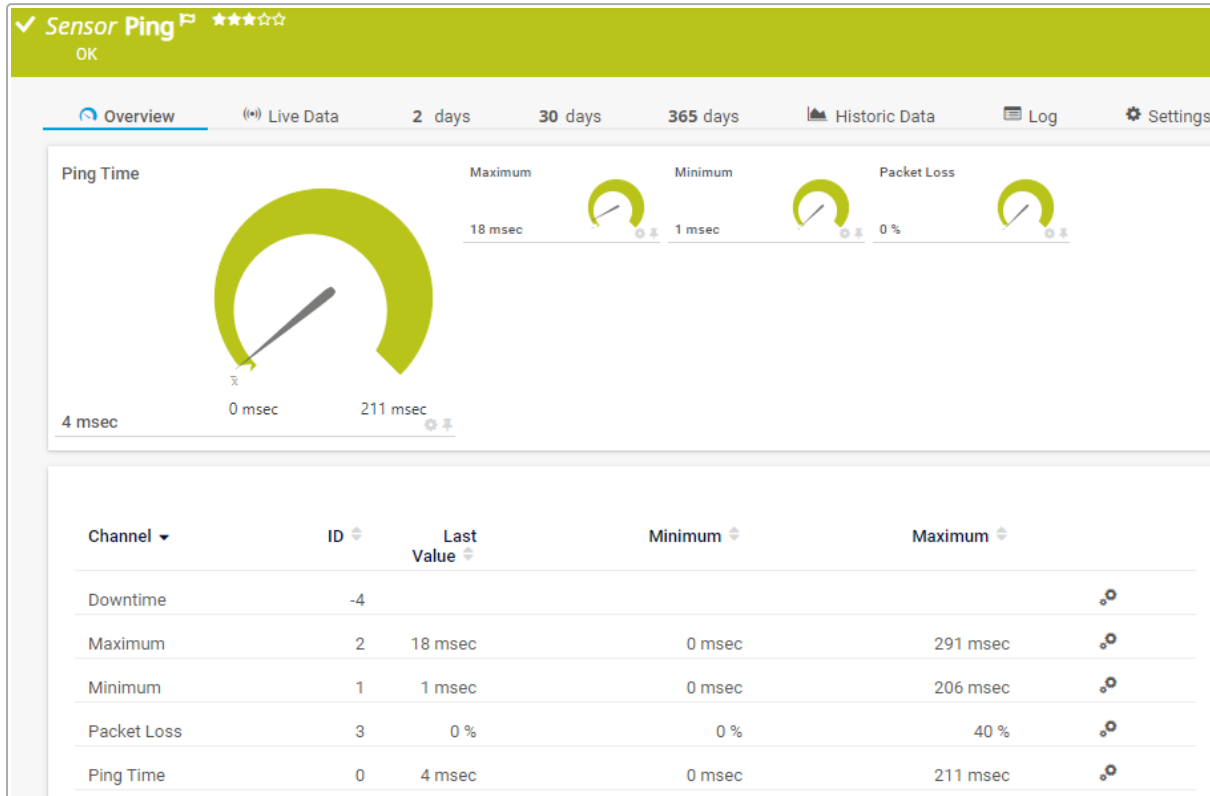
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.135 Ping Sensor

The Ping sensor sends an Internet Control Message Protocol (ICMP) echo request ("ping") from the probe system to the parent device to monitor its availability.

**i** The default number of pings per scanning interval is 5.



Ping Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Ping
- French: Ping
- German: Ping
- Japanese: Ping
- Portuguese: Ping
- Russian: Пинг
- Simplified Chinese: Ping
- Spanish: Ping

### Remarks

Consider the following [remarks](#) and requirements for this sensor:



Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Multi-platform probe	You can add this sensor to a multi-platform probe.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">How to create/customize statistical Ping sensor?</a></li> <li>Knowledge Base: <a href="#">Can I create an inverse Ping sensor?</a></li> </ul>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- pingsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Ping Settings

**Ping Settings**

Timeout (Sec.) ⓘ 5

---

Packet Size (Bytes) ⓘ 32

---

Ping Method ⓘ  Send one single ping  
 Send multiple ping requests (default)

---

Ping Count ⓘ 5

---

Ping Delay (ms) ⓘ 5

---

Acknowledge Automatically ⓘ  Show down status on error (default)  
 Show down (acknowledged) status on error

Ping Settings

Setting	Description
Timeout (Sec.)	Enter a timeout in seconds for the ping. If the reply takes longer than this value, PRTG cancels the request and shows an error message. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).
Packet Size (Bytes)	Enter the packet size for the ping in bytes. You can enter any value between <b>1</b> and <b>10000</b> . Enter an integer.  ⓘ We recommend that you use the default value.
Ping Method	Define the kind of ping check that the sensor performs with each scanning interval: <ul style="list-style-type: none"> <li>▪ Send one single ping: Send a single ping only. The sensor then shows the ping time only.  ⓘ This setting is useful for monitoring availability.</li> <li>▪ Send multiple ping requests (default): Send multiple pings in a row. The sensor then also shows the minimum and the maximum ping time as well as the packet loss (in percent).  ⓘ This setting is useful if you want to create reports about average ping times out of a series of ping requests.</li> </ul> <p> ⓘ If you select this setting, all of the ping requests must be lost for the sensor to show the Down <a href="#">status</a>. For example, if only one ping request is answered in a series of five, the sensor still shows the Up status.</p>

Setting	Description
Ping Count	<p>This setting is only visible if you select Send multiple ping requests (default) above.</p> <p>Enter the number of pings that the sensor sends in a row in one scanning interval. Enter an integer. The default value is 5.</p>
Ping Delay (ms)	<p>This setting is only visible if you select Send multiple ping requests (default) above.</p> <p>Enter the time in milliseconds (ms) that the sensor waits between two ping requests. Enter an integer. The default value is 5.</p> <p><b>i</b> Increase the value if the target device drops ping packets because of denial of service (DoS) suspicion.</p>
Acknowledge Automatically	<p>Define if you want to automatically <a href="#">acknowledge</a> the Down status of the sensor:</p> <ul style="list-style-type: none"> <li>Show down status on error (default): Do not automatically acknowledge an alarm if this sensor changes to the Down status.</li> <li>Show down (acknowledged) status on error: Automatically acknowledge an alarm. If this sensor changes to the Down status, it automatically shows the Down (Acknowledged) status instead.</li> </ul>

## Sensor Display

**Sensor Display**


Primary Channel **i** Downtime

---


Graph Type **i**  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>↑</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	Define how this sensor shows different channels:

Setting	Description
	<ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Maximum	The maximum ping time when using more than one ping per interval
Minimum	The minimum ping time when using more than one ping per interval
Packet Loss	The packet loss when using more than one ping per interval (%)
Ping Time	The ping time

Channel	Description
	 This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

How to create/customize statistical Ping sensor?

- <https://kb.paessler.com/en/topic/1873>

Can I create an inverse Ping sensor?

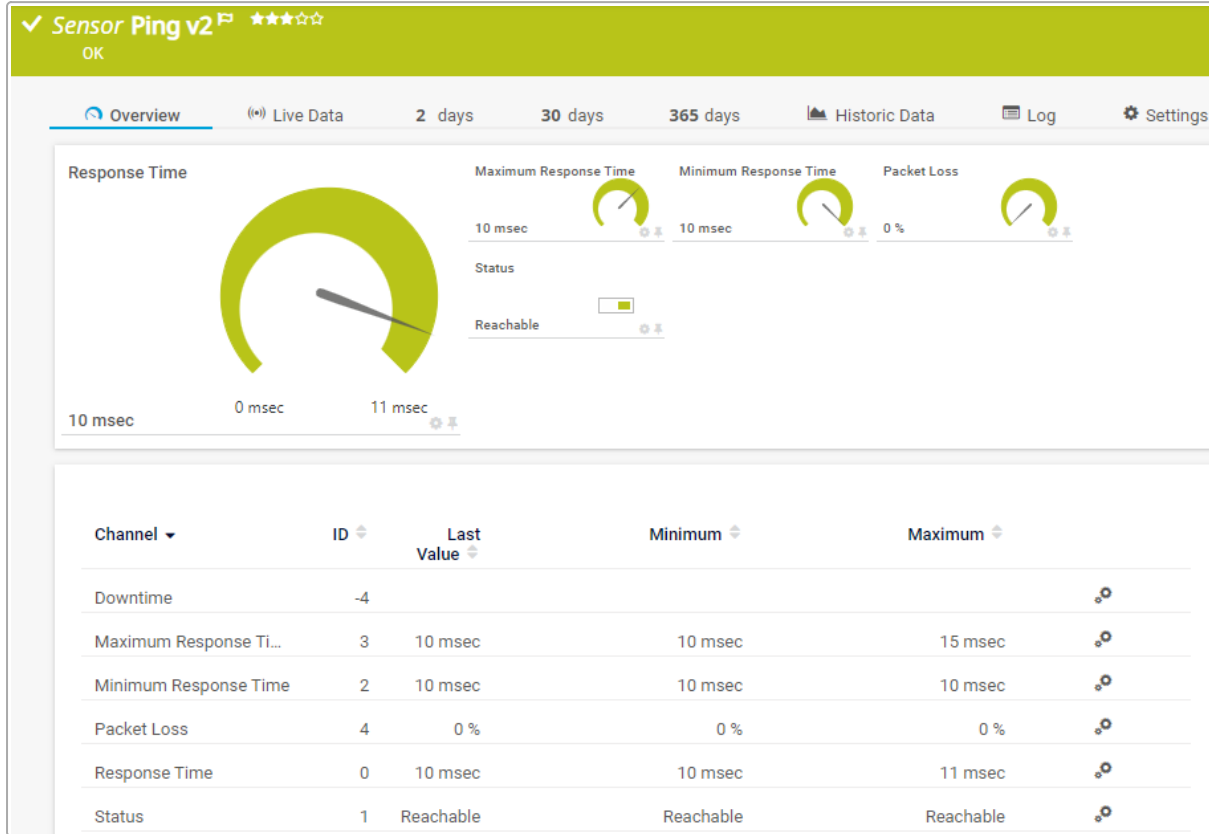
- <https://kb.paessler.com/en/topic/10203>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.136 Ping v2 Sensor

The Ping v2 sensor sends an Internet Control Message Protocol (ICMP) echo request ("ping") from the probe system to the parent device to monitor its availability.



Ping v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Ping v2
- French: Ping v2
- German: Ping v2
- Japanese: Ping v2
- Portuguese: Ping v2
- Russian: ПИНГ v2
- Simplified Chinese: Ping v2
- Spanish: Ping v2

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Scanning interval	The recommended scanning interval of this sensor is <b>1 minute</b> .
Multi-platform probe	You can add this sensor to a multi-platform probe.
Knowledge Base	Knowledge Base: <a href="#">How to create/customize statistical Ping sensor?</a>

### Add Sensor

Setting	Description
Inverted Error Status	<p>Select if you want the sensor to show the Down status if the target is reachable:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Show the Down status if the target is not reachable.</li> <li>▪ Enable: Show the Down status if the target is reachable.</li> </ul> <p><b>i</b> To change this behavior after sensor creation, open the <a href="#">channel settings</a> of channel Status and change the Lookup. Select <a href="#">prtg.standardlookups.paessler.icmp.reachability_state</a> if you want the sensor to show the Down status if the target is not reachable. Select <a href="#">prtg.standardlookups.paessler.icmp.reachability_state_reversed</a> if you want the sensor to show the Down status if the target is reachable.</p> <p><b>i</b> If you select Enable, Status is the primary channel.</p>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ exampletag ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Example Name

Basic Sensor Settings







The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- icmp
- ping
- pingsensor



■ For more information about basic sensor settings, see section [Sensor Settings](#) .

## Ping Settings

**Ping Settings**

Timeout (Sec.) 	5
Packet Size (Bytes) 	32
Ping Method 	<input type="radio"/> Send one single ping <input checked="" type="radio"/> Send multiple ping requests (default)
Ping Count 	5
Ping Delay (ms) 	5
Time to Live (Hops) 	64

Ping Settings

Setting	Description
Timeout (Sec.)	Enter a timeout in seconds for the ping. If the reply takes longer than this value, PRTG cancels the request and shows an error message. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).
Packet Size (Bytes)	Enter the packet size for the ping in bytes. You can enter any value between <b>1</b> and <b>10000</b> . Enter an integer.   We recommend that you use the default value.
Ping Method	Define the kind of ping check that the sensor performs with each scanning interval: <ul style="list-style-type: none"> <li>▪ <b>Send one single ping:</b> Send a single ping only. The sensor then shows the ping time only.</li> </ul>  This setting is useful for monitoring availability.



Setting	Description
	<ul style="list-style-type: none"> <li>Send multiple ping requests (default): Send multiple pings in a row. The sensor then also shows the minimum and the maximum ping time as well as the packet loss (in percent).                             <ul style="list-style-type: none"> <li><b>i</b> This setting is useful if you want to create reports about average ping times out of a series of ping requests.</li> <li><b>i</b> If you select this setting, all of the ping requests must be lost for the sensor to show the Down <a href="#">status</a>. For example, if only one ping request is answered in a series of five, the sensor still shows the Up status.</li> </ul> </li> </ul>
Ping Count	<p>This setting is only visible if you select Send multiple ping requests (default) <a href="#">above</a>.</p> <p>Enter the number of pings that the sensor sends in a row in one scanning interval. Enter an integer. The default value is <b>5</b>.</p>
Ping Delay (ms)	<p>This setting is only visible if you select Send multiple ping requests (default) <a href="#">above</a>.</p> <p>Enter the time in milliseconds (ms) that the sensor waits between two ping requests. Enter an integer. The default value is <b>5</b>.</p> <ul style="list-style-type: none"> <li><b>i</b> Increase the value if the target device drops ping packets because of denial of service (DoS) suspicion.</li> </ul>
Time to Live (Hops)	<p>Define the time to live (TTL) for the request. You can limit the number of network hops that the request can traverse before it is dropped. The default value is <b>64</b>.</p>

## Sensor Display

**Sensor Display**


Primary Channel **ⓘ** Downtime

---

Graph Type **ⓘ** 
 Show channels independently (default)
   
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p>


Setting	Description
	<p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

**Result Handling** 
  
 Discard result (default)
  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>



## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Maximum Response Time	The maximum ping time when using more than one ping per interval
Minimum Response Time	The minimum ping time when using more than one ping per interval
Packet Loss	The packet loss when using more than one ping per interval (%)
Response Time	The ping time  This channel is the primary channel by default.
Status	The target status <ul style="list-style-type: none"> <li>▪ Up status: Reachable</li> <li>▪ Down status: Unreachable</li> </ul>  This is the primary channel if you enable Inverted Error Status.

## More

### ■ KNOWLEDGE BASE

How to create/customize statistical Ping sensor?

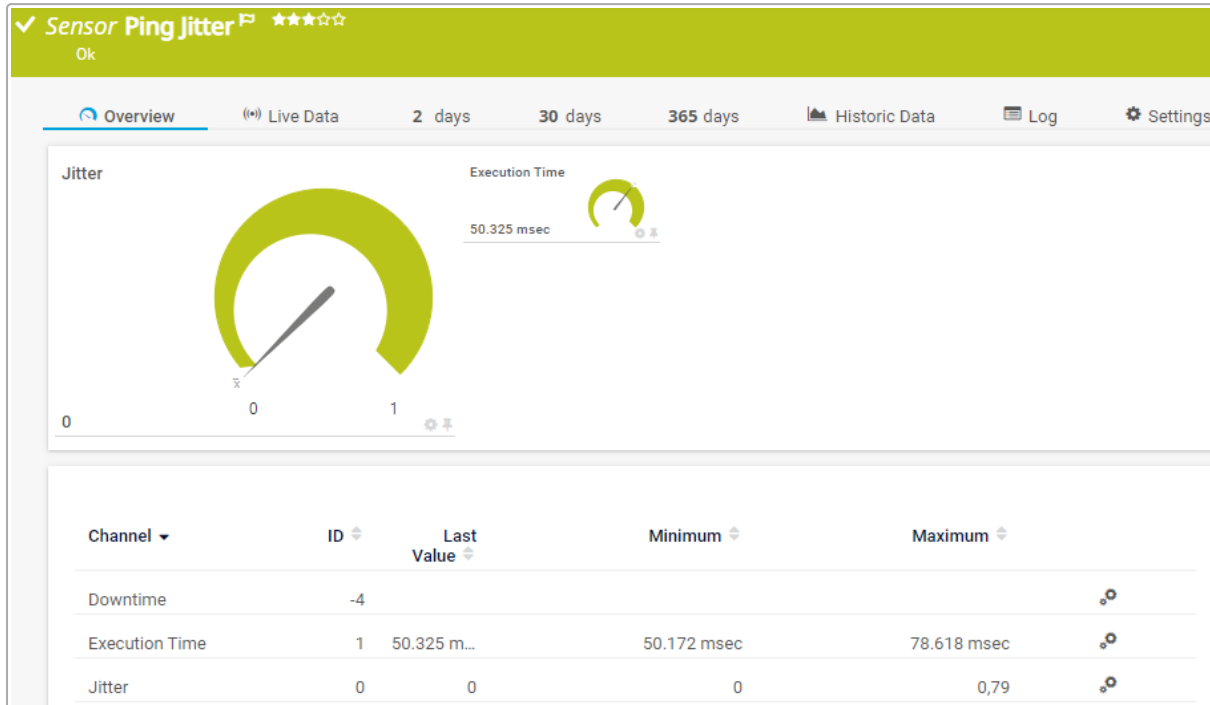
- <https://kb.paessler.com/en/topic/1873>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.137 Ping Jitter Sensor

The Ping Jitter sensor sends a series of Internet Control Message Protocol (ICMP) echo requests ("pings") to a URI to determine the statistical jitter.



Ping Jitter Sensor



For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Ping Jitter
- French: Gigue du Ping
- German: Ping Jitter
- Japanese: Ping ジッター監視
- Portuguese: Jitter Ping
- Russian: Дрожание пинга
- Simplified Chinese: Ping 抖动
- Spanish: Jitter de Ping

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node. If the sensor shows the error PE087, additionally install .NET 3.5 on the probe system.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Windows Server	We recommend Windows Server 2016 on the probe system for best performance of this sensor.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- ptfsensor

 For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Settings

#### Sensor Settings

**Ping Count** ⓘ

Sensor Settings

Setting	Description
Ping Count	Define the number of ICMP pings that the sensor sends. Enter an integer. The default value is <b>50</b> .

## Debug Options

**Debug Options**

**Result Handling** ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display


**Sensor Display**

**Primary Channel** ⓘ Downtime


---

**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Execution Time	The execution time
Jitter	<p>The statistical jitter value</p> <p>The <b>Real Time Jitter</b> value is updated every time a packet is received using the formula described in RFC 1889:</p> <pre>Jitter = Jitter + ( abs( ElapsedTime - OldElapsedTime ) - Jitter ) / 16</pre> <p>The <b>Statistical Jitter</b> value is calculated according to the first x packets received using the statistical variance formula:</p> <pre>Jitter Statistical = SquareRootOf( SumOf( ( ElapsedTime[i] - Average) ^ 2 ) / ( ReceivedPacketCount - 1 ) )</pre> <p><b>i</b> This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

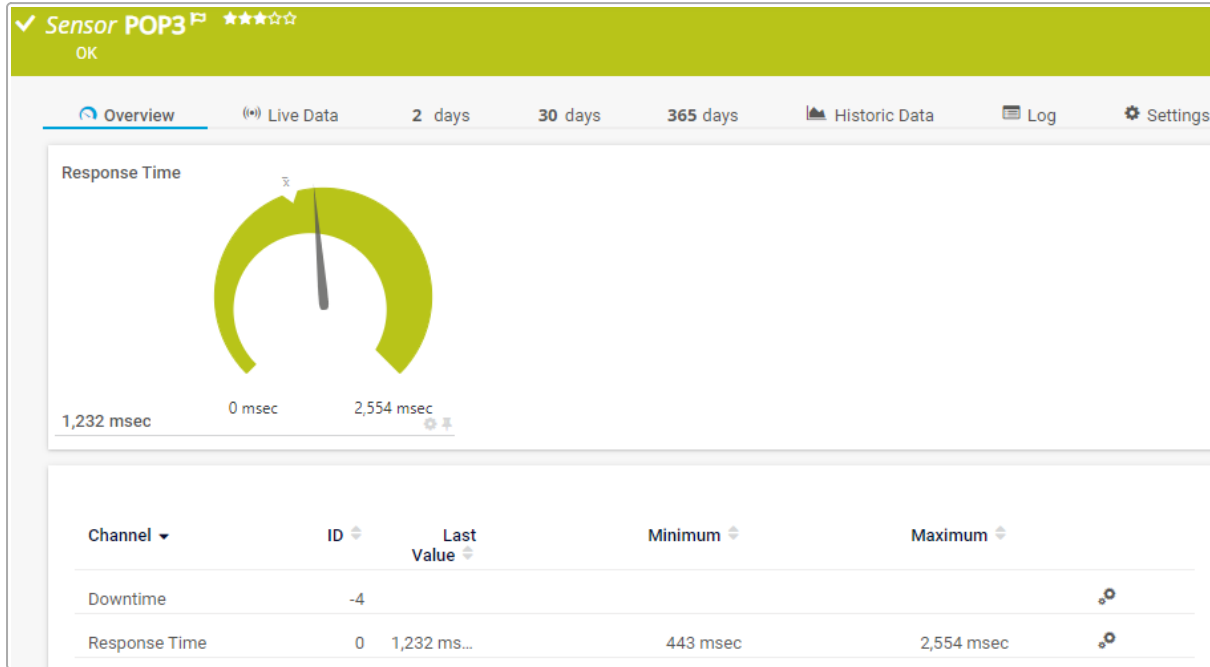
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>



## 7.8.138 POP3 Sensor

The POP3 sensor monitors an email server via the Post Office Protocol version 3 (POP3).



POP3 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: POP3
- French: POP3
- German: POP3
- Japanese: POP3
- Portuguese: POP3
- Russian: POP3
- Simplified Chinese: POP3
- Spanish: POP3

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
SRP ciphers	This sensor does not support Secure Remote Password (SRP) ciphers.

Remark	Description
Microsoft 365 mailboxes	This sensor does not support Microsoft 365 mailboxes. If you want to monitor a Microsoft 365 mailbox, use the <a href="#">Microsoft 365 Mailbox</a> <sup>1252</sup> sensor.
IPv4	This sensor only supports IPv4.
Performance impact	This sensor has a <b>low</b> performance impact.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- mailsensor
- pop3sensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### POP3 Specific

#### POP3 Specific

**Timeout (Sec.)** ⓘ 60

---

**Port** ⓘ 995

POP3 Specific

Setting	Description
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).

Setting	Description
	<p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
Port	<p>Specify the port that the sensor uses for the POP3 connection. The default port for unsecure connections is <b>110</b> and the default port for secure connections is <b>995</b>. The actual setting depends on the server you connect to. Enter an integer.</p> <p><b>i</b> We recommend that you use the default value.</p> <p><b>i</b> If the connection is unsuccessful, try a different port number.</p>

## Connection Security

**Connection Security**

Transport-Level Security **i**

Use transport-level security if available using StartTLS  
 Use transport-level security if available  
 Enforce transport-level security using StartTLS  
 Enforce transport-level security (default)

Connection Security

Setting	Description
Transport-Level Security	<p>Define how the sensor handles the security of the connection:</p> <ul style="list-style-type: none"> <li>▪ Use transport-level security if available using StartTLS: Try to connect to the server via a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection and StartTLS. If the server does not support this, the sensor tries to connect without connection security.</li> <li>▪ Use transport-level security if available: Try to connect to the server via an SSL/TLS-secured connection. If the server does not support this, the sensor tries to connect without connection security.</li> <li>▪ Enforce transport-level security using StartTLS: Try to connect to the server via an SSL/TLS-secured connection and StartTLS. If the server does not support this, the sensor shows the Down <a href="#">status</a>.</li> <li>▪ Enforce transport-level security (default): Try to connect to the server via an SSL/TLS-secured connection. If the server does not support this, the sensor shows the Down status.</li> </ul> <p><b>i</b> If the sensor connects to a server via StartTLS, the connection is first established without connection security. After the connection has been established, the sensor sends a certain command (<b>StartTLS</b>) over the unsecured connection to negotiate a secure connection via SSL/TLS.</p>

Setting	Description
	<p><b>i</b> If the sensor does <b>not</b> use StartTLS, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If no secure connection is possible, no communication takes place.</p>

### Authentication

**Authentication**

**POP3 Authentication Method** ⓘ

- Without login (default)
- User name and password
- 128-bit MD5 hash value (APOP)

**Result Handling** ⓘ

- Discard result (default)
- Store result

Authentication

Setting	Description
POP3 Authentication Method	<p>Select the authentication method for the POP3 connection:</p> <ul style="list-style-type: none"> <li>Without login (default): Only monitor the connection to the POP3 server.</li> <li>User name and password: Log in to the POP3 server with user name and password. <ul style="list-style-type: none"> <li> This is a simple login. It is not secure.</li> </ul> </li> <li>128-bit MD5 hash value (APOP): Send the password in an encrypted form using APOP. <ul style="list-style-type: none"> <li> The POP3 server that you connect to must support this option.</li> </ul> </li> </ul>
User Name	<p><a href="#">This setting is only visible if you select User name and password or 128-bit MD5 hash value (APOP) above.</a></p> <p>Enter a user name for POP3 authentication. Enter a string.</p>
Password	<p><a href="#">This setting is only visible if you select User name and password or 128-bit MD5 hash value (APOP) above.</a></p> <p>Enter a user name for POP3 authentication. Enter a string.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display


**Sensor Display**

Primary Channel Downtime


---


Graph Type  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Response Time	The response time  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

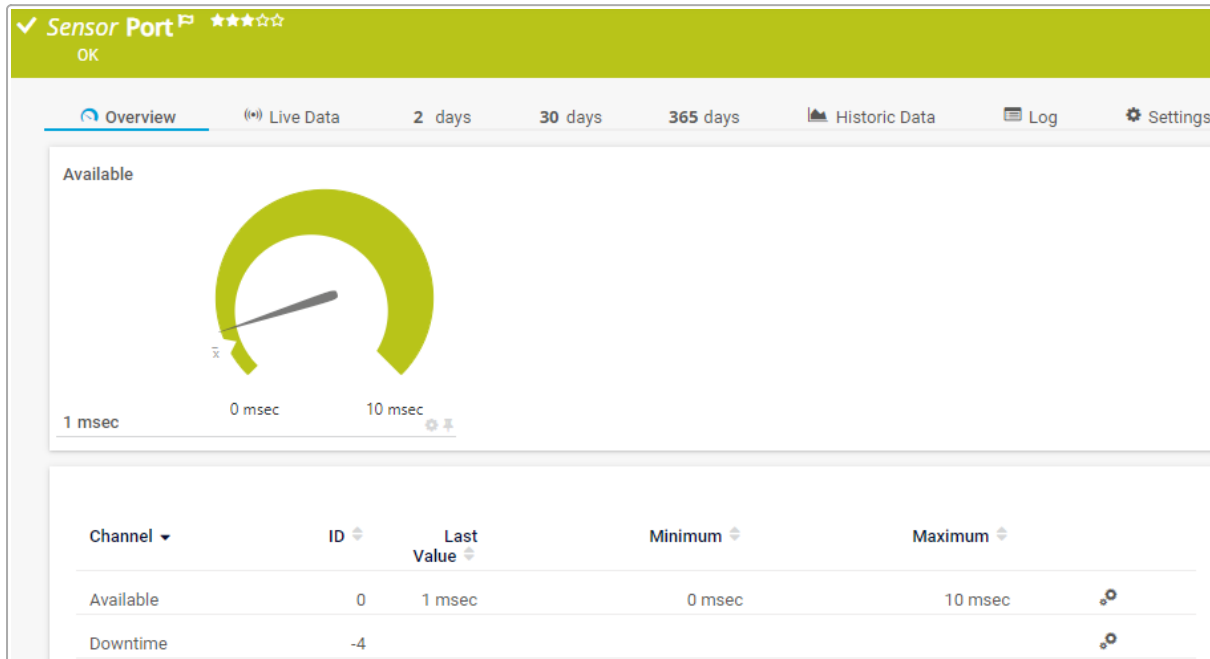
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.139 Port Sensor

The Port sensor monitors a network service by connecting to its port. It tries to connect to the specified TCP/IP port number of a device and waits for the request to be accepted.

**i** Depending on your settings, the sensor can alert you either when the monitored port is open or when it is closed.



Port Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Poort
- French: Port
- German: Port
- Japanese: ポート
- Portuguese: Porta
- Russian: Порт
- Simplified Chinese: 端口
- Spanish: Puerto

### Remarks

Consider the following [remarks](#) and requirements for this sensor:



Remark	Description
SRP ciphers	This sensor does not support Secure Remote Password (SRP) ciphers.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- portsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Port Specific

#### Port Specific

**Timeout (Sec.)** ⓘ 60

---

**Port** ⓘ 80

Port Specific

Setting	Description
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The

Setting	Description
	<p>maximum timeout value is 900 seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
Port	Enter the number of the port to which this sensor connects. Enter an integer.

### Connection Security

**Connection Security**

Transport-Level Security **i**  Do not use transport-level security (default)  
 Use transport-level security

Connection Security

Setting	Description
Transport-Level Security	<p>Define the security of the connection:</p> <ul style="list-style-type: none"> <li>Do not use transport-level security (default): Establish the connection without connection security.</li> <li>Use transport-level security: Establish the connection with the strongest Secure Sockets Layer (SSL)/Transport Layer Security (TLS) method that the target device provides.</li> </ul>

### Advanced Sensor Settings

**Advanced Sensor Settings**

Goal **i**  Open  
 Closed

Command Handling **i**  Do not send a command (default)  
 Send a command

Result Handling **i**  Discard result (default)  
 Store result

Advanced Sensor Settings

Setting	Description
Goal	<p>Define how the sensor reports on the port:</p> <ul style="list-style-type: none"> <li>▪ Open: Show the Up <a href="#">status</a> if the port is open, and the Down status if the port is closed.</li> <li>▪ Closed: Show the Up status if the port is closed, and the Down status if the port is open.</li> </ul>
Command Handling	<p><a href="#">This setting is only visible if you select Open above.</a></p> <p>Define whether the sensor sends a command after it opens the port:</p> <ul style="list-style-type: none"> <li>▪ Do not send a command (default): Only check if a connection to the port is possible.</li> <li>▪ Send a command: Open a Telnet session to the respective port and send a command.  <span style="color: red;">ⓘ</span> You cannot use this option if the target device is a web server.</li> </ul>
Command	<p><a href="#">This setting is only visible if you select Send a command above.</a></p> <p>Enter the command that the sensor sends to the respective port in a Telnet session. Enter a string.</p> <p><span style="color: red;">ⓘ</span> You cannot use line breaks. You can only use a simple Telnet command in a single line.</p>
Response	<p>Define if the sensor further processes the response:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do not check the response.</li> <li>▪ Check response code (integer): Check if the response matches a defined response code. Define the response code below.</li> <li>▪ Check response text: Check if the response matches a defined response text. Define the response text below.</li> </ul>
Allowed Response Code	<p><a href="#">This setting is only visible if you select Check response code (integer) above.</a></p> <p>Enter the code that the target device must return. If the target device does not return this code, the sensor shows the Down status. Enter an integer.</p>
Check for Keywords (positive)	<p><a href="#">This setting is only visible if you select Check response text above.</a></p> <p>Check if the response contains a specific keyword:</p> <ul style="list-style-type: none"> <li>▪ Disable: Do not check for positive keywords.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Enable keyword check (positive): Check if a specific keyword exists in the received value. Define the keyword below. If the response does not contain the keyword, the sensor shows the Down status.</li> </ul>
<p>Response Must Include (Down Status if Not Included)</p>	<p><b>This setting is only visible if you select</b> Enable keyword check (positive) <b>above.</b></p> <p>Define the search string that the response must contain. You can enter a simple string in plain text or a <a href="#">regular expression (regex)</a>.</p> <ul style="list-style-type: none"> <li>❗ The search string must be case-sensitive.</li> <li>❗ If the data does <b>not</b> include the search pattern, the sensor shows the Down status.</li> </ul>
<p>Search Method</p>	<p>Define the method with which you want to provide the search string:</p> <ul style="list-style-type: none"> <li>▪ Simple string search (default): Search for a simple string in plain text.</li> <li>❗ The characters <b>*</b> and <b>?</b> work as placeholders. <b>*</b> stands for no number or any number of characters and <b>?</b> stands for exactly one character. You cannot change this behavior. The literal search for these characters is only possible with a regex.</li> <li>▪ Regular expression: Search with a regex.</li> <li>❗ PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</li> </ul>
<p>Check for Keywords (negative)</p>	<p><b>This setting is only visible if you select</b> Simple string search (default) <b>above.</b></p> <p>Check if the response does <b>not</b> contain a specific keyword:</p> <ul style="list-style-type: none"> <li>▪ Disable: Do not check for negative keywords.</li> <li>▪ Enable keyword check (negative): Check if a specific keyword does not exist in the received value. Define the keyword below. If the response does contain the keyword, the sensor shows the Down status.</li> </ul>
<p>Response Must Not Include (Down Status if Included)</p>	<p><b>This setting is only visible if you select</b> Enable keyword check (negative) <b>above.</b></p> <p>Define the search string that the response must <b>not</b> contain. You can enter a simple string in plain text or a regex.</p> <ul style="list-style-type: none"> <li>❗ The search string must be case-sensitive.</li> <li>❗ If the data does include the search pattern, the sensor shows the Down status.</li> </ul>

Setting	Description
Search Method	<p>Define the method with which you want to provide the search string:</p> <ul style="list-style-type: none"> <li>Simple string search (default): Search for a simple string in plain text.</li> </ul> <p><b>i</b> The characters <code>*</code> and <code>?</code> work as placeholders. <code>*</code> stands for no number or any number of characters and <code>?</code> stands for exactly one character. You cannot change this behavior. The literal search for these characters is only possible with a regex.</p> <ul style="list-style-type: none"> <li>Regular expression: Search with a regex.</li> </ul> <p><b>i</b> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the <code>\Logs\sensors</code> subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are <code>Result of Sensor [ID].txt</code> and <code>Result of Sensor [ID].Data.txt</code>. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**


Primary Channel **i** Downtime

---


Graph Type **i**  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>+</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p>

Setting	Description
	<ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Available	<p>The time until a request to a port is accepted</p> <ul style="list-style-type: none"> <li> This channel is the primary channel by default.</li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>

## More

 KNOWLEDGE BASE

What security features does PRTG include?

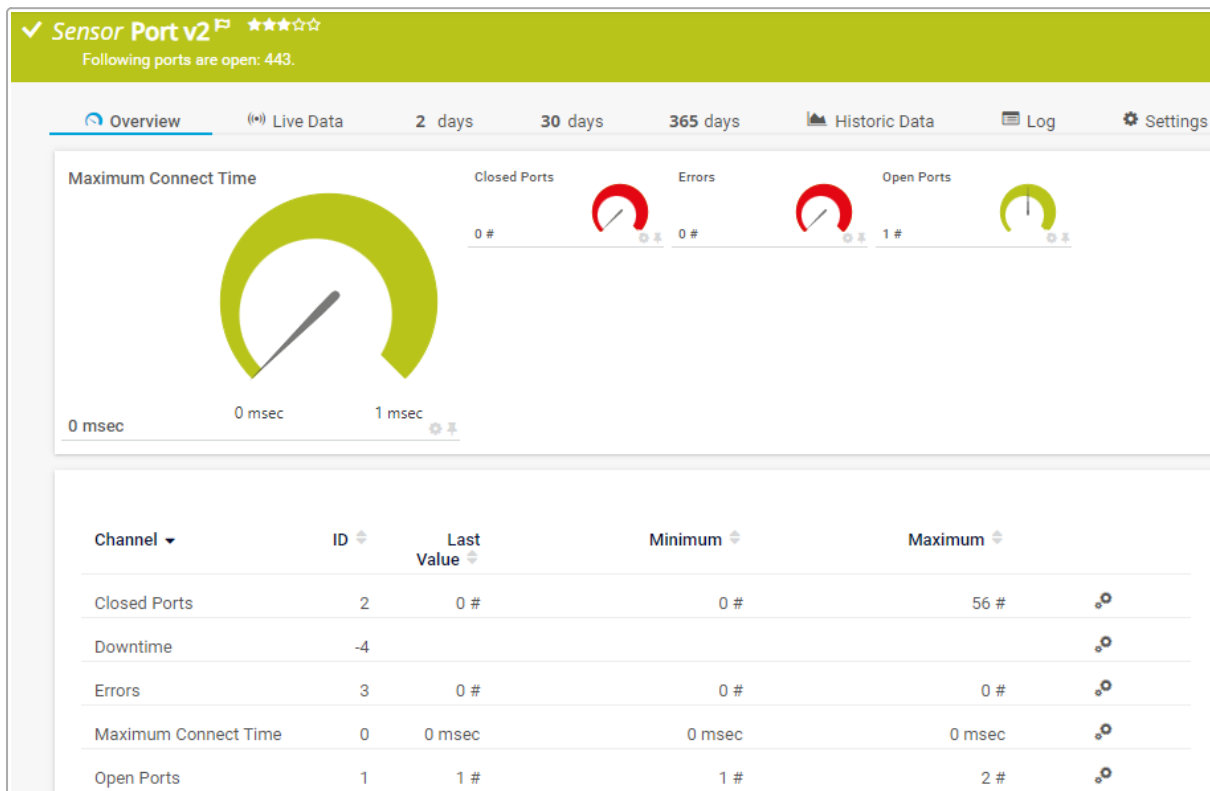
- <https://kb.paessler.com/en/topic/61108>

## 7.8.140 Port v2 Sensor (BETA)

The Port v2 sensor monitors a network service by connecting to one or more of its TCP/IP ports.

**i** Depending on your settings, the sensor can alert you either when the monitored port is open or when it is closed.

**BETA** This sensor is in beta status. The operating methods and the available settings are still subject to change. Do not expect that all functions work properly, or that this sensor works as expected at all.



Port v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Poort v2
- French: Port v2
- German: Port v2
- Japanese: ポート v2
- Portuguese: Porta v2
- Russian: Порт v2
- Simplified Chinese: Port v2
- Spanish: Puerto v2



## Remarks

Consider the following [remarks](#)<sup>[1627]</sup> and requirements for this sensor:

Remark	Description
Enabled Beta Sensors experimental feature	This sensor requires that the Beta Sensors <a href="#">experimental feature</a> is enabled.  ■ For more information, see the Knowledge Base: <a href="#">What are beta sensors and how can I use them?</a>
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Scanning interval	This sensor has a fixed minimum scanning interval for performance reasons. You cannot use a shorter scanning interval. Consequently, shorter scanning intervals in the <a href="#">Monitoring</a> settings are not available for this sensor.  <ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">5 minutes</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Known Issues

- The sensor shows the Unknown state if a sensor scan was executed during the scan of the port list. If this issue occurs, reduce the list of monitored ports or increase the [Scanning Interval](#)<sup>[1630]</sup> of the sensor. The scan of each port takes about two seconds. For example, if you monitor the ports [1-900](#), the sensor needs around 1,800 seconds (30 minutes) to complete the port list.

## Add Sensor

Setting	Description
Goal	Define how the sensor reports on the ports:  <ul style="list-style-type: none"> <li>▪ Open: Shows the Up <a href="#">status</a> if the port is open, and the Down status if the port is closed.</li> <li>▪ Closed: Shows the Up status if the port is closed, and the Down status if the port is open.</li> </ul> <p>❗ You can modify the limits in the channel settings to change the sensor behavior. For more information, see section <a href="#">Channel Settings</a>.</p>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- portrangesensor
- portsensor
- tcp

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Port Specific

### Port Specific

**Timeout (Sec.)** ⓘ 5

---

**Port-by-Port Delay (ms)** ⓘ 0

---

**Port List** ⓘ 443


Port Specific

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p>ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
Port-by-Port Delay (ms)	<p>Define how long the sensor waits before it tries to connect to the next port. The maximum delay value is <b>100</b> ms.</p>


Setting	Description
Port List	Enter the port numbers that the sensor tries to connect to. Enter one port number per line. PRTG supports the port numbers 1 - 65535. You can also specify port ranges by using A-B, for example 8080-8090. Enter an integer.

## Sensor Display




**Sensor Display**

Primary Channel  Downtime

---

Graph Type   Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result: Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Closed Ports	The number of closed ports
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Errors	The number of errors

Channel	Description
	<p>ⓘ This channel has a default limit:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: 0</li> </ul>
Maximum Connect Time	<p>The maximum time until a request to connect to a port was accepted</p> <p>ⓘ This channel is the primary channel by default.</p>
Open Ports	The number of open ports

## More

### ■ KNOWLEDGE BASE

What are beta sensors and how can I use them?

- <https://kb.paessler.com/en/topic/88697>

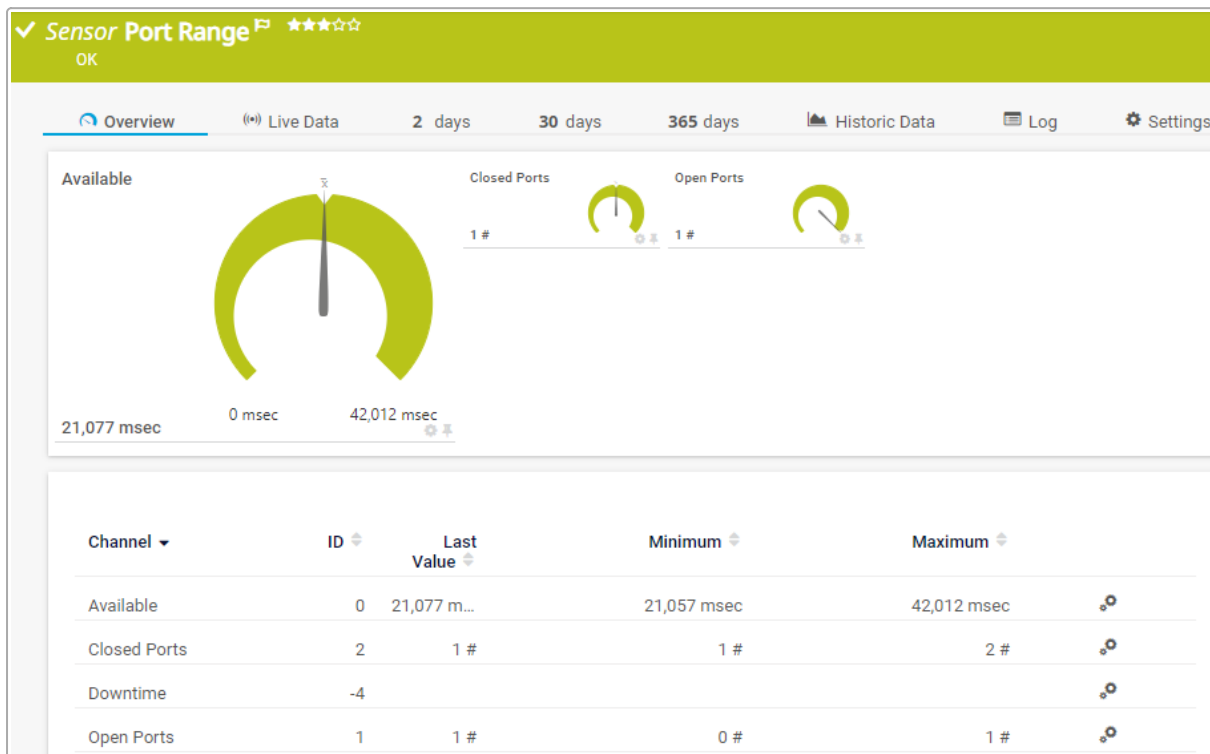
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.141 Port Range Sensor

The Port Range sensor monitors a network service by connecting to various TCP/IP ports. It tries to connect to the specified TCP/IP port numbers of a device in succession and waits for the device to accept each request.

- Optionally, you can set limits in the [channel settings](#). This way, you can get alerts about open and closed ports.



Port Range Sensor

- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Poortbereik
- French: Plage de port
- German: Portbereich
- Japanese: ポート範囲
- Portuguese: Intervalo de portas
- Russian: Диапазон портов
- Simplified Chinese: 端口范围
- Spanish: Rango de puerto

## Remarks

Consider the following [remarks](#)<sup>[1633]</sup> and requirements for this sensor:

Remark	Description
SRP ciphers	This sensor does not support Secure Remote Password (SRP) ciphers.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- portrangesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Port Range Specific

### Port Range Specific

Timeout (Sec.) ⓘ

---

Port-by-Port Delay (ms) ⓘ

---

Port Range Selection Method ⓘ  Port range  
 List of ports

---

Range Start ⓘ

---

Range End ⓘ

---

If Value Changes ⓘ  Ignore (default)  
 Trigger 'change' notification

Port Range Specific

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p> ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
Port-by-Port Delay (ms)	<p>Define how long the sensor waits in milliseconds (ms) to go to the next port while it runs through all specified ports.</p>
Port Range Selection Method	<p>Define whether you want to monitor all ports within a range or if you want to monitor several individual ports:</p> <ul style="list-style-type: none"> <li>▪ Port range: Monitor ports within a range.</li> <li>▪ List of ports: Monitor several individual ports.</li> </ul>
Range Start	<p><b>This setting is only visible if you select Port range above.</b></p> <p>Enter the port number where the scan starts. Enter an integer.</p>
Range End	<p><b>This setting is only visible if you select Port range above.</b></p> <p>Enter the port number where the scan ends. Enter an integer.</p>
Port List	<p><b>This setting is only visible if you select List of ports above.</b></p>



Setting	Description
	Enter the numbers of the ports that the sensor tries to connect to. Enter one or more individual integers. Enter each port in one line.
If Value Changes	<p>Define what the sensor does if the number of <a href="#">closed ports</a> or <a href="#">open ports</a> changes:</p> <ul style="list-style-type: none"> <li>Ignore (default): Do nothing.</li> <li>Trigger 'change' notification: Send an internal message that indicates a change. <ul style="list-style-type: none"> <li><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</li> </ul> </li> </ul>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Available	The time until requests to ports are accepted  This channel is the primary channel by default.
Closed Ports	The number of closed ports
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Open Ports	The number of open ports

## More

### ■ KNOWLEDGE BASE

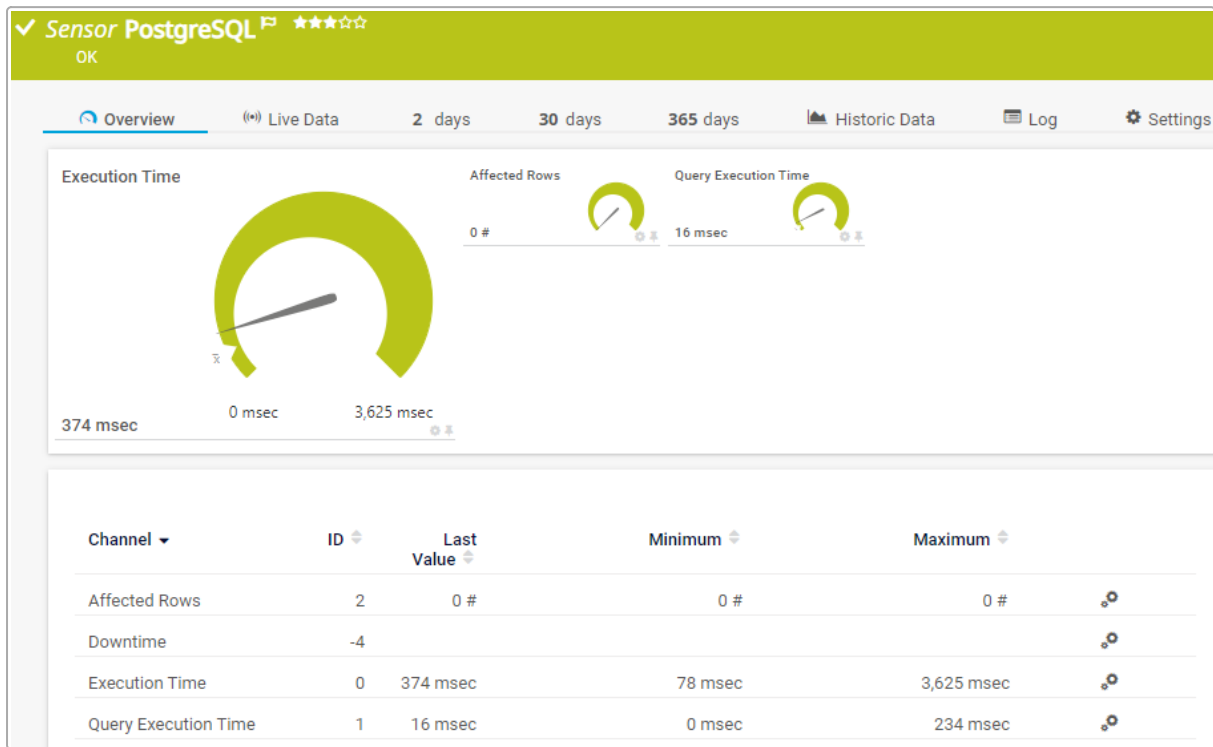
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.142 PostgreSQL Sensor

The PostgreSQL sensor monitors a database on a PostgreSQL server and executes a query.

- i** The sensor can also process the data table and show the values that you define in individual channels.



PostgreSQL Sensor

- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1647</sup>.

### Sensor in Other Languages

- Dutch: PostgreSQL
- French: PostgreSQL
- German: PostgreSQL
- Japanese: PostgreSQL
- Portuguese: PostgreSQL
- Russian: PostgreSQL
- Simplified Chinese: PostgreSQL
- Spanish: PostgreSQL

### Remarks

Consider the following [remarks](#)<sup>1637</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
SQL query storage	<p>This sensor requires that you store the SQL query in a file on the probe system. In a cluster, copy the file to every cluster node. Save the SQL script with the query in the \Custom Sensors\sql\postgresql subfolder of the <a href="#">PRTG program directory</a>.</p> <ul style="list-style-type: none"> <li>■ For more information, see the Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a></li> </ul>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <ul style="list-style-type: none"> <li>ⓘ If the framework is missing, you cannot create this sensor.</li> <li>■ For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></li> </ul>
PostgreSQL version	This sensor supports as of PostgreSQL 7.x.
IPv6	This sensor supports IPv6.
Lookups	This sensor can use <a href="#">lookups</a> <sup>[1644]</sup> . Select Lookup as Channel #x Unit and define the lookup file in Channel #x Lookup.
Credentials	Define the credentials for database management systems in settings that are higher in the object hierarchy.
Knowledge Base	Knowledge Base: <a href="#">How can I monitor strings from an SQL database and show a sensor status depending on it?</a>
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- sqlsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Database Specific

### Database Specific

**Database** ⓘ MyDatabase

---

**SSL Mode** ⓘ  Disable  
 Allow  
 Prefer  
 Require

Database Specific

Setting	Description
Database	Enter the name of the PostgreSQL database to which the sensor connects, for example <a href="#">MyDatabase</a> . This is a logical entity on the database server where database objects exist.
SSL Mode	<p>Select the PostgreSQL Secure Sockets Layer (SSL) mode for the connection:</p> <ul style="list-style-type: none"> <li>▪ Disable: Do not use SSL.</li> <li>▪ Allow: Use SSL if the server demands it.</li> <li>▪ Prefer: Use SSL if the server supports it.</li> <li>▪ Require: Always use SSL and deny the connection if the server does not support it.</li> </ul>

Setting	Description
	<p>The SSL mode options that you can choose are the same as the values of the PostgreSQL <code>sslmode</code> parameter. PRTG sends it with the sensor requests.</p> <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> PostgreSQL SSL connections require OpenSSL to be installed on both the target server and on the probe system.</li> <li><span style="color: blue;">❗</span> For more information about the PostgreSQL SSL modes, refer to the PostgreSQL documentation.</li> </ul>

## Data

**Data**

SQL Query File ⓘ *Demo Serveruptime.sql*

Input Parameter Handling ⓘ  Do not use input parameter (default)  
 Use input parameter

Transaction Handling ⓘ  Do not use transaction (default)  
 Use transaction and always roll back  
 Use transaction and commit on success






Data Processing ⓘ *Only execute query (default)*

Result Handling ⓘ  Discard result (default)  
 Store result

Data

Setting	Description
SQL Query File	<p>Select the SQL query file that includes a valid SQL statement that the sensor executes on the server with every scanning interval. The list contains SQL scripts from the <code>\Custom Sensors\sql</code> subfolder of the <a href="#">PRTG program directory</a> on the probe system. Store your script there. If you use the script on a cluster probe, you must store the script on all cluster nodes.</p> <p>A correct expression in the file could be: <code>SELECT AVG(UnitPrice) FROM Products</code>. If you want to use transactions, separate the individual steps with semicolons <code>;</code>.</p> <ul style="list-style-type: none"> <li><span style="color: blue;">❗</span> Note that with each request, PRTG transfers the full result set, so use filters and limits in your query.</li> <li><span style="color: blue;">❗</span> The demo script <code>Demo Serveruptime.sql</code> is available by default. You can use it to monitor the uptime of the target server.</li> </ul>

Setting	Description
	<p>■ See also the Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a></p> <p>ⓘ You cannot change this value after sensor creation.</p>
Input Parameter Handling	<p>Define if you want to pass a parameter to the SQL query file:</p> <ul style="list-style-type: none"> <li>▪ Do not use input parameter (default): Execute the SQL query file without using variables.</li> <li>▪ Use input parameter: Execute an SQL query file that contains a variable. Provide the parameter that you want to use in the query below.</li> </ul>
Input Parameter	<p><b>This setting is only visible if you select Use input parameter above.</b></p> <p>Enter the parameter that you want to pass to the SQL query file. This parameter replaces the variables <code>@prtg</code>, <code>:prtg</code>, or <code>?</code> in the SQL query, considering the general rules for SQL variables.</p> <p>You can also use PRTG placeholders for custom sensors (command-line parameters) as input parameters, for example, <code>%sensorid</code> or <code>%deviceid</code>. For more information, see section <a href="#">Custom Sensors</a>.</p> <p>ⓘ Provide strings as they are and do not surround them with quotation marks. PRTG automatically and correctly inserts string parameters into the query.</p>
Transaction Handling	<p>Define if you want to use transactions and if they affect the database content:</p> <ul style="list-style-type: none"> <li>▪ Do not use transaction (default): Do not execute transactions.</li> <li>▪ Use transaction and always roll back: The query does not change data in the database. In the SQL query file, separate the single steps of the transaction with semicolons.</li> <li>▪ Use transaction and commit on success: The query changes data in the database. The changes only apply if all execution steps succeed without any errors. In the SQL query file, separate the single steps of the transaction with semicolons.</li> </ul>
Data Processing	<p>Define whether the sensor processes data from the database:</p> <ul style="list-style-type: none"> <li>▪ Only execute query (default): Only show information about the number of affected rows and the execution time of the query. Affected rows are rows that were changed by the query (for example, created, deleted, or edited).</li> <li>▪ Count table rows: Execute a <b>SELECT</b> statement and monitor how many rows of the data table this statement returns.</li> <li>▪ Process data table: Read and analyze the data table. If you select this option, the sensor counts rows with <b>SELECT</b> statements as well.</li> </ul>

Setting	Description
	<p> You cannot change this value after sensor creation.</p>
DBNull Handling	<p><a href="#">This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</a></p> <p>Define the sensor behavior if the query returns <b>DBNull</b>:</p> <ul style="list-style-type: none"> <li>▪ Error: Show the Down status if the query returns <b>DBNull</b>.</li> <li>▪ Number 0: Recognize the result <b>DBNull</b> as a valid value and interpret it as the number <b>0</b>.</li> </ul>
Select Channel Value by	<p><a href="#">This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</a></p> <p>Define how to select the desired cell in the database table:</p> <ul style="list-style-type: none"> <li>▪ Column number: Determine the channel value by using the value in row 0 of the column whose number you specify in Channel #x Column Number.</li> <li>▪ Column name: Determine the channel value by using the value in row 0 of the column whose name you specify in Channel #x Column Name.</li> <li>▪ Row number: Determine the channel value by using the value in column 0 of the row whose number you specify in Channel #x Row Number.</li> <li>▪ Key value pair: Determine the channel value by searching in column 0 for the key you specify in Channel #x Key and by returning the value in column 1 of the same row where the key value was found.</li> </ul> <p> Defining how the desired cell in the database table is selected is necessary to configure the cells that are used in the channels.</p> <p> The option you select here also defines the method of how to optionally determine a value for the sensor message. For more information, see setting Use Data Table Value in Message.</p> <p> For an example for channel value selection, see section <a href="#">Monitoring Databases</a>.</p>
Channel #2 - #10	<p><a href="#">This setting is only visible if you select Process data table above.</a></p> <p>You can define up to 10 channels. You must define at least one channel, so you see all available settings for <b>Channel #1</b>. Specify how to handle all other possible channels:</p> <ul style="list-style-type: none"> <li>▪ Disable: Do not create this channel.</li> <li>▪ Enable: Create this channel.</li> </ul> <p> It is not possible to enable or disable channels after sensor creation.</p>



Setting	Description
Channel #x Name	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation.</p> <p>Enter a name for the channel. Enter a string. The sensor dynamically generates channels with this name as identifier.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Channel #x Column Number	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation and if you select Column number for the setting Select Channel Value by.</p> <p>Provide the number of the column to use to determine the channel value in row 0. Enter an integer.</p>
Channel #x Column Name	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation and if you select Column name for the setting Select Channel Value by.</p> <p>Provide the name of the column to use to determine the channel value in row 0. Enter an integer.</p>
Channel #x Row Number	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation and if you select Row number for the setting Select Channel Value by.</p> <p>Provide the number of the column to use to determine the channel value in row 0. Enter an integer.</p>
Channel #x Key	<p>This setting is only visible if you select Process data table for the setting Data Processing during sensor creation and if you select Key value pair for the setting Select Channel Value by.</p> <p>Provide the key to search for in column 0 of the data table. The value in column 1 of the same row where the key value was found to use to determine the channel value. Enter a string.</p>
Channel #x Mode	<p>This setting is only visible if you select Process data table above.</p> <p>Define how to display the determined value in the channel:</p> <ul style="list-style-type: none"> <li>▪ Absolute (default): Show the value as the sensor retrieves it from the data table.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Difference: The sensor calculates and shows the difference between the last and the current value returned from the data table.</li> <li>ⓘ This mode is not compatible with the unit Lookup.</li> <li>ⓘ This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative and decreasing values.</li> <li>ⓘ You cannot change this value after sensor creation.</li> </ul>
Channel #x Unit	<p>This setting is only visible if you select Process data table above.</p> <p>Define the unit of the channel value:</p> <ul style="list-style-type: none"> <li>▪ BytesBandwidth</li> <li>▪ BytesMemory</li> <li>▪ BytesDisk</li> <li>▪ Temperature</li> <li>▪ Percent</li> <li>▪ TimeResponse</li> <li>▪ TimeSeconds</li> <li>▪ TimeHours</li> <li>▪ Count</li> <li>▪ CPU</li> <li>▪ BytesFile</li> <li>▪ SpeedDisk</li> <li>▪ SpeedNet</li> <li>▪ Custom</li> <li>▪ Lookup</li> </ul> <p>■ For more information about the available units, see section <a href="#">Custom Sensors</a>.</p> <p>ⓘ To use <a href="#">lookups</a> with this channel, select Lookup and define the lookup file in Channel #x Lookup. Do not use Custom if you use lookups with this sensor.</p> <p>ⓘ It is not possible to use the unit Lookup in combination with the Difference mode. You are not able to create the sensor in this case.</p>
Channel #x Custom Unit	<p>This setting is only visible if you select Custom above.</p> <p>Define a unit for the channel value. Enter a string.</p>

Setting	Description
Channel #x Lookup	<p>This setting is only visible if you select <a href="#">Lookup</a> above.</p> <p>Select a <a href="#">lookup</a> file that you want to use with this channel.</p>
Use Data Table Value in Message	<p>This setting is only visible if you select <a href="#">Process data table</a> for the setting <a href="#">Data Processing</a> during sensor creation.</p> <p>Define if the sensor message shows a value from the data table:</p> <ul style="list-style-type: none"> <li>▪ <b>Disable:</b> Do not use a custom sensor message.</li> <li>▪ <b>Enable:</b> Define a custom sensor message with a defined value of the data table. Define the value selection below.</li> </ul> <p><b>i</b> The method of how to determine a value for the sensor message is defined in the setting <a href="#">Select Channel Value by</a> above.</p>
Message Column Number	<p>This setting is only visible if you select <a href="#">Process data table</a> for the setting <a href="#">Data Processing</a> during sensor creation, if you select <a href="#">Column name</a> for the setting <a href="#">Select Channel Value by</a>, and if you select <a href="#">Enable</a> above.</p> <p>Enter the number of a column. The sensor message shows the value in row 0 of this column. Enter an integer.</p>
Message Column Name	<p>This setting is only visible if you select <a href="#">Process data table</a> for the setting <a href="#">Data Processing</a> during sensor creation, if you select <a href="#">Column name</a> for the setting <a href="#">Select Channel Value by</a>, and if you select <a href="#">Enable</a> above.</p> <p>Enter the name of a column. The sensor message shows the value in row 0 of this column. Enter a string.</p> <p><b>i</b> Columns start with index 0.</p>
Message Row Number	<p>This setting is only visible if you select <a href="#">Process data table</a> for the setting <a href="#">Data Processing</a> during sensor creation, if you select <a href="#">Row number</a> for the setting <a href="#">Select Channel Value by</a>, and if you select <a href="#">Enable</a> above.</p> <p>Enter the name of a column. The sensor message shows the value in row 0 of this column. Enter the number of a row. The sensor message shows the value in column 0 of this row. Enter an integer.</p> <p><b>i</b> Rows start with index 0.</p>
Message Key	<p>This setting is only visible if you select <a href="#">Process data table</a> for the setting <a href="#">Data Processing</a> during sensor creation, if you select <a href="#">Key value pair</a> for the setting <a href="#">Select Channel Value by</a>, and if you select <a href="#">Enable</a> above.</p>

Setting	Description
	Enter a key to search for in column 0 of the data table. The sensor message shows the value in column 1 of the row where the key was found. Enter a string.
Message	<p><b>This setting is only visible if you enable</b> <a href="#">Use Data Table Value in Message above</a>.</p> <p>Define the sensor message. Enter a string. Use the placeholder <code>{0}</code> at the position where you want to display the value.</p> <p>Example: <a href="#">The message is {0}</a></p> <p><b>i</b> PRTG does not support the number sign (#) in sensor messages. If a message contains a number sign, PRTG clips the message at this point.</p>
If Message Changes	<p><b>This setting is only visible if you select</b> <a href="#">Process data table for the setting Data Processing during sensor creation</a>.</p> <p>Define what the sensor does when its message changes:</p> <ul style="list-style-type: none"> <li>Ignore (default): Do nothing.</li> <li>Trigger 'change' notification: Send an internal message that indicates a change. <ul style="list-style-type: none"> <li><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</li> </ul> </li> </ul>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the <code>\Logs\sensors</code> subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are <code>Result of Sensor [ID].txt</code>, <code>Result of Sensor [ID].Data.txt</code>, and <code>Result of Sensor [ID].log</code>. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display


**Sensor Display**

Primary Channel **i** Downtime


---


Graph Type **i** 
 Show channels independently (default)
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.


Channel	Description
Affected Rows	The number of rows that were addressed by the query (including <b>SELECT</b> statements if you process data tables)

Channel	Description
Execution Time	The execution time of the entire request (including connection buildup, query execution, transaction handling, disconnection)   This channel is the primary channel by default.
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Query Execution Time	The execution time of the specified query

## SQL Variables

You can use the following variables in the SQL query file to be replaced by an input parameter. This is useful if you have various SQL sensors with queries that differ in only one parameter.

- Microsoft SQL, MySQL, PostgreSQL: @prtg
- Oracle SQL: :prtg
- ADO SQL: ? (question mark)

 @prtg, :prtg, and ? are common SQL query parameters and they are used in a parameterized SQL query. This means that the query and the parameter are forwarded without any changes to the database. This leads to some restrictions on the database side. For example, you cannot use variables as placeholders for table names or as lists in IN operators.

Examples for variables usage:

```
SELECT * FROM Table WHERE name = @prtg
SELECT @prtg FROM Table
```

## More

### ■ KNOWLEDGE BASE

How can I monitor strings from an SQL database and show a sensor status depending on it?

- <https://kb.paessler.com/en/topic/63259>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

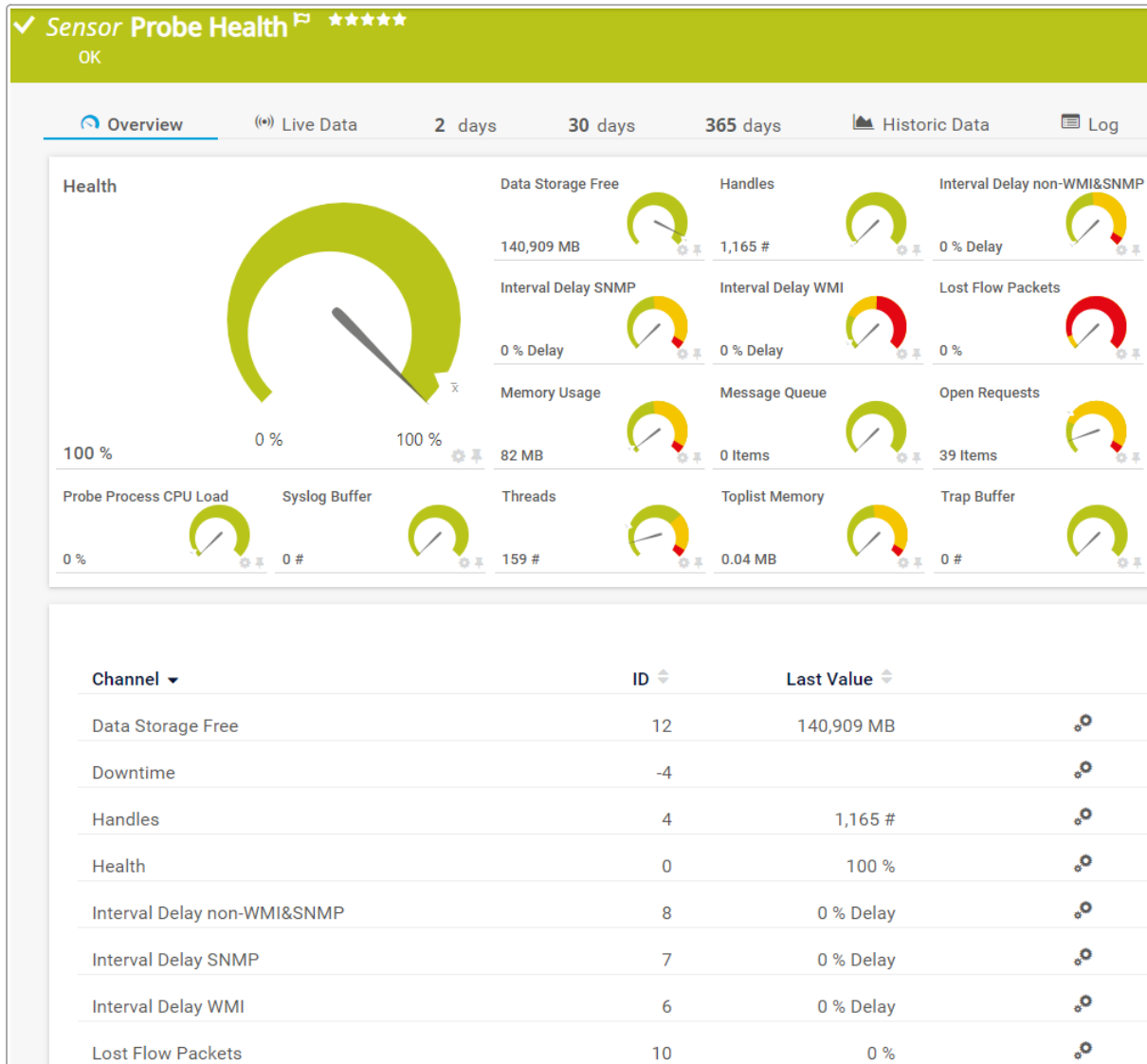
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.143 Probe Health Sensor

The Probe Health sensor monitors internal PRTG parameters. It shows the status of the probe system and checks various parameters of the probe system that can affect the quality of the monitoring results.

**i** This sensor does not support multi-platform probes. Use the [Multi-Platform Probe Health<sup>1347</sup>](#) sensor instead.



Probe Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List<sup>1651</sup>](#).


### Sensor in Other Languages

- Dutch: Probe Status
- French: État de la sonde
- German: Zustand der Probe

- Japanese: プローブ正常性
- Portuguese: Funcionamento da sonda
- Russian: Работоспособность зонда
- Simplified Chinese: 探针健康状况
- Spanish: Salud de sonda

## Remarks

Consider the following [remarks](#)<sup>[1650]</sup> and requirements for this sensor:

Remark	Description
Sensor creation	PRTG automatically creates this sensor. You cannot delete it.
Probe device	You can create this sensor only on a <a href="#">probe device</a> .
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.  PRTG dynamically creates limits for the Data Storage Free <a href="#">channel</a> <sup>[1652]</sup> of this sensor.
Knowledge Base	Knowledge Base: <a href="#">My probe system is running out of disk space. What can I do?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- probehealthsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.



## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Data Storage Free	<p>The free disk space on the probe system</p> <p><b>i</b> PRTG dynamically creates limits for this channel. This means that Enable alerting based on limits is enabled in the <a href="#">channel settings</a> but the limits are empty. Because of this, you cannot save any changes to the channel settings. Enter limits or select Disable limits to save changes to the channel settings.</p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Handles	<p>The counter for the data structures of the operating system. It is responsible for internal resource management. Investigate obviously increasing values that occur repeatedly.</p>
Health	<p>The sum of the probe state as a value between 100% (healthy) and 0% (failing). Investigate frequent or repeated health values below 100%.</p> <p><b>i</b> This channel is the primary channel by default.</p>
Interval Delay non-WMI&SNMP	<p>The interval delay in percent for all sensors that are not of the type SNMP or WMI. If this value is above 0%, try to increase the <a href="#">scanning intervals</a> or distribute your sensors among <a href="#">probes</a>.</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: 100%</li> <li>▪ Upper warning limit: 50%</li> </ul>
Interval Delay SNMP	<p>The interval delay in percent for SNMP sensors. If this value is above 0%, there are probably too many SNMP v3 sensors that are very slow. In this case, try to increase the scanning intervals or distribute the sensors among probes.</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: 100%</li> <li>▪ Upper warning limit: 50%</li> </ul>
Interval Delay WMI	<p>The interval delay in percent for WMI sensors. If this value is above 0%, WMI sensors were not able to check the target device according to their interval. 100% means that WMI sensors are checked with twice their interval on average. For values above 0%, try to increase the scanning intervals or distribute the sensors among probes to keep the number of WMI sensors per probe below 120 (with a 60-second scanning interval) or 600 (with a 300-second scanning interval).</p>

Channel	Description
	<p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: <b>100%</b></li> <li>▪ Upper warning limit: <b>50%</b></li> </ul>
Lost Flow Packets	<p>The number of lost <b>Flow</b> packets. The higher this value, the less flow packages PRTG can handle. Usually, this value should be <b>0%</b>. Investigate increasing values.</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: <b>10%</b></li> <li>▪ Upper warning limit: <b>1%</b></li> </ul>
Memory Usage	<p>The amount of memory that is used by the PRTG probe service as reported by the memory manager. Investigate obviously increasing values that occur repeatedly. If the value is constantly above <b>2 GB</b>, this indicates that PRTG runs at its limits. In this case, you should distribute some sensors among <b>remote probes</b>.</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: <b>3221225472 bytes</b></li> <li>▪ Upper warning limit: <b>1610612736 bytes</b></li> </ul>
Message Queue	<p>The number of monitoring results that have not been processed by the PRTG core server yet. This value should usually stay below <b>1/10</b> of the sensor count.</p>
Open Requests	<p>The number of active monitoring requests. This value should stay below the maximum of <b>500</b> open requests.</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: <b>400</b></li> <li>▪ Upper warning limit: <b>100</b></li> </ul>
Probe Process CPU Load	<p>The CPU load (%) that the probe process causes. Extensive CPU load can lead to false, incomplete, and incorrect monitoring results. This value should usually stay below <b>50%</b>.</p>
Syslog Buffer	<p>The number of buffered syslog packages. Usually, this value should be <b>0</b> (or very low). Investigate increasing values.</p>
Syslog Drop	<p>The number of dropped syslog packages</p>

Channel	Description
Threads	<p>The number of program parts that are running simultaneously. This value can increase with heavy load. Usually, the number should not exceed <a href="#">100</a>.</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: <a href="#">1400</a></li> <li>▪ Upper warning limit: <a href="#">1000</a></li> </ul>
Toplist Memory	<p>The amount of RAM that the <a href="#">Toplists</a> on this probe are using. Stay below <a href="#">1 GB</a> memory usage (depending on the available memory on the probe system). If necessary, reduce the number of Toplists or distribute them among probes.</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: <a href="#">2147483648 bytes</a></li> <li>▪ Upper warning limit: <a href="#">1073741824 bytes</a></li> </ul>
Trap Buffer	<p>The number of buffered SNMP traps. Usually, this value should be <a href="#">0</a> (or very low). Investigate increasing values.</p>

## More

### ■ KNOWLEDGE BASE

My probe system is running out of disk space. What can I do?

- <https://kb.paessler.com/en/topic/64628>

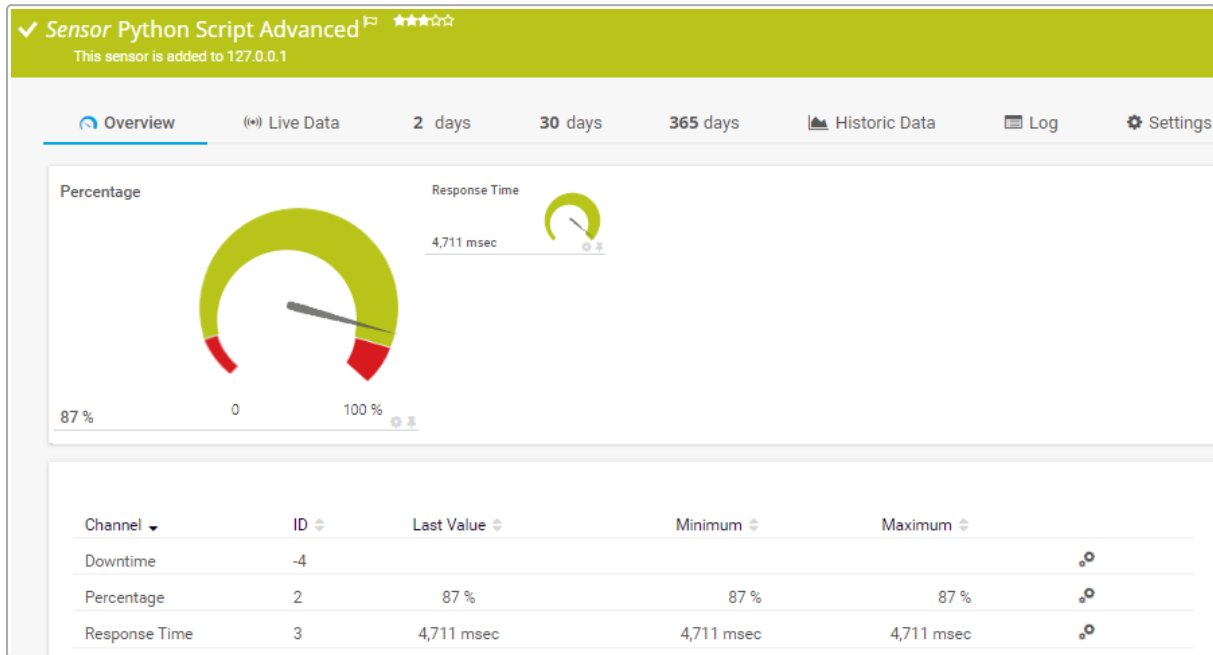
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.144 Python Script Advanced Sensor

The Python Script Advanced sensor executes a Python script on the probe system. This option is available as part of the PRTG API.

- i The return value of this sensor must be valid JavaScript Object Notation (JSON) or Extensible Markup Language (XML).



Python Script Advanced Sensor


- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Python Script Geavanceerd
- French: Script Python avancé
- German: Python-Skript (Erweitert)
- Japanese: Python スクリプト( 上級)
- Portuguese: Script Python (avançado)
- Russian: Скрипт Python (дополнительно)
- Simplified Chinese: Python 脚本高级
- Spanish: Script Python (avanzado)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
File storage	This sensor requires that you store the script file on the probe system. In a cluster, copy the file to every cluster node.
Windows Server	We recommend Windows Server 2016 on the probe system for best performance of this sensor.
Channels	This sensor does not officially support more than <a href="#">50 channels</a> . This sensor does not support channel values greater than 2^62.
Print commands	This sensor does not support print commands in the Python script. They lead to an invalid JSON result.
Exceptions	This sensor does not support exceptions in the Python script.
Python environment	PRTG uses its own Python environment. This is located in the \python subfolder of the PRTG program directory. To avoid issues, we recommend that you do not have other Python environments running on a probe system. We also recommend that you do not uninstall the paesslerag_prtg_sensor_api package.
Timeout	The timeout of the sensor is its <a href="#">scanning interval</a> <sup>1662</sup> minus 1 second. Make sure that your Python script does not run longer than this.
Sensor usage	For best sensor usage, we recommend that the return value is JSON encoded.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">What is the Mutex Name in the EXE/Script sensor settings?</a></li> <li>▪ Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a></li> <li>▪ Knowledge Base: <a href="#">After updating to PRTG 20.1.55, my Python Script Advanced sensors are down</a></li> </ul>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- json
- python
- pythonxml
- script
- xml

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Credentials for Script Sensors

Click  to interrupt the [inheritance](#).

### Credentials for Script Sensors

inherit from

**Placeholder 1 Description** ⓘ

**Placeholder 1** ⓘ

Credentials for Script Sensors

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder1</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.

Setting	Description
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder2</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder3</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder4</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder5</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.



## Sensor Settings

**Sensor Settings**

■ Important: The Python script file must be stored on the parent probe system of the sensor.

Script ▼

Security Context ⓘ  
 Use security context of PRTG probe service (default)  
 Use Windows credentials from parent device

Device Credentials ⓘ  
 Do not transmit device credentials (default)  
 Transmit Windows credentials  
 Transmit Linux credentials  
 Transmit SNMP credentials  
 Transmit all device credentials

Additional Parameters ⓘ

Mutex Name ⓘ

Sensor Settings

Setting	Description
Script	<p>Select a Python script from the list. The sensor executes it with every <a href="#">scanning interval</a> <sup>1662</sup>.</p> <p>This list shows all Python script files that are available in the \Custom Sensors\python subfolder of the <a href="#">PRTG program directory</a> on the probe system. For the files to appear in this list, store the files in this subfolder with the extension <a href="#">.py</a>.</p> <p><span style="color: #c00000;">ⓘ</span> To show the expected values and sensor status, your files must return the expected XML or JSON format to standard output. The values and message must be embedded in the XML or JSON. We recommend JSON-encoded return values.</p> <p><span style="color: #0070c0;">■</span> For more information on how to create custom sensors and for the return format, see section <a href="#">Custom Sensors</a>.</p> <p><span style="color: #c00000;">ⓘ</span> If you use custom sensors on the <a href="#">cluster probe</a>, copy your files to every cluster node.</p> <p><span style="color: #c00000;">ⓘ</span> You cannot change this value after sensor creation.</p>
Security Context	<p>Define the Windows user account that the sensor uses to run the Python interpreter:</p> <ul style="list-style-type: none"> <li>▪ Use security context of PRTG probe service (default): Run the Python script file under the same Windows user account that the probe system runs under. By default, this is the Windows system user account.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Use Windows credentials from parent device: Use the Windows user account from the <a href="#">settings of the parent device</a>.</li> </ul>
Device Credentials	<p>PRTG adds the device credentials to the JSON object that is passed to the script as a command-line parameter. Define if you want to transmit device credentials to the Python script:</p> <ul style="list-style-type: none"> <li>Do not transmit device credentials: Transmit no device credentials to the script.</li> <li>Transmit Windows credentials: Transmit <a href="#">Windows credentials</a> to the script.</li> <li>Transmit Linux credentials: Transmit <a href="#">Linux credentials</a> to the script.</li> <li>Transmit SNMP credentials: Transmit <a href="#">SNMP credentials</a> to the script.</li> <li>Transmit all device credentials: Transmit Windows, Linux, and Simple Network Management Protocol (SNMP) credentials to the script.</li> </ul> <p><b>i</b> The sensor transmits all parameters in plain text.</p>
Additional Parameters	<p>Define additional parameters to add to the JSON object that is passed to the script as a command-line parameter. Enter a string or leave the field empty.</p> <p><b>i</b> The sensor passes a custom JSON object within a dictionary to the script. The dictionary contains the key <a href="#">params</a> that contains all additional parameters in one string.</p> <p>Use the following command to load the dictionary that the sensor sends to the script:</p> <pre>data = json.loads(sys.argv[1])</pre> <p>Use the following command to load the additional parameters:</p> <pre>params = json.loads(data["params"])</pre> <p><b>i</b> If the string contains more than one parameter, you can use the <a href="#">Split()</a> function in Python to split the string.</p> <p><b>i</b> The sensor transmits all parameters in plain text.</p>
Mutex Name	<p>Define a mutual exclusion (mutex) name for the process. Enter a string or leave the field empty.</p> <p><b>i</b> PRTG executes all Python Script Advanced sensors that have the same mutex serially, not simultaneously. This is useful if you use a lot of sensors and want to avoid high resource usage because of simultaneously running processes.</p> <p><b>■</b> See the Knowledge Base: <a href="#">What is the Mutex Name in the EXE/Script sensor settings?</a></p>

## Debug Options

**Debug Options**

**Result Handling** ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].Data.txt and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p> ⓘ You can use Store result to inspect the passed JSON object that contains all parameters. This way, you can find out which key you can access when you script.</p> <p> ☁ This option is not available in PRTG Hosted Monitor.</p> <p> ⓘ PRTG masks transmitted passwords in the log file.</p> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display


**Sensor Display**

**Primary Channel** ⓘ Downtime


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.</p>


Setting	Description
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	<p>The values that the Python script returns in several channels</p> <ul style="list-style-type: none"> <li> For more information about the return value format, see section <a href="#">Custom Sensors</a>.</li> </ul>

## More

 KNOWLEDGE BASE

What is the Mutex Name in the EXE/Script sensor settings?

- <https://kb.paessler.com/en/topic/6673>

Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

After updating to PRTG 20.1.55, my Python Script Advanced sensors are down

- <https://kb.paessler.com/en/topic/87502>

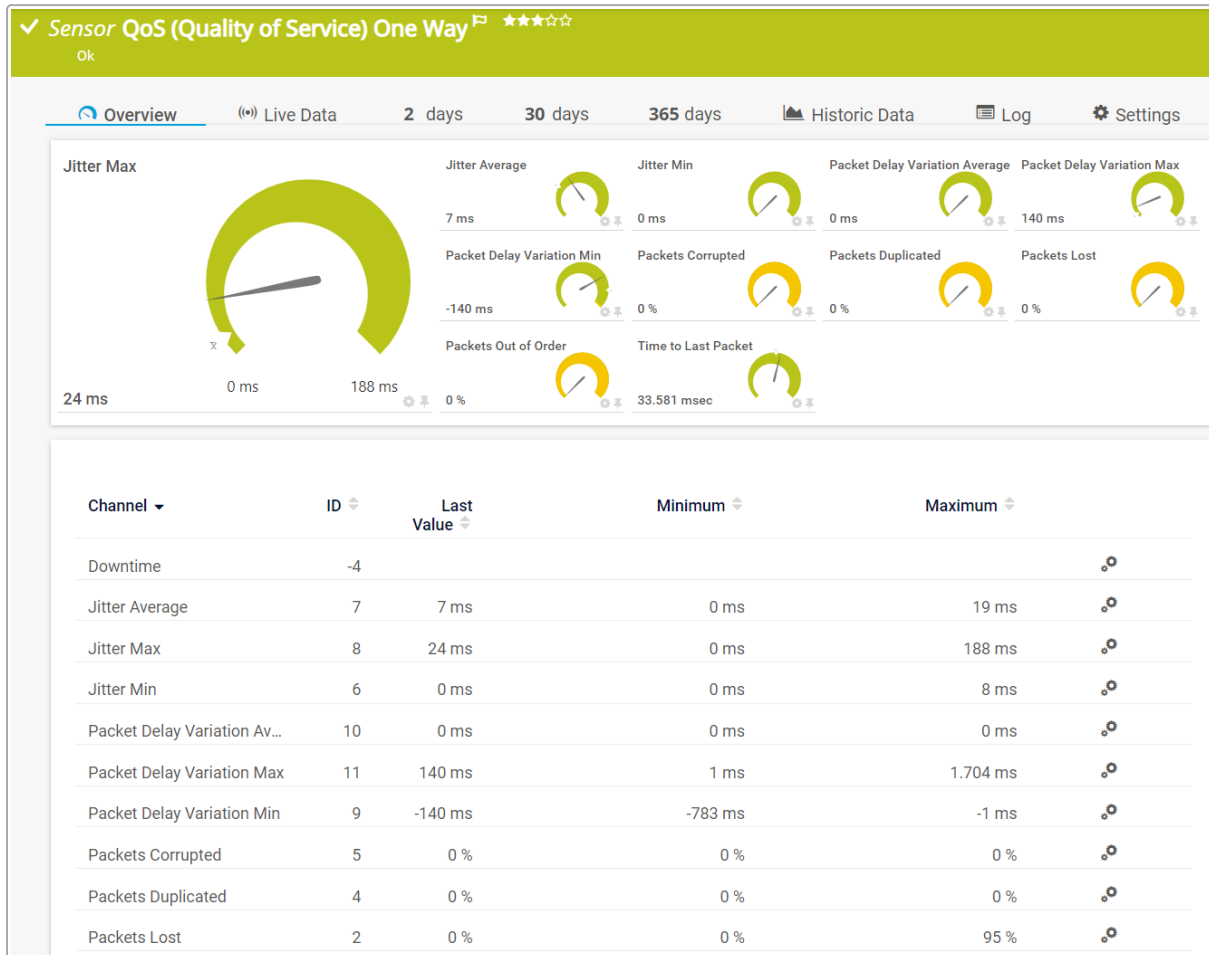
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.145 QoS (Quality of Service) One Way Sensor

The QoS (Quality of Service) One Way sensor monitors parameters regarding the quality of a network connection between two probes.

- ① The sensor sends a series of User Datagram Protocol (UDP) packets from the source probe to a target probe and measures several parameters.



QoS (Quality of Service) One Way Sensor

- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).


### Sensor in Other Languages

- Dutch: QoS (Quality of Service) Eén Richting
- French: QoS (qualité de service) unidirectionnel
- German: QoS (Quality of Service) Unidirektional
- Japanese: 一方向 QoS( Quality of Service)
- Portuguese: Unidirecional QoS (qualidade de serviço)
- Russian: Одностороннее качество обслуживания
- Simplified Chinese: QoS (服务质量) 单向

- Spanish: Unidireccional QoS (calidad de servicio)

## Remarks

Consider the following [remarks](#) <sup>1665</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <b>high</b> performance impact. We recommend that you use no more than <b>200</b> of this sensor on each probe.
Remote probe	This sensor requires that you configure at least one <a href="#">classic remote probe</a> in your PRTG Network Monitor setup, and at least two classic remote probes in PRTG Hosted Monitor.
IPv4	This sensor only supports IPv4.
Sensor creation	You can create this sensor on the probe device of a local probe or a classic remote probe.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  X +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- qossensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Quality of Service Measurement

<b>Quality of Service Measurement</b>	
Timeout (Sec.) ⓘ	60
Target Probe ⓘ	Local Probe ▾
Target Host/IP Address ⓘ	127.0.0.1
Port ⓘ	50000
Number of Packets ⓘ	1000
Packet Size (Bytes) ⓘ	172
Packet Delay (ms) ⓘ	20
<p><small>Use "Windows Policy-based Quality of Service" if you need to apply QoS parameters to the test packets of this sensor (for example, DSCP parameters). These parameters cannot be set from inside PRTG. See <a href="https://technet.microsoft.com/en-us/library/hh831689.aspx">https://technet.microsoft.com/en-us/library/hh831689.aspx</a> and <a href="https://msdn.microsoft.com/library/aa374094.aspx">https://msdn.microsoft.com/library/aa374094.aspx</a> for details.</small></p>	

Quality of Service Measurement

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p> ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
Target Probe	<p>Define the target probe that receives the UDP packets. The dropdown list shows all local probes and remote probes in your setup.</p> <p>If you want to run the sensor on the local probe, select a remote probe as the Target Probe. If no remote probe is available, <a href="#">install and connect a remote probe</a> first.</p> <p>If you want to run the sensor on a remote probe, select either a different remote probe or the local probe as the target. The sensor measures values for the network track between the parent probe and the target probe.</p> <p> ⓘ You must make sure that firewalls or network address translation (NAT) rules allow UDP packets to reach the target probe. The probe automatically opens the Windows firewall on the target system.</p> <p> ☁ In PRTG Hosted Monitor, you can only select a different remote probe as the target probe. QoS measurements for connections to the hosted probe are not possible.</p>
Target Host/IP Address	Define the IP address of the target probe.
Port	Define the <b>source</b> and <b>target</b> port for the UDP packets. Both the source probe and the target probe use this port. Enter an integer. The default port is <b>50000</b> . PRTG supports the port numbers <b>1024-65536</b> for UDP packets.



Setting	Description
	<ul style="list-style-type: none"> <li><span style="color: red;">❗</span> Use a different port for each QoS (Quality of Service) One Way sensor to make sure that PRTG can assign packets correctly.</li> <li><span style="color: red;">❗</span> The port must be available on both the source system and the target system.</li> </ul>
Number of Packets	<p>Define the number of packets that the sensor sends with each scanning interval. Enter an integer. The default value is <b>1000</b>. The minimum value is <b>10</b>. The maximum value is <b>1000</b>.</p> <p><span style="color: blue;">❗</span> We recommend that you use the default value.</p>
Packet Size (Bytes)	<p>Define the size of the packets in bytes that the sensor sends. Enter an integer. The default value is <b>172</b>. The minimum value is <b>172</b>. The maximum value is <b>4500</b>.</p> <p><span style="color: blue;">❗</span> We recommend that you use the default value.</p>
Packet Delay (ms)	<p>Define the time in milliseconds (ms) that the sensor waits between two packets. Enter an integer. The default value is <b>20</b>. The minimum value is <b>10</b>. The maximum value is <b>1000</b>.</p> <p><span style="color: blue;">❗</span> We recommend that you use the default value.</p>

## Sensor Display

**Sensor Display**

Primary Channel ❗ Downtime


---

Graph Type ❗  Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><span style="color: blue;">❗</span> You can set a different primary channel later by clicking <span style="color: blue;">⚙</span> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p>

Setting	Description
	<ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Jitter Average	The average jitter
Jitter Max	The maximum jitter  This channel is the primary channel by default.
Jitter Min	The minimum jitter

Channel	Description
Packet Delay Variation Average	The average packet delay variation
Packet Delay Variation Max	The maximum packet delay variation
Packet Delay Variation Min	The minimum packet delay variation ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper warning limit: 100</li> </ul>
Packets Corrupted	The corrupted packets (%) ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper warning limit: 0</li> </ul>
Packets Duplicated	The duplicated packets (%) ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper warning limit: 0</li> </ul>
Packets Lost	The lost packets (%) ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper warning limit: 1</li> </ul>
Packets Out Of Order	The out of order packets (%) ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper warning limit: 0</li> </ul>
Time to Last Packet	The time to the last packet ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper warning limit: 1</li> </ul>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

■ PAESSLER WEBSITE

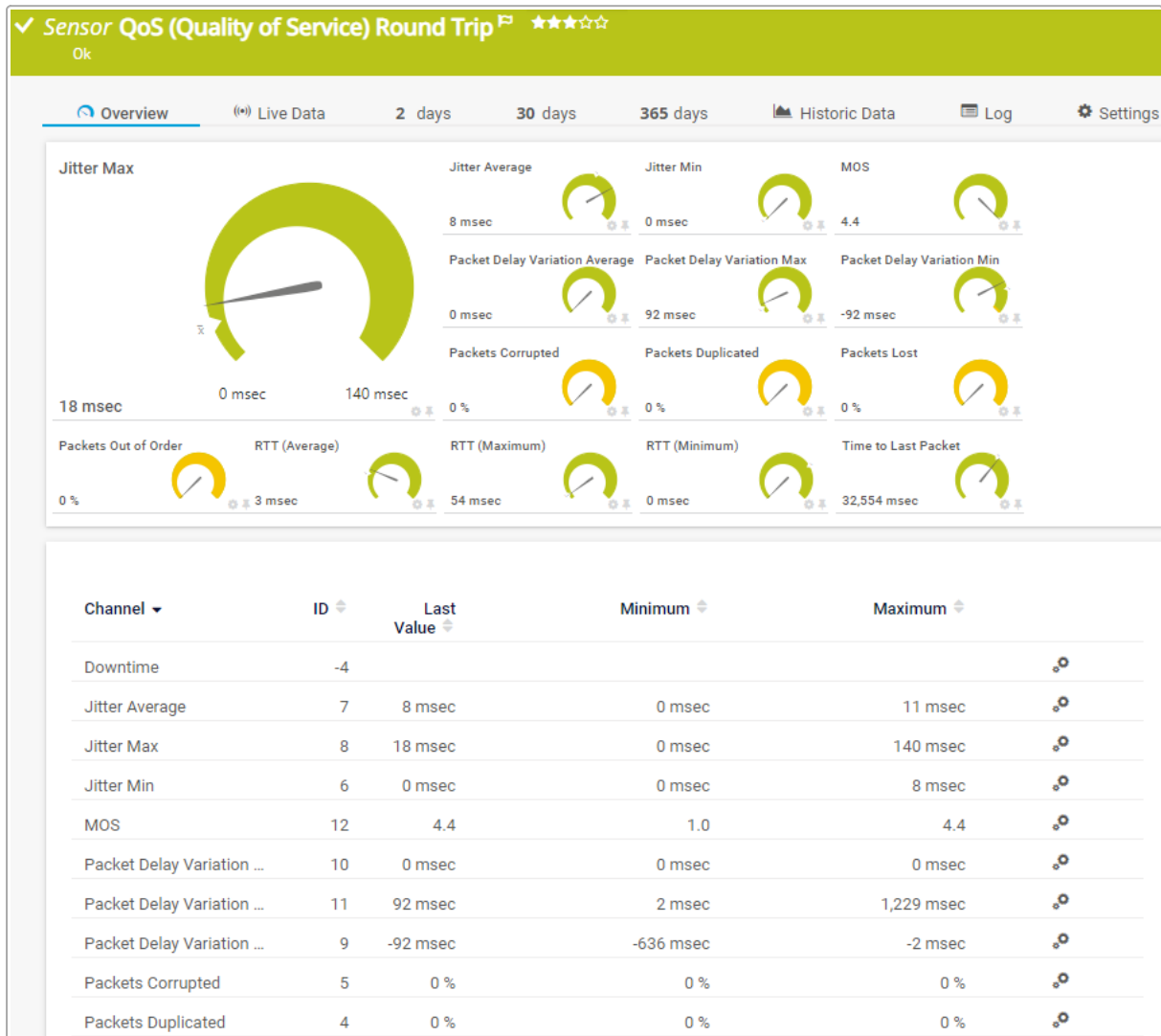
How to connect PRTG through a firewall in 4 steps

- <https://www.paessler.com/support/how-to/firewall>

## 7.8.146 QoS (Quality of Service) Round Trip Sensor

The QoS (Quality of Service) Round Trip sensor monitors parameters regarding the quality of a network connection between two probes.

**i** The sensor sends a series of User Datagram Protocol (UDP) packets from the source probe to a target probe at the end of the connection line. Then, the target probe sends the packets back to the source probe.



QoS (Quality of Service) Round Trip Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1670</sup>.


### Sensor in Other Languages

- Dutch: QoS (Quality of Service) Heen en weer
- French: QoS (qualité de service) aller-retour
- German: QoS (Quality of Service) Round Trip
- Japanese: ラウンドトリップ QoS( Quality of Service)

- Portuguese: Ida e volta QoS (qualidade de serviço)
- Russian: Цикл тестирования качества обслуживания
- Simplified Chinese: QoS (服务质量) 往返
- Spanish: Ida y vuelta QoS (calidad de servicio)

## Remarks

Consider the following [remarks](#) <sup>1672</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Remote probe	This sensor requires that you configure at least one <a href="#">classic remote probe</a> in your PRTG Network Monitor setup and at least two classic remote probes in PRTG Hosted Monitor, or you must set up the <a href="#">PRTG QoS Reflector</a> tool on the target system at the endpoint of the connection that you want to monitor.
Cluster probe	This sensor does not support cluster probes. You can only set it up on local probes or remote probes.
IPv4	This sensor only supports IPv4.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">How can I monitor QoS round trips without using remote probes?</a></li> <li>▪ Knowledge Base: <a href="#">How does PRTG calculate the MOS score for QoS sensors?</a></li> <li>▪ Knowledge Base: <a href="#">What connection settings are necessary for the QoS (Quality of Service) Round Trip sensor?</a></li> </ul>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- qossensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Quality of Service Measurement

### Quality of Service Measurement

**Timeout (Sec.)** ⓘ 60

---

**QoS Target** ⓘ  Probe (default)  
 Custom target

**Target Probe** ⓘ Local Probe ▼

---

**Target Host/IP Address** ⓘ 127.0.0.1

---

**Port** ⓘ 50000

---

**Number of Packets** ⓘ 1000

---

**Packet Size (Bytes)** ⓘ 172

---






**Packet Delay (ms)** ⓘ 20

---

Use "Windows Policy-based Quality of Service" if you need to apply QoS parameters to the test packets of this sensor (for example, DSCP parameters). These parameters cannot be set from inside PRTG. See <https://technet.microsoft.com/en-us/library/hh831689.aspx> and <https://msdn.microsoft.com/library/aa374094.aspx> for details.

Quality of Service Measurement

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

Setting	Description
QoS Target	<p>Define the type of target that receives the UDP packets:</p> <ul style="list-style-type: none"> <li>▪ Probe (default): Use a probe as the connection endpoint.</li> <li>▪ Custom target: Use the <a href="#">PRTG QoS Reflector</a> as the connection endpoint.</li> </ul> <p> For more information about the QoS Reflector, see the Knowledge Base: <a href="#">How can I monitor QoS round trips without using remote probes?</a></p>
Target Probe	<p><a href="#">This setting is only visible if you select Probe (default) above.</a></p> <p>Define the target probe that receives the UDP packets. The dropdown list shows all local probes and remote probes in your setup.</p> <p>If you want to run the sensor on the local probe, select a remote probe as the Target Probe. If no remote probe is available, <a href="#">install and connect a remote probe</a> first. Alternatively, you can use the <a href="#">PRTG QoS Reflector</a>.</p> <p>If you want to run the sensor on a remote probe, select either a different remote probe or the local probe as the target. The sensor measures values for the network track between the parent probe and the target probe.</p> <p> You must make sure that firewalls or network address translation (NAT) rules allow UDP packets to reach the target probe. The probe automatically opens the Windows firewall on the target system. For more information, see the Knowledge Base: <a href="#">What connection settings are necessary for the QoS (Quality of Service) Round Trip sensor?</a></p> <p> In PRTG Hosted Monitor, you can only select a different remote probe as the target probe. QoS measurements for connections to the hosted probe are not possible.</p>
Target Host/IP Address	<p>Define the IP address of the QoS target:</p> <ul style="list-style-type: none"> <li>▪ If you use the <a href="#">QoS Reflector</a>, enter the address of the system on which the reflector script runs.</li> <li>▪ If you use a probe, enter the address of the probe to which the source probe connects.</li> </ul>
Port	<p>Define the <a href="#">source</a> and <a href="#">target</a> port for the UDP packets. Both the source probe and the target probe use this port. Enter an integer. The default port is <a href="#">50000</a>. PRTG supports the port numbers <a href="#">1024-65536</a> for UDP packets.</p> <p> Use a different port for each QoS (Quality of Service) Round Trip sensor to make sure that PRTG can assign packets correctly.</p> <p> The port must be available on both the source system and the target system.</p>



Setting	Description
Number of Packets	<p>Define the number of packets that the sensor sends with each scanning interval. Enter an integer. The default value is <b>1000</b>. The minimum value is <b>10</b>. The maximum value is <b>1000</b>.</p> <p><b>i</b> We recommend that you use the default value.</p>
Packet Size (Bytes)	<p>Define the size of the packets in bytes that the sensor sends. Enter an integer. The default value is <b>172</b>. The minimum value is <b>172</b>. The maximum value is <b>4500</b>.</p> <p><b>i</b> We recommend that you use the default value.</p>
Packet Delay (ms)	<p>Define the time in milliseconds (ms) that the sensor waits between two packets. Enter an integer. The default value is <b>20</b>. The minimum value is <b>10</b>. The maximum value is <b>1000</b>.</p> <p><b>i</b> We recommend that you use the default value.</p>

## Sensor Display


**Sensor Display**

Primary Channel **⌵** Downtime


Graph Type **⌵**
 Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>


Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Jitter Average	The average jitter
Jitter Max	The maximum jitter  This channel is the primary channel by default.
Jitter Min	The minimum jitter
MOS	The MOS

Channel	Description
Packet Delay Variation Average	The average packet delay variation
Packet Delay Variation Max	The maximum packet delay variation
Packet Delay Variation Min	The minimum packet delay variation ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper warning limit: 100</li> </ul>
Packets Corrupted	The corrupted packets (%) ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper warning limit: 0</li> </ul>
Packets Duplicated	The duplicated packets (%) ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper warning limit: 0</li> </ul>
Packets Lost	The lost packets (%) ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper warning limit: 1</li> </ul>
Packets Out Of Order	The out of order packets (%) ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper warning limit: 0</li> </ul>
RTT (Average)	The average RTT
RTT (Maximum)	The maximum RTT
RTT (Minimum)	The minimum RTT

## More

### ■ KNOWLEDGE BASE

How can I monitor QoS round trips without using remote probes?

- <https://kb.paessler.com/en/topic/61176>

How does PRTG calculate the MOS score for QoS sensors?

- <https://kb.paessler.com/en/topic/59491>

What connection settings are necessary for the QoS (Quality of Service) Round Trip sensor?

- <https://kb.paessler.com/en/topic/65410>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## ■ PAESSLER WEBSITE

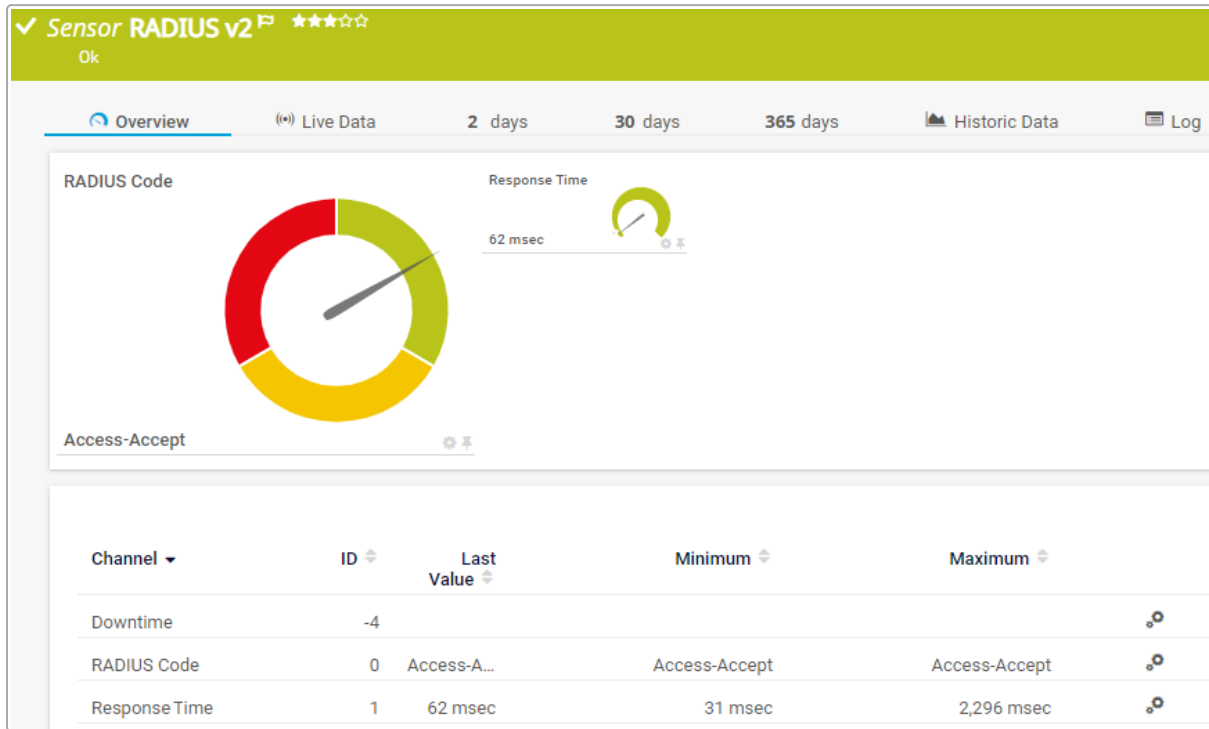
How to connect PRTG through a firewall in 4 steps

- <https://www.paessler.com/support/how-to/firewall>

## 7.8.147 RADIUS v2 Sensor

The RADIUS v2 sensor monitors a Remote Authentication Dial-In User Service (RADIUS) server according to [RFC 2865](#).

- ❶ The sensor tries to authenticate itself against the server. If authentication fails, the sensor shows the Down [status](#).



RADIUS v2 Sensor



- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1683]</sup>.

### Sensor in Other Languages

- Dutch: RADIUS v2
- French: RADIUS v2
- German: RADIUS v2
- Japanese: RADIUS V2
- Portuguese: RADIUS v2
- Russian: RADIUS v2
- Simplified Chinese: RADIUS v2
- Spanish: RADIUS v2

### Remarks

Consider the following [remarks](#)<sup>[1679]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Plain text authentication	This sensor only supports plain text authentication (Password Authentication Protocol (PAP)).
IPv4	This sensor only supports IPv4.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  X +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- radiussensor


 For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## RADIUS Specific

### RADIUS Specific

Timeout (Sec.) ⓘ	60
User Name ⓘ	johnqpublic
Password ⓘ	.....
Shared Secret ⓘ	.....
Port ⓘ	1812
NAS Identification ⓘ	<input checked="" type="radio"/> Use NAS IP address (default) <input type="radio"/> Use NAS identifier ⓘ
NAS IP Address ⓘ	192.0.2.0
Result Handling ⓘ	<input checked="" type="radio"/> Discard result (default) <input type="radio"/> Store result

RADIUS Specific

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
User Name	<p>Enter the user name for the authentication against the RADIUS server. Enter a string.</p>
Password	<p>Enter the password for the authentication between the client (the probe system) and the RADIUS server. Enter a string.</p>
Shared Secret	<p>Enter the shared secret for the authentication between the authenticator (the probe system) and the RADIUS server. Enter a string.</p>
Port	<p>Enter the number of the port for the connection to the RADIUS server. The default value is <b>1812</b>. Enter an integer.</p>
NAS Identification	<p>Define how to identify the network access server (NAS):</p> <ul style="list-style-type: none"> <li>▪ Use NAS IP address (default): Enter the NAS IP Address for identification below.</li> <li>▪ Use NAS identifier: Enter the NAS Identifier below.</li> </ul>
NAS IP Address	<p><b>This setting is only visible if you select Use NAS IP address (default) above.</b></p> <p>Enter a valid IP address for the NAS that originates the access request.</p>
NAS Identifier	<p><b>This setting is only visible if you select Use NAS identifier above.</b></p> <p>Enter an identifier for the NAS that originates the access request.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>



## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
RADIUS Code	<p>The RADIUS code</p> <ul style="list-style-type: none"> <li>▪ Up status: Accept-Accept</li> <li>▪ Warning status: Access-Challenge</li> <li>▪ Down status: Access-Reject</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Response Time	The response time

## More

### ■ KNOWLEDGE BASE

Which .NET version does PRTG require?

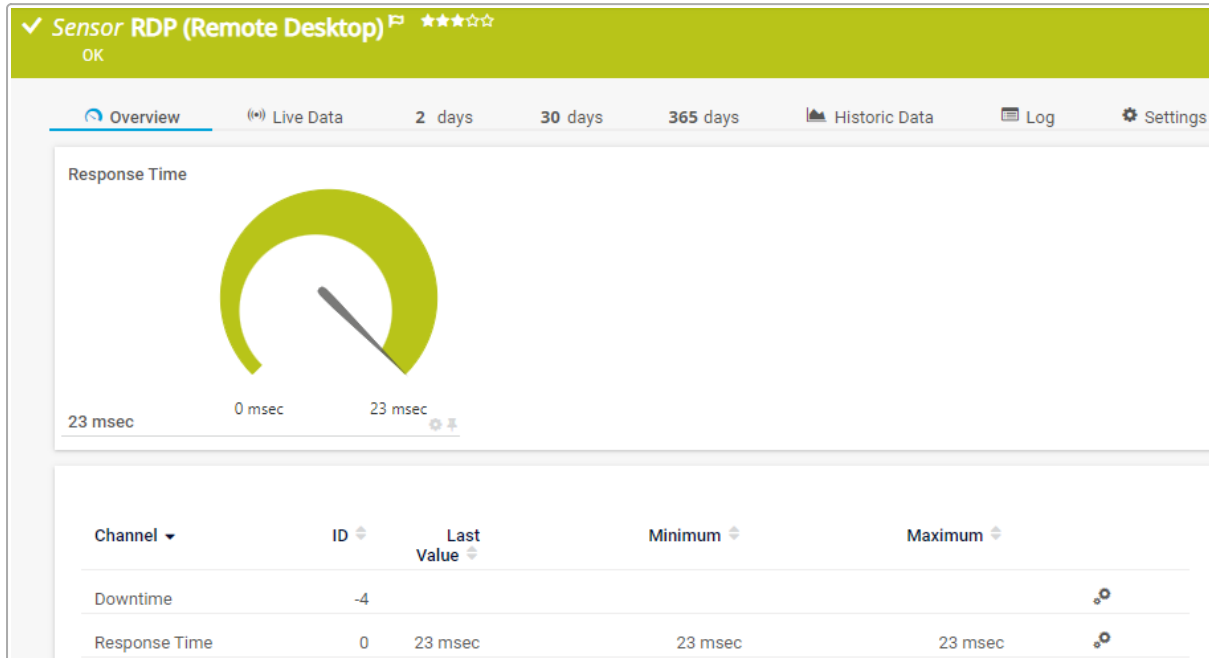
- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.148 RDP (Remote Desktop) Sensor

The RDP (Remote Desktop) sensor monitors remote desktop services such as Remote Desktop Protocol (RDP) or Terminal Services Client.



RDP (Remote Desktop) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: RDP (Remote Desktop)
- French: RDP (Bureau à distance)
- German: RDP (Remotedesktop)
- Japanese: RDP( リモートデスクトップ)
- Portuguese: RDP (desktop remoto)
- Russian: RDP (удаленный рабочий стол)
- Simplified Chinese: RDP (远程桌面)
- Spanish: RDP (escritorio remoto)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- rdpensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Specific

#### Sensor Specific


**Timeout (Sec.)** ⓘ 60

---

**Port** ⓘ 3389

Sensor Specific

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p> ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
Port	<p>Enter the number of the port to which this sensor connects. Enter an integer. The default value is <b>3389</b>.</p>

Setting	Description
	 We recommend that you use the default value.




## Sensor Display

**Sensor Display**


Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Response Time	The response time ⓘ This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Does PRTG impair my Citrix environment?

- <https://kb.paessler.com/en/topic/61880>

## 7.8.149 Redfish Power Supply Sensor

The Redfish Power Supply sensor monitors the power supply of a Redfish Scalable Platforms Management API (Redfish)-capable server.



Redfish Power Supply Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Redfish Voeding
- French: Redfish alimentation
- German: Redfish Stromversorgung
- Japanese: Redfish 電源
- Portuguese: Fonte de alimentação Redfish
- Russian: Блок питания Redfish
- Simplified Chinese: Redfish 电源
- Spanish: Suministro de alimentación Redfish

## Remarks

Consider the following [remarks](#)<sup>1690</sup> and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for Redfish in settings that are higher in the <a href="#">object hierarchy</a> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Redfish support	Supporters of the Redfish standard include <a href="#">Dell</a> , <a href="#">Eaton</a> , <a href="#">Emerson</a> , <a href="#">Fujitsu</a> , <a href="#">HPE</a> , <a href="#">Intel</a> , <a href="#">Lenovo</a> , <a href="#">NetApp</a> , <a href="#">Supermicro</a> , and <a href="#">VMware</a> .
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- powersupply
- redfish

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.



## Redfish Specific

**Redfish Specific**

**Name** ⓘ *Example*

**Model** ⓘ *123456-A01*

**Manufacturer** ⓘ *ManufacturerName*

**Serial Number** ⓘ *12345ABCDE*

Redfish Specific

ⓘ The information in the Redfish Specific settings reflects the status of the system at the time of sensor creation. If any setting changes after creation, the Redfish Specific settings do not reflect the change. Add the sensor anew to update the displayed settings.

Setting	Description
Name	The name of the power supply that this sensor monitors.
Model	The model of the power supply that this sensor monitors.
Manufacturer	The manufacturer of the power supply that this sensor monitors.
Serial Number	The serial number of the power supply that this sensor monitors.

## Sensor Display


**Sensor Display**

**Primary Channel** ⓘ Downtime

**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>



Setting	Description
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


### Debug Options

**Result Handling** 
  
 Discard result (default)
  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>



## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Input Voltage	The input voltage
Input Watts	The input watts
Output Load	The output load  This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper error limit: 99%</li> <li>▪ Upper warning limit: 90%</li> </ul>
Output Watts	The output watts
Power Efficiency	The power efficiency
Power Supply Status	The power supply status <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Critical</li> <li>▪ Unknown status: Offline / Absent</li> </ul>  This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

I want to know which of my systems support the PRTG Redfish sensors. Can you help me?

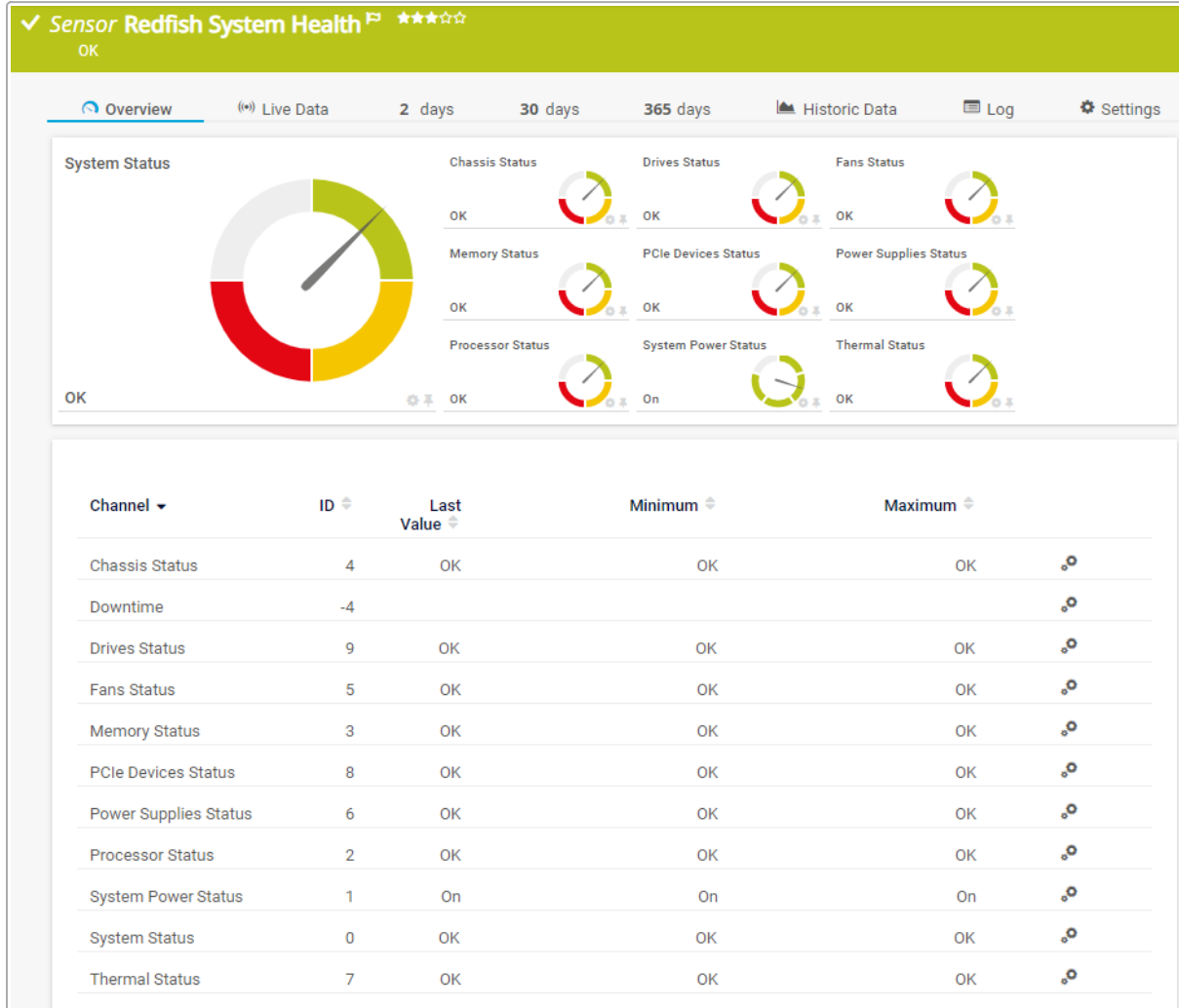
- <https://kb.paessler.com/en/topic/89858>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.150 Redfish System Health Sensor

The Redfish System Health sensor monitors the system health of a Redfish Scalable Platforms Management API (Redfish)-capable server.



Redfish System Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Redfish Systeemstatus
- French: Redfish état du système
- German: Redfish Systemzustand
- Japanese: Redfish システム正常性
- Portuguese: Saúde do sistema Redfish
- Russian: Работоспособность системы Redfish
- Simplified Chinese: Redfish 系统健康状况

- Spanish: Salud del sistema Redfish

## Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for Redfish in settings that are higher in the <a href="#">object hierarchy</a> .
Read permissions	This sensor requires at least read permissions for the target system. Without sufficient permissions to a subsystem, the sensor will show the Down status.
Supermicro	If you want to monitor Supermicro, then this sensor requires full administrator access.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Redfish support	Supporters of the Redfish standard include <a href="#">Dell</a> , <a href="#">Eaton</a> , <a href="#">Emerson</a> , <a href="#">Fujitsu</a> , <a href="#">HPE</a> , <a href="#">Intel</a> , <a href="#">Lenovo</a> , <a href="#">NetApp</a> , <a href="#">Supermicro</a> , and <a href="#">VMware</a> .
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ

**Priority** ⓘ

Example Name

---

exampletag ✕ +

---

★★★★☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- redfish

- restsensor

For more information about basic sensor settings, see section [Sensor Settings](#).

### Redfish Specific

**Redfish Specific**

**Name** ⓘ *Example*

**Model** ⓘ *123456-A01*

**Manufacturer** ⓘ *ManufacturerName*

**Serial Number** ⓘ *12345ABCDE*

**Asset Tag** ⓘ

Redfish Specific

**i** The information in the Redfish Specific settings reflects the status of the system at the time of sensor creation. If any setting changes after creation, the Redfish Specific settings do not reflect the change. Add the sensor anew to update the displayed settings.

Setting	Description
Name	The name of the system that this sensor monitors.
Model	The model of the system that this sensor monitors.
Manufacturer	The manufacturer of the system that this sensor monitors.
Serial Number	The serial number of the system that this sensor monitors.
Asset Tag	The asset tag of the system that this sensor monitors.

### Sensor Display

**Sensor Display**




**Primary Channel** ⓘ Downtime

**Graph Type** ⓘ

Show channels independently (default)


Stack channels on top of each other

Sensor Display


Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><a href="#">This setting is only visible if you select</a> Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**

**Result Handling** 
 Discard result (default)  
 Store result


Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>



Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Chassis Status	<p>The chassis status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Critical</li> <li>▪ Unknown status: Offline / Absent</li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Drives Status	<p>The drives status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Critical</li> <li>▪ Unknown status: Offline / Absent</li> </ul>
Fans Status	<p>The fans status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> </ul>

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Down status: Critical</li> <li>▪ Unknown status: Offline / Absent</li> </ul>
Memory Status	<p>The memory status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Critical</li> <li>▪ Unknown status: Offline / Absent</li> </ul>
PCIe Devices Status	<p>The PCIe drives status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Critical</li> <li>▪ Unknown status: Offline / Absent</li> </ul>
Power Supplies Status	<p>The power supplies status</p> <ul style="list-style-type: none"> <li>▪ Up status: Off, On, Powering Off, Powering On</li> <li>▪ Unknown status: Unknown</li> </ul>
Processor Status	<p>The processor status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Critical</li> <li>▪ Unknown status: Offline / Absent</li> </ul>
System Power Status	<p>The system power status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Critical</li> <li>▪ Unknown status: Offline / Absent</li> </ul>
System Status	<p>The system status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> </ul>

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Down status: Critical</li> <li>▪ Unknown status: Offline / Absent</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Thermal Status	<p>The thermal status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Critical</li> <li>▪ Unknown status: Offline / Absent</li> </ul>

## More

### ■ KNOWLEDGE BASE

I want to know which of my systems support the PRTG Redfish sensors. Can you help me?

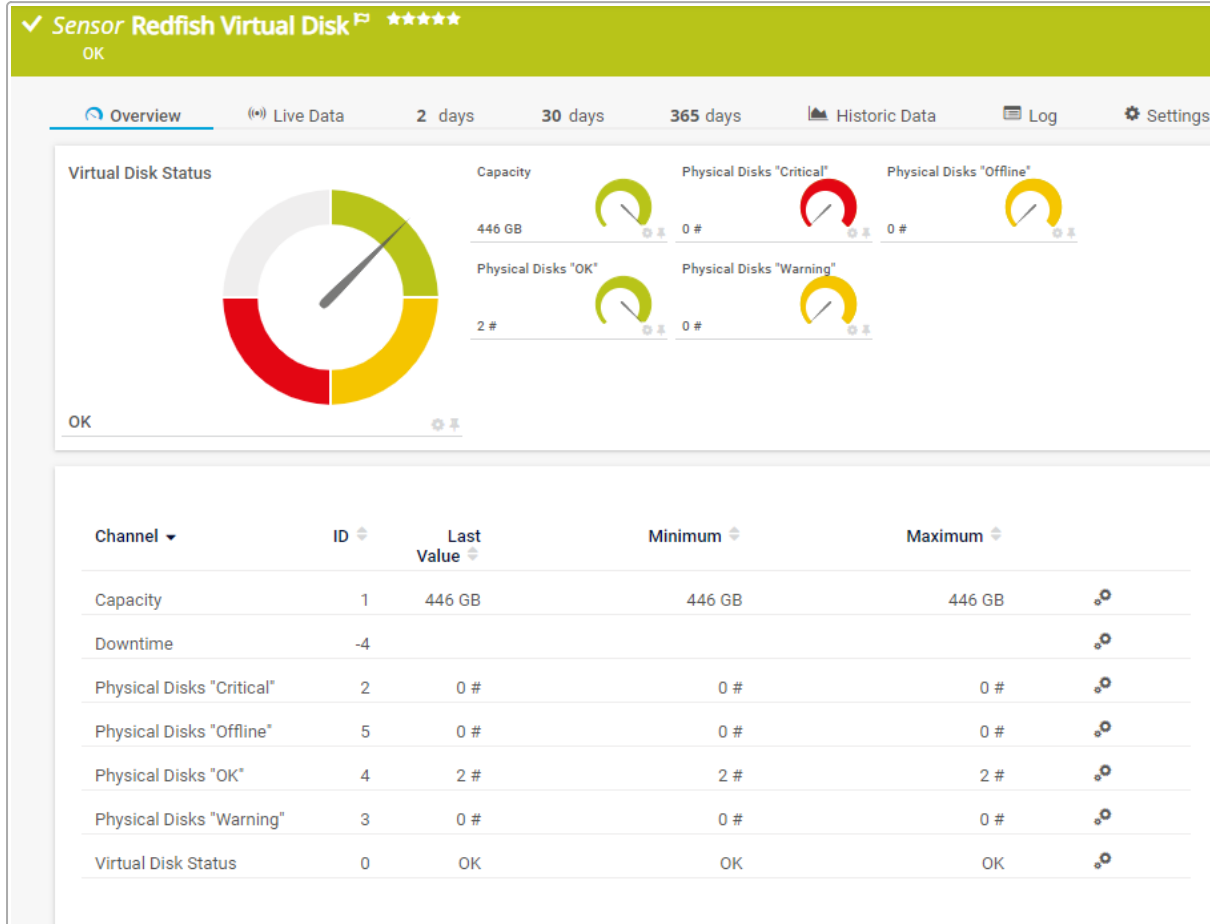
- <https://kb.paessler.com/en/topic/89858>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.151 Redfish Virtual Disk Sensor

The Redfish Virtual Disk sensor monitors the virtual disk of a Redfish Scalable Platforms Management API (Redfish)-capable server.



Redfish Virtual Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) [1702].

### Sensor in Other Languages

- Dutch: Redfish Virtuele Schijf
- French: Redfish disque virtuel
- German: Redfish Virtueller Datenträger
- Japanese: Redfish 仮想ディスク
- Portuguese: Disco físico Redfish
- Russian: Виртуальный диск Redfish
- Simplified Chinese: Redfish 虚拟磁盘
- Spanish: Disco virtual Redfish

## Remarks

Consider the following [remarks](#)<sup>[1703]</sup> and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for Redfish in settings that are higher in the <a href="#">object hierarchy</a> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Redfish support	Supporters of the Redfish standard include <a href="#">Dell</a> , <a href="#">Eaton</a> , <a href="#">Emerson</a> , <a href="#">Fujitsu</a> , <a href="#">HPE</a> , <a href="#">Intel</a> , <a href="#">Lenovo</a> , <a href="#">NetApp</a> , <a href="#">Supermicro</a> , and <a href="#">VMware</a> .
Multi-platform probe	You can add this sensor to a multi-platform probe.
Knowledge Base	Knowledge Base: <a href="#">I want to know which of my systems support the PRTG Redfish sensors. Can you help me?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

Example Name

---

**Tags** ⓘ

exampletag ✕ +

---

**Priority** ⓘ

★★★★☆☆

Example Name

---

exampletag ✕ +

---

★★★★☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- logicaldisk
- redfish
- virtualdisk
- virtualvolume

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Redfish Specific

**Redfish Specific**

**Virtual Disk Name** ⓘ *Virtual Disk 1*

**Capacity** ⓘ *837.750 GB*

**RAID Level** ⓘ *RAID1*

**Physical Disks Count** ⓘ *2*

**System Name** ⓘ *Example (Local Storage Controller)*

Redfish Specific

ⓘ The information in the Redfish Specific settings reflects the status of the system at the time of sensor creation. If any setting changes after creation, the Redfish Specific settings do not reflect the change. Add the sensor anew to update the displayed settings.

Setting	Description
Virtual Disk Name	The name of the virtual disk that this sensor monitors.
Capacity	The capacity of the virtual disk that this sensor monitors.
RAID Level	The RAID level of the virtual disk that this sensor monitors.
Physical Disks Count	The number of physical disks connected to the virtual disk that this sensor monitors.
System Name	The name of the system that the virtual disk belongs to.

## Sensor Display

**Sensor Display**




**Primary Channel** ⓘ *Downtime*

**Graph Type** ⓘ

Show channels independently (default)


Stack channels on top of each other

Sensor Display


Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><a href="#">This setting is only visible if you select</a> Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**


**Result Handling** 
 Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.


 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Capacity	The capacity of the virtual disk
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Physical Disks "Critical"	<p>The number of physical disks in the critical status</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper error limit: 0</li> </ul>
Physical Disks "Offline"	<p>The number of physical disks in the offline status</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper error limit: 0</li> </ul>
Physical Disks "OK"	The number of physical disks in the OK status
Physical Disks "Warning"	<p>The number of physical disks in the warning status</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper error limit: 0</li> </ul>



Channel	Description
Virtual Disk Status	<p>The virtual disk status</p> <ul style="list-style-type: none"><li>▪ Up status: OK</li><li>▪ Warning status: Warning</li><li>▪ Down status: Critical</li><li>▪ Unknown status: Offline / Absent</li></ul> <p> This channel is the primary channel by default.</p>

## More

### KNOWLEDGE BASE

I want to know which of my systems support the PRTG Redfish sensors. Can you help me?

- <https://kb.paessler.com/en/topic/89858>

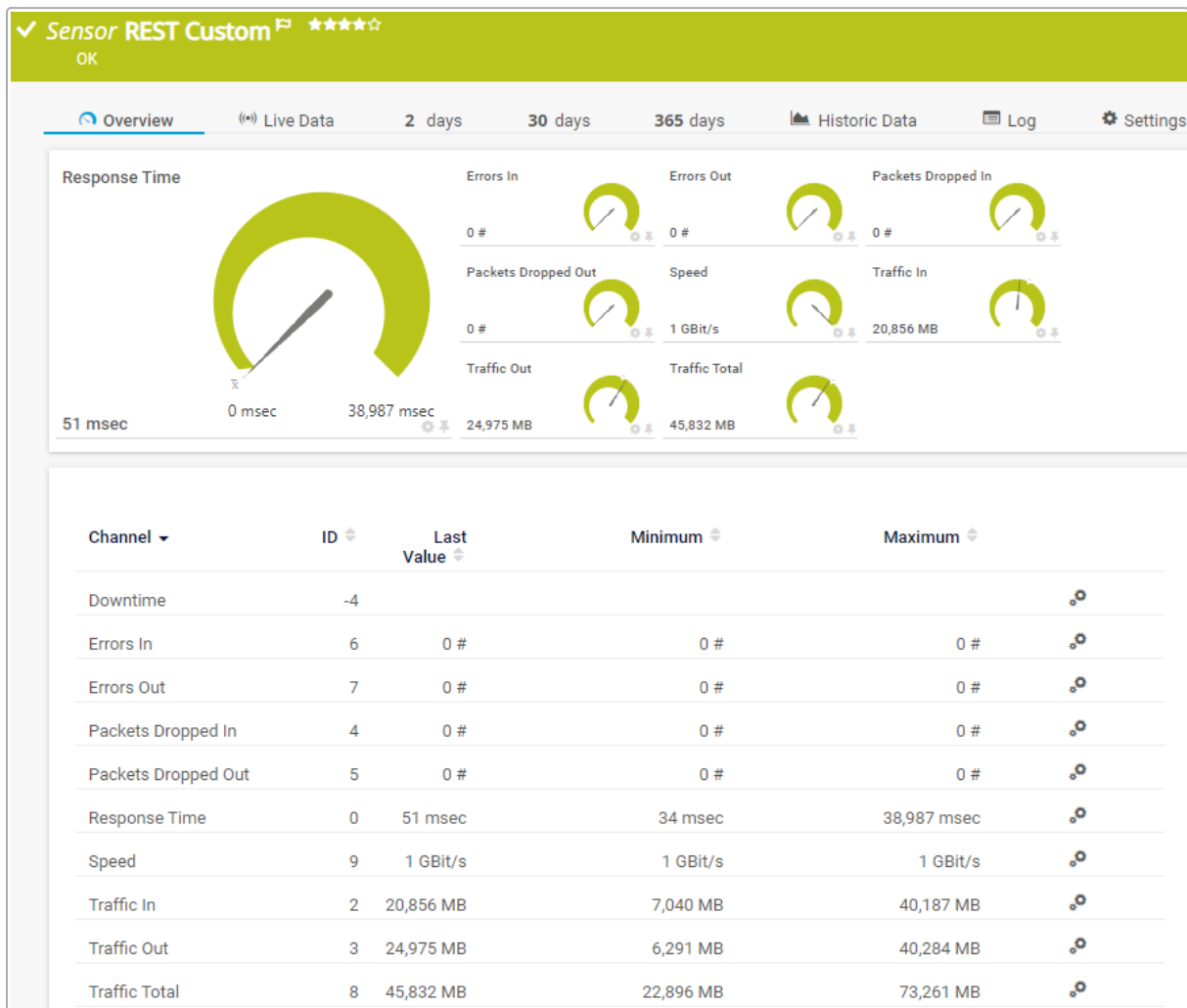
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.152 REST Custom Sensor

The REST Custom sensor queries a Representational State Transfer (REST) application programming interface (API) endpoint and maps the JavaScript Object Notation (JSON) or Extensible Markup Language (XML) result to sensor values.

- i** The mapping rule must be available as a REST configuration file in JSON template (\*.template) format according to the PRTG API definition for custom sensors.



REST Custom Sensor

- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1726]</sup>.

### Sensor in Other Languages

- Dutch: REST Aangepast
- French: REST personnalisé
- German: REST (Benutzerdef.)
- Japanese: REST カスタム
- Portuguese: REST (customizado)

- Russian: Специальные настройки REST
- Simplified Chinese: REST 自定义
- Spanish: REST (personalizado)

## Remarks

Consider the following [remarks](#)<sup>1709</sup> and requirements for this sensor:

Remark	Description
File storage	The sensor requires that you store the REST configuration file that contains the mapping rules on the probe system. In a cluster, copy the file to every cluster node.
Channels	This sensor does not officially support more than <a href="#">50 channels</a> . If there are more than 50 channel mappings in the REST configuration file, the sensor shows an error.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
Cluster	In a cluster, status changes triggered by limits only work on the master node.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- restcustomsensor
- restsensor

For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## REST Specific

**REST Specific**

**Request Method** <sup>i</sup>  GET (default)  
 POST

**Request Protocol** <sup>i</sup>  HTTP (default)  
 HTTPS

**Authentication Method** <sup>i</sup>  No authentication (default)  
 Basic authentication  
 Basic authentication with Windows credentials from parent device  
 Token

**HTTP Headers** <sup>i</sup>  Do not send custom HTTP headers  
 Send custom HTTP headers

**Timeout (Sec.)** <sup>i</sup>

**REST Query** <sup>i</sup>

**REST Configuration** <sup>i</sup>

REST Specific

Setting	Description
Request Method	<p>Select an HTTP request method to determine how the sensor requests the REST API:</p> <ul style="list-style-type: none"> <li>▪ GET (default): Use the GET method to request the REST API.</li> <li>▪ POST: Use the POST method to request the REST API.</li> </ul> <p><sup>i</sup> If you use the POST method, use the content type, for example <a href="#">application/x-www-form-urlencoded</a>, as HTTP header. In section HTTP Headers, select Send custom HTTP headers and enter the content type in the Custom HTTP Headers field.</p>
Postdata	<p><a href="#">This setting is only visible if you select POST above.</a></p> <p>Enter the data part for the POST request.</p> <p><sup>i</sup> If you use the POST method, use the content type, for example <a href="#">application/x-www-form-urlencoded</a>, as HTTP header. In section HTTP Headers, select Send custom HTTP headers and enter the content type in the Custom HTTP Headers field.</p>
Request Protocol	<p>Define the security protocol of the HTTP request:</p> <ul style="list-style-type: none"> <li>▪ HTTP (default): Send the REST query via HTTP (not secure).</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ HTTPS: Send the REST query via secure HTTPS.</li> </ul>
Certificate Acceptance	<p><a href="#">This setting is only visible if you select HTTPS above.</a></p> <p>Select the kind of certificates that you want the sensor to accept for the connection:</p> <ul style="list-style-type: none"> <li>▪ Accept trusted certificates only (default): Accept only trusted certificates issued by a certificate authority (CA).</li> <li>▪ Accept all certificates: Accept all certificates, including self-signed certificates.</li> </ul>
Authentication Method	<p>Select the authentication method for access to the REST API:</p> <ul style="list-style-type: none"> <li>▪ No authentication (default): Do not use any authentication for the request.</li> <li>▪ Basic authentication: Use a user name and password for authentication.</li> <li>▪ Basic authentication with Windows credentials from parent device: Use the Windows credentials from the parent device.  <input type="checkbox"/> For more information, see section <a href="#">Inheritance of Settings</a>.</li> <li>▪ Token: Use a <a href="#">JSON Web Token (JWT)</a> or <a href="#">OAuth2 Bearer Token</a> for authentication.</li> </ul>
User Name	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter a user name for the REST API. Enter a string.</p>
Password	<p><a href="#">This setting is only visible if you select Basic authentication above.</a></p> <p>Enter a password for the REST API. Enter a string.</p>
Token	<p><a href="#">This setting is only visible if you select Token above.</a></p> <p>Enter a JWT or OAuth2 Bearer Token that the REST API requires for authentication.</p>
HTTP Headers	<p>Define if you want to send custom HTTP headers to the target URL:</p> <ul style="list-style-type: none"> <li>▪ Do not send custom HTTP headers</li> <li>▪ Send custom HTTP headers</li> </ul>
Custom HTTP Headers	<p><a href="#">This setting is only visible if you select Send custom HTTP headers above.</a></p>

Setting	Description
	<p>Enter a list of custom HTTP headers with their respective values that you want to transmit to the target URL, each pair in one line. The syntax of a header-value pair is <code>header1:value1</code>.</p> <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> If you enter more than one header-value pair, you must separate them with delimiters. The syntax is <code>header1:value1 header2:value2 header3:value3</code></li> <li><span style="color: red;">❗</span> The sensor does not support the header field names <code>user-agent</code>, <code>content-length</code>, <code>host</code>.</li> <li><span style="color: red;">❗</span> Make sure that the HTTP header statement is valid. Otherwise, the sensor request cannot be successful.</li> <li><span style="color: red;">❗</span> If you select the POST as Request Method setting above, enter the content type, for example <code>application/x-www-form-urlencoded</code>, as the custom HTTP header.</li> </ul>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <code>900</code> seconds (15 minutes).</p> <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</li> </ul>
REST Query	<p>The REST query that this sensor executes. To change it, enter a valid query for the target REST API. The syntax is: <code>[:port]/path[?var1=val1&amp;...]</code></p> <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> The sensor always inherits the first part of the address from the address of the parent device. Only enter the path to the REST endpoint of the parent device. You can override the port if necessary.</li> </ul> <p>For example, if you add the sensor to a probe device, a query to the REST API of your PRTG installation that returns the number of sensors on the probe could look like this:</p> <pre style="background-color: #f0f0f0; padding: 5px;">/api/table.json? id=1&amp;passhash=&lt;passhash&gt;&amp;username=&lt;username&gt;&amp;content=sensorx ref&amp;noraw=1&amp;filter_basetype=probe&amp;columns=totalsens=extraw</pre>
REST Configuration	<p>Select a REST configuration file from the list. The sensor uses it to map the JSON or XML result from the REST query to sensor values.</p> <p>The default REST configuration file is <code>channelDiscovery</code>. If you select this file, the sensor parses the returned JSON or XML and automatically creates channels based on available values: one channel for each number and boolean for strings if they are convertible into numbers.</p> <p>This list shows all REST configuration files that are available in the <code>\Custom Sensors\rest</code> subfolder of the <a href="#">PRTG program directory</a> on the probe system. For the files to appear in this list, store the files as JSON template (*.template) in this subfolder.</p>

Setting	Description
	<p>☁ To use custom REST configurations in PRTG Hosted Monitor, <a href="#">contact the Paessler support team</a>, or add this sensor to a remote probe instead and save the file on the remote probe system.</p> <p>❗ To show the expected values and sensor status, your files must return the expected JSON format. Channels, values, and messages must be embedded in valid JSON using JSONPath. For more information, see section <a href="#">Define Channels and Select Channel Values</a> <sup>1714</sup>.</p> <p>■ For more information on how to create custom sensors and for the return format, see section <a href="#">Custom Sensors</a>.</p> <p>❗ If you use custom sensors on the <a href="#">cluster probe</a>, copy your files to every cluster node.</p>

## Debug Options

**Debug Options**

Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>❗ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Define Channels and Select Channel Values

In your REST configuration file, you must define which values of the returned JSON or XML are mapped to which channels.



- A channel is defined by the channel key in your REST configuration. See the JSON Return Format: Minimum Example in section [Custom Sensors](#).
- A channel value is defined by an expression that retrieves and processes the value from the JSON source. The expression can contain [JSONPath](#)<sup>[1716]</sup>, [gval operators](#)<sup>[1720]</sup>, and [functions](#)<sup>[1722]</sup>.

### Example

For this example, we take PRTG as REST endpoint and query the sensor status statistics for the local probe. The REST query that we enter in the sensor settings looks like this:

```
/api/table.json?id=1&passhash=<passhash>&username=<username>&content=sensorxref&
noraw=1&filter_basetype=probe&columns=totalsens=extraw,upsens=extraw,
downsens=extraw,partialdownsens=extraw,warnsens=extraw,pausedsens=extraw,
unusualsens=extraw,undefinedsens=extraw,downacksens=extraw
```

This REST query returns some JSON, for example:

```
{
  "prtg-version": "17.3.33.2517",
  "treesize": 1,
  "state": "ok",
  "sensorxref": [
    {
      "totalsens": 28,
      "upsens": 18,
      "downsens": 0,
      "partialdownsens": 0,
      "warnsens": 0,
      "pausedsens": 9,
      "unusualsens": 1,
      "undefinedsens": 0,
      "downacksens": 0
    }
  ]
}
```

Your REST configuration has to translate this JSON for the sensor. It has to be available as JSON template (\*template) in the \Custom Sensors\rest subfolder of the [PRTG program directory](#) on the probe system. See section [Custom Sensors](#) for details about the JSON return format.

The following example returns two channels from the JSON resource that are added to the sensor in PRTG, Total (total sensor count) and Alarms (sensors in the Down status), each selected by their keys in the returned JSON.

```
{
  "prtg": {
    "result": [
      {
        "channel": "Total" ,
        "value": $.sensorxref[0].totalsens
      },
      {
        "channel": "Alarms" ,
        "value": $.sensorxref[0].downsens
      }
    ]
  }
}
```

The channel values are the values of the corresponding properties of the REST result defined in JSONPath notation, [\\$.sensorxref\[0\].totalsens](#) (28) and [\\$.sensorxref\[0\].downsens](#) (0).

Each value's property (destination) and the text property is set to the appropriate transformation rules from source to destination. This is the JSON path of the source. The sensor replaces each path with the value from the source.

- ⓘ Several REST configuration files are available in the \Custom Sensors\rest subfolder by default. They are ready for use. You can also analyze them to see how to write your own REST configuration.

## JSONPath

The REST Custom sensor uses [JSONPath](#) to assign values from the returned JSON to channels. With JSONPath, you provide the path to the value in the JSON source that you want to monitor in a channel.

- ⓘ The JSONPath implementation that PRTG uses for the REST Custom sensor might differ from other JSONPath implementations. You can [test and debug your definitions](#)<sup>[1724]</sup> using the command line. To test simple JSONPath expressions and calculations, you can also use [JSONPath Online Evaluator](#)<sup>[1726]</sup>, for example. Note that this tool might not work properly with complex JSONPath expressions that PRTG supports.

### Example




To demonstrate the practical usage of JSONPath, we use this JSON example that a REST query might have returned as reference in this section.







```
{
  "devices": [
    {
      "firmware": {
        "id": "0.7",
        "date": "2017-05-18T17:11:43.7049944Z",
        "channel": "beta"
      },
      "networks": {
        "a": {
          "rx_bytes": 35985021,
          "rx_packets": 176791,
          "rx_errors": 0,
          "rx_dropped": 476,
          "tx_bytes": 7229493,
          "tx_packets": 35518,
          "tx_errors": 0,
          "tx_dropped": 1
        },
        "b": {
          "rx_bytes": 40085321,
          "tx_bytes": 55294975
        }
      }
    },
    {
      "networks": {
        "a": {
          "rx_bytes": 63685865,
          "tx_bytes": 7229472
        }
      }
    }
  ]
}
```

### REST Custom Sensor: JSONPath

Root

The dollar sign (\$) matches the root element of the JSON data.

REST Custom Sensor: JSONPath	
Child	<p>You can match a child with <code>.&lt;key&gt;</code> or <code>[&lt;key&gt;]</code>.</p> <ul style="list-style-type: none"> <li><code>.&lt;key&gt;</code> must only contain letters, numbers, and underscore (<code>_</code>). Hyphens (<code>-</code>) are not supported.</li> <li><code>[&lt;key&gt;]</code> must only contain a number or a quoted string.</li> </ul> <p> Example</p> <p>This expression matches 35985021 in the example above:</p> <pre>\$.devices.0.networks.a.rx_bytes</pre> <p>You get the same result with this expression:</p> <pre>\$["devices"][0]["networks"]["a"]["rx_bytes"]</pre> <p>If an element contains a hyphen (<code>-</code>), the <code>.&lt;key&gt;</code> notation does not work. Use the <code>[&lt;key&gt;]</code> notation in this case:</p> <pre>\$["data"][0]["system-stats"]["temps"]["Board (CPU)"]</pre>
Wildcard	<p>To match multiple values, you can use the asterisk symbol (<code>*</code>).</p> <ul style="list-style-type: none"> <li><code>.*</code></li> <li><code>[*]</code></li> </ul> <p> Example</p> <p>This expression matches 35985021 and 40085321 in the example above:</p> <pre>\$.devices[0].networks.*.rx_bytes</pre>
Recursive Descent	<p>You can match all subitems of a node with two dots (<code>..</code>).</p> <p> Example</p> <p>This expression matches 7229493 and 55294975 and 7229472 in the example above:</p> <pre>\$...tx_bytes</pre>
Union	<p>You can match multiple children with <code>[&lt;key1&gt;,&lt;key2&gt;,&lt;...&gt;]</code>.</p> <p> Example</p> <p>This expression matches 35985021 and 7229493 in the example above:</p> <pre>\$.devices.0.networks.a["rx_bytes","tx_bytes"]</pre>
Slice	<p>You can match multiple children of an array with <code>[&lt;begin&gt;:&lt;end&gt;]</code> or <code>[&lt;begin&gt;:&lt;end&gt;:&lt;step&gt;]</code>.</p> <ul style="list-style-type: none"> <li>By default, <code>begin</code>, <code>end</code>, and <code>step</code> are either integers or empty.</li> </ul>

REST Custom Sensor: JSONPath	
	<ul style="list-style-type: none"> <li>The default approach is to go step by step from the first array element to the last element.</li> <li><b>Step</b> can also be a negative integer to go through the array in reversed order.</li> </ul> <p> Example</p> <p>This expression matches 63685865 in the example above:</p> <pre>\$.devices[-1:].networks.a.rx_bytes</pre>
Current	<p>The @ symbol matches the current element.</p> <p> Example</p> <p>This expression matches 40.085321 and 55.294975 in the example above and can be used to receive a percentage value:</p> <pre>\$.devices[1].networks.a.[ "rx_bytes", "tx_bytes" ] (@/100000000*100)</pre>
Filter	<p>You can filter matches with [?&lt;expression&gt;].</p> <p> Example</p> <p>This expression matches 35985021 in the example above because the first device is the only one with a beta channel:</p> <pre>\$.devices[?@.firmware.channel=="beta"].networks.a.rx_bytes</pre>
Script	<p>You can modify matches with (&lt;expression&gt;) and keys with [&lt;expression&gt;].</p> <p> Example</p> <p>This expression matches true and false in the example above because only the first device has a beta channel:</p> <pre>\$.devices[*](@.firmware.channel=="beta")</pre>
Placeholder	<p>Placeholders give access to values of wildcards in a match. A placeholder #n (where n is a natural number) represents the value of the nth wildcard. You can use this in the keys of JSON arrays.</p> <p> Example</p> <p>This expression creates a JSON map from ids to the corresponding firmware channel and matches {"0.7":"beta"} in the example above:</p> <pre>{\$.devices[#0].id:\$.devices[*].channel}</pre> <p> This is an extension of the official JSONPath.</p>

REST Custom Sensor: JSONPath	
Constant	<ul style="list-style-type: none"> <li>Numeric constants as 64-bit floating point: 12345.678</li> <li>String constants with double quotation marks ("): "switch"</li> <li>Boolean constants: true and false</li> </ul>
Operator	<ul style="list-style-type: none"> <li>Parentheses control the order of evaluation: (&lt;expression&gt;)</li> <li>Arrays with brackets: [&lt;expression&gt;, &lt;expression&gt;, ...]</li> <li>Objects: {&lt;expression&gt;:&lt;expression&gt;, &lt;expression&gt;:&lt;expression&gt;, ...}</li> <li>Conditionals: &lt;condition&gt; ? &lt;expression&gt; : &lt;expression&gt;</li> </ul>

### Calculating Channel Values and Functions






You can perform calculations with the values of the source JSON or XML. The sensor uses the Paessler [gval](#) package for the calculations. For more information, refer to the [gval documentation](#)<sup>1726</sup>.

The following operators and functions are available to calculate channel values.




REST Custom Sensor: Operators				
	Operator	Description	Operand Type	Output Type
Infix Modifiers	+	plus	number	number
	-	minus	number	number
	*	times	number	number
	**	power of	number	number
	%	modulo	number	number
	/	divide	number	number
	&	bitwise and	number	number
		bitwise or	number	number
	^	bitwise xor	number	number

REST Custom Sensor: Operators				
	<<	shift left	number	number
	>>	shift right	number	number
Logical Infix Operators	>	greater than	number/string	bool
	>=	equal or greater than	number/string	bool
	<	less than	number/string	bool
	<=	equal or less than	number/string	bool
	==	equal	any	bool
	!=	not equal	any	bool
	=~	match regular expression	string	bool
	!~	mismatch regular expression	string	bool
	in	contains element	any, array	bool
	&&	and	and	bool
		or	or	bool
	??	coalescence	any	any
Prefix Operators	-	negative	number	number
	~	bitwise not	number	number

REST Custom Sensor: Operators				
	!	not	bool	bool

REST Custom Sensor: Functions	
duration(start,end)	<ul style="list-style-type: none"> <li>Calculates the nanoseconds between start and end.</li> <li>Both parameters must be RFC3339 date time strings.</li> </ul> <p> Example</p> <pre>duration(\$.devices[0].firmware.date, "017-05-18T17:11:43.7049944Z")</pre>
now()	<ul style="list-style-type: none"> <li>Returns the current date time in RFC3339.</li> </ul> <p> Example</p> <pre>duration(\$.devices[0].firmware.date, now())</pre>
number(string, [base])	<ul style="list-style-type: none"> <li>Converts a string to a floating point number.</li> <li>If the base is not set, it is detected via the prefix of the string. <ul style="list-style-type: none"> <li>"0": base = 8</li> <li>"0X": base = 16</li> <li>otherwise: base = 10</li> <li>Decimals are only supported at base 10.</li> </ul> </li> </ul> <p> Examples</p> <pre>number("10.5") number("a", 16)</pre>
len(object/array/string)	<ul style="list-style-type: none"> <li>Returns the length of an array or string and counts the number of properties in a JSON object.</li> </ul> <p> Example</p> <pre>len(\$..(number(@)))</pre> <p>This expression counts every number or string that can be converted into a number. It returns 13 in the example above.</p>
sum(array-/object-of-numbers)	<ul style="list-style-type: none"> <li>Returns the sum of an array of numbers.</li> </ul> <p> Example</p>



REST Custom Sensor: Functions	
	<pre>sum([1,2,3])</pre> <p>This expression returns 6.</p>
mean(array-/object-of-numbers)	<ul style="list-style-type: none"> <li>Returns the average value of an array of numbers.</li> </ul> <p> Example</p> <pre>mean([1,2,3])</pre> <p>This expression returns 2.</p>
lookup(string, string, string, ...)	<ul style="list-style-type: none"> <li>Returns the index of the specified string in a string list, or -1 if the string is not found.</li> </ul> <p> Example</p> <pre>lookup(\$.device[0].firmware.channel, "stable", "beta", "alpha")</pre> <p>This expression returns 1 because \$.device[0].firmware.channel resolves to beta.</p>
implode(array-/object-of-string, string)	<ul style="list-style-type: none"> <li>Returns the concatenation of each string in the array, separated by the specified string.</li> </ul> <p> Example</p> <pre>implode(\$.tx_bytes, ",")</pre> <p>This expression returns 7229493,7229472.</p>

## Generic Channels

You can create a template in your REST configuration that defines generic channels. Generic channels are created based on the data that the REST endpoint returns. When the returned value is an array or object, the sensor creates a channel for each element and concatenates the corresponding key to the channel name.

### Example

Imagine that you want to have a total byte channel for each network card that is defined in the JSON example above. You can do this by creating a dynamic channel like in the following example.

```
{
  "prtg": {
    "result": [
      {
        "value": {
          "Total bytes on device" + #0 + " in network " + #1: $.devices.*.networks[*]
          (@.rx_bytes + @.tx_bytes)
        },
        "CustomUnit": "Bytes"
      }
    ]
  }
}
```

**i** Every channel must have a unique name. You cannot remove channels once they have been added and they keep their last received value. You can add new channels.

## XML Sources

If the REST source returns XML instead of JSON, the sensor transforms the XML result to JSON before replacing the value paths with source values. Because of this, you do not know the structure of the source JSON to correctly provide the paths.

In this case, manually execute the sensor executable `rest.exe` from the `\Sensor System` subfolder of the [PRTG program directory](#) on the probe system. Execute `rest.exe` with the address of the XML endpoint and the parameter `passthrough`. The `rest` executable returns the converted XML to a JSON result that you can use to define the desired paths.

```
rest.exe <xml-endpoint-url> passthrough
```

## Usage and Debugging

To create a suitable REST configuration for the sensor, you might want to check the returned JSON or XML and see what happens when your mapping rules apply.

The REST Custom sensor is an EXE sensor, so you can test and debug your configuration by executing `rest.exe` with several parameters. The `rest.exe` file is located in the `\Sensor System` subfolder of the PRTG program directory.

The command syntax is as follows:


```
rest.exe url template|passthrough|channelDiscovery [flags]
```

### rest.exe: Parameters

url

- Address of the REST API endpoint that returns JSON or XML

rest.exe: Parameters	
template	<ul style="list-style-type: none"> <li>Fully qualified path and file name of your REST configuration file used to map the JSON result to the sensor</li> </ul>
passthrough	<ul style="list-style-type: none"> <li>No mapping, only returning the queried JSON or XML</li> <li>Useful to analyze XML that has been converted to JSON</li> </ul>
channelDiscovery	<ul style="list-style-type: none"> <li>Creates a channel for every number or boolean in the returned JSON or XML</li> <li>If possible, it converts string values to number or boolean values.</li> </ul>

rest.exe: Flags	
-authtoken <string>	<ul style="list-style-type: none"> <li>JWT or OAuth2 Bearer Token to send with the request in authorization header as Bearer</li> </ul>
-authusername <string>	<ul style="list-style-type: none"> <li>User name for basic authentication</li> </ul>
-authuserpwd <string>	<ul style="list-style-type: none"> <li>User password for basic authentication</li> </ul>
-customheaders <string>	<ul style="list-style-type: none"> <li>key1:val1 key2:val2 ...</li> </ul>
-post=<int>	<ul style="list-style-type: none"> <li>{1 0}</li> <li>Default: 0</li> <li>0 results in a GET request.</li> <li>1 results in a POST request.</li> </ul> <p> Example</p> <pre>-customheaders 'Content-Type: application/x-www-form-urlencoded' -post=1 -requestbody 'myvar=value'</pre>
-proxy <string>	<ul style="list-style-type: none"> <li>Proxy server connection</li> </ul>
-proxyusername <string>	<ul style="list-style-type: none"> <li>Proxy user name with basic authentication</li> </ul>
-proxyuserpwd <string>	<ul style="list-style-type: none"> <li>Proxy user password with basic authentication</li> </ul>
-requestbody <string>	<ul style="list-style-type: none"> <li>Body of the request</li> </ul>

rest.exe: Flags	
	<p><b>i</b> You can only use this flag a POST request (-post=1).</p> <p><b>Example</b></p> <pre>-customheaders 'Content-Type: application/x-www-form-urlencoded' -post=1 -requestbody 'myvar=value'</pre>
-timeout <integer>	<ul style="list-style-type: none"> <li>▪ Sensor timeout in seconds</li> <li>▪ Default: 10</li> </ul>
-tlsignore=<int>	<ul style="list-style-type: none"> <li>▪ {1 0}</li> <li>▪ Default: 0</li> <li>▪ 1 accepts self-signed certificates on HTTPS connections</li> </ul>
-template	<ul style="list-style-type: none"> <li>▪ Returns the discovered template if you use channelDiscovery.</li> </ul>

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Response Time	<p>The response time</p> <p><b>i</b> This channel is the primary channel by default.</p>
[Value]	<p>The values that a REST API returns in several channels</p> <p><b>■</b> For more information about the return value format, see section <a href="#">Custom Sensors</a>.</p>

## More

**■** PRTG MANUAL

- [Data Storage](#)

## ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Can I create a sensor to monitor the number of paused or unknown sensors?

- <https://kb.paessler.com/en/topic/2653>

## ■ MISCELLANEOUS

Paessler JSONPath

- <https://github.com/PaesslerAG/jsonpath>

Paessler Gval

- <https://github.com/PaesslerAG/gval>

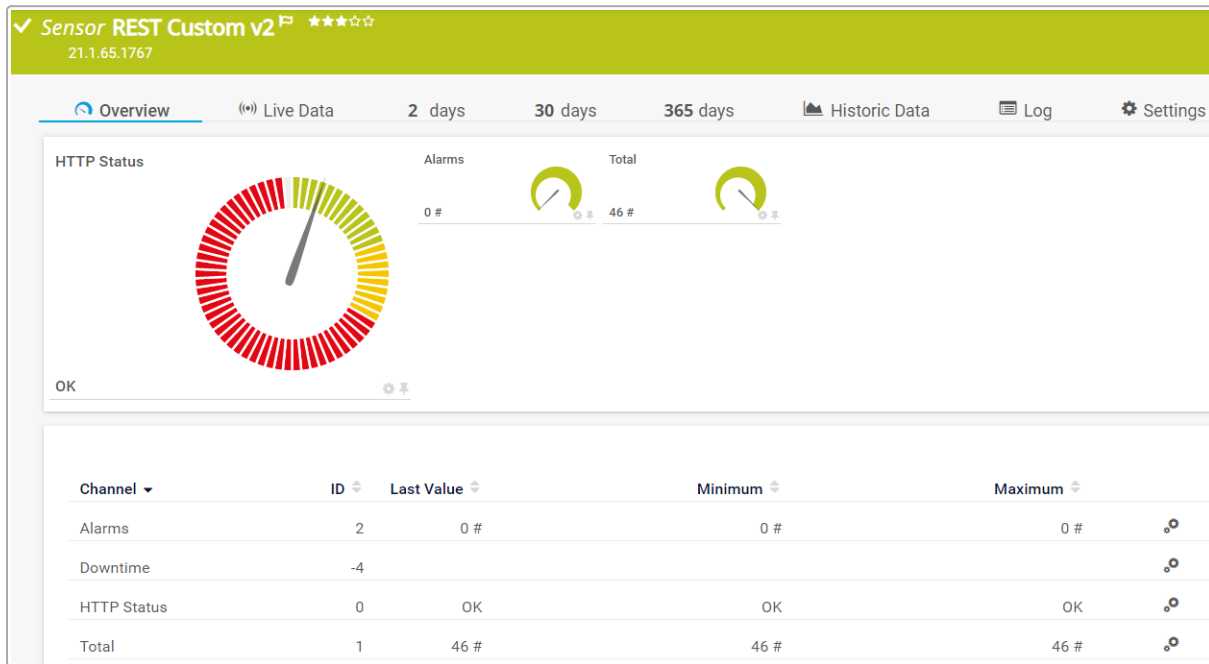
JSONPath Online Evaluator

- <https://jsonpath.com/>

## 7.8.153 REST Custom v2 Sensor (BETA)

The REST Custom v2 sensor queries a JavaScript Object Notation (JSON) or Extensible Markup Language (XML) Representational State Transfer (REST) application programming interface (API) endpoint and maps the JSON or XML result to sensor values.

**BETA** This sensor is in beta status. The operating methods and the available settings are still subject to change. Do not expect that all functions work properly, or that this sensor works as expected at all.



REST Custom v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: REST Aangepast v2
- French: REST personnalisé v2
- German: REST (Benutzerdefiniert) v2
- Japanese: REST カスタム v2
- Portuguese: REST (customizado) v2
- Russian: Специальные настройки REST v2
- Simplified Chinese: REST 自定义 v2
- Spanish: REST (personalizado) v2

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Enabled Beta Sensors experimental feature	This sensor requires that the Beta Sensors <a href="#">experimental feature</a> is enabled.  ■ For more information, see the Knowledge Base: <a href="#">What are beta sensors and how can I use them?</a>
JSONPath and XPath version	This sensor supports JSONPath and XPath <a href="#">1.0</a> .
Smart URL replacement	This sensor supports <a href="#">smart URL replacement</a> <sup>1747</sup> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Credentials	You can define <a href="#">credentials for REST API</a> in settings that are higher in the <a href="#">object hierarchy</a> .
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Limitations

- Strings that contain angled brackets (< and >) cannot be mapped manually. This affects the following settings: Channel #x Strings mapped to the 'Up' status, Channel #x Strings mapped to the 'Warning' status, and Channel #x Strings mapped to the 'Down' status. We are already working on a solution.

## Add Sensor

Setting	Description
Channel #2 - #10	You can define up to 10 channels. You must define at least one channel, so you see all available settings for <a href="#">Channel #1</a> . Specify how to handle all other possible channels:  ❗ It is not possible to enable or disable channels after sensor creation.
Channel #x JSONPath/XPath	Enter the JSONPath or XPath of the JSON or XML result that you want to monitor.  JSONPath example:

Setting	Description
	<pre>\$.store.book[0].year</pre> <p>XPath example:</p> <pre>/store/book[1]/year</pre>
Channel #x Name	<p>Enter a name for the channel. Enter a string. For example, <b>Total</b>.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Channel #x Unit	<p>Enter the unit for the value that this sensor monitors. For example, <b>#</b>.</p> <p><b>i</b> You can change this value later in the <a href="#">channel settings</a> of this sensor.</p>

### Basic Sensor Settings

#### Basic Sensor Settings

Sensor Name **i**

Example Name

Tags **i**

exampletag ✕ +

Priority **i**

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- rest

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.



## REST Specific

**REST Specific**

Request URL ⓘ

Request Method ⓘ  GET (default)  
 POST

Custom Headers ⓘ

Timeout (Sec.) ⓘ

Content Type ⓘ  JSON (default)  
 XML

Custom Sensor Message ⓘ

REST Specific

Setting	Description
Request URL	<p>Enter the URL of the JSON or XML REST API endpoint that you want to request.</p> <p>Example URL:</p> <pre>https://:1616/api/health?token=%restbearertoken&amp;name=%restusername&amp;refresh=true</pre> <p><b>i</b> You can use the following placeholders in this field: <code>%restusername</code>, <code>%restpassword</code>, <code>%restbearertoken</code>, <code>%restplaceholder1</code>, <code>%restplaceholder2</code>, <code>%restplaceholder3</code>, <code>%restplaceholder4</code>, and <code>%restplaceholder5</code>. You can define these placeholders in the <a href="#">credentials for REST API</a> in settings that are higher in the <a href="#">object hierarchy</a>.</p> <p><b>■</b> PRTG uses a smart URL replacement with which you can use the parent device's IP address or Domain Name System (DNS) name setting as part of the URL. For more information, see section <a href="#">Smart URL Replacement</a><sup>[1747]</sup>.</p> <p><b>i</b> If you enter <code>127.0.0.1</code> as IP address of the parent device, PRTG requests the following URL:</p> <pre>https://127.0.0.1:1616/api/health?token=%restbearertoken&amp;name=%restusername&amp;refresh=true</pre>
Request Method	<p>Select the HTTP request method that the sensor uses to request the REST API:</p> <ul style="list-style-type: none"> <li>▪ GET (default): Use the GET method to request the REST API.</li> <li>▪ POST: Use the POST method to request the REST API.</li> </ul>

Setting	Description
POST Body	<p>This setting is only visible if you select POST above.</p> <p>Enter the data part for the POST request.</p> <p><b>i</b> You can use the following placeholders in this field: <a href="#">%restusername</a>, <a href="#">%restpassword</a>, <a href="#">%restbearertoken</a>, <a href="#">%restplaceholder1</a>, <a href="#">%restplaceholder2</a>, <a href="#">%restplaceholder3</a>, <a href="#">%restplaceholder4</a>, and <a href="#">%restplaceholder5</a>. You can define these placeholders in the <a href="#">credentials for REST API</a> in settings that are higher in the <a href="#">object hierarchy</a>.</p>
Custom Headers	<p>Enter a list of custom HTTP headers with their respective values that you want to transmit to the target URL. The syntax of a header-value pair is <a href="#">header1:value1</a>.</p> <p>Custom header example:</p> <pre data-bbox="486 896 1353 1025">host:host1.example.com User-Agent:PRTG sensor 0.1 X-API-Key: %restplaceholder1</pre> <p><b>i</b> If you enter more than one header-value pair, enter each pair in one line:  header1:value1  header2:value2  header3:value3</p> <p><b>i</b> Make sure that the HTTP header statement is valid. Otherwise, the sensor request cannot be successful.</p> <p><b>i</b> You can use the following placeholders in this field: <a href="#">%restusername</a>, <a href="#">%restpassword</a>, <a href="#">%restbearertoken</a>, <a href="#">%restplaceholder1</a>, <a href="#">%restplaceholder2</a>, <a href="#">%restplaceholder3</a>, <a href="#">%restplaceholder4</a>, and <a href="#">%restplaceholder5</a>. You can define these placeholders in the <a href="#">credentials for REST API</a> in settings that are higher in the <a href="#">object hierarchy</a>.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
Content Type	<p>Select the type of the content that the sensor queries:</p> <ul style="list-style-type: none"> <li>▪ JSON (default)</li> <li>▪ XML</li> </ul>
Custom Sensor Message	<p>Enter the JSONPath or XPath from which you want to receive a string that the sensor shows as the permanent sensor message.</p>

Setting	Description
	<p>JSONPath example:</p> <pre>\$.store.book[0].title</pre> <p>XPath example:</p> <pre>/store/book[1]/title</pre>

## Channel Settings

**Channel Settings**

Channel #1 ⓘ `$.store.book[0].price`

JSONPath/XPath



Channel #1 Type ⓘ *Absolute (float)*

Channel Settings

Setting	Description
Channel #x JSONPath/XPath	<p>Enter the JSONPath or XPath of the JSON or XML result that you want to monitor.</p> <p>JSONPath example:</p> <pre>\$.store.book[0].year</pre> <p>XPath example:</p> <pre>/store/book[1]/year</pre>
Channel #x Name	<p>Enter a name for the channel. Enter a string. For example, <b>Total</b>. PRTG dynamically generates channels with this name as the identifier.</p> <p><span style="font-size: small;">ⓘ</span> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({}), PRTG replaces them with braces ({}), PRTG replaces them with braces ({}), PRTG replaces them with braces ({}). For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Channel #x Value Type	<p>Select the value type that the channel displays:</p> <ul style="list-style-type: none"> <li>▪ Absolute (integer): Integer64 values with or without an operational sign, such as <b>10</b> or <b>120</b> or <b>-12</b> or <b>120</b>.</li> <li>▪ Absolute (float): Double values, such as <b>-5.80</b> or <b>8.23</b>.</li> </ul> <p><span style="font-size: small;">ⓘ</span> If you select Absolute (float), the sensor automatically shows all decimal places of the received value in the channel. You can define how many decimal places of the channel's data that you want to display in graphs and tables in the <a href="#">channel settings</a>.</p>


Setting	Description
	<ul style="list-style-type: none"> <li>▪ Delta (counter): Counter values. The sensor calculates the difference between the last and the current value. Enter an integer. The sensor additionally divides the delta value by a time period to indicate a speed value.               <ul style="list-style-type: none"> <li>ⓘ This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative values and decreasing values.</li> </ul> </li> <li>▪ Status (string): The sensor shows a status depending on how you map the returned strings and shows the returned strings as sensor message.</li> <li>▪ Lookup: The sensors shows a status depending on how you define values in a <a href="#">custom lookup file</a>.</li> <li>ⓘ Absolute (integer) and Absolute (float) support the extraction of numerical values from a received string. The sensor parses the numerical value from the beginning of the string until it encounters the first element that is not part of a numerical value, for example a letter. The sensor ignores whitespace characters.</li> <li>ⓘ You cannot change this value after sensor creation.</li> </ul>
Channel #x Unit	<p>This setting is only visible if you select Absolute (integer), Absolute (float), or Delta (counter) as Channel #x Value Type.</p> <p>Select the unit that the channel displays:</p> <ul style="list-style-type: none"> <li>▪ Custom (default)</li> <li>▪ Percent</li> <li>▪ Percent (CPU)</li> <li>▪ Temperature (celsius)</li> <li>▪ Time (milliseconds)</li> <li>▪ Time (hours)</li> <li>▪ Time (seconds)</li> <li>▪ Bytes (memory)</li> <li>▪ Bytes (disk)</li> <li>▪ Bytes (file)</li> <li>▪ Bytes (bandwidth)</li> <li>▪ Bytes per second (disk)</li> <li>▪ Bytes per second (network)</li> </ul> <p>ⓘ You cannot change this value after sensor creation.</p>

Setting	Description
Channel #x Custom Unit	<p>This setting is only visible if you select Custom (default) as Channel #x Unit.</p> <p>Enter the custom unit of the value of this channel. Enter a string.</p>
Channel #x Strings mapped to the 'Up' status	<p>This setting is only visible if you select Status (string) as Channel #x Value Type.</p> <p>Enter the strings that the sensor maps to the Up status in a comma-separated list.</p> <p><b>i</b> If a string contains a comma, you must put the string in quotation marks. For example, to map the string <code>Friday,2nd</code> enter <code>"Friday,2nd"</code>. If a string contains quotation marks, you must escape the quotation marks using a backslash (<code>\</code>) and put the string in quotation marks. For example, to map the string <code>Friday "2nd"</code> enter <code>"Friday \"2nd\""</code>.</p>
Channel #x Strings mapped to the 'Warning' status	<p>This setting is only visible if you select Status (string) as Channel #x Value Type.</p> <p>Enter the strings that the sensor maps to the Warning status in a comma-separated list.</p> <p><b>i</b> If a string contains a comma, you must put the string in quotation marks. For example, to map the string <code>Friday,2nd</code> enter <code>"Friday,2nd"</code>. If a string contains quotation marks, you must escape the quotation marks using a backslash (<code>\</code>) and put the string in quotation marks. For example, to map the string <code>Friday "2nd"</code> enter <code>"Friday \"2nd\""</code>.</p>
Channel #x Strings mapped to the 'Down' status	<p>This setting is only visible if you select Status (string) as Channel #x Value Type.</p> <p>Enter the strings that the sensor maps to the Down status in a comma-separated list.</p> <p><b>i</b> If a string contains a comma, you must put the string in quotation marks. For example, to map the string <code>Friday,2nd</code> enter <code>"Friday,2nd"</code>. If a string contains quotation marks, you must escape the quotation marks using a backslash (<code>\</code>) and put the string in quotation marks. For example, to map the string <code>Friday "2nd"</code> enter <code>"Friday \"2nd\""</code>.</p>
Channel #x Handling of Unknown Strings	<p>This setting is only visible if you select Status (string) as Channel #x Value Type.</p> <p>Select the status to which the sensor maps all unknown strings in the returned result that are not manually mapped to the Up, the Warning, or the Down status:</p> <ul style="list-style-type: none"> <li>▪ 'Up' status: Map all unknown strings to the Up status.</li> </ul>


Setting	Description
	<ul style="list-style-type: none"> <li>'Warning' status: Map all unknown strings to the Warning status.</li> <li>'Down' status (default): Map all unknown strings to the Down status.</li> </ul>
Channel #x Lookup ID	<p>This setting is only visible if you select <b>Lookup as Channel #x Value Type</b>.</p> <p>Enter the ID of the lookup you wish to use. You can find the ID in the <a href="#">ValueLookup</a> parameter in the lookup file.</p> <p><input type="checkbox"/> For more information, see section <a href="#">Define Lookups</a>.</p> <p> You cannot change this value after sensor creation.</p>
Channel #2 - #10	<p>You can define up to 10 channels. You must define at least one channel, so you see all available settings for <b>Channel #1</b>. Specify how to handle all other possible channels:</p> <ul style="list-style-type: none"> <li>Disable: Do not create this channel.</li> <li>Enable: Create this channel.</li> </ul> <p> It is not possible to enable or disable channels after sensor creation.</p>

## Sensor Display



**Sensor Display**


Primary Channel  Downtime

---

Graph Type   Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>



## Debug Options

**Debug Options**


Result Handling 

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## JSONPath

The REST Custom v2 sensor uses [JSONPath](#) to assign values from the returned JSON to channels. With JSONPath, you provide the path to the value in the JSON source that you want to monitor in a channel.

ⓘ The JSONPath implementation that PRTG uses for the REST Custom v2 sensor might differ from other JSONPath implementations. To test simple JSONPath expressions and calculations, you can use [JSONPath Online Evaluator - jsonpath.com](https://jsonpath.com), for example. Note that this tool might not work properly with complex JSONPath expressions that PRTG supports.



 Example

To demonstrate the practical usage of JSONPath, we use this JSON example that a REST query might have returned as reference in this section.

```
{
  "devices": [
    {
      "firmware": {
        "id": "0.7",
        "date": "2017-05-18T17:11:43.7049944Z",
        "channel": "beta"
      },
      "networks": {
        "a": {
          "rx_bytes": 35985021,
          "rx_packets": 176791,
          "rx_errors": 0,
          "rx_dropped": 476,
          "tx_bytes": 7229493,
          "tx_packets": 35518,
          "tx_errors": 0,
          "tx_dropped": 1
        },
        "b": {
          "rx_bytes": 40085321,
          "tx_bytes": 55294975
        }
      }
    },
    {
      "networks": {
        "a": {
          "rx_bytes": 63685865,
          "tx_bytes": 7229472
        }
      }
    }
  ]
}
```

REST Custom v2 Sensor: JSONPath	
Root	The dollar sign (\$) matches the root element of the JSON data.
Child	<p>You can match a child with <code>.&lt;key&gt;</code> or <code>[&lt;key&gt;]</code>.</p> <ul style="list-style-type: none"> <li><code>.&lt;key&gt;</code> must only contain letters, numbers, and underscore (<code>_</code>). Hyphens (<code>-</code>) must be escaped with quotation marks.</li> <li><code>[&lt;key&gt;]</code> must only contain a number or a quoted string.</li> </ul> <p> Example</p> <p>This expression matches 35985021 in the example above:</p> <pre>\$.devices.0.networks.a.rx_bytes</pre> <p>You get the same result with this expression:</p> <pre>["\$devices"][0]["networks"]["a"]["rx_bytes"]</pre> <p>If an element contains a hyphen (<code>-</code>), the <code>.&lt;key&gt;</code> notation does not work. Use the <code>[&lt;key&gt;]</code> notation in this case:</p> <pre>["\$data"][0]["system-stats"]["temps"]["Board (CPU)"]</pre>
Wildcard	<p>To match multiple values, you can use the asterisk symbol (<code>*</code>).</p> <ul style="list-style-type: none"> <li><code>.*</code></li> <li><code>[*]</code></li> </ul> <p> Example</p> <p>This expression matches 35985021 and 40085321 in the example above:</p> <pre>\$.devices[0].networks.*.rx_bytes</pre>
Recursive Descent	<p>You can match all subitems of a node with two dots (<code>..</code>).</p> <p> Example</p> <p>This expression matches 7229493 and 55294975 and 7229472 in the example above:</p> <pre>\$...tx_bytes</pre>
Union	<p>You can match multiple children with <code>[&lt;key1&gt;,&lt;key2&gt;,&lt;...&gt;]</code>.</p> <p> Example</p> <p>This expression matches 35985021 and 7229493 in the example above:</p> <pre>\$.devices.0.networks.a["rx_bytes","tx_bytes"]</pre>
Slice	<p>You can match multiple children of an array with <code>[&lt;begin&gt;:&lt;end&gt;]</code> or <code>[&lt;begin&gt;:&lt;end&gt;:&lt;step&gt;]</code>.</p>

REST Custom v2 Sensor: JSONPath	
	<ul style="list-style-type: none"> <li>By default, <b>begin</b>, <b>end</b>, and <b>step</b> are either integers or empty.</li> <li>The default approach is to go step by step from the first array element to the last element.</li> <li><b>Step</b> can also be a negative integer to go through the array in reversed order.</li> </ul> <p> Example</p> <p>This expression matches 63685865 and 7229472 in the example above:</p> <pre>\$.devices[-1:].networks.a[rx_bytes,tx_bytes]</pre>
Current	<p>The @ symbol matches the current element.</p> <p> Example</p> <p>This expression matches 63685865 and 7229472 in the example above:</p> <pre>\$.devices[(@.length-1)].networks.a.rx_bytes</pre>
Filter	<p>You can filter matches with [?(&lt;expression&gt;)].</p> <p> Example</p> <p>This expression matches 35985021 in the example above because the first device is the only one with a beta channel:</p> <pre>\$.devices[?(@.firmware.channel=="beta")].networks.a.rx_bytes</pre>
Constant	<ul style="list-style-type: none"> <li>Numeric constants as 64-bit floating point: 12345.678</li> <li>String constants with double quotation marks ("): "switch"</li> <li>Boolean constants: true and false <ul style="list-style-type: none"> <li> If the JSONPath points to a boolean, the sensor translates true as 1 and false as 0.</li> </ul> </li> </ul>
Functions	<p>You can use functions on top level or in filters.</p> <p>This expression returns the number items in the element devices in the example above:</p> <pre>length(\$.devices)</pre> <p> For more information about functions, see <a href="#">JsonCons JSONPath   Functions</a>.</p>
Operator	<ul style="list-style-type: none"> <li>Parentheses control the order of evaluation: (&lt;expression&gt;)</li> <li>Arrays with brackets: [&lt;expression&gt;, &lt;expression&gt;, ...]</li> <li>Objects: {&lt;expression&gt;:&lt;expression&gt;, &lt;expression&gt;:&lt;expression&gt;, ...}</li> </ul>





① For more information about JSONPath, see [JsonCons JSONPath](#).


## REST Custom v2 Sensor: XPath

### Example

To demonstrate the practical usage of XPath, we use this XML example that a REST query might have returned as reference in this section.

```
<?xml version="1.0" encoding="UTF-8" ?>
<root>
  <devices>
    <firmware>
      <id type="major">0</id>
      <id type="minor">7</id>
      <date>2017-05-18T17:11:43.7049944Z</date>
      <channel>beta</channel>
    </firmware>
    <networks>
      <a>
        <rx_bytes>35985021</rx_bytes>
        <rx_packets>176791</rx_packets>
        <rx_errors>0</rx_errors>
        <rx_dropped>476</rx_dropped>
        <tx_bytes>7229493</tx_bytes>
        <tx_packets>35518</tx_packets>
        <tx_errors>0</tx_errors>
        <tx_dropped>1</tx_dropped>
      </a>
      <b>
        <rx_bytes>40085321</rx_bytes>
        <tx_bytes>55294975</tx_bytes>
      </b>
    </networks>
  </devices>
  <devices>
    <networks>
      <a>
        <rx_bytes>63685865</rx_bytes>
        <tx_bytes>7229472</tx_bytes>
      </a>
    </networks>
  </devices>
</root>
```

REST Custom v2 Sensor: XPath	
Root	The slash symbol (/) matches the root element of the XML data.
Child	<p>You can match a child by its name with /&lt;key&gt; or [&lt;key&gt;] or by its index with [&lt;index&gt;].</p> <ul style="list-style-type: none"> <li>▪ /&lt;key&gt; must only contain letters, numbers, and underscore (_). Hyphens (-) must be escaped with quotation marks.</li> <li>▪ [&lt;key&gt;] must only contain a number or a quoted string.</li> <li>▪ [&lt;index&gt;] must only contain a number.</li> </ul> <p> Example</p> <p>This expression matches 35985021 in the example above:</p> <pre>/root/devices[1]/networks/a/rx_bytes</pre> <p>This expression matches major in the example above:</p> <pre>/root/devices[1]/firmware/id[1]/@type</pre>
Wildcard	<p>To match multiple values, you can use the asterisk symbol (*).</p> <ul style="list-style-type: none"> <li>▪ /*</li> <li>▪ /@*</li> <li>▪ [*]</li> <li>▪ [@*]</li> </ul> <p> Example</p> <p>This expression matches 35985021 and 40085321 in the example above:</p> <pre>/root/devices[1]/networks/*/rx_bytes</pre>
Recursive Descent	<p>You can match all subitems of a node with two slashes (//).</p> <p> Example</p> <p>This expression matches 7229493 and 55294975 and 7229472 in the example above:</p> <pre>//tx_bytes</pre>
Union	<p>You can match multiple queries by combining them with the vertical bar symbol ( ).</p> <p> Example</p> <p>This expression matches 35985021 and 7229493 in the example above:</p> <pre>/root/devices[1]/networks/a/rx_bytes   /root/devices[1]/networks/a/tx_bytes</pre>

REST Custom v2 Sensor: XPath	
Filter	<p>You can filter matches with [&lt;expression&gt;].</p> <p> <b>Example</b></p> <p>This expression matches 35985021 in the example above because the first device is the only one with a beta channel:</p> <pre>/root/devices[firmware/channel='beta']/networks/a/rx_bytes</pre> <p>This expression matches 0 in the example above:</p> <pre>/root/devices[1]/firmware[1]/id[@type='major']</pre>
Constant	<ul style="list-style-type: none"> <li>▪ Numeric constants as 64-bit floating point: 12345.678</li> <li>▪ String constants with double quotation marks ("): "switch"</li> <li>▪ Boolean constants: true and false <ul style="list-style-type: none"> <li>ⓘ If the XPath points to a boolean, the sensor translates true as 1 and false as 0.</li> </ul> </li> </ul>
Functions	<p>You can use functions on top level or in filters.</p> <p>This expression returns the number of items in the devices element in the example above:</p> <pre>count(/root/devices[position() &lt; 3])</pre> <p>ⓘ For more information about functions, see <a href="#">XML Path Language (Core Function Library)</a>.</p>
Operator	<ul style="list-style-type: none"> <li>▪ Parentheses control the order of evaluation: (&lt;expression&gt;)</li> </ul>

ⓘ For more information about XPath, see [XML Path Language \(XPath\)](#).

## Calculating Channel Values

The REST Custom v2 sensor supports the following arithmetic:

- Addition (+)
- Subtraction (-)
- Multiplication (\*)
- Division (div, /)
- Equal (=)
- Not equal (!=)

 Examples

XML	JSON
<pre>&lt;root&gt;   &lt;one&gt;1&lt;/one&gt;   &lt;two value_int="2"&gt;2&lt;/two&gt;   &lt;two_point5&gt;2.5&lt;/two_point5&gt;   &lt;four&gt;4&lt;/four&gt; &lt;/root&gt;</pre>	<pre>{   "root": {     "one": 1,     "two": 2,     "two_string": "2",     "two_point5": 2.5,     "four": 4   } }</pre>

XML	JSON	Description	Result (XML)	Result (JSON)
/root/one + /root/two	<code>eval(\$.root.one + \$.root.two)</code>	Addition of the numbers	3	3
n/a	<code>eval(\$.root.one + to_number(\$.root.two_string))</code>	Addition of a number and a string	n/a	3
/root/one + /root/two/@value_int	n/a	Addition of a number and an attribute value	3	n/a
/root/four div /root/two	<code>eval(\$.root.four / \$.root.two)</code>	Division of two integers. The expected result is an integer	2	2
/root/one div /root/two	<code>eval(\$.root.one / \$.root.two)</code>	Division of two integers, the expected result is a floating-point number	0.5	0



XML	JSON	Description	Result (XML)	Result (JSON)
n/a	<code>eval(\$.root.one / \$.root.two * 1.0)</code>	Division of two integers with a floating point number as result	n/a	0.5
<code>/root/one div /root/two_point5</code>	<code>eval(\$.root.one / \$root.two_point5)</code>	Division of a float and an integer	0.4	0.4
<code>/root/one = /root/two</code>	<code>eval(\$.root.one == \$.root.two)</code>	If entries are equal	0 (false)	0 (false)

## Smart URL Replacement

Instead of entering a complete address in the Request URL field of the REST Custom v2 sensor, you can only enter the protocol followed by a colon and three forward slashes (this means that you can enter either <http://> or <https://>, or even a simple forward slash / as the equivalent for <http://>). PRTG automatically fills in the parent device's IP Address/DNS Name in front of the third forward slash.


Whether this results in a valid URL or not depends on the IP address or Domain Name System (DNS) name of the parent device. In combination with cloning devices, you can use smart URL replacement to create many similar devices.

For example, if you create a device with the DNS name [www.example.com](http://www.example.com) and you add a REST Custom v2 sensor to it, you can provide values in the following ways:

- If you enter <https://> in the Request URL field, PRTG automatically creates the URL <https://www.example.com/>
- If you enter [/help](http://www.example.com/help) in the Request URL field, PRTG automatically creates the URL <http://www.example.com/help>
- It is also possible to provide a port number in the Request URL field. It is taken over by the device's DNS name and is internally added, for example, <https://:1616/>

 Smart URL replacement does not work for sensors that run on the probe device.

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
HTTP Status	<p>The HTTP status that the requested URL returns</p> <ul style="list-style-type: none"> <li>▪ Up status: Continue, Switching Protocols, Processing, OK, Created, Accepted, Non-Authoritative Information, No Content, Reset Content, Partial Content, Multi-Status, Already Reported, IM Used</li> <li>▪ Warning status: Multiple Choices, Moved Permanently, Found, See Other, Not Modified, Use Proxy, Switch Proxy (deprecated), Temporary Redirect, Permanent Redirect,</li> <li>▪ Down status: Bad Request, Unauthorized, Payment Required, Forbidden, Not Found, Method Not Allowed, Not Acceptable, Proxy Authentication Required, Request Time-out, Conflict, Gone, Length Required, Precondition Failed, Request Entity Too Large, Request URL Too Long, Unsupported Media Type, Requested Range Not Satisfiable, Expectation Failed, I'm a teapot, Policy Not Fulfilled, There are too many connections from your internet address, Unprocessable Entity, Locked, Failed Dependency, Unordered Collection, Upgrade Required, Precondition Required, Too Many Requests, Request Header Fields Too Large, No Response, The request should be retried after doing the appropriate action, Unavailable For Legal Reasons, Internal Server Error, Not Implemented, Bad Gateway, Service Unavailable, Gateway Time-out, HTTP Version not supported, Variant Also Negotiates[13], Insufficient Storage, Loop Detected, Bandwidth Limit Exceeded, Not Extended</li> <li>▪ Unknown status: Unknown</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
[Value]	The values that a REST API returns in several channels

## More

### ■ KNOWLEDGE BASE

What are beta sensors and how can I use them?

- <https://kb.paessler.com/en/topic/88697>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Can I create a sensor to monitor the number of paused or unknown sensors?

- <https://kb.paessler.com/en/topic/2653>

■ MISCELLANEOUS

JSONPath Online Evaluator

- <https://jsonpath.com/>

JsonCons JSONPath

- <https://danielaparker.github.io/JsonCons.Net/articles/JsonPath/JsonCons.JsonPath.html>

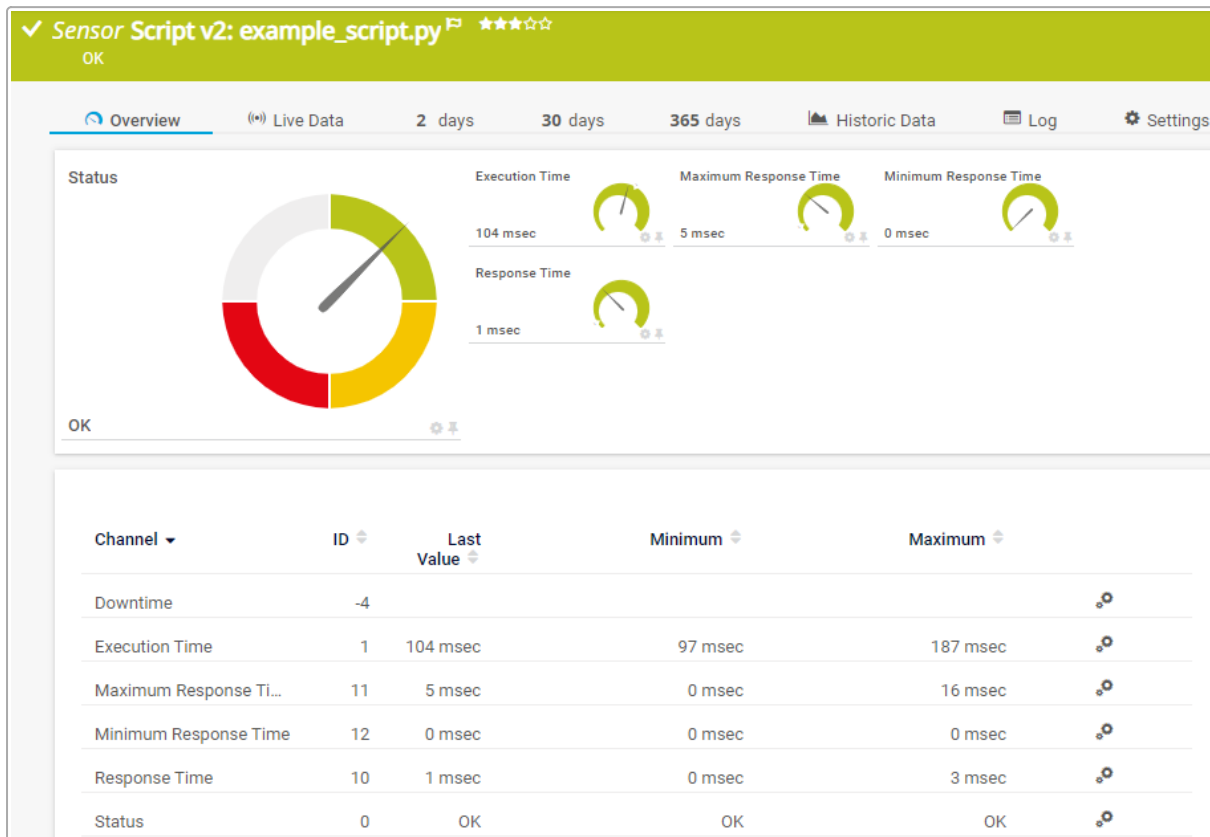
Stefan Gössner JSONPath

- <https://goessner.net/articles/JsonPath/>

## 7.8.154 Script v2 Sensor

The Script v2 sensor runs a Python script (.py) on the probe system.

**i** The return result of this sensor must comply with the provided JavaScript Object Notation (JSON) schema. For more information, see the [Remarks](#) below.



Script v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Script v2
- French: Script v2
- German: Skript v2
- Japanese: スクリプト v2
- Portuguese: Script v2
- Russian: Скрипт v2
- Simplified Chinese: Script v2
- Spanish: Script v2

## Remarks

Consider the following [remarks](#) <sup>(1751)</sup> and requirements for this sensor:

Remark	Description
Python	This sensor requires that Python is installed for the Windows user account that the probe runs under.
File storage	This sensor requires that you store the script file on the probe system. In a cluster, copy the file to every cluster node.   You must store the script file in the \Custom Sensors\scripts subfolder of the <a href="#">PRTG program directory</a> of the probe system on Windows systems or in the /opt/paessler/share/scripts directory of the probe system on Linux systems.
Channel IDs	This sensor supports the channel IDs <a href="#">10 to 2,147,483,647</a> .
IPv6	This sensor supports IPv6.
Channels	This sensor supports up to <a href="#">50 channels</a> .
Placeholders	You can define placeholders in <a href="#">credentials for script sensors</a> settings that are higher in the <a href="#">object hierarchy</a> .
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Parameters	This sensor invokes all scripts with the <code>-E</code> parameter as a security measure. This parameter ignores all python* environmental variables when starting the script.
Example scripts	This sensor comes with example scripts. For more information, see the Knowledge Base: <a href="#">I want to use the Script v2 sensor example scripts. What do I need to know?</a>
JSON schema	For more information about the JSON schema that this sensor uses, see the Knowledge Base: <a href="#">Where can I find the JSON schema against which the Script v2 sensor validates my script output?</a>
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">30 seconds</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">1 minute</a>.</li> </ul>

Remark	Description
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.
Multi-platform probe	You can add this sensor to a multi-platform probe.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

**Tags** ⓘ exampletag ✕ ⊕

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- exesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Script Specific

#### Script Specific

**Name** ⓘ *example\_script.py*

**Type** ⓘ *Python*

Script Specific

Setting	Description
Name	Select one or more Python scripts from the list. PRTG creates one <a href="#">scanning interval</a> <sup>1755</sup> for each script that you select. The sensor executes it with every

Setting	Description
	<p>This list shows all Python script files that are available in the \Custom Sensors\scripts subfolder of the <a href="#">PRTG program directory</a> of the probe system on Windows systems or in the /opt/paessler/share/scripts directory of the probe system on Linux systems. For the files to appear in this list, store the files in this subfolder with the extension <code>.py</code>.</p> <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> To show the expected values and sensor status, your scripts must return the expected JSON format to standard output (stdout). The Script v2 sensor validates the results that the script returns against the provided JSON schema. For more information, see the Knowledge Base: <a href="#">Where can I find the JSON schema against which the Script v2 sensor validates my script output?</a></li> <li><span style="color: red;">❗</span> If you use custom sensors on the <a href="#">cluster probe</a>, copy your files to every cluster node.</li> <li><span style="color: red;">❗</span> You cannot change this value after sensor creation.</li> </ul>
Type	The type of the script file.

### Script Settings

**Script Settings**

Timeout (Sec.) ⓘ

Parameters ⓘ

Script Settings

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</li> </ul>
Parameters	<p>If your script file uses parameters, you can enter them here. You can use placeholders as well. Enter a string or leave the field empty.</p> <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> You can define placeholders in the <a href="#">credentials for script sensors</a> in the settings of a parent object and use the <code>%host</code> and <code>%sensorid</code> placeholders. The sensor replaces the parameters with their values and passes them to the script as strings via <code>stdin</code>.</li> </ul>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**


Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options



Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><b>i</b> If you select Store result, the sensor writes the standard error (stderr) streams in clear text to the last sensor result file. Do not return sensitive information via the scripts that you run with this sensor.</p> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Execution Time	The execution time of the script
Status	<p>The status that the script returns</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Error</li> <li>▪ Unknown status: Unknown</li> </ul>

Channel	Description
	 This channel is the primary channel by default.
[Value]	The values that the script file returns in several channels

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

I want to use the Script v2 sensor example scripts. What do I need to know?

- <https://kb.paessler.com/en/topic/91349>

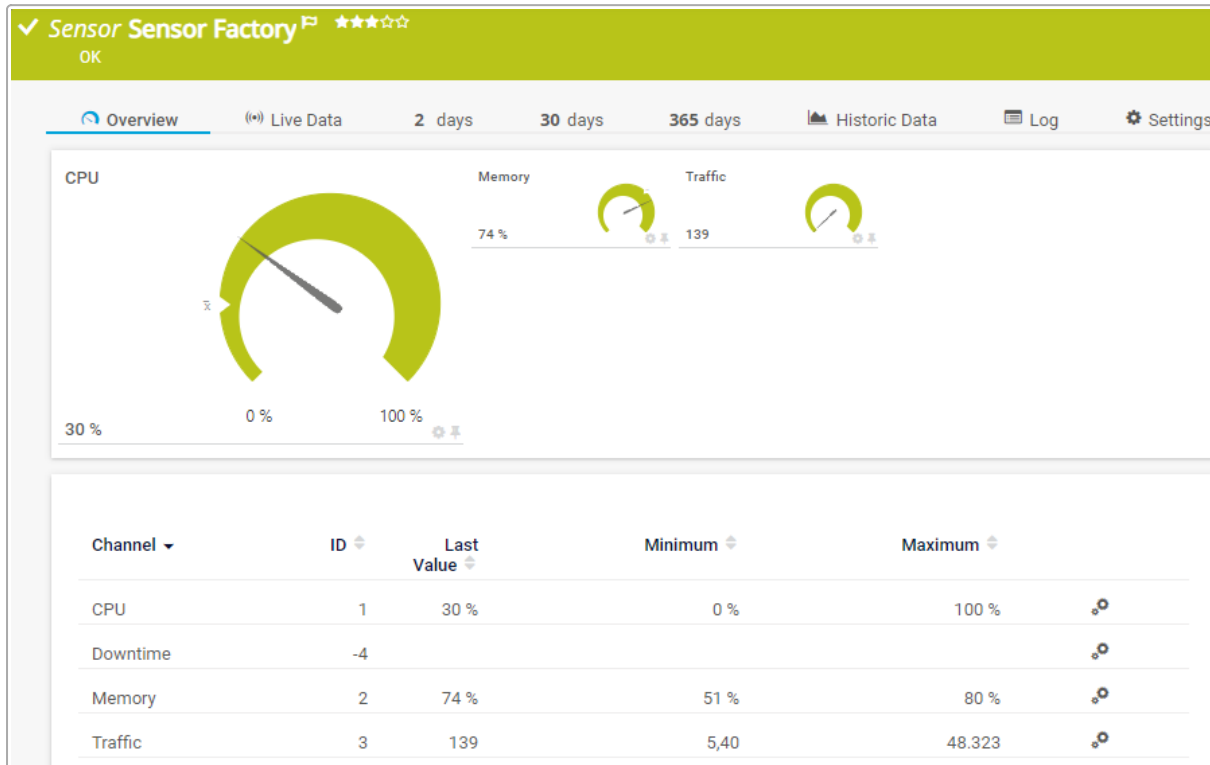
Where can I find the JSON schema against which the Script v2 sensor validates my script output?

- <https://kb.paessler.com/en/topic/91280>

## 7.8.155 Sensor Factory Sensor

The Sensor Factory sensor monitors entire business processes that involve several components. You can create a customized sensor with channels based on data from other sensors ("source sensors").

**i** If you want to create only a cumulated sensor status based on specific source sensors, we recommend that you use the [Business Process](#)<sup>[740]</sup> sensor.



Sensor Factory Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1768]</sup>.

### Sensor in Other Languages

- Dutch: Sensor Fabriek
- French: Capteur combiné
- German: Formelsensor
- Japanese: センサーファクトリ
- Portuguese: Sensor de fórmula
- Russian: Фабрика сенсоров
- Simplified Chinese: 传感器出厂
- Spanish: Sensor combinado

### Remarks

Consider the following [remarks](#)<sup>[1757]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor can have a very high impact on the performance of the PRTG core server system. We recommend that you use no more than 50 of this sensor per PRTG core server.
Channels	This sensor does not officially support more than <a href="#">50 channels</a> .
Channel definitions	This sensor does not support <a href="#">channel definitions</a> that refer to channels of Sensor Factory sensors.
Reports	Uptime or downtime data for this sensor is not available in <a href="#">reports</a> .
Scanning interval	Make sure that the <a href="#">scanning interval</a> of this sensor is equal to or greater than the scanning interval of the source sensors to avoid incorrect sensor behavior. For example, "no data" messages or erratic changes of the sensor state can be a result of an invalid scanning interval.
Flow sensors	This sensor might not work with <a href="#">flow sensors</a> . Sensors that use <a href="#">active flow timeout</a> , for example <a href="#">NetFlow and jFlow sensors</a> , are not supported by this sensor.
Knowledge Base	Knowledge Base: <a href="#">How can I monitor the overall status of the business process "email"?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- factorysensor

■ For more information about basic sensor settings, see section [Sensor Settings](#).

## Sensor Factory Specific Settings

**Sensor Factory Specific Settings**

**Channel Definition** ⓘ

#1: CPU  
Channel(128630,0)

#2: Memory

**Status Handling** ⓘ

Show down status when one or more source sensors are in the down status (default)

Show warning status when one or more source sensors are in the down status


Use custom formula



**If a Source Sensor Has No Data** ⓘ

Do not calculate the channels that use the sensor (default)

Calculate the channels and use zero as source value

Sensor Factory Specific Settings

Setting	Description
Channel Definition	<p>Enter a channel definition for the Sensor Factory sensor. Using a specific syntax, you can refer to data from channels of other sensors. You can also calculate values. Enter one channel definition for each new channel that you want to add to the Sensor Factory sensor.</p> <p> For more information, see section <a href="#">Define Channels</a> <sup>[176]</sup>.</p>
Status Handling	<p>Define if the Sensor Factory sensor enters the Down status or to the Warning status if one of the source sensors is in the Down <a href="#">status</a>:</p> <ul style="list-style-type: none"> <li>▪ Show down status when one or more source sensors are in the down status (default): If at least one source sensor that you use in a channel definition is in the Down status, the Sensor Factory sensor shows the Down status as well until all referred sensors leave this status. While the Sensor Factory sensor is in the Down status, it still shows data of all available channels. <ul style="list-style-type: none"> <li>ⓘ If a <a href="#">lookup definition</a> or an <a href="#">error limit</a> triggers the Down status of the source sensor, the Sensor Factory does not show the Down status. This is because the Sensor Factory should only show this status if it cannot calculate values.</li> </ul> </li> <li>▪ Show warning status when one or more source sensors are in the down status: If at least one source sensor that you use in a channel definition is in the Down status, the Sensor Factory sensor shows the Warning status until all referred sensors leave the Down status. <ul style="list-style-type: none"> <li>ⓘ If a lookup definition or an error limit triggers the Down status of the source sensor, the Sensor Factory does not show the Warning status. This is because the Sensor Factory sensor should only show this status if it cannot calculate values.</li> </ul> </li> <li>▪ Use custom formula: Define the status of the Sensor Factory sensor by adding a Status Definition below.</li> </ul>
Status Definition	<p>This setting is only visible if you select Use custom formula <a href="#">above</a>.</p>

Setting	Description
	<p>Define when the sensor switches to the Down status. You can use the <a href="#">status()</a> function in combination with Boolean operations. For advanced users, it is also possible to calculate a status value.</p> <p> For more information, see section <a href="#">Define Sensor Status: status() Function</a> <sup>1767</sup>.</p>
If a Source Sensor Has No Data	<p>Choose how this Sensor Factory sensor reacts if a source sensor referred to in the channel definition does not provide any data (for example, because it is set to the Paused status or does not exist):</p> <ul style="list-style-type: none"> <li>▪ Do not calculate the channels that use the sensor (default): For defined channels that use one or more sensors that deliver no data, no data is shown.</li> <li>▪ Calculate the channels and use zero as source value: If a source sensor that you use in a channel definition does not deliver any data, zero values are filled in instead. The Sensor Factory sensor calculates the channel value and shows it using these zero values.</li> </ul> <p> If a sensor in the channel of a Sensor Factory sensor has no data, the Sensor Factory sensor always shows the Warning status, no matter which of the above options you select.</p>

## Sensor Display



**Sensor Display**


Primary Channel ⓘ Downtime

---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Define Channels

The channels of a Sensor Factory sensor are controlled by the Channel Definition text field. Using a special syntax, you can refer to other sensors' channels, calculate values, and add horizontal lines. You can define Sensor Factory channels using data from any other sensor's channels on your PRTG core server.

 Make sure that no channel definitions refer to channels of Sensor Factory sensors.

### Example

You see a definition of two Sensor Factory sensor channels. Both use the `channel()` function that collects data from the channels of other sensors in your monitoring and displays them:

```
#1:Local Probe Health
channel(1001,0)
#2:Local Traffic Out[kbit]
channel(1004,1)
```

The first channel of the Sensor Factory sensor (#1) collects data from the Health channel (ID 0) of the Probe Health sensor (ID 1001) running on the probe device. The second channel (#2) collects data from the Traffic Out channel (ID 1) of a traffic sensor (ID 1004) measuring the system's local network card. Both channels are shown together in the Sensor Factory sensor's data tables and graphs.

The basic syntax for a Sensor Factory sensor channel definition looks like this:

```
#<id>:<name>[<unit>]
<formula>
```

For each channel, one section is used. A section begins with the number sign (#). Function names in formulas are not case-sensitive.

The parameters include the following:

- <id> is the ID of the Sensor Factory sensor's channel. It must be a unique number that is greater than 0.
- <name> is the name of the Sensor Factory sensor's channel (displayed in graphs and tables).
- [<unit>] is an optional unit description for the Sensor Factory sensor's channel (for example, bytes). If you do not provide a unit, the Sensor Factory sensor automatically selects a suitable unit string (recommended).
- <formula> contains the formula to calculate the Sensor Factory sensor's channel. For the formula, you can use the following functions: [channel\(\)](#)<sup>[1762]</sup>, [min\(\)](#)<sup>[1763]</sup>, [max\(\)](#)<sup>[1763]</sup>, [avg\(\)](#)<sup>[1764]</sup>, or [percent\(\)](#)<sup>[1764]</sup>.

## Define Channels: channel() Function

The channel() function allows the Sensor Factory sensor to read the data from a channel of a source sensor. The syntax is:

```
channel(<sensorId>,<channelId>)
```

The parameters include the following:

- <sensorId> is the ID of the source sensor. It is displayed on the sensor's Overview tab.
- <channelId> is the ID of the channel of the source sensor. It is displayed in the respective field of the [channel settings](#).

### Example

```
channel(2001,2)
```

This function reads the data from channel ID 2 of the source sensor with the ID 2001.

```
#1:Sample
channel(2001,2)
```

This full channel definition reads the data from channel ID 2 of the source sensor with the ID 2001 and displays it in the first Sensor Factory sensor channel (#1), without any additional calculations.

## Define Channels: Formula Calculations

Within a formula, the following elements are allowed to perform calculations with the values that are returned by one or more functions.



- Basic operations: + (add), - (subtract), \* (multiply), / (divide)  
Example:  $3 + 5 * 2$
- Parentheses: ()  
Example:  $3 * (2 + 6)$
- Compare: = (equal), <> (not equal), > (greater), < (less), >= (greater or equal), <= (less or equal)  
If the comparison resolves to true, the value is **10,000**. If false, the value is **0**. For delta sensors, the speed is compared.

 Example

You see a Sensor Factory sensor channel definition with calculation.

```
#1:Traffic Total x Minus Traffic Out y
( channel(2001,-1) - channel(1004,1) ) * 2
```

This full channel definition results in a Sensor Factory sensor that shows a calculation with values from two channels (channel IDs **-1** and **1**) of two traffic sensors (sensor IDs **2001** and **1004**). The returned values are subtracted and then multiplied by two.

Channels can be gauge values (for example, ping **ms**) or delta values (for example, traffic **kbit/s**). Not all combinations are allowed in a formula.

 When performing percentage calculation, use the [percent\(\) Function](#)<sup>1764</sup> to make sure you obtain the expected values.

There are calculations you **cannot** do:

- You cannot add or subtract a delta from a gauge channel (and vice versa).
- You cannot multiply two delta channels.
- You cannot compare a delta with a gauge channel.
- You cannot use a channel of (another) Sensor Factory sensor channel in the formula.

## Define Channels: min() and max() Functions

The min() and max() functions return the minimum or maximum of two values. The syntax is:

```
min(<a> , <b> )
max(<a> , <b> )
```

Values for <a> and <b> are either numbers or [channel\(\)](#)<sup>1762</sup> functions.

 Examples

```
min(10,5)
```

This function returns 5, because this is the smaller value out of 10 and 5.

```
min( channel(2001,1),channel(2002,1) )
```

This function returns the minimum of the values of channel 1 of the source sensor with ID 2001 and channel 1 of the source sensor with ID 2002.

### Define Channels: avg() Function

The avg() function returns the average of the two values. This equals:  $(a+b) / 2$ . The syntax is:

```
avg(<a>,<b>)
```

Values for <a> and <b> are either numbers or [channel\(\)](#)<sup>[1762]</sup> functions.

 Examples

```
avg(20,10)
```

This function returns 15:  $(20+10) / 2 = 15$ .

```
avg( channel(2001,1),channel(2002,1) )
```

This function returns the average of channel 1 of the source sensor with ID 2001 and channel 1 of the source sensor with ID 2002.

### Define Channels: percent() Function

The percent() function calculates the percent value of two specified values, for example, a channel and a fixed value. The syntax is:

```
percent(<source>,<maximum>,<unit>)
```

The parameters include the following:

- <source> is the value the percent is calculated for. This is usually a [channel\(\)](#)<sup>[1762]</sup> function.
- <maximum> is the limit value used for the percent calculation.
- <unit> is an optional unit the maximum is provided in. You can use constants with this function (see [Define Channels: Constants](#)<sup>[1766]</sup> below for a list). This can be used for absolute values (for example, [Ping sensors](#)<sup>[1594]</sup>) or calculated delta values (for example, traffic sensors). If no unit is provided, 1 is used.
  - ① The sensor adds the unit string % automatically.

PRTG calculates:  $\text{<source> / <maximum> * <unit> * 100}$

 Examples

```
#1:Usage Traffic In
percent(channel(2001,0),100,kilobit)
#2:Usage Traffic Out
percent(channel(2001,1),100,kilobit)
```

This full channel definition results in a Sensor Factory sensor that shows two channels of a traffic sensor (sensor ID [2001](#)): Traffic in (channel ID [0](#)) and traffic out (channel ID [1](#)). The Sensor Factory sensor displays the values % of maximum bandwidth (100 kilobit/second).

```
#1:Ping %
percent(channel(2002,0),200)
```

This full channel definition results in a Sensor Factory sensor that shows the Ping Time channel (channel ID [0](#)) of a Ping sensor (sensor ID [2002](#)). The sensor displays the values as a percentage of 200 ms.

## Define Channels: Horizontal Lines

You can add lines to the graph using a formula without the channel() function. Use a fixed value instead. The syntax is:

```
#<id>:<name>[<unit>]
<value>
```

The parameters include the following:

- **<id>** is the ID of the Sensor Factory sensor's channel and must be a unique number greater than 1. Although the Sensor Factory sensor does not show a horizontal line as a channel, the ID has to be unique.
- **<name>** is the name of the Sensor Factory sensor's channel. PRTG does not display this name in graphs and tables, but you can use it as a comment to describe the nature of the line.
- **[<unit>]** is an optional unit description (for example, [kbit/s](#)). If you do not provide a unit, PRTG automatically applies the line to the scale of the first Sensor Factory sensor's channel. If your Sensor Factory sensor uses different units, provide a unit to make sure the line is added for the right scale. Enter the unit exactly as shown in your graph's legend. If you enter a unit that does not yet exist in your graph, a new scale is added automatically.
- **<value>** contains a number defining where the line is shown in the graph.

### Examples

```
#5:Line at 100ms [ms]
100
```

This channel definition results in a graph that shows a horizontal line at the value of 100 on the ms scale.

```
#6:Line at 2 Mbit/s [kbit/s]
2000
```

This channel definition results in a graph that shows a horizontal line at the value of 2000 on the kbit/s scale.

```
#1:Ping Time
channel(2002,0)
#2:Line at 120ms [ms]
120
```

This full channel definition results in a Sensor Factory sensor that shows the Ping Time channel (channel ID 0) of a Ping sensor (sensor ID 2002). Additionally, the sensor graphs show a horizontal line at 120 ms.

## Define Channels: Constants

The following constants are defined and can be used in calculations:

- one = 1
- kilo = 1000
- mega = 1000 \* kilo
- giga = 1000 \* mega
- tera = 1000 \* giga
- byte = 1
- kilobyte = 1024
- megabyte = 1024 \* kilobyte
- gigabyte = 1024 \* megabyte
- terabyte = 1024 \* gigabyte
- bit = 1/8
- kilobit = kilo / 8
- megabit = mega / 8
- gigabit = giga / 8
- terabit = tera / 8

## Define Sensor Status: status() Function

You can control the status of a Sensor Factory sensor via the Status Definition text field if you enable the custom formula option in the [sensor settings](#)<sup>1758</sup>. Using a special syntax, you can define when the Sensor Factory sensor changes to the Down status. In all other cases, the sensor is in the Up status. The syntax is:

```
status(sensorID) <boolean> status(sensorID)
```

The parameters include the following:

- <sensorid> is the ID of the source sensor that you want to check the status of. It is displayed on the sensor's Overview tab.
- <boolean> is one of the Boolean operators AND, OR, or NOT. If the resulting expression is **true**, the Sensor Factory sensor changes to the Down status.

### Examples

```
status(2031) AND status(2044)
```

This changes the Sensor Factory sensor to the Down status if both source sensors, with IDs **2031** and **2044**, are in the Down status. Otherwise the Sensor Factory sensor shows the Up status.

```
status(2031) OR status(2044)
```

This changes the Sensor Factory sensor to the Down status if at least one of the source sensors with ID **2031** or ID **2044** is in the Down status. Otherwise the Sensor Factory sensor shows the Up status.

```
status(2031) AND NOT status(2044)
```

This changes the Sensor Factory sensor to the Down status if the source sensor with ID **2031** is in the Down status, but the source sensor with ID **2044** is **not** in the Down status. Otherwise the Sensor Factory sensor shows the Up status.

**i** A status() function with NOT has to be connected with AND or OR if it is combined with other status() functions:

```
status(sensorID) AND NOT status(sensorID)
status(sensorID) OR NOT status(sensorID)
```

```
( status(2031) AND status(2044) ) OR status(2051)
```

This changes the Sensor Factory sensor to the Down status if both the source sensor with ID **2031** and the source sensor with ID **2044** are in the Down status, or if the source sensor with ID **2051** is in the Down status. Otherwise the Sensor Factory sensor shows the Up status.

Additionally, the following elements are allowed to perform calculations and comparisons with the values that are returned by the status functions:

- Basic operations: + (add), - (subtract), \* (multiply), / (divide)  
Example: **3 + 5 \* 2**

- Parentheses: ( )  
Example:  $3 * (2 + 6)$
- Compare: = (equal), <> (not equal), > (greater), < (less), >= (greater or equal), <= (less or equal)  
If the comparison resolves to true, the value is 10,000. If false, the value is 0. For delta sensors, the speed is compared.

Internally, the status() function returns the Downtime channel of the source sensor in hundreds of percent (10,000 = 100%).


- true corresponds to a value of 10,000, which is the Down status.
- false corresponds to a value of 0, which is the Up status.

If you understand this, you can use more complex formulas.

 Example

```
( status(1031) + status(1032) + status(1033) + status(1034) ) >= 20000
```

This changes the Sensor Factory sensor to the Down status if at least any two of the source sensors with IDs 1031, 1032, 1033, or 1034 are in the Down status. Otherwise the Sensor Factory sensor shows the Up status.

 You can also use the status() function in [channel definitions](#). Using this functionality, it is possible, for example, to display the numeric status value of source sensors in a Sensor Factory sensor channel.

## Using Sensor Factory Sensors in a Cluster


If you run PRTG in a [failover cluster](#), note the following:

- If you add a Sensor Factory sensor underneath the [cluster probe](#), and in the Sensor Factory formula you refer to a channel of a source sensor running on the cluster probe as well, the Sensor Factory sensor shows the data of all cluster nodes for this channel.
- If you add a Sensor Factory sensor underneath the [local probe](#), and in the Sensor Factory formula you refer to a channel of a sensor running on the cluster probe, the Sensor Factory sensor only shows data of the primary master node for this channel.

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
[Custom]	The monitoring results from other sensors or devices. Samples for usage are: <ul style="list-style-type: none"> <li>▪ Show single channels of one or more sensors in one graph.</li> </ul>

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Use the data from single channels of one or more sensors to calculate new values (for example, you can subtract, multiply, and divide).</li> <li>▪ Create graphs with data from other sensors' channels and add horizontal lines at specific vertical positions.</li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p> <p> The Sensor Factory sensor does not show values in the Downtime channel because they cannot be calculated for this sensor.</p>

## More

### KNOWLEDGE BASE

How can I monitor the overall status of the business process "email"?

- <https://kb.paessler.com/en/topic/60737>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Can you help me understand when the Sensor Factory sensor changes to the down status and why?

- <https://kb.paessler.com/en/topic/79458>

What can I do with the Sensor Factory sensors of PRTG?

- <https://kb.paessler.com/en/topic/583>

### VIDEO TUTORIAL

Sensor Factory sensor

- <https://www.paessler.com/support/videos-and-webinars/videos/factory-sensor>

## 7.8.156 sFlow Sensor

The sFlow sensor receives traffic data from an sFlow v5-compatible device and shows the traffic by type. This sensor has several filter options to divide traffic into different channels.

- ❗ Make sure that the target device supports sFlow v5.
- ℹ This sensor analyzes only header traffic.

✓ **Sensor sFlow** ★★★★★  
OK

Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings

**Top Talkers**

**Top Connections**

**Top Protocols**

[Add Toplist](#)

**Total**

14 Mbit/s

Chat

0 Mbit/s

Citrix

0 Mbit/s

FTP/P2P

0.02 Mbit/s

Infrastructure

0.93 Mbit/s

Mail

0.10 Mbit/s

NetBIOS

< 0.01 Mbit/s

Other

0 Mbit/s

Remote Control

0 Mbit/s

Various

8.10 Mbit/s

**www**

5.15 Mbit/s

Channel ▾	ID ▾	Last Value (volume) ▾	Last Value (speed) ▾	Minimum ▾	Maximum ▾	⚙
Chat	3004	0 MByte	0 Mbit/s	0 Mbit/s	0.54 Mbit/s	⚙
Citrix	3010	0 MByte	0 Mbit/s	0 Mbit/s	< 0.01 Mbit/s	⚙
Downtime	-4					⚙
FTP/P2P	3002	0.61 MB...	0.02 Mbi...	0 Mbit/s	0.49 Mbit/s	⚙
Infrastructure	3007	33 MByte	0.93 Mbi...	0 Mbit/s	3.32 Mbit/s	⚙

sFlow Sensor

■ For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

1770



## Sensor in Other Languages

- Dutch: sFlow
- French: sFlow
- German: sFlow
- Japanese: sFlow
- Portuguese: sFlow
- Russian: sFlow
- Simplified Chinese: sFlow
- Spanish: sFlow

## Remarks

Consider the following [remarks](#)<sup>[1771]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
sFlow	This sensor requires that the sFlow v5 export is enabled on the target system. The target system must send the flow data stream to the IP address of the probe system.
Cluster probe	This sensor does not support cluster probes. You can only set it up on local probes or remote probes.
IPv4	This sensor only supports IPv4.
RAW data	This sensor accepts RAW data only. The stream must be sent via IPv4.
Limitations	This sensor has several <a href="#">limitations</a> <sup>[1772]</sup> .
Clone sensor	If you clone this sensor to the <b>same</b> probe, PRTG keeps the <a href="#">selected IP addresses</a> <sup>[1773]</sup> on which it listens for Flow (NetFlow, jFlow, sFlow, IPFIX) packets. If you clone this sensor to a <b>different</b> probe, PRTG selects <b>all</b> available IP addresses by default.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">How can I change the default groups and channels for flow and Packet Sniffer sensors?</a></li> <li>▪ Knowledge Base: <a href="#">Where is the volume line in graphs?</a></li> </ul>

Remark	Description
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Limitations

There are some limitations that you should consider before you use this sensor:

- This sensor only supports sFlow v5 datagrams.
- This sensor only supports IPv4 flows.
- This sensor only supports the "raw packet header" format.
- This sensor only supports the "Flow sample" and "Extended flow" formats. It cannot process "Counter" formats.
- This sensor only processes samples where the source ID matches the ifIndex of the input interface (avoiding double-counted traffic) and ascending sequence numbers.
- This sensor only supports sample packets of the Ethernet type "IP" (with optional VLAN tag)
- This sensor only supports sampled packets of the types TCP and UDP.

✂ We recommend that you use [sFlow Tester](#) for debugging.

## Basic Sensor Settings

**Basic Sensor Settings**

Sensor Name ⓘ Example Name

Tags ⓘ  ✕ ⊕

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- bandwidthsensor
- sflowsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## sFlow v5 Specific Settings

### sFlow v5 Specific Settings

Receive Packets on UDP Port ⓘ

---

Sender IP Address ⓘ

---

Receive Packets on IP Address ⓘ

<input checked="" type="checkbox"/>	<input type="checkbox"/> Probe's Local IP Addresses
<input checked="" type="checkbox"/>	<input type="text" value="192.0.2.0"/>

---

Stream Data Handling ⓘ

Discard stream data (default)

Store stream data only for the 'Other' channel

Store all stream data

sFlow v5 Specific Settings

Setting	Description
Receive Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the UDP port number in the sFlow export options of the hardware router device. The default port is <b>6343</b> . Enter an integer.
Sender IP Address	Enter the IP address of the sending device that you want to receive the sFlow from. Enter an IP address to only receive data from a specific device or leave the field empty to receive data from any device on the specified port.
Receive Packets on IP Address	<p>Select the IP addresses on which PRTG listens to sFlow packets. The list of IP addresses is specific to your setup. To select an IP address, enable a check box in front of the respective line. The IP address that you select must match the IP address in the sFlow export options of the hardware router device.</p> <p><b>i</b> When you configure the export, make sure that you select the appropriate sFlow v5 for this sensor</p> <p><b>i</b> You can also select all items or cancel the selection by using the check box in the table header.</p>
Stream Data Handling	<p>Define what PRTG does with the stream and packet data:</p> <ul style="list-style-type: none"> <li>▪ Discard stream data (default): Do not store the stream and packet data.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Store stream data only for the 'Other' channel: Only store stream and packet data that is not otherwise filtered and is therefore accounted to the default Other channel. PRTG stores this data in the \StreamLog subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Streams Sensor [ID] (1).csv. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> <li>Store all stream data: Store all stream and packet data. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><b>i</b> Use with caution. It can create huge data files. We recommend that you only use this setting for a short time.</p>

## Channel Configuration

Channel Configuration

Channel Selection ⓘ

Group	✕	✓	🔍	Content
Web	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	WWW Traffic: HTTP, HTTPS
File Transfer	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	File Transfer: FTP (Control)
Mail	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Mail Traffic: IMAP, POP3, SMTP
Chat	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Chat, Instant Messaging: IRC, AIM
Remote Control	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Remote Control: RDP, SSH, Telnet, VNC
Infrastructure	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Network Services: DHCP, DNS, Ident, ICMP, SNMP
NetBIOS	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	NetBIOS: NETBIOS
Citrix	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Citrix: Citrix
Other Protocols	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Various: Other UDP, Other TCP


**Note** You can change the default configuration for groups and channels. This way, you do not have to customize this setting each time that you add this sensor type. For details, see the Knowledge Base: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)

Channel Configuration

Setting	Description
Channel Selection	<p>Define the categories that the sensor accounts the traffic to:</p> <ul style="list-style-type: none"> <li>Web: Internet web traffic.</li> <li>File Transfer: Traffic from FTP.</li> <li>Mail: Internet mail traffic.</li> <li>Chat: Traffic from chat and instant messaging.</li> <li>Remote Control: Traffic from remote control applications such as RDP, SSH, Telnet, and Virtual Network Computing (VNC).</li> <li>Infrastructure: Traffic from network services such as DHCP, DNS, Ident, ICMP, and SNMP.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ NetBIOS: Traffic from NetBIOS communication.</li> <li>▪ Citrix: Traffic from Citrix applications.</li> <li>▪ Other Protocols: Traffic from various other protocols via UDP and TCP.</li> </ul> <p>For each group, you can select how many channels the sensor uses, that is, how detailed the sensor divides the traffic:</p> <ul style="list-style-type: none"> <li>▪ No (✘): Do not account traffic of this group in its own channel. The sensor accounts all traffic of this group to the default channel named Other.</li> <li>▪ Yes (✔): Count all traffic of this group and summarize it in one channel.</li> <li>▪ Detail (🔍): Count all traffic of this group and further divide it into different channels. The traffic appears in several channels that you can see in the Content column. <ul style="list-style-type: none"> <li>ⓘ Extensive use of this option can cause load problems on the probe system. We recommend that you set specific, well-chosen filters for the data that you really want to analyze.</li> </ul> </li> </ul> <p><span style="color: #0070C0;">■</span> You can change the default configuration for groups and channels. For more information, see the Knowledge Base: <a href="#">How can I change the default groups and channels for flow and Packet Sniffer sensors?</a></p>

## Filtering

■ For more information, see section [Filter Rules](#) .

**Filtering**

**Filters** *To include and exclude specific traffic, you can define filter rules based on the following format guidelines:*

- field[filter]

*Fields:*

IP, Port, SourceIP, SourcePort, DestinationIP, DestinationPort, Protocol (values TCP, UDP, ICMP, OSPFIGP or any number), ToS, DSCP

*Additional IPFIX fields:*

Interface, ASI, InboundInterface, OutboundInterface, SourceASI, DestinationASI, MAC, SourceMAC, DestinationMAC, Mask, SourceMask, DestinationMask ('Masks' represent subnet masks in the form of a single number ('number of contiguous bits')), NextHop (IP Address), VLAN, SourceVLAN, DestinationVLAN ('VLANs' represent a VLAN identifier)

Include Filter ⓘ

Exclude Filter ⓘ

Filtering

Setting	Description
Include Filter	Define if you want to filter any traffic. If you leave this field empty, the sensor includes all traffic. To include specific traffic only, define filters using a special <a href="#">syntax</a> .
Exclude Filter	First, the sensor considers the filters in Include Filter. From this subset, you can explicitly exclude traffic, using the same syntax.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Primary Toplist

Primary Toplist

Primary Toplist ⓘ
Top Connections

Primary Toplist

Setting	Description
Primary Toplist	<p>Define which Toplist is the primary Toplist of the sensor:</p> <ul style="list-style-type: none"> <li>▪ Top Talkers</li> <li>▪ Top Connections</li> <li>▪ Top Protocols</li> <li>▪ <a href="#">[Any custom Toplists you add]</a></li> </ul> <p>ⓘ PRTG shows the primary Toplist in maps when you add a Toplist object.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Toplists

For all Flow (NetFlow, jFlow, sFlow, IPFIX) and Packet Sniffer sensors, Toplists are available on the sensor's Overview tab. Using Toplists, you can review traffic data for small time periods in great detail.

■ For more information, see section [Toplists](#).

## Filter Rules

■ For more information, see section [Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Chat	The traffic from chat and instant messaging (IRC, AIM)
Citrix	The traffic from Citrix applications
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
FTP/P2P	The traffic from file transfer (FTP/P2P)
Infrastructure	The traffic from network services (DHCP, DNS, Ident, ICMP, SNMP)
Mail	The internet mail traffic (IMAP, POP3, SMTP)
NetBIOS	The traffic from NetBIOS communication
Other	The traffic from various other protocols (UDP, TCP)
Remote Control	The traffic from remote control applications (RDP, SSH, Telnet, Virtual Network Computing (VNC))
Total	The total traffic <span>ⓘ</span> This channel is the primary channel by default.
Various	The traffic from various other sources
WWW	The traffic from the web (HTTP, HTTPS)

## More

### ■ KNOWLEDGE BASE

How can I change the default groups and channels for flow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>



 PAESSLER TOOLS

sFlow Tester

- <https://www.paessler.com/tools/sflowtester>

## 7.8.157 sFlow (Custom) Sensor

The sFlow (Custom) sensor receives traffic data from an sFlow v5-compatible device and shows the traffic by type. With this sensor, you can define your own channel definitions to divide traffic into different channels.

- ❗ Make sure that the target device supports sFlow v5.
- ℹ This sensor analyzes only header traffic.

✓ **Sensor sFlow (Custom)** ★★★★☆  
OK

Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings

Top Talkers

Top Connections

Top Protocols

Add Toplist

**Total**

14 Mbit/s

Chat		Citrix		FTP/P2P	
0 Mbit/s		0 Mbit/s		0.02 Mbit/s	
Infrastructure		Mail		NetBIOS	
0.93 Mbit/s		0.10 Mbit/s		< 0.01 Mbit/s	
Other		Remote Control		Various	
0 Mbit/s		0 Mbit/s		8.10 Mbit/s	

www

5.15 Mbit/s

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	
Chat	3004	0 MByte	0 Mbit/s	0 Mbit/s	0.54 Mbit/s	
Citrix	3010	0 MByte	0 Mbit/s	0 Mbit/s	< 0.01 Mbit/s	
Downtime	-4					
FTP/P2P	3002	0.61 MB...	0.02 Mbi...	0 Mbit/s	0.49 Mbit/s	
Infrastructure	3007	33 MByte	0.93 Mbi...	0 Mbit/s	3.32 Mbit/s	

sFlow (Custom) Sensor


■ For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1787</sup>.

## Sensor in Other Languages

- Dutch: sFlow (Custom)
- French: sFlow personnalisé
- German: sFlow (Benutzerdef.)
- Japanese: sFlow( カスタム)
- Portuguese: sFlow (customizado)
- Russian: sFlow (нестандартный)
- Simplified Chinese: sFlow (自定义)
- Spanish: sFlow (personalizado)

## Remarks

Consider the following [remarks](#)<sup>1781</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
sFlow	This sensor requires that the sFlow v5 export is enabled on the target system. The target system must send the flow data stream to the IP address of the probe system.
RAW data	This sensor accepts RAW data.
Limitations	This sensor has several <a href="#">limitations</a> <sup>1781</sup> .
Cluster probe	This sensor does not support cluster probes. You can only set it up on local probes or remote probes.
IPv4	This sensor only supports IPv4.
Channels	This sensor does not officially support more than <b>50 channels</b> .
Knowledge Base	Knowledge Base: <a href="#">Where is the volume line in graphs?</a>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Limitations

There are some limitations that you should consider before you use this sensor:

- This sensor only supports sFlow v5 datagrams.
- This sensor only supports IPv4 flows.
- This sensor only supports the "raw packet header" format.
- This sensor only supports the "Flow sample" and "Extended flow" formats. It cannot process "Counter" formats.
- This sensor only processes samples where the source ID matches the ifIndex of the input interface (avoiding double-counted traffic) and ascending sequence numbers.
- This sensor only supports sample packets of the Ethernet type "IP" (with optional VLAN tag)
- This sensor only supports sampled packets of the types TCP and UDP.

✂ We recommend that you use [sFlow Tester](#) for debugging.

## Basic Sensor Settings

Basic Sensor Settings

Sensor Name ⓘ Example Name

---

Tags ⓘ  ✕ ⊕

---

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- bandwidthsensor
- sflowsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## sFlow v5 Specific Settings

### sFlow v5 Specific Settings

Receive Packets on UDP Port ⓘ

---

Sender IP Address ⓘ

---

Receive Packets on IP Address ⓘ

<input checked="" type="checkbox"/>	Probe's Local IP Addresses
<input checked="" type="checkbox"/>	192.0.2.0

---

Channel Definition ⓘ

---

Stream Data Handling ⓘ

Discard stream data (default)

Store stream data only for the 'Other' channel

Store all stream data

sFlow v5 Specific Settings

Setting	Description
Receive Packets on UDP Port	<p>Enter the UDP port number on which the flow packets are received. It must match the UDP port number in the sFlow export options of the hardware router device. The default port is <b>6343</b>. Enter an integer.</p> <p><span style="color: red;">❗</span> When you configure the export, make sure that you select the appropriate sFlow v5 for this sensor</p>
Sender IP Address	<p>Enter the IP address of the sending device that you want to receive the sFlow from. Enter an IP address to only receive data from a specific device or leave the field empty to receive data from any device on the specified port.</p>
Receive Packets on IP Address	<p>Select the IP addresses on which PRTG listens to sFlow packets. The list of IP addresses is specific to your setup. To select an IP address, enable a check box in front of the respective line. The IP address that you select must match the IP address in the sFlow export options of the hardware router device.</p> <p><span style="color: red;">❗</span> When you configure the export, make sure that you select the appropriate sFlow v5 for this sensor</p> <p><span style="color: red;">❗</span> You can also select all items or cancel the selection by using the check box in the table header.</p>

Setting	Description
Channel Definition	<p>Enter a channel definition to divide the traffic into different channels. Enter each definition in one line. The sensor accounts all traffic that you do not define a channel for to the default channel Other.</p> <ul style="list-style-type: none"> <li><span style="color: #0070C0;">■</span> For more information, see section <a href="#">Channel Definitions for Flow, IPFIX and Packet Sniffer Sensors</a>.</li> <li><span style="color: #C00000;">i</span> Extensive use of many filters can cause load problems on the probe system. We recommend that you define specific, well-chosen filters for the data that you really want to analyze. We recommend that you do not use more than 20 channels in graphs and tables, and not more than 100 channels in total. For performance reasons, we recommend that you add several sensors with fewer channels each.</li> </ul>
Stream Data Handling	<p>Define what PRTG does with the stream and packet data:</p> <ul style="list-style-type: none"> <li>▪ Discard stream data (default): Do not store the stream and packet data.</li> <li>▪ Store stream data only for the 'Other' channel: Only store stream and packet data that is not otherwise filtered and is therefore accounted to the default Other channel. PRTG stores this data in the \StreamLog subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Streams Sensor [ID] (1).csv. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> <li>▪ Store all stream data: Store all stream and packet data. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <ul style="list-style-type: none"> <li><span style="color: #C00000;">i</span> Use with caution. It can create huge data files. We recommend that you only use this setting for a short time.</li> </ul>

## Filtering

■ For more information, see section [Filter Rules](#) 1787.

**Filtering**

**Filters** To include and exclude specific traffic, you can define filter rules based on the following format guidelines:

- field[filter]

**Fields:**

IP, Port, SourceIP, SourcePort, DestinationIP, DestinationPort, Protocol (values TCP, UDP, ICMP, OSPFIGP or any number), ToS, DSCP

**Additional IPFIX fields:**

Interface, ASI, InboundInterface, OutboundInterface, SourceASI, DestinationASI, MAC, SourceMAC, DestinationMAC, Mask, SourceMask, DestinationMask ('Masks' represent subnet masks in the form of a single number ('number of contiguous bits')), NextHop (IP Address), VLAN, SourceVLAN, DestinationVLAN ('VLANs' represent a VLAN identifier)

Include Filter ⓘ

Exclude Filter ⓘ

Filtering

Setting	Description
Include Filter	Define if you want to filter any traffic. If you leave this field empty, the sensor includes all traffic. To include specific traffic only, define filters using a special <a href="#">syntax</a> .
Exclude Filter	First, the sensor considers the filters in Include Filter. From this subset, you can explicitly exclude traffic, using the same syntax.

## Sensor Display


**Sensor Display**

Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display


Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.  ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.
Graph Type	Define how this sensor shows different channels:

Setting	Description
	<ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Primary Toplist


**Primary Toplist** Primary Toplist ⓘ Top Connections

Primary Toplist

Setting	Description
Primary Toplist	<p>Define which Toplist is the primary Toplist of the sensor:</p> <ul style="list-style-type: none"> <li>Top Talkers</li> <li>Top Connections</li> <li>Top Protocols</li> <li><a href="#">[Any custom Toplists you add]</a></li> </ul> <p> PRTG shows the primary Toplist in maps when you add a Toplist object.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).



## Toplists

For all Flow (NetFlow, jFlow, sFlow, IPFIX) and Packet Sniffer sensors, Toplists are available on the sensor's Overview tab. Using Toplists, you can review traffic data for small time periods in great detail.

■ For more information, see section [Toplists](#).

## Filter Rules

■ For more information, see section [Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
[Custom]	The traffic by type according to the channel definition
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Other	All traffic for which no channel is defined
Total	The total traffic ⓘ This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

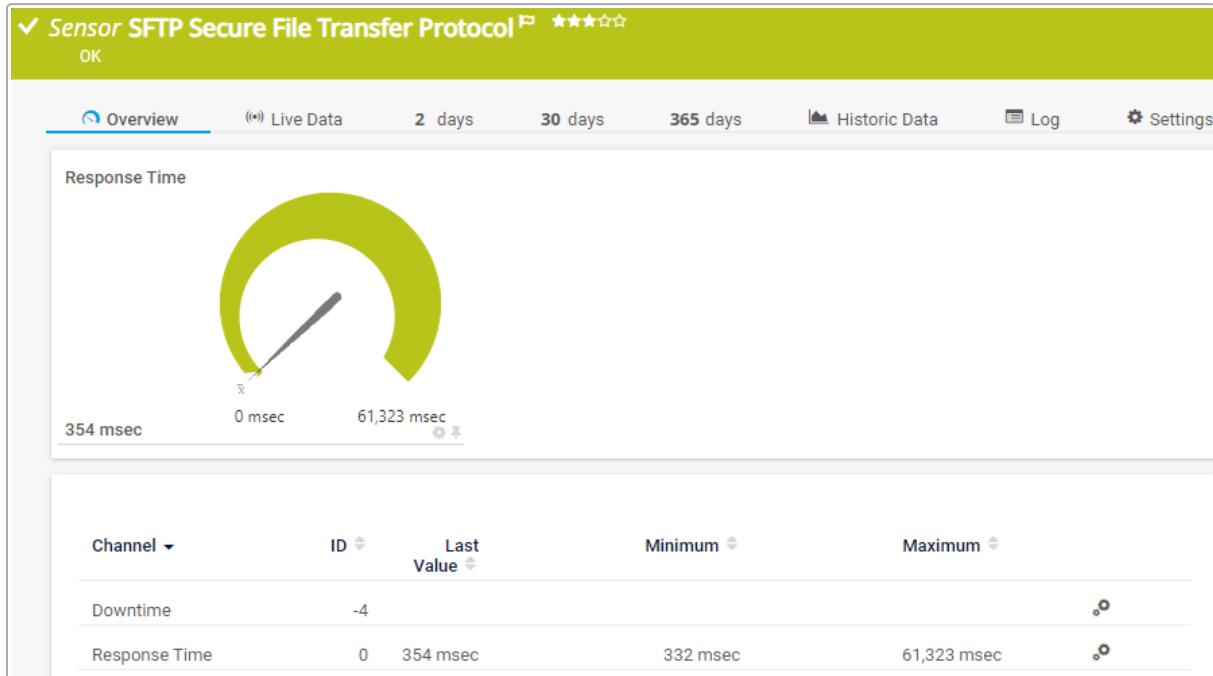
### ✂ PAESSLER TOOLS

sFlow Tester

- <https://www.paessler.com/tools/sflowtester>

## 7.8.158 SFTP Secure File Transfer Protocol Sensor

The SFTP Secure File Transfer Protocol sensor monitors File Transfer Protocol (FTP) servers of a Linux/Unix system via the Secure Shell (SSH) File Transfer Protocol (FTP over SSH).



SFTP Secure File Transfer Protocol Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SFTP Secure File Transfer Protocol
- French: Protocole sécurisé de transfert de fichiers (SFTP)
- German: SFTP Secure File Transfer Protocol
- Japanese: SFTP( Secure File Transfer Protocol)
- Portuguese: SFTP Secure File Transfer Protocol
- Russian: Защищенный протокол передачи файлов SFTP
- Simplified Chinese: SFTP 安全文件传输协议
- Spanish: SFTP Secure File Transfer Protocol

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for Linux/Solaris/macOS (SSH/WBEM) systems in the settings of the parent device.
Distributions	This sensor does not support all Linux/Unix and macOS distributions.
Performance impact	This sensor has a <b>medium</b> performance impact.
IPv4	This sensor only supports IPv4.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">Which encryption algorithms do PRTG SSH sensors support?</a></li> <li>Knowledge Base: <a href="#">SSH and SFTP sensors in Unknown status</a></li> </ul>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- sftpsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## SSH Specific

**SSH Specific**

Connection Timeout (Sec.) ⓘ 60

---

Shell Timeout (Sec.) ⓘ 10

---





SSH Port Inheritance ⓘ  Inherit port from parent device (default)  
 Do not inherit port (enter a custom SSH port)

SSH Engine ⓘ  Inherit from parent device (default)  
 Default  
 Compatibility mode (deprecated)

Result Handling ⓘ  Discard result (default)  
 Store result  
 Store result in case of error

SSH Specific

Setting	Description
Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time that the sensor waits to establish a connection to the host. Keep this value as low as possible. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p> ⓘ Make sure that the connection timeout is a value that is higher than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (for example, <a href="#">cat /proc/loadavg</a>). The maximum value is 300 seconds (5 minutes). Enter an integer.</p> <p> ⓘ Make sure that the shell timeout is a value that is lower than the connection timeout to avoid potential errors.</p>
SSH Port Inheritance	<p>Define which port this sensor uses for the SSH connection:</p> <ul style="list-style-type: none"> <li>▪ Inherit port from parent device (default): Use the port number as defined in the <a href="#">Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems</a> section of the parent device settings.</li> <li>▪ Do not inherit port (enter a custom SSH port): Define a custom port number below and do not use the port number from the parent device settings.</li> </ul>

Setting	Description
Custom SSH Port	<p>This setting is only visible if you select Do not inherit port (enter a custom SSH port) <a href="#">above</a>.</p> <p>Enter the port number (between 1 and 65535) that this sensor uses for the SSH connection. Enter an integer.</p>
SSH Engine	<p>Select the SSH engine that you want to use to <a href="#">access data with this SSH sensor</a>:</p> <ul style="list-style-type: none"> <li>▪ Inherit from parent device (default): Use the SSH engine that you defined in the parent device settings or higher up in the <a href="#">object hierarchy</a>. If you have not changed the SSH engine, this is the recommended option.</li> <li>▪ Default: This is the default SSH engine. It provides the best performance and security. It is set by default in objects that are higher up in the hierarchy, so usually you can keep the Inherit from parent device (default) option.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default SSH engine does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions. It is deprecated. We will remove this legacy mode soon, so try to get your SSH sensors to run with the default SSH engine.</li> </ul> <p> We strongly recommend that you use the default SSH engine.</p> <p> The option you select here overrides the selection of the SSH engine in a higher object: a parent device, group, probe, or root.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> <li>▪ Store result in case of error: Store the last sensor result only if the sensor shows the Down status.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Response Time	The response time  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

Which encryption algorithms do PRTG SSH sensors support?

- <https://kb.paessler.com/en/topic/90689>

SSH and SFTP sensors in Unknown status

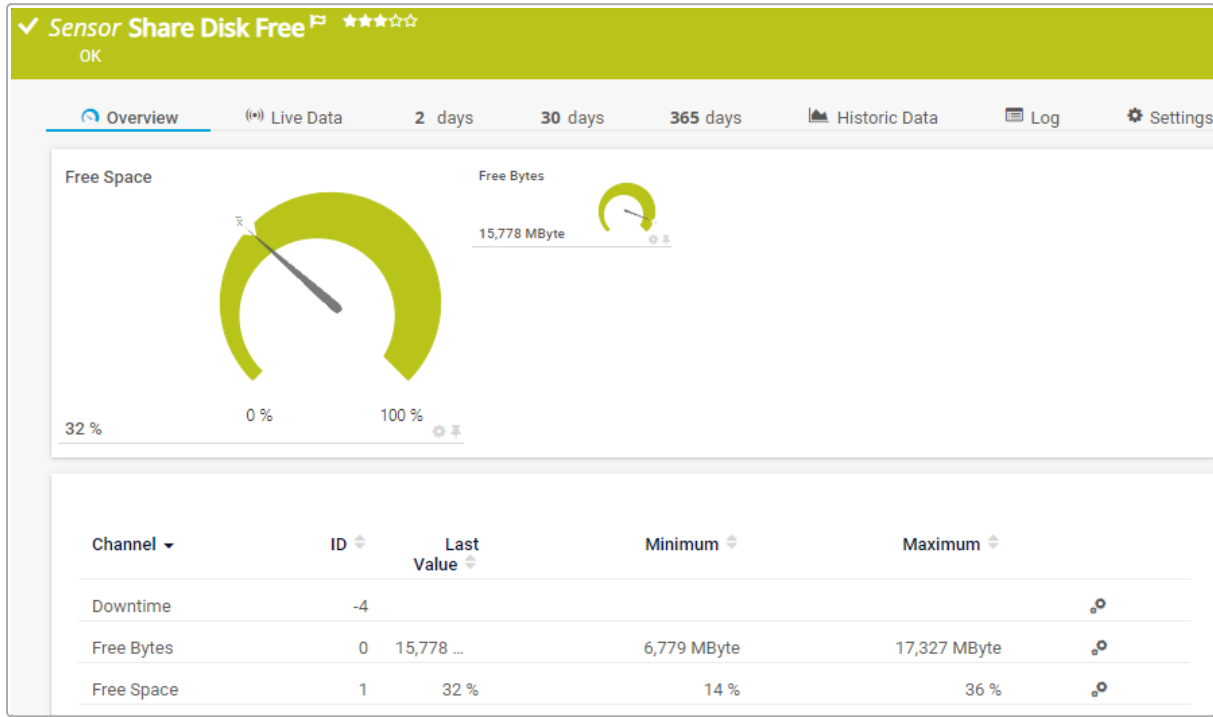
- <https://kb.paessler.com/en/topic/79174>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.159 Share Disk Free Sensor

The Share Disk Free sensor monitors free disk space of a share (Windows/Samba) using Server Message Block (SMB).



Share Disk Free Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Share Disk Ruimte
- French: Espace disponible du disque partagé
- German: Freigaben-Speicherplatz
- Japanese: 共有ディスク空き容量
- Portuguese: Disco livre para compartilhamento
- Russian: Свободное дисковое пространство общего ресурса
- Simplified Chinese: 共享的磁盘可用空间
- Spanish: Espacio libre en disco compartido

### Remarks

Consider the following [remarks](#) and requirements for this sensor:



Remark	Description
LanmanServer service	<p>This sensor requires that the <a href="#">LanmanServer</a> service runs on the target system.</p> <ul style="list-style-type: none"> <li><span style="border: 1px solid black; border-radius: 50%; padding: 2px;">i</span> The display name of the service is <a href="#">Server</a>.</li> <li><span style="border: 1px solid black; border-radius: 50%; padding: 2px;">i</span> To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.</li> </ul>
Quotas	<p>This sensor only works if no quotas are enabled on the target share. If there are quotas enabled for the user account that this sensor uses to connect to the share, the absolute value is okay, but the percentage variable shows incorrect values.</p>
Share name	<p>You can only enter a share name, for example, <a href="#">C\$</a>. Do not enter a complete Universal Naming Convention (UNC) name. The sensor takes the server name <a href="#">\\server\</a> from the parent device.</p>
IPv6	<p>This sensor supports IPv6.</p>
Performance impact	<p>This sensor has a <a href="#">medium</a> performance impact.</p>
Knowledge Base	<p>Knowledge Base: <a href="#">What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032</a></p>
Hosted probe	<p> You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.</p>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ

**Priority** ⓘ

Example Name

---

exampletag x +

---

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- diskspacesensor

- smbdiskspacesensor

For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Share Configuration

Share Configuration
Share ⓘ *share01*

Share Configuration

Setting	Description
Share	The name of the share that this sensor monitors.

## Sensor Display

Sensor Display

Primary Channel ⓘ Downtime


Graph Type ⓘ
 Show channels independently (default)
  Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Bytes	The free space
Free Space	The free space (%)  This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032

- <https://kb.paessler.com/en/topic/513>

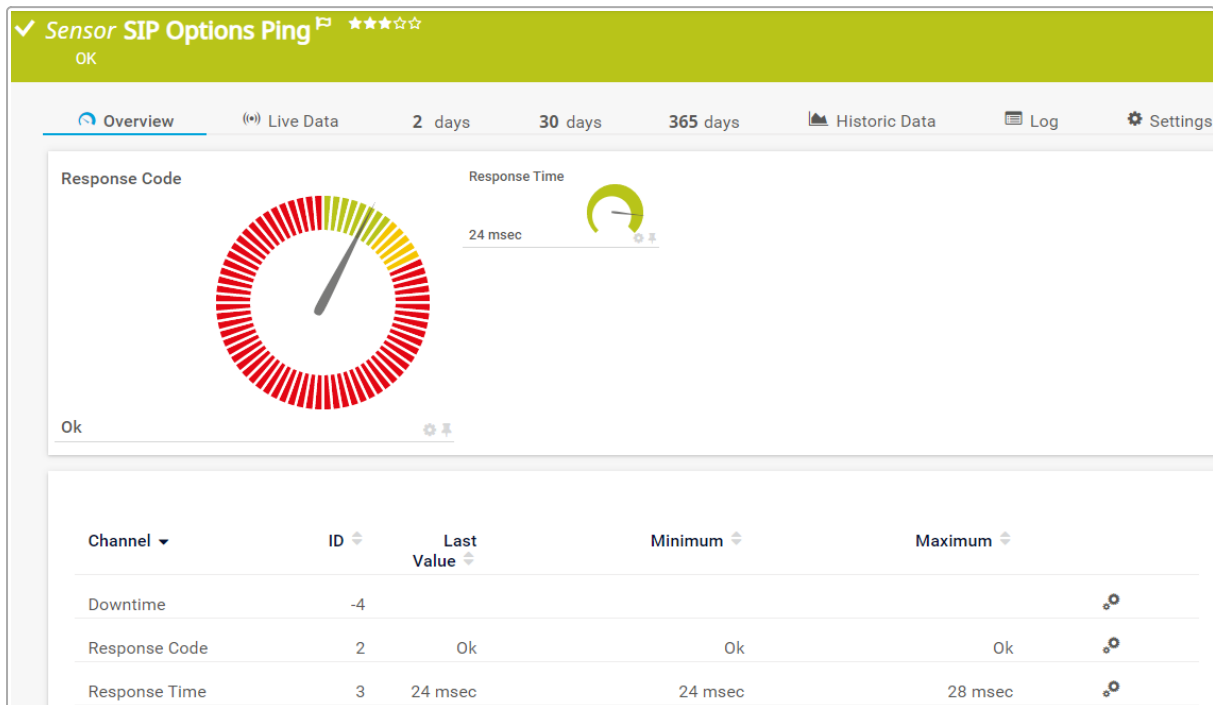
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.160 SIP Options Ping Sensor

The SIP Options Ping sensor monitors the connectivity to a Session Initiation Protocol (SIP) server using SIP options "ping". The sensor sends **auth** and **options** requests to the SIP server.

**i** You can use this sensor to monitor Voice over IP (VoIP) services.



SIP Options Ping Sensor



For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SIP Opties Ping
- French: SIP Options Ping
- German: SIP Options Ping
- Japanese: SIP オプション Ping
- Portuguese: Options SIP Ping
- Russian: Пинг параметров SIP
- Simplified Chinese: SIP 选项 Ping
- Spanish: Opciones SIP Ping

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Error message	An SIP server might return the error ' <a href="#">480 Service temporarily unavailable</a> ' until at least one reachable SIP client is connected to the server.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  X +

**Priority** ⓘ ★★★★☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- pingsensor
- sipsensor

 For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### SIP Specific

#### SIP Specific

**Port** ⓘ

**User Name** ⓘ

**Password** ⓘ

**Timeout (Sec.)** ⓘ

**Retry Count** ⓘ

SIP Specific

Setting	Description
Port	Enter the number of the port to which this sensor connects. Enter an integer. The default User Datagram Protocol (UDP) port is <a href="#">5060</a> .
User Name	Enter the user name of the SIP user account that this sensor logs in to after a successful connection to the SIP server. Enter a string.
Password	Enter the password of the SIP user account that this sensor logs in to after a successful connection to the SIP server. Enter a string.
Timeout (Sec.)	Enter the timeout for the connection to the SIP server. Enter an integer. The maximum timeout value is <a href="#">300</a> seconds (5 minutes).
Retry Count	If the connection to the SIP server fails, the sensor tries to connect again. Enter the maximum number of retries. After the sensor reaches the maximum count, it shows the Down <a href="#">status</a> . Enter an integer.

### Debug Options

#### Debug Options

**Result Handling** ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.



## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Response Code	<p>The response code</p> <ul style="list-style-type: none"> <li> You can individually define the status for each individual response code by editing the <a href="#">lookup</a> file prtg.standardlookups.sip.statuscode.</li> <li> This channel is the primary channel by default.</li> </ul>
Response Time	The response time

## More

### ■ KNOWLEDGE BASE

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

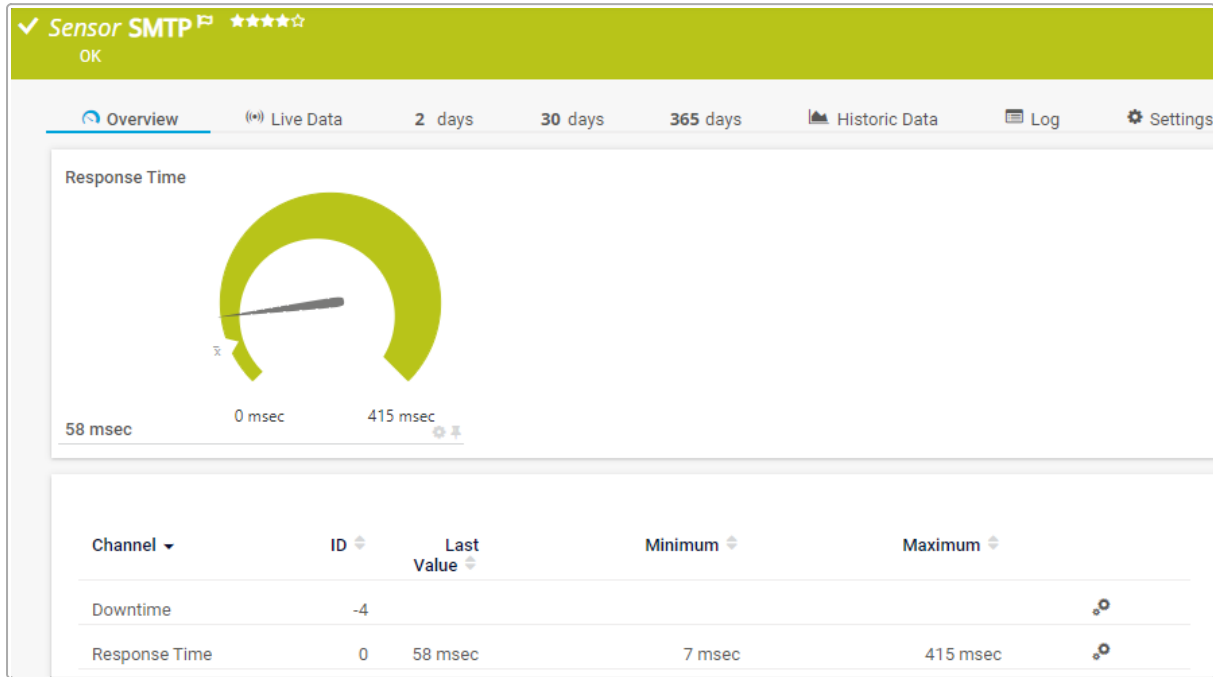
- <https://kb.paessler.com/en/topic/61108>



## 7.8.161 SMTP Sensor

The SMTP sensor monitors a mail server using the Simple Mail Transfer Protocol (SMTP).

**i** The sensor can optionally send a test email with every check.



SMTP Sensor

■ For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1803</sup>.

### Sensor in Other Languages

- Dutch: SMTP
- French: SMTP
- German: SMTP
- Japanese: SMTP
- Portuguese: SMTP
- Russian: SMTP
- Simplified Chinese: SMTP
- Spanish: SMTP

### Remarks

Consider the following [remarks](#)<sup>1803</sup> and requirements for this sensor:

Remark	Description
SRP ciphers	This sensor does not support Secure Remote Password (SRP) ciphers.
IPv4	This sensor only supports IPv4.
Performance impact	This sensor has a <b>low</b> performance impact.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- mailsensor
- smtpsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### SMTP Specific

#### SMTP Specific

**Timeout (Sec.)** ⓘ 60

---

**Port** ⓘ 25

SMTP Specific

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is 900 seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
Port	<p>Enter the number of the port that the sensor uses to send an email via SMTP. The default port for unsecure connections is 25 and the default ports for secure connections are 465 or 587. The actual setting depends on the server that you connect to. Enter an integer.</p> <p><b>i</b> We recommend that you use the default value.</p> <p><b>i</b> If the connection is unsuccessful, try a different port number.</p>

## Authentication

**Authentication**

SMTP Authentication Method **i**  None (default)  User name and password

HELO Ident **i** \_\_\_\_\_

Authentication

Setting	Description
SMTP Authentication Method	<p>Define if you want to use authentication for the SMTP connection:</p> <ul style="list-style-type: none"> <li>None (default): Do not use any authentication method.</li> <li>User name and password: Authenticate against the SMTP server via user name and password.</li> </ul>
User Name	<p>This setting is only visible if you select User name and password above.</p> <p>Enter a user name for SMTP authentication. Enter a string.</p>
Password	<p>This setting is only visible if you select User name and password above.</p> <p>Enter a password for SMTP authentication. Enter a string.</p>
HELO Ident	<p>Enter a server name for the HELO part of the mail protocol.</p>

Setting	Description
	<p><b>i</b> For some mail servers, the HELO identifier must be the valid principal host domain name for the client host. For more information, see <a href="#">SMTP RFC 2821</a>.</p> <p><b>i</b> If you leave this field empty, the value defaults to the computer name.</p> <p><b>i</b> Only ASCII characters are allowed.</p>

## Connection Security

**Connection Security**

Transport-Level Security **i**

Use transport-level security if available using StartTLS  
 Use transport-level security if available  
 Enforce transport-level security using StartTLS  
 Enforce transport-level security (default)

Connection Security

Setting	Description
Transport-Level Security	<p>Define how the sensor handles the security of the connection:</p> <ul style="list-style-type: none"> <li>▪ Use transport-level security if available using StartTLS: Try to connect to the server via a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection and StartTLS. If the server does not support this, the sensor tries to connect without connection security.</li> <li>▪ Use transport-level security if available: Try to connect to the server via an SSL/TLS-secured connection. If the server does not support this, the sensor tries to connect without connection security.</li> <li>▪ Enforce transport-level security using StartTLS: Try to connect to the server via an SSL/TLS-secured connection and StartTLS. If the server does not support this, the sensor shows the Down <a href="#">status</a>.</li> <li>▪ Enforce transport-level security (default): Try to connect to the server via an SSL/TLS-secured connection. If the server does not support this, the sensor shows the Down status.</li> </ul> <p><b>i</b> If the sensor connects to a server via StartTLS, the connection is first established without connection security. After the connection has been established, the sensor sends a certain command (<a href="#">StartTLS</a>) over the unsecured connection to negotiate a secure connection via SSL/TLS.</p> <p><b>i</b> If the sensor does <b>not</b> use StartTLS, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If no secure connection is possible, no communication takes place.</p>

## Monitoring

**Monitoring**

**Email Handling** ⓘ  Do not send an email (default)  
 Send an email

**Result Handling** ⓘ  Discard result (default)  
 Store result

Monitoring

Setting	Description
Email Handling	<p>Define the monitoring approach when connecting to the SMTP server:</p> <ul style="list-style-type: none"> <li>▪ Do not send an email (default): Do not send an email, only connect to the SMTP server.</li> <li>▪ Send an email: Send an email through the SMTP server. If there is an error when sending the email, this triggers an error message and the sensor changes to the Down status.</li> </ul>
From	<p><a href="#">This setting is only visible if you select Send an email above.</a></p> <p>Specify the address of the sender of the email. Enter a valid email address.</p>
To	<p><a href="#">This setting is only visible if you select Send an email above.</a></p> <p>Specify the address that PRTG sends the email to. Enter a valid email address.</p> <p> ⓘ If you define more than one recipient, separate the individual email addresses with commas.</p>
Subject	<p><a href="#">This setting is only visible if you select Send an email above.</a></p> <p>Specify the subject that the email contains. Enter a string or leave the field empty.</p>
Content	<p><a href="#">This setting is only visible if you select Send an email above.</a></p> <p>Specify the body that the email contains. Enter a string or leave the field empty.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **ⓘ** Downtime

---


Graph Type **ⓘ**  Show channels independently (default)

Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Response Time	The response time  This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

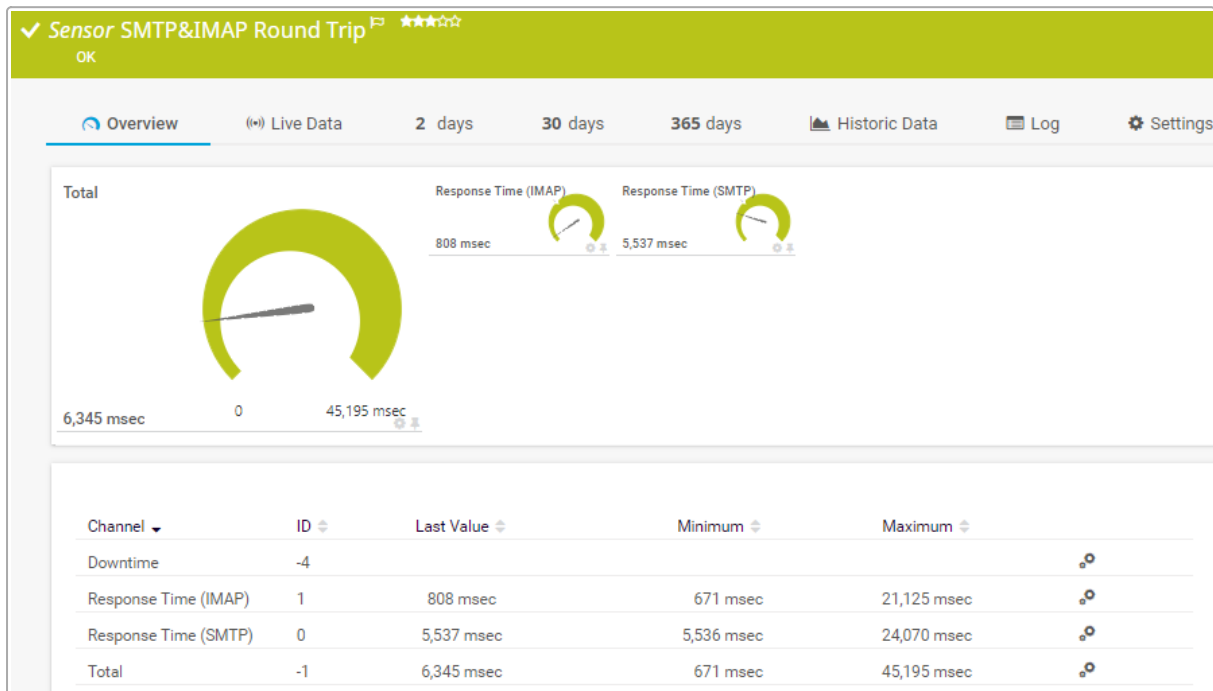
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.162 SMTP&IMAP Round Trip Sensor

The SMTP&IMAP Round Trip sensor monitors the time it takes for an email to reach an Internet Message Access Protocol (IMAP) mailbox using the Simple Mail Transfer Protocol (SMTP). It sends an email via the parent device (an SMTP server) and then scans a dedicated IMAP mailbox until the email arrives.

**i** The SMTP&IMAP Round Trip sensor automatically deletes these emails from the mailbox as soon as PRTG retrieves them. The emails only remain in the mailbox if a timeout or a restart of the PRTG core server occurs during sensor runtime.



SMTP&IMAP Round Trip Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SMTP & IMAP Round Trip
- French: SMTP & IMAP aller-retour
- German: SMTP&IMAP-Übermittlung
- Japanese: SMTP & IMAP ラウンドトリップ
- Portuguese: Ida e volta SMTP&IMAP
- Russian: Цикл SMTP&IMAP
- Simplified Chinese: SMTP 和 IMAP 往返
- Spanish: Ida y vuelta SMTP&IMAP



## Remarks

Consider the following [remarks](#)<sup>[1811]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Parent device	This sensor requires that the parent device is an SMTP server.
SRP ciphers	This sensor does not support Secure Remote Password (SRP) ciphers.
Microsoft 365 mailboxes	This sensor does not support Microsoft 365 mailboxes. If you want to monitor a Microsoft 365 mailbox, use the <a href="#">Microsoft 365 Mailbox</a> <sup>[1252]</sup> sensor.
IPv4	This sensor only supports IPv4.
Dedicated email accounts	Use dedicated email accounts with this sensor. Make sure that each sensor uses its own email accounts.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- `imapsensor`
- `mailsensor`
- `roundtrip`

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Email Settings

**Email Settings**

From ⓘ johnqpublic@example.com

---

To ⓘ janeqpublic@example.com

---

HELO Ident ⓘ mail.example.com

Email Settings

Setting	Description
From	Specify the email address of the email's sender. Enter a valid email address.
To	Specify the address that PRTG sends the emails to. Enter a valid email address. ⓘ You can only enter one email address.
HELO Ident	Enter a server name for the HELO part of the mail protocol. ⓘ For some mail servers, the HELO identifier must be the valid principal host domain name for the client host. For more information, see <a href="#">SMTP RFC 2821</a> . ⓘ Only ASCII characters are allowed.

### Step 1: Send Email Using Parent Device (SMTP Server)

ⓘ In this step, you configure how the sensor sends the emails. The sensor uses the IP Address/DNS Name of the parent device (an SMTP server).

**Step 1: Send Email Using Parent Device (SMTP Server)**

Port ⓘ 25

---

Timeout for SMTP Connection (Sec.) ⓘ 300

---

SMTP Authentication Method ⓘ  None (default)  
 User name and password

---

Additional Text for Email Subject ⓘ

Step 1: Send Email Using Parent Device (SMTP Server)

Setting	Description
Port	<p>Enter the number of the port that the sensor uses to send an email via SMTP. The default port for unsecure connections is <b>25</b> and the default ports for secure connections are <b>465</b> or <b>587</b>. The actual setting depends on the server that you connect to. Enter an integer.</p> <p><b>i</b> We recommend that you use the default value.</p> <p><b>i</b> If the connection is unsuccessful, try a different port number.</p>
Timeout for SMTP Connection (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
SMTP Authentication Method	<p>Define if you want to use authentication for the SMTP connection:</p> <ul style="list-style-type: none"> <li>▪ None (default): Do not use any authentication method.</li> <li>▪ User name and password: Authenticate against the SMTP server via user name and password.</li> </ul>
User Name	<p><b>This setting is only visible if you select User name and password above.</b></p> <p>Enter a user name for SMTP authentication. Enter a string.</p>
Password	<p><b>This setting is only visible if you select User name and password above.</b></p> <p>Enter a password for SMTP authentication. Enter a string.</p>
Additional Text for Email Subject	<p>PRTG automatically creates the subject part of the round trip email. The subject consists of the string <b>PRTG Roundtrip Mail:</b>, followed by a unique globally unique identifier (GUID) to correctly identify the email in the IMAP mailbox, for example, <b>PRTG Roundtrip Mail: {5E858D9C-AC70-466A-9B2A-55630165D276}</b>.</p> <p>Use this field to place your custom text before the automatically created text.</p>

## Connection Security

**Connection Security**

Transport-Level Security **i**

Use transport-level security if available using StartTLS  
 Use transport-level security if available  
 Enforce transport-level security using StartTLS  
 Enforce transport-level security (default)

Connection Security

Setting	Description
Transport-Level Security	<p>Define how the sensor handles the security of the connection:</p> <ul style="list-style-type: none"> <li>▪ Use transport-level security if available using StartTLS: Try to connect to the server via a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection and StartTLS. If the server does not support this, the sensor tries to connect without connection security.</li> <li>▪ Use transport-level security if available: Try to connect to the server via an SSL/TLS-secured connection. If the server does not support this, the sensor tries to connect without connection security.</li> <li>▪ Enforce transport-level security using StartTLS: Try to connect to the server via an SSL/TLS-secured connection and StartTLS. If the server does not support this, the sensor shows the Down <a href="#">status</a>.</li> <li>▪ Enforce transport-level security (default): Try to connect to the server via an SSL/TLS-secured connection. If the server does not support this, the sensor shows the Down status.</li> </ul> <p>ⓘ If the sensor connects to a server via StartTLS, the connection is first established without connection security. After the connection has been established, the sensor sends a certain command (<a href="#">StartTLS</a>) over the unsecured connection to negotiate a secure connection via SSL/TLS.</p> <p>ⓘ If the sensor does <b>not</b> use StartTLS, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If no secure connection is possible, no communication takes place.</p>

## Step 2: Check an IMAP Mailbox until Email Arrives


ⓘ In this step, you configure how to receive the emails that the sensor sends.

## Step 2: Check an IMAP Mailbox until Email Arrives

IP Address/DNS Name ⓘ	www.example.com
Mailbox ⓘ	INBOX
Port ⓘ	993
Connection Interval (Sec.) ⓘ	10
Maximum Trip Time (Sec.) ⓘ	300
User Name ⓘ	johnqpublic
Password ⓘ	.....
Search Method ⓘ	<input checked="" type="radio"/> Search for the email directly (default) <input type="radio"/> Search through all available emails


Step 2: Check an IMAP Mailbox until Email Arrives

Setting	Description
IP Address/DNS Name	Specify the IMAP server. Enter a valid IP address or Domain Name System (DNS) name.
Mailbox	Specify the IMAP mailbox that you want to check. Enter the IMAP mailbox or folder name, for example <b>INBOX</b> .  ⓘ The IMAP mailbox or folder name must <b>not</b> match the sender of the email in the From field. Otherwise, the sensor might incorrectly interpret unsuccessful round trips as successful.
Port	Specify the port that the sensor uses for the IMAP connection. The default port for unsecure connections is <b>143</b> and the default port for secure connections is <b>993</b> . The actual setting depends on the server you connect to.. Enter an integer.  ⓘ We recommend that you use the default value. ⓘ If the connection is unsuccessful, try a different port number.
Connection Interval (Sec.)	Enter the number of seconds the sensor waits between two connections to the IMAP server. PRTG repeatedly checks the mailbox in this scanning interval until the email arrives. Enter an integer.

Setting	Description
Maximum Trip Time (Sec.)	Enter the maximum number of seconds an email can take to arrive in the IMAP mailbox. PRTG continuously checks the mailbox in this scanning interval until the email arrives. If it does not arrive within the maximum trip time, the sensor shows an error message. Enter an integer.
User Name	Enter a user name for IMAP authentication. Enter a string.
Password	Enter a password for IMAP authentication. Enter a string.   The password must <b>not</b> contain spaces, percent signs (%), or the character combination !*.
Search Method	Define how to search for the round trip email in the mailbox: <ul style="list-style-type: none"> <li>▪ Search for the email directly (default): Send a <b>SEARCH</b> command to directly find the round trip email on the IMAP server.</li> <li>▪ Search through all available emails: Search through all available emails in the mailbox locally to find the round trip email. This might take some time if you have many emails in your mailbox.</li> </ul>

## Connection Security

**Connection Security**

IMAP Specific 

Use transport-level security if available using StartTLS (default)

Use transport-level security if available

Enforce transport-level security using StartTLS

Enforce transport-level security

Connection Security

Setting	Description
Transport-Level Security	Define how the sensor handles the security of the connection: <ul style="list-style-type: none"> <li>▪ Use transport-level security if available using StartTLS: Try to connect to the server via a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection and StartTLS. If the server does not support this, the sensor tries to connect without connection security.</li> <li>▪ Use transport-level security if available: Try to connect to the server via an SSL/TLS-secured connection. If the server does not support this, the sensor tries to connect without connection security.</li> <li>▪ Enforce transport-level security using StartTLS: Try to connect to the server via an SSL/TLS-secured connection and StartTLS. If the server does not support this, the sensor shows the Down <a href="#">status</a>.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Enforce transport-level security (default): Try to connect to the server via an SSL/TLS-secured connection. If the server does not support this, the sensor shows the Down status.</li> </ul> <p><b>i</b> If the sensor connects to a server via StartTLS, the connection is first established without connection security. After the connection has been established, the sensor sends a certain command (<a href="#">StartTLS</a>) over the unsecured connection to negotiate a secure connection via SSL/TLS.</p> <p><b>i</b> If the sensor does <b>not</b> use StartTLS, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If no secure connection is possible, no communication takes place.</p>

### Debug Options

**Debug Options**

Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>☁</b> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.



Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Response Time (IMAP)	The response time of the IMAP server
Response Time (SMTP)	The response time of the SMTP server
Total	The sum of the response time of the IMAP server and the SMTP server  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

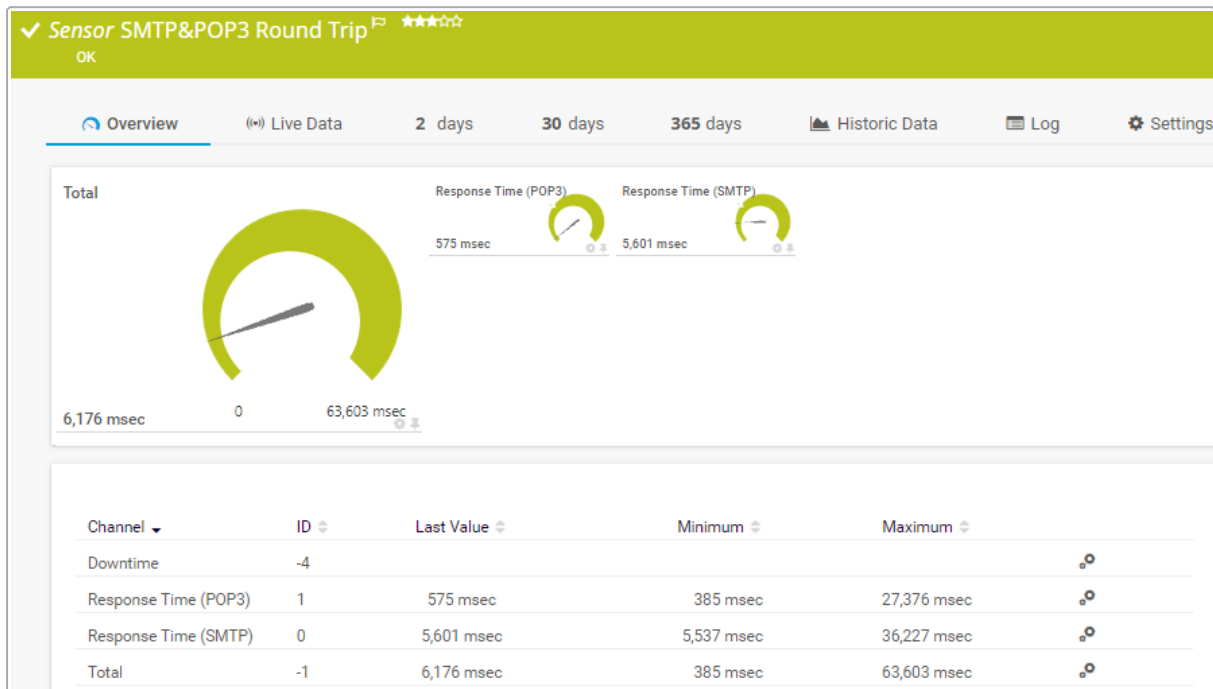
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.163 SMTP&POP3 Round Trip Sensor

The SMTP&POP3 Round Trip sensor monitors the time it takes for an email to reach a Post Office Protocol version 3 (POP3) mailbox using the Simple Mail Transfer Protocol (SMTP). It sends an email using the parent device (an SMTP server) and then scans a dedicated POP3 mailbox until the email comes in.

**i** The SMTP&POP3 Round Trip sensor automatically deletes these emails from the mailbox as soon as PRTG has retrieved them. Emails only remain in the mailbox if a timeout or a restart of the PRTG core server occurs during sensor runtime.



SMTP&POP3 Round Trip Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1820</sup>.

### Sensor in Other Languages

- Dutch: SMTP & POP3 Round Trip
- French: SMTP & POP3 aller-retour
- German: SMTP&POP3-Übermittlung
- Japanese: SMTP&POP3 ラウンドトリップ
- Portuguese: Ida e volta SMTP&POP3
- Russian: Цикл SMTP и POP3
- Simplified Chinese: SMTP 和 POP3 往返
- Spanish: Ida y vuelta SMTP&POP3

## Remarks

Consider the following [remarks](#)<sup>[1821]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Parent device	This sensor requires that the parent device is an SMTP server.
SRP ciphers	This sensor does not support Secure Remote Password (SRP) ciphers.
Microsoft 365 mailboxes	This sensor does not support Microsoft 365 mailboxes. If you want to monitor a Microsoft 365 mailbox, use the <a href="#">Microsoft 365 Mailbox</a> <sup>[1252]</sup> sensor.
IPv4	This sensor only supports IPv4.
Dedicated email accounts	Use dedicated email accounts with this sensor. Make sure that each sensor uses its own email accounts.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- mailsensor
- pop3sensor
- roundtrip

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Email Settings

**Email Settings**

From ⓘ johnqpublic@example.com

---

To ⓘ janeqpublic@example.com

---

HELO Ident ⓘ mail.example.com

Email Settings

Setting	Description
From	Specify the email address of the email's sender. Enter a valid email address.
To	Specify the address that PRTG sends the emails to. Enter a valid email address.  ⓘ You can only enter one email address.
HELO Ident	Enter a server name for the HELO part of the mail protocol.  ⓘ For some mail servers, the HELO identifier must be the valid principal host domain name for the client host. For more information, see <a href="#">SMTP RFC 2821</a> .  ⓘ Only ASCII characters are allowed.

### Step 1: Send Email Using Parent Device (SMTP Server)

ⓘ In this step, you configure how the sensor sends the emails. The sensor uses the IP Address/DNS Name of the parent device (an SMTP server).

**Step 1: Send Email Using Parent Device (SMTP Server)**

Port ⓘ 25

---

Timeout for SMTP Connection (Sec.) ⓘ 300

---

SMTP Authentication Method ⓘ  None (default)  
 User name and password

---

Additional Text for Email Subject ⓘ

Step 1: Send Email Using Parent Device (SMTP Server)

Setting	Description
Port	<p>Enter the number of the port that the sensor uses to send an email via SMTP. The default port for unsecure connections is <b>25</b> and the default ports for secure connections are <b>465</b> or <b>587</b>. The actual setting depends on the server that you connect to. Enter an integer.</p> <p><b>i</b> We recommend that you use the default value.</p> <p><b>i</b> If the connection is unsuccessful, try a different port number.</p>
Timeout for SMTP Connection (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
SMTP Authentication Method	<p>Define if you want to use authentication for the SMTP connection:</p> <ul style="list-style-type: none"> <li>▪ None (default): Do not use any authentication method.</li> <li>▪ User name and password: Authenticate against the SMTP server via user name and password.</li> </ul>
User Name	<p><b>This setting is only visible if you select User name and password above.</b></p> <p>Enter a user name for SMTP authentication. Enter a string.</p>
Password	<p><b>This setting is only visible if you select User name and password above.</b></p> <p>Enter a password for SMTP authentication. Enter a string.</p>
Additional Text for Email Subject	<p>PRTG automatically creates the subject part of the round trip email. The subject consists of the string <b>PRTG Roundtrip Mail:</b>, followed by a unique globally unique identifier (GUID) to correctly identify the email in the IMAP mailbox, for example, <b>PRTG Roundtrip Mail: {5E858D9C-AC70-466A-9B2A-55630165D276}</b>.</p> <p>Use this field to place your custom text before the automatically created text.</p>

## Connection Security

**Connection Security**

Transport-Level Security **i**

Use transport-level security if available using StartTLS  
 Use transport-level security if available  
 Enforce transport-level security using StartTLS  
 Enforce transport-level security (default)

Connection Security

Setting	Description
Transport-Level Security	<p>Define how the sensor handles the security of the connection:</p> <ul style="list-style-type: none"> <li>▪ Use transport-level security if available using StartTLS: Try to connect to the server via a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection and StartTLS. If the server does not support this, the sensor tries to connect without connection security.</li> <li>▪ Use transport-level security if available: Try to connect to the server via an SSL/TLS-secured connection. If the server does not support this, the sensor tries to connect without connection security.</li> <li>▪ Enforce transport-level security using StartTLS: Try to connect to the server via an SSL/TLS-secured connection and StartTLS. If the server does not support this, the sensor shows the Down <a href="#">status</a>.</li> <li>▪ Enforce transport-level security (default): Try to connect to the server via an SSL/TLS-secured connection. If the server does not support this, the sensor shows the Down status.</li> </ul> <p><b>i</b> If the sensor connects to a server via StartTLS, the connection is first established without connection security. After the connection has been established, the sensor sends a certain command (<a href="#">StartTLS</a>) over the unsecured connection to negotiate a secure connection via SSL/TLS.</p> <p><b>i</b> If the sensor does <b>not</b> use StartTLS, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If no secure connection is possible, no communication takes place.</p>

## Step 2: Check a POP3 Mailbox until Email Arrives

**i** In this step, you configure how to receive the sent emails.

**Step 2: Check a POP3 Mailbox until Email Arrives**

<b>IP Address/DNS Name</b> <b>i</b>	<input type="text" value="www.example.com"/>
<b>Port</b> <b>i</b>	<input type="text" value="995"/>
<b>Connection Interval (Sec.)</b> <b>i</b>	<input type="text" value="5"/>
<b>Maximum Trip Time (Sec.)</b> <b>i</b>	<input type="text" value="300"/>
<b>POP3 Authentication Method</b> <b>i</b>	<input checked="" type="radio"/> Without login (default) <input type="radio"/> User name and password <input type="radio"/> 128-bit MD5 hash value (APOP)

Step 2: Check a POP3 Mailbox until Email Arrives

Setting	Description
IP Address/DNS Name	Specify the POP3 server. Enter a valid IP address or Domain Name System (DNS) name.
Port	<p>Specify the port that the sensor uses for the POP3 connection. The default port for unsecure connections is <b>110</b> and the default port for secure connections is <b>995</b>. The actual setting depends on the server you connect to. Enter an integer.</p> <p><b>i</b> We recommend that you use the default value.</p> <p><b>i</b> If the connection is unsuccessful, try a different port number.</p>
Connection Interval (Sec.)	Enter the number of seconds the sensor waits between two connections to the POP3 server. PRTG continuously checks the mailbox in this scanning interval until the email arrives. Enter an integer.
Maximum Trip Time (Sec.)	Enter the maximum number of seconds an email can take to arrive in the POP3 mailbox. PRTG continuously checks the mailbox in the interval that you specify above until the email arrives. If it does not arrive within the maximum trip time, the sensor triggers an error message. Enter an integer.
POP3 Authentication Method	<p>Select the authentication method for the POP3 connection:</p> <ul style="list-style-type: none"> <li>▪ Without login (default): Only monitor the connection to the POP3 server.</li> <li>▪ User name and password: Log in to the POP3 server with user name and password. <ul style="list-style-type: none"> <li><b>i</b> This is a simple login. It is not secure.</li> </ul> </li> <li>▪ 128-bit MD5 hash value (APOP): Send the password in an encrypted form using APOP. <ul style="list-style-type: none"> <li><b>i</b> The POP3 server that you connect to must support this option.</li> </ul> </li> </ul>
User Name	<p><b>This setting is only visible if you select User name and password or 128-bit MD5 hash value (APOP) above.</b></p> <p>Enter a user name for POP3 authentication. Enter a string.</p>
Password	<p><b>This setting is only visible if you select User name and password or 128-bit MD5 hash value (APOP) above.</b></p> <p>Enter a user name for POP3 authentication. Enter a string.</p>

## Connection Security

**Connection Security**

POP3 Specific ⓘ

Use transport-level security if available using StartTLS  
 Use transport-level security if available  
 Enforce transport-level security using StartTLS  
 Enforce transport-level security (default)

Connection Security

Setting	Description
Transport-Level Security	<p>Define how the sensor handles the security of the connection:</p> <ul style="list-style-type: none"> <li>▪ Use transport-level security if available using StartTLS: Try to connect to the server via a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection and StartTLS. If the server does not support this, the sensor tries to connect without connection security.</li> <li>▪ Use transport-level security if available: Try to connect to the server via an SSL/TLS-secured connection. If the server does not support this, the sensor tries to connect without connection security.</li> <li>▪ Enforce transport-level security using StartTLS: Try to connect to the server via an SSL/TLS-secured connection and StartTLS. If the server does not support this, the sensor shows the Down <a href="#">status</a>.</li> <li>▪ Enforce transport-level security (default): Try to connect to the server via an SSL/TLS-secured connection. If the server does not support this, the sensor shows the Down status.</li> </ul> <p>ⓘ If the sensor connects to a server via StartTLS, the connection is first established without connection security. After the connection has been established, the sensor sends a certain command (<a href="#">StartTLS</a>) over the unsecured connection to negotiate a secure connection via SSL/TLS.</p> <p>ⓘ If the sensor does <b>not</b> use StartTLS, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If no secure connection is possible, no communication takes place.</p>

## Debug Options

**Debug Options**

Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options



Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Response Time (POP3)	The response time of the POP3 server
Response Time (SMTP)	The response time of the SMTP server
Total	The sum of the response time of the SMTP server and the POP3 server  This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

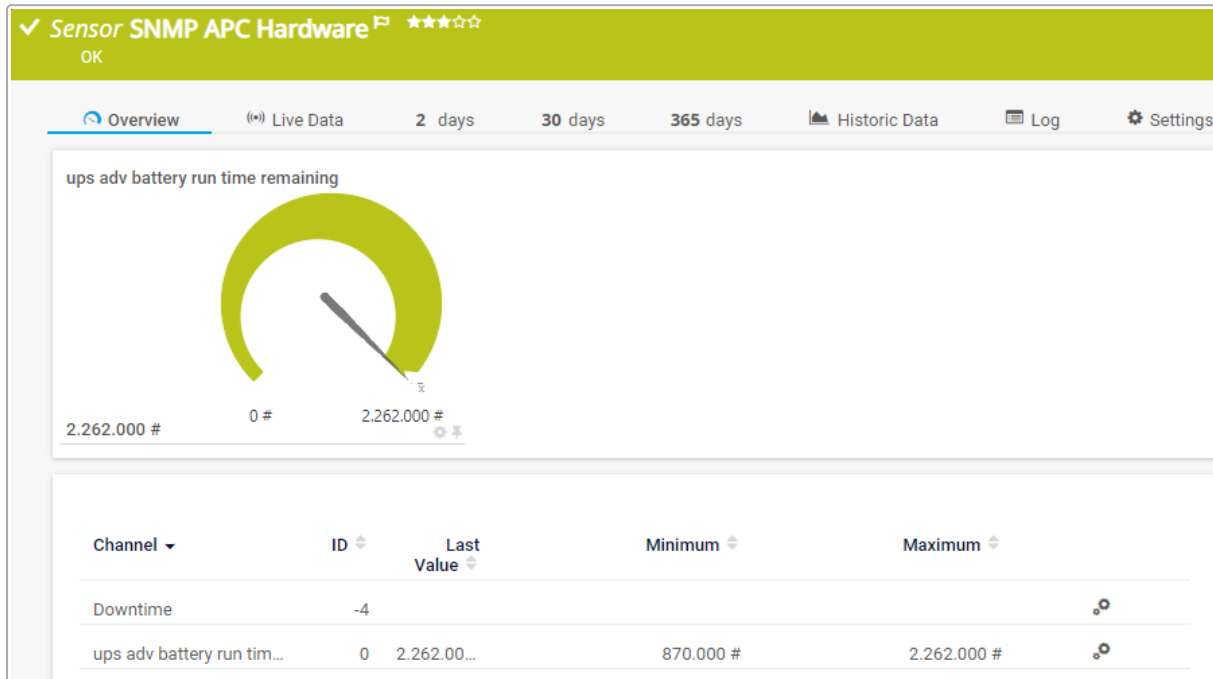
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.164 SNMP APC Hardware Sensor

The SNMP APC Hardware sensor monitors performance counters on an APC UPS device via the Simple Network Management Protocol (SNMP).

**i** The SNMP APC Hardware sensor does not appear as a running sensor, instead it is created as an [SNMP Custom Advanced](#) sensor.



SNMP APC Hardware Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP APC Hardware
- French: APC matériel (SNMP)
- German: SNMP APC Hardware
- Japanese: SNMP APC ハードウェア
- Portuguese: Hardware APC (SNMP)
- Russian: Оборудование SNMP APC
- Simplified Chinese: SNMP APC 硬件
- Spanish: Hardware APC (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">How can I monitor additional counters with the SNMP APC Hardware sensor?</a></li> <li>Knowledge Base: <a href="#">How can I monitor an APC UPS that does not support SNMP?</a></li> </ul>

## Add Sensor

APC UPS Specific

Setting	Description
Category	Select the performance counters that you want to monitor. PRTG creates one SNMP Custom Advanced sensor with all performance counters of each category that you select.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- apcups

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### APC UPS Specific

**APC UPS Specific**

**Interface** ⓘ *PowerNet-MIB/ups adv battery/ups adv battery run*

**Unit String** ⓘ #

**Multiplication** ⓘ

**Division** ⓘ

**If Value Changes** ⓘ  Ignore (default)  
 Trigger 'change' notification

APC UPS Specific

Setting	Description
Interface	TheSe name of the interface (performance counter) that this sensor monitors.
Unit String	Define the unit of the numeric data that this sensor monitors at the OID. Enter a string.
Multiplication	If you want to multiply the received data with a certain value, enter the quotient. Enter an integer.
Division	If you want to divide the received data by a certain value, enter the divisor. Enter an integer.
If Value Changes	<p>Define what the sensor does when its value changes:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> <li>▪ Trigger 'change' notification: Send an internal message that indicates a change.</li> </ul> <p> ⓘ In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</p>


### Sensor Display

**Sensor Display**


**Primary Channel** ⓘ Downtime


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
[ <a href="#">Performance Counter</a> ]	<p>The performance counters on an APC UPS device</p> <ul style="list-style-type: none"><li>▪ Actual voltage of battery</li><li>▪ Capacity of battery</li><li>▪ Input and output frequency</li><li>▪ Input and output voltage</li><li>▪ Output load</li><li>▪ Remaining runtime of battery</li><li>▪ Temperature of battery</li></ul>

## More

### KNOWLEDGE BASE

How can I monitor additional counters with the SNMP APC Hardware sensor?

- <https://kb.paessler.com/en/topic/60367>

How can I monitor an APC UPS that does not support SNMP?

- <https://kb.paessler.com/en/topic/63674>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

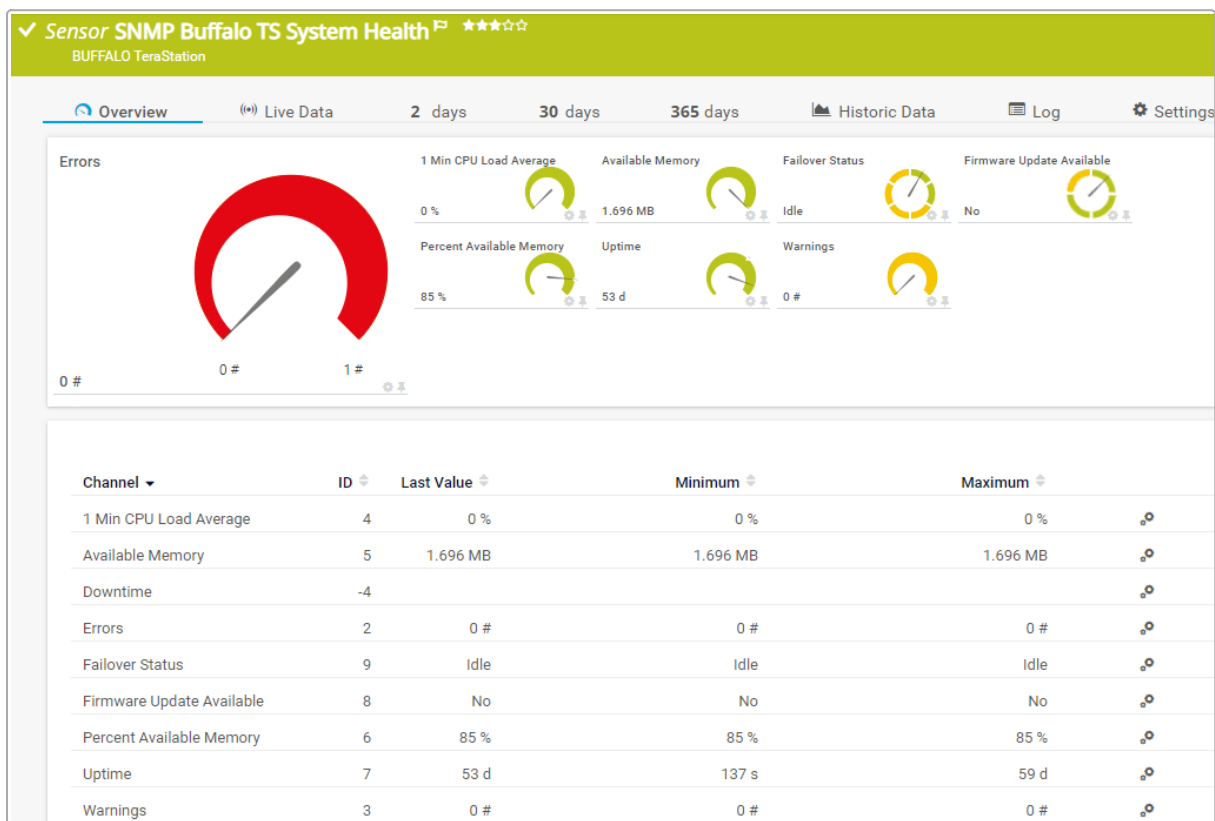
- <https://kb.paessler.com/en/topic/46863>

## 7.8.165 SNMP Buffalo TS System Health Sensor

The SNMP Buffalo TS System Health sensor monitors the system health of a Buffalo TeraStation network-attached storage (NAS) via the Simple Network Management Protocol (SNMP).

**i** This sensor supports the following TeraStation systems: [3000](#), [3010](#), [3020](#), [5000](#), [5010](#), [6000](#), and [7000](#) series.

**i** Run an [auto-discovery](#) with the device template Buffalo TeraStation NAS to automatically create [SNMP Custom Table sensors](#)<sup>[1917]</sup> with additional useful information about the TeraStation, for example, array status, disk smart status, disk status, and Internet Small Computer System Interface (iSCSI) status. This device template also creates [SNMP sensors](#) for traffic, memory, and load average on the TeraStation.



SNMP Buffalo TS System Health Sensor

**■** For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1837]</sup>.

### Sensor in Other Languages

- Dutch: SNMP Buffalo TS Systeemstatus
- French: Buffalo TS état du système (SNMP)
- German: SNMP Buffalo TS System Health
- Japanese: SNMP Buffalo TS システムの正常性
- Portuguese: Saúde do sistema Buffalo TS (SNMP)



- Russian: Работоспособность системы Buffalo TS по SNMP
- Simplified Chinese: SNMP Buffalo TS 系统健康状况
- Spanish: Salud de sistema Buffalo TS (SNMP)

## Remarks

Consider the following [remarks](#)<sup>1835</sup> and requirements for this sensor:

Remark	Description
TeraStation series	This sensor supports the <a href="#">TeraStation 3000</a> , <a href="#">3010</a> , <a href="#">3020</a> , <a href="#">5000</a> , <a href="#">5010</a> , <a href="#">6000</a> , and <a href="#">7000</a> series.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Error message	In certain cases, this sensor might show an error message. If this occurs, open the <a href="#">settings of the parent device</a> , section SNMP Compatibility Options, and set the Walk Mode to Use GETNEXT requests.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- buffalots
- snmpbuffalots
- systemhealth

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
1 Min CPU Load Average	The average CPU load (%)
Available Memory	The available memory
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Errors	<p>The number of errors</p> <p><b>i</b> This channel is the primary channel by default.</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper error limit: 0</li> </ul>
Failover Status	<p>The failover status</p> <ul style="list-style-type: none"> <li>Up status: Busy, Idle</li> <li>Warning status: Initializing, Starting Backup, Starting Main, Stopping</li> </ul>
Firmware Update Available	<p>If a firmware update is available</p> <ul style="list-style-type: none"> <li>Up status: No, Unknown, Latest</li> <li>Warning status: Yes</li> </ul>
Percent Available Memory	The available memory (%)
Uptime	The uptime
Warnings	<p>The number of warnings</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper warning limit: 0</li> </ul>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

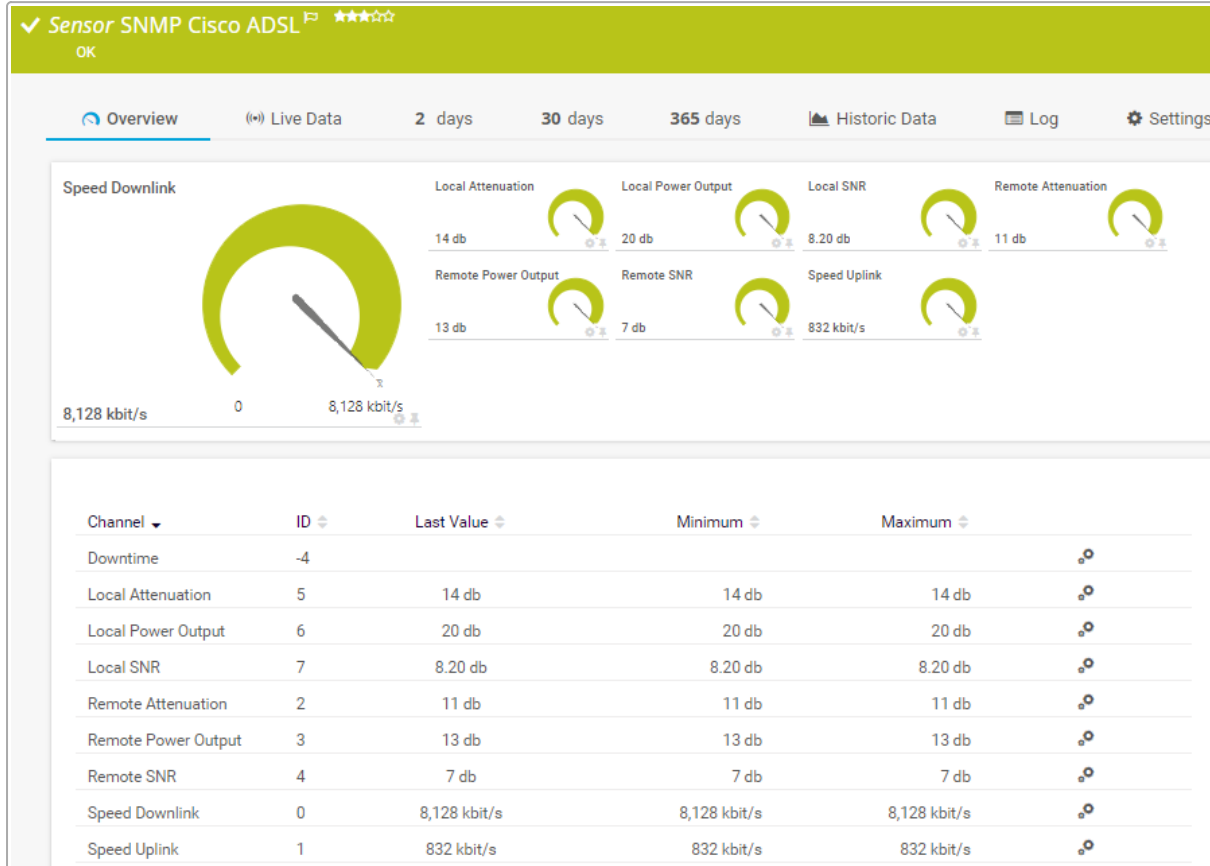
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.166 SNMP Cisco ADSL Sensor

The SNMP Cisco ADSL sensor monitors asymmetric digital subscriber line (ADSL) statistics of a Cisco router via the Simple Network Management Protocol (SNMP).



SNMP Cisco ADSL Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Cisco ADSL
- French: Cisco ADSL (SNMP)
- German: SNMP Cisco ADSL
- Japanese: SNMP Cisco ADSL
- Portuguese: Cisco ADSL (SNMP)
- Russian: SNMP Cisco ADSL
- Simplified Chinese: SNMP Cisco ADSL
- Spanish: Cisco ADSL (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- snmpciscoadsl

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Cisco ADSL Settings

#### Cisco ADSL Settings

**Line Index** ⓘ 13

Cisco ADSL Settings

Setting	Description
Line Index	The line index (performance counter) that this sensor monitors.

### Sensor Display

#### Sensor Display

**Primary Channel** ⓘ Downtime


---

**Graph Type** ⓘ


Show channels independently (default)

Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Local Attenuation	The local attenuation
Local Power Output	The local power output
Local SNR	The local SNR
Remote Attenuation	The remote attenuation
Remote Power Output	The remote power output
Remote SNR	The remote SNR
Speed Downlink	The downlink speed  This channel is the primary channel by default.
Speed Uplink	The uplink speed

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

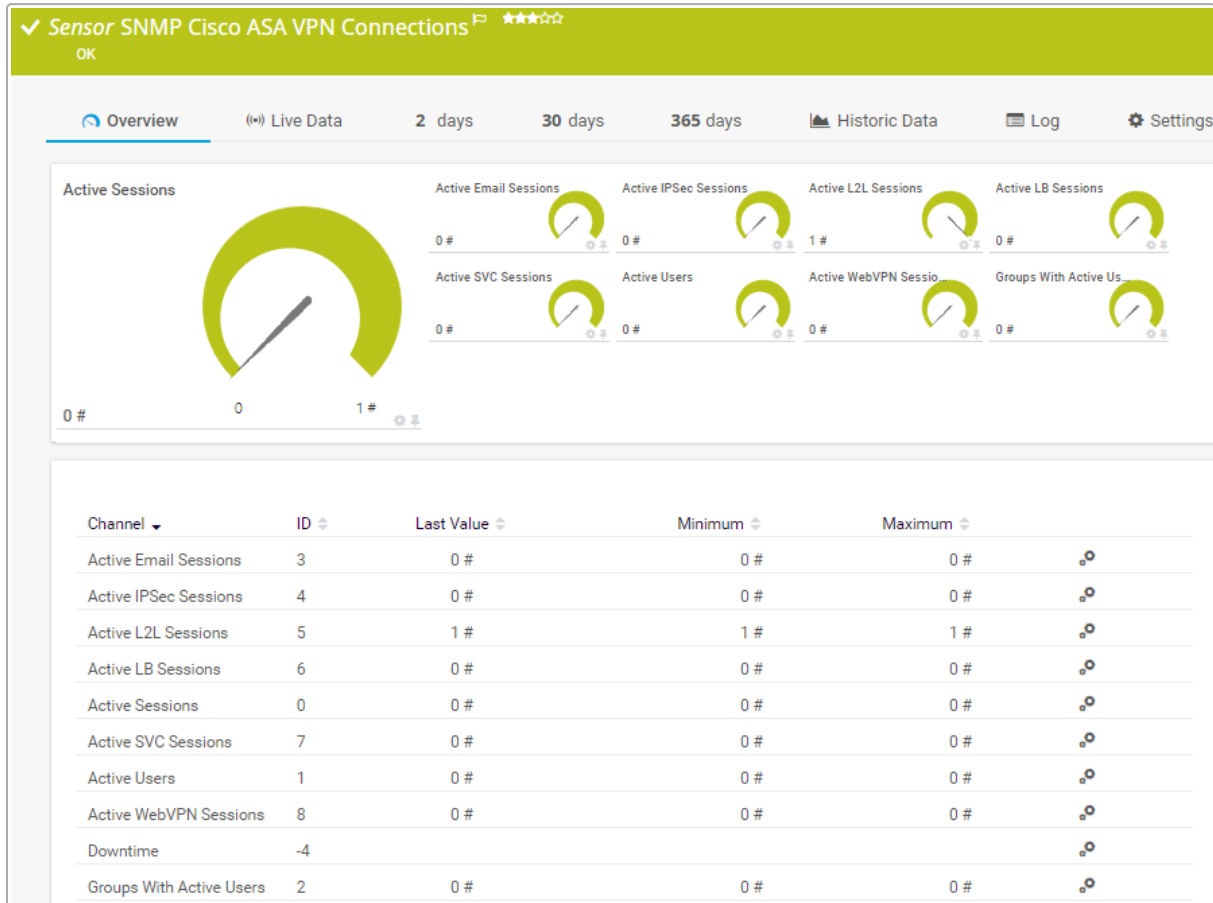
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>



## 7.8.167 SNMP Cisco ASA VPN Connections Sensor

The SNMP Cisco ASA VPN Connections sensor monitors the VPN connections on a Cisco Adaptive Security Appliance via the Simple Network Management Protocol (SNMP).



SNMP Cisco ASA VPN Connections Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1845]</sup>.

### Sensor in Other Languages

- Dutch: SNMP Cisco ASA VPN Verbindingen
- French: Cisco ASA connexions VPN (SNMP)
- German: SNMP Cisco ASA VPN-Verbindungen
- Japanese: SNMP Cisco ASA VPN 接続数
- Portuguese: Conexões VPN Cisco ASA (SNMP)
- Russian: Подключения SNMP Cisco ASA VPN
- Simplified Chinese: SNMP Cisco ASA VPN 连接
- Spanish: Conexiones VPN Cisco ASA (SNMP)

## Remarks

Consider the following [remarks](#)<sup>1844</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- snmpciscoasavpnconnectionssensor
- snmpciscoasavpnsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Sensor Display


### Sensor Display

**Primary Channel** ⓘ


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are

Setting	Description
	<p>available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Active Email Sessions	The number of active email sessions
Active IPsec Sessions	The number of active IPsec sessions
Active L2L Sessions	The number of active L2L sessions

Channel	Description
Active LB Sessions	The number of active LB sessions
Active Sessions	The total number of active sessions <span>ⓘ</span> This channel is the primary channel by default.
Active SVC Sessions	The number of active SVC sessions
Active Users	The number of active users
Active WebVPN Sessions	The number of active WebVPN users
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Groups With Active Users	The number of groups with active users

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

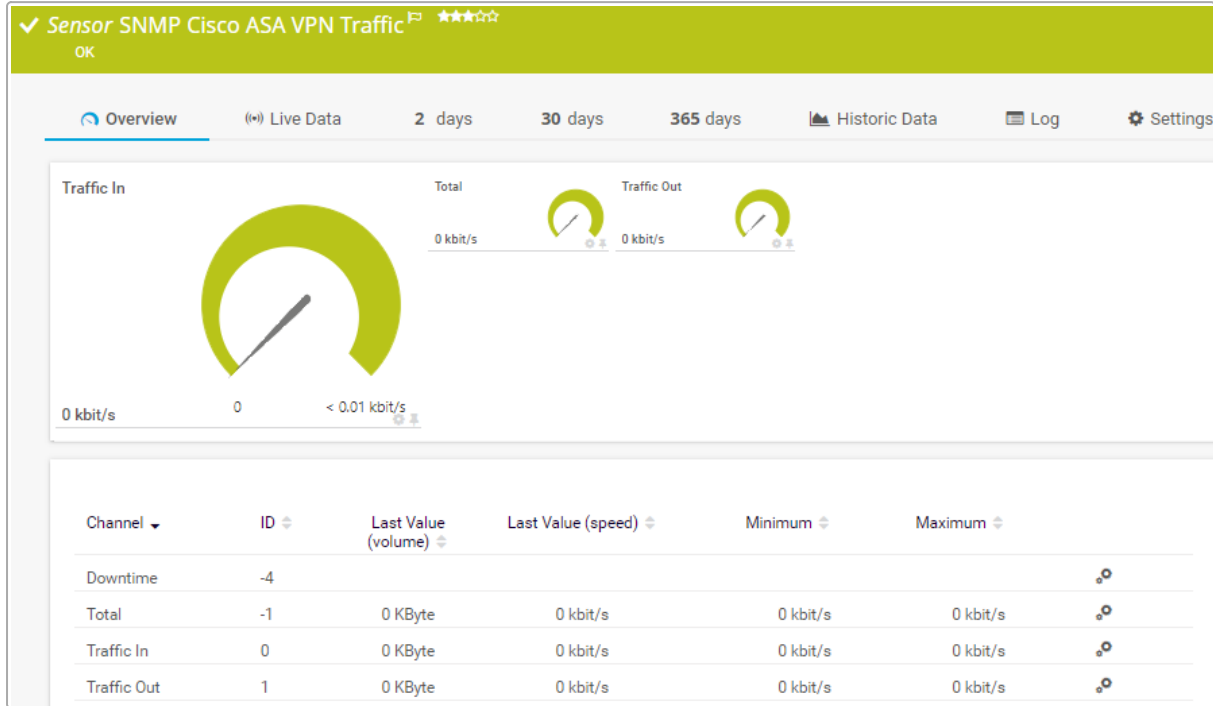
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.168 SNMP Cisco ASA VPN Traffic Sensor

The SNMP Cisco ASA VPN Traffic sensor monitors the traffic of an Internet Protocol Security (IPsec) VPN connection on a Cisco Adaptive Security Appliance via the Simple Network Management Protocol (SNMP).



SNMP Cisco ASA VPN Traffic Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Cisco ASA VPN Verkeer
- French: Cisco ASA trafic VPN (SNMP)
- German: SNMP Cisco ASA VPN-Datenverkehr
- Japanese: SNMP Cisco ASA VPN トラフィック
- Portuguese: Tráfego VPN Cisco ASA (SNMP)
- Russian: Трафик SNMP Cisco ASA VPN
- Simplified Chinese: SNMP Cisco ASA VPN 流量
- Spanish: Tráfico VPN Cisco ASA (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPsec connections	This sensor can monitor IPsec connections only.
Permanent connections	This sensor is intended to monitor permanent connections. It shows an error if a connection is interrupted.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Knowledge Base	Knowledge Base: <a href="#">I get the error PE123 when using the SNMP Cisco ASA VPN Traffic sensor. What can I do?</a>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- snmpciscoasavpnsensor
- snmpciscoasavpntrafficsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### ASA VPN Specific

#### ASA VPN Specific

**Remote IP Address** ⓘ 192.0.2.0

---

**Sensor Behavior** ⓘ  Show down status if no connection is active (default)  
 Show warning status if no connection is active  
 Stay in up status if no connection is active

**IKE Version Handling** ⓘ  IKEv1 (default)  
 IKEv1 and IKEv2

ASA VPN Specific

Setting	Description
Remote IP Address	<p>The IP address of the connection that this sensor monitors.</p> <p><b>i</b> PRTG shows this value for reference purposes only. We strongly recommend that you only change it if the Paessler support team explicitly asks you to do so. Wrong usage can result in incorrect monitoring data.</p>
Sensor Behavior	<p>Define the <a href="#">sensor status</a> if no active connection is available:</p> <ul style="list-style-type: none"> <li>▪ Show down status if no connection is active (default): Set the sensor to the Down status if no connection is active.</li> <li>▪ Show warning status if no connection is active: Set the sensor to the Warning status if no connection is active.</li> <li>▪ Stay in up status if no connection is active: Stay in the Up status if no connection is active.</li> </ul>
IKE Version Handling	<p>Select the engine for the Internet Key Exchange (IKE) version handling:</p> <ul style="list-style-type: none"> <li>▪ IKEv1 (default): Select this option if the tunnel on the device uses IKEv1.</li> <li>▪ IKEv1 and IKEv2: Select this option if the tunnel on the device uses IKEv1 or IKEv2.</li> </ul> <p><b>i</b> The IKEv1 and IKEv2 option is in beta status and might not work properly.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime


---

Graph Type **i**  Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>+</b> below a channel gauge on the sensor's Overview tab.</p>

Setting	Description
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Total	The total traffic
Traffic In	<p>The incoming traffic</p> <p> This channel is the primary channel by default.</p>
Traffic Out	The outgoing traffic



## More

### ■ KNOWLEDGE BASE

I get the error PE123 when using the SNMP Cisco ASA VPN Traffic sensor. What can I do?

- <https://kb.paessler.com/en/topic/59643>

What security features does PRTG include?

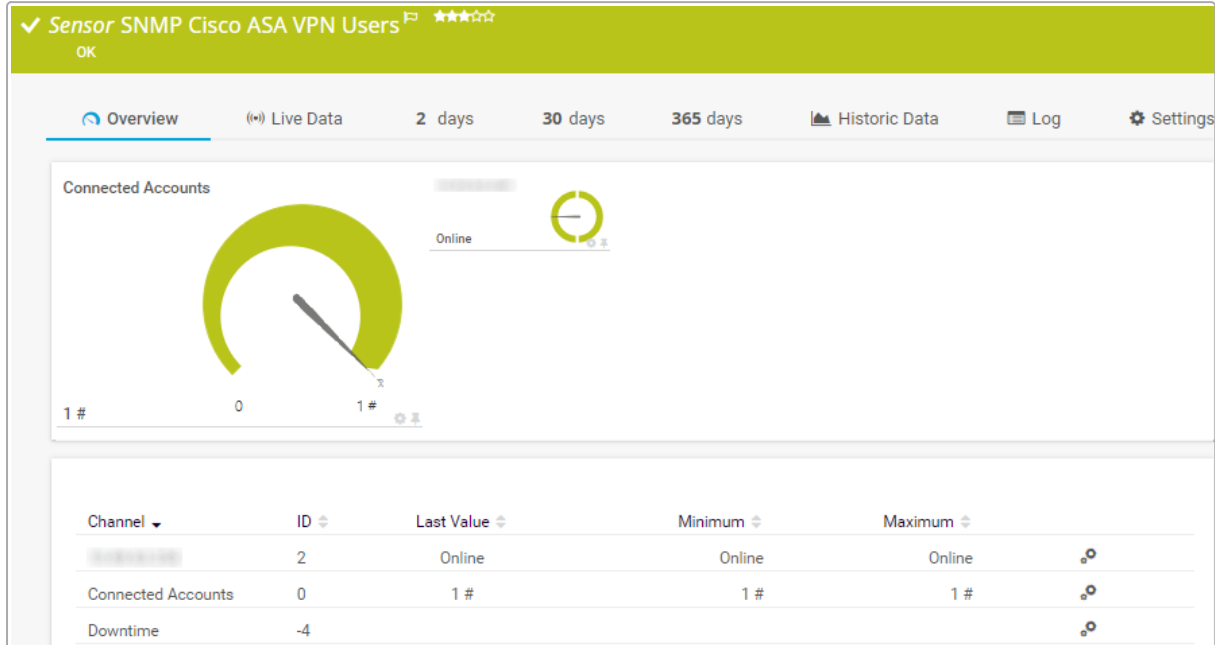
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.169 SNMP Cisco ASA VPN Users Sensor

The SNMP Cisco ASA VPN Users sensor monitors account connections to a VPN on a Cisco Adaptive Security Appliance via the Simple Network Management Protocol (SNMP).



SNMP Cisco ASA VPN Users Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1854</sup>.

### Sensor in Other Languages

- Dutch: SNMP Cisco ASA VPN Gebruikers
- French: Cisco ASA utilisateurs VPN (SNMP)
- German: SNMP Cisco ASA VPN-Benutzer
- Japanese: SNMP Cisco ASA VPN ユーザー数
- Portuguese: Usuários VPN Cisco ASA (SNMP)
- Russian: Пользователи SNMP Cisco ASA VPN
- Simplified Chinese: SNMP Cisco ASA VPN 用户
- Spanish: Usuarios VPN Cisco ASA (SNMP)

### Remarks

Consider the following [remarks](#)<sup>1852</sup> and requirements for this sensor:

Remark	Description
VPN users	Do not use this sensor to monitor more than 50 VPN users, especially if they are all connected simultaneously. For more information, see the Knowledge Base: <a href="#">My SNMP Cisco ASA VPN Users sensor shows a user limit error. Why? What can I do?</a>
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- snmpciscoasavpnsensor
- snmpciscoasavpntrafficsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Display


#### Sensor Display

**Primary Channel** ⓘ Downtime


---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
[Account]	<p>The account status</p> <ul style="list-style-type: none"> <li>▪ Up status: Offline, Online</li> </ul>

Channel	Description
Connected Accounts	The number of connected accounts  This channel is the primary channel by default.
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

## More

### KNOWLEDGE BASE

My SNMP Cisco ASA VPN Users sensor shows a user limit error. Why? What can I do?

- <https://kb.paessler.com/en/topic/64053>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

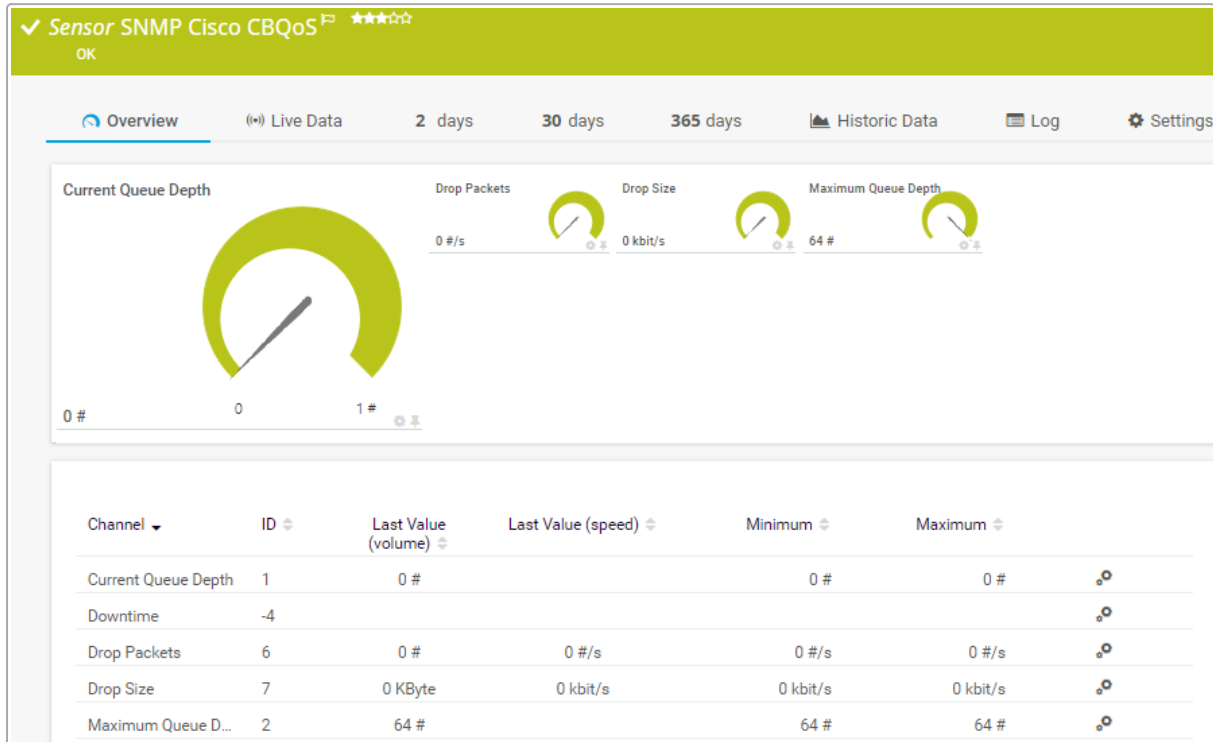
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.170 SNMP Cisco CBQoS Sensor

The SNMP Cisco CBQoS sensor monitors network parameters using Cisco's Class Based Quality of Service (CBQoS) via the Simple Network Management Protocol (SNMP).

**i** The sensor supports the classes [Class Map](#), [Match Statement](#), and [Queueing](#).



SNMP Cisco CBQoS Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Cisco CBQoS
- French: Cisco CBQoS (SNMP)
- German: SNMP Cisco CBQoS
- Japanese: SNMP Cisco CBQoS
- Portuguese: CBQoS Cisco (SNMP)
- Russian: SNMP Cisco CBQoS
- Simplified Chinese: SNMP Cisco CBQoS
- Spanish: CBQoS Cisco (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv4	This sensor only supports IPv4.
Performance impact	This sensor has a <b>very low</b> performance impact.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- cbqossensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Class Based QoS Specific

#### Class Based QoS Specific

**Object Type** ⓘ *Match Statement*

**Interface** ⓘ *Main Interface:1 input*

**Description** ⓘ *Match protocol http*

**BitMask** ⓘ 3

**ObjectID** ⓘ 12.345678

**ConfigID** ⓘ 123456

Class Based QoS Specific

Setting	Description
Object Type	The object type of the parameter that this sensor monitors.
Interface	The interface of the parameter that this sensor monitors.
Description	The description of the parameter that this sensor monitors.
BitMask	The number of available channels for the parameter that this sensor monitors.
ObjectID	The ObjectID of the parameter that this sensor monitors.
ConfigID	The ConfigID of the parameter that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>



Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Current Queue Depth	The current queue depth
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Drop Packets	The number of drop packets
Drop Size	The drop size
Maximum Queue Depth	The maximum queue depth
No Buffer Drop Packets	The number of drop packets without buffer
Post Policy Size	The post policy size
Pre Policy Packets	The number of pre-policy packets

Channel	Description
Pre Policy Size	The pre-policy size

## More

### KNOWLEDGE BASE

What security features does PRTG include?

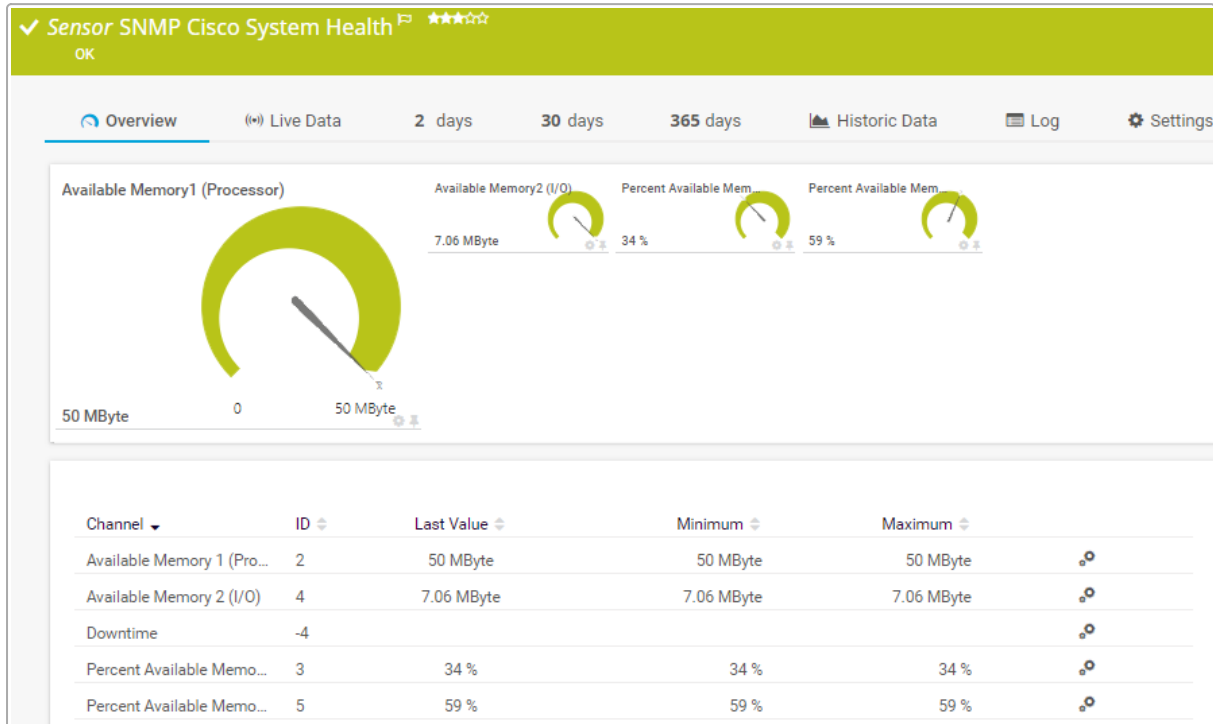
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.171 SNMP Cisco System Health Sensor

The SNMP Cisco System Health sensor monitors the system health of a Cisco device via the Simple Network Management Protocol (SNMP).



SNMP Cisco System Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1864]</sup>.

### Sensor in Other Languages

- Dutch: SNMP Cisco Systemstatus
- French: Cisco état du système (SNMP)
- German: SNMP Cisco Systemzustand
- Japanese: SNMP Cisco システムの正常性
- Portuguese: Saúde do sistema Cisco (SNMP)
- Russian: Работоспособность системы устройства SNMP Cisco
- Simplified Chinese: SNMP Cisco 系统健康状况
- Spanish: Salud de sistema Cisco (SNMP)

### Remarks

Consider the following [remarks](#)<sup>[1861]</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Additional tags	SNMP Cisco System Health sensors that are created with the <a href="#">Cisco Device (Generic)</a> device template for auto-discovery can have additional tags.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- snmpciscosystemhealthsensor
- systemhealth

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Cisco System Health Specific

#### Cisco System Health Specific

**Measurements** ⓘ 1

Cisco System Health Specific

Setting	Description
Measurements	The ID of the measurement that this sensor monitors.

### Debug Options

**Debug Options**

**Result Handling** ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### Sensor Display

**Sensor Display**

**Primary Channel** ⓘ

Downtime


---

**Graph Type** ⓘ


Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are

Setting	Description
	<p>available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

- i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.
- i** PRTG creates one sensor per component.

Channel	Description
Available Memory [#]	The available memory
CPU [#]	The CPU load (%)

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Fan [#] State	<p>The fan status</p> <ul style="list-style-type: none"> <li>▪ Up status: Normal</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Critical, Not Functioning, Shutdown</li> <li>▪ Unknown status: Not Present</li> </ul>
Percent Available Memory [#]	The available memory (%)
Power Supply [#]	<p>The power supply status</p> <ul style="list-style-type: none"> <li>▪ Up status: Normal</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Critical, Not Functioning, Shutdown</li> <li>▪ Unknown status: Not Present</li> </ul>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

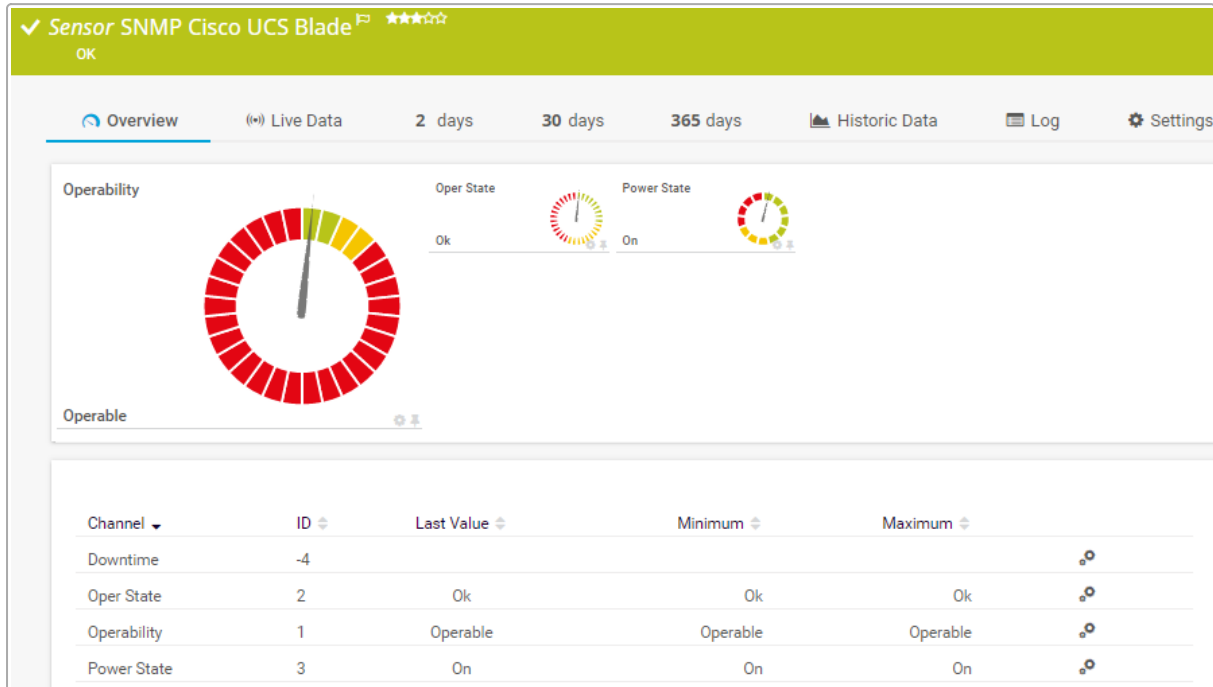
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.172 SNMP Cisco UCS Blade Sensor

The SNMP Cisco UCS Blade sensor monitors the health status of a Cisco Unified Computing System (UCS) blade server via the Simple Network Management Protocol (SNMP).



SNMP Cisco UCS Blade Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Cisco UCS Blade
- French: Cisco UCS serveur Blade (SNMP)
- German: SNMP Cisco UCS Blade
- Japanese: SNMP Cisco UCS ブレード
- Portuguese: Blade Cisco UCS (SNMP)
- Russian: Блейд-сервер SNMP Cisco UCS
- Simplified Chinese: SNMP Cisco UCS 刀片
- Spanish: Blade Cisco UCS (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:



Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- blade
- snmpciscosystemhealthsensor
- systemhealth
- ucs
- ucssystemhealth

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Settings

#### Sensor Settings

**Blade Servers** ⓘ *sys/chassis-1/blade-1*

---

**Channel Mask** ⓘ *7*

---

**Model** ⓘ *UCSB-B200-M3*

---

**Serial Number** ⓘ *ABCD1234-5678EFGH*

Sensor Settings

Setting	Description
Blade Servers	The blade server that this sensor monitors.
Channel Mask	The available channels for the blade server that this sensor monitors.
Model	The model of the blade server that this sensor monitors.
Serial Number	The serial number blade server that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Oper State	<p>The oper status</p> <ul style="list-style-type: none"> <li>▪ Up status: Config, Diagnostics, Disabled, Discovery, Ok, Pending Reassociation, Pending Reboot, Test, Unconfig</li> <li>▪ Warning status: Bios Restore, CMOS Reset, Decommissioning, Degraded, Maintenance, Power Problem, Restart, Thermal Problem, Voltage Problem</li> <li>▪ Down status: Compute Failed, Compute Mismatch, Config Failure, Diagnostics Failed, Discovery Failed, Inaccessible, Indeterminate, Inoperable, Maintenance Failed, Power Off, Removed, Test Failed, Unassociated, Unconfig Failed</li> </ul>
Operability	<p>The operability status</p> <ul style="list-style-type: none"> <li>▪ Up status: Auto Upgrade, Operable</li> <li>▪ Warning status: Degraded, Unknown</li> <li>▪ Down status: Accessibility Problem, Bios Post Timeout, Chassis Limit Exceeded, Config, Decommissioning, Disabled, Equipment Problem, Discovery, Discovery Failed, Fabric Connection Problem, Fabric Unsupported Connection, Identify, Identity Unestablishable, Inoperable, Link Activate Blocked, Malformed Fru, Not Supported, Peer Comm Problem, Performance Problem, Post Failure, Power Problem, Powered Off, Removed, Thermal Problem, Upgrade Problem, Voltage Problem</li> </ul> <p> This channel is the primary channel by default.</p>
Power State	The power status

Channel	Description
	<ul style="list-style-type: none"><li>▪ Up status: Off Duty, Ok, On, Online, Power Save, Test</li><li>▪ Warning status: Degraded, Not Supported, Unknown</li><li>▪ Down status: Error, Failed, Off, Offline</li></ul>

## More

### KNOWLEDGE BASE

What security features does PRTG include?

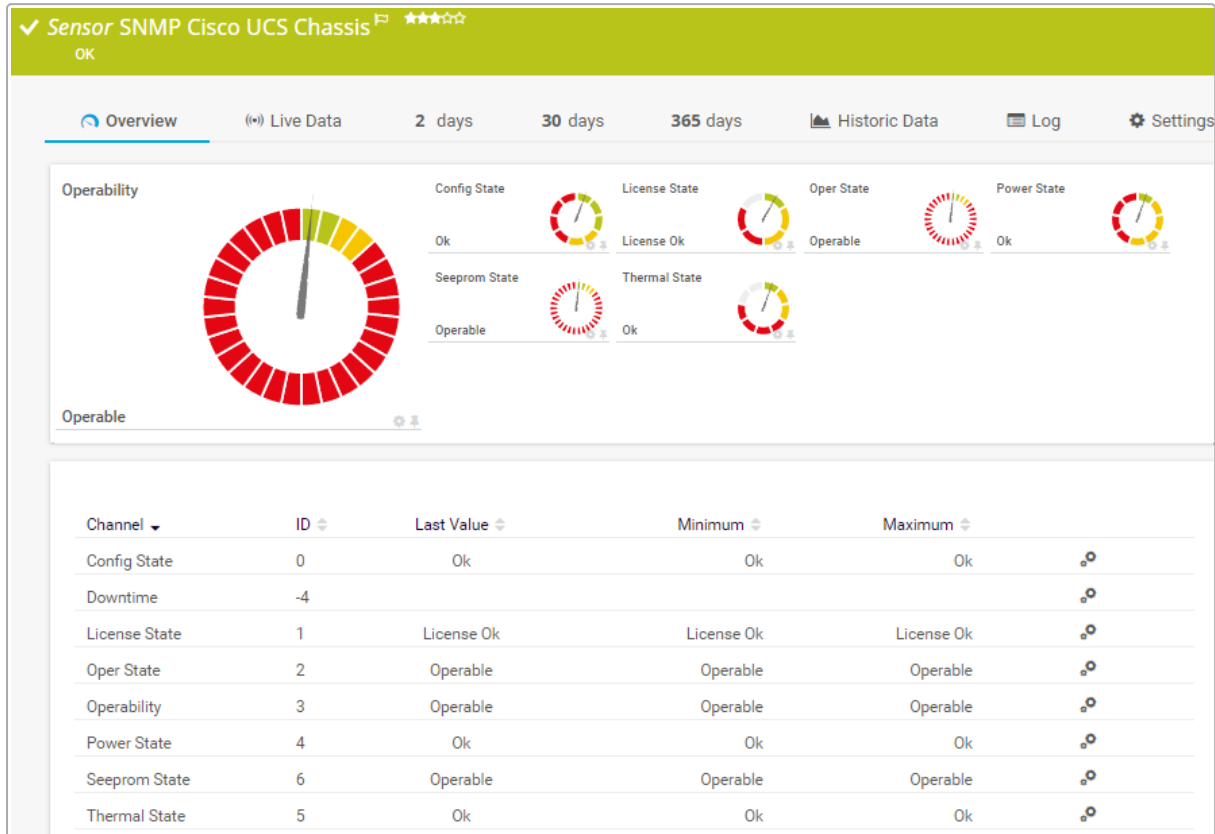
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.173 SNMP Cisco UCS Chassis Sensor

The SNMP Cisco UCS Chassis sensor monitors the health status of the chassis of a Cisco Unified Computing System (UCS) device via the Simple Network Management Protocol (SNMP).



SNMP Cisco UCS Chassis Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List<sup>1873</sup>](#).

### Sensor in Other Languages

- Dutch: SNMP Cisco UCS Chassis
- French: Cisco UCS châssis (SNMP)
- German: SNMP Cisco UCS Chassis
- Japanese: SNMP Cisco UCS シャーシ
- Portuguese: Chassi Cisco UCS (SNMP)
- Russian: Копныс SNMP Cisco UCS
- Simplified Chinese: SNMP Cisco UCS 机箱
- Spanish: Chasis Cisco UCS (SNMP)

### Remarks

Consider the following [remarks<sup>1871</sup>](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- chassis
- snmpciscosystemhealthsensor
- systemhealth
- ucs
- ucssystemhealth

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Settings

#### Sensor Settings

**Chassis** ⓘ *sys/chassis-1*

Sensor Settings

Setting	Description
Chassis	The chassis that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Config State	<p>The configuration status</p> <ul style="list-style-type: none"> <li>▪ Up status: Acknowledged, Auto Acknowledge, OK</li> <li>▪ Warning status: Ack in Progress, Evaluation</li> <li>▪ Down status: Removing, UnAcknowledged, UnInitalized, Unsupported Connectivity</li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
License State	<p>The license status</p> <ul style="list-style-type: none"> <li>▪ Up status: License Ok</li> <li>▪ Warning status: License Grace Period, Unknown</li> <li>▪ Down status: License Expired, License Insufficient</li> <li>▪ Unknown status: Not Applicable</li> </ul>
Oper State	<p>The oper status</p> <ul style="list-style-type: none"> <li>▪ Up status: Auto Upgrade, Operable</li> <li>▪ Warning status: Degraded, Unknown</li> <li>▪ Down status: Accessibility Problem, Bios Post Timeout, Chassis Limit Exceeded, Config, Decomissioning, Disabled, Equipment Problem, Discovery, Discovery Failed, Fabric Connection Problem, Fabric Unsupported Connection, Identify, Identity Unestablishable, Inoperable, Link Activate Blocked, Malformed Fru, Not Supported, Peer Comm Problem, Performance Problem, Post Failure, Power Problem, Powered Off, Removed, Thermal Problem, Upgrade Problem, Voltage Problem</li> </ul>
Operability	<p>The operability status</p> <ul style="list-style-type: none"> <li>▪ Up status: Auto Upgrade, Operable</li> <li>▪ Warning status: Degraded, Unknown</li> <li>▪ Down status: Accessibility Problem, Bios Post Timeout, Chassis Limit Exceeded, Config, Decomissioning, Disabled, Equipment Problem, Discovery, Discovery Failed, Fabric Connection Problem, Fabric Unsupported Connection, Identify, Identity Unestablishable, Inoperable, Link Activate Blocked, Malformed Fru, Not Supported, Peer Comm Problem, Performance Problem, Post Failure, Power Problem, Powered Off, Removed, Thermal Problem, Upgrade Problem, Voltage Problem</li> </ul> <p> This channel is the primary channel by default.</p>



Channel	Description
Power State	<p>The power status</p> <ul style="list-style-type: none"> <li>▪ Up status: Ok</li> <li>▪ Warning status: Input Degraded, Output Degraded, Redundancy Degraded, Unknown</li> <li>▪ Down status: Failed, Input Failed, Output Failed, Redundancy Failed</li> </ul>
Seeprom State	<p>The serial electrically erasable programmable read-only memory (SEEPROM) state</p> <ul style="list-style-type: none"> <li>▪ Up status: Auto Upgrade, Operable</li> <li>▪ Warning status: Degraded, Unknown</li> <li>▪ Down status: Accessibility Problem, Bios Post Timeout, Chassis Limit Exceeded, Config, Decommissioning, Disabled, Equipment Problem, Discovery, Discovery Failed, Fabric Connection Problem, Fabric Unsupported Connection, Identify, Identity Unestablishable, Inoperable, Link Activate Blocked, Malformed Fru, Not Supported, Peer Comm Problem, Performance Problem, Post Failure, Power Problem, Powered Off, Removed, Thermal Problem, Upgrade Problem, Voltage Problem</li> </ul>
Thermal State	<p>The thermal status</p> <ul style="list-style-type: none"> <li>▪ Up status: Ok</li> <li>▪ Warning status: Lower Non Critical, Upper Non Critical</li> <li>▪ Down status: Lower Critical, Lower Non Recoverable, Upper Critical, Upper Non Recoverable</li> <li>▪ Unknown status: Not Supported, Unknown</li> </ul>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

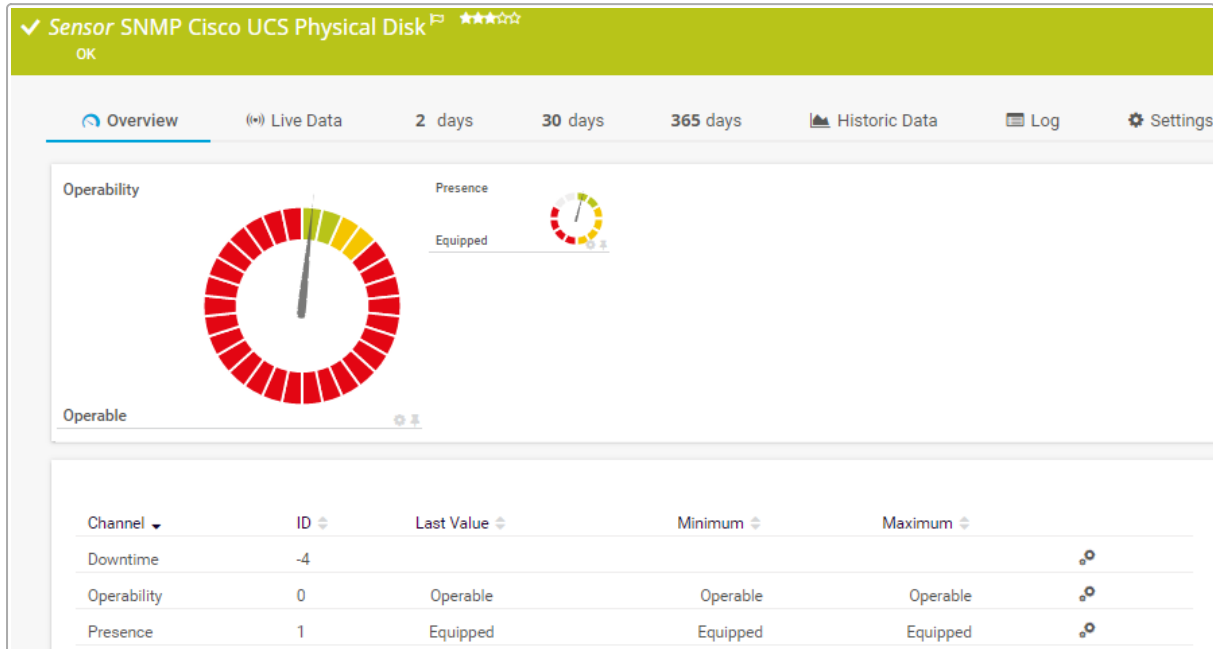
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.174 SNMP Cisco UCS Physical Disk Sensor

The SNMP Cisco UCS Physical Disk sensor monitors a physical disk of a Cisco Unified Computing System (UCS) device via the Simple Network Management Protocol (SNMP).



SNMP Cisco UCS Physical Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP-Cisco UCS fysieke schijf
- French: Cisco UCS disque physique (SNMP)
- German: SNMP Cisco UCS Physikalisches Laufwerk
- Japanese: SNMP Cisco UCS 物理ディスク
- Portuguese: Disco físico Cisco UCS (SNMP)
- Russian: Физический диск SNMP Cisco UCS
- Simplified Chinese: SNMP Cisco UCS 物理磁盘
- Spanish: Disco físico Cisco UCS (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.

Remark	Description
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Add Sensor dialog	The Add Sensor dialog only shows working disks that have the status <a href="#">Up</a> or <a href="#">Warning</a> .

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- snmp
- snmpciscophysicaldisksensor
- ucs

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### UCS Physical Disk

#### UCS Physical Disk

**Disk** ⓘ Example/pd-1

---

**Display Name** ⓘ pd-1

UCS Physical Disk

Setting	Description
Disk	The physical disk that this sensor monitors.

Setting	Description
Display Name	The display name of the physical disk that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

❗ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Operability	<p>The operability status</p> <ul style="list-style-type: none"> <li>▪ Up status: Auto Upgrade, Operable</li> <li>▪ Warning status: Degraded, Unknown</li> <li>▪ Down status: Accessibility Problem, Bios Post Timeout, Chassis Limit Exceeded, Config, Decommissioning, Disabled, Equipment Problem, Discovery, Discovery Failed, Fabric Connection Problem, Fabric Unsupported Connection, Identify, Identity Unestablishable, Inoperable, Link Activate Blocked, Malformed Fru, Not Supported, Peer Comm Problem, Performance Problem, Post Failure, Powered Off, Power Problem, Removed, Thermal Problem, Upgrade Problem, Voltage Problem</li> </ul> <p>❗ This channel is the primary channel by default.</p>
Presence	<p>The connection status</p> <ul style="list-style-type: none"> <li>▪ Up status: Equipped, Equipped Not Primary</li> <li>▪ Warning status: Equipped Identity Unestablishable, Mismatch, Mismatch Identity Unestablishable, Missing,</li> <li>▪ Down status: Equipped With Malformed Fru, Inaccessible, Not Supported, Unauthorized</li> <li>▪ Unknown status: Empty, Unknown</li> </ul>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

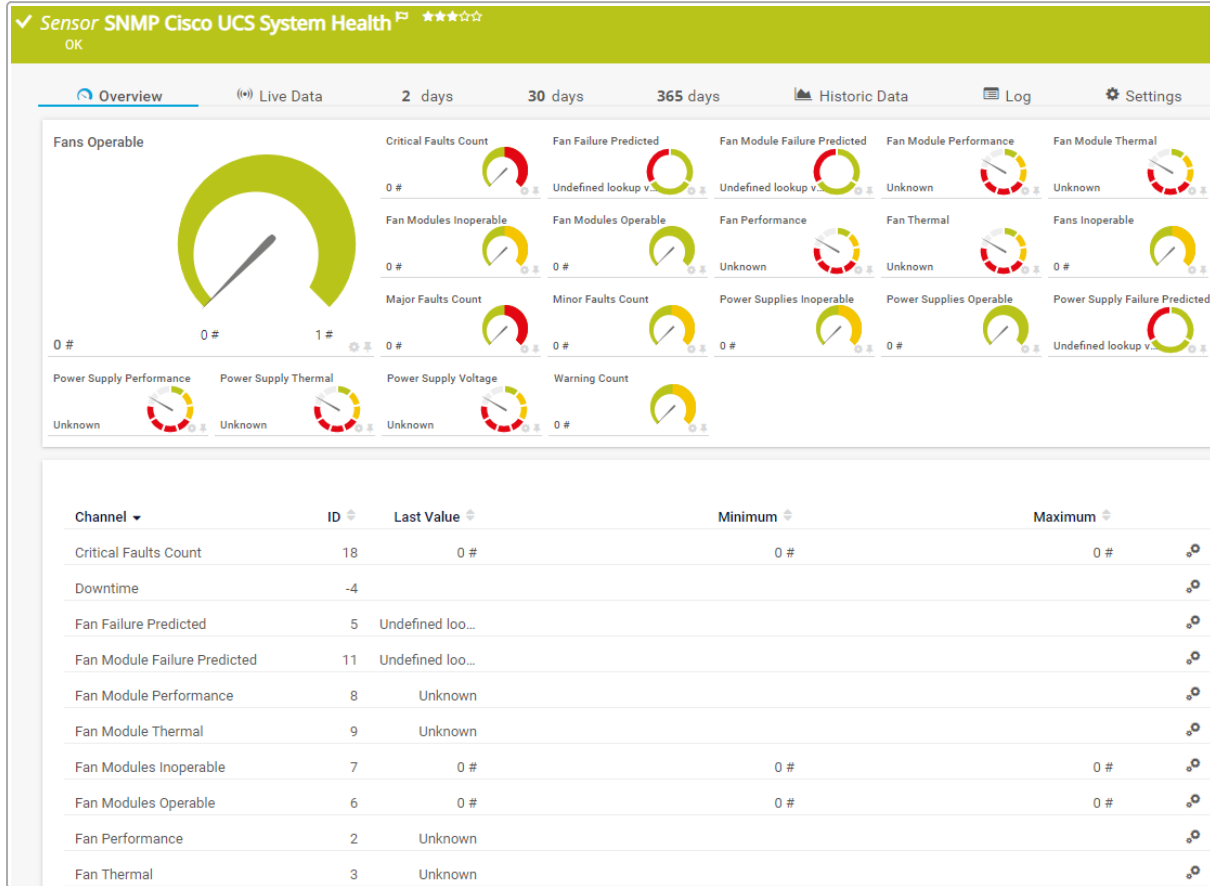
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.175 SNMP Cisco UCS System Health Sensor

The SNMP Cisco UCS System Health sensor monitors the system health of a Cisco Unified Computing System (UCS) device via the Simple Network Management Protocol (SNMP).



SNMP Cisco UCS System Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1882</sup>.

### Sensor in Other Languages

- Dutch: SNMP Cisco UCS Systemstatus
- French: Cisco UCS état du système (SNMP)
- German: SNMP Cisco UCS Systemzustand
- Japanese: SNMP Cisco UCS システムの正常性
- Portuguese: Saúde do sistema Cisco UCS (SNMP)
- Russian: Работоспособность системы SNMP Cisco UCS
- Simplified Chinese: SNMP Cisco UCS 系统健康状况
- Spanish: Salud de sistema Cisco UCS (SNMP)

## Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ

**Priority** ⓘ

Example Name

exampletag ✕ +

★★★★☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- snmpciscosystemhealthsensor
- systemhealth
- ucs
- ucssystemhealth

■ For more information about basic sensor settings, see section [Sensor Settings](#).

## Sensor Display

### Sensor Display

**Primary Channel** ⓘ


**Graph Type** ⓘ

Downtime


Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Critical Faults Count	<p>The number of critical faults (that are not yet acknowledged in the UCS logs)</p> <p><b>i</b> This channel has a default limit:</p>



Channel	Description
	<ul style="list-style-type: none"> <li>Upper error limit: 0.5</li> </ul>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Fan Failure Predicted	<p>The predicted fan failure status</p> <ul style="list-style-type: none"> <li>Up status: No, Not Available</li> <li>Down status: Yes</li> </ul>
Fan Module Failure Predicted	<p>The predicted fan module failure status</p> <ul style="list-style-type: none"> <li>Up status: No, Not Available</li> <li>Down status: Yes</li> </ul>
Fan Module Performance	<p>The fan module performance status</p> <ul style="list-style-type: none"> <li>Up status: Ok</li> <li>Warning status: Lower Non Critical, Upper Non Critical</li> <li>Down status: Lower Critical, Lower Non Recoverable, Upper Critical, Upper Non Recoverable</li> <li>Unknown status: Not Supported, Unknown</li> </ul>
Fan Module Thermal	<p>The fan module thermal status</p> <ul style="list-style-type: none"> <li>Up status: Ok</li> <li>Warning status: Lower Non Critical, Upper Non Critical</li> <li>Down status: Lower Critical, Lower Non Recoverable, Upper Critical, Upper Non Recoverable</li> <li>Unknown status: Not Supported, Unknown</li> </ul>
Fan Modules Inoperable	<p>The number of operable fan modules</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper warning limit: 0.5</li> </ul>
Fan Modules Operable	The number of inoperable fan modules
Fan Performance	<p>The fan performance</p> <ul style="list-style-type: none"> <li>Up status: Ok</li> <li>Warning status: Lower Non Critical, Upper Non Critical</li> </ul>

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Down status: Lower Critical, Lower Non Recoverable, Upper Critical, Upper Non Recoverable</li> <li>▪ Unknown status: Not Supported, Unknown</li> </ul>
Fan Thermal	<p>The fan thermal status</p> <ul style="list-style-type: none"> <li>▪ Up status: Ok</li> <li>▪ Warning status: Lower Non Critical, Upper Non Critical</li> <li>▪ Down status: Lower Critical, Lower Non Recoverable, Upper Critical, Upper Non Recoverable</li> <li>▪ Unknown status: Not Supported, Unknown</li> </ul>
Fans Inoperable	<p>The number of inoperable fan modules</p> <p>ⓘ This channel has a default limit:</p> <ul style="list-style-type: none"> <li>▪ Upper warning limit: 0.5</li> </ul>
Fans Operable	<p>The number of operable fan modules</p> <p>ⓘ This channel is the primary channel by default.</p>
Major Faults Count	<p>The number of major faults (that are not yet acknowledged in the UCS logs)</p> <p>ⓘ This channel has a default limit:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: 0.5</li> </ul>
Minor Faults Count	<p>The number of minor faults (that are not yet acknowledged in the UCS logs)</p> <p>ⓘ This channel has a default limit:</p> <ul style="list-style-type: none"> <li>▪ Upper warning limit: 0.5</li> </ul>
Power Supplies Inoperable	<p>The number of inoperable power supplies</p> <p>ⓘ This channel has a default limit:</p> <ul style="list-style-type: none"> <li>▪ Upper warning limit: 0.5</li> </ul>
Power Supplies Operable	<p>The number of operable power supplies</p>
Power Supply Failure Predicted	<p>The predicted power supply failure status</p> <ul style="list-style-type: none"> <li>▪ Up status: No, Not Available</li> </ul>

Channel	Description
	<ul style="list-style-type: none"> <li>Down status: Yes</li> </ul>
Power Supply Performance	<p>The power supply performance status</p> <ul style="list-style-type: none"> <li>Up status: Ok</li> <li>Warning status: Lower Non Critical, Upper Non Critical</li> <li>Down status: Lower Critical, Lower Non Recoverable, Upper Critical, Upper Non Recoverable</li> <li>Unknown status: Not Supported, Unknown</li> </ul>
Power Supply Thermal	<p>The power supply thermal status</p> <ul style="list-style-type: none"> <li>Up status: Ok</li> <li>Warning status: Lower Non Critical, Upper Non Critical</li> <li>Down status: Lower Critical, Lower Non Recoverable, Upper Critical, Upper Non Recoverable</li> <li>Unknown status: Not Supported, Unknown</li> </ul>
Power Supply Voltage	<p>The power supply voltage status</p> <ul style="list-style-type: none"> <li>Up status: Ok</li> <li>Warning status: Lower Non Critical, Upper Non Critical</li> <li>Down status: Lower Critical, Lower Non Recoverable, Upper Critical, Upper Non Recoverable</li> <li>Unknown status: Not Supported, Unknown</li> </ul>
Warning Count	<p>The number of warnings (that are not yet acknowledged in the UCS logs)</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper warning limit: 0.5</li> </ul>

## More

### KNOWLEDGE BASE

What security features does PRTG include?

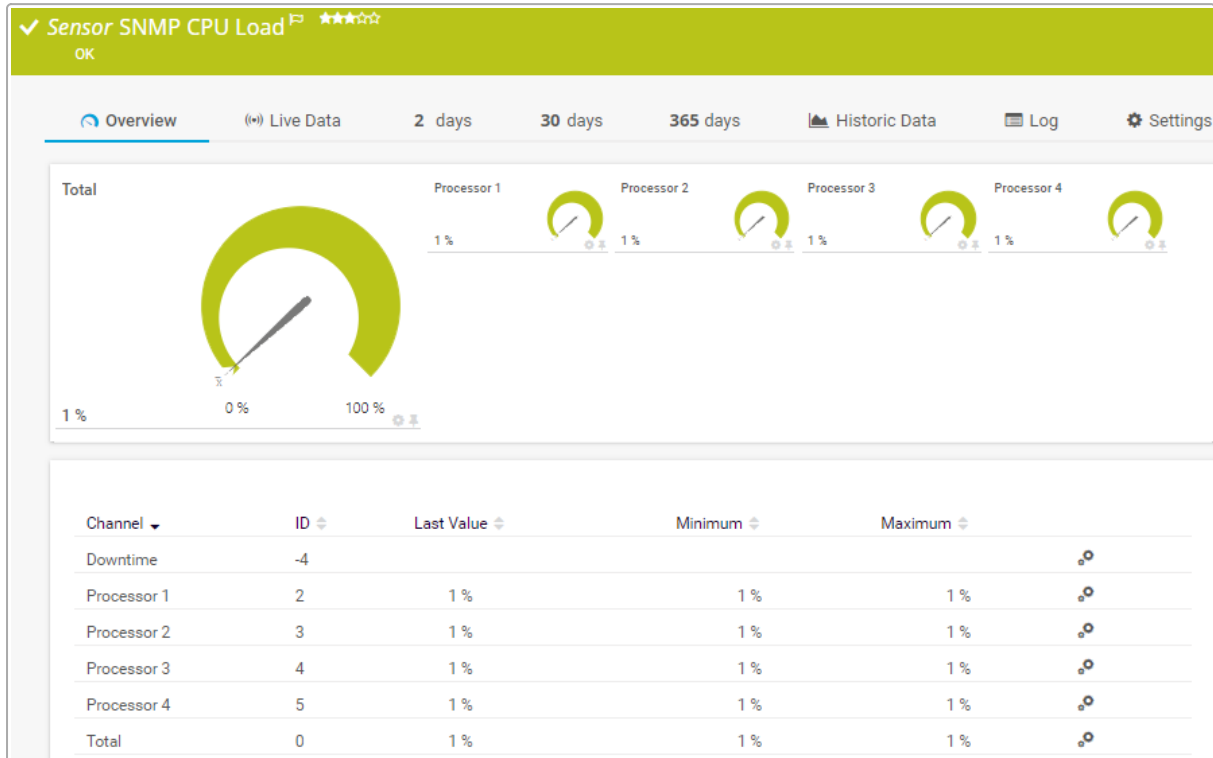
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.176 SNMP CPU Load Sensor

The SNMP CPU Load sensor monitors the system load via the Simple Network Management Protocol (SNMP).



SNMP CPU Load Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP CPU Load
- French: Charge CPU (SNMP)
- German: SNMP CPU-Last
- Japanese: SNMP CPU の負荷
- Portuguese: Carga CPU (SNMP)
- Russian: Загрузка ЦП SNMP
- Simplified Chinese: SNMP CPU 负载
- Spanish: Carga CPU (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
Localhost	It might not work to query data from a probe device via SNMP (querying <a href="#">localhost</a> , <a href="#">127.0.0.1</a> , or <a href="#">::1</a> ). <a href="#">Add this device</a> with the IP address that it has in your network and create the sensor on this device instead.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- cpu
- cpuloadsensor
- snmp

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Debug Options

#### Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	Define what PRTG does with the sensor result:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other above.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Processor [#]	The CPU load (%)
Total	The total CPU load (%)  This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

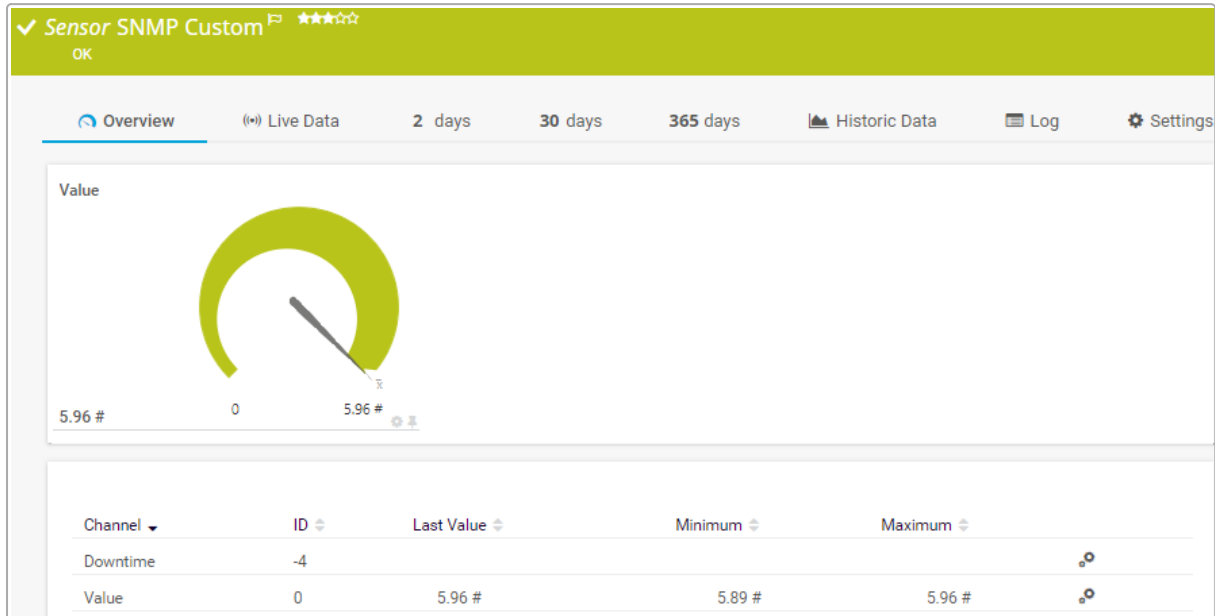
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.177 SNMP Custom Sensor

The SNMP Custom sensor monitors a single parameter that is returned by a specific object identifier (OID) via the Simple Network Management Protocol (SNMP).



SNMP Custom Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1894</sup>.

### Sensor in Other Languages

- Dutch: SNMP (Klant specifiek)
- French: SNMP personnalisé
- German: SNMP (Benutzerdef.)
- Japanese: SNMP カスタム
- Portuguese: SNMP (customizado)
- Russian: Пользовательские параметры SNMP
- Simplified Chinese: SNMP 自定义
- Spanish: SNMP (personalizado)

### Remarks

Consider the following [remarks](#)<sup>1890</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.



Remark	Description
Performance impact	This sensor has a <b>very low</b> performance impact.
Localhost	It might not work to query data from a probe device via SNMP (querying <a href="#">localhost</a> , <a href="#">127.0.0.1</a> , or <a href="#">::1</a> ). <a href="#">Add this device</a> with the IP address that it has in your network and create the sensor on this device instead.
Knowledge Base	Knowledge Base: <a href="#">How do I find out which OID I need for an SNMP Custom sensor?</a>

### Add Sensor

Setting	Description
Channel Name	<p>Enter a name for the channel in which the sensor shows the results for the OID. Enter a string.</p> <p><b>i</b> You can change this value later in the <a href="#">channel settings</a> of this sensor.</p>
Unit String	<p>Enter the unit for the values that this sensor returns. Enter a string.</p> <p><b>i</b> PRTG uses the unit string for display purposes and shows it in graphs, data tables, and gauges.</p> <p><b>i</b> You can change this value later in the <a href="#">channel settings</a> of this sensor.</p>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** i

Example Name

---

**Tags** i

exampletag x +

---

**Priority** i

★★★★☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- snmpcustomsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## OID Settings

### OID Settings

**OID** ⓘ

---

**Value Type** ⓘ

---

**Multiplication** ⓘ

---

**Division** ⓘ

---

**If Value Changes** ⓘ  Ignore (default)  
 Trigger 'change' notification

OID Settings

Setting	Description
OID	<p>Enter the OID of the SNMP object that you want to receive numeric data from.</p> <p> ⓘ Most OIDs begin with <b>1.3.6.1</b>. However, OIDs that start with <b>1.0</b>, or <b>1.1</b>, or <b>1.2</b> are also allowed. If you want to entirely disable the validation of your entry, add the string <b>norfccheck:</b> to the beginning of the OID, for example, <b>norfccheck:2.0.0.0.1</b>.</p>
Value Type	<p>Select the expected numeric type of the results at the OID:</p> <ul style="list-style-type: none"> <li>▪ Absolute (unsigned integer): Integers without an operational sign, such as <b>10</b> or <b>120</b>.</li> <li>▪ Absolute (signed integer): Integers with an operational sign, such as <b>-12</b> or <b>120</b>.</li> <li>▪ Absolute (float): Float values, such as <b>-5.80</b> or <b>8.23</b>.</li> <li>▪ Delta (counter): Counter values. PRTG calculates the difference between the last and the current value. PRTG additionally divides the delta value by a time period to indicate a speed value.</li> </ul> <p> ⓘ This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative values and decreasing values.</p> <p> ⓘ You cannot change this value after sensor creation.</p>

Setting	Description
Multiplication	If you want to multiply the received data with a certain value, enter the multiplier. Use the default value <b>1</b> to not change the received value. Enter an integer.
Division	If you want to divide the received data by a certain value, enter the divisor. Use the default value <b>1</b> to not change the received value. Enter an integer.
If Value Changes	<p>Define what the sensor does when its value changes:</p> <ul style="list-style-type: none"> <li>Ignore (default): Do nothing.</li> <li>Trigger 'change' notification: Send an internal message that indicates a change. <ul style="list-style-type: none"> <li><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</li> </ul> </li> </ul>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>

Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other above.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	<p>The single numeric value (int64) for a specified OID</p> <p> This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

How do I find out which OID I need for an SNMP Custom sensor?

- <https://kb.paessler.com/en/topic/903>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

 VIDEO TUTORIAL

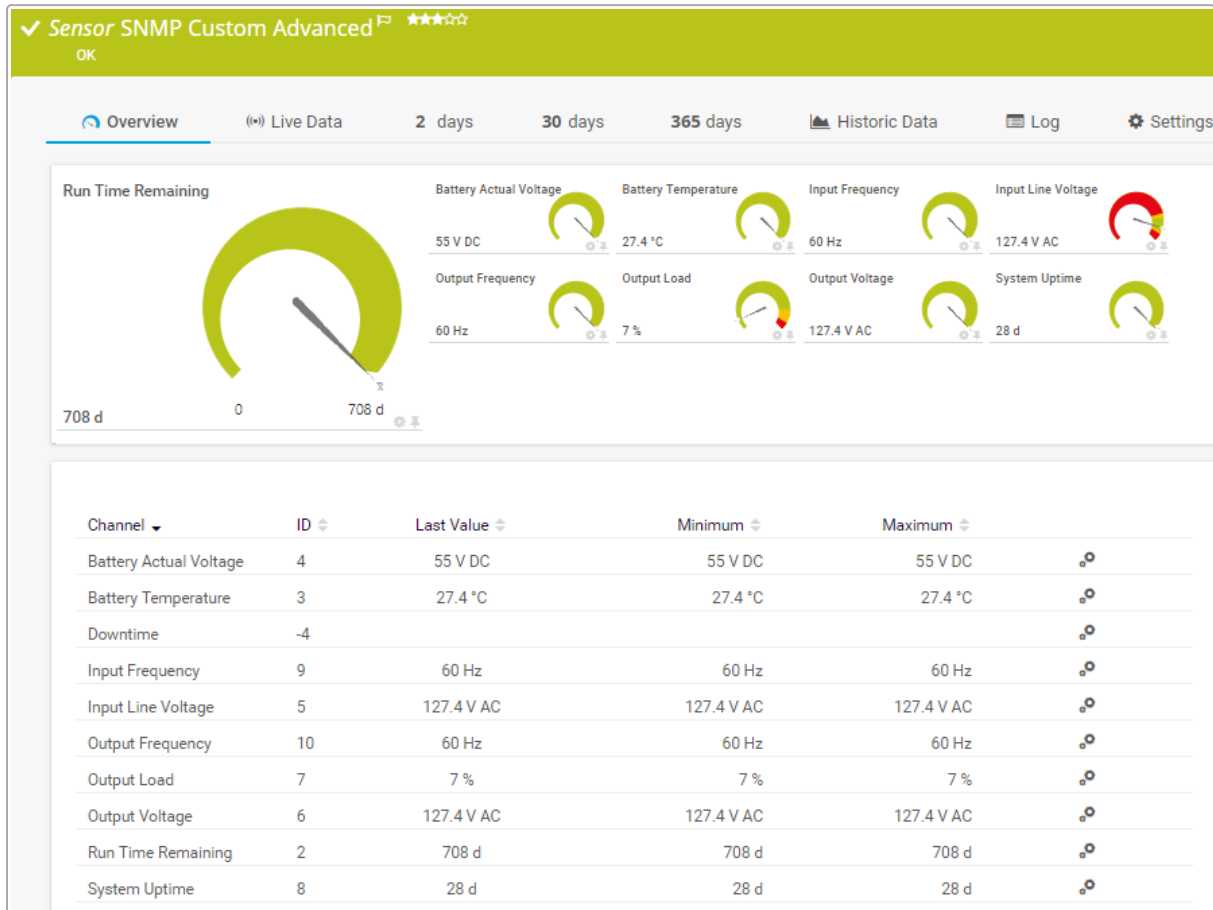
SNMP Custom sensor and SNMP Custom Library sensor

- <https://www.paessler.com/support/videos-and-webinars/videos/snmp-custom-and-library-sensor>

## 7.8.178 SNMP Custom Advanced Sensor

The SNMP Custom Advanced sensor monitors numeric values returned for object identifiers (OID) via the Simple Network Management Protocol (SNMP).

- ❶ The [SNMP Library](#) <sup>[2058]</sup> sensor automatically creates SNMP Custom Advanced sensors when the Management Information Base (MIB) file that you import contains single values.



SNMP Custom Advanced Sensor

- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) <sup>[1907]</sup>.

### Sensor in Other Languages

- Dutch: SNMP Aanpasbaar Geavanceerd
- French: SNMP personnalisé avancé
- German: SNMP (Benutzerdef. erweitert)
- Japanese: SNMP カスタムアドバンスト
- Portuguese: SNMP (customizado / avançado)
- Russian: Дополнительные пользовательские параметры SNMP
- Simplified Chinese: SNMP 自定义高级

- Spanish: SNMP (personalizado / avanzado)

## Remarks

Consider the following [remarks](#)<sup>1897</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
Lookups	This sensor can use <a href="#">lookups</a> <sup>1899</sup> . Select Lookup as Channel #x Unit and define the lookup file in Channel #x Lookup.
Localhost	It might not work to query data from a probe device via SNMP (querying <a href="#">localhost</a> , <a href="#">127.0.0.1</a> , or <a href="#">::1</a> ). <a href="#">Add this device</a> with the IP address that it has in your network and create the sensor on this device instead.
Knowledge Base	Knowledge Base: <a href="#">How do I find out which OID I need for an SNMP Custom sensor?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  X +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- snmpcustomadvanced
- snmpcustomsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.




## OID Settings

OID Settings	
Channel #1 Name ⓘ	1
Channel #1 OID ⓘ	1.3.6.1.2.1.1.3.0
Channel #1 Value Type ⓘ	Absolute (unsigned integer, for example "10", "120")
Channel #1 Unit ⓘ	Count
Channel #2 ⓘ	Disable

OID Settings

Setting	Description
Channel #x Name	Enter a name for the channel in which the sensor shows the results at the OID. Enter a string.
Channel #x OID	<p>Enter the OID of the SNMP object from which you want to receive numeric data.</p> <p>ⓘ Most OIDs begin with <a href="#">1.3.6.1</a>. However, OIDs that start with <a href="#">1.0</a>, or <a href="#">1.1</a>, or <a href="#">1.2</a> are also allowed. If you want to entirely disable the validation of your entry, add the string <a href="#">norfccheck:</a> to the beginning of the OID, for example, <a href="#">norfccheck:2.0.0.0.1</a>.</p>
Channel #x Value Type	<p>Select the expected numeric type of the results at the OID:</p> <ul style="list-style-type: none"> <li>▪ Absolute (unsigned integer): Integers without an operational sign, such as <a href="#">10</a> or <a href="#">120</a>.</li> <li>▪ Absolute (signed integer): Integers with an operational sign, such as <a href="#">-12</a> or <a href="#">120</a>.</li> <li>▪ Absolute (float): Float values, such as <a href="#">-5.80</a> or <a href="#">8.23</a>.</li> <li>▪ Delta (counter): Counter values. PRTG calculates the difference between the last and the current value. PRTG additionally divides the delta value by a time period to indicate a speed value.</li> </ul> <p>ⓘ This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative values and decreasing values.</p> <p>ⓘ Absolute (float) and Delta (counter) are not compatible with the unit Lookup.</p> <p>ⓘ You cannot change this value after sensor creation.</p>
Channel #x Unit	Define the unit of the numeric data that this sensor receives from the OID:



Setting	Description
	<ul style="list-style-type: none"> <li>▪ BytesBandwidth</li> <li>▪ BytesMemory</li> <li>▪ BytesDisk</li> <li>▪ Temperature</li> <li>▪ Percent</li> <li>▪ TimeResponse</li> <li>▪ TimeSeconds</li> <li>▪ TimeHours</li> <li>▪ Count</li> <li>▪ CPU</li> <li>▪ BytesFile</li> <li>▪ SpeedDisk</li> <li>▪ SpeedNet</li> <li>▪ Custom</li> <li>▪ Lookup</li> </ul> <p> For more information about the available units, see section <a href="#">Custom Sensors</a>.</p> <p> To use <a href="#">lookups</a> with this channel, select Lookup and define the lookup file in Channel #x Lookup. Do not use Custom if you use lookups with this sensor.</p> <p> You cannot use the unit Lookup if you select the value type Delta (counter) or Absolute (float). You are not able to create the sensor in this case.</p>
Channel #x Custom Unit	<p><a href="#">This setting is only visible if you select Custom above.</a></p> <p>Define a unit for the channel value. Enter a string.</p>
Channel #x Lookup	<p><a href="#">This setting is only visible if you select Lookup above.</a></p> <p>Select a <a href="#">lookup</a> file that you want to use with this channel.</p>
Channel #2 - #10	<p>You can define up to 10 channels. You must define at least one channel, so you see all available settings for <a href="#">Channel #1</a>. Specify how to handle all other possible channels:</p> <ul style="list-style-type: none"> <li>▪ Disable: Do not create this channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Enable: Create this channel.</li> </ul> <p><b>i</b> It is not possible to enable or disable channels after sensor creation.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	The numeric value for a specified OID (up to 10 OIDs are possible) that refers to a specific SNMP device

## More

### ■ KNOWLEDGE BASE

How do I find out which OID I need for an SNMP Custom sensor?

- <https://kb.paessler.com/en/topic/903>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

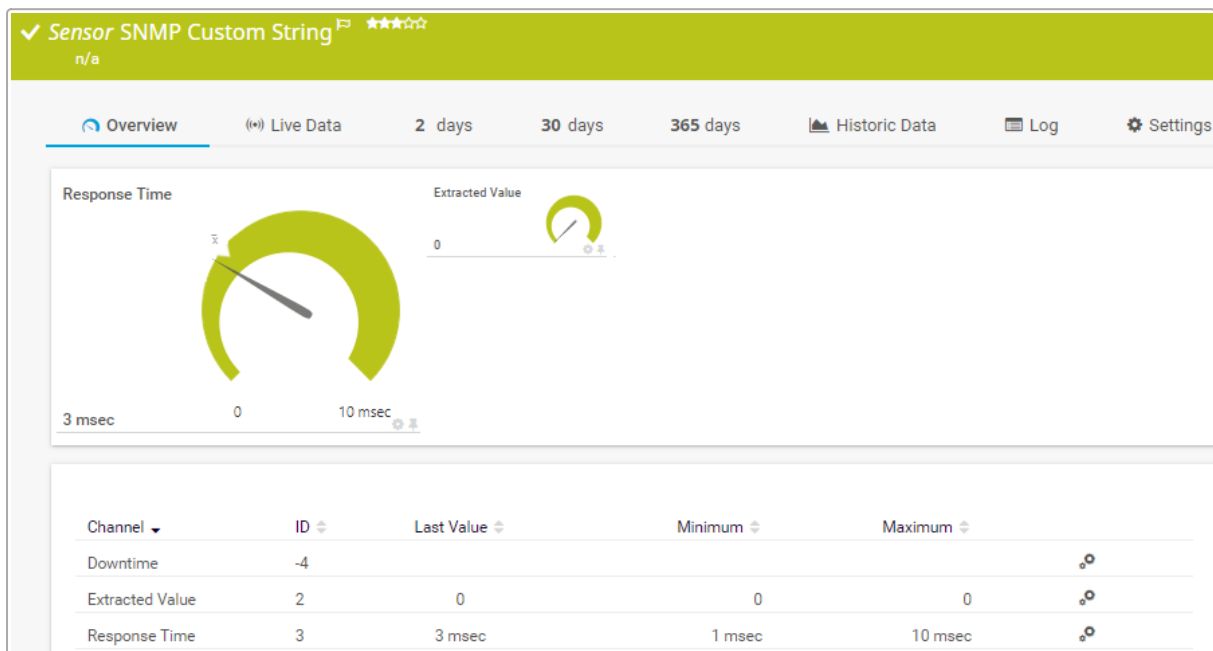
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.179 SNMP Custom String Sensor

The SNMP Custom String sensor monitors a string returned by a specific object identifier (OID) via the Simple Network Management Protocol (SNMP). It can check for keywords. If you want to set limits to the channel value, you can also extract a numeric value contained in the string.

- ❶ In the sensor message, the sensor shows the string that you [search](#) for and the reason for the Warning or Down [status](#).
- ❷ The [SNMP Library](#) sensor automatically creates SNMP Custom String sensors when the Management Information Base (MIB) file that you import contains string values.



SNMP Custom String Sensor

- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Aangepaste Tekenreeks
- French: Chaîne personnalisée (SNMP)
- German: SNMP-Zeichenfolge
- Japanese: SNMP カスタム文字列
- Portuguese: Sequência de caracteres (customizado) (SNMP)
- Russian: SNMP: строка ответа
- Simplified Chinese: SNMP 自定义字符串
- Spanish: Cadena (personalizado) (SNMP)

## Remarks

Consider the following [remarks](#)<sup>[1903]</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Localhost	It might not work to query data from a probe device via SNMP (querying <a href="#">localhost</a> , <a href="#">127.0.0.1</a> , or <a href="#">::1</a> ). <a href="#">Add this device</a> with the IP address that it has in your network and create the sensor on this device instead.
Knowledge Base	Knowledge Base: <a href="#">How do I find out which OID I need for an SNMP Custom sensor?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- snmpcustomstringsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## OID Settings

OID Settings
OID ⓘ 1.3.6.1.2.1.1.3.0

---

Maximum String Length ⓘ

If Value Changes ⓘ

Ignore (default)
 Trigger 'change' notification

OID Settings

Setting	Description
OID	<p>Enter the OID of the SNMP object that you want to receive a string from.</p> <p> ⓘ Most OIDs begin with <a href="#">1.3.6.1</a>. However, OIDs that start with <a href="#">1.0</a>, or <a href="#">1.1</a>, or <a href="#">1.2</a> are also allowed. If you want to entirely disable the validation of your entry, add the string <a href="#">norfccheck:</a> to the beginning of the OID, for example, <a href="#">norfccheck:2.0.0.0.1</a>.</p>
Maximum String Length	<p>Define the maximum length of the string that PRTG receives from the SNMP object at the OID. If the string is longer than this value, the sensor shows the Down status. Enter an integer or leave the field empty.</p>
If Value Changes	<p>Define what the sensor does when its value changes:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> <li>▪ Trigger 'change' notification: Send an internal message that indicates a change.</li> </ul> <p> ⓘ In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</p>

## Keyword Search

**Keyword Search**

Response Must Include (Down Status If Not Included) ⓘ

Search Method ⓘ  Simple string search (default)  
 Regular expression

---

Response Must Not Include (Down Status If Included) ⓘ

Search Method ⓘ  Simple string search (default)  
 Regular expression

---

Response Must Include (Warning Status If Not Included) ⓘ

Search Method ⓘ  Simple string search (default)  
 Regular expression










---

Response Must Not Include (Warning Status If Included) ⓘ

Search Method ⓘ  Simple string search (default)  
 Regular expression

Keyword Search

Setting	Description
Response Must Include (Down Status if Not Included)	<p>Define the search string that must be part of the data that PRTG receives from the SNMP object at the OID. You can enter a simple string in plain text or a <a href="#">regular expression (regex)</a>.</p> <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> The search string must be case-sensitive.</li> <li><span style="color: blue;">i</span> If the data does <b>not</b> include the search pattern, the sensor shows the Down status.</li> </ul>
Search Method	<p>Define the method with which you want to provide the search string:</p> <ul style="list-style-type: none"> <li>▪ Simple string search (default): Search for a simple string in plain text.</li> <li><span style="color: blue;">i</span> The characters <b>*</b> and <b>?</b> work as placeholders. <b>*</b> stands for no number or any number of characters and <b>?</b> stands for exactly one character. You cannot change this behavior. The literal search for these characters is only possible with a regex.</li> <li>▪ Regular expression: Search with a regex.</li> <li><span style="color: blue;">i</span> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</li> </ul>

Setting	Description
Response Must Not Include (Down Status if Included)	<p>Define the search string that must <b>not</b> be part of the data that PRTG receives from the SNMP object at the OID. You can enter a simple string in plain text or a regex.</p> <ul style="list-style-type: none"> <li> The search string must be case-sensitive.</li> <li> If the data does include the search pattern, the sensor shows the Down status.</li> </ul>
Search Method	<p>Define the method with which you want to provide the search string:</p> <ul style="list-style-type: none"> <li>▪ Simple string search (default): Search for a simple string in plain text.</li> <li> The characters <b>*</b> and <b>?</b> work as placeholders. <b>*</b> stands for no number or any number of characters and <b>?</b> stands for exactly one character. You cannot change this behavior. The literal search for these characters is only possible with a regex.</li> <li>▪ Regular expression: Search with a regex.</li> <li> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</li> </ul>
Response Must Include (Warning Status If Not Included)	<p>Define the search string that must be part of the data that PRTG receives from the SNMP object at the OID. You can enter a simple string in plain text or a regex.</p> <ul style="list-style-type: none"> <li> The search string must be case-sensitive.</li> <li> If the data does <b>not</b> include the search pattern, the sensor shows the Warning status.</li> </ul>
Search Method	<p>Define the method with which you want to provide the search string:</p> <ul style="list-style-type: none"> <li>▪ Simple string search (default): Search for a simple string in plain text.</li> <li> The characters <b>*</b> and <b>?</b> work as placeholders. <b>*</b> stands for no number or any number of characters and <b>?</b> stands for exactly one character. You cannot change this behavior. The literal search for these characters is only possible with a regex.</li> <li>▪ Regular expression: Search with a regex.</li> <li> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</li> </ul>
Response Must Not Include (Warning Status If Included)	<p>Define the search string that must <b>not</b> be part of the data that PRTG receives from the SNMP object at the OID. You can enter a simple string in plain text or a regex.</p> <ul style="list-style-type: none"> <li> The search string must be case-sensitive.</li> </ul>



Setting	Description
	<p><b>i</b> If the data does include the search pattern, the sensor shows the Warning status.</p>
Search Method	<p>Define the method with which you want to provide the search string:</p> <ul style="list-style-type: none"> <li>▪ Simple string search (default): Search for a simple string in plain text.</li> </ul> <p><b>i</b> The characters <b>*</b> and <b>?</b> work as placeholders. <b>*</b> stands for no number or any number of characters and <b>?</b> stands for exactly one character. You cannot change this behavior. The literal search for these characters is only possible with a regex.</p> <ul style="list-style-type: none"> <li>▪ Regular expression: Search with a regex.</li> </ul> <p><b>i</b> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</p>

## Extended Processing

**Extended Processing**

**Interpret Result As** **i**

String (default)

Bytes in hexadecimal notation

Bytes in decimal notation

**Numeric Value Extraction** **i**

Do not use extraction (default)

Use a regular expression for extraction

Extended Processing

Setting	Description
Interpret Result As	<p>Define the type of the received string:</p> <ul style="list-style-type: none"> <li>▪ String (default): Handle the result as a common string.</li> <li>▪ Bytes in hexadecimal notation: Handle the result as bytes in hexadecimal notation. For example, select this option if you monitor MAC addresses.</li> <li>▪ Bytes in decimal notation: Handle the result as bytes in decimal notation. For example, select this option if you monitor IP addresses.</li> </ul>
Numeric Value Extraction	<p>Define if you want to filter out a numeric value from the received string:</p> <ul style="list-style-type: none"> <li>▪ Do not use extraction (default): Do not extract a float value. Use the result as a string value.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Use a regular expression for extraction: Use a regular expression (regex) to identify a numeric value in the string and to convert it to a float value to use it, for example, with channel limits. Define below. See also the <a href="#">example</a><sup>[1908]</sup>. <ul style="list-style-type: none"> <li>For more information, see section <a href="#">Channel Settings</a>.</li> </ul> </li> </ul>
Regular Expression	<p><b>This setting is only visible if you select</b> Use a regular expression for extraction <a href="#">above</a>.</p> <p>Enter a regular expression to identify the numeric value that you want to extract from the string returned by the SNMP object at the specified OID. You can use capturing groups.</p> <p><b>i</b> Make sure that the expression only returns numbers, including the decimal and thousands separators.</p> <p><b>i</b> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</p>
Index of Capturing Group	<p><b>This setting is only visible if you select</b> Use a regular expression for extraction <a href="#">above</a>.</p> <p>If your regex uses capturing groups, specify which one captures the number. Enter an integer or leave the field empty.</p>
Decimal Separator	<p><b>This setting is only visible if you select</b> Use a regular expression for extraction <a href="#">above</a>.</p> <p>Define the character for the decimal separator of the number. Enter a string or leave the field empty.</p>
Thousands Separator	<p><b>This setting is only visible if you select</b> Use a regular expression for extraction <a href="#">above</a>.</p> <p>Define the character for the thousands separator of the number. Enter a string or leave the field empty.</p>

## Sensor Display




**Sensor Display**

Primary Channel ⓘ Downtime


---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display


Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Number Extraction with Regular Expression

 If you want to extract a number in the response string via a regex, note that the index for captures in this sensor is based on 1 (not on 0). Furthermore, capturing groups are not automatically created. The example below illustrates this issue.

Consider the following string as returned by a request for CPU usage:

```
5 Sec (3.49%), 1 Min (3.555%), 5 Min (3.90%)
```

Assuming you would like to filter for the number **3.555**, this is the percentage in the second parentheses. Enter the following regex in the Regular Expression field:

```
(\d+\.\d+).*?(\d+\.\d+).*?(\d+\.\d+)
```

As Index of Capturing Group, enter **3**. This extracts the desired number **3.555**.

The index must be 3 in this case because the capturing groups here are the following:

- Group 1 contains **3.49%**, **1 Min (3.555)**, **5 Min (3.90)**
- Group 2 contains **3.49**
- Group 3 contains **3.555**
- Group 4 contains **3.90**

Keep this note about index and capturing groups in mind when using number extraction.

- i** It is not possible to match an empty string with the PRTG regex sensor search.
- i** PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section [Regular Expressions](#).

## Channel List

- i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Extracted Value	The value extracted from the string (optional)
Response Time	The response time <b>i</b> This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

How do I find out which OID I need for an SNMP Custom sensor?

- <https://kb.paessler.com/en/topic/903>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

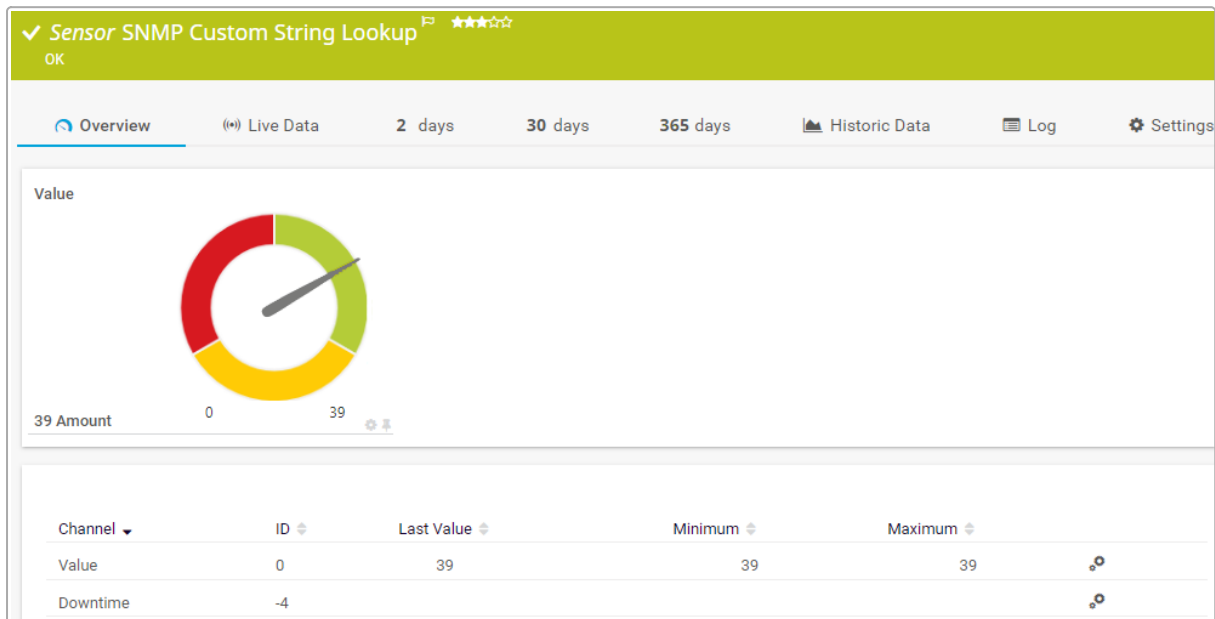
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.180 SNMP Custom String Lookup Sensor

The SNMP Custom String Lookup sensor monitors a string that a specific object identifier (OID) returns via the Simple Network Management Protocol (SNMP). It can map the string directly to a [sensor status](#) by using a [defined lookup file](#).

**i** Basically, this sensor does a "reverse lookup". You need to define all potential return strings in the lookup file as text values, each in one lookup entry. Graphs and data tables show the value to which the string is mapped, usually an integer ([lookup type](#) SingleInt). For more information, see section [Example](#)<sup>1914</sup>.



SNMP Custom String Lookup Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1913</sup>.

### Sensor in Other Languages

- Dutch: SNMP Aangepaste Tekst Lookup
- French: Recherche chaînes personnalisée (SNMP)
- German: SNMP-Zeichenfolge mit Lookup
- Japanese: SNMP カスタム文字列のルックアップ
- Portuguese: Pesquisa da sequência de caracteres (customizado) (SNMP)
- Russian: Подстановка пользовательской строки по SNMP
- Simplified Chinese: SNMP 自定义字符串查询
- Spanish: Búsqueda de cadena (personalizado) (SNMP)

### Remarks

Consider the following [remarks](#)<sup>1911</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Localhost	It might not work to query data from a probe device via SNMP (querying <a href="#">localhost</a> , <a href="#">127.0.0.1</a> , or <a href="#">::1</a> ). <a href="#">Add this device</a> with the IP address that it has in your network and create the sensor on this device instead.
Knowledge Base	Knowledge Base: <a href="#">How do I find out which OID I need for an SNMP Custom sensor?</a>

## Add Sensor

Setting	Description
Channel Name	<p>Enter a name for the channel in which the sensor shows the results for the OID. Enter a string.</p> <p><b>i</b> You can change this value later in the <a href="#">channel settings</a> of this sensor.</p>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** i

**Tags** i

**Priority** i

Example Name

exampletag
✕
+

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- snmpcustomsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## OID Settings

### OID Settings

**OID** ⓘ 1.3.6.1.2.1.1.3.0

---

**Lookup** ⓘ *oid.paessler.hplaserjet.jamstatus*

**If Value Changes** ⓘ  Ignore (default)  
 Trigger 'change' notification

OID Settings

Setting	Description
OID	<p>Enter the OID of the SNMP object that you want to receive a string from.</p> <p>ⓘ Most OIDs begin with <a href="#">1.3.6.1</a>. However, OIDs that start with <a href="#">1.0</a>, or <a href="#">1.1</a>, or <a href="#">1.2</a> are also allowed. If you want to entirely disable the validation of your entry, add the string <a href="#">norfccheck:</a> to the beginning of the OID, for example, <a href="#">norfccheck:2.0.0.0.1</a>.</p>
Lookup	<p>Select a lookup file that is available in the \lookups\custom subfolder of the <a href="#">PRTG program directory</a> on the probe system.</p> <p>ⓘ The lookup file must contain all potential strings that the OID can return.</p> <p>ⓘ You cannot change this value after sensor creation.</p>
If Value Changes	<p>Define what the sensor does when its value changes:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> <li>▪ Trigger 'change' notification: Send an internal message that indicates a change.</li> </ul> <p>ⓘ In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</p>

## Sensor Display




### Sensor Display

**Primary Channel** ⓘ Downtime


---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display


Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Example

 You must provide all possible return strings for this sensor in one lookup file. For example, consider an OID that can return one of the three strings [Good](#), [Deficient](#), or [Bad](#). Then you must [define a lookup file](#) for this sensor that contains all these possible string values as text, each text value in one lookup entry:



```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="mylookupfile" desiredValue="0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="PaeValueLookup.xsd">
  <Lookups>
    <SingleInt state="OK" value="0">
      Good
    </SingleInt>
    <SingleInt state="Warning" value="1">
      Deficient
    </SingleInt>
    <SingleInt state="Error" value="2">
      Bad
    </SingleInt>
  </Lookups>
</ValueLookup>
```

If a retrieved string matches one of the text values, the sensor maps it into the defined integer ("reverse lookup") that is shown, for example, in data graphs. Depending on the integer, the sensor shows the respective status and converts the integer back to the original string to show it as a channel value. If the OID returns a string that the lookup definition does not contain, the sensor shows the Down status with a corresponding error message.

For example, you create an SNMP Custom String Lookup sensor, apply the example lookup definition from above (store it into the \lookups\custom subfolder of the PRTG program directory), and the specified OID returns the string **Good**. Then the sensor maps the string **Good** to the integer **0** that is shown in the live graph of the sensor, for example. According to the status definition `state="OK"`, the sensor status is Up in this case. The integer **0** is converted back to the string **Good**, which is shown as the channel value.


**i** The string match is not case-sensitive.

**i** Use the lookup type `SingleInt` for this sensor. `BitFields` and ranges are not supported.

**■** If you [imported an SNMP library](#) (this is an `.oidlib` file) that contains [lookups](#) (you can see this in section [Lookup](#) in the MIB Importer), you can define your own sensor states for returning values. Use the lookupname of the imported SNMP library as id parameter in a custom lookup definition. This overrides the lookups that an `.oidlib` file might contain with your own status definitions. See section [Define Lookups](#) for details about this mechanism.

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	The retrieved string value and its status, as defined in the corresponding lookup file   This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

How do I find out which OID I need for an SNMP Custom sensor?

- <https://kb.paessler.com/en/topic/903>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

### PAESSLER TOOLS

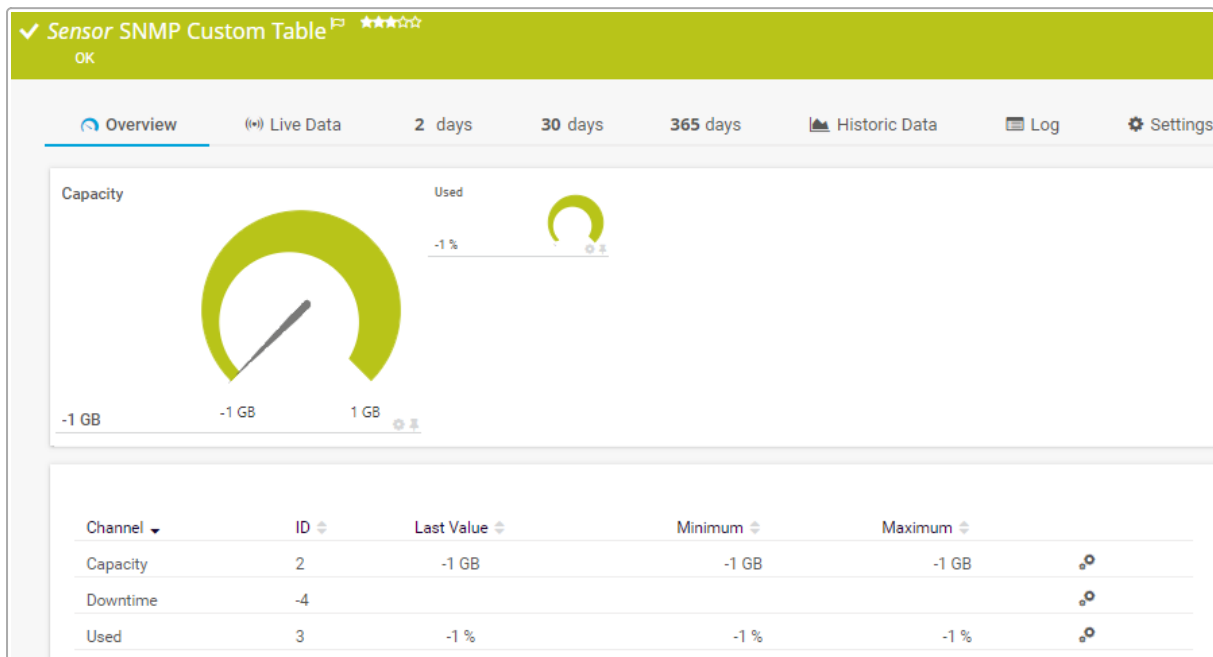
MIB Importer

- <https://www.paessler.com/tools/mibimporter>

## 7.8.181 SNMP Custom Table Sensor

The SNMP Custom Table sensor monitors entries from a table that is provided via the Simple Network Management Protocol (SNMP). You can create one new sensor per table row. For each sensor, you can define up to ten channels. Each channel shows the value of one defined table column.

- ❶ The [SNMP Library](#)<sup>[2058]</sup> sensor automatically creates SNMP Custom Table sensors when the Management Information Base (MIB) file that you import contains tables.



SNMP Custom Table Sensor

- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1923]</sup>.

### Sensor in Other Languages

- Dutch: SNMP Aangepaste Tabel
- French: Table personnalisée (SNMP)
- German: SNMP (Benutzerdef. Tabelle)
- Japanese: SNMP カスタムテーブル
- Portuguese: Tabela (customizada) (SNMP)
- Russian: Нестандартная таблица SNMP
- Simplified Chinese: SNMP 自定义表
- Spanish: Tabla (personalizado) (SNMP)

### Remarks

Consider the following [remarks](#)<sup>[1917]</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
Lookups	This sensor can use <a href="#">lookups</a> <sup>1920</sup> . Select Lookup as Channel #x Unit and define the lookup file in Channel #x Lookup.
Localhost	It might not work to query data from a probe device via SNMP (querying <a href="#">localhost</a> , <a href="#">127.0.0.1</a> , or <a href="#">::1</a> ). <a href="#">Add this device</a> with the IP address that it has in your network and create the sensor on this device instead.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">How do I find out which OID I need for an SNMP Custom sensor?</a></li> <li>Knowledge Base: <a href="#">What can I monitor with the SNMP Custom Table sensor?</a></li> </ul>

### Add Sensor

Setting	Description
Table	The sensor shows you the table that the OID returns. Select the table rows that contain the data that you want to monitor. PRTG creates one sensor for each table row that you select.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

**Tags** ⓘ 

✕
+

**Priority** ⓘ 
★
★
★
☆
☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- snmpcustomsensor
- snmpcustomtable

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## SNMP Table

SNMP Table
Table OID ⓘ **1.3.6.1.2.1.1.3.0**

SNMP Table

Setting	Description
Table OID	<p>Enter the object identifier (OID) of the SNMP table that you want to monitor. The OID must directly point to an object that represents an SNMP table. PRTG creates one SNMP Custom Table sensor for each table row that you select.</p> <ul style="list-style-type: none"> <li>ⓘ If you do not enter an OID, you cannot proceed with channel creation.</li> <li>ⓘ You cannot change this value after sensor creation.</li> </ul>

## Table Specific

Table Specific

Identifier ⓘ **196608**

---

Identification Column ⓘ *table\_index*

---

Channel #1 Name ⓘ CPU Load (1 min average)

---

Channel #1 Column ⓘ hrProcessorLoad

---

Channel #1 Value Type ⓘ *Absolute (signed integer, for example "-12", "120")*

---

Channel #1 Unit ⓘ Percent




---

Channel #2 ⓘ *Disable*

Table Specific

Setting	Description
Identifier	This is the value of the column that you selected as the Identification Column during sensor creation. PRTG also displays it in the sensor name to distinguish it from other sensors you created for the same table with other table rows.
Identification Column	Define the identification column for the sensors that you want to create. The sensors use this column to uniquely identify each table row.

Setting	Description
	<ul style="list-style-type: none"> <li><span style="color: red;">i</span> We recommend that you use a unique identification column because it allows the sensors to keep track of changing indexes.</li> <li><span style="color: red;">i</span> The value of the column that you select as identification column replaces the <a href="#">[rowidentifier]</a> in the sensor name. This lets you distinguish sensors that you create for the same SNMP table.</li> <li><span style="color: red;">i</span> After sensor creation, this setting shows the table column that you chose as identification column.</li> </ul>
Channel #x Name	Enter a name for the channel in which the sensor shows the desired result. Enter a string.
Channel #x Column	Select the table column that, together with the table row, points to the value that you want to monitor in this channel. You can choose between the available columns of the table that you monitor.
Channel #x Value Type	<p>Select the expected numeric type of the results at the OID:</p> <ul style="list-style-type: none"> <li>▪ Absolute (unsigned integer): Integers without an operational sign, such as <a href="#">10</a> or <a href="#">120</a>.</li> <li>▪ Absolute (signed integer): Integers with an operational sign, such as <a href="#">-12</a> or <a href="#">120</a>.</li> <li>▪ Absolute (float): Float values, such as <a href="#">-5.80</a> or <a href="#">8.23</a>.</li> <li>▪ Delta (counter): Counter values. PRTG calculates the difference between the last and the current value. PRTG additionally divides the delta value by a time period to indicate a speed value.</li> </ul> <ul style="list-style-type: none"> <li><span style="color: red;">i</span> This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative values and decreasing values.</li> <li><span style="color: red;">i</span> Absolute (float) and Delta (counter) are not compatible with the unit Lookup.</li> <li><span style="color: red;">i</span> See <a href="#">below</a> <sup>[1919]</sup> for other channel settings that you can also change after sensor creation.</li> <li><span style="color: red;">i</span> This sensor monitors numeric values only. Make sure that you do not select columns that return strings because they lead to the <a href="#">Down status</a>. For example, if you monitor an ifTable, we recommend that you do not select an ifDescr column because this results in an error.</li> <li><span style="color: red;">i</span> You cannot change this value after sensor creation.</li> </ul>
Channel #x Unit	<p>Define the unit of the data that this sensor receives in this channel:</p> <ul style="list-style-type: none"> <li>▪ BytesBandwidth</li> <li>▪ BytesMemory</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ BytesDisk</li> <li>▪ Temperature</li> <li>▪ Percent</li> <li>▪ TimeResponse</li> <li>▪ TimeSeconds</li> <li>▪ TimeHours</li> <li>▪ Count</li> <li>▪ CPU</li> <li>▪ BytesFile</li> <li>▪ SpeedDisk</li> <li>▪ SpeedNet</li> <li>▪ Custom</li> <li>▪ Lookup</li> </ul> <p> For more information about the available units, see section <a href="#">Custom Sensors</a>.</p> <p> To use <a href="#">lookups</a> with this channel, select Lookup and define the lookup file in Channel #x Lookup. Do not use Custom if you use lookups with this sensor.</p> <p> You cannot use the unit Lookup if you select the value type Delta (counter) or Absolute (float). You are not able to create the sensor in this case.</p>
Channel #x Custom Unit	<p><a href="#">This setting is only visible if you select Custom above.</a></p> <p>Define a unit for the channel value. Enter a string.</p>
Channel #x Lookup	<p><a href="#">This setting is only visible if you select Lookup above.</a></p> <p>Select a <a href="#">lookup</a> file that you want to use with this channel.</p>
Channel #2 - #10	<p>You can define up to 10 channels. You must define at least one channel, so you see all available settings for <a href="#">Channel #1</a>. Specify how to handle all other possible channels:</p> <ul style="list-style-type: none"> <li>▪ Disable: Do not create this channel.</li> <li>▪ Enable: Create this channel.</li> </ul>

Setting	Description
	<p><b>i</b> It is not possible to enable or disable channels after sensor creation.</p> <p><b>i</b> All channels that you define during the creation of an SNMP Custom Table sensor are the same for all sensors for each table row.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>



## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	The returned numeric values in up to ten channels per table row

## More

### ■ KNOWLEDGE BASE

How do I find out which OID I need for an SNMP Custom sensor?

- <https://kb.paessler.com/en/topic/903>

What can I monitor with the SNMP Custom Table sensor?

- <https://kb.paessler.com/en/topic/68539>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

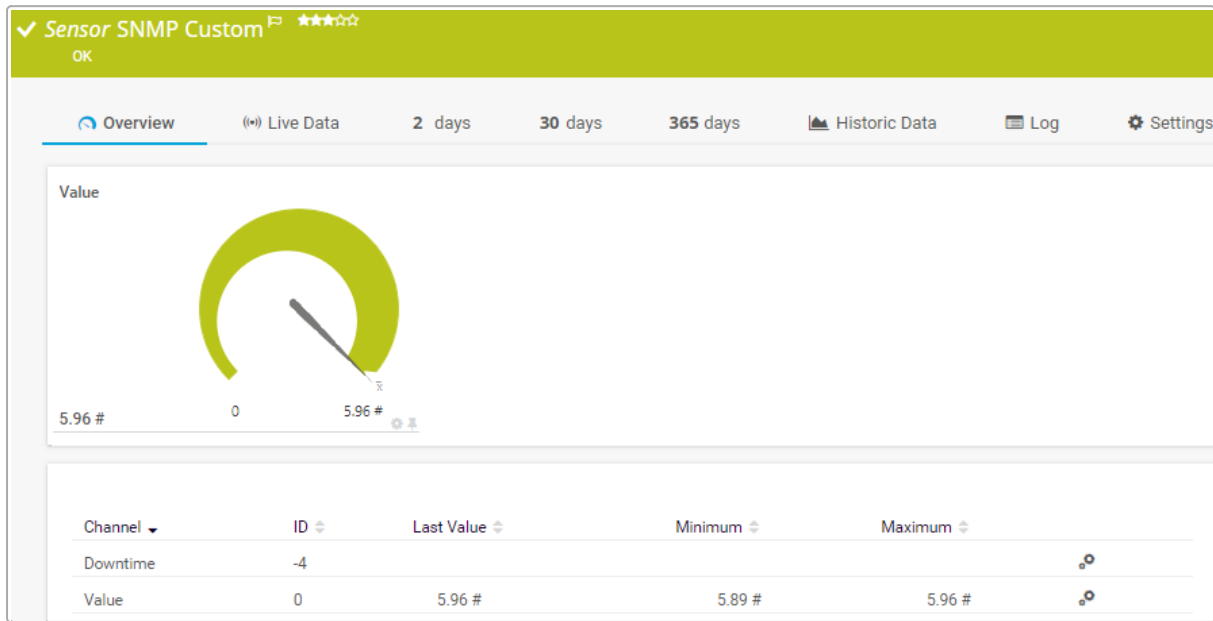
Can I monitor UPS systems complying with the UPS MIB (RFC-1628) with PRTG?

- <https://kb.paessler.com/en/topic/72117>

## 7.8.182 SNMP Custom v2 Sensor (BETA)

The SNMP Custom v2 sensor monitors a single parameter that is returned by a specific object identifier (OID) or Abstract Syntax Notation One (ASN.1) Management Information Base (MIB) via the Simple Network Management Protocol (SNMP).

**BETA** This sensor is in beta status. The operating methods and the available settings are still subject to change. Do not expect that all functions work properly, or that this sensor works as expected at all.



SNMP Custom v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1923</sup>.

### Sensor in Other Languages

- Dutch: SNMP Aangepast v2
- French: SNMP personnalisé v2
- German: SNMP (Benutzerdef.) v2
- Japanese: SNMP カスタム v2
- Portuguese: SNMP (customizado) v2
- Russian: SNMP Custom v2
- Simplified Chinese: SNMP 自定义 v2
- Spanish: SNMP (personalizado) v2

### Remarks

Consider the following [remarks](#)<sup>1924</sup> and requirements for this sensor:

Remark	Description
Enabled Beta Sensors experimental feature	This sensor requires that the Beta Sensors <a href="#">experimental feature</a> is enabled.  ■ For more information, see the Knowledge Base: <a href="#">What are beta sensors and how can I use them?</a>
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Localhost	It might not work to query data from a probe device via SNMP (querying <a href="#">localhost</a> , <a href="#">127.0.0.1</a> , or <a href="#">::1</a> ). <a href="#">Add this device</a> with the IP address that it has in your network and create the sensor on this device instead.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">1 minute</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.
Knowledge Base	Knowledge Base: <a href="#">How do I find out which OID I need for an SNMP Custom sensor?</a>

## Basic Sensor Settings

### Basic Sensor Settings

Sensor Name ⓘ

Tags ⓘ

Priority ⓘ

Example Name

exampletag ✕ +

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- snmp
- snmpcustomsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## SNMP Custom Specific

### SNMP Custom Specific

**OID or ASN.1 MIB Name** ⓘ 1.3.5.1.2.1.1.3.0

**Value Type** ⓘ *Time (unsigned integer)*

**Channel Unit** ⓘ *Time (seconds, default)*

SNMP Custom Specific

Setting	Description
OID or ASN.1 MIB Name	<p>Enter the OID or ASN.1 MIB name of the SNMP object that you want to receive numeric data from.</p> <p> ⓘ Most OIDs begin with <b>1.3.6.1</b>. However, OIDs that start with <b>1.0</b>, or <b>1.1</b>, or <b>1.2</b> are also allowed. If you want to entirely disable the validation of your entry, add the string <b>norfccheck:</b> to the beginning of the OID, for example, <b>norfccheck:2.0.0.0.1</b>.</p>
Value Type	<p>Select the expected numeric type of the result:</p> <ul style="list-style-type: none"> <li>▪ Absolute (unsigned integer) (default): Integers without an operational sign, such as <b>10</b> or <b>120</b>.</li> <li>▪ Absolute (signed integer): Integers with an operational sign, such as <b>-12</b> or <b>120</b>.</li> <li>▪ Absolute (floating point): Float values, such as <b>-5.80</b> or <b>8.23</b>.</li> <li>▪ Delta (unsigned integer): Integers without an operational sign, such as <b>10</b> or <b>120</b>. The sensor calculates the difference between the last value and the current value.</li> <li>▪ Time (unsigned integer): Integers without an operational sign, such as <b>10</b> or <b>120</b>. The sensor measures the response time.</li> </ul> <p> ⓘ You cannot change this value after sensor creation.</p>
Channel Unit	<p>Define the unit of the numeric data that this sensor receives. The following options are only visible if you select Absolute (unsigned integer), Absolute (signed integer), Absolute (floating point), or Delta (unsigned integer) as Value Type:</p>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Custom</li> <li>▪ Count (default)</li> <li>▪ Percent (CPU)</li> <li>▪ Temperature (°C)</li> <li>▪ Bytes (memory)</li> <li>▪ Bytes (disk)</li> <li>▪ Bytes (bandwidth)</li> <li>▪ Bytes per second (disk)</li> <li>▪ Bytes per second (network)</li> </ul> <p>The following options are only visible if you select Time (unsigned integer) as Value Type:</p> <ul style="list-style-type: none"> <li>▪ Time (milliseconds)</li> <li>▪ Time (seconds, default)</li> <li>▪ Time (hours)</li> </ul> <p><span style="color: #0070C0;">■</span> For more information about the available units, see section <a href="#">Custom Sensors</a>.</p> <p><span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px;">i</span> You cannot change this value after sensor creation.</p>
Multiplication	If you want to multiply the received data with a certain value, enter the multiplier. Use the default value <b>1</b> to not change the received value. Enter an integer.
Division	If you want to divide the received data by a certain value, enter the divisor. Use the default value <b>1</b> to not change the received value. Enter an integer.

## Sensor Display


**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

**Result Handling** **i**
 Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <p>Do not store the sensor result.</p> <p>Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</p> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Result	The single numeric value for a specified OID  This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

How do I find out which OID I need for an SNMP Custom sensor?

- <https://kb.paessler.com/en/topic/903>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

How do I use Management Information Base (MIB) folders with the SNMP Custom v2 sensor?

- <https://kb.paessler.com/en/topic/91688>

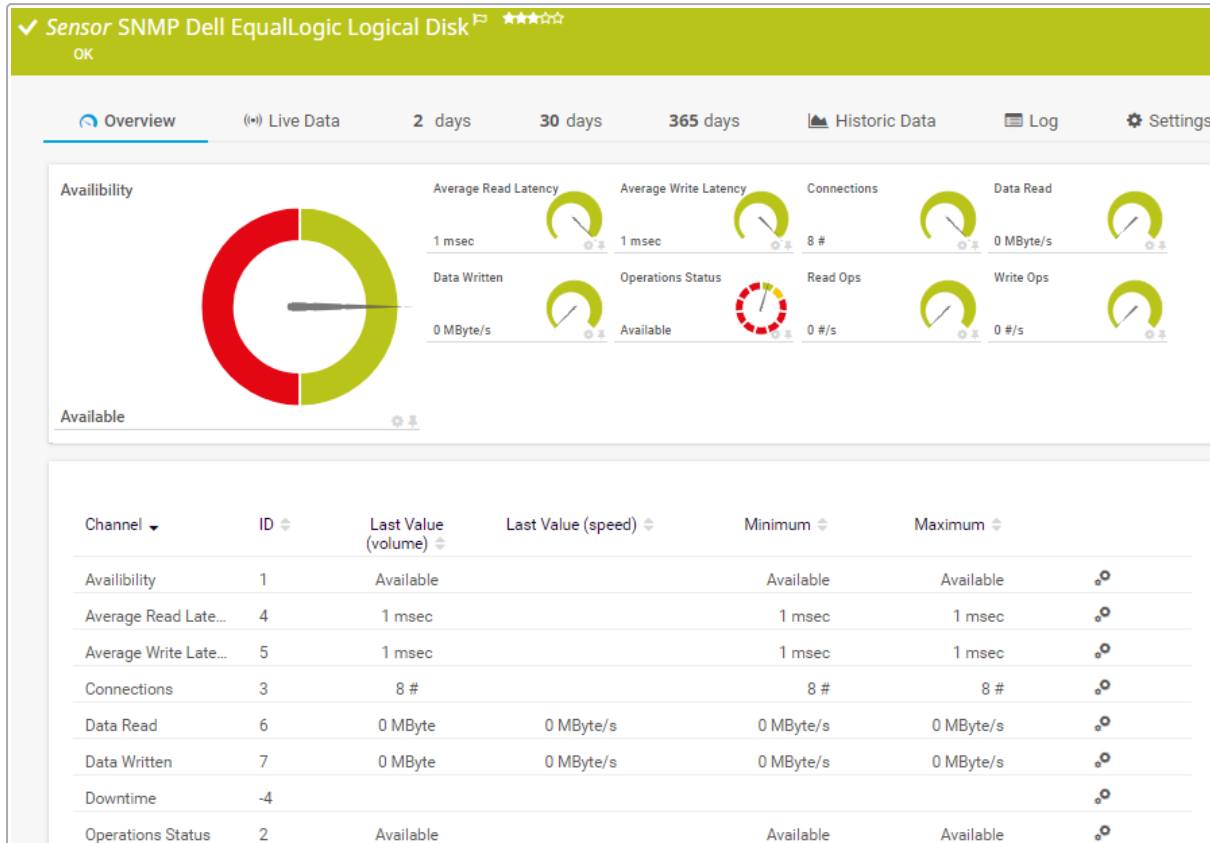
### VIDEO TUTORIAL

SNMP Custom sensor and SNMP Custom Library sensor

- <https://www.paessler.com/support/videos-and-webinars/videos/snmp-custom-and-library-sensor>

## 7.8.183 SNMP Dell EqualLogic Logical Disk Sensor

The SNMP Dell EqualLogic Logical Disk sensor monitors a volume of a Dell EqualLogic storage system via the Simple Network Management Protocol (SNMP).



SNMP Dell EqualLogic Logical Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1933</sup>.

### Sensor in Other Languages

- Dutch: SNMP Dell EqualLogic Logische Schijf
- French: Dell EqualLogic disque logique (SNMP)
- German: SNMP Dell EqualLogic Logischer Datenträger
- Japanese: SNMP Dell EqualLogic 論理ディスク
- Portuguese: Disco lógico Dell EqualLogic (SNMP)
- Russian: Логический диск SNMP Dell EqualLogic
- Simplified Chinese: SNMP Dell EqualLogic 逻辑磁盘
- Spanish: Disco lógico Dell EqualLogic (SNMP)

### Remarks

Consider the following [remarks](#)<sup>1930</sup> and requirements for this sensor:



Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- dell
- dellequallogic
- snmpdell

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Dell EqualLogic Specific

#### Dell EqualLogic Specific

**Volumes** ⓘ Storage eql01/example

---

**Member ID** ⓘ 123456789

---

**Volume ID** ⓘ 1a2b3d4c

---

**Volume Description** ⓘ

Dell EqualLogic Specific

Setting	Description
Volumes	The volume that this sensor monitors.
Member ID	The member ID of the volume that this sensor monitors.
Volume ID	The ID of the volume that this sensor monitors.
Volume Description	The description of the volume that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Availability	<p>The availability status</p> <ul style="list-style-type: none"> <li>▪ Up status: Available</li> <li>▪ Down status: Missing Members</li> </ul> <p> This channel is the primary channel by default.</p>
Average Read Latency	The average read latency
Average Write Latency	The average write latency
Connections	The number of connections
Data Read	The data read speed
Data Written	The data write speed
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Operations Status	<p>The operations status</p> <ul style="list-style-type: none"> <li>▪ Up status: Available</li> <li>▪ Warning status: Available But No New Connections</li> <li>▪ Down status: Not Available, Not Available Due To, Not Available Due To Internal Error, Not Available Due To Lost Cached Blocks, Not Available Due To Members Offline, Not Available Due To Missing Pages, Not Available Due To No Space For Auto Grow, Not Available Due To Snap Reserve Met, Not Available Due To Thin Max Growth Met,</li> </ul>

Channel	Description
Read Ops	The number of disk read operations
Write Ops	The number of disk write operations

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

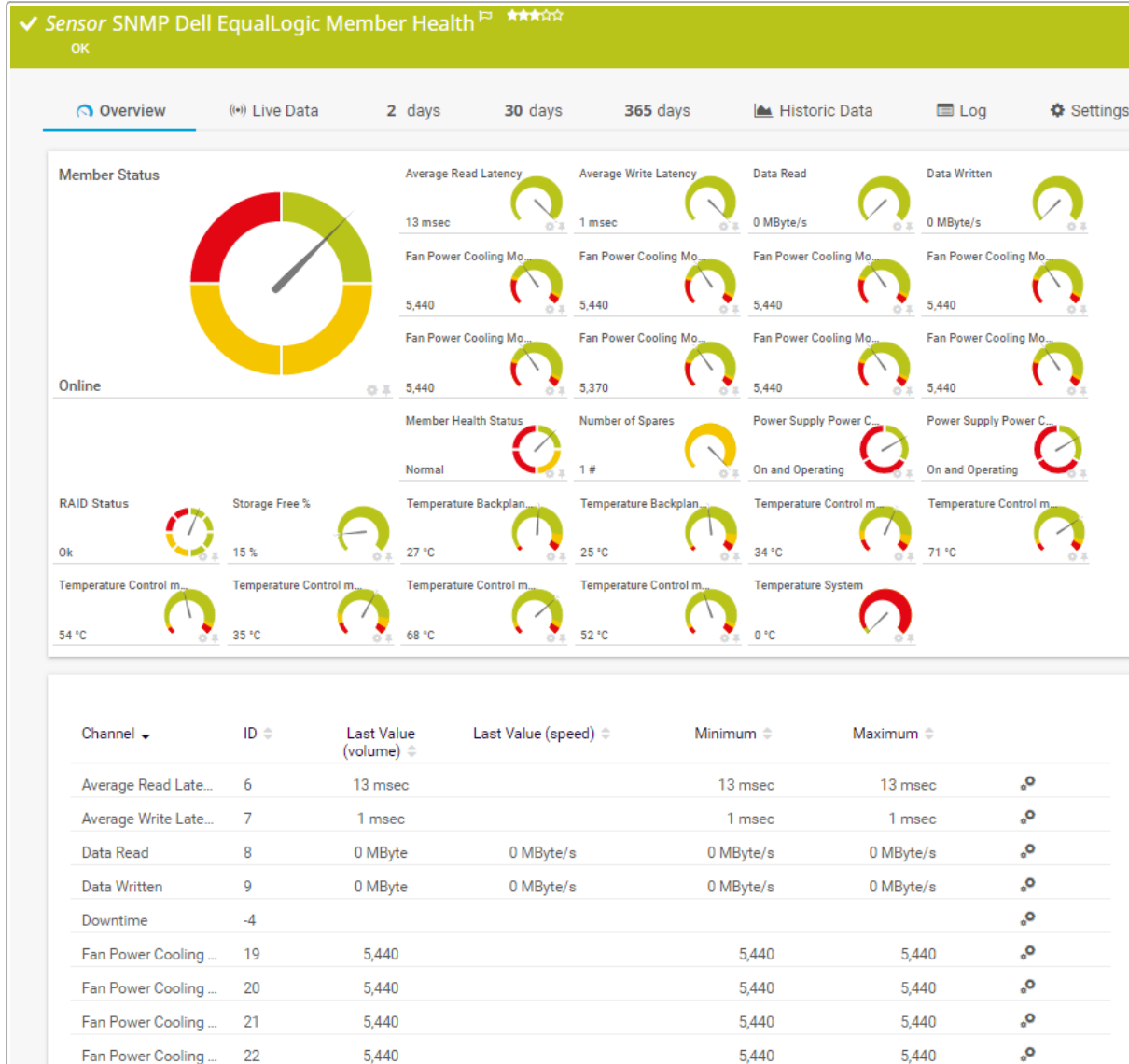
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.184 SNMP Dell EqualLogic Member Health Sensor

The SNMP Dell EqualLogic Member Health sensor monitors the health of an array member of an EqualLogic storage system via the Simple Network Management Protocol (SNMP).



SNMP Dell EqualLogic Member Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Dell EqualLogic Lid Gezondheid
- French: Dell EqualLogic état du composant (SNMP)
- German: SNMP Dell EqualLogic Member-Zustand
- Japanese: SNMP Dell EqualLogic のメンバー 正常性
- Portuguese: Funcionamento do membro Dell EqualLogic (SNMP)

- Russian: Работоспособность элемента Dell EqualLogic по SNMP
- Simplified Chinese: SNMP Dell EqualLogic 成员 健康状况
- Spanish: Salud de miembro Dell EqualLogic (SNMP)

## Remarks

Consider the following [remarks](#)<sup>1936</sup> and requirements for this sensor:

Remark	Description
SNMP v1	This sensor works with <a href="#">SNMP v2c</a> and <a href="#">SNMP v3</a> . It does not support <a href="#">SNMP v1</a> . Make sure that you set the correct SNMP Version in the <a href="#">settings</a> of an object that is higher in the <a href="#">object hierarchy</a> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

**Tags** ⓘ exampletag ✕ ⊕

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- dell
- dellequallogic
- snmpdell

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Dell EqualLogic Specific

**Dell EqualLogic Specific**

Array Member ⓘ *examplegroup1/member2*

Group ID ⓘ *1*

Member ID ⓘ *0123456789*

Dell EqualLogic Specific

Setting	Description
Array Member	The name of the member that this sensor monitors.
Group ID	The group ID of the member that this sensor monitors.
Member ID	The ID of the group member that this sensor monitors.

## Sensor Display


**Sensor Display**

Primary Channel ⓘ *Downtime*


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Average Read Latency	The average read latency
Average Write Latency	The average write latency
Data Read	The data read speed
Data Written	The data write speed
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status



Channel	Description
Fan Power Cooling Module [#] Fan [#]	The power of the cooling module fan
Member Health Status	The member health status <ul style="list-style-type: none"> <li>Up status: Normal</li> <li>Warning status: Warning</li> <li>Down status: Critical, Unknown</li> </ul>
Member Status	The member status <ul style="list-style-type: none"> <li>Up status: Online</li> <li>Warning status: Vacated, Vacating</li> <li>Down status: Offline</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Number of Spares	The number of spare drives <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Lower warning limit: 1</li> </ul>
Power Supply Power Cooling Module [#]	The power supply cooling module status <ul style="list-style-type: none"> <li>Up status: On and Operating</li> <li>Down status: Failed or No Data, No AC Power</li> </ul>
RAID Status	The RAID status <ul style="list-style-type: none"> <li>Up status: Expanding, Mirroring, Ok, Verifying</li> <li>Warning status: Degraded, Reconstructing</li> <li>Down status: Catastrophic Loss, Failed</li> </ul>
Storage Free %	The free storage (%)
Temperature Control Module [#] [Module]	The control module temperature

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

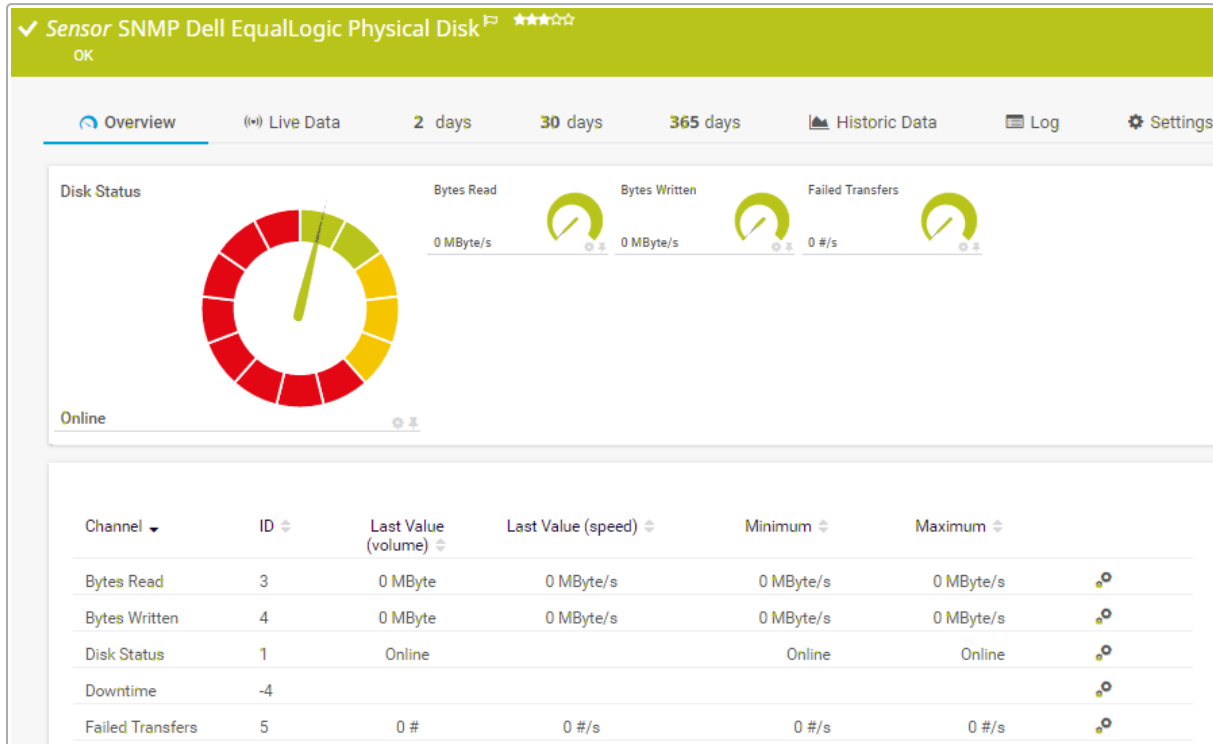
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.185 SNMP Dell EqualLogic Physical Disk Sensor

The SNMP Dell EqualLogic Physical Disk sensor monitors a disk in a Dell EqualLogic storage system via the Simple Network Management Protocol (SNMP).



SNMP Dell EqualLogic Physical Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Dell EqualLogic Fysieke Schijf
- French: Dell EqualLogic disque physique (SNMP)
- German: SNMP Dell EqualLogic Physikalischer Datenträger
- Japanese: SNMP Dell EqualLogic 物理ディスク
- Portuguese: Disco físico Dell EqualLogic (SNMP)
- Russian: Физический диск Dell EqualLogic по SNMP
- Simplified Chinese: SNMP Dell EqualLogic 物理磁盘
- Spanish: Disco físico Dell EqualLogic (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

**Basic Sensor Settings**

Sensor Name ⓘ Example Name

Tags ⓘ  ✕ +

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- dell
- dellequallogic
- snmpdell

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Dell EqualLogic Specific

#### Dell EqualLogic Specific

**Disk** ⓘ *Example*

**Group ID** ⓘ *1*

**Member ID** ⓘ *0123456789*

**Disk Slot** ⓘ *0*

**Serial Number** ⓘ *0123\_4567*

**Manufactured** ⓘ

Dell EqualLogic Specific

Setting	Description
Disk	The physical disk that this sensor monitors.
Group ID	The group ID of the physical disk that this sensor monitors.
Member ID	The group member ID of the physical disk that this sensor monitors.
Disk Slot	The slot number of the physical disk that this sensor monitors.
Serial Number	The serial number of the physical disk that this sensor monitors.
Manufactured	The production date of the physical disk that this sensor monitors. If this field is empty, the physical disk does not provide information about the date (this depends on the manufacturer).


### Sensor Display

#### Sensor Display


**Primary Channel** ⓘ Downtime


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Bytes Read	The number of bytes read
Bytes Written	The number of bytes written

Channel	Description
Disk Status	<p>The disk health status</p> <ul style="list-style-type: none"> <li>▪ Up status: Online, Spare</li> <li>▪ Warning status: Alt-Sig, History Of Failures, Replacement</li> <li>▪ Down status: Encrypted, Failed, Not Approved, Offline, Preempt Failed, Too Small, Unhealthy, Unsupported Version</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Failed Transfers	<p>The number of failed transfers</p>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

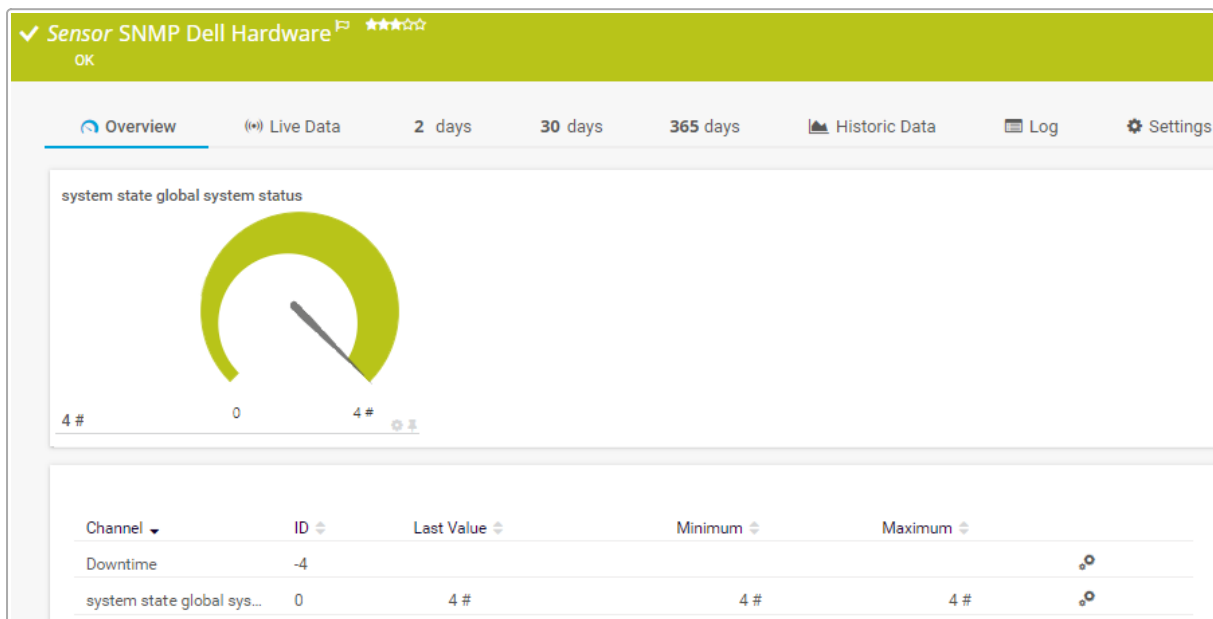
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.186 SNMP Dell Hardware Sensor

The SNMP Dell Hardware sensor monitors performance counters on a Dell hardware device via the Simple Network Management Protocol (SNMP).

- ❶ The data that you can monitor with this sensor depends on the available performance counters on the target system.
- ❶ The SNMP Dell Hardware sensor does not appear as a running sensor, instead it is created as an [SNMP Custom Advanced](#)<sup>[1996]</sup> sensor or an [SNMP Custom Table](#)<sup>[1917]</sup> sensor with up to 10 channels per category.



SNMP Dell Hardware Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1949]</sup>.

### Sensor in Other Languages

- Dutch: SNMP Dell Hardware
- French: Dell matériel (SNMP)
- German: SNMP Dell Hardware
- Japanese: SNMP Dell ハードウェア
- Portuguese: Hardware Dell (SNMP)
- Russian: Оборудование Dell по SNMP
- Simplified Chinese: SNMP Dell 硬件
- Spanish: Hardware Dell (SNMP)

### Remarks

Consider the following [remarks](#)<sup>[1946]</sup> and requirements for this sensor:



Remark	Description
Dell OpenManage Server Administrator	<p>This sensor requires the <a href="#">Dell OpenManage Server Administrator</a> on the target system.</p> <p><b>i</b> Make sure that you enable SNMP in the OMSA.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">What do I need to monitor Dell servers?</a></p>
Counters	<p>Select the counters that you want to monitor with caution. We recommend that you select only a few counters in the Add Sensor dialog. Use the search in the table header to filter for specific counters. Selecting too many counters might result in thousands of sensors or the sensor creation is canceled.</p>
IPv6	<p>This sensor supports IPv6.</p>
Performance impact	<p>This sensor has a <b>very low</b> performance impact.</p>
Knowledge Base	<p>Knowledge Base: <a href="#">What do I need to monitor Dell servers?</a></p>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ exampletag ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

**Example Name**

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- dell

**■** For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Dell Hardware Specific

**Dell Hardware Specific**

**Interface** ⓘ *MIB-Dell-10892/system state: 1/system state ampe*

**Unit String** ⓘ #

**Multiplication** ⓘ

**Division** ⓘ

**If Value Changes** ⓘ  Ignore (default)  
 Trigger 'change' notification

Dell Hardware Specific

Setting	Description
Interface	The name of the interface (performance counter) that this sensor monitors.
Unit String	Define the unit of the numeric data that the sensor receives at the specified OID. Enter a string.
Multiplication	If you want to multiply the received data with a certain value, enter the multiplier. Enter an integer.
Division	If you want to divide the received data by a certain value, enter the divisor. Enter an integer.
If Value Changes	<p>Define what the sensor does when its value changes:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> <li>▪ Trigger 'change' notification: Send an internal message that indicates a change.</li> </ul> <p> ⓘ In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</p>


## Sensor Display

**Sensor Display**


**Primary Channel** ⓘ Downtime


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
[ <a href="#">Performance Counter</a> ]	<p>The value returned by a specific Dell hardware OID, for example</p> <ul style="list-style-type: none"><li>▪ Data about the system management software</li><li>▪ Data about system status</li><li>▪ Information about chassis and BIOS</li><li>▪ Various hardware parameters</li><li>▪ Other valuable data</li></ul>

## More

### KNOWLEDGE BASE

What do I need to monitor Dell servers?

- <https://kb.paessler.com/en/topic/45333>

What security features does PRTG include?

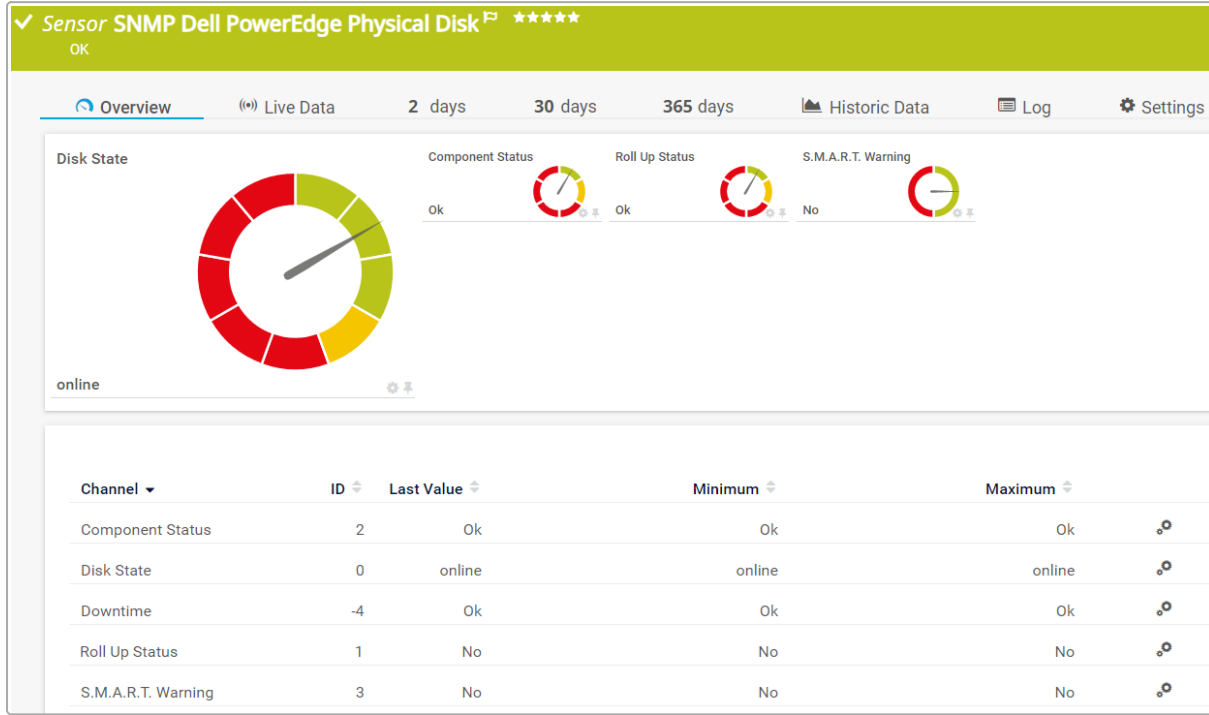
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.187 SNMP Dell PowerEdge Physical Disk Sensor

The SNMP Dell PowerEdge Physical Disk sensor monitors a physical disk in a Dell PowerEdge server via the Simple Network Management Protocol (SNMP).



SNMP Dell PowerEdge Physical Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1954</sup>.

### Sensor in Other Languages

- Dutch: SNMP-Dell PowerEdge Fysieke Schijf
- French: Dell PowerEdge disque physique (SNMP)
- German: SNMP Dell PowerEdge Physikalischer Datenträger
- Japanese: SNMP Dell PowerEdge 物理ディスク
- Portuguese: Disco físico Dell PowerEdge (SNMP)
- Russian: Физический диск Dell PowerEdge по SNMP
- Simplified Chinese: SNMP Dell PowerEdge 物理磁盘
- Spanish: Disco físico Dell PowerEdge (SNMP)

### Remarks

Consider the following [remarks](#)<sup>1951</sup> and requirements for this sensor:

Remark	Description
Dell OpenManage Server Administrator or iDRAC 7	<p>This sensor requires Integrated Dell Remote Access Controller (iDRAC) 7 or the Dell OpenManage Server Administrator (OMSA) on the target system.</p> <ul style="list-style-type: none"> <li><span>ⓘ</span> Make sure that you enable SNMP in the OMSA. <ul style="list-style-type: none"> <li><span>■</span> For more information, see the Knowledge Base: <a href="#">What do I need to monitor Dell servers?</a></li> </ul> </li> <li><span>ⓘ</span> You can also monitor Dell PowerEdge servers with this sensor via iDRAC 7.</li> </ul>
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">What do I need to monitor Dell servers?</a></li> <li>▪ Knowledge Base: <a href="#">I can't add Dell PowerEdge sensors to PRTG. What can I do?</a></li> <li>▪ Knowledge Base: <a href="#">My Dell PowerEdge sensor fails to validate disks and I can't add it. What can I do?</a></li> </ul>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★★★★☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- dell
- physicaldisk
- snmpdell
- snmpdellphysicaldisksensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Dell PowerEdge Physical Disk Settings

Dell PowerEdge Physical Disk Settings

Disk <sup>?</sup> Example

Data Source <sup>?</sup> iDRAC

Dell PowerEdge Physical Disk Settings

Setting	Description
Disk	The physical disk that this sensor monitors.
Data Source	The interface that PRTG uses to get monitoring data. This is either Dell OMSA or iDRAC.

## Sensor Display

Sensor Display

Primary Channel <sup>?</sup> Downtime

Graph Type <sup>?</sup>


- Show channels independently (default)
- Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><sup>i</sup> You can set a different primary channel later by clicking <sup>?</sup> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><sup>i</sup> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>

Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other above.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.


 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Component Status	<p>The component status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Non Critical</li> <li>▪ Down status: Critical, Non Recoverable, Other, Unknown</li> </ul>
Disk State	<p>The disk status</p> <ul style="list-style-type: none"> <li>▪ Up status: Non-Raid, Online, Ready</li> <li>▪ Warning status: Foreign</li> <li>▪ Down status: Blocked, Critical, Failed, Non Recoverable, Other, Removed, Unknown</li> </ul> <p> This channel is the primary channel by default.</p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>



Channel	Description
Roll Up Status	<p>The roll up status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Non Critical</li> <li>▪ Down status: Critical, Non Recoverable, Other, Unknown</li> </ul> <p> This channel requires that Dell OMSA is installed on the target system.</p>
S.M.A.R.T. Warning	<p>The S.M.A.R.T. warning status</p> <ul style="list-style-type: none"> <li>▪ Up status: No</li> <li>▪ Down status: Yes</li> </ul>

## More

### KNOWLEDGE BASE

What do I need to monitor Dell servers?

- <https://kb.paessler.com/en/topic/45333>

I can't add Dell PowerEdge sensors to PRTG. What can I do?

- <https://kb.paessler.com/en/topic/68040>

My Dell PowerEdge sensor fails to validate disks and I can't add it. What can I do?

- <https://kb.paessler.com/en/topic/61784>

What security features does PRTG include?

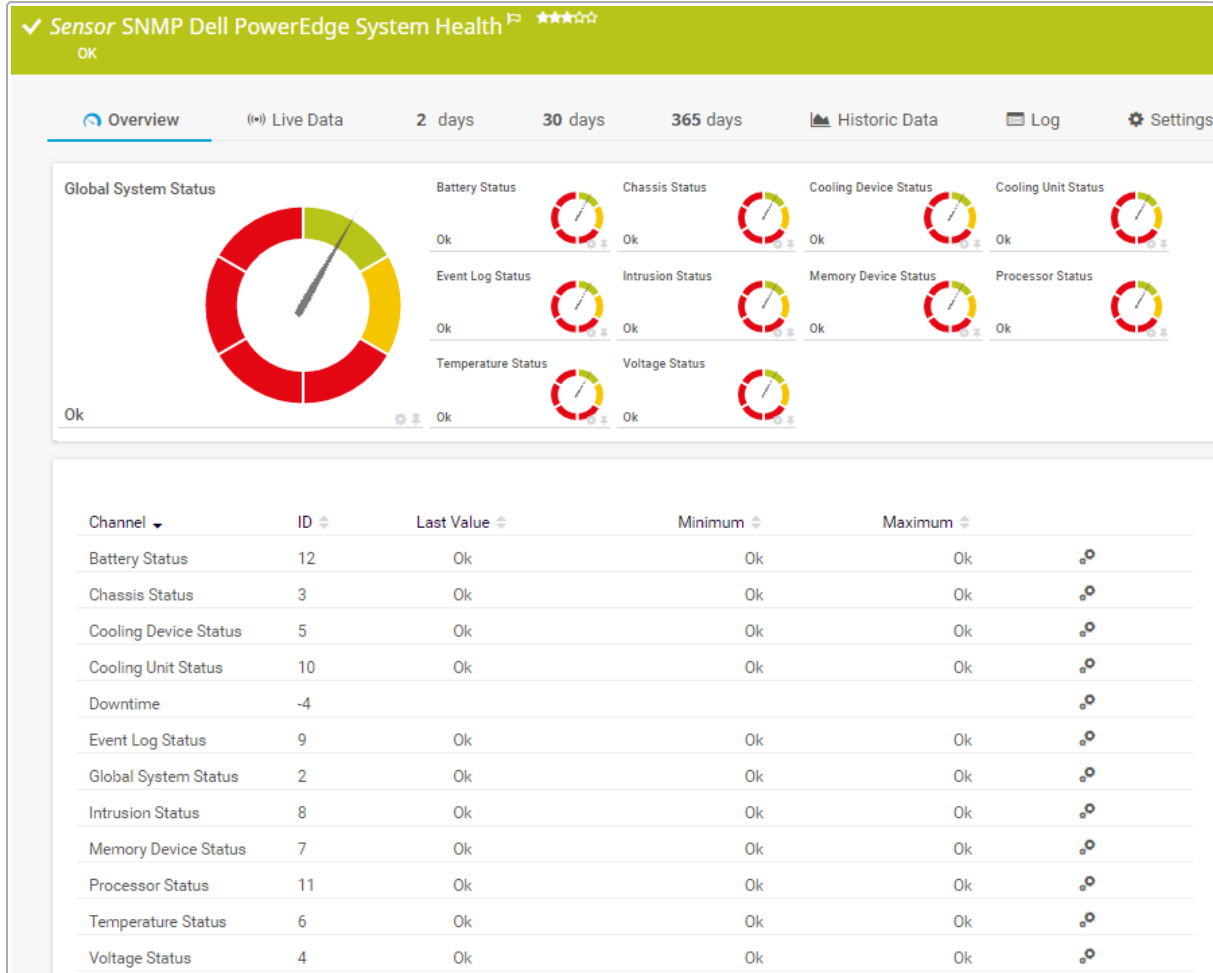
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.188 SNMP Dell PowerEdge System Health Sensor

The SNMP Dell PowerEdge System Health sensor monitors the system health of a Dell PowerEdge server via the Simple Network Management Protocol (SNMP).



SNMP Dell PowerEdge System Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Dell PowerEdge Systeemstatus
- French: Dell PowerEdge état du système (SNMP)
- German: SNMP Dell PowerEdge Systemzustand
- Japanese: SNMP Dell PowerEdge システムの正常性
- Portuguese: Saúde do sistema Dell PowerEdge (SNMP)
- Russian: Работоспособность системы Dell PowerEdge по SNMP
- Simplified Chinese: SNMP Dell PowerEdge 系统健康状况
- Spanish: Salud de sistema Dell PowerEdge (SNMP)

## Remarks

Consider the following [remarks](#) <sup>1957</sup> and requirements for this sensor:

Remark	Description
Dell OpenManage Server Administrator or iDRAC 7	<p>This sensor requires Integrated Dell Remote Access Controller (iDRAC) 7 or the Dell OpenManage Server Administrator (OMSA) on the target system.</p> <ul style="list-style-type: none"> <li><span>ⓘ</span> Make sure that you enable SNMP in the OMSA. <ul style="list-style-type: none"> <li><span>■</span> For more information, see the Knowledge Base: <a href="#">What do I need to monitor Dell servers?</a></li> </ul> </li> <li><span>ⓘ</span> You can also monitor Dell PowerEdge servers with this sensor via iDRAC 7.</li> </ul>
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">Why does my Dell PowerEdge System Health sensor show a power unit status error after iDRAC update?</a></li> <li>▪ Knowledge Base: <a href="#">What do I need to monitor Dell servers?</a></li> <li>▪ Knowledge Base: <a href="#">I can't add Dell PowerEdge sensors to PRTG. What can I do?</a></li> </ul>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ

**Priority** ⓘ

Example Name

exampletag ✕ +

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- dell

- snmpdell
- snmpdellssystemhealthsensor
- systemhealth

For more information about basic sensor settings, see section [Sensor Settings](#).

### Dell PowerEdge System Health Specific

**Dell PowerEdge System Health Specific**

**Chassis** ⓘ *Example*

**Channel Mask** ⓘ *104959*

**Data Source** ⓘ *iDRAC*

Dell PowerEdge System Health Specific

Setting	Description
Chassis	The chassis that this sensor monitors.
Channel Mask	The channel mask that describes which channels are available.
Data Source	The interface that PRTG uses to get monitoring data. This is either Dell OMSA or iDRAC.

### Sensor Display


**Sensor Display**

**Primary Channel** ⓘ Downtime


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>

Setting	Description
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Ampere Status	<p>The ampere status</p> <ul style="list-style-type: none"> <li>Up status: OK</li> <li>Warning status: Non Critical</li> <li>Down status: Critical, Non Recoverable, Other, Unknown</li> </ul>
Battery Status	<p>The battery status</p> <ul style="list-style-type: none"> <li>Up status: OK</li> <li>Warning status: Non Critical</li> </ul>

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Down status: Critical, Non Recoverable, Other, Unknown</li> </ul>
Chassis Status	<p>The chassis status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Non Critical</li> <li>▪ Down status: Critical, Non Recoverable, Other, Unknown</li> </ul>
Cooling Device Status	<p>The cooling device status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Non Critical</li> <li>▪ Down status: Critical, Non Recoverable, Other, Unknown</li> </ul>
Cooling Unit Status	<p>The cooling unit status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Non Critical</li> <li>▪ Down status: Critical, Non Recoverable, Other, Unknown</li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Global System Status	<p>The global system status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Non Critical</li> <li>▪ Down status: Critical, Non Recoverable, Other, Unknown</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Intrusion Status	<p>The intrusion status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Non Critical</li> <li>▪ Down status: Critical, Non Recoverable, Other, Unknown</li> </ul>
Memory Device Status	<p>The memory device status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Non Critical</li> </ul>

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Down status: Critical, Non Recoverable, Other, Unknown</li> </ul>
Power Supply Status	<p>The power supply status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Non Critical</li> <li>▪ Down status: Critical, Non Recoverable, Other, Unknown</li> </ul>
Power Unit Status	<p>The power unit status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Non Critical</li> <li>▪ Down status: Critical, Non Recoverable, Other, Unknown</li> </ul>
Processor Status	<p>The processor status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Non Critical</li> <li>▪ Down status: Critical, Non Recoverable, Other, Unknown</li> </ul>
Temperature Status	<p>The temperature status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Non Critical</li> <li>▪ Down status: Critical, Non Recoverable, Other, Unknown</li> </ul>
Voltage Status	<p>The voltage status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Non Critical</li> <li>▪ Down status: Critical, Non Recoverable, Other, Unknown</li> </ul>

## More

### ■ KNOWLEDGE BASE

Why does my Dell PowerEdge System Health sensor show a power unit status error after iDRAC update?

- <https://kb.paessler.com/en/topic/72855>

What do I need to monitor Dell servers?

- <https://kb.paessler.com/en/topic/45333>

I can't add Dell PowerEdge sensors to PRTG. What can I do?

- <https://kb.paessler.com/en/topic/68040>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

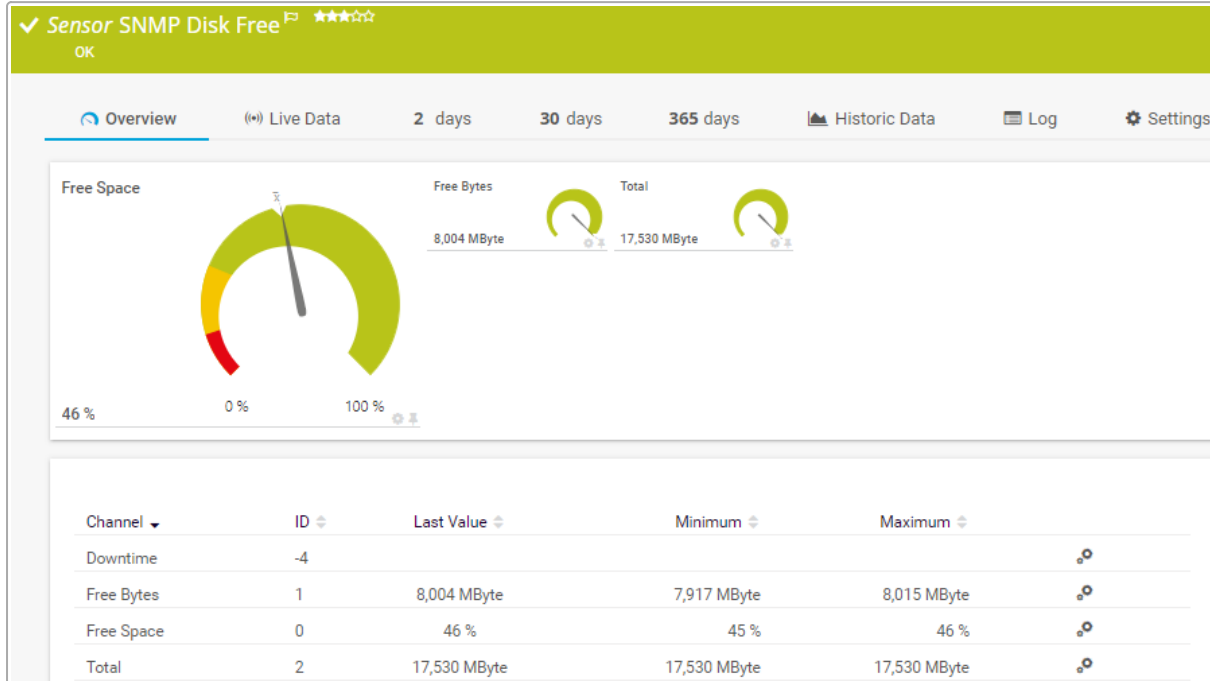
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>



## 7.8.189 SNMP Disk Free Sensor

The SNMP Disk Free sensor monitors the free disk space on a logical disk via the Simple Network Management Protocol (SNMP).



SNMP Disk Free Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP vrije schijf ruimte
- French: Espace disponible disque (SNMP)
- German: SNMP Datenträgerspeicher
- Japanese: SNMP ディスク空き容量
- Portuguese: Disco livre (SNMP)
- Russian: Свободное пространство по SNMP
- Simplified Chinese: SNMP 磁盘可用空间
- Spanish: Espacio libre en disco (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Localhost	It might not work to query data from a probe device via SNMP (querying <a href="#">localhost</a> , <a href="#">127.0.0.1</a> , or <a href="#">::1</a> ). <a href="#">Add this device</a> with the IP address that it has in your network and create the sensor on this device instead.
OID values	This sensor uses more generic object identifier (OID) values than the <a href="#">SNMP Linux Disk Free</a> <sup>20661</sup> sensor.

### Basic Sensor Settings

#### Basic Sensor Settings

Sensor Name ⓘ

Tags ⓘ

Priority ⓘ

Example Name

---

exampletag ✕ +

---

★★★★☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- diskfree
- diskspacesensor
- snmpdiskfreesensor
- snmp

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>6671</sup>.

### Disk Free Settings

#### Disk Free Settings

Disk ⓘ

C:\ Label: Serial Number 1a2b3c4d

---

Disk Free Settings

Setting	Description
Disk	<p>The name of the disk that this sensor monitors.</p> <p><b>i</b> PRTG shows this value for reference purposes only. We strongly recommend that you only change it if the Paessler support team explicitly asks you to do so. Wrong usage can result in incorrect monitoring data.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>



## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Bytes	The free space
Free Space	<p>The free space (%)</p> <p> This channel is the primary channel by default.</p> <p> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: <a href="#">10%</a></li> <li>▪ Lower warning limit: <a href="#">25%</a></li> </ul>
Total	The total space

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

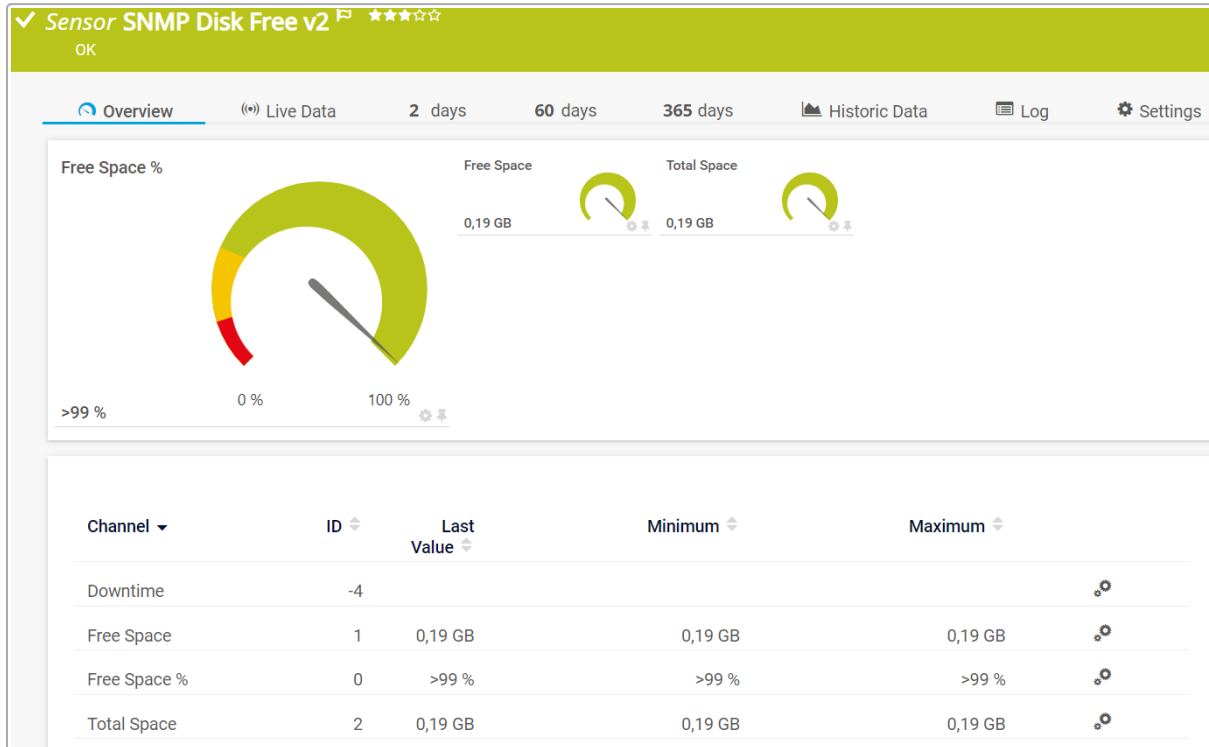
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.190 SNMP Disk Free v2 Sensor (BETA)

The SNMP Disk Free v2 sensor monitors the free disk space on a logical disk via the Simple Network Management Protocol (SNMP). The sensor uses HOST-RESOURCES-V2-MIB::hrStorageTable.



SNMP Disk Free v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>1971</sup>.

### Sensor in Other Languages

- Dutch: SNMP Vrije Schijf Ruimte v2
- French: Espace disque disponible v2 (SNMP)
- German: SNMP Datenträgerspeicher v2
- Japanese: SNMP ディスク空き容量 v2
- Portuguese: Disco livre (SNMP) v2
- Russian: SNMP Disk Free v2
- Simplified Chinese: SNMP 磁盘可用空间版本 2
- Spanish: Espacio libre en disco (SNMP) v2

### Remarks

Consider the following [remarks](#)<sup>1967</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Localhost	It might not work to query data from a probe device via SNMP (querying <a href="#">localhost</a> , <a href="#">127.0.0.1</a> , or <a href="#">::1</a> ). <a href="#">Add this device</a> with the IP address that it has in your network and create the sensor on this device instead.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">1 minute</a>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ exampletag ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Example Name

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- diskfree
- diskspacesensor
- snmp
- snmpdiskfreesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## SNMP Disk Free Specific

### SNMP Disk Free Specific

**Disk** ⓘ

/

**Type** ⓘ

Fixed Disk

**Size** ⓘ

3 GiB

SNMP Disk Free Specific

Setting	Description
Disk	<p>The name of the disk that this sensor monitors.</p> <p><b>ⓘ</b> PRTG shows this value for reference purposes only. We strongly recommend that you only change it if the Paessler support team explicitly asks you to do so. Wrong usage can result in incorrect monitoring data.</p>
Type	The type of the disk that this sensor monitors.
Size	The size of the disk that this sensor monitors.

## Sensor Display

### Sensor Display

**Primary Channel** ⓘ


Downtime

**Graph Type** ⓘ

Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.

Setting	Description
	<p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.           <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**


**Result Handling** 
  
 Discard result (default)
   
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <p>Do not store the sensor result.</p> <p>Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</p> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>





## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Space	The free space
Free Space %	<p>The free space (%)</p> <p> This channel is the primary channel by default.</p> <p> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: <a href="#">10%</a></li> <li>▪ Lower warning limit: <a href="#">25%</a></li> </ul>
Total Space	The total space

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

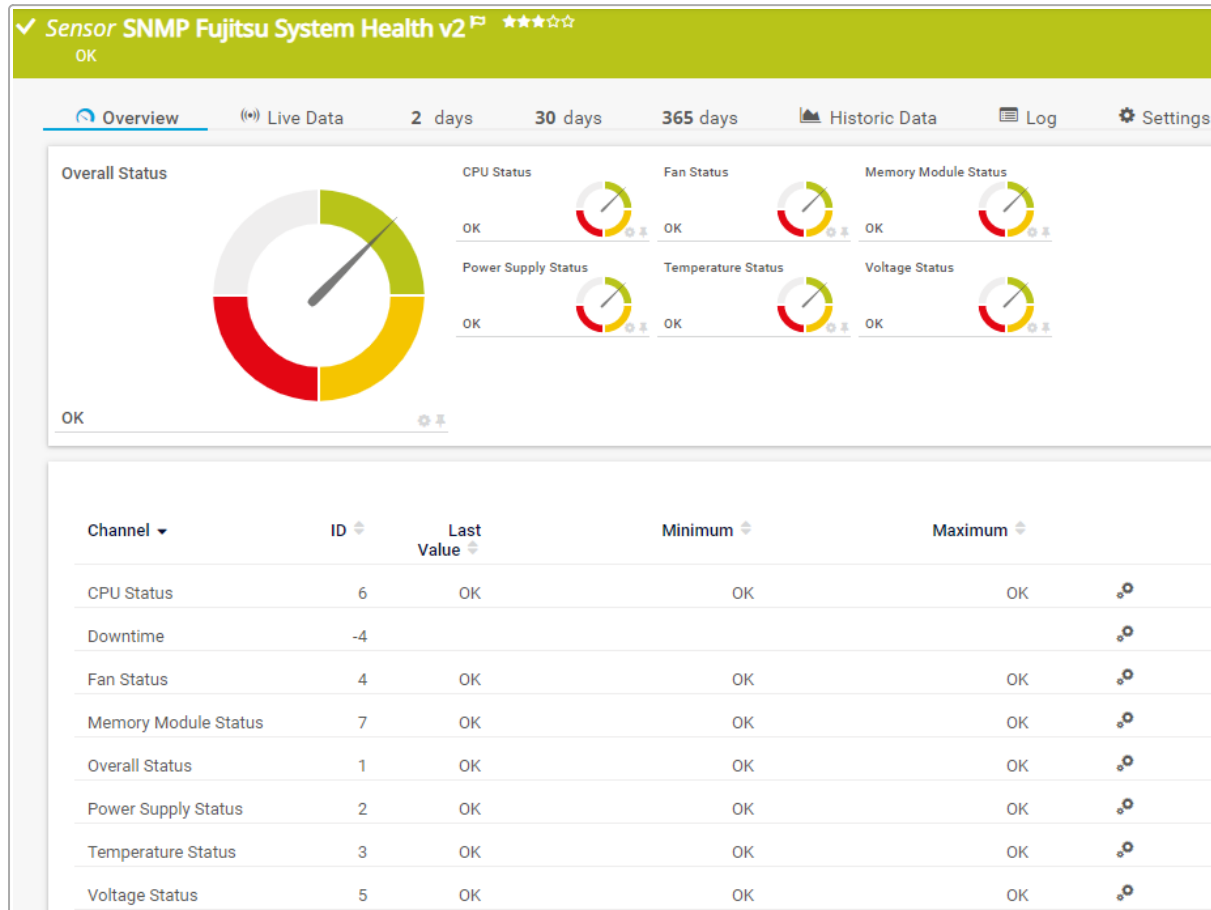
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.191 SNMP Fujitsu System Health v2 Sensor

The SNMP Fujitsu System Health v2 sensor monitors the status of a Fujitsu PRIMERGY server via the integrated Remote Management Controller (iRMC) and Simple Network Management Protocol (SNMP). The sensor might also work on other Fujitsu devices that have an iRMC available like PRIMEQUEST servers, some storage systems of the ETERNUS product line, and CELSIUS workstations in racks.



SNMP Fujitsu System Health v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[197]</sup>.

### Sensor in Other Languages

- Dutch: SNMP Fujitsu Systeemstatus v2
- French: Fujitsu état du système v2 (SNMP)
- German: SNMP Fujitsu Systemzustand v2
- Japanese: SNMP Fujitsu システム正常性 v2
- Portuguese: Saúde do sistema Fujitsu (SNMP) v2
- Russian: Работоспособность системы Fujitsu по SNMP, версия 2
- Simplified Chinese: SNMP Fujitsu 系统健康状况版本 2
- Spanish: Salud de sistema Fujitsu (SNMP) v2

## Remarks

Consider the following [remarks](#)<sup>[1973]</sup> and requirements for this sensor:

Remark	Description
SNMP	This sensor requires SNMP to be enabled in the iRMC via ServerView.
Parent device	Use an iRMC interface as the parent device for this sensor.
SNMP v1	This sensor does not support SNMP v1.
iRMC S5	As of iRMC S5, additional counters for physical disks and logical disks are supported.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- fujitsu
- irmc
- snmp
- snmpfujitsusystemhealthsensor
- systemhealth

For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## System Specific

### System Specific

**Measurement** ⓘ *sc2CPU*

**Sensor Version** ⓘ *2*

**Identifier** ⓘ

**OID Index** ⓘ *1.1*

System Specific

Setting	Description
Measurement	The type of measurement that this sensor monitors.
Sensor Version	The version of the sensor definition that was used to create this sensor.
Identifier	The value that the sensor uses to find the component in the OID table. ⓘ The identifier has the following format: <a href="#">RowIndex</a>   <a href="#">Unique</a>   <a href="#">Measurement</a> . For example, <a href="#">1.1 BATT 3.0V Voltage</a> .
OID Index	The OID table index that this sensor uses.

## Debug Options

### Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].Data.txt and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul>

Setting	Description
	<p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CPU Status	<p>The CPU status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Error</li> <li>▪ Unknown status: Unknown</li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Fan Status	<p>The fan status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Error</li> <li>▪ Unknown status: Unknown</li> </ul>
Memory Module Status	<p>The memory module status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Error</li> <li>▪ Unknown status: Unknown</li> </ul>
Overall Status	<p>The overall status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> </ul>

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Warning status: Warning</li> <li>▪ Down status: Error</li> <li>▪ Unknown status: Unknown</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Power Supply Status	<p>The power supply status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Error</li> <li>▪ Unknown status: Unknown</li> </ul>
Temperature Status	<p>The temperature status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Error</li> <li>▪ Unknown status: Unknown</li> </ul>
Voltage Status	<p>The voltage status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Error</li> <li>▪ Unknown status: Unknown</li> </ul>

**i** The sensor can also show CPU speed and core count, fan speed, number of correctable and uncorrectable errors of the memory module, service processor battery status, condition of the power supply, power limit status, and power consumption.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

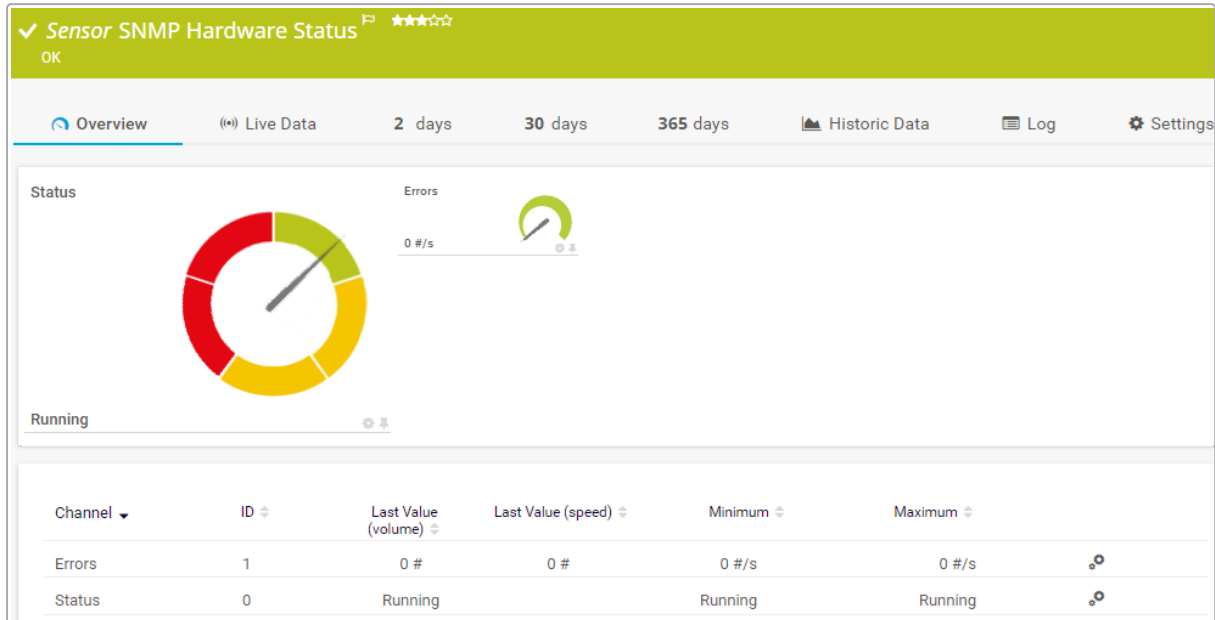
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.192 SNMP Hardware Status Sensor

The SNMP Hardware Status sensor monitors the status of a server's hardware component via the Simple Network Management Protocol (SNMP).



SNMP Hardware Status Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Hardware Status
- French: Statut matériel (SNMP)
- German: SNMP Hardwarezustand
- Japanese: SNMP ハードウェア正常性
- Portuguese: Status do hardware (SNMP)
- Russian: Статус оборудования по SNMP
- Simplified Chinese: SNMP 硬件状态
- Spanish: Estado de hardware (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.



Remark	Description
Performance impact	This sensor has a <b>very low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Localhost	It might not work to query data from a probe device via SNMP (querying <a href="#">localhost</a> , <a href="#">127.0.0.1</a> , or <a href="#">::1</a> ). <a href="#">Add this device</a> with the IP address that it has in your network and create the sensor on this device instead.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- hardwarestatus

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Hardware Specific

#### Hardware Specific

**Hardware Components** ⓘ 1

---

**Product ID** ⓘ 0.0

---

**Description** ⓘ *Send to Microsoft OneNote 16 Driver*

---

**Type** ⓘ *Printer*

Hardware Specific

Setting	Description
Hardware Components	The hardware component that this sensor monitors.
Product ID	The product ID of the hardware component that this sensor monitors.
Description	The description of the hardware component that this sensor monitors.
Type	The type of the hardware component that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Errors	The number of errors
Status	<p>The hardware component status</p> <ul style="list-style-type: none"> <li>▪ Up status: Running</li> <li>▪ Warning status: Warning, Testing</li> <li>▪ Down status: Down, Unknown</li> </ul> <p> This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

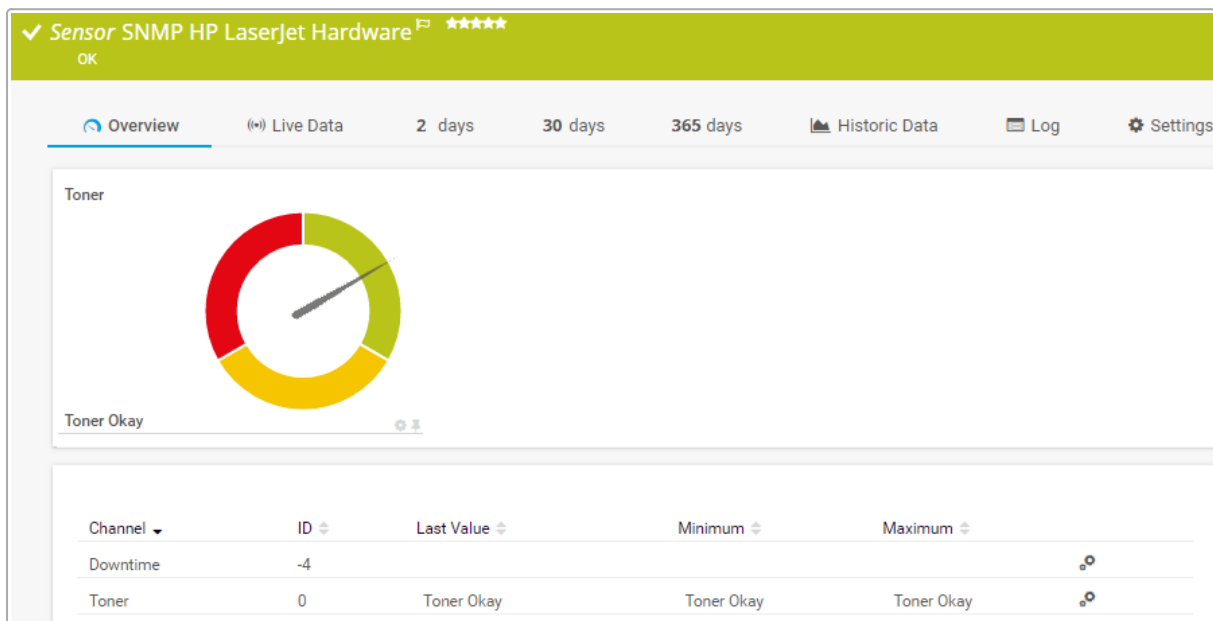
## 7.8.193 SNMP HP LaserJet Hardware Sensor

The SNMP HP LaserJet Hardware sensor monitors performance counters on an HP LaserJet hardware device via the Simple Network Management Protocol (SNMP).

**i** The SNMP HP LaserJet Hardware sensor does not appear as a running sensor, instead it is created as an [SNMP Custom Advanced](#) sensor.

The following performance counters are available:

- Toner/Status
- Paper/Status
- Jam/Status



SNMP HP LaserJet Hardware Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP HP LaserJet Hardware
- French: HP LaserJet matériel (SNMP)
- German: SNMP HP LaserJet Hardware
- Japanese: SNMP HP LaserJet ハードウェア
- Portuguese: Hardware HP LaserJet (SNMP)
- Russian: Оборудование HP LaserJet по SNMP
- Simplified Chinese: SNMP HP LaserJet 硬件
- Spanish: Hardware HP LaserJet (SNMP)

## Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ

**Priority** ⓘ

Example Name

exampletag
×
+

★★★★☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- hplaserjet

For more information about basic sensor settings, see section [Sensor Settings](#).

## HP LaserJet Specific

### HP LaserJet Specific

**Interface** ⓘ

**If Value Changes** ⓘ

HP Laserjet / Jam/Status

Ignore (default)

Trigger 'change' notification

HP LaserJet Specific

Setting	Description
Interface	The name of the interface (performance counter) that this sensor monitors.
If Value Changes	<p>Define what the sensor does when its value changes:</p> <ul style="list-style-type: none"> <li>Ignore (default): Do nothing.</li> <li>Trigger 'change' notification: Send an internal message that indicates a change. <ul style="list-style-type: none"> <li><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</li> </ul> </li> </ul>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Jam	The paper jam status <ul style="list-style-type: none"> <li>▪ Up status: No Jam Detected</li> <li>▪ Down status: Paper Jam Detected</li> </ul>
Paper	The paper status <ul style="list-style-type: none"> <li>▪ Up status: Paper Okay</li> <li>▪ Down status: Manual Paper Feed Required, Out Of Paper Or No Cassette Loaded</li> </ul>
Toner	The toner status <ul style="list-style-type: none"> <li>▪ Up status: Toner Okay</li> <li>▪ Warning status: Toner Low</li> <li>▪ Down status: No Toner Cartridge Loaded</li> </ul>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

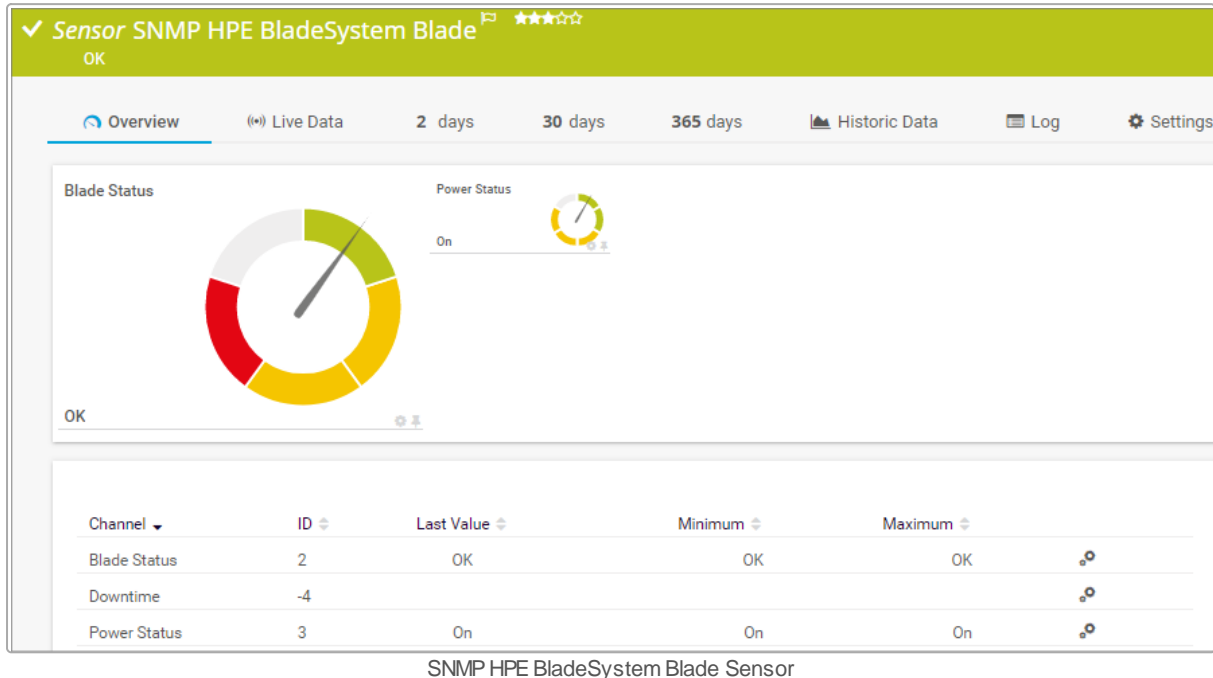
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>



## 7.8.194 SNMP HPE BladeSystem Blade Sensor

The SNMP HPE BladeSystem Blade sensor monitors the status of an HPE BladeSystem via the Simple Network Management Protocol (SNMP).



For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP HPE BladeSystem Blade
- French: HPE BladeSystem serveur blade (SNMP)
- German: SNMP HPE BladeSystem Blade
- Japanese: SNMP HPE BladeSystem ブレード
- Portuguese: Blade HPE BladeSystem (SNMP)
- Russian: Блейд-модуль HPE BladeSystem по SNMP
- Simplified Chinese: SNMP HPE BladeSystem 刀片
- Spanish: Blade HPE BladeSystem (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Parent device	This sensor requires that the IP address or Domain Name System (DNS) name in the settings of the parent device points to the HPE BladeSystem Enclosure hosting the Onboard Administrator.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

**Basic Sensor Settings**

Sensor Name ⓘ Example Name

Tags ⓘ  ✕ ⊕

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- blade
- bladesystem
- hpe
- snmp

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### HPE BladeSystem Specific

**HPE BladeSystem Specific**

Server Blades ⓘ 1A2B3C4D5E

HPE BladeSystem Specific

Setting	Description
Server Blades	The server blade that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Blade Status	<p>The blade status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Degraded</li> <li>▪ Down status: Failed</li> <li>▪ Unknown status: Other</li> </ul> <p>ⓘ This channel is the primary channel by default.</p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Power Status	<p>The power status</p> <ul style="list-style-type: none"> <li>▪ Up status: On, Rebooting</li> <li>▪ Warning status: Off, Power Stagged Off, Unknown</li> <li>▪ Unknown status: Other</li> </ul>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

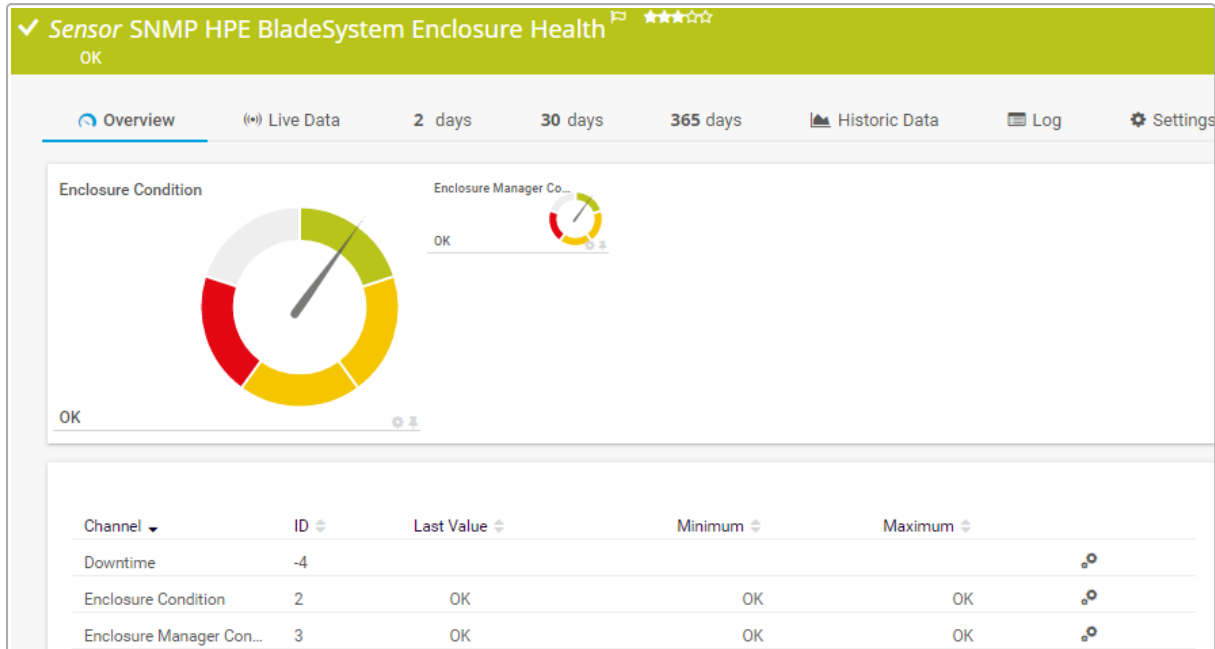
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.195 SNMP HPE BladeSystem Enclosure System Health Sensor

The SNMP HPE BladeSystem Enclosure Health sensor monitors the health of an HPE BladeSystem device via the Simple Network Management Protocol (SNMP).



SNMP HPE BladeSystem Enclosure HealthSensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[1993]</sup>.

### Sensor in Other Languages

- Dutch: SNMP HPE BladeSystem Behuizing Status
- French: HPE BladeSystem état du boîtier (SNMP)
- German: SNMP HPE BladeSystem Gehäuse-Zustand
- Japanese: SNMP HPE BladeSystem エンクロージャの正常性
- Portuguese: Saúde do gabinete HPE BladeSystem (SNMP)
- Russian: Работоспособность корпуса HPE BladeSystem по SNMP
- Simplified Chinese: SNMP HPE BladeSystem 外壳运行状况
- Spanish: Salud de gabinete HPE BladeSystem (SNMP)

### Remarks

Consider the following [remarks](#)<sup>[1991]</sup> and requirements for this sensor:

Remark	Description
Parent device	This sensor requires that the IP address or Domain Name System (DNS) name in the settings of the parent device points to the HPE BladeSystem Enclosure hosting the Onboard Administrator.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- blade
- bladesystem
- health
- hpe
- snmp
- systemhealth

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Enclosure Condition	<p>The enclosure condition</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Degraded</li> <li>▪ Down status: Failed</li> <li>▪ Unknown status: Other</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Enclosure Manager Condition	<p>The enclosure manager condition</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Degraded, Unknown</li> <li>▪ Down status: Failed</li> <li>▪ Unknown status: Other</li> </ul>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

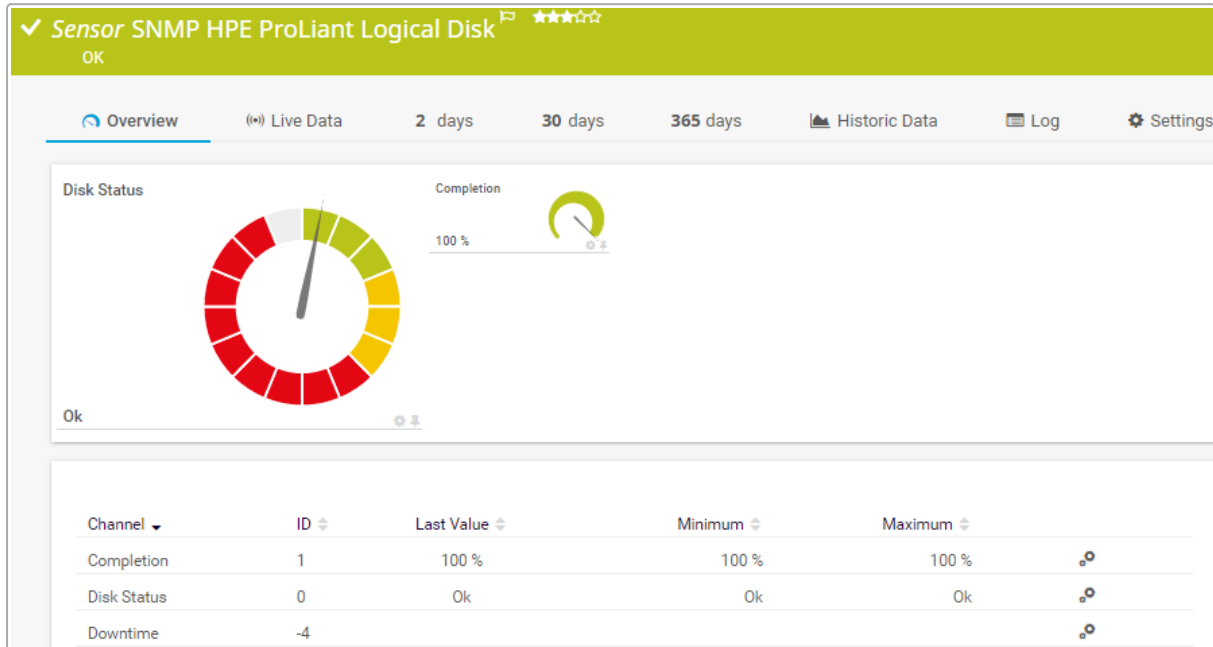
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>



## 7.8.196 SNMP HPE ProLiant Logical Disk Sensor

The SNMP HPE ProLiant Logical Disk sensor monitors a logical disk in an HPE server via the Simple Network Management Protocol (SNMP).



SNMP HPE ProLiant Logical Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP HPE ProLiant Logische Schijf
- French: HPE ProLiant disque logique (SNMP)
- German: SNMP HPE ProLiant Logischer Datenträger
- Japanese: SNMP HPE ProLiant 論理ディスク
- Portuguese: Disco lógico HPE ProLiant (SNMP)
- Russian: Логический диск HPE ProLiant по SNMP
- Simplified Chinese: SNMP HPE ProLiant 逻辑磁盘
- Spanish: Disco lógico HPE ProLiant (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
HPE system management tools	<p>For Gen10 servers: This sensor requires <a href="#">HPE Agentless Management</a> and the <a href="#">HPE Agentless Management Service</a> on the target system.</p> <p>For Gen10 servers: Use the HPE Integrated Lights Out (iLO) interface as the parent device.</p> <p>For Gen9 servers or earlier: This sensor requires <a href="#">HPE Insight Management Agents</a> and <a href="#">HPE Insight Management WBEM Providers</a> on the target system.</p> <p><b>i</b> For Gen9 servers or earlier, this sensor requires a specific HPE system management tool to be installed on the target system to report data via SNMP: <a href="#">HPE Insight Management Agents</a>. To receive SNMP data from redundant array of independent disks (RAID) controllers, the sensor also requires <a href="#">HPE Insight Management Agents</a>. For Gen10 servers, this sensor no longer requires HPE system management tools. Instead, the sensor requires the <a href="#">HPE Agentless Management Service</a> to be installed on the target system.</p> <p><b>■</b> For more information and download links, see the Knowledge Base: <a href="#">Monitor HP ProLiant via SNMP?</a></p> <p>For Gen9 servers or earlier, some of the HPE object identifiers (OID) that <b>i</b> this sensor uses are only accessible via the iLO interface. If this sensor throws an error that it cannot find "such device types", create a device that points to the address of the HPE iLO interface (if available) and add the sensor to this device. We recommend that you use the <a href="#">Agentless Management</a> feature with configured SNMP. You can set this up in the iLO configuration interface under Administration   Management   SNMP Settings. For Gen10 servers, use the HPE iLO interface as parent device for this sensor.</p>
iLO versions	This sensor supports iLO as of iLO 3. We recommend that you use at least iLO 4.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

## Basic Sensor Settings

Basic Sensor Settings

Sensor Name ⓘ

Tags ⓘ

exampletag ✕ +

Priority ⓘ

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- hpe
- logicaldisk
- snmphpe
- snmphpelogicaldisksensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## HPE ProLiant Logical Disk Settings

HPE ProLiant Logical Disk Settings

Disk ⓘ

HPE ProLiant Logical Disk Settings

Setting	Description
Disk	The name of the disk that this sensor monitors.

## Sensor Display


Sensor Display

Primary Channel ⓘ


Graph Type ⓘ


Show channels independently (default)
   
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Completion	<p>The completion (%)</p> <p><b>i</b> This is only important when the disk status is "Reconstructing" or "Expanding" and illustrates the progress of this task.</p>

Channel	Description
Disk Status	<p>The disk status</p> <ul style="list-style-type: none"> <li>▪ Up status: Expanding, Ok, Rebuilding</li> <li>▪ Warning status: Ready For Rebuild, Recovering, Unconfigured</li> <li>▪ Down status: Bad Connect, Erasing, Failed, Multipath Access Degraded, Not Available, Overheating, Queued For Expansion, Shutdown, Wrong Drive,</li> <li>▪ Unknown status: Other</li> </ul> <p> This channel is the primary channel by default.</p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>

## More

### KNOWLEDGE BASE

Monitor HP ProLiant via SNMP?

- <https://kb.paessler.com/en/topic/33133>

What security features does PRTG include?

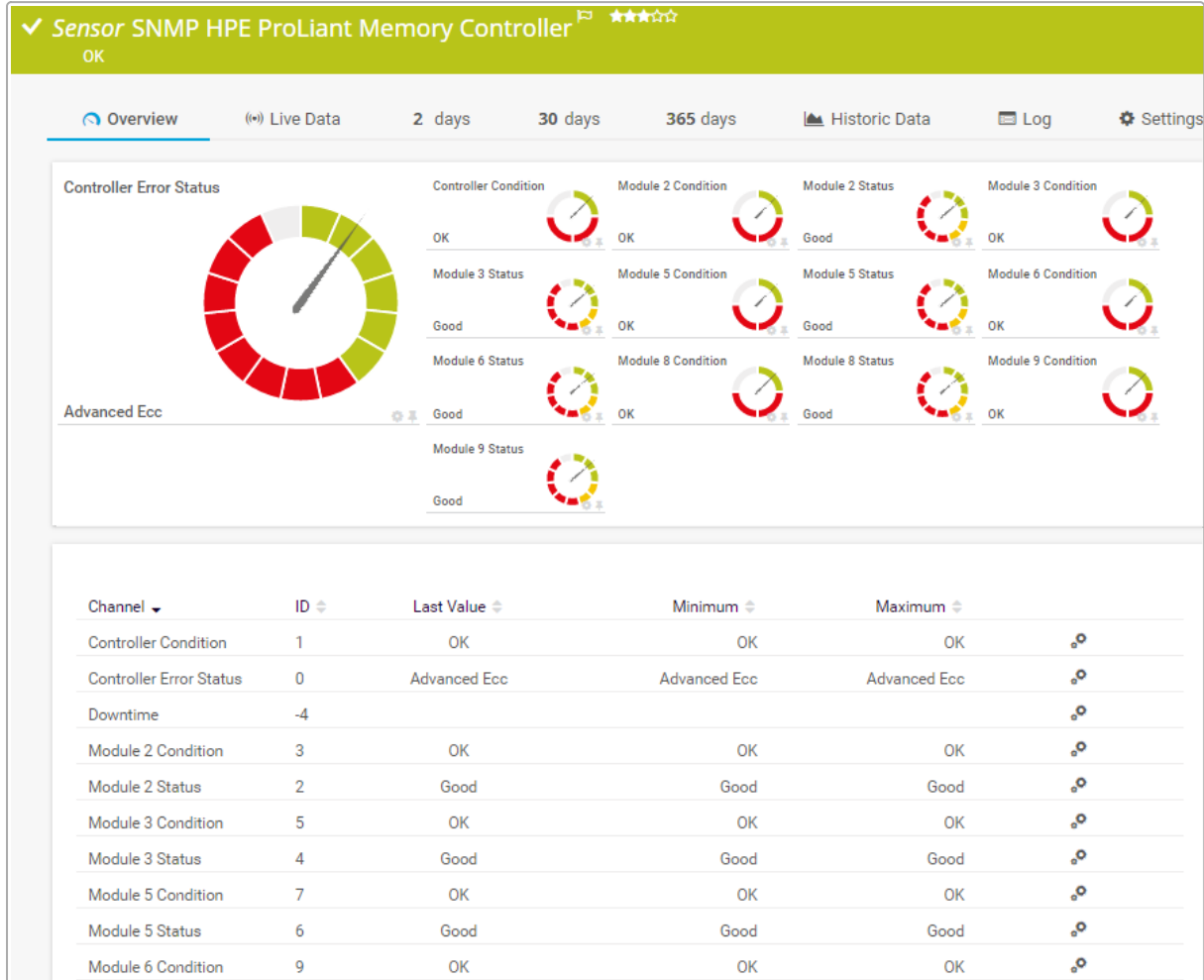
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.197 SNMP HPE ProLiant Memory Controller Sensor

The SNMP HPE ProLiant Memory Controller sensor monitors a memory controller in an HPE server via the Simple Network Management Protocol (SNMP).



SNMP HPE ProLiant Memory Controller Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP HPE ProLiant Geheugencontroller
- French: HPE ProLiant contrôleur de mémoire (SNMP)
- German: SNMP HPE ProLiant Speichercontroller
- Japanese: SNMP HPE ProLiant メモリコントローラー
- Portuguese: Controlador de memória HPE ProLiant (SNMP)
- Russian: Контроллер памяти HPE ProLiant по SNMP
- Simplified Chinese: SNMP HPE ProLiant 内存控制器
- Spanish: Controlador de memoria HPE ProLiant (SNMP)

## Remarks

Consider the following [remarks](#) <sup>[2001]</sup> and requirements for this sensor:

Remark	Description
HPE system management tools	<p>For Gen10 servers: This sensor requires <a href="#">HPE Agentless Management</a> and the <a href="#">HPE Agentless Management Service</a> on the target system.</p> <p>For Gen10 servers: Use the HPE Integrated Lights Out (iLO) interface as the parent device.</p> <p>For Gen9 servers or earlier: This sensor requires <a href="#">HPE Insight Management Agents</a> and <a href="#">HPE Insight Management WBEM Providers</a> on the target system.</p> <p><b>i</b> For Gen9 servers or earlier, this sensor requires a specific HPE system management tool to be installed on the target system to report data via SNMP: <a href="#">HPE Insight Management Agents</a>. To receive SNMP data from redundant array of independent disks (RAID) controllers, the sensor also requires <a href="#">HPE Insight Management Agents</a>. For Gen10 servers, this sensor no longer requires HPE system management tools. Instead, the sensor requires the <a href="#">HPE Agentless Management Service</a> to be installed on the target system.</p> <p><b>■</b> For more information and download links, see the Knowledge Base: <a href="#">Monitor HP ProLiant via SNMP?</a></p> <p>For Gen9 servers or earlier, some of the HPE object identifiers (OID) that <b>i</b> this sensor uses are only accessible via the iLO interface. If this sensor throws an error that it cannot find "such device types", create a device that points to the address of the HPE iLO interface (if available) and add the sensor to this device. We recommend that you use the <a href="#">Agentless Management</a> feature with configured SNMP. You can set this up in the iLO configuration interface under Administration   Management   SNMP Settings. For Gen10 servers, use the HPE iLO interface as parent device for this sensor.</p>
iLO versions	This sensor supports iLO as of iLO 3. We recommend that you use at least iLO 4.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Modules	If modules are inserted at a later point, you must add this sensor anew.
Knowledge Base	Knowledge Base: <a href="#">Which lookup values are supported by the SNMP HPE ProLiant Memory Controller sensor?</a>

## Basic Sensor Settings

Basic Sensor Settings

Sensor Name ⓘ Example Name

Tags ⓘ

exampletag X +

Priority ⓘ

★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- hpe
- memorycontroller
- snmphpe
- snmphmemorycontrollersensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## HPE ProLiant Memory Controller Settings

HPE ProLiant Memory Controller Settings

Controller ⓘ Memory Controller CPU 1

HPE ProLiant Memory Controller Settings

Setting	Description
Controller	The name of the controller that this sensor monitors.

## Sensor Display

Sensor Display


Primary Channel ⓘ Downtime

Graph Type ⓘ


Show channels independently (default)
   
 Stack channels on top of each other


Sensor Display



Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Controller Condition	<p>The controller condition</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Degraded</li> </ul>

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Down status: Failed</li> <li>▪ Unknown status: Other</li> </ul>
Controller Error Status	<p>The controller error status</p> <ul style="list-style-type: none"> <li>▪ Up status: Advanced Ecc, Lock Step, Memory Raid, Mirrored, No Error, OnlineSpare</li> <li>▪ Down status: Bus Error, Config Error, Dimm Ecc Error, Lock Step Error, Mirrored Dimm Error, Power Error, Raid Dimm Error, Unlock Error</li> <li>▪ Unknown status: Other</li> </ul> <p> This channel is the primary channel by default.</p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Module [#] Condition	<p>The module condition</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Down status: Degraded, Failed</li> <li>▪ Unknown status: Other</li> </ul>
Module [#] Status	<p>The module status</p> <ul style="list-style-type: none"> <li>▪ Up status: Add, Good, Present</li> <li>▪ Warning status: Not Present, Upgrade</li> <li>▪ Down status: Bad Config, Degraded, Does Not Match, Missing, Not Supported</li> <li>▪ Unknown status: Other</li> </ul>

## More

### KNOWLEDGE BASE

Which lookup values are supported by the SNMP HPE ProLiant Memory Controller sensor?

- <https://kb.paessler.com/en/topic/44803>

Monitor HP ProLiant via SNMP?

- <https://kb.paessler.com/en/topic/33133>

What security features does PRTG include?

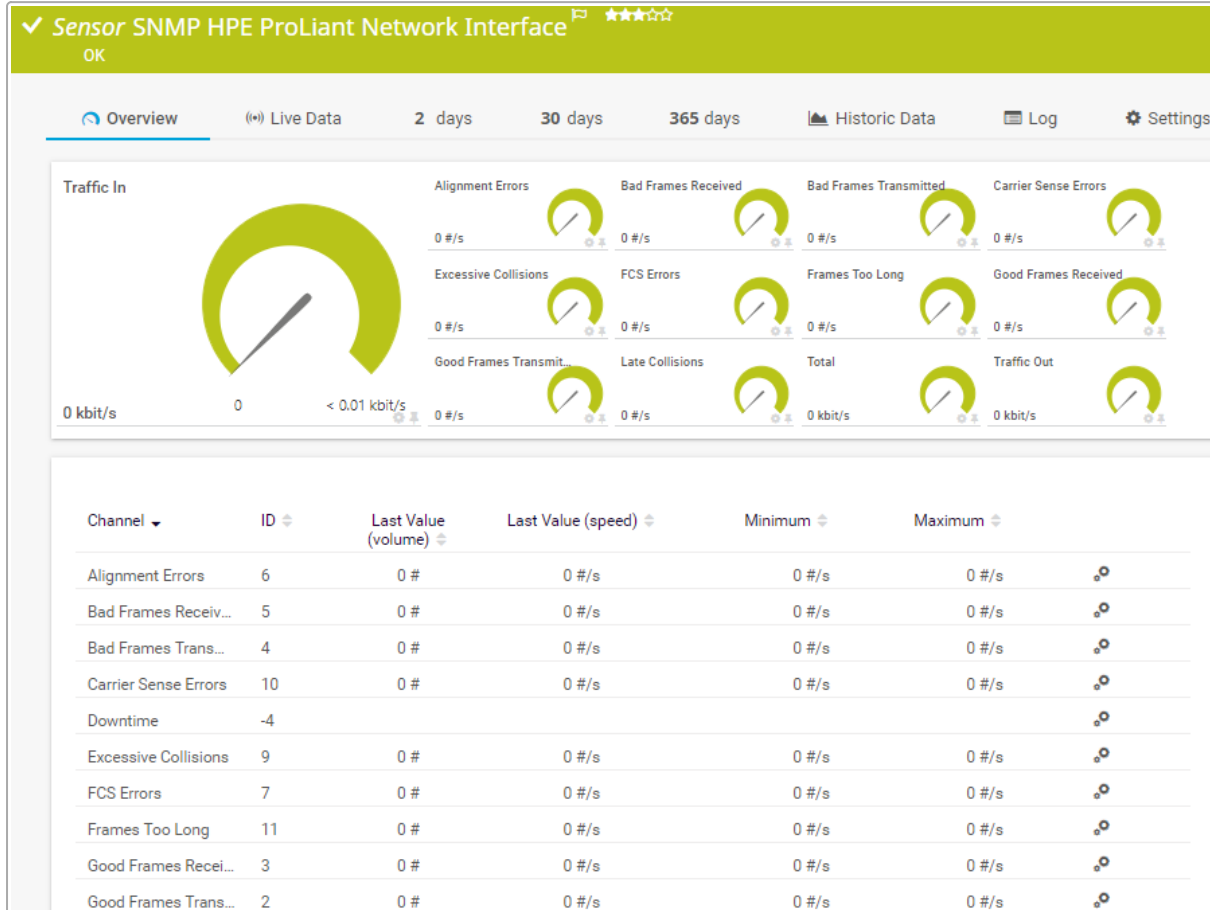
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.198 SNMP HPE ProLiant Network Interface Sensor

The SNMP HPE ProLiant Network Interface sensor monitors a network interface in an HPE server via the Simple Network Management Protocol (SNMP).



SNMP HPE ProLiant Network Interface Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP HPE ProLiant Netwerkindertace
- French: HPE ProLiant interface réseau (SNMP)
- German: SNMP HPE ProLiant Netzwerkschnittstelle
- Japanese: SNMP HPE ProLiant ネットワークインターフェース
- Portuguese: Interface de rede HPE ProLiant (SNMP)
- Russian: Сетевой интерфейс HPE ProLiant по SNMP
- Simplified Chinese: SNMP HPE ProLiant 网络接口
- Spanish: Interfaz de red HPE ProLiant (SNMP)

## Remarks

Consider the following [remarks](#) <sup>[2007]</sup> and requirements for this sensor:

Remark	Description
HPE system management tools	<p>For Gen10 servers: This sensor requires <a href="#">HPE Agentless Management</a> and the <a href="#">HPE Agentless Management Service</a> on the target system.</p> <p>For Gen10 servers: Use the HPE Integrated Lights Out (iLO) interface as the parent device.</p> <p>For Gen9 servers or earlier: This sensor requires <a href="#">HPE Insight Management Agents</a> and <a href="#">HPE Insight Management WBEM Providers</a> on the target system.</p> <p><b>i</b> For Gen9 servers or earlier, this sensor requires a specific HPE system management tool to be installed on the target system to report data via SNMP: <a href="#">HPE Insight Management Agents</a>. To receive SNMP data from redundant array of independent disks (RAID) controllers, the sensor also requires <a href="#">HPE Insight Management Agents</a>. For Gen10 servers, this sensor no longer requires HPE system management tools. Instead, the sensor requires the <a href="#">HPE Agentless Management Service</a> to be installed on the target system.</p> <p><b>■</b> For more information and download links, see the Knowledge Base: <a href="#">Monitor HP ProLiant via SNMP?</a></p> <p>For Gen9 servers or earlier, some of the HPE object identifiers (OID) that <b>i</b> this sensor uses are only accessible via the iLO interface. If this sensor throws an error that it cannot find "such device types", create a device that points to the address of the HPE iLO interface (if available) and add the sensor to this device. We recommend that you use the <a href="#">Agentless Management</a> feature with configured SNMP. You can set this up in the iLO configuration interface under Administration   Management   SNMP Settings. For Gen10 servers, use the HPE iLO interface as parent device for this sensor.</p>
iLO versions	This sensor supports iLO as of iLO 3. We recommend that you use at least iLO 4.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Sensor creation	During sensor creation, the status of each available network interface is shown. If this status is <a href="#">Link Failure</a> , it is still possible to add a sensor for the respective interface. Though, most likely the sensor for this interface does not work correctly. The error message in this case is <a href="#">No Such Name (SNMP error # 2)</a> .

## Basic Sensor Settings

Basic Sensor Settings
Sensor Name ⓘ Example Name

---

Tags ⓘ

exampletag ✕ +

---

Priority ⓘ
★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- hpe
- snmphpe
- snmphnetworkinterfacesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## HPE ProLiant Network Interface Settings

HPE ProLiant Network Interface Settings
Network Interfaces ⓘ e1

HPE ProLiant Network Interface Settings

Setting	Description
Network Interfaces	The name of the network interface that this sensor monitors.

## Sensor Display

Sensor Display
Primary Channel ⓘ Downtime


---

Graph Type ⓘ


Show channels independently (default)

Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Alignment Errors	The number of alignment errors
Bad Frames Received	The number of bad frames received

Channel	Description
Bad Frames Transmitted	The number of bad frames transmitted
Carrier Sense Errors	The number of carrier sense errors
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Excessive Collisions	The number of excessive collisions
FCS Errors	The number of FCS errors
Frames Too Long	The number of frames that are too long
Good Frames Received	The number of good frames received
Good Frames Transmitted	The number of good frames transmitted
Late Collisions	The number of late collisions
Total	The total traffic
Traffic In	The incoming traffic <b>i</b> This channel is the primary channel by default.
Traffic Out	The outgoing traffic

## More

### ■ KNOWLEDGE BASE

Monitor HP ProLiant via SNMP?

- <https://kb.paessler.com/en/topic/33133>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

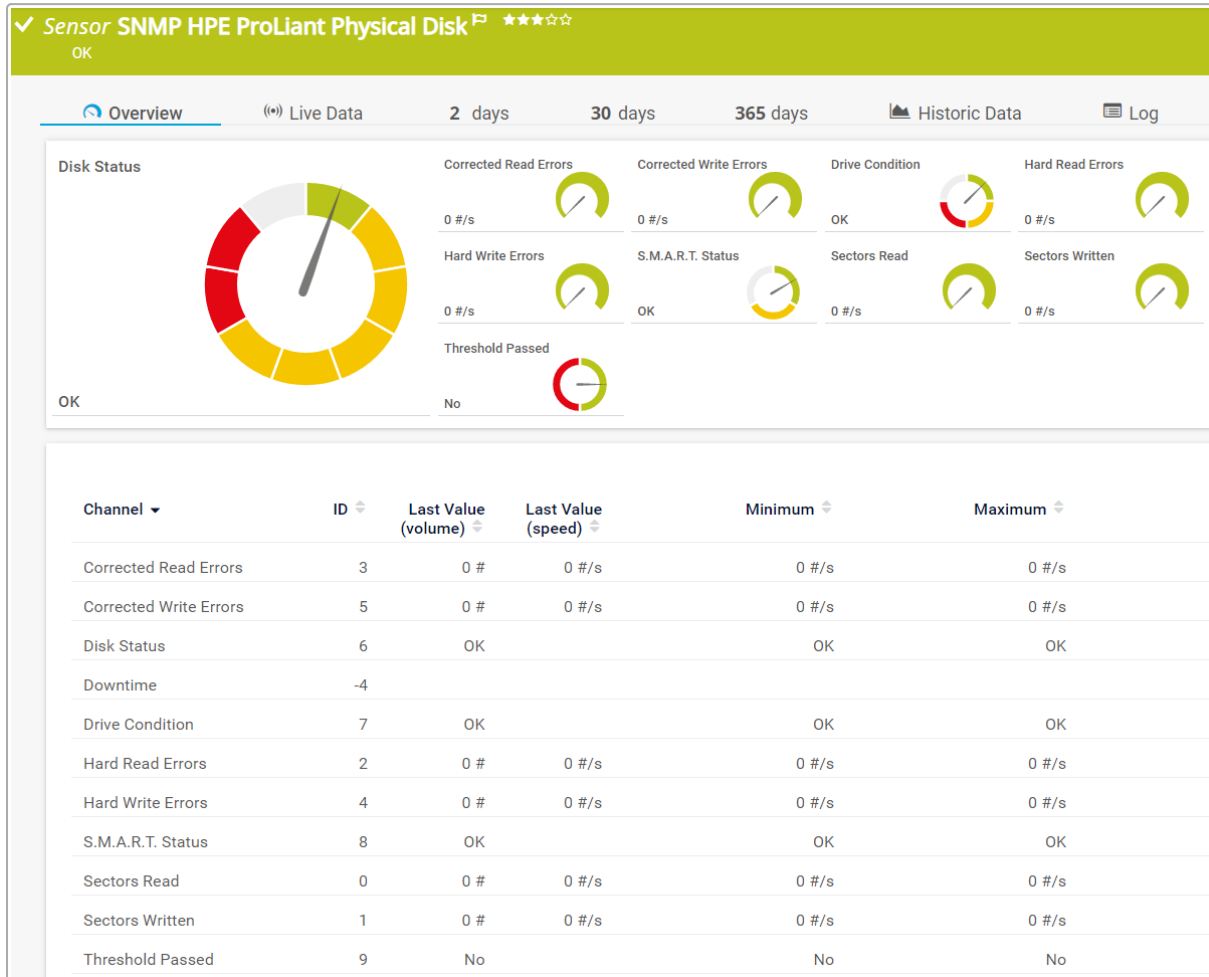
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>



## 7.8.199 SNMP HPE ProLiant Physical Disk Sensor

The SNMP HPE ProLiant Physical Disk sensor monitors a physical disk in an HPE server via the Simple Network Management Protocol (SNMP).



SNMP HPE ProLiant Physical Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) [2014].

### Sensor in Other Languages

- Dutch: SNMP HPE ProLiant Fysieke Schijf
- French: HPE ProLiant disque physique (SNMP)
- German: SNMP HPE ProLiant Physikalischer Datenträger
- Japanese: SNMP HPE ProLiant 物理ディスク
- Portuguese: Disco físico HPE ProLiant (SNMP)
- Russian: Физический диск HPE ProLiant по SNMP
- Simplified Chinese: SNMP HPE ProLiant 物理磁盘
- Spanish: Disco físico HPE ProLiant (SNMP)

## Remarks

Consider the following [remarks](#) <sup>[2012]</sup> and requirements for this sensor:

Remark	Description
HPE system management tools	<p>For Gen10 servers: This sensor requires <a href="#">HPE Agentless Management</a> and the <a href="#">HPE Agentless Management Service</a> on the target system.</p> <p>For Gen10 servers: Use the HPE Integrated Lights Out (iLO) interface as the parent device.</p> <p>For Gen9 servers or earlier: This sensor requires <a href="#">HPE Insight Management Agents</a> and <a href="#">HPE Insight Management WBEM Providers</a> on the target system.</p> <p><b>i</b> For Gen9 servers or earlier, this sensor requires a specific HPE system management tool to be installed on the target system to report data via SNMP: <a href="#">HPE Insight Management Agents</a>. To receive SNMP data from redundant array of independent disks (RAID) controllers, the sensor also requires <a href="#">HPE Insight Management Agents</a>. For Gen10 servers, this sensor no longer requires HPE system management tools. Instead, the sensor requires the <a href="#">HPE Agentless Management Service</a> to be installed on the target system.</p> <p><b>■</b> For more information and download links, see the Knowledge Base: <a href="#">Monitor HP ProLiant via SNMP?</a></p> <p>For Gen9 servers or earlier, some of the HPE object identifiers (OID) that <b>i</b> this sensor uses are only accessible via the iLO interface. If this sensor throws an error that it cannot find "such device types", create a device that points to the address of the HPE iLO interface (if available) and add the sensor to this device. We recommend that you use the <a href="#">Agentless Management</a> feature with configured SNMP. You can set this up in the iLO configuration interface under Administration   Management   SNMP Settings. For Gen10 servers, use the HPE iLO interface as parent device for this sensor.</p>
iLO versions	This sensor supports iLO as of iLO 3. We recommend that you use at least iLO 4.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
"Limited Monitoring" mode	The sensor only shows Disk Status and no other channels if it runs in "Limited Monitoring" mode. For more information, see the Knowledge Base: <a href="#">SNMP HPE ProLiant Physical Disk sensor not showing all information</a> .

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ exampletag ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Example Name

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- hpe
- physicaldisk
- snmphpe
- snmphpephysicaldisksensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## HPE ProLiant Physical Disk Settings

### HPE ProLiant Physical Disk Settings

**Disk** ⓘ

Example

HPE ProLiant Physical Disk Settings

Setting	Description
Disk	The ID of the physical disk that this sensor monitors.

## Sensor Display


### Sensor Display

**Primary Channel** ⓘ


**Graph Type** ⓘ 
 Show channels independently (default)
  Stack channels on top of each other


Downtime

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Corrected Read Errors	The corrected read errors
Corrected Write Errors	The corrected write errors

Channel	Description
Disk Status	<p>The disk status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Erase Done, Erase Queued, Erasing, Not Authenticated, Predictive Failure</li> <li>▪ Down status: Failed, SSD Wear Out</li> <li>▪ Unknown status: Other</li> </ul> <p> This channel is the primary channel by default.</p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Drive Condition	<p>The drive condition</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Degraded</li> <li>▪ Down status: Failed</li> <li>▪ Unknown status: Other</li> </ul>
Hard Read Errors	The number of hard read errors
Hard Write Errors	The number of hard write errors
S.M.A.R.T. Status	<p>The S.M.A.R.T. status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Replace Drive</li> <li>▪ Unknown status: Other</li> </ul>
Sectors Read	The number of sectors read
Sectors Written	The number of sectors written
Threshold Passed	<p>If the threshold is passed</p> <ul style="list-style-type: none"> <li>▪ Up status: No</li> <li>▪ Down status: Yes</li> </ul>

## More

### ■ KNOWLEDGE BASE

SNMP HPE ProLiant Physical Disk sensor not showing all information

- <https://kb.paessler.com/en/topic/70009>

Monitor HP ProLiant via SNMP?

- <https://kb.paessler.com/en/topic/33133>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.200 SNMP HPE ProLiant System Health Sensor

The SNMP HPE ProLiant System Health sensor monitors the system health of an HPE ProLiant server via the Simple Network Management Protocol (SNMP).



SNMP HPE ProLiant System Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP HPE ProLiant Systemstatus
- French: HPE ProLiant état du système (SNMP)
- German: SNMP HPE ProLiant Systemzustand
- Japanese: SNMP HPE ProLiant システム正常性
- Portuguese: Saúde do sistema HPE ProLiant (SNMP)

- Russian: Работоспособность системы HPE ProLiant по SNMP
- Simplified Chinese: SNMP HPE ProLiant 系统健康状况
- Spanish: Salud de sistema HPE ProLiant (SNMP)

## Remarks

Consider the following [remarks](#)<sup>2018</sup> and requirements for this sensor:

Remark	Description
HPE system management tools	<p>For Gen10 servers: Use the HPE Integrated Lights Out (iLO) interface as the parent device.</p> <p>For Gen9 servers or earlier: This sensor requires <a href="#">HPE Insight Management Agents</a> and <a href="#">HPE Insight Management WBEM Providers</a> on the target system.</p> <p><b>i</b> For Gen9 servers or earlier, this sensor requires a specific HPE system management tool to be installed on the target system to report data via SNMP: <a href="#">HPE Insight Management Agents</a>. To receive SNMP data from redundant array of independent disks (RAID) controllers, the sensor also requires <a href="#">HPE Insight Management Agents</a>. For Gen10 servers, this sensor no longer requires HPE system management tools.</p> <p><b>■</b> For more information and download links, see the Knowledge Base: <a href="#">Monitor HP ProLiant via SNMP?</a></p> <p>For Gen9 servers or earlier, some of the HPE object identifiers (OID) that <b>i</b> this sensor uses are only accessible via the iLO interface. If this sensor throws an error that it cannot find "such device types", create a device that points to the address of the HPE iLO interface (if available) and add the sensor to this device. We recommend that you use the <a href="#">Agentless Management</a> feature with configured SNMP. You can set this up in the iLO configuration interface under Administration   Management   SNMP Settings. For Gen10 servers, use the HPE iLO interface as parent device for this sensor.</p>
iLO versions	This sensor supports iLO as of iLO 3. We recommend that you use at least iLO 4.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for temperatures and broken frames.



Remark	Description
RAID controllers	Redundant array of independent disks (RAID) controllers that have no hard disks assigned might cause the Down <a href="#">status</a> . In this case, deactivate the respective controllers in the HPE ProLiant BIOS to avoid sensor errors.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- hpe
- snmp hpe
- snmp hpe system health sensor
- system health

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Display

### Sensor Display


**Primary Channel** ⓘ Downtime

---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.

Setting	Description
	<p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.           <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CPU Fan Status	<p>The CPU fan status</p> <ul style="list-style-type: none"> <li>Up status: OK</li> <li>Warning status: Degraded</li> <li>Down status: Failed</li> <li>Unknown status: Other</li> </ul>

Channel	Description
Disk Controller Status	<p>The disk controller status</p> <ul style="list-style-type: none"> <li>Up status: OK</li> <li>Warning status: Degraded</li> <li>Down status: Failed</li> <li>Unknown status: Other</li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Fans Broken	<p>The number of broken fans</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper error limit: 0</li> </ul>
Fans Running	<p>The number of running fans</p>
Fault Tolerant Fans Broken	<p>The number of fault-tolerant broken fans</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper error limit: 0</li> </ul>
Fault Tolerant Fans Running	<p>The number of fault-tolerant running fans</p>
Overall Status	<p>The overall status</p> <ul style="list-style-type: none"> <li>Up status: OK</li> <li>Warning status: Degraded</li> <li>Down status: Failed</li> <li>Unknown status: Other</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Power Consumption [#]	<p>The power consumption</p>
Power Consumption [#] (%)	<p>The power consumption (%)</p>
Power Supply [#] Condition	<p>The power supply condition</p> <ul style="list-style-type: none"> <li>Up status: OK</li> </ul>

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Down status: Degraded, Failed</li> <li>▪ Unknown status: Other</li> </ul>
Power Supply [#] Status	<p>The power supply status</p> <ul style="list-style-type: none"> <li>▪ Up status: No Error</li> <li>▪ Down status: Bist Failure, Brownout, Calibration Table Invalid, Dac Failure, Eprom Failure, Fan Failure, General Failure, Give Up On Startup, Interlock Open, No Power Input, Nvram Invalid, Orring Diode Failed, Ram Test Failed, Temp Failure, Voltage Channel Failed, Vref Failure</li> </ul>
System Fan Status	<p>The system fan status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Degraded</li> <li>▪ Down status: Failed</li> <li>▪ Unknown status: Other</li> </ul>
Temperature [#] ([Component])	<p>The temperature of the component</p>
Thermal Status	<p>The thermal status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Degraded</li> <li>▪ Down status: Failed</li> <li>▪ Unknown status: Other</li> </ul>

## More

### ■ KNOWLEDGE BASE

Monitor HP ProLiant via SNMP?

- <https://kb.paessler.com/en/topic/33133>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Why is my SNMP HPE ProLiant System Health sensor in the error status after updating PRTG?

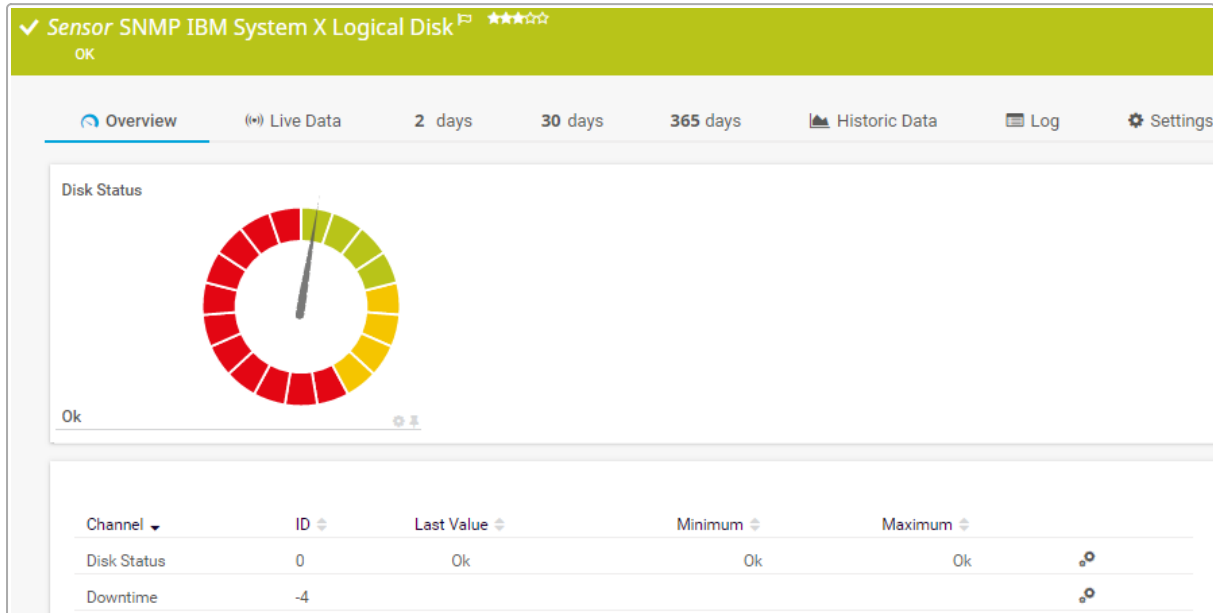
- <https://kb.paessler.com/en/topic/61805>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.201 SNMP IBM System X Logical Disk Sensor

The SNMP IBM System X Logical Disk sensor monitors a logical disk in an IBM server via the Simple Network Management Protocol (SNMP).



SNMP IBM System X Logical Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP IBM System X Logical Disk
- French: IBM System X disque logique (SNMP)
- German: SNMP IBM System X Logischer Datenträger
- Japanese: SNMP IBM System X 論理 ディスク
- Portuguese: Disco lógico IBM System X (SNMP)
- Russian: Логический диск IBM System X по SNMP
- Simplified Chinese: SNMP IBM System X 逻辑 磁盘
- Spanish: Disco lógico IBM System X (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IBM Systems Director Platform Agent	This sensor requires the <a href="#">IBM Systems Director Platform Agent</a> on the target system.

Remark	Description
	<p>■ For more information, see the Knowledge Base: <a href="#">What are the requirements to monitor IBM System x?</a></p>
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">What are the requirements to monitor IBM System x?</a></li> <li>Knowledge Base: <a href="#">IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)</a></li> </ul>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- ibm
- logicaldisk
- snmpibm
- snmpibmlogicaldisksensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## IBM System X Logical Disk Settings

IBM System X Logical Disk Settings
Disk ⓘ Example

IBM System X Logical Disk Settings

Setting	Description
Disk	The ID of the logical disk that this sensor monitors.

## Sensor Display

Sensor Display


Primary Channel ⓘ Downtime  
Graph Type ⓘ  Show channels independently (default)  Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>




## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Disk Status	<p>The disk status</p> <ul style="list-style-type: none"> <li>▪ Up status: Completed, In Service, Ok, Power Mode</li> <li>▪ Warning status: Dormant, Predictive Failure, Starting, Stressed</li> <li>▪ Down status: Aborted, Degraded, Error, Lost Communication, No Contact, Non-Recoverable Error, Other, Stopped, Stopping, Supporting Entity In Error, Unknown</li> </ul> <p> This channel is the primary channel by default.</p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>

## More

### ■ KNOWLEDGE BASE

What are the requirements to monitor IBM System x?

- <https://kb.paessler.com/en/topic/59393>

IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)

- <https://kb.paessler.com/en/topic/73914>

What security features does PRTG include?

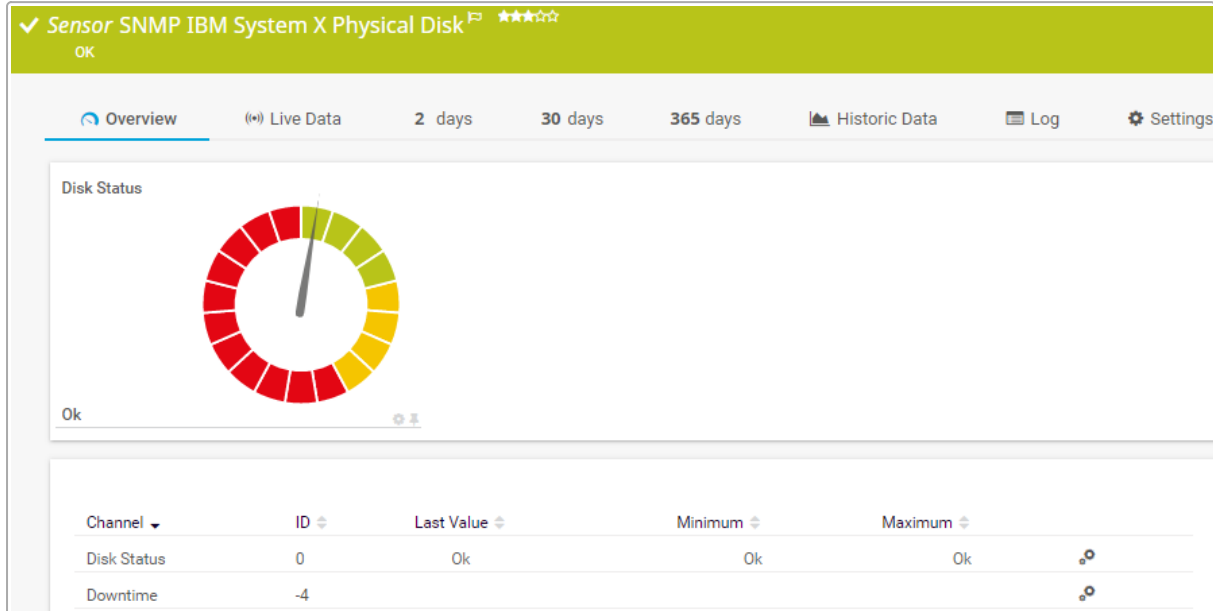
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.202 SNMP IBM System X Physical Disk Sensor

The SNMP IBM System X Physical Disk sensor monitors a physical disk in an IBM server via the Simple Network Management Protocol (SNMP).



SNMP IBM System X Physical Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP IBM System X Physical Disk
- French: IBM System X disque physique (SNMP)
- German: SNMP IBM System X Physikalischer Datenträger
- Japanese: SNMP IBM System X 物理ディスク
- Portuguese: Disco físico IBM System X (SNMP)
- Russian: Физический диск IBM System X по SNMP
- Simplified Chinese: SNMP IBM System X 物理磁盘
- Spanish: Disco físico IBM System X (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IBM Systems Director Platform Agent	This sensor requires the <a href="#">IBM Systems Director Platform Agent</a> on the target system.

Remark	Description
	<p>■ For more information, see the Knowledge Base: <a href="#">What are the requirements to monitor IBM System x?</a></p>
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">What are the requirements to monitor IBM System x?</a></li> <li>Knowledge Base: <a href="#">IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)</a></li> </ul>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- ibm
- physicaldisk
- snmpibm
- snmpibmphysicaldisksensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## IBM System X Physical Disk Settings

IBM System X Physical Disk Settings
Disk ⓘ
Example

IBM System X Physical Disk Settings

Setting	Description
Disk	The ID of the physical disk that this sensor monitors.

## Sensor Display

Sensor Display


Primary Channel ⓘ Downtime

Graph Type ⓘ
 Show channels independently (default)
  Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>ⓘ</b> You can set a different primary channel later by clicking <b>⚙</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>ⓘ</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Disk Status	<p>The disk status</p> <ul style="list-style-type: none"> <li>▪ Up status: Completed, In Service, Ok, Power Mode</li> <li>▪ Warning status: Dormant, Predictive Failure, Starting, Stressed</li> <li>▪ Down status: Aborted, Degraded, Error, Lost Communication, No Contact, Non-Recoverable Error, Other, Stopped, Stopping, Supporting Entity In Error, Unknown</li> </ul> <p> This channel is the primary channel by default.</p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>

## More

### ■ KNOWLEDGE BASE

What are the requirements to monitor IBM System x?

- <https://kb.paessler.com/en/topic/59393>

IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)

- <https://kb.paessler.com/en/topic/73914>

What security features does PRTG include?

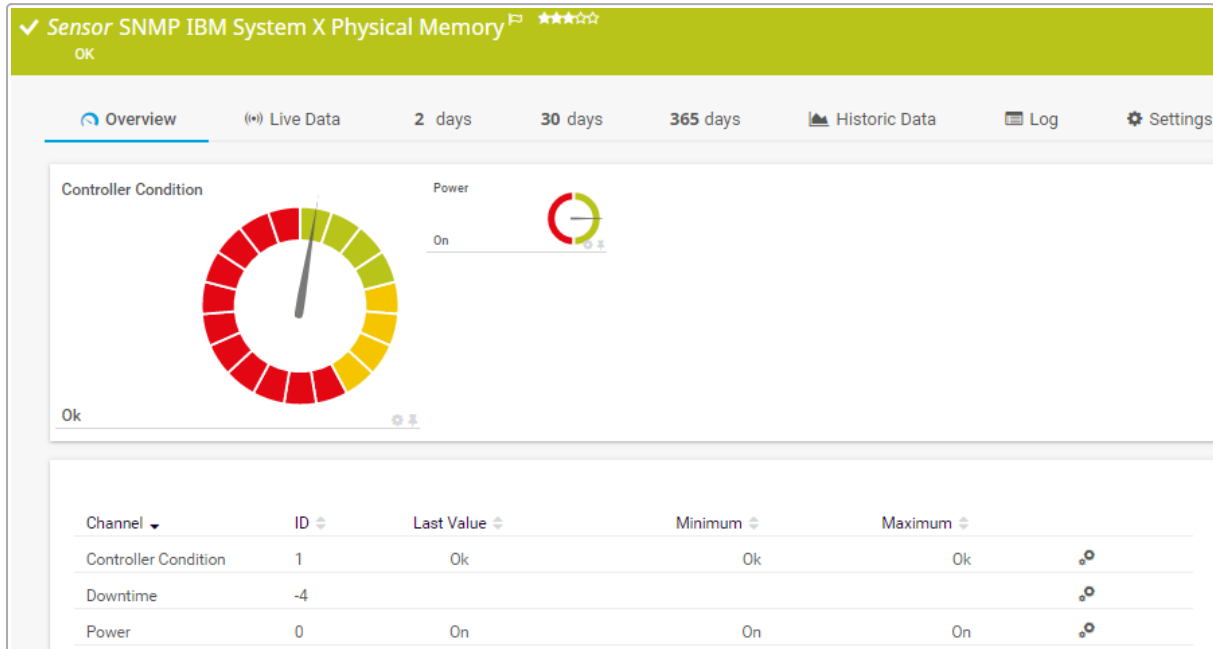
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.203 SNMP IBM System X Physical Memory Sensor

The SNMP IBM System X Physical Memory sensor monitors the memory modules in an IBM server via the Simple Network Management Protocol (SNMP).



SNMP IBM System X Physical Memory Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2035]</sup>.

### Sensor in Other Languages

- Dutch: SNMP IBM System X Physical Memory
- French: IBM System X mémoire physique (SNMP)
- German: SNMP IBM System X Physikalischer Speicher
- Japanese: SNMP IBM System X 物理メモリ
- Portuguese: Memória física IBM System X (SNMP)
- Russian: Физическая память IBM System X по SNMP
- Simplified Chinese: SNMP IBM System X 物理内存
- Spanish: Memoria física IBM System X (SNMP)

### Remarks

Consider the following [remarks](#)<sup>[2032]</sup> and requirements for this sensor:

Remark	Description
IBM Systems Director Platform Agent	This sensor requires the <a href="#">IBM Systems Director Platform Agent</a> on the target system.  ■ For more information, see the Knowledge Base: <a href="#">What are the requirements to monitor IBM System x?</a>
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">What are the requirements to monitor IBM System x?</a></li> <li>Knowledge Base: <a href="#">IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)</a></li> </ul>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag X +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- ibm
- memorycontroller
- snmpibm
- snmpibmphysicalmemorysensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>[667]</sup>.

## IBM System X Physical Memory Settings

**IBM System X Physical Memory Settings**

**Name** ⓘ *DIMM 1:Bank 1*

**Caption** ⓘ *System Memory*

**Serial Number** ⓘ *1111aaaa-22bb-cc33-dd44-555555eeeeeee*

**Size** ⓘ *1024 MB*

IBM System X Physical Memory Settings

Setting	Description
Name	The name of the memory module that this sensor monitors.
Caption	The caption of the memory module that this sensor monitors.
Serial Number	The serial number of the memory module that this sensor monitors.
Size	The size of the memory module that this sensor monitors.

## Sensor Display

**Sensor Display**


**Primary Channel** ⓘ *Downtime*

**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.  ⓘ You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.
Graph Type	Define how this sensor shows different channels:  ▪ Show channels independently (default): Show a graph for each channel.



Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Controller Condition	<p>The memory controller condition</p> <ul style="list-style-type: none"> <li>Up status: Completed, In Service, Ok, Power Mode</li> <li>Warning status: Dormant, Predictive Failure, Starting, Stressed</li> <li>Down status: Aborted, Degraded, Error, Lost Communication, No Contact, Non-Recoverable Error, Other, Stopped, Stopping, Supporting Entity In Error, Unknown</li> </ul> <p> This channel is the primary channel by default.</p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>

Channel	Description
Power	The power status <ul style="list-style-type: none"><li>▪ Up status: On</li><li>▪ Down status: Off</li></ul>

## More

### KNOWLEDGE BASE

What are the requirements to monitor IBM System x?

- <https://kb.paessler.com/en/topic/59393>

IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)

- <https://kb.paessler.com/en/topic/73914>

What security features does PRTG include?

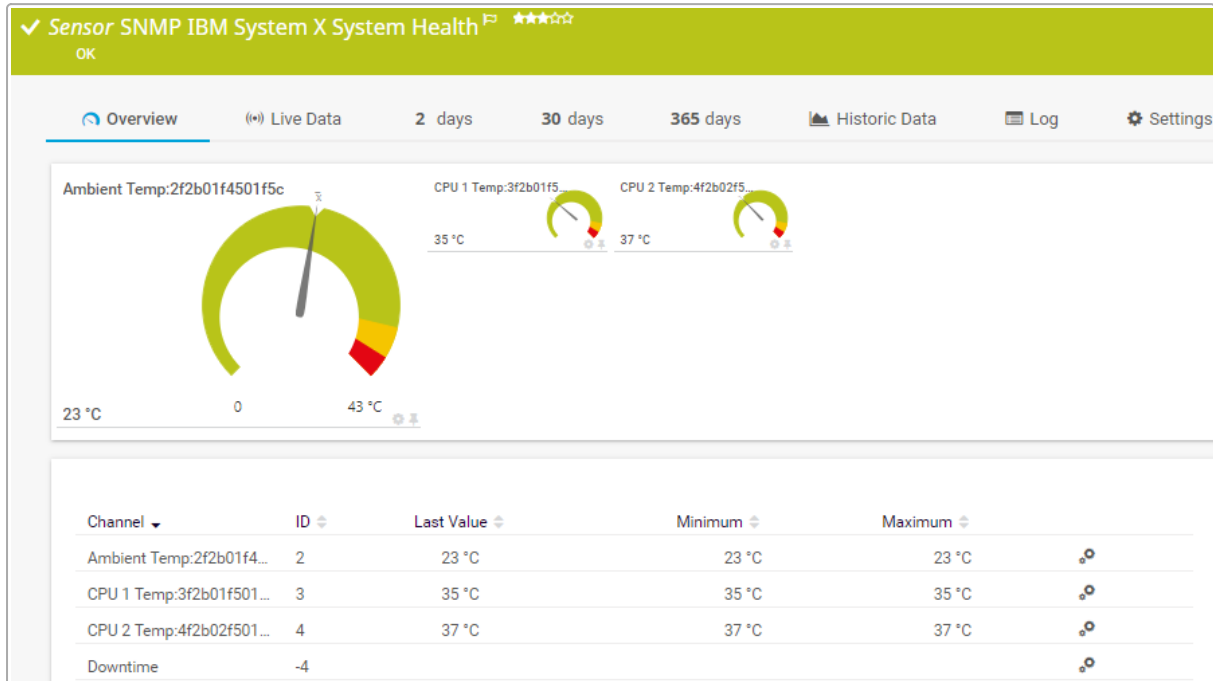
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.204 SNMP IBM System X System Health Sensor

The SNMP IBM System X System Health sensor monitors the system health of an IBM device via the Simple Network Management Protocol (SNMP).



SNMP IBM System X System Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP IBM System X Systemstatus
- French: IBM System X état du système (SNMP)
- German: SNMP IBM System X Systemzustand
- Japanese: SNMP IBM System X システムの正常性
- Portuguese: Saúde do sistema IBM System X (SNMP)
- Russian: Работоспособность системы IBM System X по SNMP
- Simplified Chinese: SNMP IBM System X 系统健康状况
- Spanish: Salud de sistema IBM System X (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IBM Systems Director Platform Agent	This sensor requires the <a href="#">IBM Systems Director Platform Agent</a> on the target system.  ■ For more information, see the Knowledge Base: <a href="#">What are the requirements to monitor IBM System x?</a>
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
IMM	This sensor can also run directly on an Integrated Management Module (IMM) network port and can show the overall health of IMM.
Unexpected format	If the IBM device returns a string in an unexpected format for the percentage of fan revolutions (for example, "offline"), this sensor shows -1% in the corresponding channel. You can define the Down status for this via <a href="#">channel limits</a> .
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">What are the requirements to monitor IBM System x?</a></li> <li>Knowledge Base: <a href="#">IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)</a></li> </ul>

**i** The SNMP IBM System X System Health sensor can also run directly on an IMM network port and can show the overall health of IMM.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- snmpibmsystemhealthsensor
- systemhealth

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### IBM System X System Health Specific

**IBM System X System Health Specific**

**Source** ⓘ *Integrated Management Module*

**Measurement** ⓘ *Fans*

IBM System X System Health Specific

Setting	Description
Source	The source of the measurement that this sensor monitors.
Measurement	The type of measurement that this sensor monitors.

### Sensor Display

**Sensor Display**


**Primary Channel** ⓘ *Downtime*

**Graph Type** ⓘ


Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking <b>↑</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Ambient Temp	The ambient temperature
CMOS Battery	The CMOS battery voltage
CPU [#] Temp	The CPU temperature
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Fan [#] Tach	The fan RPM or the percentage of the possible maximum
Overall Status	The overall status

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Up status: Normal, System Level</li> <li>▪ Warning status: Non Critical</li> <li>▪ Down status: Critical</li> </ul>
SysBrd 3.3V	The 3.3V-system board voltage
SysBrd 5V	The 5V-system board voltage
SysBrd 12V	The 12V-system board voltage

## More

### ■ KNOWLEDGE BASE

What are the requirements to monitor IBM System x?

- <https://kb.paessler.com/en/topic/59393>

IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)

- <https://kb.paessler.com/en/topic/73914>

What security features does PRTG include?

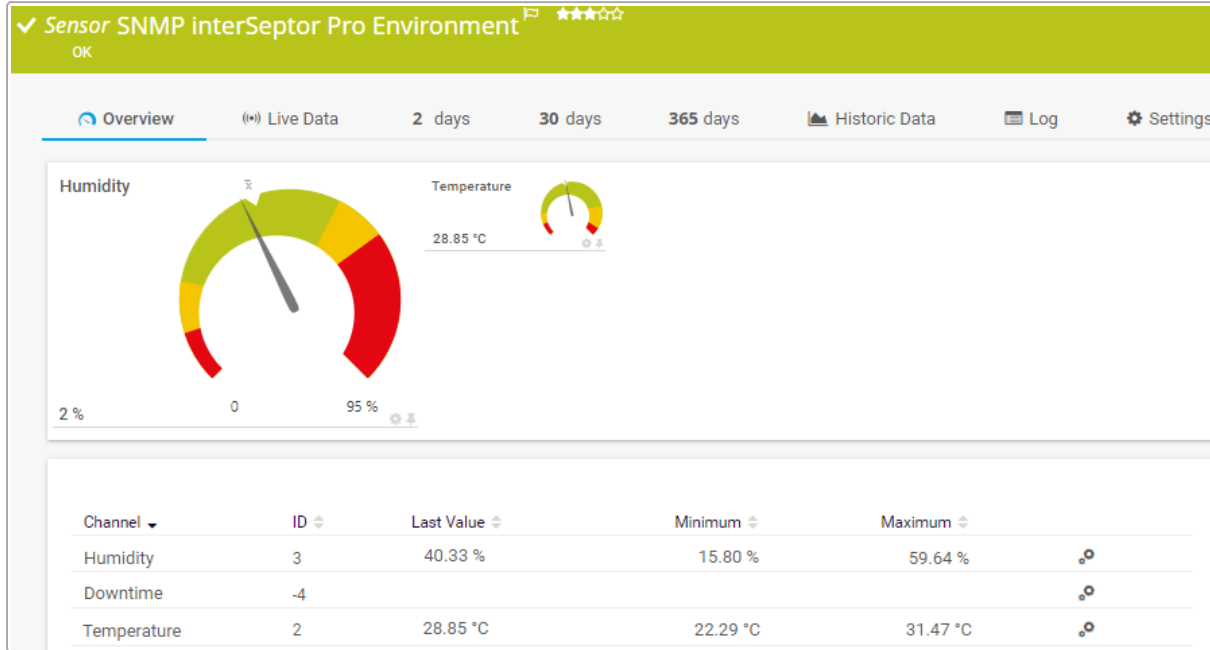
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.205 SNMP interSeptor Pro Environment Sensor

The SNMP interSeptor Pro Environment sensor queries data from a Jakarta interSeptor Pro environmental monitoring system via the Simple Network Management Protocol (SNMP).



SNMP interSeptor Pro Environment Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2045]</sup>.

### Sensor in Other Languages

- Dutch: SNMP interSeptor Pro Omgeving
- French: interSeptor Pro environnement (SNMP)
- German: SNMP interSeptor Pro Umgebung
- Japanese: SNMP interSeptor Pro 環境
- Portuguese: Ambiente interSeptor Pro (SNMP)
- Russian: Окружающая среда interSeptor Pro по SNMP
- Simplified Chinese: SNMP interSeptor Pro 环境
- Spanish: Entorno interSeptor Pro (SNMP)

### Remarks

Consider the following [remarks](#)<sup>[2042]</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.



Remark	Description
Performance impact	This sensor has a <b>very low</b> performance impact.
IP address	To monitor data of an interSeptor Pro device with this sensor, you must add the IP address of your PRTG core server system to Access Control in the interSeptor Pro control panel. Open the interSeptor Pro web interface, select InterSeptor Pro Menu   System Configuration   Access Control, and allow access for the IP address of PRTG.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- environment
- interseptor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### InterSeptor Environment Specific

#### InterSeptor Environment Specific

**Name** ⓘ *Sensor1-1*

---

**Measuring Point** ⓘ *0*

InterSeptor Environment Specific

Setting	Description
Name	The name of the measuring point that this sensor monitors.

Setting	Description
Measuring Point	The measuring point that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

❗ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Humidity	The humidity (%)
Temperature	The temperature

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

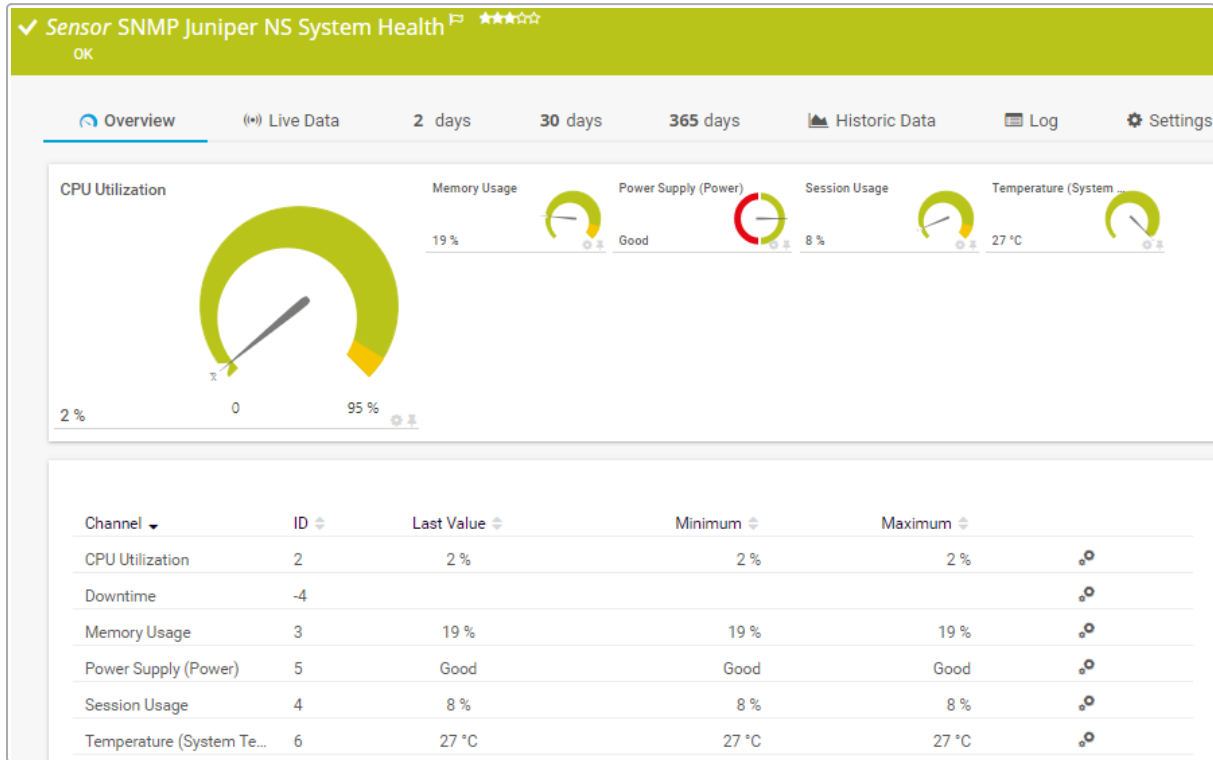
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.206 SNMP Juniper NS System Health Sensor

The SNMP Juniper NS System Health sensor monitors the system health of a Juniper NetScreen device via the Simple Network Management Protocol (SNMP).



SNMP Juniper NS System Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2048]</sup>.

### Sensor in Other Languages

- Dutch: SNMP Juniper NS systeemstatus
- French: Juniper NS état du système (SNMP)
- German: SNMP Juniper NS Systemzustand
- Japanese: SNMP Juniper NS のシステム正常性
- Portuguese: Saúde do sistema Juniper NS (SNMP)
- Russian: Работоспособность системы Juniper NS по SNMP
- Simplified Chinese: SNMP Juniper NS 系统健康状况
- Spanish: Salud de sistema Juniper NS (SNMP)

### Remarks

Consider the following [remarks](#)<sup>[2046]</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- snmpjuniper
- systemhealth

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Display

#### Sensor Display


**Primary Channel** ⓘ Downtime

---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.

Setting	Description
	<p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CPU Utilization	<p>The CPU usage</p> <p><b>i</b> This channel is the primary channel by default.</p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>

Channel	Description
Memory Usage	The memory usage (%)
Power Supply (Power)	The power supply status <ul style="list-style-type: none"><li>▪ Up status: Good</li><li>▪ Down status: Fail</li></ul>
Session Usage	The session usage (%)
Temperature (System Temperature)	The system temperature

## More

### KNOWLEDGE BASE

What security features does PRTG include?

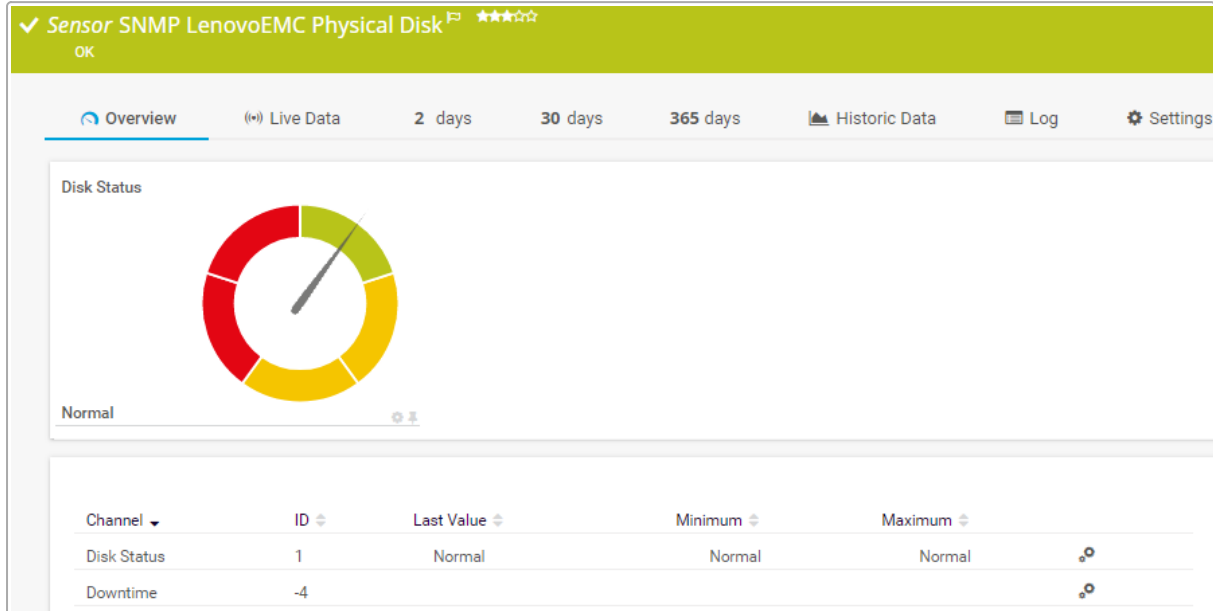
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.207 SNMP LenovoEMC Physical Disk Sensor

The SNMP LenovoEMC Physical Disk sensor monitors a physical disk in a LenovoEMC network-attached storage (NAS) via the Simple Network Management Protocol (SNMP).



SNMP LenovoEMC Physical Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP LenovoEMC fysieke schijf
- French: LenovoEMC disque physique (SNMP)
- German: SNMP LenovoEMC Physikalischer Datenträger
- Japanese: SNMP LenovoEMC 物理ディスク
- Portuguese: Disco físico LenovoEMC (SNMP)
- Russian: Физический диск LenovoEMC по SNMP
- Simplified Chinese: SNMP LenovoEMC 物理磁盘
- Spanish: Disco físico LenovoEMC (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.



Remark	Description
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

**Tags** ⓘ  ✕ +

**Priority** ⓘ

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- lenovoemc
- physicaldisk
- snmplenovoemc

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### LenovoEMC NAS Settings

#### LenovoEMC NAS Settings

**Disk** ⓘ

1

**Name** ⓘ

Disk 1

**Size** ⓘ

1863.02GB

LenovoEMC NAS Settings

Setting	Description
Disk	The ID of the physical disk that this sensor monitors.

Setting	Description
Name	The name of the physical disk that this sensor monitors.
Size	The size of the physical disk that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Disk Status	<p>The disk status</p> <ul style="list-style-type: none"> <li>▪ Up status: Normal</li> <li>▪ Warning status: Foreign, Unknown</li> <li>▪ Down status: Faulted, Missing</li> </ul> <p> This channel is the primary channel by default.</p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>

## More

### KNOWLEDGE BASE

What security features does PRTG include?

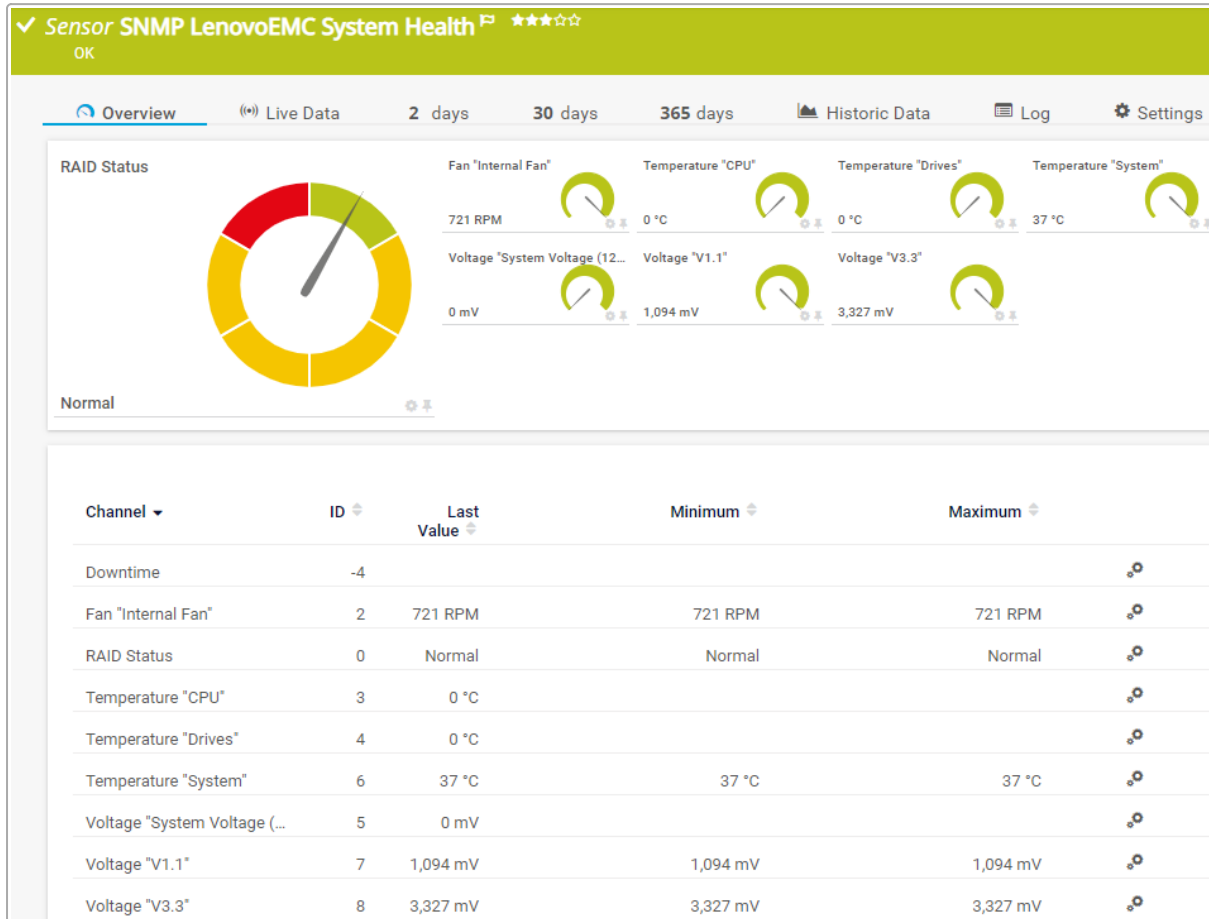
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.208 SNMP LenovoEMC System Health Sensor

The SNMP LenovoEMC System Health sensor monitors the system health of a LenovoEMC network-attached storage (NAS) via the Simple Network Management Protocol (SNMP).



SNMP LenovoEMC System Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2058]</sup>.

### Sensor in Other Languages

- Dutch: SNMP LenovoEMC Systeemstatus
- French: LenovoEMC état du système (SNMP)
- German: SNMP LenovoEMC Systemzustand
- Japanese: SNMP LenovoEMC システム正常性
- Portuguese: Saúde do sistema LenovoEMC (SNMP)
- Russian: Работоспособность системы LenovoEMC по SNMP
- Simplified Chinese: SNMP LenovoEMC 系统健康状况
- Spanish: Salud sistema LenovoEMC (SNMP)

## Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- lenovoemc
- snmplenovoemc
- systemhealth

■ For more information about basic sensor settings, see section [Sensor Settings](#).

## Sensor Display


### Sensor Display

**Primary Channel** ⓘ Downtime


---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Fan "Internal Fan"	The fan RPM
RAID Status	<p>The RAID status</p> <ul style="list-style-type: none"> <li>▪ Up status: Normal</li> <li>▪ Warning status: Degraded, RebuildFS, Rebuilding, Unknown</li> <li>▪ Down status: Faulted</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Temperature "CPU"	The CPU temperature
Temperature "Drives"	The temperature of the drives
Temperature "System"	The temperature of the system
Voltage "System Voltage (12V)"	The system voltage (12V)
Voltage "V1.1"	The voltage of the 1.1V-battery
Voltage "V3.3"	The voltage of the 3.3V-battery

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

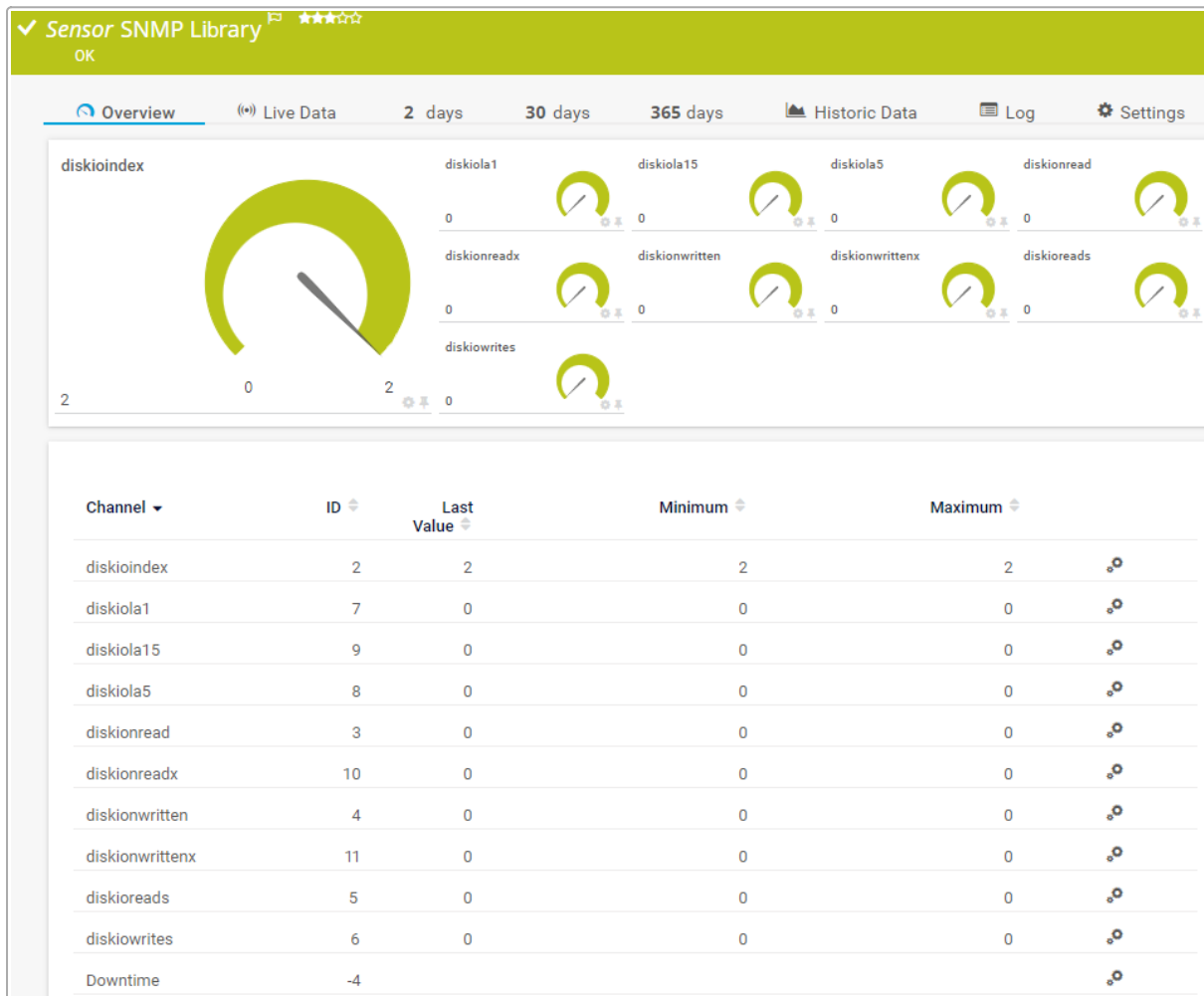
## 7.8.209 SNMP Library Sensor

The SNMP Library sensor uses a Management Information Base (MIB) file to create sensors that monitor a device via the Simple Network Management Protocol (SNMP).

- ❶ The content of the MIB file determines which data types are available for monitoring. When you create the sensor, it provides a list of counters that the target device returns based on every object identifier (OID) in the MIB file.
- ❷ The SNMP Library sensor does not appear as a running sensor. It uses the meta-scan facility of the probe to find or to match OIDs from the MIB file. It is useful because you do not need to manually enter OIDs.

To monitor SNMP-capable devices and to add sensors via the SNMP Library sensor, download the manufacturer's MIB files for the target device, convert the MIB files to the [OID library](#) format, and [import](#) them into PRTG. PRTG also provides [precompiled .oidlib files](#) that contain the OIDs of SNMP counters for the most common network devices.

For more information, see the Knowledge Base: [How do SNMP, MIBs and OIDs work?](#)



SNMP Custom Advanced Sensor Created by SNMP Library Sensor




## Sensor in Other Languages

- Dutch: SNMP Bibliotheek
- French: Bibliothèque (SNMP)
- German: SNMP-Bibliothek
- Japanese: SNMP ライブラリ
- Portuguese: Biblioteca (SNMP)
- Russian: Библиотека SNMP
- Simplified Chinese: SNMP 库
- Spanish: Biblioteca (SNMP)

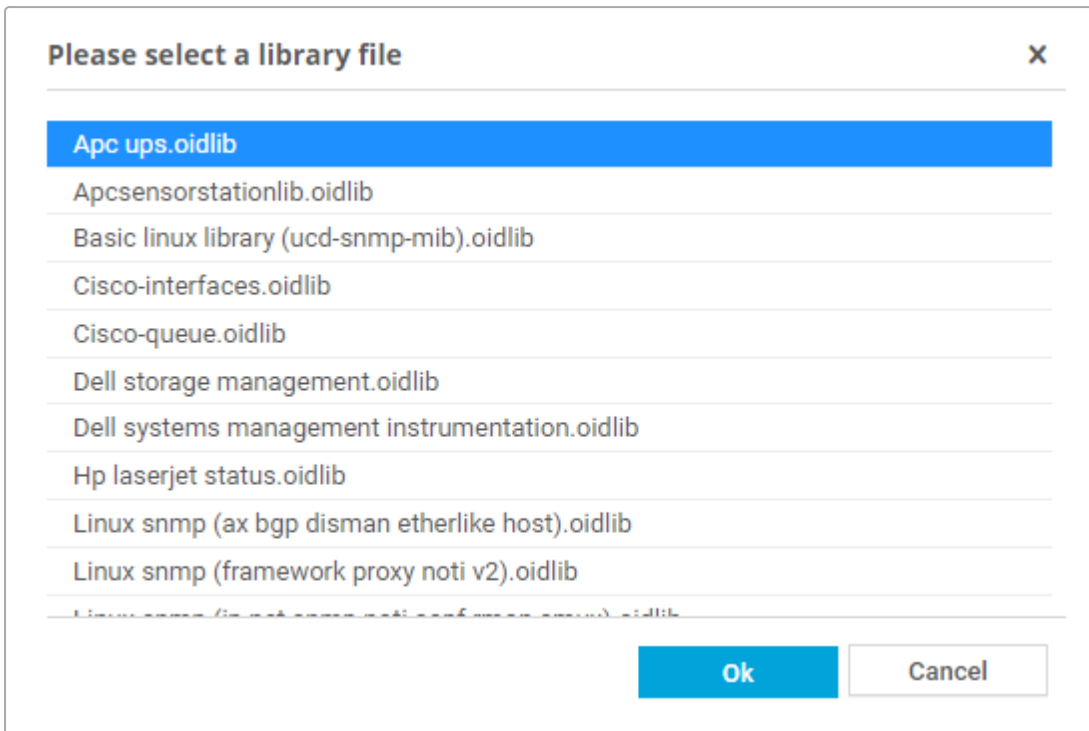
## Remarks

Consider the following [remarks](#) <sup>2059</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">How do SNMP, MIBs and OIDs work?</a></li> <li>▪ Knowledge Base: <a href="#">How can I import my MIB files into PRTG?</a></li> <li>▪ Knowledge Base: <a href="#">Can't find a sensor for my device in PRTG but I believe it supports SNMP. How to proceed?</a></li> </ul>
PRTG Hosted Monitor	 To import MIB files into PRTG Hosted Monitor, see section <a href="#">Manage a PRTG Hosted Monitor Subscription</a> .

## Add Sensor

PRTG shows a list of [.oidlib](#) files that are available on the system. This list contains all library files in the `\snmplibs` subfolder of the [PRTG program directory](#). It contains both the default PRTG library files and your own library files.



List of SNMP Library Files

The library file names in the list indicate their purpose. Select a library file that is suitable for the target device (for example, choose an MIB file that you imported) and confirm via Ok.

**i** If the library file not suitable for the target device, this results in the error message [The scan for available monitoring items has failed on this device: No such object \(SNMP error # 222\)](#). If you see this message, click Cancel and try to add the sensor with a different library file.

The SNMP Library sensor takes a list of OIDs that you import from an MIB file into an `.oidlib` file and tests the OIDs against the target device to find the OIDs that the target device supports. This discovery process is the [meta-scan](#). If the sensor finds counters for the target device, the sensor settings open with a list of all available monitoring items. The list of SNMP table values sequentially presents row values to help you find the values you are interested in.

**i** You can also use the search to find the desired group or category. The search matches individual strings, so if your string has a space in it, put the search string in double quotation marks ("").

Select the counters that you want to monitor and click Save. PRTG creates sensors based on the OID types of the selected counters.

### Add Sensor Settings

Setting	Description
Library	The path to the <code>.oidlib</code> file that this sensor uses.

Setting	Description
Category	<p>Select the parameters that you want to monitor. The list is specific to your setup. The list contains all counters that are available in the <code>.oidlib</code> file that match the target device.</p> <p>Depending on the type of the selected entries, PRTG creates the following sensors:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">SNMP Custom Advanced</a><sup>[1896]</sup>: For up to 10 channels for 10 OIDs each. For example, 22 selected single values result in 3 sensors: 2 sensors with 10 channels and 1 sensor with 2 channels.</li> <li>▪ <a href="#">SNMP Custom String</a><sup>[1902]</sup>: For each selected entry that returns a string value.</li> <li>▪ <a href="#">SNMP Custom Table</a><sup>[1917]</sup>: For up to 10 channels for 10 columns per row. The channels represent the values in the columns of the same row.</li> </ul> <p><b>i</b> Once you create a custom SNMP sensor, you can create a <a href="#">device template</a> from it and prepare it for distribution. For example, you can refine the template with better name templates.</p>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ

**Priority** ⓘ

Example Name

---

exampletag ✕ +

---

★★★★☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- snmplibrarysensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Sensor Specific

The available sensor settings depend on the sensor that the SNMP Library sensor creates. For more information about settings, see the sections of these sensors:

- [SNMP Custom Advanced](#)<sup>[1898]</sup>
- [SNMP Custom String](#)<sup>[1904]</sup>

- [SNMP Custom Table](#) 

## Sensor Display




**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

- For more information, see section [Inheritance of Settings](#).

## Import MIB Files

✂ Additionally, you can create your own `.oidlib` files by importing the device manufacturers' MIB files with the free [MIB Importer](#) tool. You can convert your MIB files and save the `.oidlib` file results to the `\snmplibs` subfolder of the [PRTG program directory](#).

■ For more information about the MIB Importer, see the Knowledge Base: [How can I import my MIB files into PRTG?](#)

If the `.oidlib` files that you import contain [lookups](#) (you can see this in section [Lookup](#) in the MIB Importer), you can define your own sensor states for the values that the lookups return. Add an SNMP Library sensor with this `.oidlib` file. PRTG then creates a lookup definition file using the lookupname of the chosen library as id parameter.

ⓘ PRTG adds the lookups without status definitions, so the sensor shows the Warning [status](#) by default. You must edit the corresponding lookup files to get reliable alarms. Override the lookup definition with your own custom lookup. For more information, see section [Define Lookups](#).

☁ To import MIB files into PRTG Hosted Monitor, see section [Manage a PRTG Hosted Monitor Subscription](#).

## Default .oidlib Files Overview

PRTG comes with the following `.oidlib` files.

ⓘ The `.oidlib` files might not support all devices or parameters.

.oidlib File	Description
APC UPS.oidlib	Monitors uninterruptible power supplies (UPSs) from APC American Power Conversion Corp.
APCSensorstationlib.oidlib	Monitors alarm status, communication status, humidity, and temperature as shown by an APC sensor station.
Basic Linux Library (UCD-SNMP-MIB).oidlib	Monitors basic system parameters on Linux systems, such as memory, disk and swap, CPU, and more.
cisco-interfaces.oidlib	Monitors Cisco-specific parameters, for example, the number of present network interfaces on a system, several states of an interface (admin, oper, speed, type, errors, discards, etc.), and more.
cisco-queue.oidlib	Monitors queues on a Cisco interface, for example, queue depth and its maximum, discarded messages from the queue, the number of the queue within the queue set, and more.

.oidlib File	Description
Dell Storage Management.oidlib	Monitors Dell storage devices. Possible parameters include disk arrays, battery and power supply, fan and temperature, virtual disk, and more.
Dell Systems Management Instrumentation.oidlib	Monitors the hardware of Dell systems. Possible parameters include ACPower and battery, alerts, base board, BIOS, Baseboard Management Controller (BMC), chassis, COO, cooling, event log, firmware, integrated development environment (IDE), keyboard, memory, port, network, processor, Small Computer System Interface (SCSI), system, temperature, USB, universally unique identifier (UUID), and more.
HP LaserJet Status.oidlib	Monitors toner, paper, and jam status of an HP LaserJet printer.
Linux SNMP (AXBGP DisMan EtherLike Host).oidlib	Monitors different aspects of Linux systems.  ⓘ This file might detect a very large number of interfaces. It might take a few seconds until the selection table appears.
Linux SNMP (Framework Proxy Noti v2).oidlib	Monitors different aspects of Linux systems.  ⓘ This file might detect a very large number of interfaces. It might take a few seconds until the selection table appears.
Linux SNMP (IP Net SNMP Noti OSPF RMON SMUX).oidlib	Monitors different aspects of Linux systems.  ⓘ This file might detect a very large number of interfaces. It might take a few seconds until the selection table appears.
Linux SNMP (Source TCP UCD UDP).oidlib	Monitors different aspects of Linux systems.  ⓘ This file might detect a very large number of interfaces. It might take a few seconds until the selection table appears.
Paessler Common OID Library.oidlib	Monitors many common hardware devices. It is used for several sensors and is encrypted.
SNMP Informant std.oidlib	Monitors logical disks, processor, memory, and network interface on Windows systems.

## More

### ■ KNOWLEDGE BASE

How do SNMP, MIBs and OIDs work?

- <https://kb.paessler.com/en/topic/653>

How can I import my MIB files into PRTG?

- <https://kb.paessler.com/en/topic/733>

Can't find a sensor for my device in PRTG but I believe it supports SNMP. How to proceed?

- <https://kb.paessler.com/en/topic/65638>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

How can I monitor EMC Isilon storage systems with PRTG?

- <https://kb.paessler.com/en/topic/71413>

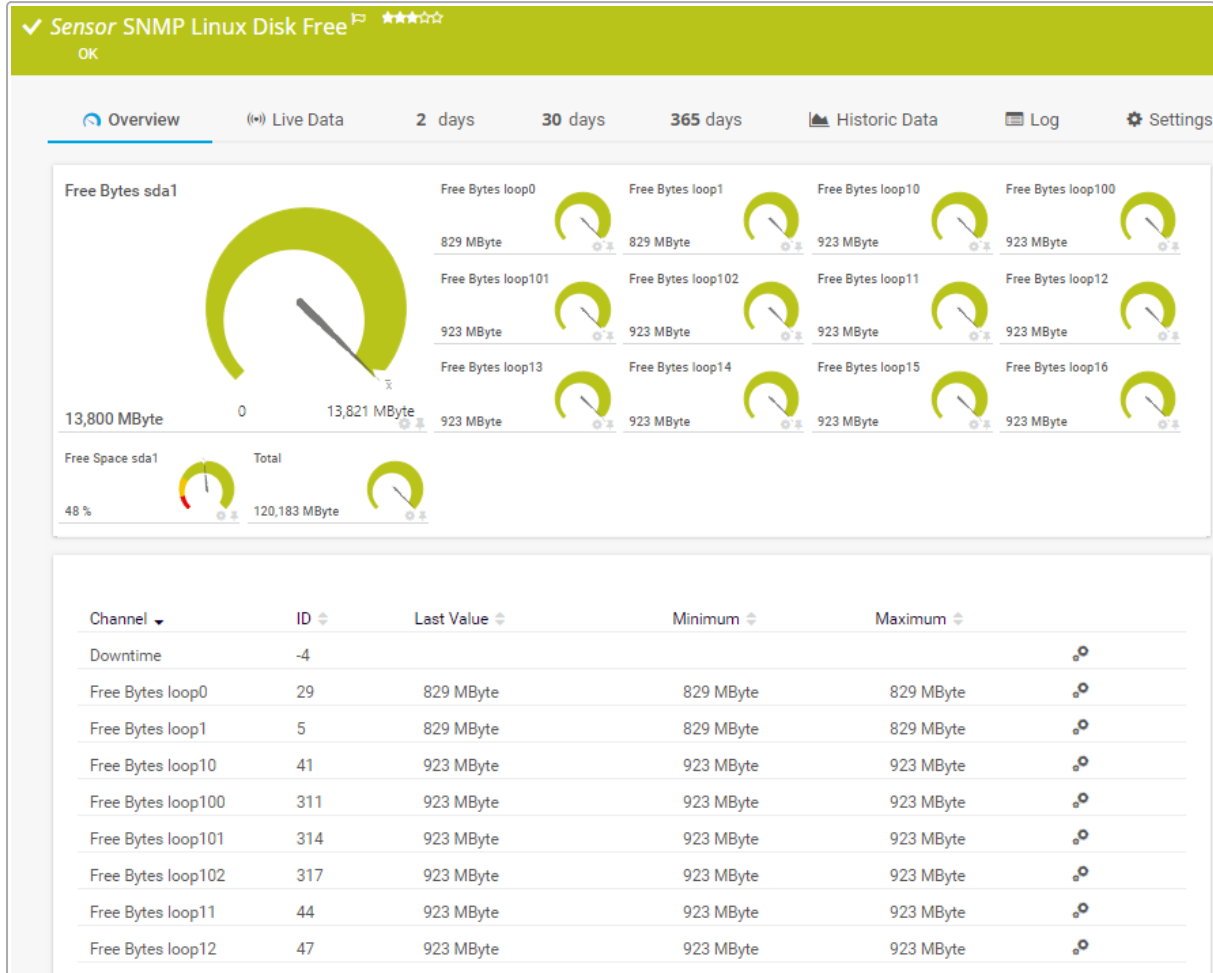
### ✂ PAESSLER TOOLS

MIB Importer

- <https://www.paessler.com/tools/mibimporter>

## 7.8.210 SNMP Linux Disk Free Sensor

The SNMP Linux Disk Free sensor monitors the free space on disks of a Linux/Unix system via the Simple Network Management Protocol (SNMP).



SNMP Linux Disk Free Sensor

The free space that this sensor returns shows the disk space that is not yet used. Not all of this space might be available for use because a part of this space might be reserved by the system, for example, for redundancy purposes. For more information, see the Knowledge Base: [Why do SSH Disk Free and SNMP Linux Disk Free show different values for my target Linux system?](#)

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Linux vrije schijf ruimte
- French: Linux espace disponible du disque (SNMP)
- German: SNMP Linux-Datenträgerspeicher
- Japanese: SNMP Linux ディスクの空き容量
- Portuguese: Disco livre Linux (SNMP)



- Russian: Свободное пространство диска в Linux по SNMP
- Simplified Chinese: SNMP Linux 磁盘可用空间
- Spanish: Espacio libre en disco Linux (SNMP)

## Remarks

Consider the following [remarks](#)<sup>2067</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">Why do SSH Disk Free and SNMP Linux Disk Free show different values for my target Linux system?</a></li> <li>▪ Knowledge Base: <a href="#">Monitoring Linux problem - SNMP port not reachable</a></li> </ul>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag × ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- diskspacesensor
- snmpdiskfreesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Set Limits Checked for ALL Disks

In this section, you can set limits that are valid for all channels and all drives. With limits, you can define when the sensor shows the Warning or Down [status](#), depending on the data provided by all drives that this sensor monitors. If you want to individually define limits for separate channels, use the limit settings in the [channel settings](#).

**i** All limits that you define here are valid in addition to the limits in the particular channel settings. The limits are valid simultaneously, so the first limit that is breached applies.

**Set Limits Checked For ALL Disks**

*Use the channel settings to set separate error limits or warning limits for each disk.*

Percentage Limit Check **i**  Only use the limits in the settings of the percentage channels  
 Use the limits of both the sensor and the channel settings (default)

Upper Error Limit **i** \_\_\_\_\_

Upper Warning Limit **i** \_\_\_\_\_

Lower Warning Limit **i** 25





Lower Error Limit **i** 10

Size Limit Check **i**  Only use the limits in the settings of the byte size channels (default)  
 Use the limits of both the sensor and the channel settings

Alarm on Missing/Removed Disk **i**  Deactivate alarm (default)  
 Activate alarm

Set Limits Checked for ALL Disks

Setting	Description
Percentage Limit Check	<p>By default, the sensor enables percentage limits with a lower warning limit and a lower error limit. Enable or disable a limit check for the free space in percentage channels of all drives:</p> <ul style="list-style-type: none"> <li>▪ Only use the limits in the settings of the percentage channels: Do not define sensor limits that are valid for all percentage channels. The sensor only uses the limits that you define in the settings of the particular "free space in percent" channels to determine the status.</li> <li>▪ Use the limits of both the sensor and the channel settings (default): Define sensor limits that are valid for all percentage channels. Additional fields appear below. The sensor shows the Warning or the Down status when free space limits are above or below the limits.</li> </ul>
Upper Error Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings (default) <b>above.</b></p> <p>Specify an upper limit in percent for the Down status. If the free disk space of one of your drives exceeds this value, the sensor changes to the Down status. Enter an integer or leave the field empty.</p> <p><b>i</b> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>

Setting	Description
Upper Warning Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings (default) <a href="#">above</a>.</p> <p>Specify an upper limit in percent for the Warning status. If the free disk space of one of your drives exceeds this value, the sensor changes to the Warning status. Enter an integer or leave the field empty.</p> <p> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Lower Warning Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings (default) <a href="#">above</a>.</p> <p>Specify a lower limit in percent for the Warning status. If the free disk space of one of your drives falls below this value, the sensor changes to the Warning status. Enter an integer or leave the field empty.</p> <p> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Lower Error Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings (default) <a href="#">above</a>.</p> <p>Specify a lower limit in percent for the Down status. If the free disk space of one of your drives falls below this value, the sensor changes to the Down status. Enter an integer or leave the field empty.</p> <p> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Size Limit Check	<p>Enable or disable a limit check for the free bytes channels of all drives:</p> <ul style="list-style-type: none"> <li>▪ Only use the limits in the settings of the byte size channels (default): Do not define sensor limits that are valid for all byte size channels. The sensor only uses limits that you define in the settings of the particular free space in bytes channels to determine the status.</li> <li>▪ Use the limits of both the sensor and the channel settings: Define limits for the sensor that are valid for all byte size channels. Additional fields appear below. The sensor shows the Warning or Down status when free space limits are above or below the value.</li> </ul> <p> By default, byte size limits are not enabled for drives.</p>

Setting	Description
Upper Error Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings <a href="#">above</a>.</p> <p>Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (the default unit is <b>MB</b>). If the free disk space of one of your drives exceeds this value, the sensor changes to the Down status. Enter an integer or leave the field empty.</p> <p><b>i</b> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Upper Warning Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings <a href="#">above</a>.</p> <p>Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (the default unit is <b>MB</b>). If the free disk space of one of your drives exceeds this value, the sensor changes to the Warning status. Enter an integer or leave the field empty.</p> <p><b>i</b> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Lower Warning Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings <a href="#">above</a>.</p> <p>Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (the default unit is <b>MB</b>). If the free disk space of one of your drives falls below this value, the sensor changes to the Warning status. Enter an integer or leave the field empty.</p> <p><b>i</b> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Lower Error Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings <a href="#">above</a>.</p> <p>Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (the default unit is <b>MB</b>). If the free disk space of one of your drives falls below this value, the sensor changes to the Down status. Enter an integer or leave the field empty.</p>

Setting	Description
	<p><b>i</b> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Alarm on Missing/Removed Disk	<p>If a monitored disk is removed or not found, the sensor sets the values to zero. Select the alarm approach in this case:</p> <ul style="list-style-type: none"> <li>▪ Deactivate alarm (default): Do not send an alert for a removed disk.</li> <li>▪ Activate alarm: Send an alert if a monitored disk is removed or not found.</li> </ul>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Bytes [ <a href="#">Partition</a> ]	The free space
Free INodes [ <a href="#">Partition</a> ]	The free index nodes (%)
Free Space [ <a href="#">Partition</a> ]	The free space (%)
Total	The free total disk space

## More

### ■ KNOWLEDGE BASE

Why do SSH Disk Free and SNMP Linux Disk Free show different values for my target Linux system?

- <https://kb.paessler.com/en/topic/43183>

Monitoring Linux problem - SNMP port not reachable

- <https://kb.paessler.com/en/topic/5353>

What security features does PRTG include?

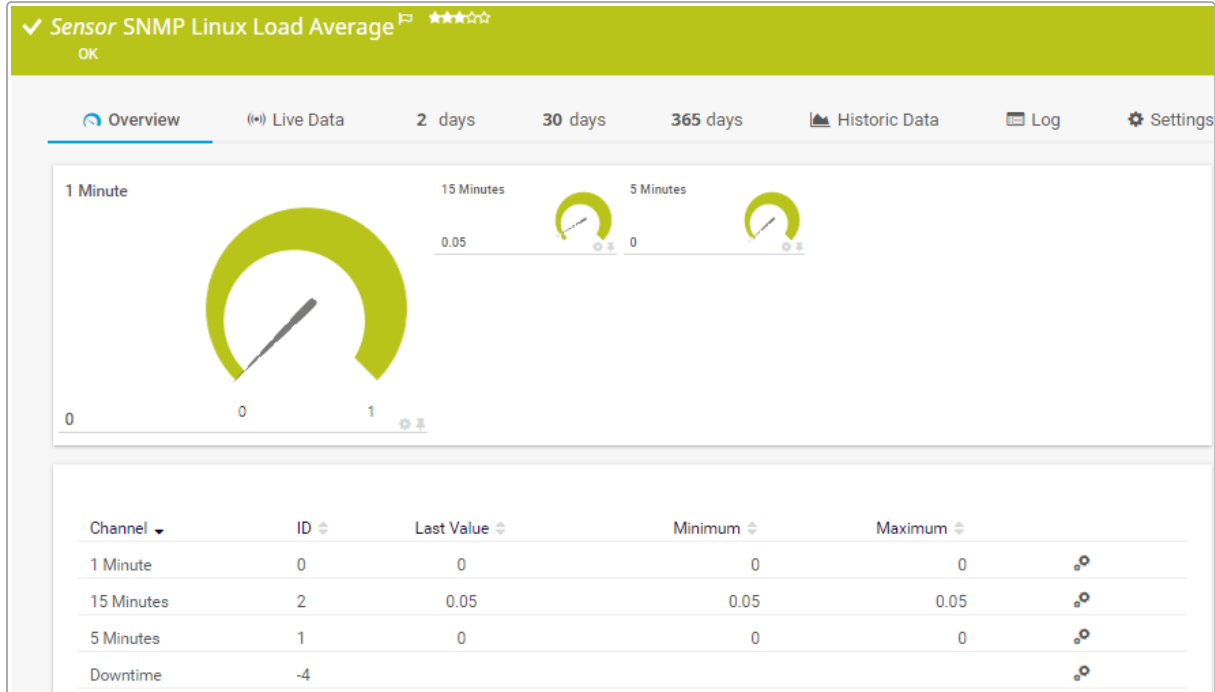
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.211 SNMP Linux Load Average Sensor

The SNMP Linux Load Average sensor monitors the system load average of a Linux/Unix system via the Simple Network Management Protocol (SNMP).



SNMP Linux Load Average Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2076]</sup>.

### Sensor in Other Languages

- Dutch: SNMP Linux Gemiddelde belasting
- French: Linux charge moyenne (SNMP)
- German: SNMP Linux Durchschnittliche Last
- Japanese: SNMP Linux の負荷平均
- Portuguese: Carga média Linux (SNMP)
- Russian: Средняя загрузка Linux по SNMP
- Simplified Chinese: SNMP Linux 负载平均值
- Spanish: Promedio de carga Linux (SNMP)

### Remarks

Consider the following [remarks](#)<sup>[2074]</sup> and requirements for this sensor:



Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Knowledge Base	Knowledge Base: <a href="#">Monitoring Linux problem - SNMP port not reachable</a>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- snmploadsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Display

#### Sensor Display

**Primary Channel** ⓘ Downtime

---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>

Setting	Description
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
1 Minute	<p>The average system load within a 1-minute interval</p> <p><b>i</b> This channel is the primary channel by default.</p>
5 Minutes	The average system load within a 5-minute scanning interval
15 Minutes	The average system load within a 15-minute interval
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

## More

### ■ KNOWLEDGE BASE

Monitoring Linux problem - SNMP port not reachable

- <https://kb.paessler.com/en/topic/5353>

What security features does PRTG include?

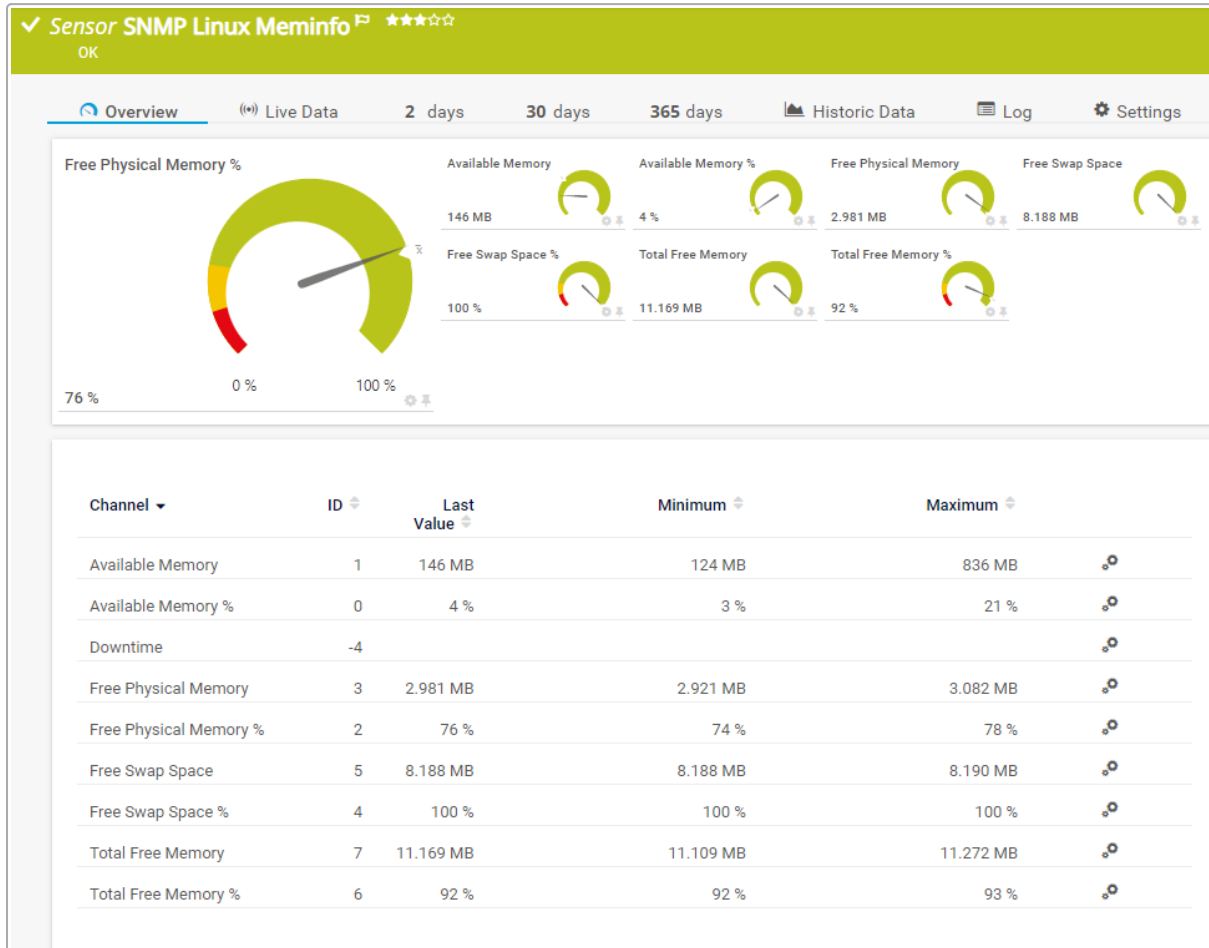
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.212 SNMP Linux Meminfo Sensor

The SNMP Linux Meminfo sensor monitors the memory usage of a Linux/Unix system via the Simple Network Management Protocol (SNMP).



SNMP Linux Meminfo Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Linux meminfo
- French: Linux information mémoire (SNMP)
- German: SNMP Linux Speicherinfo
- Japanese: SNMP Linux メモリ情報
- Portuguese: Meminfo Linux (SNMP)
- Russian: Linux Meminfo no SNMP
- Simplified Chinese: SNMP Linux 内存信息
- Spanish: Meminfo Linux (SNMP)

## Remarks

Consider the following [remarks](#) <sup>[2079]</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Knowledge Base	Knowledge Base: <a href="#">Monitoring Linux problem - SNMP port not reachable</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ ★★★★☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- memorysensor
- snmpmeminfosensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>[667]</sup>.


## Sensor Display

### Sensor Display


**Primary Channel** ⓘ


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Available Memory	The available memory
Available Memory %	The available memory (%)

Channel	Description
	<p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: 5%</li> <li>▪ Lower warning limit: 10%</li> </ul>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Physical Memory	The free physical memory
Free Physical Memory %	<p>The free physical memory (%)</p> <p><b>i</b> This channel is the primary channel by default.</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: 10%</li> <li>▪ Lower warning limit: 20%</li> </ul>
Free Swap Space	The free swap memory
Free Swap Space %	<p>The free swap memory (%)</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: 10%</li> <li>▪ Lower warning limit: 20%</li> </ul>
Total Free Memory	The total free memory (physical memory plus swap)
Total Free Memory %	<p>The total free memory (%) (physical memory plus swap)</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: 10%</li> <li>▪ Lower warning limit: 20%</li> </ul>

## More

### ■ KNOWLEDGE BASE

Monitoring Linux problem - SNMP port not reachable

- <https://kb.paessler.com/en/topic/5353>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

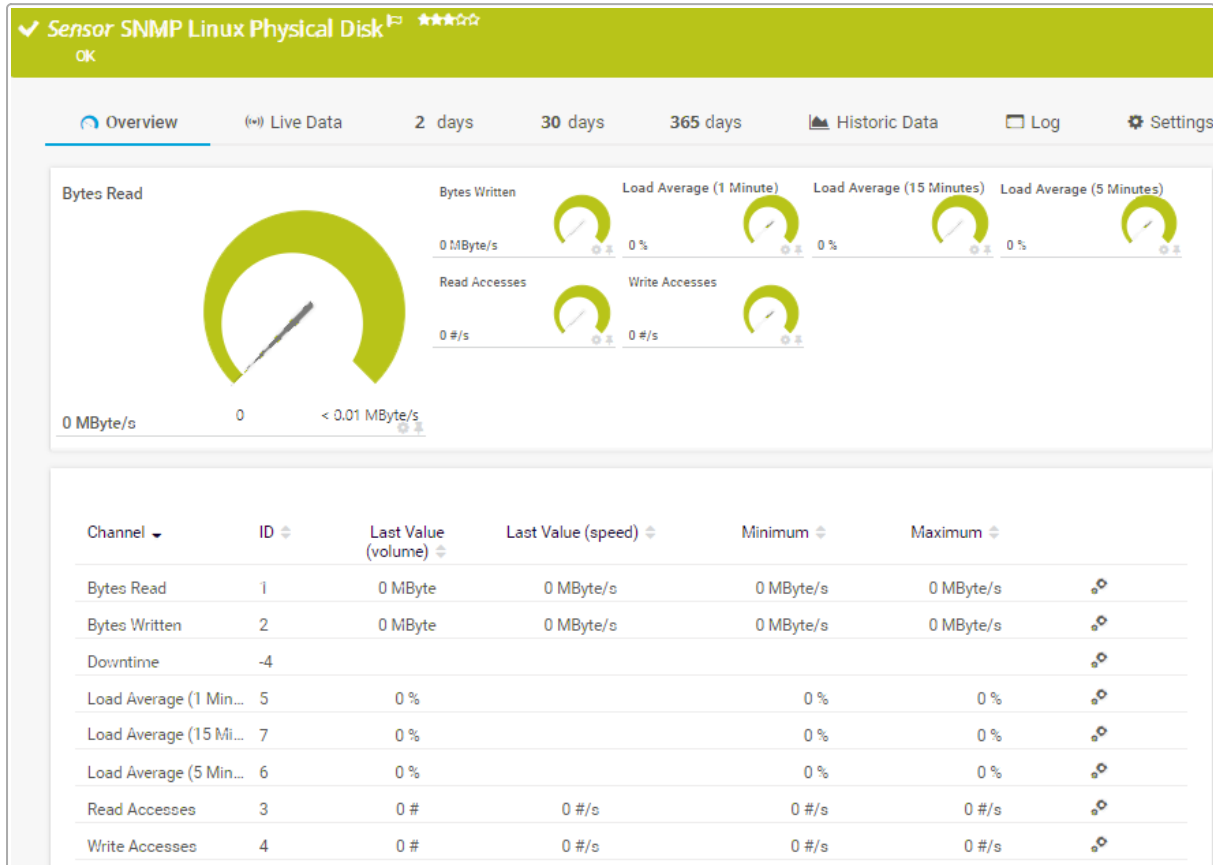
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>



## 7.8.213 SNMP Linux Physical Disk Sensor

The SNMP Linux Physical Disk sensor monitors the input/output (I/O) on disks of a Linux/Unix system via the Simple Network Management Protocol (SNMP).



SNMP Linux Physical Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Linux Fysieke Schijf
- French: Linux disque physique (SNMP)
- German: SNMP Linux Physikalischer Datenträger
- Japanese: SNMP Linux 物理ディスクを監視する
- Portuguese: Disco físico Linux (SNMP)
- Russian: Физический диск Linux по SNMP
- Simplified Chinese: SNMP Linux 物理磁盘
- Spanish: Disco físico Linux (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
Knowledge Base	Knowledge Base: <a href="#">Monitoring Linux problem - SNMP port not reachable</a>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- physicaldisk
- snmpphysicaldisksensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Physical Disk Settings

#### Physical Disk Settings

**Disk** ⓘ *loop0*

---

**BitMask** ⓘ 2

Physical Disk Settings

Setting	Description
Disk	The physical disk that this sensor monitors.
BitMask	The bitmask that might be necessary for bug tracking purposes.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Bytes Read	The number of bytes read <b>i</b> This channel is the primary channel by default.
Bytes Written	The number of bytes written
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Load Average (1 Minute)	The load average (1 minute) (%)
Load Average (5 Minutes)	The load average (5 minutes) (%)
Load Average (15 Minutes)	The load average (15 minutes) (%)
Read Accesses	The number of read accesses
Write Accesses	The number of write accesses

## More

### ■ KNOWLEDGE BASE

Monitoring Linux problem - SNMP port not reachable

- <https://kb.paessler.com/en/topic/5353>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

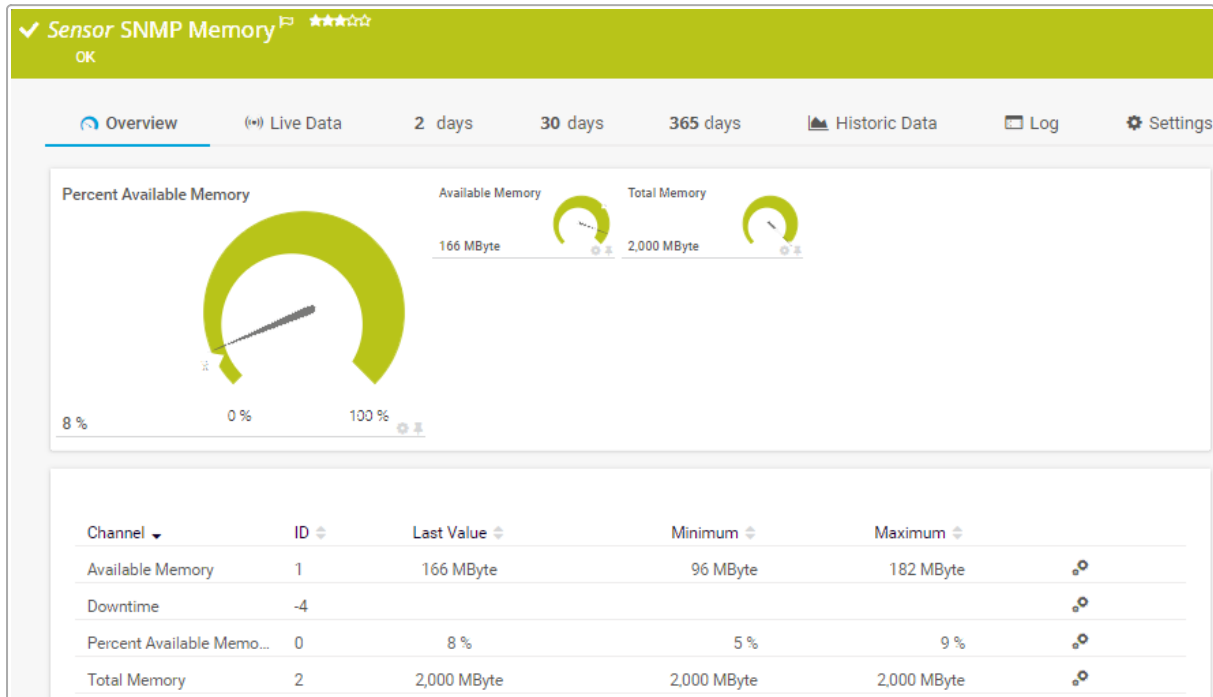
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.214 SNMP Memory Sensor

The SNMP Memory sensor monitors the memory usage of a system via the Simple Network Management Protocol (SNMP).

**i** This sensor uses more generic object identifier (OID) values in comparison to the [SNMP Linux Meminfo<sub>\[2078\]</sub>](#) sensor.



SNMP Memory Sensor

■ For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List<sub>\[2089\]</sub>](#).

### Sensor in Other Languages

- Dutch: SNMP Geheugen
- French: Mémoire (SNMP)
- German: SNMP Speicher
- Japanese: SNMP メモリ
- Portuguese: Memória (SNMP)
- Russian: Память по SNMP
- Simplified Chinese: SNMP 内存
- Spanish: Memoria (SNMP)

### Remarks

Consider the following [remarks<sub>\[2087\]</sub>](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
Localhost	It might not work to query data from a probe device via SNMP (querying <a href="#">localhost</a> , <a href="#">127.0.0.1</a> , or <a href="#">::1</a> ). <a href="#">Add this device</a> with the IP address that it has in your network and create the sensor on this device instead.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- memory
- memorysensor
- snmp
- snmpmemorysensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Memory Settings

#### Memory Settings

**Memory Type** ⓘ *Virtual Memory*

Memory Settings

Setting	Description
Memory Type	The type of memory that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Available Memory	The available memory
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Percent Available Memory	The available memory (%) <b>i</b> This channel is the primary channel by default.
Total Memory	The total memory

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

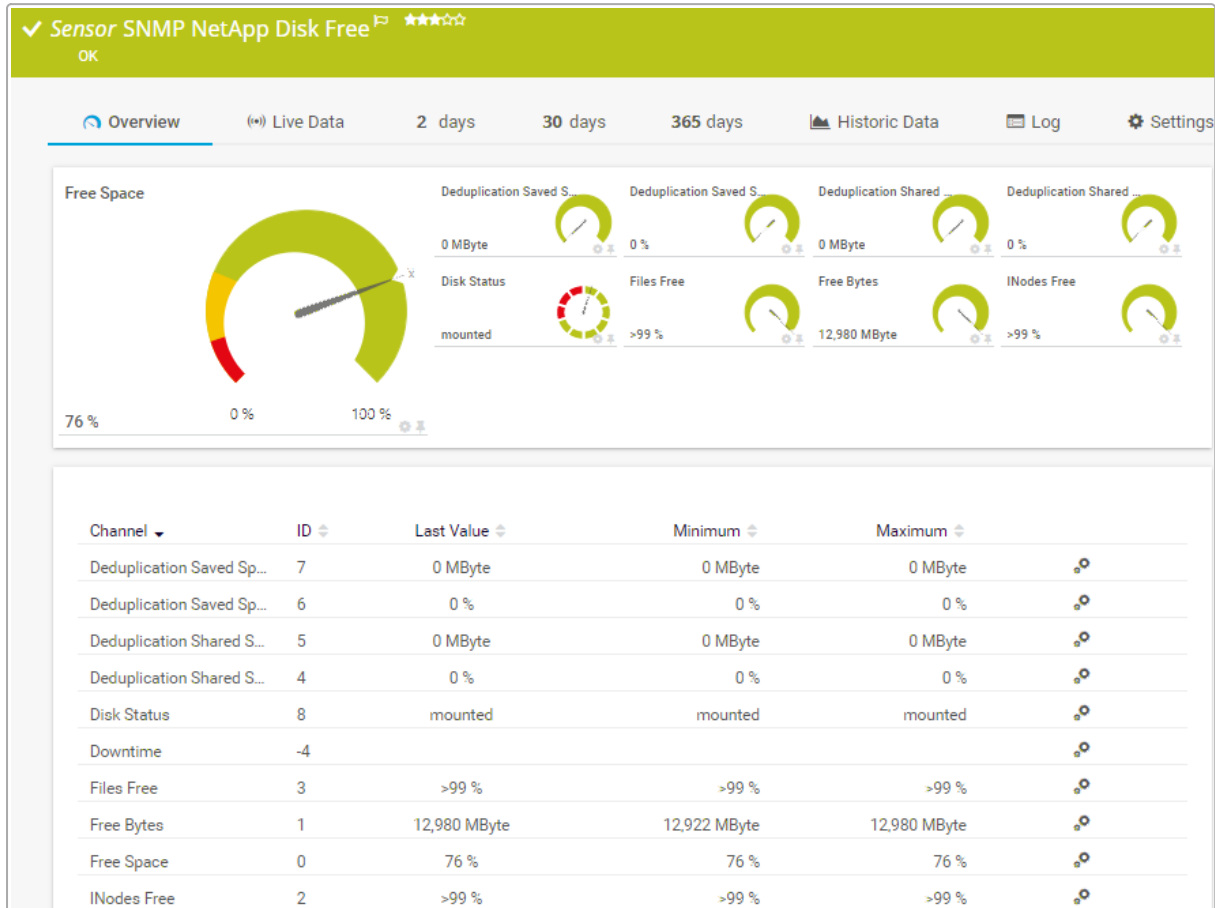
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>



## 7.8.215 SNMP NetApp Disk Free Sensor

The SNMP NetApp Disk Free sensor monitors the free space on disks of a NetApp storage system via the Simple Network Management Protocol (SNMP).



SNMP NetApp Disk Free Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP NetApp Schijf Vrije Ruimte
- French: NetApp espace disponible du disque (SNMP)
- German: SNMP NetApp-Datenträgerspeicher
- Japanese: SNMP NetApp 空きディスク
- Portuguese: Disco livre NetApp (SNMP)
- Russian: Свободное пространство диска NetApp по SNMP
- Simplified Chinese: SNMP NetApp 磁盘可用空间
- Spanish: Espacio libre en disco NetApp (SNMP)

## Remarks

Consider the following [remarks](#)<sup>2092</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Knowledge Base	Knowledge Base: <a href="#">How can I monitor capacity and used disk space on a NetApp?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

Example Name

**Tags** ⓘ

exampletag ✕ +

**Priority** ⓘ

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- netapp
- snmpdiskfreesensor
- snmpnetapp
- snmpnetappdiskfreesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## NetApp Disk Free Settings

### NetApp Disk Free Settings

**File System** ⓘ
AGGR\_01\_SAS

**Virtual Disk** ⓘ

NetApp Disk Free Settings

Setting	Description
File System	The name of the disk that this sensor monitors.
Virtual Disk	The name of the virtual disk that this sensor monitors (if applicable).

## Sensor Display

### Sensor Display

**Primary Channel** ⓘ
Downtime

**Graph Type** ⓘ


Show channels independently (default)
  Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other above.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Deduplication Saved Space	The deduplication saved space
Deduplication Saved Space %	The deduplication saved space (%)
Deduplication Shared Space	The deduplication shared space
Deduplication Shared Space %	The deduplication shared space (%)
Disk Status	<p>The disk status</p> <ul style="list-style-type: none"> <li>▪ Up status: Creating, Mounted, Mounting, Nofsinfo, Replayed, Replaying, Unmounting</li> <li>▪ Down status: Destroying, Frozen, Unmounted</li> </ul>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Files Free	The free files (%)
Free Bytes	The free space
Free Space	<p>The free space (%)</p> <p><b>i</b> This channel is the primary channel by default.</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: 10%</li> <li>▪ Lower warning limit: 25%</li> </ul>
INodes Free	The free index nodes (%)

## More

### ■ KNOWLEDGE BASE

How can I monitor capacity and used disk space on a NetApp?

- <https://kb.paessler.com/en/topic/61231>

What security features does PRTG include?

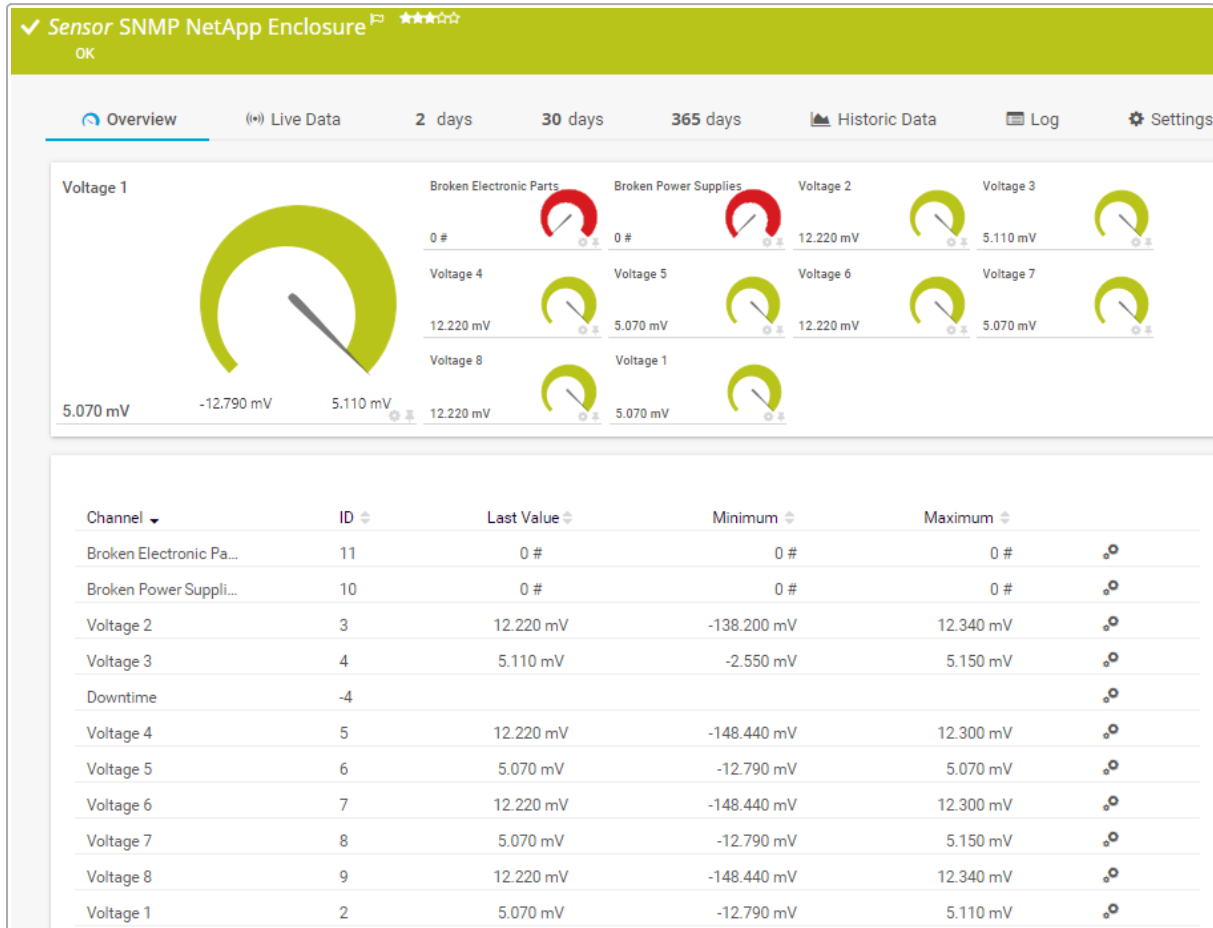
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.216 SNMP NetApp Enclosure Sensor

The SNMP NetApp Enclosure sensor monitors the power supply and cooling of an enclosure that is part of a NetApp storage system via the Simple Network Management Protocol (SNMP).



SNMP NetApp Enclosure Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP NetApp Behuizing
- French: NetApp boîtier (SNMP)
- German: SNMP NetApp Enclosure
- Japanese: SNMP NetApp エンクロージャ
- Portuguese: Gabinete NetApp (SNMP)
- Russian: Корпус NetApp по SNMP
- Simplified Chinese: SNMP NetApp 机箱
- Spanish: Gabinete NetApp (SNMP)

## Remarks

Consider the following [remarks](#)<sup>[2097]</sup> and requirements for this sensor:

Remark	Description
NetApp versions	This sensor only supports NetApp versions up to 8.2.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- netapp
- snmpnetapp
- snmpnetappenclosuresensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## NetApp Enclosure Settings

### NetApp Enclosure Settings

**Enclosure** ⓘ 1A2B3C4D5E

---

**Measurement** ⓘ Currents

NetApp Enclosure Settings

Setting	Description
Enclosure	The identifier of the enclosure that this sensor monitors.
Measurement	The type of measurement that this sensor monitors.

### NetApp Specific

**NetApp Specific**

N/A Measurement Handling ⓘ  Set sensor to down status (default)  
 Interpret as valid

NetApp Specific

Setting	Description
N/A Measurement Handling	<p>Define the sensor behavior if the requested NetApp value is not available (N/A values):</p> <ul style="list-style-type: none"> <li>Set sensor to down status (default): Set the sensor to the Down <a href="#">status</a> if a measurement is not available. <ul style="list-style-type: none"> <li>ⓘ We recommend that you use this setting to not miss any hardware errors.</li> </ul> </li> <li>Interpret as valid: Handle unavailable measurements as valid sensor results to keep the sensor in the Up status. <ul style="list-style-type: none"> <li>ⓘ This might be useful, for example, if a hardware sensor on the NetApp is disabled for some reason but actually there is no hardware error. If the NetApp returns an N/A measurement, the sensor interprets this as 0. <ul style="list-style-type: none"> <li>ⓘ We recommend that you use the lookup file <code>prtg.standardlookups.netapp.notavailable.ovl</code> for channels with unavailable measurements if you select this option. This replaces 0 with the message <a href="#">Not Available</a>. Open the <a href="#">settings</a> of the affected channels and select this file in section Lookup. For more information, see section <a href="#">Define Lookups</a>.</li> </ul> </li> </ul> </li> </ul>

### Sensor Display


**Sensor Display**

Primary Channel ⓘ Downtime


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display



Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Broken Electronic Parts	The number of broken electronic parts
Broken Power Supplies	The number of broken power supplies

Channel	Description
Current [#]	The current
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Fan [#]	The fan RPM
Fans Failed	The number of failed fans
Voltage [#]	The voltage

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

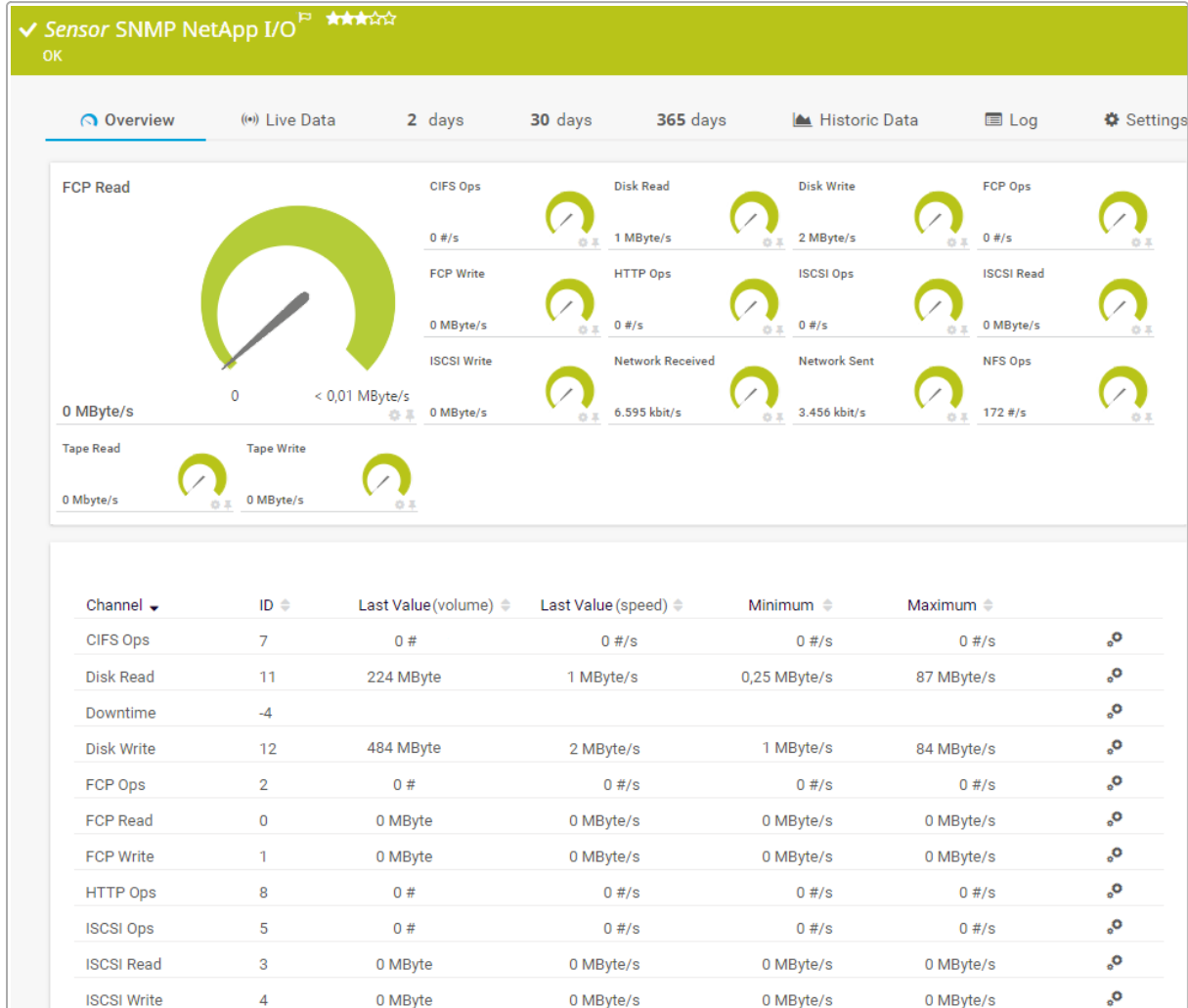
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.217 SNMP NetApp I/O Sensor

The SNMP NetApp I/O sensor monitors the input/output operations per second (IOPS) on a NetApp storage system via the Simple Network Management Protocol (SNMP).



SNMP NetApp I/O Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP NetApp I/O
- French: NetApp E/S (SNMP)
- German: SNMP NetApp E/A
- Japanese: SNMP NetApp I/O
- Portuguese: E/S NetApp (SNMP)
- Russian: Ввод-вывод NetApp по SNMP
- Simplified Chinese: SNMP NetApp I/O

- Spanish: E/S NetApp (SNMP)

## Remarks

Consider the following [remarks](#)<sup>[2102]</sup> and requirements for this sensor:

Remark	Description
NetApp versions	This sensor only supports NetApp versions up to 8.2.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
NetApp I/O	If you use NetApp cDOT 8.3 or NetApp ONTAP as of version 9.0, we recommend that you use the <a href="#">NetApp I/O</a> <sup>[1378]</sup> sensor.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- netapp
- snmpnetapp
- snmpnetappiosensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Sensor Display


### Sensor Display

**Primary Channel** ⓘ Downtime


---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CIFS Ops	The number of CIFS operations
Disk Read	The disk read speed

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Disk Write	The disk write speed
FCP Ops	The number of FCP operations
FCP Read	The FCP read speed  This channel is the primary channel by default.
FCP Write	The FCP write speed
HTTP Ops	The number of HTTP operations
iSCSI Ops	The number of iSCSI operations
iSCSI Read	The iSCSI read speed
iSCSI Write	The iSCSI read speed
Network Received	The number of bytes received
Network Sent	The number of bytes sent
NFS Ops	The number of NFS operations
Tape Read	The tape read speed
Tape Write	The tape write speed

## More

### KNOWLEDGE BASE

What security features does PRTG include?

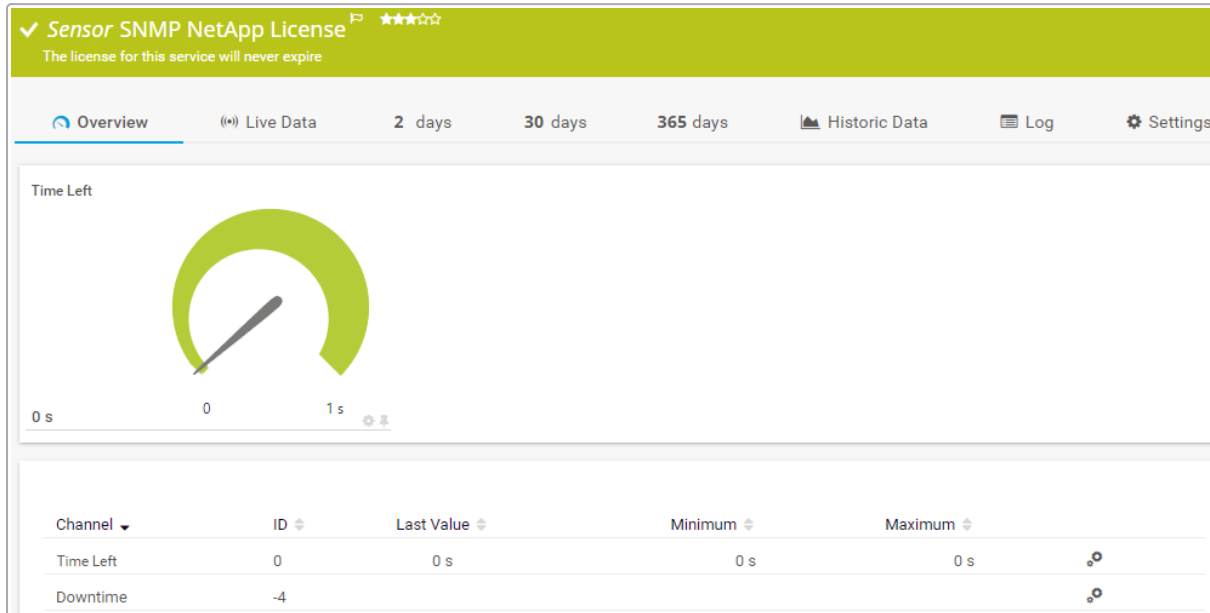
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.218 SNMP NetApp License Sensor

The SNMP NetApp License sensor monitors the licenses for the services of a NetApp storage system via the Simple Network Management Protocol (SNMP).



SNMP NetApp License Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2107]</sup>.

### Sensor in Other Languages

- Dutch: SNMP NetApp licentie
- French: NetApp Licence (SNMP)
- German: SNMP NetApp Lizenz
- Japanese: SNMP NetApp ライセンス
- Portuguese: Licença NetApp (SNMP)
- Russian: Лицензия NetApp по SNMP
- Simplified Chinese: SNMP NetApp 许可证
- Spanish: Licencia NetApp (SNMP)

### Remarks

Consider the following [remarks](#)<sup>[2105]</sup> and requirements for this sensor:

Remark	Description
NetApp versions	This sensor only supports NetApp versions up to 8.2.

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- netapp
- snmpnetapp
- snmpnetapplicenseselector

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### NetApp License Settings

#### NetApp License Settings

**License for Service** ⓘ *SnapMirror License*

NetApp License Settings

Setting	Description
License for Service	The name of the license whose service this sensor monitors.



## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Time Left	The time until the license for a service expires  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

What security features does PRTG include?

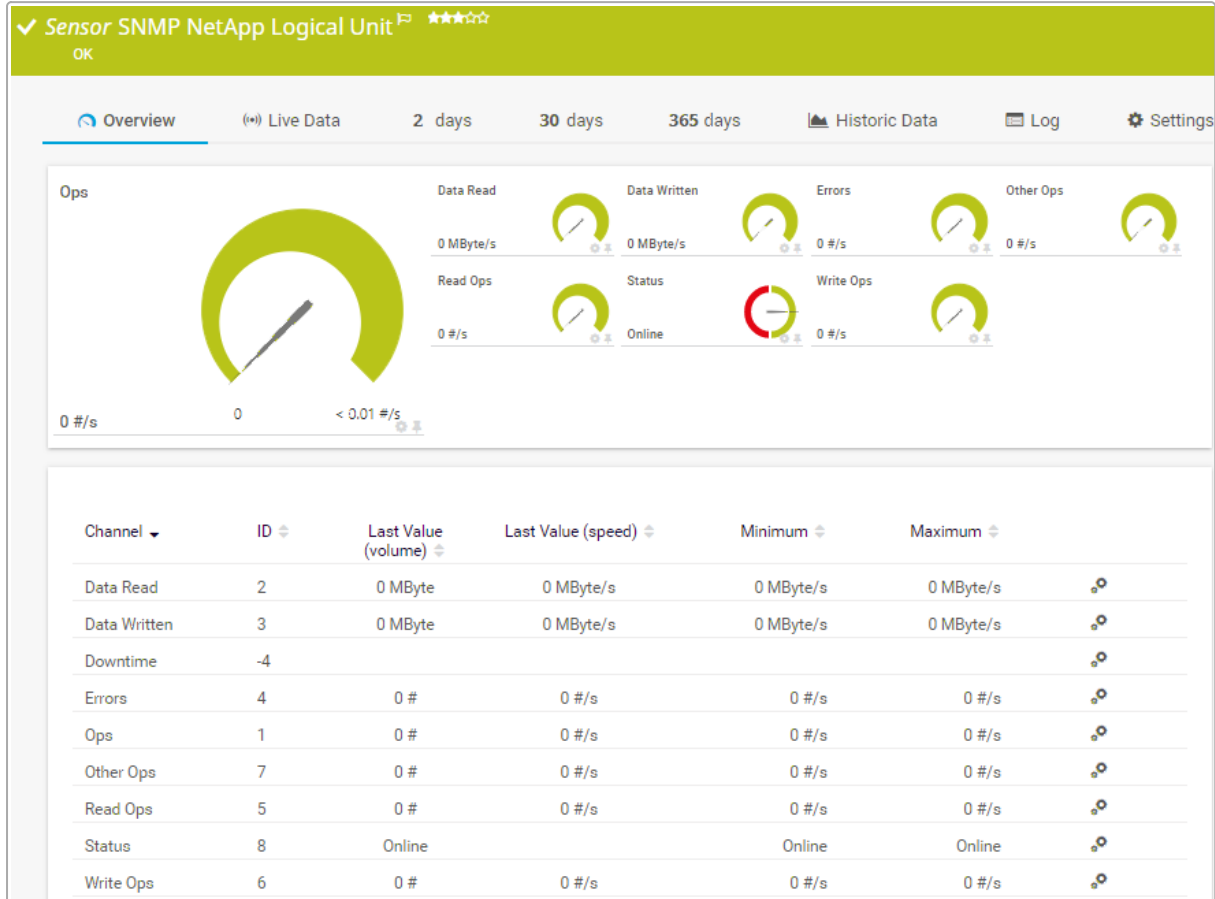
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.219 SNMP NetApp Logical Unit Sensor

The SNMP NetApp Logical Unit sensor monitors the input/output operations per second (IOPS) on a logical unit of a NetApp storage system via the Simple Network Management Protocol (SNMP).



SNMP NetApp Logical Unit Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2112]</sup>.

### Sensor in Other Languages

- Dutch: SNMP NetApp Logical Unit
- French: NetApp unité logique (SNMP)
- German: SNMP NetApp Logische Einheit
- Japanese: SNMP NetApp 論理ユニット
- Portuguese: Unidade lógica NetApp (SNMP)
- Russian: Логический блок NetApp по SNMP
- Simplified Chinese: SNMP NetApp 逻辑单元
- Spanish: Unidad lógica NetApp (SNMP)

## Remarks

Consider the following [remarks](#)<sup>[2110]</sup> and requirements for this sensor:

Remark	Description
NetApp versions	This sensor only supports NetApp versions up to 8.2.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
NetApp LUN	If you use NetApp cDOT 8.3 or NetApp ONTAP as of version 9.0, we recommend that you use the <a href="#">NetApp LUN</a> <sup>[1403]</sup> sensor.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

Example Name

**Tags** ⓘ

exampletag
 ✕
+

**Priority** ⓘ

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- netapp
- snmpdiskfreesensor
- snmpnetapp
- snmpnetappdiskfreesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## NetApp Logical Unit Settings

**NetApp Logical Unit Settings**

**Logical Unit** ⓘ /vol/vo\_mysql\_I0/mysql\_I0/mysql\_I0.lun

**Alignment Monitoring** ⓘ Do not check alignment (default)

**Volume** ⓘ mysql\_I0

**Comment** ⓘ

NetApp Logical Unit Settings

Setting	Description
Logical Unit	The name of the logical unit that this sensor monitors.
Alignment Monitoring	Select if the sensor checks the alignment of the logical unit: <ul style="list-style-type: none"> <li>Do not check alignment (default)</li> <li>Check alignment (if available)</li> </ul> <p> ⓘ You cannot change this value after sensor creation.</p>
Volume	The volume that this sensor monitors.
Comment	Comments for the logical unit that this sensor monitors.

## Sensor Display


**Sensor Display**

**Primary Channel** ⓘ Downtime


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.

Setting	Description
	<p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.           <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Data Read	The data read speed
Data Written	The data write speed
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Errors	The number of errors
Ops	The total number of operations <span>ⓘ</span> This channel is the primary channel by default.
Other Ops	The number of other operations
Read Ops	The number of disk read operations
Status	The logical unit status <ul style="list-style-type: none"> <li>▪ Up status: Online</li> <li>▪ Down status: Offline</li> </ul>
Write Ops	The number of disk write operations

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

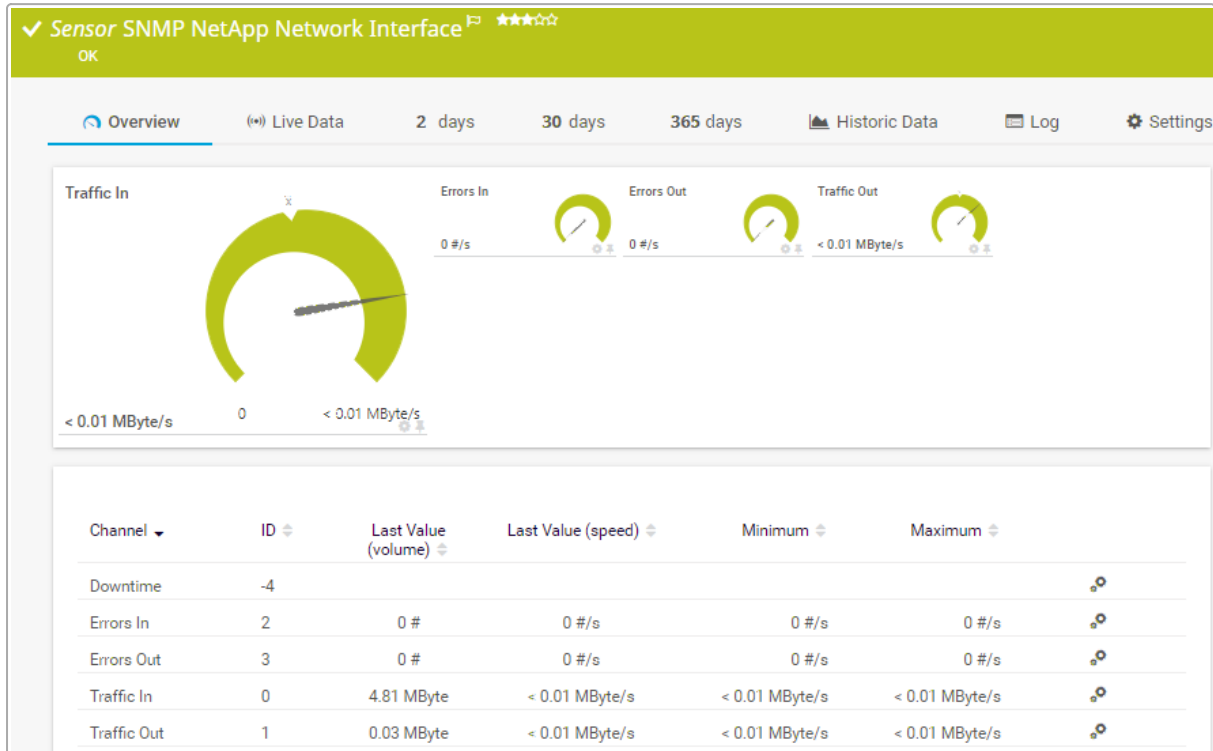
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.220 SNMP NetApp Network Interface Sensor

The SNMP NetApp Network Interface sensor monitors a network card of a NetApp storage system via the Simple Network Management Protocol (SNMP).



SNMP NetApp Network Interface Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP NetApp Network Interface
- French: NetApp interface réseau (SNMP)
- German: SNMP NetApp Netzwerkschnittstelle
- Japanese: SNMP NetApp ネットワークインターフェース
- Portuguese: Interface de rede NetApp (SNMP)
- Russian: Сетевой интерфейс NetApp по SNMP
- Simplified Chinese: SNMP NetApp 网络接口
- Spanish: Interfaz de red NetApp (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:



Remark	Description
NetApp versions	This sensor only supports NetApp versions up to 8.2.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.
NetApp NIC	If you use NetApp cDOT 8.3 or NetApp ONTAP as of version 9.0, we recommend that you use the <a href="#">NetApp NIC</a> <sup>1418</sup> sensor.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- netapp
- snmpnetapp
- snmpnetappnetworkinterfacesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### NetApp Network Interface Settings

#### NetApp Network Interface Settings

**Network Interface** ⓘ netapp01

NetApp Network Interface Settings

Setting	Description
Network Interface	The name of the network interface that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Errors In	The number of incoming errors
Errors Out	The number of outgoing errors
Traffic In	The incoming traffic <span>ⓘ</span> This channel is the primary channel by default.
Traffic Out	The outgoing traffic

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

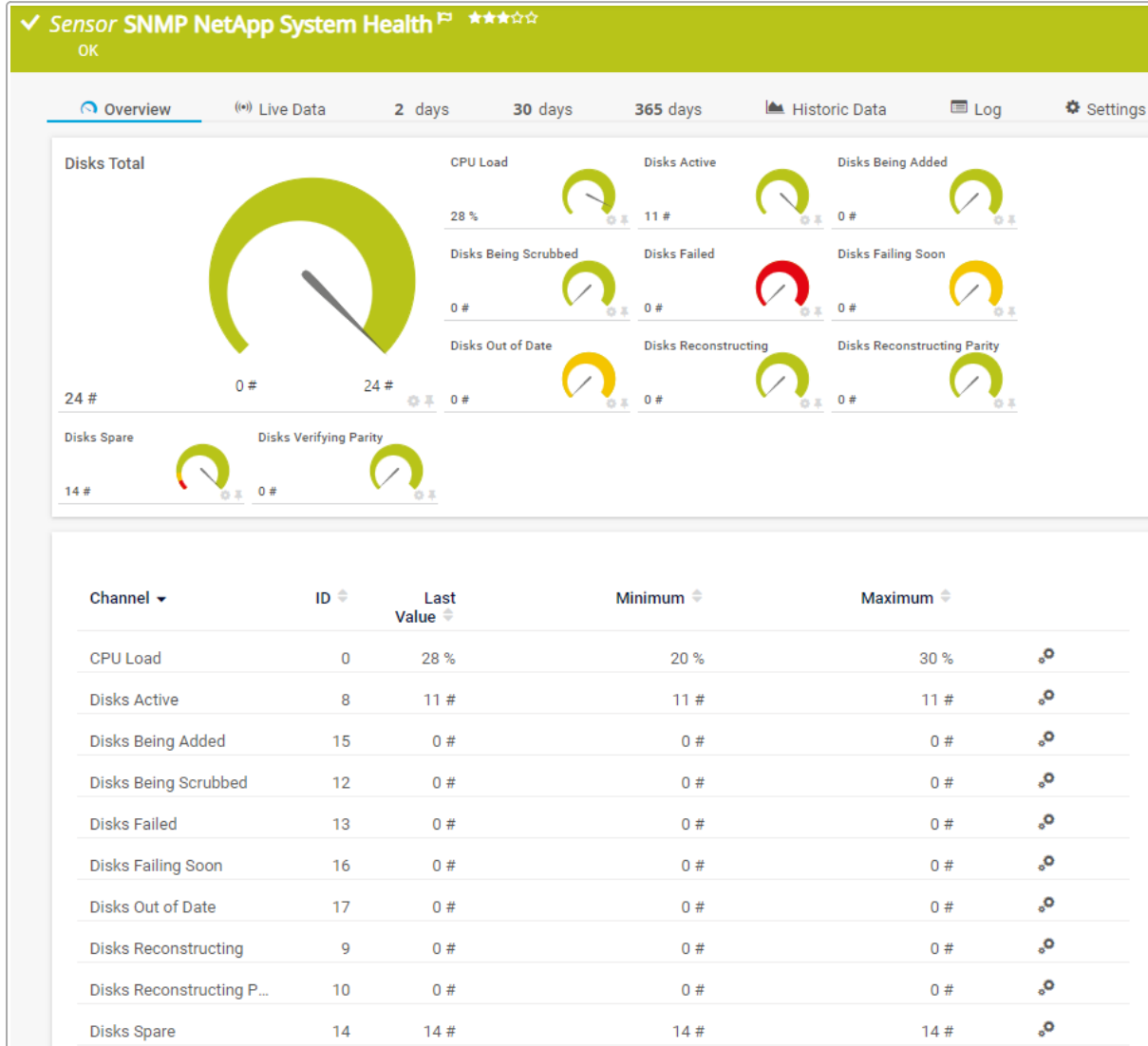
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.221 SNMP NetApp System Health Sensor

The SNMP NetApp System Health sensor monitors the status of a NetApp storage system via the Simple Network Management Protocol (SNMP).



SNMP NetApp System Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2120]</sup>.

### Sensor in Other Languages

- Dutch: SNMP NetApp Systemstatus
- French: NetApp état du système (SNMP)
- German: SNMP NetApp Systemzustand
- Japanese: SNMP NetApp システム正 常 性
- Portuguese: Saúde do sistema NetApp (SNMP)
- Russian: Работоспособность системы NetApp по SNMP

- Simplified Chinese: SNMP NetApp 系统健康状况
- Spanish: Salud de sistema NetApp (SNMP)

## Remarks

Consider the following [remarks](#)<sup>[2119]</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
NetApp System Health	If you use NetApp cDOT 8.3 or NetApp ONTAP as of version 9.0 or later, we recommend that you use the <a href="#">NetApp System Health</a> <sup>[1457]</sup> sensor.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- netapp
- snmpnetapp
- snmpnetappsystemhealthsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CPU Load	The CPU load (%)
Disks Active	The number of active disks
Disks Being Added	The number of disks being added
Disks Being Scrubbed	The number of disks being scrubbed
Disks Failed	The number of failed disks ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper error limit: 0</li> </ul>
Disks Failing Soon	The number of disks that will fail soon ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper error limit: 0</li> </ul>
Disks Out Of Date	The number of disks that are out of date ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper error limit: 0</li> </ul>
Disks Reconstructing	The number of disks that are reconstructing
Disks Reconstructing Parity	The number of disks that are reconstructing parity
Disks Spare	The number of spare disks ⓘ This channel has default limits: <ul style="list-style-type: none"> <li>▪ Lower error limit 1</li> <li>▪ Lower warning limit: 2</li> </ul>
Disks Total	The total number of disks ⓘ This channel is the primary channel by default.
Disks Verifying Parity	The number of disks that are verifying parity
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

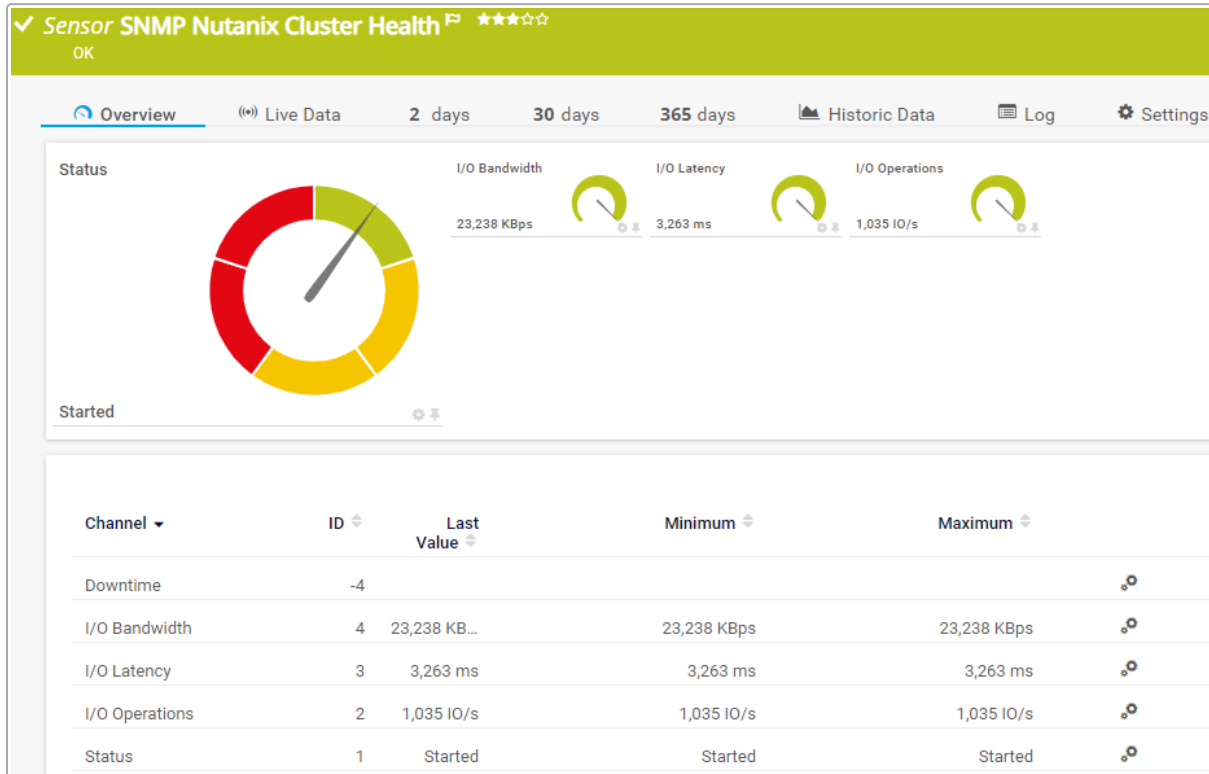
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>



## 7.8.222 SNMP Nutanix Cluster Health Sensor

The SNMP Nutanix Cluster Health sensor monitors the status and the performance of a Nutanix cluster via the Simple Network Management Protocol (SNMP).



SNMP Nutanix Cluster Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2127]</sup>.

### Sensor in Other Languages

- Dutch: SNMP Nutanix Cluster Health
- French: Nutanix état de cluster (SNMP)
- German: SNMP Nutanix Clusterzustand
- Japanese: SNMP Nutanix クラスターの正常性
- Portuguese: Funcionamento do cluster Nutanix (SNMP)
- Russian: Работоспособность кластера SNMP Nutanix
- Simplified Chinese: SNMP Nutanix 群集运行状况
- Spanish: Salud de clúster Nutanix (SNMP)

### Remarks

Consider the following [remarks](#)<sup>[2123]</sup> and requirements for this sensor:

Remark	Description
SNMP v3	Nutanix devices only support <a href="#">SNMP v3</a> . Make sure that you select SNMP v3 in the <a href="#">credentials for SNMP devices</a> settings of the parent device.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- nutanix
- snmp
- snmpnutanixclusterhealthsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## System Specific

**System Specific**

Measurement ⓘ *ntxCluster*

Sensor Version ⓘ 2

Identifier ⓘ

OID Index ⓘ

System Specific

Setting	Description
Measurement	The type of measurement that this sensor monitors.
Sensor Version	The version of the sensor definition that was used to create this sensor.
Identifier	The value that the sensor uses to find the component in the OID table.
OID Index	The OID table index that this sensor uses.

## Debug Options

**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].Data.txt and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul>

Setting	Description
	<p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
I/O Bandwidth	The bandwidth of I/O operations
I/O Latency	The latency of I/O operations
I/O Operations	The number of I/O operations
Status	<p>The Nutanix cluster status</p> <ul style="list-style-type: none"> <li>▪ Up status: Started</li> <li>▪ Warning status: Starting, Stopping</li> <li>▪ Down status: Stopped, Unknown</li> </ul> <p> This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

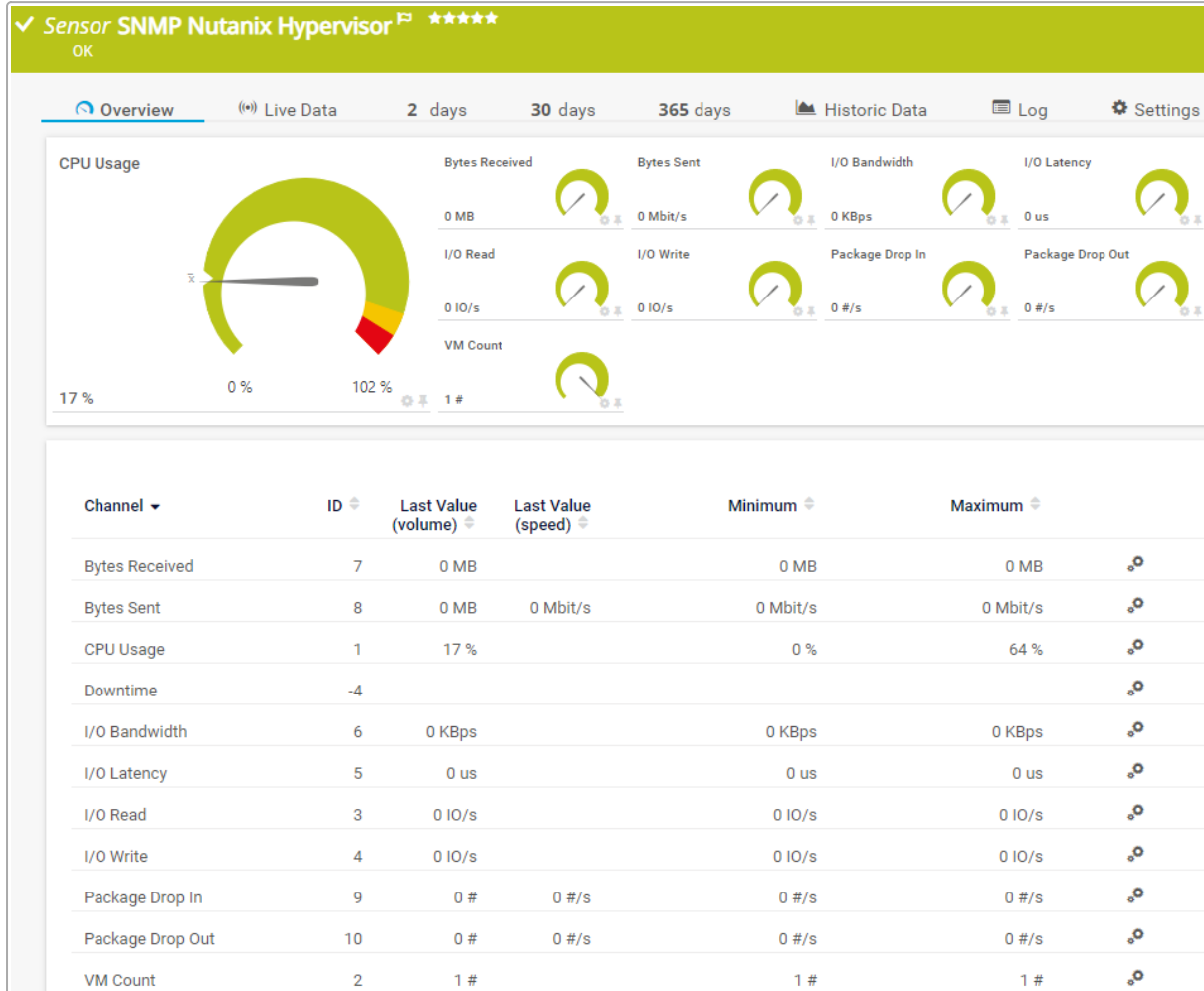
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.223 SNMP Nutanix Hypervisor Sensor

The SNMP Nutanix Hypervisor sensor monitors a Nutanix hypervisor via the Simple Network Management Protocol (SNMP).



SNMP Nutanix Hypervisor Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2132]</sup>.

### Sensor in Other Languages

- Dutch: SNMP Nutanix Hypervisor
- French: Nutanix hyperiseur (SNMP)
- German: SNMP Nutanix Hypervisor
- Japanese: SNMP Nutanix ハイパーバイザー
- Portuguese: Hipervisor Nutanix (SNMP)
- Russian: Гипервизор SNMP Nutanix
- Simplified Chinese: SNMP Nutanix 虚拟机监控程序
- Spanish: Hipervisor Nutanix (SNMP)

## Remarks

Consider the following [remarks](#)<sup>[2129]</sup> and requirements for this sensor:

Remark	Description
SNMP v3	Nutanix devices only support <a href="#">SNMP v3</a> . Make sure that you select SNMP v3 in the <a href="#">credentials for SNMP devices</a> settings of the parent device.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- nutanix
- snmp
- snmpnutanixhypervisorsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## System Specific

### System Specific

<b>Measurement</b> ⓘ	<i>ntxHypervisor</i>
<b>Sensor Version</b> ⓘ	2
<b>Identifier</b> ⓘ	0123_4567
<b>OID Index</b> ⓘ	1

System Specific

Setting	Description
Measurement	The type of measurement that this sensor monitors.
Sensor Version	The version of the sensor definition that was used to create this sensor.
Identifier	The value that the sensor uses to find the component in the OID table.
OID Index	The OID table index that this sensor uses.

## Debug Options

### Debug Options

<b>Result Handling</b> ⓘ	<input checked="" type="radio"/> Discard result (default) <input type="radio"/> Store result
--------------------------	---

Debug Options

Setting	Description
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].Data.txt and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul>



Setting	Description
	<p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Bytes Received	The number of bytes received
Bytes Sent	The number of bytes sent
CPU Usage	The CPU usage  This channel is the primary channel by default.
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
I/O Bandwidth	The bandwidth of I/O operations
I/O Latency	The latency of I/O operations
I/O Read	The read speed of I/O operations
I/O Write	The write speed of I/O operations
Package Drop In	The number of dropped incoming packages
Package Drop Out	The number of dropped outgoing packages
VM Count	The number of VMs

## More

■ KNOWLEDGE BASE

What security features does PRTG include?

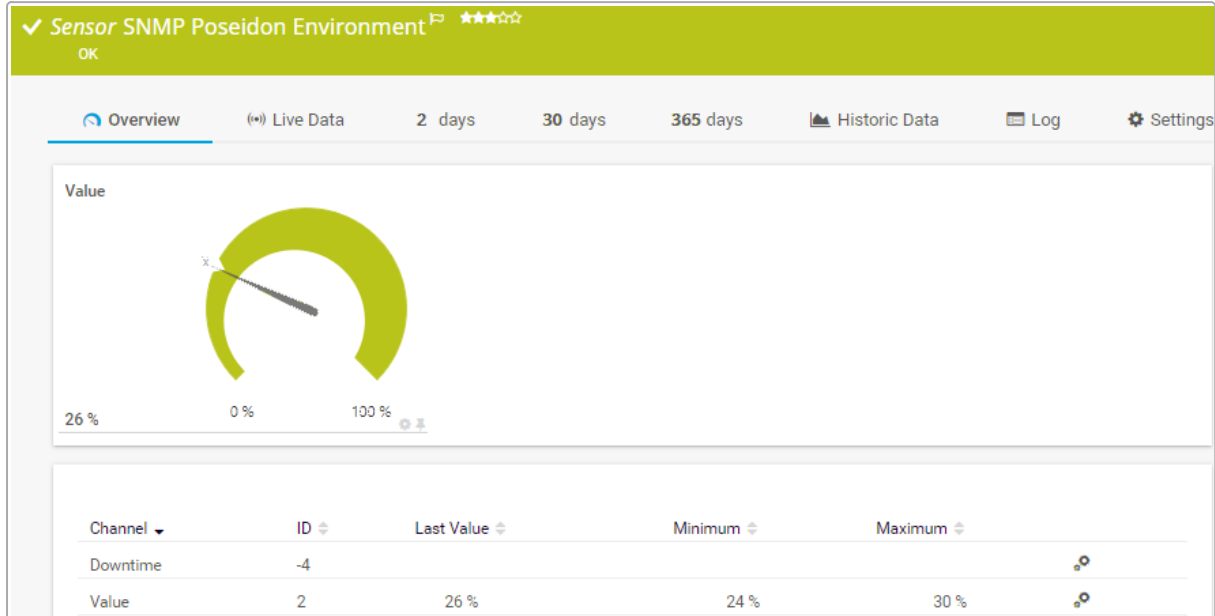
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.224 SNMP Poseidon Environment Sensor

The SNMP Poseidon Environment sensor monitors performance counters for environmental measurements on Poseidon hardware via the Simple Network Management Protocol (SNMP).



SNMP Poseidon Environment Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Poseidon Omgeving
- French: Poseidon environnement (SNMP)
- German: SNMP Poseidon-Umgebung
- Japanese: SNMP Poseidon 環境
- Portuguese: Ambiente Poseidon (SNMP)
- Russian: Окружающая среда Poseidon по SNMP
- Simplified Chinese: SNMP Poseidon 环境
- Spanish: Entorno Poseidon (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.

Remark	Description
Performance impact	This sensor has a <b>very low</b> performance impact.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- apcups

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Poseidon Environment Specific

#### Poseidon Environment Specific

**Name** ⓘ Humidity

---

**Unit** ⓘ Percent

---

**Measuring Point** ⓘ 14963

Poseidon Environment Specific

Setting	Description
Name	The name of the measurement that this sensor monitors.
Unit	The unit of the value measurement that this sensor monitors.
Measuring Point	The measuring points that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	The humidity (%) or the temperature

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

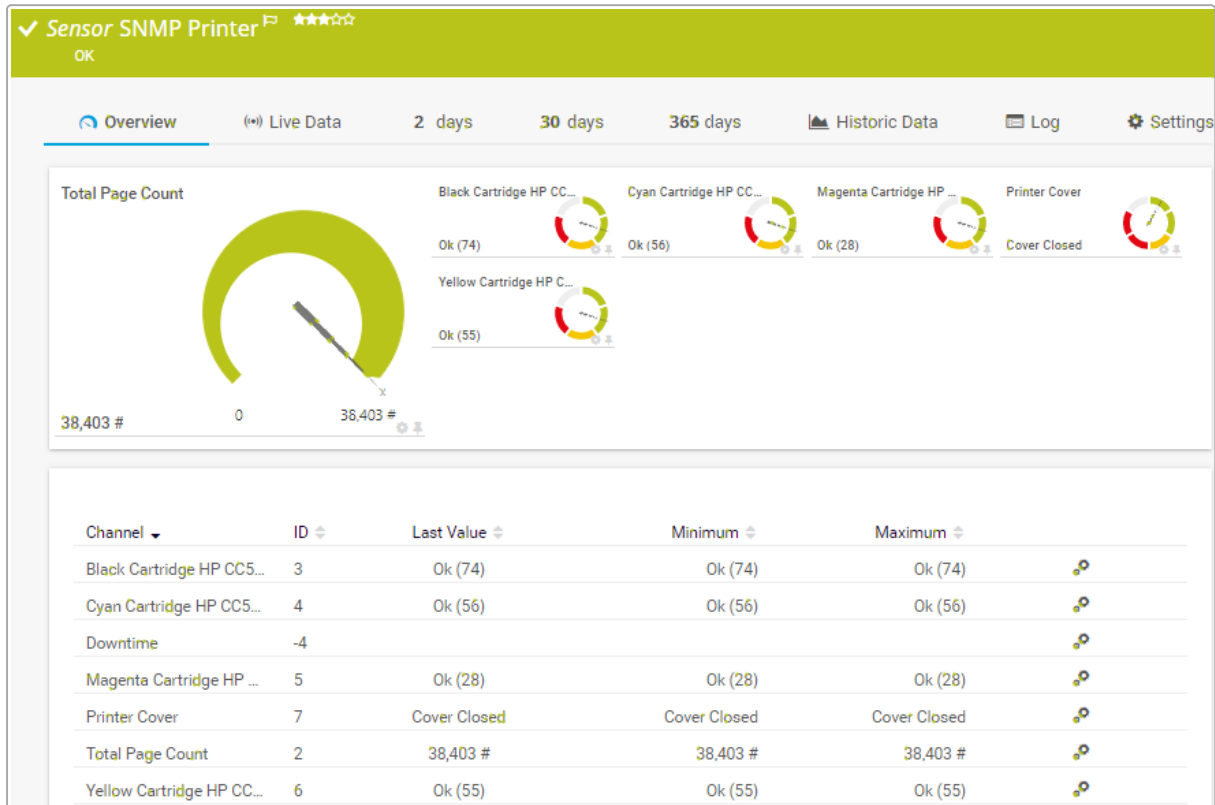
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.225 SNMP Printer Sensor

The SNMP Printer sensor monitors various types of printers via the Simple Network Management Protocol (SNMP).

- ① The sensor supports the following printers, among others: [HP OfficeJet](#) printers, [HP LaserJet](#) printers, [RICOH SP 5200](#), [SP 3410](#), [SP C242DN](#), [MP C3003](#), and [MP C2503](#).
- ① The sensor also shows the printer status as the sensor message.



SNMP Printer Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[214]</sup>.

### Sensor in Other Languages

- Dutch: SNMP Printer
- French: Imprimante (SNMP)
- German: SNMP Drucker
- Japanese: SNMP プリンター
- Portuguese: Impressora (SNMP)
- Russian: Принтер по SNMP
- Simplified Chinese: SNMP 打印机
- Spanish: Impresora (SNMP)



## Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Printers	This sensor supports the following printers, among others: <a href="#">HP OfficeJet printers</a> , <a href="#">HP LaserJet printers</a> , <a href="#">RICOH SP 5200</a> , <a href="#">SP 3410</a> , <a href="#">SP C242DN</a> , <a href="#">MP C3003</a> , and <a href="#">MP C2503</a> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Channels	We recommend that you do not rename channels of the sensor. Renaming a channel creates a new empty channel.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- printer
- snmp

For more information about basic sensor settings, see section [Sensor Settings](#).

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Black Cartridge [ <a href="#">Printer</a> ]	<p>The cartridge fill level</p> <ul style="list-style-type: none"> <li>▪ Up status: No Restriction, Not Empty, Ok</li> <li>▪ Warning status: Low</li> <li>▪ Down status: Critical</li> <li>▪ Unknown status: Unknown</li> </ul>
Cyan Cartridge [ <a href="#">Printer</a> ]	<p>The cartridge fill level</p> <ul style="list-style-type: none"> <li>▪ Up status: No Restriction, Not Empty, Ok</li> <li>▪ Warning status: Low</li> <li>▪ Down status: Critical</li> <li>▪ Unknown status: Unknown</li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Magenta Cartridge [ <a href="#">Printer</a> ]	<p>The cartridge fill level</p> <ul style="list-style-type: none"> <li>▪ Up status: No Restriction, Not Empty, Ok</li> <li>▪ Warning status: Low</li> <li>▪ Down status: Critical</li> <li>▪ Unknown status: Unknown</li> </ul>
Printer Cover	<p>The printer cover status</p> <ul style="list-style-type: none"> <li>▪ Up status: Cover Closed, Interlock Closed</li> <li>▪ Warning status: Other</li> <li>▪ Down status: Cover Open, Interlock Open</li> <li>▪ Unknown status: Unknown</li> </ul>
Total Page Count	<p>The total number of printed pages</p> <p> This channel is the primary channel by default.</p>
Yellow Cartridge [ <a href="#">Printer</a> ]	<p>The cartridge fill level</p> <ul style="list-style-type: none"> <li>▪ Up status: No Restriction, Not Empty, Ok</li> <li>▪ Warning status: Low</li> <li>▪ Down status: Critical</li> </ul>

Channel	Description
	<ul style="list-style-type: none"><li data-bbox="488 376 823 409">▪ Unknown status: Unknown</li></ul>

## More

### KNOWLEDGE BASE

What security features does PRTG include?

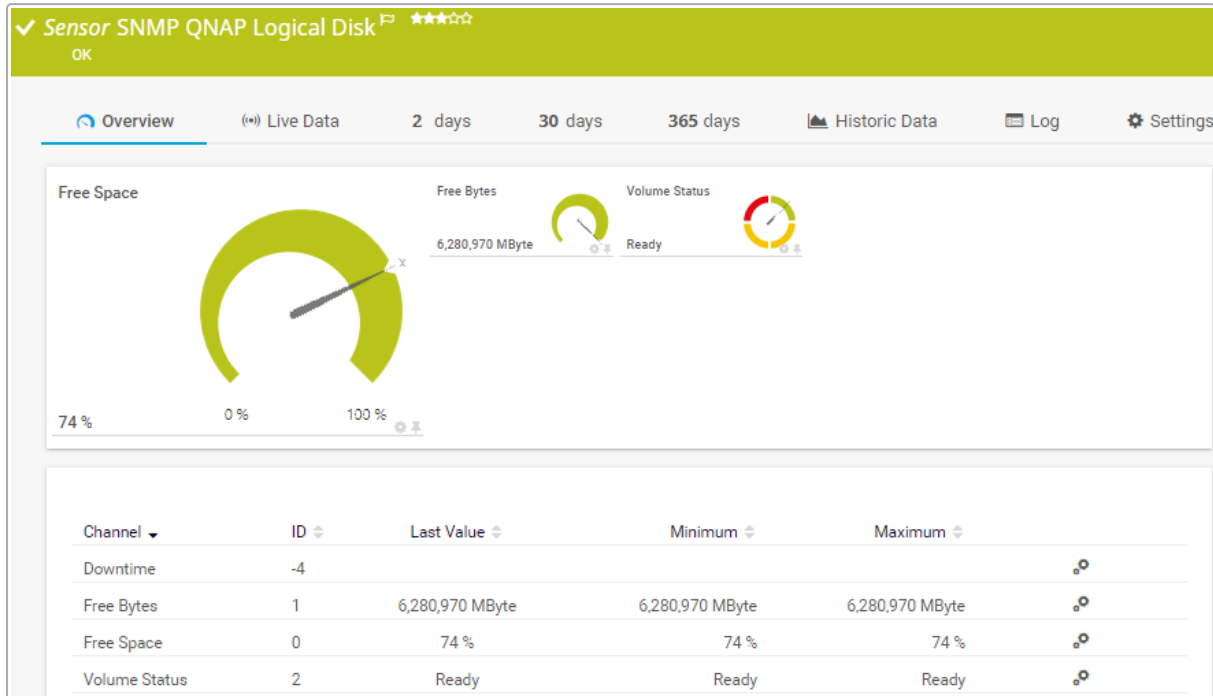
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.226 SNMP QNAP Logical Disk Sensor

The SNMP QNAP Logical Disk sensor monitors a logical disk in a Quality Network Appliance Provider (QNAP) network-attached storage (NAS) via the Simple Network Management Protocol (SNMP).



SNMP QNAP Logical Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2146]</sup>.

### Sensor in Other Languages

- Dutch: SNMP QNAP Logische Schijf
- French: QNAP disque logique (SNMP)
- German: SNMP QNAP Logischer Datenträger
- Japanese: SNMP QNAP 論理ディスク
- Portuguese: Disco lógico QNAP (SNMP)
- Russian: Логический диск QNAP по SNMP
- Simplified Chinese: SNMP QNAP 逻辑磁盘
- Spanish: Disco lógico QNAP (SNMP)

### Remarks

Consider the following [remarks](#)<sup>[2143]</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- logicaldisk
- qnap
- snmpqnap

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### QNAP NAS Settings

#### QNAP NAS Settings

**Disk** ⓘ 1

---

**Description** ⓘ [RAID5 Disk Volume: Host Drive: 1 2 3 4]

---

**File System** ⓘ EXT4

QNAP NAS Settings

Setting	Description
Disk	The logical disk that this sensor monitors.
Description	The name of the disk that this sensor monitors.
File System	The file system of the disk that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display


Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Bytes	The free space
Free Space	The free space (%)  This channel is the primary channel by default.
Volume Status	The volume status <ul style="list-style-type: none"> <li>▪ Up status: Ready</li> <li>▪ Warning status: In Degraded Mode, Rebuilding, Synchronizing</li> <li>▪ Down status: Failure</li> </ul>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Why do I get DoS alarms on my QNAP?

- <https://kb.paessler.com/en/topic/80421>

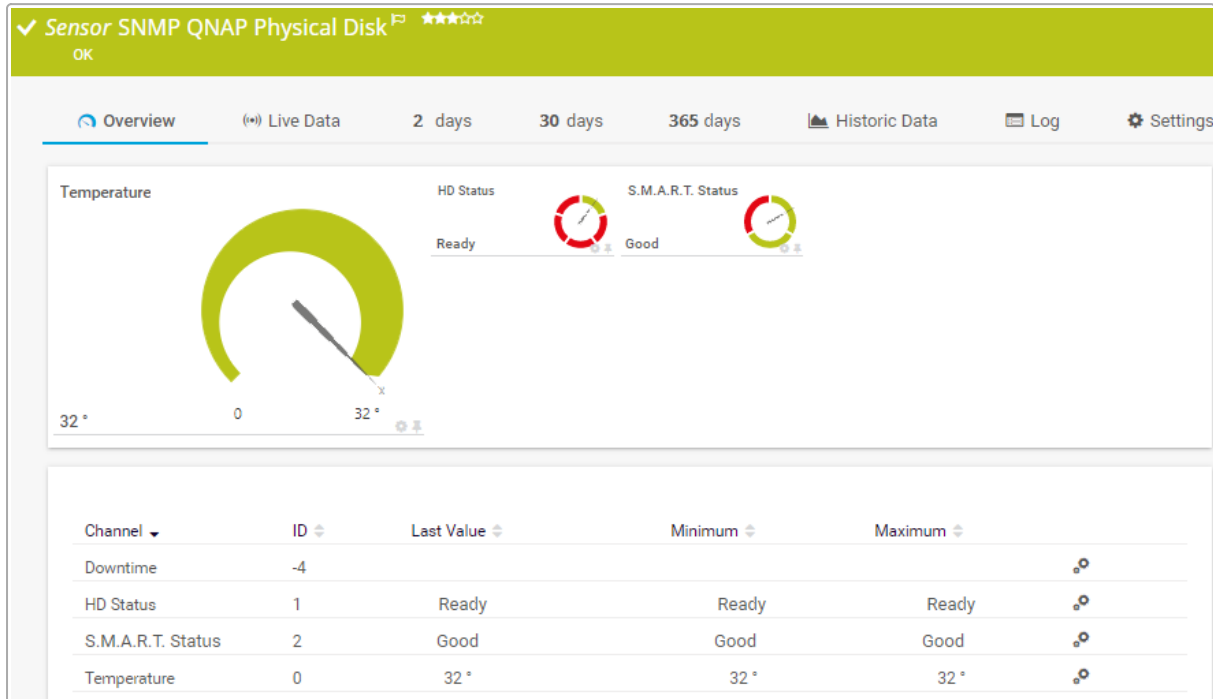
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>



## 7.8.227 SNMP QNAP Physical Disk Sensor

The SNMP QNAP Physical Disk sensor monitors a physical disk in a Quality Network Appliance Provider (QNAP) network-attached storage (NAS) via the Simple Network Management Protocol (SNMP).



SNMP QNAP Physical Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2150]</sup>.

### Sensor in Other Languages

- Dutch: SNMP QNAP Fysieke Schijf
- French: QNAP disque physique (SNMP)
- German: SNMP QNAP Physikalischer Datenträger
- Japanese: SNMP QNAP 物理ディスク
- Portuguese: Disco físico QNAP (SNMP)
- Russian: Физический диск QNAP по SNMP
- Simplified Chinese: SNMP QNAP 物理磁盘
- Spanish: Disco físico QNAP (SNMP)

### Remarks

Consider the following [remarks](#)<sup>[2147]</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- physicaldisk
- qnap
- snmpqnap

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### QNAP NAS Settings

#### QNAP NAS Settings

**Disk** ⓘ 1

---

**Description** ⓘ HDD1

---

**Model** ⓘ ABCD1234-5678EFGH

---

**Capacity** ⓘ 2.73 TB

---

**Unit** ⓘ Celsius

QNAP NAS Settings

Setting	Description
Disk	The physical disk that this sensor monitors.
Description	Information about the physical disk that this sensor monitors.
Model	The model of the physical disk that this sensor monitors.
Capacity	The capacity of the physical disk that this sensor monitors.
Unit	The unit of temperature measurement.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other above.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
HD Status	The disk status <ul style="list-style-type: none"> <li>▪ Up status: Ready</li> <li>▪ Down status: Invalid, No Disk, RwError, Unknown</li> </ul>
S.M.A.R.T. Status	The S.M.A.R.T. status <ul style="list-style-type: none"> <li>▪ Up status: Good, Normal</li> <li>▪ Down status: Bad</li> </ul>
Temperature	The temperature <p> This channel is the primary channel by default.</p>

## More

■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Why do I get DoS alarms on my QNAP?

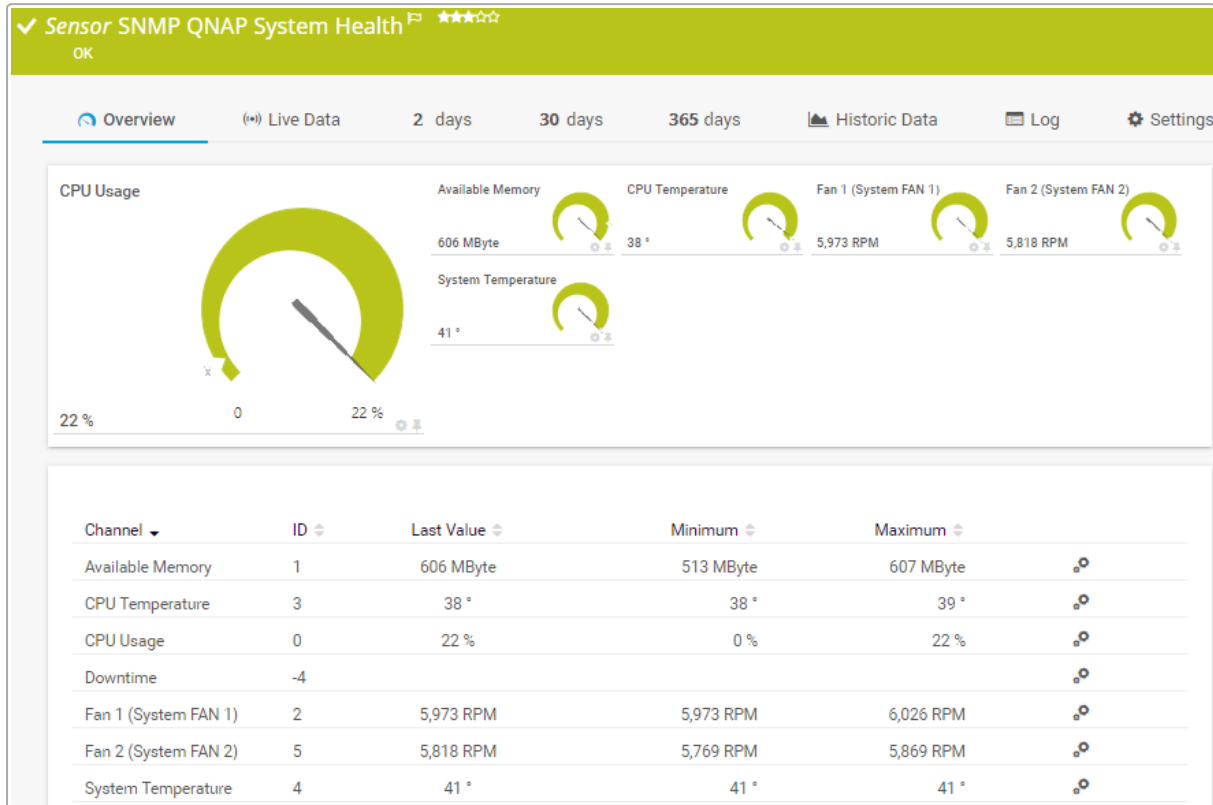
- <https://kb.paessler.com/en/topic/80421>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.228 SNMP QNAP System Health Sensor

The SNMP QNAP System Health sensor monitors the system health of a Quality Network Appliance Provider (QNAP) network-attached storage (NAS) via the Simple Network Management Protocol (SNMP).



SNMP QNAP System Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP QNAP Systeemstatus
- French: QNAP état du système (SNMP)
- German: SNMP QNAP Systemzustand
- Japanese: SNMP QNAP システム正常性
- Portuguese: Saúde do sistema QNAP (SNMP)
- Russian: Работоспособность системы QNAP по SNMP
- Simplified Chinese: SNMP QNAP 系统健康状况
- Spanish: Salud de sistema QNAP (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

**Tags** ⓘ exampletag ✕ +

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- qnap
- snmpqnap
- systemhealth

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### QNAP NAS Settings

#### QNAP NAS Settings

**Unit** ⓘ Celsius

QNAP NAS Settings

Setting	Description
Unit	The unit of temperature measurement.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.



Channel	Description
Available Memory	The available memory
CPU Temperature	The CPU temperature
CPU Usage	The CPU usage  This channel is the primary channel by default.
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Fan [#] (System FAN [#])	The fan RPM
System Temperature	The system temperature

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Why do I get DoS alarms on my QNAP?

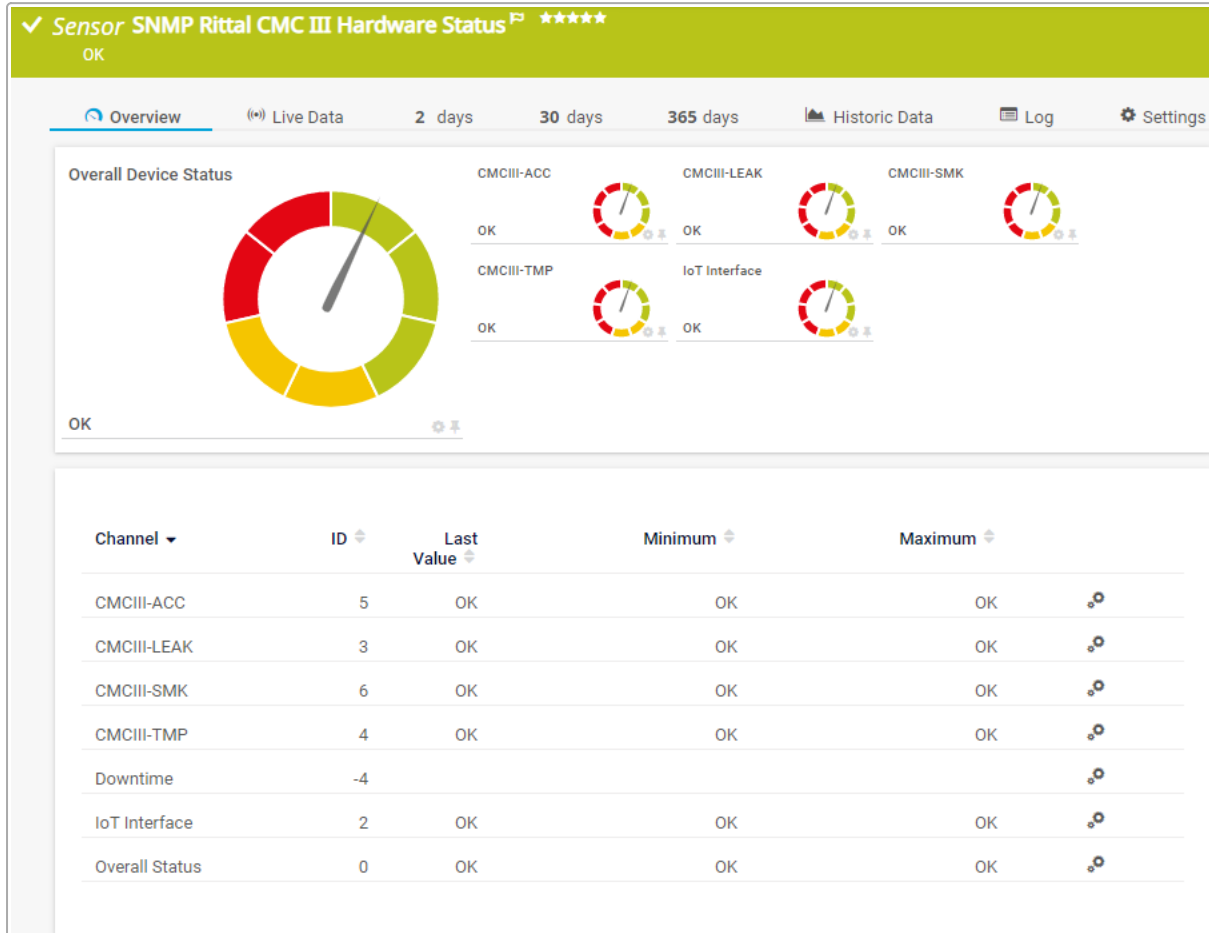
- <https://kb.paessler.com/en/topic/80421>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.229 SNMP Rittal CMC III Hardware Status Sensor

The SNMP Rittal CMC III Hardware Status sensor monitors the overall status of Rittal data center hardware, for example Rittal Computer Multi Control version 3 (CMC III) processing units, Rittal power distribution units (PDU), or Rittal IoT Interfaces and the hardware status of every attached external sensor via the Simple Network Management Protocol (SNMP).



SNMP Rittal CMC III Hardware Status Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Rittal CMC III hardwarestatus
- French: Rittal CMC III statut matériel (SNMP)
- German: SNMP Rittal CMC III Hardware Status
- Japanese: SNMP Rittal CMC III ハードウェアステータス
- Portuguese: Status hardware Rittal CMC III (SNMP)
- Russian: Состояние оборудования Rittal CMC III, SNMP
- Simplified Chinese: SNMP Rittal CMC III 硬件状态
- Spanish: Estado hardware Rittal CMC III (SNMP)

## Remarks

Consider the following [remarks](#)<sup>[2157]</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

Example Name

---

**Tags** ⓘ

exampletag ✕ +

---

**Priority** ⓘ

★★★★☆

Example Name

---

exampletag ✕ +

---

★★★★☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cmc3
- snmprittal

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Sensor Display

### Sensor Display

**Primary Channel** ⓘ

Downtime

---

**Graph Type** ⓘ

Show channels independently (default)

Stack channels on top of each other


Downtime

---


Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Setting
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Overall Device Status	<p>The overall device status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK, Update</li> <li>▪ Warning status: Warning, Detected, Changed</li> <li>▪ Down status: Alarm, Lost</li> </ul>
[Status of attached external sensor]	<p>An attached external sensor status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK; Firmware Update Pending; Firmware Update Running</li> <li>▪ Warning status: Device Detected, Confirmation Required; Device Changed</li> <li>▪ Down status: Device Not Available; Device Lost (Disconnected), Confirmation Required; Error</li> </ul>

More

■ KNOWLEDGE BASE

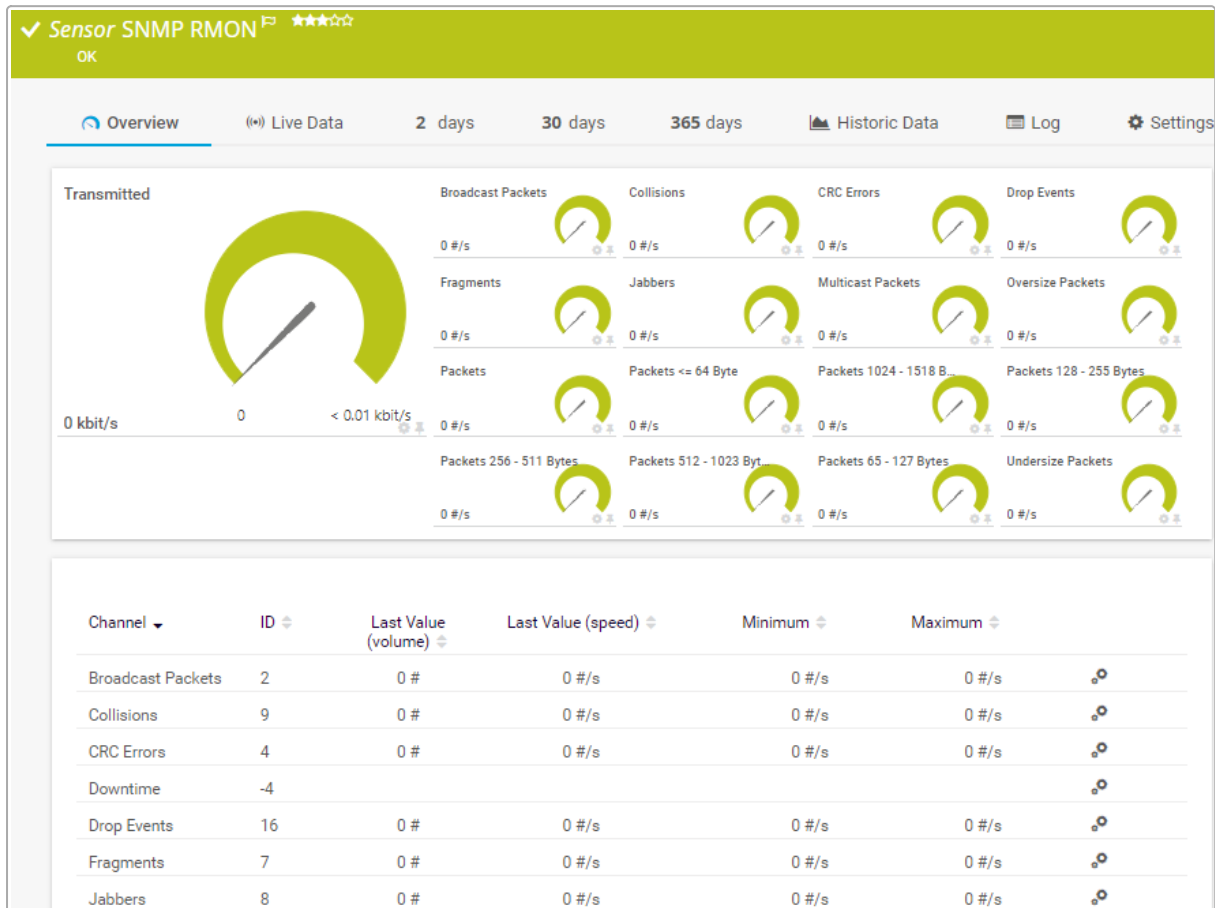
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.230 SNMP RMON Sensor

The SNMP RMON sensor monitors traffic on a device using the Remote Monitoring (RMON) standard via the Simple Network Management Protocol (SNMP).

**i** You can create it on an SNMP-compatible device that provides traffic data via RMON. Depending on the data that the device returns, PRTG displays traffic data for each port in different channels, which allows a detailed analysis. If available, the sensor queries 64-bit counters.



SNMP RMON Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP RMON
- French: RMON (SNMP)
- German: SNMP RMON
- Japanese: SNMP RMON
- Portuguese: RMON (SNMP)
- Russian: RMON no SNMP
- Simplified Chinese: SNMP RMON

- Spanish: RMON (SNMP)

## Remarks

Consider the following [remarks](#) <sup>[2161]</sup> and requirements for this sensor:

Remark	Description
Localhost	It might not work to query data from a probe device via SNMP (querying <a href="#">localhost</a> , <a href="#">127.0.0.1</a> , or <a href="#">::1</a> ). <a href="#">Add this device</a> with the IP address that it has in your network and create the sensor on this device instead.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Port name templates	You can define the displayed sensor name with port name templates in the <a href="#">SNMP compatibility options</a> of the parent device.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">What value does the Transmitted channel of an RMON sensor show?</a></li> <li>▪ Knowledge Base: <a href="#">Automatically update port name and number for SNMP Traffic sensors when the device changes them</a></li> <li>▪ Knowledge Base: <a href="#">Where is the volume line in graphs?</a></li> </ul>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ

**Priority** ⓘ

Example Name

---

exampletag ✕ +

---

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- snmprmon

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>[667]</sup>.

## RMON Specific

**RMON Specific**

Port ⓘ 1

Channel Mask ⓘ 131071

RMON Specific

Setting	Description
Port	The number of the interface port that this sensor monitors.
Channel Mask	Describes which channels are available. This information might be useful for the Paessler support team.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚡ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>



Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Broadcast Packets	The number of broadcast packets
Collisions	The number of collisions
CRC Errors	The number of CRC errors
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Drop Events	The number of drop events
Fragments	The number of fragments
Jabbers	The number of jabbers
Multicast Packets	The number of multicast packets

Channel	Description
Oversize Packets	The number of oversize packets
Packets	The number of packets
Packets <= 64 Byte	The number of packets with less than or equal to 64 bytes
Packets 65 - 127 Bytes	The number of packets with 65 - 127 bytes
Packets 128 - 255 Bytes	The number of packets with 128 - 255 bytes
Packets 256 - 511 Bytes	The number of packets with 256 - 511 bytes
Packets 512 - 1023 Bytes	The number of packets with 512 - 1023 bytes
Packets 1024 - 1518 Bytes	The number of packets with 1024 - 1518 bytes
Transmitted	The transmitted bytes <b>i</b> This channel is the primary channel by default.
Undersize Packets	The number of undersize packets

## More

### ■ KNOWLEDGE BASE

What value does the Transmitted channel of an RMON sensor show?

- <https://kb.paessler.com/en/topic/59821>

Automatically update port name and number for SNMP Traffic sensors when the device changes them

- <https://kb.paessler.com/en/topic/25893>

Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

What security features does PRTG include?

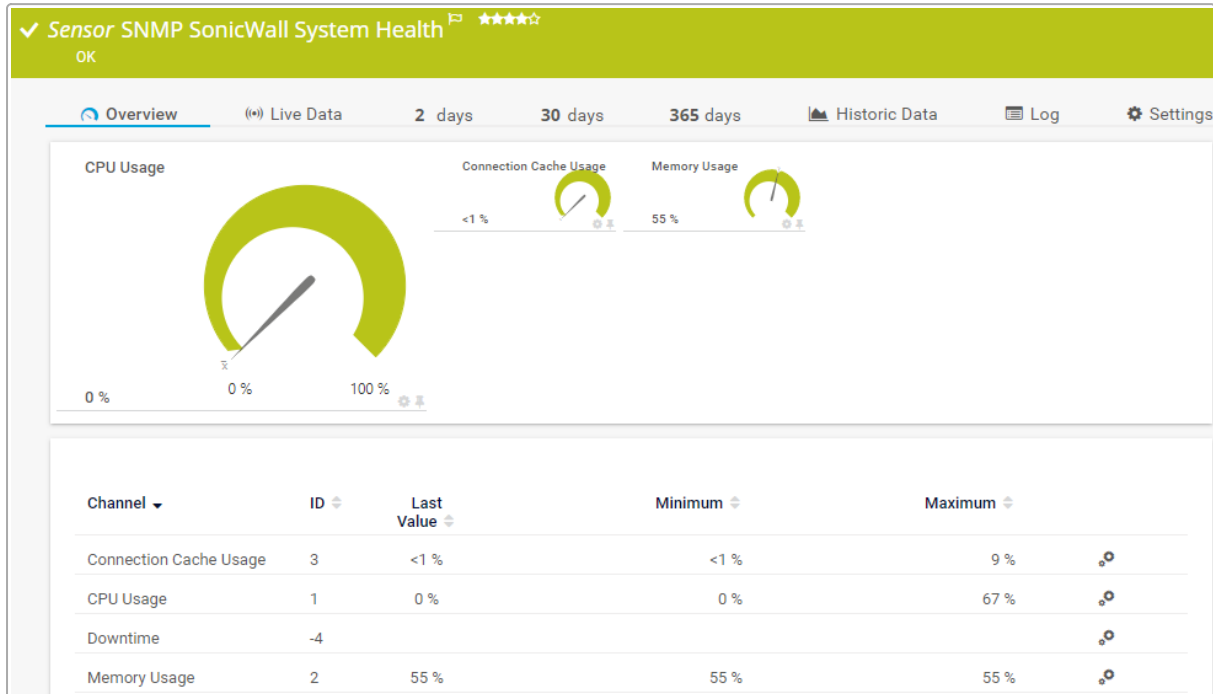
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.231 SNMP SonicWall System Health Sensor

The SNMP SonicWall System Health sensor monitors health values of a SonicWall Network Security Appliance (NSA) via the Simple Network Management Protocol (SNMP).



SNMP SonicWall System Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2167]</sup>.

### Sensor in Other Languages

- Dutch: SNMP SonicWall Systeemstatus
- French: SonicWall état du système (SNMP)
- German: SNMP SonicWall Systemzustand
- Japanese: SNMP SonicWall システム正常性
- Portuguese: Saúde do sistema SonicWall (SNMP)
- Russian: Работоспособность системы SonicWall по SNMP
- Simplified Chinese: SNMP SonicWall 系统健康状况
- Spanish: Salud de sistema SonicWall (SNMP)

### Remarks

Consider the following [remarks](#)<sup>[2168]</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Knowledge Base	Knowledge Base: <a href="#">Why does PRTG write error messages into my SonicWall log?</a>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- snmpsonicwallssystemhealthsensor
- systemhealth

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Display

#### Sensor Display


**Primary Channel** ⓘ Downtime

---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.

Setting	Description
	<p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Connection Cache Used	The connection cache usage (%)
CPU Usage	<p>The CPU usage</p> <p><b>i</b> This channel is the primary channel by default.</p>

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Memory Usage	The memory usage (%)

## More

### ■ KNOWLEDGE BASE

Why does PRTG write error messages into my SonicWall log?

- <https://kb.paessler.com/en/topic/61961>

What security features does PRTG include?

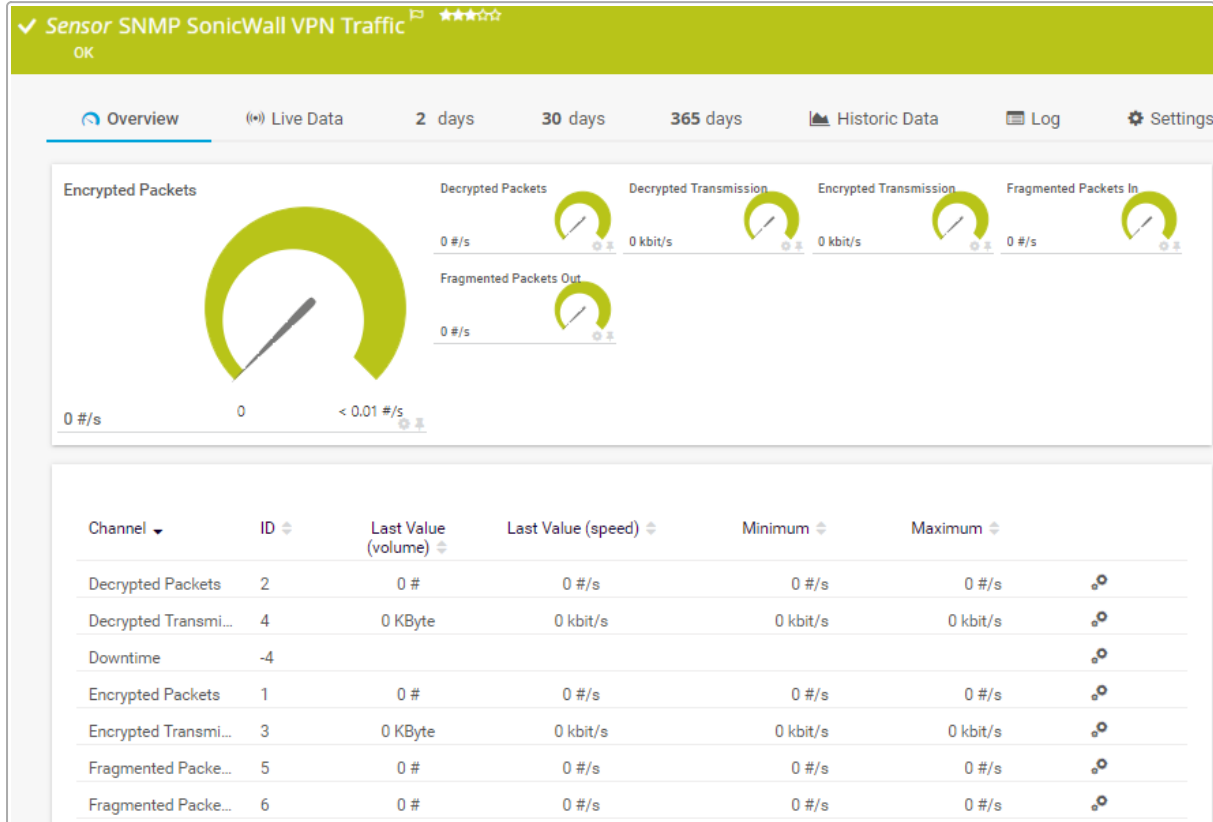
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.232 SNMP SonicWall VPN Traffic Sensor

The SNMP SonicWall VPN Traffic sensor monitors the traffic of an Internet Protocol Security (IPsec) VPN on a SonicWall Network Security Appliance (NSA) via the Simple Network Management Protocol (SNMP).



SNMP SonicWall VPN Traffic Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2173]</sup>.

### Sensor in Other Languages

- Dutch: SNMP SonicWall VPN Verkeer
- French: SonicWall trafic VPN (SNMP)
- German: SNMP SonicWall VPN-Datenverkehr
- Japanese: SNMP SonicWall VPN トラフィック
- Portuguese: Tráfego de VPN SonicWall (SNMP)
- Russian: Трафик VPN SonicWall по SNMP
- Simplified Chinese: SNMP SonicWall VPN 流量
- Spanish: Tráfico VPN SonicWall (SNMP)

### Remarks

Consider the following [remarks](#)<sup>[2169]</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Knowledge Base	Knowledge Base: <a href="#">Why does PRTG write error messages into my SonicWall log?</a>

### Add Sensor

Setting	Description
Connection	Select the connections that you want to monitor. PRTG creates one sensor for each connection that you select.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

Example Name

**Tags** ⓘ

exampletag x +

**Priority** ⓘ

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- snmpsonicwallvpntrafficsensor
- traffic

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.



## SonicWall VPN Specific

**SonicWall VPN Specific**

**Security Policy** ⓘ *WAN GroupVPN*

**Remote IP Address** ⓘ *192.0.2.0*

**Source IP Addresses** ⓘ *0.0.0.0 - 255.255.255.255*

**Destination IP Addresses** ⓘ *0.0.0.0 - 255.255.255.255*

**Index** ⓘ *82*

**Identification Method** ⓘ *Index (default)*

SonicWall VPN Specific

Setting	Description
Security Policy	The security policy of the connection that this sensor monitors.
Remote IP Address	The remote IP address of the connection that this sensor monitors.
Source IP Addresses	The source IP addresses of the connection that this sensor monitors.
Destination IP Addresses	The destination IP addresses of the connection that this sensor monitors.
Index	The index of the connection that this sensor monitors.
Identification Method	<p>Define how you want to identify the connection that you want to monitor:</p> <ul style="list-style-type: none"> <li>▪ <b>Index (default):</b> Every connection has a unique index. This is the safest method to identify your connection. If the connection is lost and reconnected, it receives a new index.</li> <li>▪ <b>Remote IP address:</b> If the target of the VPN always has the same IP address, you can use this IP address to identify the connection.</li> <li>▪ <b>Security policy name:</b> If you use a different security policy for every VPN, you can use its name to identify the connection.</li> <li>▪ <b>Remote IP address and security policy name:</b> You can also combine both identification methods.</li> <li>▪ <b>Remote IP address, security policy name, and IP address ranges:</b> If you use separate connections for specific IP address ranges, identify the connection by remote IP address, security policy name, and IP address ranges.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>IP address ranges: Use IP address ranges only to identify the connection.</li> </ul> <p><b>i</b> The sensor always uses the first connection that it finds that matches all criteria.</p> <p><b>i</b> You cannot change this value after sensor creation.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---


Graph Type **i**  Show channels independently (default)

Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Decrypted Packets	The number of decrypted packets
Decrypted Transmissions	The decrypted transmissions
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Encrypted Packets	The number of encrypted packets  This channel is the primary channel by default.
Encrypted Transmissions	The encrypted transmissions
Fragmented Packets In	The number of incoming fragmented packets
Fragmented Packets Out	The number of outgoing fragmented packets

## More

### ■ KNOWLEDGE BASE

Why does PRTG write error messages into my SonicWall log?

- <https://kb.paessler.com/en/topic/61961>

What security features does PRTG include?

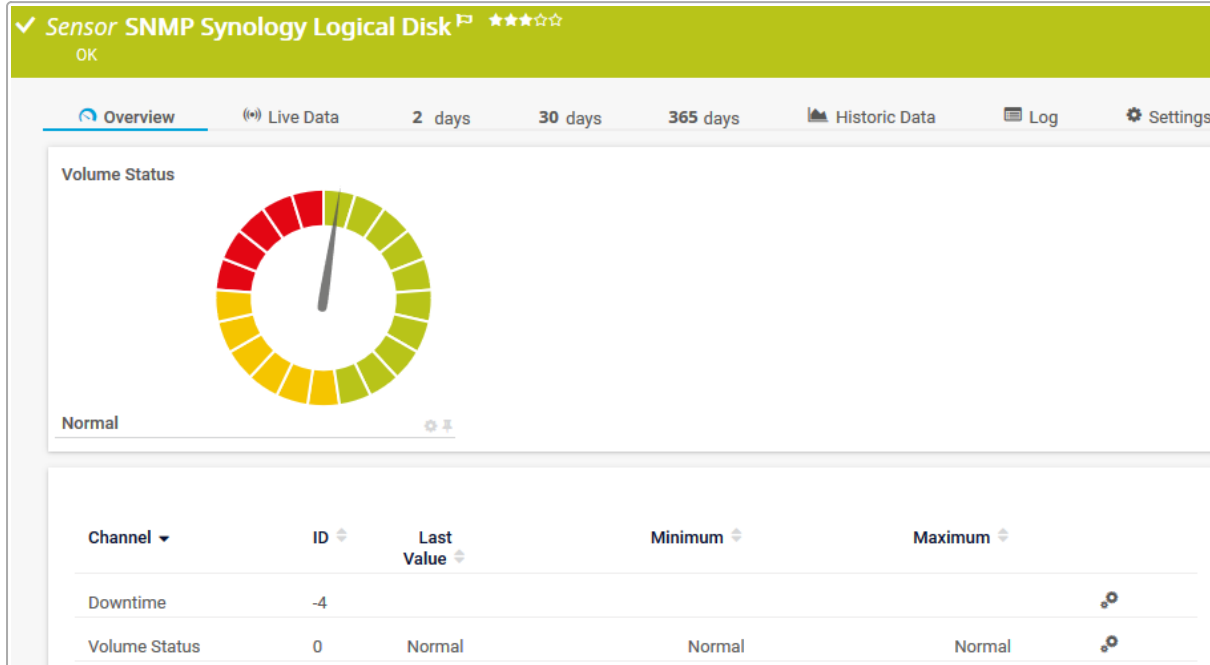
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.233 SNMP Synology Logical Disk Sensor

The SNMP Synology Logical Disk sensor monitors a logical disk in a Synology network-attached storage (NAS) via the Simple Network Management Protocol (SNMP).



SNMP Synology Logical Disk Sensor

■ For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>2177</sup>.

### Sensor in Other Languages

- Dutch: SNMP Synology Logische Schijf
- French: Synology disque logique (SNMP)
- German: SNMP Synology Logischer Datenträger
- Japanese: SNMP Synology 論理ディスク
- Portuguese: Disco lógico Synology (SNMP)
- Russian: Логический диск Synology по SNMP
- Simplified Chinese: SNMP Synology 逻辑磁盘
- Spanish: Disco lógico Synology (SNMP)

### Remarks

Consider the following [remarks](#)<sup>2174</sup> and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★★★☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- logicaldisk
- snmpsynology
- synology

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Synology NAS Settings

#### Synology NAS Settings

**Disk** ⓘ Volume 1

---

Synology NAS Settings

Setting	Description
Disk	The name of the disk that this sensor monitors.

Setting	Description
	<p><b>i</b> PRTG shows this value for reference purposes only. We strongly recommend that you only change it if the Paessler support team explicitly asks you to do so. Wrong usage can result in incorrect monitoring data.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime


---

Graph Type **i**  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Volume Status	<p>The volume status</p> <ul style="list-style-type: none"> <li>▪ Up status: Converting SHR to Pool, Data Scrubbing, Deploying, Expanding Unfinished SHR, Migrating SHR to Pool, Migrating SHR1 to SHR2, Mounting Cache, Normal, Parity Checking, Undeploying, Unmounting Cache</li> <li>▪ Warning status: Assembling, Creating, Expanding, Migrating, Repairing, Syncing</li> <li>▪ Down status: Canceling, Crashed, Degrade, Deleting, Unknown</li> </ul> <p> This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

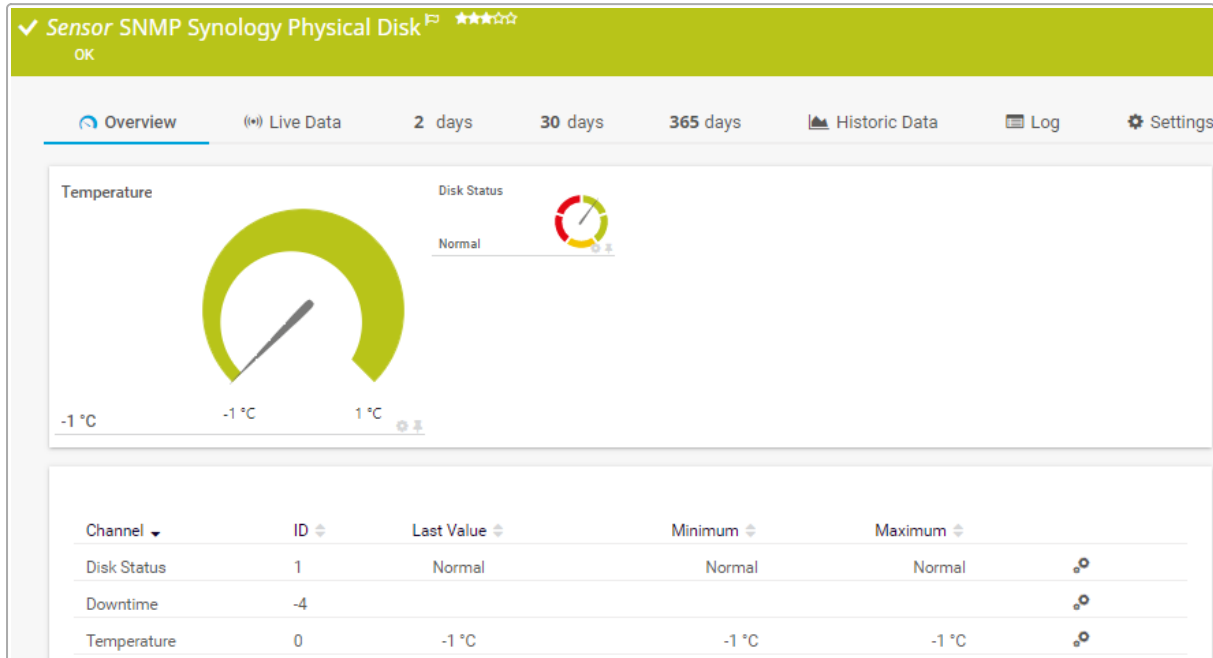
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.234 SNMP Synology Physical Disk Sensor

The SNMP Synology Physical Disk sensor monitors a physical disk in a Synology network-attached storage (NAS) via the Simple Network Management Protocol (SNMP).



SNMP Synology Physical Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP-Synology Fysieke Schijf
- French: Synology disque physique (SNMP)
- German: SNMP Synology Physikalischer Datenträger
- Japanese: SNMP Synology 物理ディスク
- Portuguese: Disco físico Synology (SNMP)
- Russian: Физический диск Synology по SNMP
- Simplified Chinese: SNMP Synology 物理磁盘
- Spanish: Disco físico Synology (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:



Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- physicaldisk
- snmpsynology
- synology

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Synology NAS Settings

#### Synology NAS Settings

**Disk Name** ⓘ Disk 1

---

**Model** ⓘ Virtual disk

---

**Type** ⓘ SATA

Synology NAS Settings

Setting	Description
Disk Name	The name of the disk that this sensor monitors.
Model	The model of the physical disk that this sensor monitors.
Type	The type of the physical disk that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Disk Status	The disk status <ul style="list-style-type: none"> <li>▪ Up status: Initialized, Normal</li> <li>▪ Warning status: NotInitialized</li> <li>▪ Down status: Crashed, SystemPartitionFailed</li> </ul>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Temperature	The temperature <p> This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

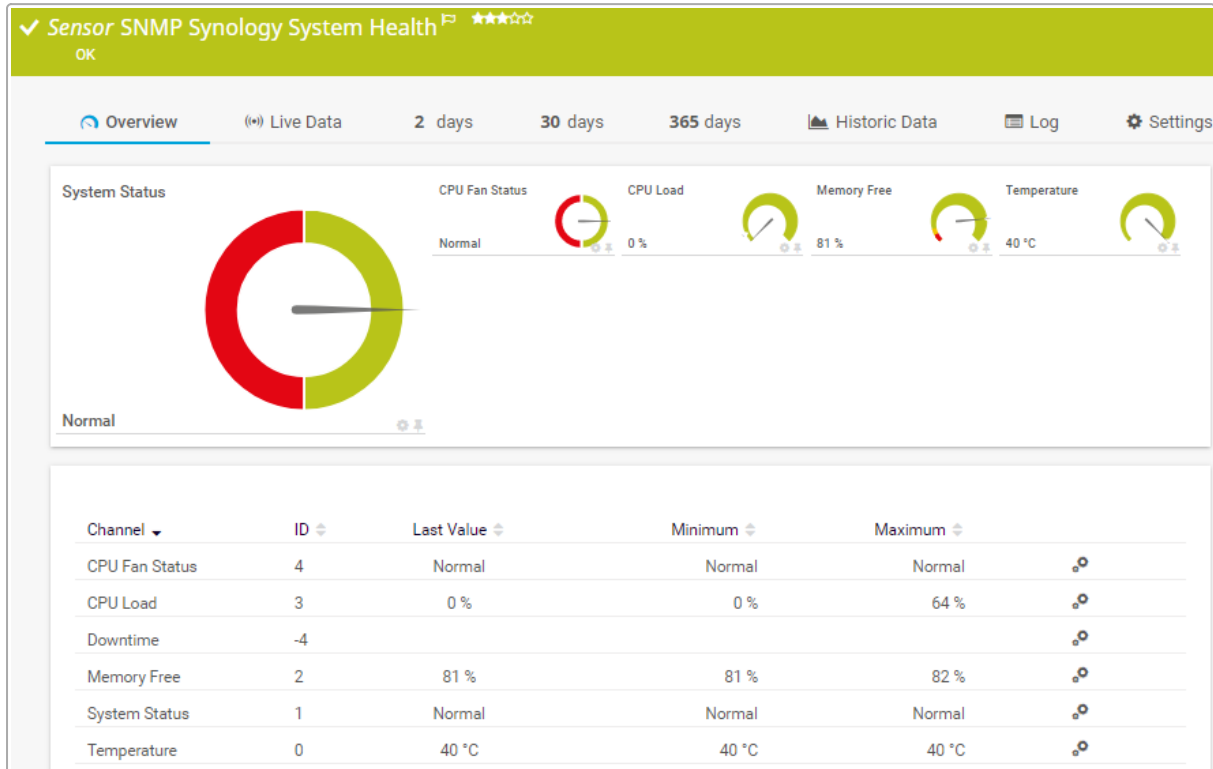
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.235 SNMP Synology System Health Sensor

The SNMP Synology System Health sensor monitors the system health of a Synology network-attached storage (NAS) via the Simple Network Management Protocol (SNMP).



SNMP Synology System Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP-Synology Systeemstatus
- French: Synology état du système (SNMP)
- German: SNMP Synology Systemzustand
- Japanese: SNMP Synology システム正常性
- Portuguese: Saúde do sistema Synology (SNMP)
- Russian: Работоспособность системы Synology по SNMP
- Simplified Chinese: SNMP Synology 系统健康状况
- Spanish: Salud de sistema Synology (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Knowledge Base	Knowledge Base: <a href="#">Why does my Synology System Health sensor show incorrect CPU and memory values?</a>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- snmpsynology
- synology
- systemhealth

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Display


#### Sensor Display

**Primary Channel** ⓘ Downtime


---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CPU Fan Status	<p>The CPU fan status</p> <ul style="list-style-type: none"> <li>▪ Up status: Normal</li> <li>▪ Down status: Failed</li> </ul>

Channel	Description
CPU Load	<p>The CPU load (%)</p> <p>■ For more information about the shown memory and CPU load values, see the Knowledge Base: <a href="#">Why does my Synology System Health sensor show incorrect CPU and memory values?</a></p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Memory Free	<p>The free memory (%)</p> <p>■ For more information about the shown memory and CPU load values, see the Knowledge Base: <a href="#">Why does my Synology System Health sensor show incorrect CPU and memory values?</a></p>
Power Status	<p>The power status</p> <ul style="list-style-type: none"> <li>▪ Up status: Normal</li> <li>▪ Down status: Failed</li> </ul>
System Fan Status	<p>The system fan status</p> <ul style="list-style-type: none"> <li>▪ Up status: Normal</li> <li>▪ Down status: Failed</li> </ul>
System Status	<p>The system status</p> <ul style="list-style-type: none"> <li>▪ Up status: Normal</li> <li>▪ Down status: Failed</li> </ul> <p>ⓘ This channel is the primary channel by default.</p>
Temperature	<p>The temperature</p>

## More

### ■ KNOWLEDGE BASE

Why does my Synology System Health sensor show incorrect CPU and memory values?

- <https://kb.paessler.com/en/topic/63283>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

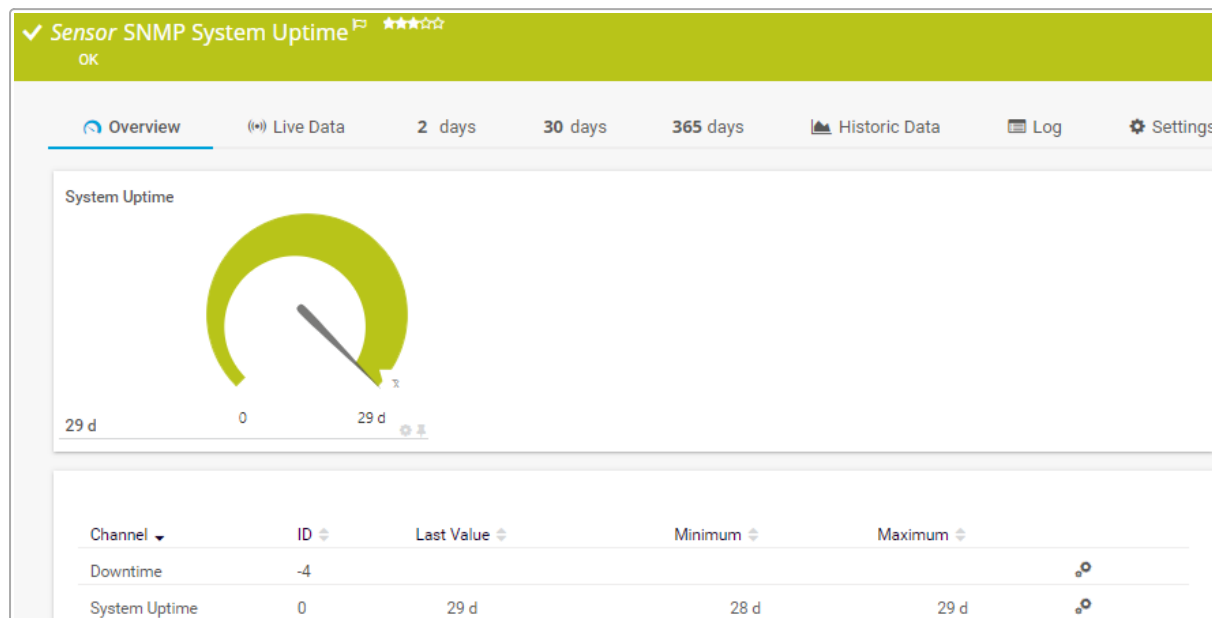
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>



## 7.8.236 SNMP System Uptime Sensor

The SNMP System Uptime sensor monitors the uptime of a device via the Simple Network Management Protocol (SNMP).



SNMP System Uptime Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Systeem Uptime
- French: Disponibilité du système (SNMP)
- German: SNMP Laufzeit
- Japanese: SNMP システムアップタイム
- Portuguese: Tempo de atividade do sistema (SNMP)
- Russian: Время бесперебойной работы системы по SNMP
- Simplified Chinese: SNMP 系统正常运行时间
- Spanish: Tiempo activo del sistema (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Localhost	It might not work to query data from a probe device via SNMP (querying <a href="#">localhost</a> , <a href="#">127.0.0.1</a> , or <a href="#">::1</a> ). <a href="#">Add this device</a> with the IP address that it has in your network and create the sensor on this device instead.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Knowledge Base	Knowledge Base: <a href="#">Why does the SNMP System Uptime sensor report wrong values?</a>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- snmpuptimesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Display

#### Sensor Display

**Primary Channel** ⓘ Downtime


---

**Graph Type** ⓘ


Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
System Uptime	The uptime  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

Why does the SNMP System Uptime sensor report wrong values?

- <https://kb.paessler.com/en/topic/61249>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

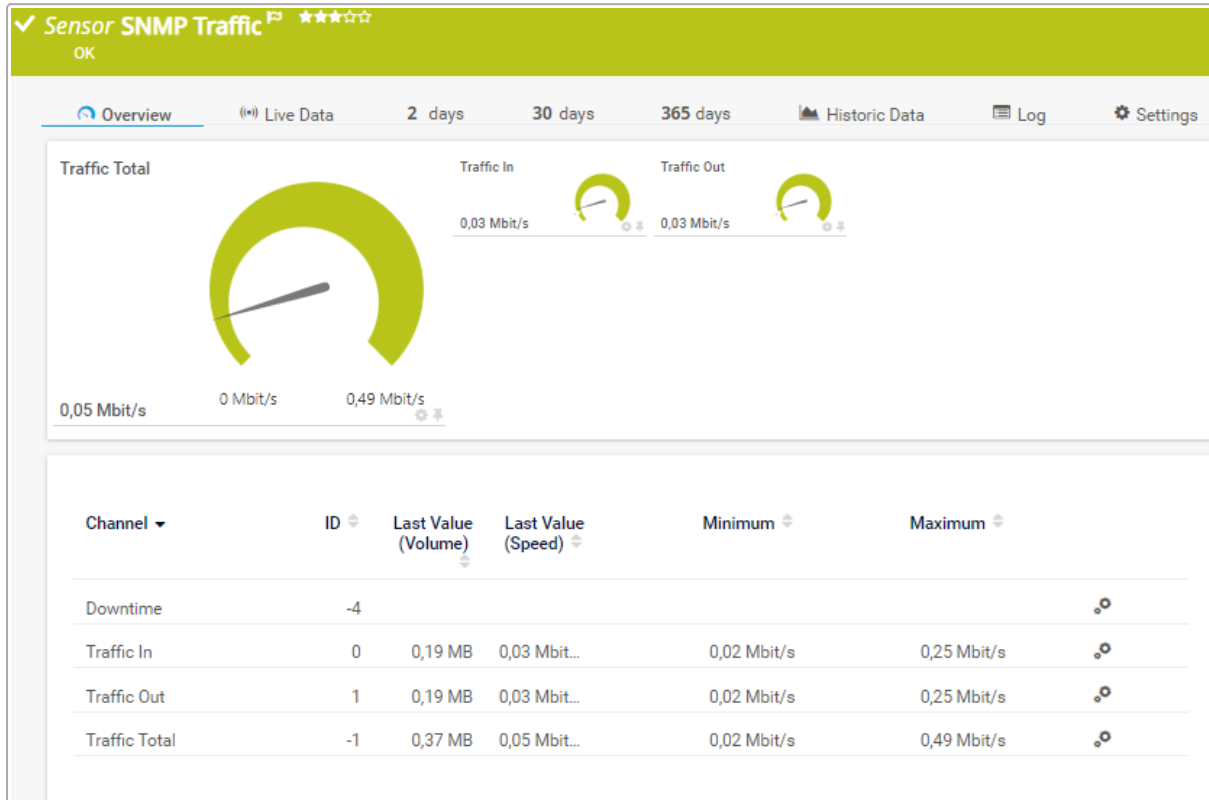
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.237 SNMP Traffic Sensor

The SNMP Traffic sensor monitors traffic on a device via the Simple Network Management Protocol (SNMP).

**i** You can create the sensor on a device that provides traffic data.



SNMP TrafficSensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Verkeer
- French: Trafic (SNMP)
- German: SNMP Datenverkehr
- Japanese: SNMP トラフィック
- Portuguese: Tráfego (SNMP)
- Russian: Трафик по SNMP
- Simplified Chinese: SNMP 流量
- Spanish: Tráfico (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
SNMP v2c or SNMP v3	We recommend that you select SNMP v2c (most common) or SNMP v3 in the <a href="#">credentials for SNMP devices</a> of the parent device (if supported by the target device). SNMP v1 does not support 64-bit counters, which might result in invalid data. For more information, see the Knowledge Base: <a href="#">SNMP Traffic sensor suddenly drops at 610Mbps</a>
Localhost	It might not work to query data from a probe device via SNMP (querying <a href="#">localhost</a> , <a href="#">127.0.0.1</a> , or <a href="#">::1</a> ). <a href="#">Add this device</a> with the IP address that it has in your network and create the sensor on this device instead.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Port name templates	You can define the displayed sensor name with port name templates in the <a href="#">SNMP compatibility options</a> of the parent device.
Auto-discovery	The <a href="#">auto-discovery</a> always creates SNMP Traffic sensors for all interfaces whose SNMP traffic counters are above 0. As a result, every interface that has had traffic since the last restart of the target system is added, even if it is currently disconnected or disabled. For more information, see the Knowledge Base: <a href="#">How does auto-discovery with SNMP Traffic sensors work?</a>
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">Automatically update port name and number for SNMP Traffic sensors when the device changes them</a></li> <li>▪ Knowledge Base: <a href="#">Where is the volume line in graphs?</a></li> </ul>

## Add Sensor

Setting	Description
Name for Traffic In Channel	<p>For the standard channel Traffic In, enter the channel name. The sensor shows it in graphs and tables.</p> <p><b>i</b> You can change this description in the <a href="#">channel settings</a> later.</p>
Name for Traffic Out Channel	<p>For the standard channel Traffic Out, enter the channel name. The sensor shows it in graphs and tables.</p> <p><b>i</b> You can change this description in the <a href="#">channel settings</a> later.</p>

Setting	Description
Name for Traffic Total Channel	For the standard channel Traffic Total, enter the channel name. The sensor shows it in graphs and tables.  ⓘ You can change this description in the <a href="#">channel settings</a> later.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- bandwidthsensor
- snmptrafficsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Traffic Specific

### Traffic Specific

**Interface Number** ⓘ 13:Ethernet0

---

**Additional Channels** ⓘ

- Errors in and errors out
- Discards in and discards out
- Unicast packets in and unicast packets out
- Non unicast packets in and non unicast packets out (32-bit only)
- Multicast packets in and multicast packets out (64-bit only)
- Broadcast packets in and broadcast packets out (64-bit only)
- Unknown Protocols

**Connection Status Handling** ⓘ

- Show down status for all disconnected states
- Show down status when disconnected, ignore when deactivated
- Ignore all disconnected states (default)

**Alias Availability** ⓘ 2

Traffic Specific

Setting	Description
Interface Number	<p>The number and name of the interface in the physical device that this sensor monitors.</p> <p><b>i</b> PRTG shows this value for reference purposes only. We strongly recommend that you only change it if the Paessler support team explicitly asks you to do so. Wrong usage can result in incorrect monitoring data.</p>
Additional Channels	<p>By default, each SNMP Traffic sensor creates the channels Traffic In, Traffic Out, and Traffic Total. Select additional channels for all interfaces. Click the respective channel names to mark the channels and to monitor their data:</p> <ul style="list-style-type: none"> <li>▪ Errors in and errors out: The number of incoming and outgoing packets that could not be delivered because of errors.</li> <li>▪ Discards in and discards out: The number of discarded incoming and outgoing packets even though no errors have been detected.</li> <li>▪ Unicast packets in unicast packets out: The number of unicast packets that have been delivered.</li> <li>▪ Non unicast packets in and non unicast packets out (32-bit only): The number of non-unicast packets that have been delivered.</li> <li>▪ Multicast packets in and multicast packets out (64-bit only): The number of delivered packets that were addressed to a multicast address.</li> <li>▪ Broadcast packets in and broadcast packets out (64-bit only): The number of delivered packets that were addressed to a broadcast address</li> <li>▪ Unknown protocols: The number of received packets that were discarded because of an unknown or unsupported protocol.</li> </ul> <p><b>i</b> You cannot delete additional channels later. You can only disable them.</p> <p><b>i</b> If the sensor shows the Warning <a href="#">status</a> with the message <a href="#">Channels not available</a>, you can disable the affected channels to remove the warning.</p>
Connection Status Handling	<p>An interface is not operational if, for example, an Ethernet port on a switch does not have a cable plugged in. This setting is valid for all selected interfaces.</p> <p>Define how PRTG reacts when an interface is operational:</p> <ul style="list-style-type: none"> <li>▪ Show down status for all disconnected states: Show the Down status for a disconnected interface. This applies every time the <a href="#">ifOperStatus</a> of the interface is not "up".</li> <li>▪ Show down status when disconnected, ignore when deactivated: Show the Down status for a disconnected interface only if it is not deliberately deactivated in the configuration. This applies if the <a href="#">ifOperStatus</a> of the interface is not "up" and the <a href="#">ifAdminStatus</a> is "up". The sensor stays in the Up status when the interface has been deactivated.</li> <li>▪ Ignore all disconnected states (default): Show the Up status.</li> </ul> <p><b>i</b> Monitoring might discontinue without notice.</p>



## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> <li>▪ Show in and out traffic as positive and negative area graph: Show channels for incoming and outgoing traffic as positive and negative area graph. This visualizes your traffic in a clear way. <ul style="list-style-type: none"> <li> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the channel settings). Manual scaling is not possible if you choose this option.</li> <li> ⓘ You cannot show a positive/negative graph for a channel if you choose to display its data in percent of maximum (available in the channel settings).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Discards In	The number of incoming discards
Discards Out	The number of outgoing discards
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Errors In	The number of incoming errors
Errors Out	The number of outgoing errors
Non-Unicast In	The number of incoming non-unicast packets
Non-Unicast Out	The number of outgoing non-unicast packets
Traffic In	The incoming traffic
Traffic Out	The outgoing traffic
Traffic Total	The total traffic  This channel is the primary channel by default.
Unicast In	The number of incoming unicast packets
Unicast Out	The number of outgoing unicast packets
Unknown Protocols In	The number of incoming, unknown protocols

## More

### ■ KNOWLEDGE BASE

How does auto-discovery with SNMP Traffic sensors work?

- <https://kb.paessler.com/en/topic/85407>

Automatically update port name and number for SNMP Traffic sensors when the device changes them

- <https://kb.paessler.com/en/topic/25893>

Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

SNMP Traffic sensor suddenly drops at 610Mbps

- <https://kb.paessler.com/en/topic/67503>

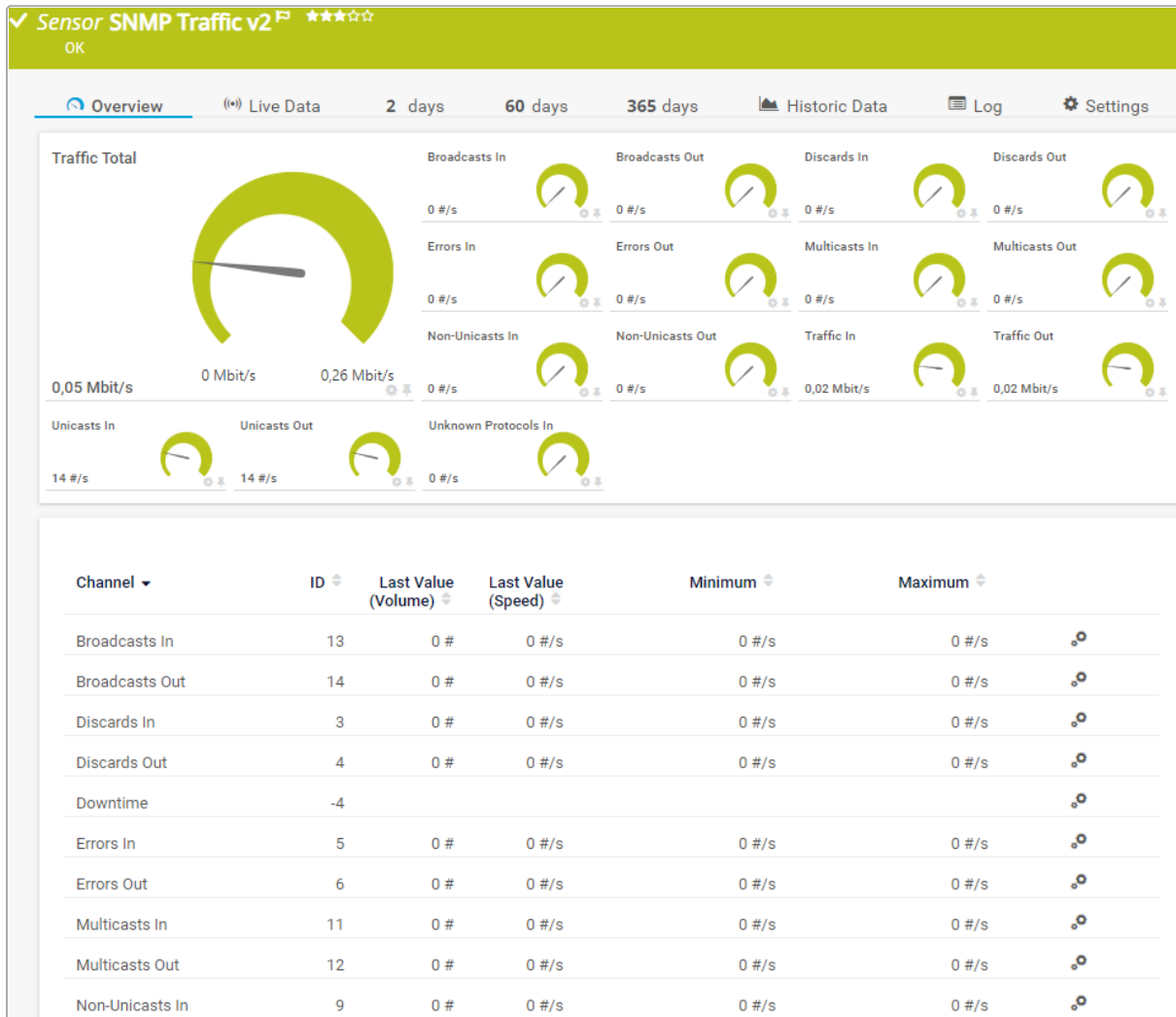
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.238 SNMP Traffic v2 Sensor (BETA)

The SNMP Traffic v2 sensor monitors bandwidth and traffic on a device via the Simple Network Management Protocol (SNMP).

**BETA** This sensor is in beta status. The operating methods and the available settings are still subject to change. Do not expect that all functions work properly, or that this sensor works as expected at all.



SNMP Traffic v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Traffic v2
- French: Trafic v2 (SNMP)
- German: SNMP-Datenverkehr v2
- Japanese: SNMP トラフィック v2

- Portuguese: Tráfego (SNMP) v2
- Russian: SNMP Traffic v2
- Simplified Chinese: SNMP 流量版本 2
- Spanish: Tráfico (SNMP) v2

## Remarks

Consider the following [remarks](#) <sup>[2199]</sup> and requirements for this sensor:

Remark	Description
Enabled Beta Sensors experimental feature	<p>This sensor requires that the Beta Sensors <a href="#">experimental feature</a> is enabled.</p> <ul style="list-style-type: none"> <li>■ For more information, see the Knowledge Base: <a href="#">What are beta sensors and how can I use them?</a></li> </ul>
SNMP v2c or SNMP v3	<p>We recommend that you select SNMP v2c (most common) or SNMP v3 in the <a href="#">credentials for SNMP devices</a> of the parent device (if supported by the target device). SNMP v1 does not support 64-bit counters, which might result in invalid data. For more information, see the Knowledge Base: <a href="#">SNMP Traffic sensor suddenly drops at 610Mbps</a></p>
Localhost	<p>It might not work to query data from a probe device via SNMP (querying <a href="#">localhost</a>, <a href="#">127.0.0.1</a>, or <a href="#">::1</a>). <a href="#">Add this device</a> with the IP address that it has in your network and create the sensor on this device instead.</p>
IPv6	<p>This sensor supports IPv6.</p>
Performance impact	<p>This sensor has a <a href="#">very low</a> performance impact.</p>
SNMP compatibility options	<p>This sensor is not affected by the following <a href="#">SNMP compatibility options</a> set in the parent device: Port Name Template, Port Name Update, Port Identification, and End Interface Index.</p>
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">1 minute</a>.</li> </ul>
Multi-platform probe	<p>You can add this sensor to a multi-platform probe.</p>
Knowledge Base	<p>Knowledge Base: <a href="#">Where is the volume line in graphs?</a></p>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- bandwidthsensor
- snmp
- snmptrafficsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## SNMP Interface

### SNMP Interface

**Description** ⓘ Example Interface

---

**64-Bit** ⓘ Yes

SNMP Interface

Setting	Description
Description	<p>The description of the interface in the physical device that this sensor monitors. The internal name is found in the ifTable under ifDescr.</p> <p><span style="color: red; font-weight: bold;">i</span> PRTG shows this value for reference purposes only. We strongly recommend that you only change it if the Paessler support team explicitly asks you to do so. Wrong usage can result in incorrect monitoring data.</p>
64-Bit	<p>If the interface that this sensor monitors uses 64-bit counters.</p> <p><span style="color: red; font-weight: bold;">i</span> PRTG shows this value for reference purposes only. We strongly recommend that you only change it if the Paessler support team explicitly asks you to do so. Wrong usage can result in incorrect monitoring data.</p>

## SNMP Traffic Specific

### SNMP Traffic Specific

**Additional Channels** ⓘ

- Errors in and errors out
- Discards in and discards out
- Unicasts in and unicasts out
- Non-unicasts in and non-unicasts out
- Multicasts in and multicasts out (64-bit only)
- Broadcasts in and broadcasts out (64-bit only)
- Unknown protocols in

**Connection Status Handling** ⓘ

- Show the 'Down' status anytime ifOperStatus is not 'Up'
- Show the 'Down' status when ifAdminStatus is 'Up' but ifOperStatus is not
- Ignore all disconnected states (default)

SNMP Traffic Specific

Setting	Description
Additional Channels	<p>By default, each SNMP Traffic v2 sensor creates the channels Traffic In, Traffic Out, and Traffic Total. Select additional channels for all interfaces. Click the respective channel names to mark the channels and to monitor their data:</p> <ul style="list-style-type: none"> <li>▪ Errors in and errors out: The number of incoming and outgoing packets that could not be delivered because of errors.</li> <li>▪ Discards in and discards out: The number of discarded incoming and outgoing packets even though no errors have been detected.</li> <li>▪ Unicasts in and unicasts out: The number of unicast packets that have been delivered.</li> <li>▪ Non-unicasts in and non-unicasts out: The number of non-unicast packets that have been delivered.  <span style="color: red;">❗</span> These channels might not function properly with 64-bit interfaces.</li> <li>▪ Multicasts in and multicasts out (64-bit only): The number of delivered packets that were addressed to a multicast address.</li> <li>▪ Broadcasts in and broadcasts out (64-bit only): The number of delivered packets that were addressed to a broadcast address.</li> <li>▪ Unknown protocols in: The number of received packets that were discarded because of an unknown or unsupported protocol.</li> </ul> <p><span style="color: red;">❗</span> You cannot delete additional channels later. You can only disable them.</p> <p><span style="color: blue;">❗</span> If the sensor shows the Warning <a href="#">status</a> with the message <a href="#">Channels not available</a>, you can disable the affected channels to remove the warning.</p>
Connection Status Handling	<p>An interface is not operational if, for example, an Ethernet port on a switch does not have a cable plugged in. This setting is valid for all selected interfaces.</p> <p>Define how PRTG reacts when an interface is operational:</p> <ul style="list-style-type: none"> <li>▪ Show the 'Down' status anytime ifOperStatus is not 'Up': Show the Down status for a disconnected interface. This applies every time the <a href="#">ifOperStatus</a> of the interface is not 'up'.</li> <li>▪ Show the 'Down' status when ifAdminStatus is 'Up' but ifOperStatus is not: Show the Down status for a disconnected interface only if it is not deliberately deactivated in the configuration. This applies if the <a href="#">ifAdminStatus</a> is 'up' and the <a href="#">ifOperStatus</a> of the interface is not 'up'. The sensor stays in the Up status when the interface has been deactivated.</li> <li>▪ Ignore all disconnected states (default): Show the Up status regardless of the ifOperStatus status.  <span style="color: blue;">❗</span> Monitoring might discontinue without notice.</li> </ul>



## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> <li>▪ Show in and out traffic as positive and negative area graph: Show channels for incoming and outgoing traffic as positive and negative area graph. This visualizes your traffic in a clear way. <ul style="list-style-type: none"> <li> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the channel settings). Manual scaling is not possible if you choose this option.</li> <li> ⓘ You cannot show a positive/negative graph for a channel if you choose to display its data in percent of maximum (available in the channel settings).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result: Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>ⓘ If you select Store result, the sensor writes the standard error (stderr) streams in clear text to the last sensor result file. Do not return sensitive information via the scripts that you run with this sensor.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Broadcasts In	The number of incoming broadcast packets
Broadcasts Out	The number of outgoing broadcast packets
Discards In	The number of incoming discards

Channel	Description
Discards Out	The number of outgoing discards
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Errors In	The number of incoming errors
Errors Out	The number of outgoing errors
Multicasts In	The number of incoming multicast packets
Multicasts Out	The number of outgoing multicast packets
Non-Unicasts In	The number of incoming non-unicast packets
Non-Unicasts Out	The number of outgoing non-unicast packets
Traffic In	The incoming traffic
Traffic Out	The outgoing traffic
Traffic Total	The total traffic  This channel is the primary channel by default.
Unicasts In	The number of incoming unicast packets
Unicasts Out	The number of outgoing unicast packets
Unknown Protocols In	The number of incoming, unknown protocols

## More

### KNOWLEDGE BASE

Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

SNMP Traffic sensor suddenly drops at 610Mbps

- <https://kb.paessler.com/en/topic/67503>

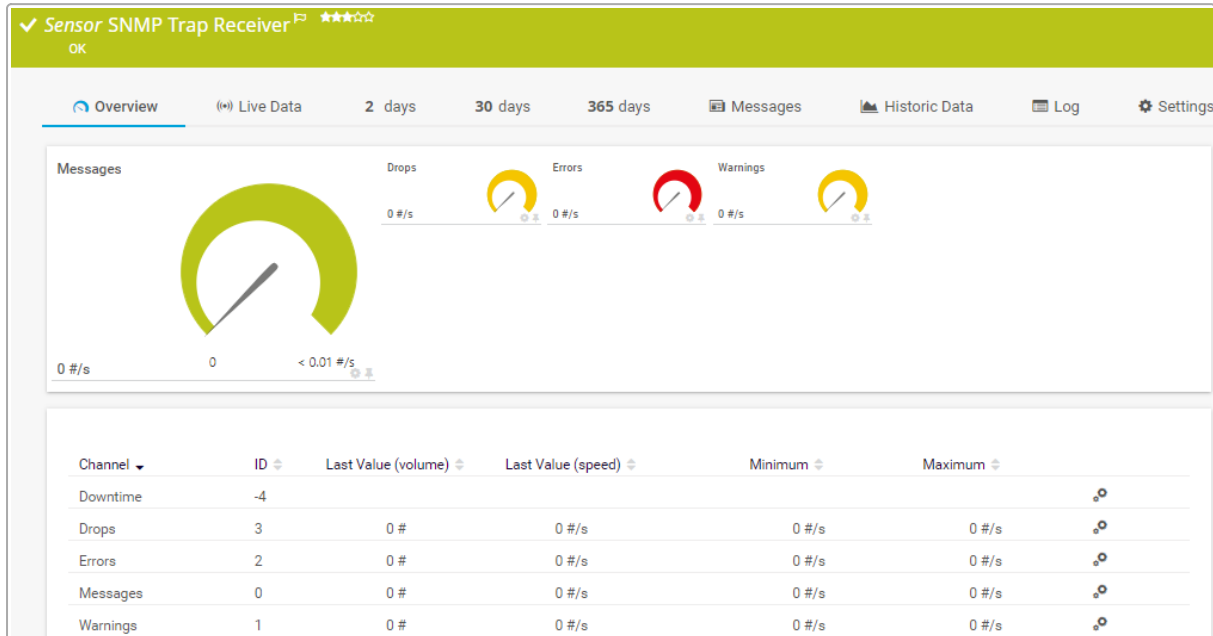
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.239 SNMP Trap Receiver Sensor

The SNMP Trap Receiver sensor receives and analyzes Simple Network Management Protocol (SNMP) traps.

**i** The sensor can also show the actual trap messages.



SNMP Trap Receiver Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Trap-ontvanger
- French: Récepteur de Trap (SNMP)
- German: SNMP-Trap-Empfänger
- Japanese: SNMP トラップレシーバー
- Portuguese: Receptor de trap SNMP
- Russian: Приемник ловушек SNMP
- Simplified Chinese: SNMP 陷阱接收程序
- Spanish: Receptor de trap SNMP

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
SNMP v3 traps	This sensor does not support SNMP v3 traps. Use SNMP v1 or v2c.
UDP	This sensor only supports the User Datagram Protocol (UDP).
Probe device	<p>Add this sensor to the probe device to receive all messages of the remote probe system.</p> <p><b>i</b> If you add the sensor to a device other than a probe device, the IP address or Domain Name System (DNS) name of the parent device must match the proper sender. For example, if you want to receive messages from a storage area network (SAN), you might need to add a device with the IP address of a specific array member that sends the messages. Providing a DNS name that points to the IP address of a whole group might not work for SANs.</p>
Specific device	Add this sensor to a specific device to directly receive all messages from this device. This is faster than using source filters.
IPv6	This sensor supports IPv6.
Placeholders	You can use <a href="#">placeholders</a> in email <a href="#">notification templates</a> to see messages when you receive email notifications.
Sensor states	The <a href="#">sensor states</a> of this sensor persist for one scanning interval only. After showing the Warning or the Down status, and if there is no warning or error message in the next scanning interval, the sensor shows the Up status again. For more information on a workaround, see the Knowledge Base: <a href="#">How can I configure sensors using speed limits to keep the status for more than one interval?</a>
Filter options	You can use the filter options to define which types of messages the sensor considers for monitoring, and which messages it categorizes as warnings or errors.
MIB file	<p>In PRTG Network Monitor, you can copy the Management Information Base (MIB) file for your traps to the \MIB subfolder of the <a href="#">PRTG program directory</a> to translate the object identifiers (OID) for the traps into readable messages. For more information, see the Knowledge Base: <a href="#">How can I show the name of a received OID in PRTG?</a></p> <p> To import MIB files into PRTG Hosted Monitor, see section <a href="#">Manage a PRTG Hosted Monitor Subscription</a>.</p>

Remark	Description
Cluster probe	This sensor does not support cluster probes. You can only set it up on local probes or remote probes.
Knowledge Base	Knowledge Base: <a href="#">How do I test an SNMP Trap Receiver sensor?</a>
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- snmptrapsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### SNMP Trap Specific

#### SNMP Trap Specific

**Port** ⓘ 162

---

**Purge Messages After** ⓘ 32 days (default)

SNMP Trap Specific

Setting	Description
Port	Enter the number of the port on which the sensor listens for SNMP traps. The default port is <b>162</b> . Enter an integer.

Setting	Description
	<b>i</b> We recommend that you use the default value.
Purge Messages After	Define for how long PRTG stores received trap messages for analysis. Choose a period of time from the dropdown list.

## Filter

For more information, see section [Filter Rules](#) <sup>2213</sup>.

**Filter**

*Filters are formulas using AND, OR, NOT, brackets, and the following fields:*

Field	Parameters	Examples
source[ip]	Enter a UDP source IP, IP range, or IP hostmask	source[10.0.23.50] source[10.0.23.10-50] source[10.0.23.10/24]
agent[ip]	Enter the IP of the object that generates the trap (V1 only)	agent[10.0.0.1]
enterprise[oid]	Enter the OID of the object that generates the trap (V1 only)	enterprise[1.3.6.1.4.1.2.6.182.1.2.31.1.0]
bindings[text]	Enter a substring to match on all OIDs and values in the bindings	bindings[ERROR] bindings[1.3.6.1.4.1.2.6.182] bindings[\"port blocked\"]
bindings[oid,value]	Enter an OID and a substring (comma separated) to match a value in the defined OID	bindings[1.3.6.1.4.1.2.6.182.1.2.71.1.0,...]
bindings[oid,value,mode]	Enter an OID, a substring, and a mode (comma separated) to match a value in the bindings. Mode can be <ul style="list-style-type: none"> <li>• <i>substring</i></li> <li>• <i>exact</i></li> <li>• <i>equal, greater, greaterorequal, less, lessorequal</i></li> </ul>	bindings[1.3.6.1.4.1.2.6.182.1.2.71.1.0,...] bindings[1.3.6.1.4.1.2.6.182.1.2.71.1.0,...]
gentrap[number]	Enter a number or range of the generic trap type	gentrap[6] gentrap[2-4]
spectrap[number]	Enter a number or range of the specific trap code	spectrap[0] spectrap[1-2]
version[number]	Enter the SNMP version (1 or 2)	version[1] version[2]
community[text]	Enter the community string to match (exact, case sensitive)	community[public] community[private]

**Include Filter** ⓘ any //

---

**Exclude Filter** ⓘ //

---

**Warning Filter** ⓘ //

---

**Error Filter** ⓘ //

Filter



Setting	Description
Include Filter	Define if you want to filter traps. If you leave this field empty or use the keyword <b>any</b> , the sensor processes all data. To include only specific types of traps, define filters using a special syntax.
Exclude Filter	Define which types of traps the sensor discards and does not process. To exclude specific types of traps, define filters using a special syntax.
Warning Filter	<p>Define which types of traps count for the Warnings channel. To categorize received traps as warning messages, define filters using a special syntax.</p> <p><b>i</b> The sensor collects messages until a scanning interval ends. As long as the scanning interval is running, no status change happens. By default, the sensor changes to the Warning <b>status</b> after a scanning interval finishes and there was at least one warning message (and no error message) during this scanning interval. The sensor shows the Warning status at least until the succeeding scanning interval finishes. If the sensor does not receive any warning or error message in this scanning interval, its status changes to the Up status again with the start of the next scanning interval.</p>
Error Filter	<p>Define which types of traps count for the Errors channel. To categorize received traps as error messages, define filters using a special syntax.</p> <p><b>i</b> The sensor collects messages until a scanning interval ends. As long as the scanning interval is running, no status change happens. By default, the sensor changes to the Down status after a scanning interval finishes and there was at least one error message during this scanning interval. The sensor shows the Down status at least until the succeeding scanning interval finishes. If the sensor does not receive any warning or error message in this scanning interval, its status changes to the Up status again with the start of the next scanning interval.</p>

## Sensor Display


**Sensor Display**

Primary Channel ⓘ Downtime


---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Debug Options

**Debug Options**

Result Handling **i**  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	Define what PRTG does with the sensor result:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\debug subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is UDP Debug Port [Port]_[Date].log. This setting is for debugging purposes. <ul style="list-style-type: none"> <li>ⓘ Use with caution. We recommend that you only use this setting for a short time because it can create huge data files.</li> </ul> </li> </ul>

## Filter Rules

Filter rules are used for the include, exclude, warning, and error definition fields of the SNMP Trap Receiver sensor. They are based on the following format:

```
field[filter]
```

You can use include and exclude filters to define which traps to monitor or use warning and error filters to define how to categorize received traps. Provide these filters in the sensor settings as formulas. Formulas are fields that you can combine with boolean operators ([AND](#), [OR](#), [NOT](#)) and brackets.

Field	Parameter	Examples
source[ip]	Enter an IP address where the UDPs come from. <a href="#">IP masks and ranges</a> are also possible.	source[10.0.23.50], source[10.0.23.10-50], source[10.0.23.10/24]
agent[ip]	Enter an IP address that specifies the object that creates the SNMP trap.  ⓘ agent[ip] only supports v1.	agent[10.0.0.1]
enterprise[oid]	Enter an OID that specifies the object that originates the trap.  ⓘ enterprise[oid] only supports v1.	enterprise[1.3.6.1.4.1.2.6.182.1.2.31.1.0]
bindings[text]	Enter a substring to match all OIDs and values in the bindings.	bindings[ERROR], bindings[1.3.6.1.4.1.2.6.182.1.2.31.1.0], bindings["port blocked"]  ⓘ It is not necessary to use quotation marks (") to find strings. If the string contains quotation marks that you want to include in the filter, you need to escape them with quotation marks.
bindings [oid,value]	Enter an OID and a substring to match a value in the specified OID. Separate the OID and the value with a comma.	bindings[1.3.6.1.4.1.2.6.182.1.2.31.1.0,error]

Field	Parameter	Examples
bindings [oid ,value,mode]	Enter an OID, a substring, and a mode to match a value in the specified OID. Separate the OID, the value, and the mode with a comma. The mode can be: <ul style="list-style-type: none"> <li>▪ substring (default): This mode works like bindings[oid,value].</li> <li>▪ exact: This mode enforces an exact match of a value.</li> <li>▪ equal, greater, greaterorequal, less, or lessorequal: This interprets and compares values as numbers. <ul style="list-style-type: none"> <li>❗ This mode only supports integers without extra characters and without thousands separators.</li> <li>❗ It also supports hex format.</li> </ul> </li> </ul>	bindings[1.3.6.1.4.1.2.6.182.1.2.31.1.0,error,exact] bindings[1.3.6.1.4.1.2.6.182.1.2.31.1.0,10,equal]
gentrap [number]	Enter a number that specifies the generic trap type. <ul style="list-style-type: none"> <li>❗ You can also enter ranges.</li> </ul>	gentrap[3], gentrap[2-6]
spectrap [number]	Enter a number that defines the specific trap code. <ul style="list-style-type: none"> <li>❗ You can also enter ranges.</li> </ul>	spectrap[4], spectrap[0-3]
version[number]	Enter a number (1 or 2) that specifies the SNMP version.	version[1], version[2]
community [text]	Enter a community string for an exact, case-sensitive match.	community[public], community[private]

## Messages Tab: Review and Analyze Traps

PRTG stores received traps as common files in the \Trap Database subfolder of the PRTG data directory. To review and analyze all received messages, you can directly access the most recent data in a [table list](#) in the PRTG web interface. You can access this list via the sensor's Overview tab.

❗ PRTG only shows received traps in the table on the Overview tab after an (automatic) page refresh following a sensor scan. The default value for [auto refresh](#) is 30 seconds.


For more details and further filter options, click the Messages tab of the SNMP Trap Receiver sensor. You see all received messages in a table list. At the top, you have display filter options to drill down into the data for specific events of your interest. The filters are the same as those that are available in the sensor settings, but you can define them without using formulas. Provide the desired parameters and PRTG automatically loads the filtered list.

❗ PRTG automatically applies boolean operators to the filters in the following manner: parameters across all columns are combined with **AND**, and parameters within a single column are combined with **OR**.

❗ The parameters that you enter in the filters must **exactly** match the parameters in the message. They are case-sensitive.

❗ You can automatically add a filter by clicking the content of a column.





### Advanced Filter Settings

You can open advanced filter settings by clicking  in the Filter row. The Advanced Filter appears in a popup window. In the text field, you can define a filter using the syntax as described in section [Filter Rules](#) <sup>2213</sup>.

If you provided filter parameters on the Messages tab, the advanced filter already includes them as a corresponding formula with the correct syntax. You can adjust this filter to your needs. You can also copy the automatically created and manually adjusted formula for usage in the filter fields of the sensor settings.

## Channel List

-  Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Drops	The number of dropped packets on the SNMP trap collector port  This channel has a default limit: <ul style="list-style-type: none"> <li>Upper warning limit: <a href="#">0.00000001</a></li> </ul>
Errors	The number of messages categorized as "error"  This channel has a default limit: <ul style="list-style-type: none"> <li>Upper error limit: <a href="#">0.00000001</a></li> </ul>
Messages	The overall number of received traps  This channel is the primary channel by default.
Warnings	The number of messages categorized as "warning"  This channel has a default limit: <ul style="list-style-type: none"> <li>Upper warning limit: <a href="#">0.00000001</a></li> </ul>

## More

### KNOWLEDGE BASE

How can I configure sensors using speed limits to keep the status for more than one interval?

- <https://kb.paessler.com/en/topic/73212>

How can I show the name of a received OID in PRTG?

- <https://kb.paessler.com/en/topic/63562>

How do I test an SNMP Trap Receiver sensor?

- <https://kb.paessler.com/en/topic/10193>

What security features does PRTG include?

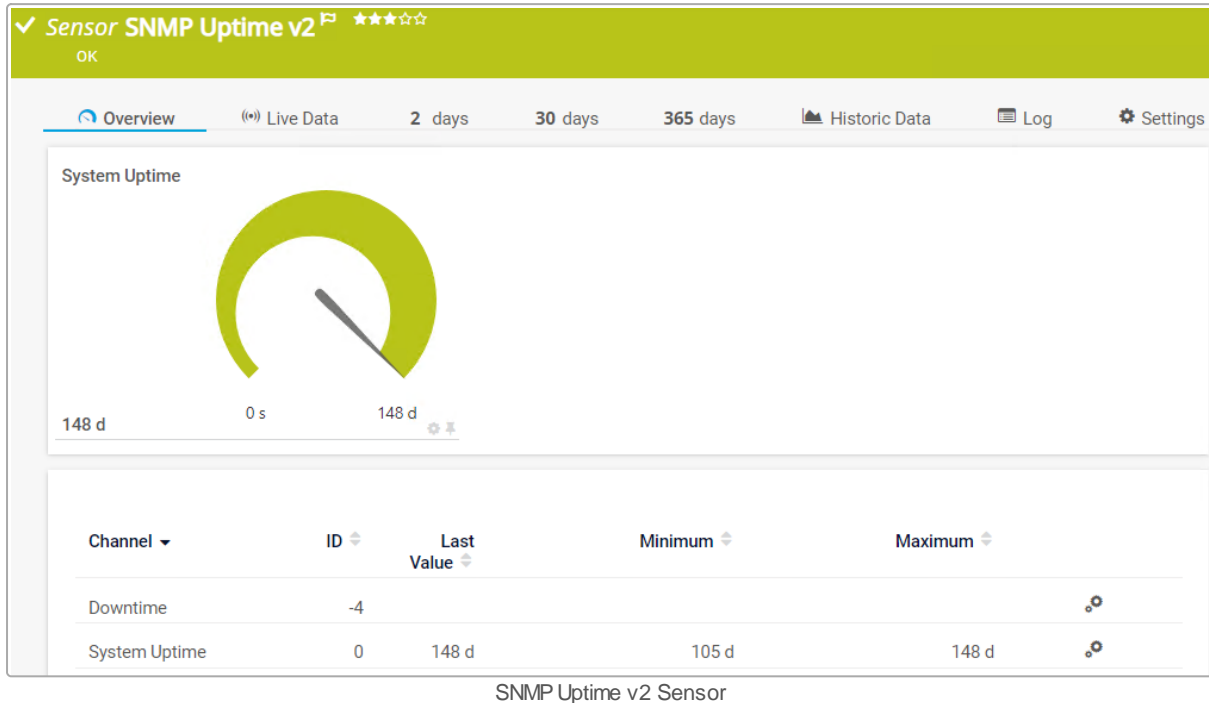
- <https://kb.paessler.com/en/topic/61108>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.240 SNMP Uptime v2 Sensor

The SNMP Uptime v2 sensor monitors the uptime of a device via the Simple Network Management Protocol (SNMP).



For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Uptime v2
- French: Disponibilité v2 (SNMP)
- German: SNMP Laufzeit v2
- Japanese: SNMP アップタイム v2
- Portuguese: Tempo de atividade (SNMP) v2
- Russian: SNMP Uptime v2
- Simplified Chinese: SNMP 正常运行时间版本 2
- Spanish: Tiempo de actividad (SNMP) v2

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for SNMP in settings that are higher in the <a href="#">object hierarchy</a> .
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <b>1 minute</b>.</li> <li>▪ The recommended scanning interval of this sensor is <b>1 minute</b>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- snmp
- snmpuptimesensor
- uptime
- uptimesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.



## SNMP Uptime Specific

**SNMP Uptime Specific**

Data Source ⓘ  Automatic (default)

Use HOST-RESOURCES-V2-MIB::hrSystemUptime

Use SNMPv2-MIB::sysUpTime

Use SNMP-FRAMEWORK-MIB::snmpEngineTime

SNMP Uptime Specific

Setting	Description
Data Source	<p>Select the object identifier (OID) the sensor gets its uptime from:</p> <ul style="list-style-type: none"> <li>▪ Automatic (default): Use <a href="#">HOST-RESOURCES-V2-MIB::hrSystemUptime</a> and fall back to <a href="#">SNMPv2-MIB::sysUpTime</a>.</li> <li>▪ Use HOST-RESOURCES-V2-MIB::hrSystemUptime: Use <a href="#">HOST-RESOURCES-V2-MIB::hrSystemUptime</a>.</li> <li>▪ Use SNMPv2-MIB::sysUpTime: Use <a href="#">SNMPv2-MIB::sysUpTime</a>.</li> <li>▪ Use SNMP-FRAMEWORK-MIB::snmpEngineTime: Use <a href="#">SNMP-FRAMEWORK-MIB::snmpEngineTime</a>.</li> </ul>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)

Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**


Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result: Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.                             <ul style="list-style-type: none"> <li><b>i</b> If you select Store result, the sensor writes the standard error (stderr) streams in clear text to the last sensor result file. Do not return sensitive information via the scripts that you run with this sensor.</li> <li><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</li> </ul> </li> </ul>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
System Uptime	The uptime ⓘ This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

Why does the SNMP System Uptime sensor report wrong values?

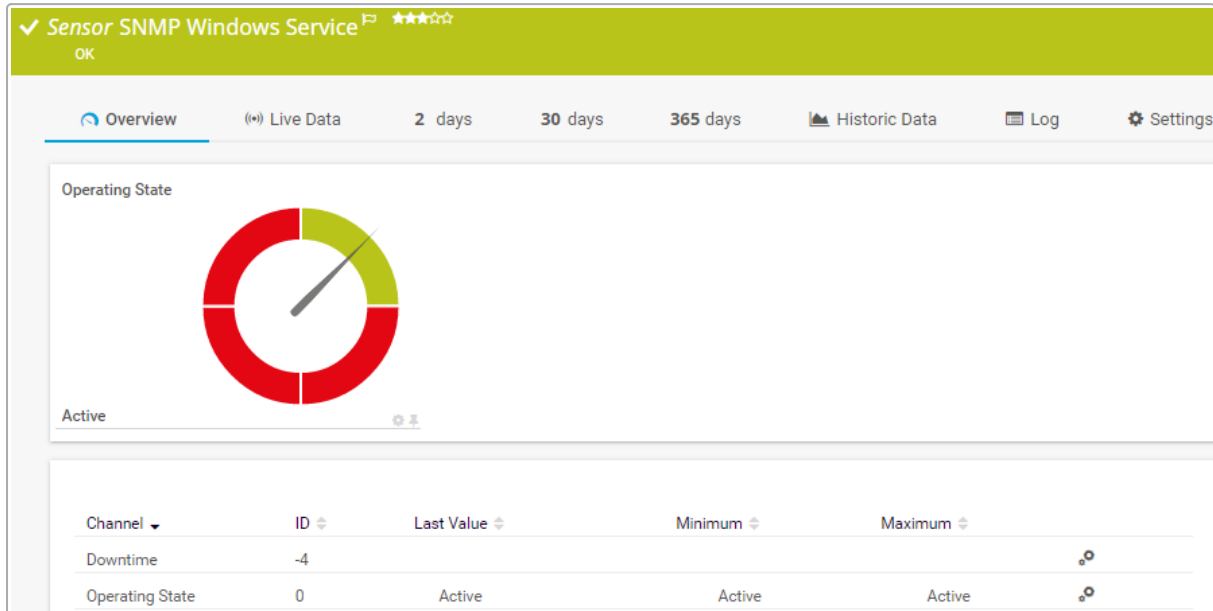
- <https://kb.paessler.com/en/topic/61249>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.241 SNMP Windows Service Sensor

The SNMP Windows Service sensor monitors a Windows service via the Simple Network Management Protocol (SNMP).



SNMP Windows Service Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNMP Windows Service
- French: Windows service (SNMP)
- German: SNMP Windows-Dienst
- Japanese: SNMP Windows サービス
- Portuguese: Serviço Windows (SNMP)
- Russian: Служба Windows по SNMP
- Simplified Chinese: SNMP Windows 服务
- Spanish: Servicio Windows (SNMP)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
"not installed" status	This sensor cannot distinguish the status "not installed" from "not running".

Remark	Description
Localhost	It might not work to query data from a probe device via SNMP (querying <a href="#">localhost</a> , <a href="#">127.0.0.1</a> , or <a href="#">::1</a> ). <a href="#">Add this device</a> with the IP address that it has in your network and create the sensor on this device instead.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- servicesensor
- snmpservicesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### SNMP Windows Service Monitor

#### SNMP Windows Service Monitor

**Service** ⓘ Power

SNMP Windows Service Monitor

Setting	Description
Service	The Windows service that this sensor monitors.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Operating State	The target device operating status <ul style="list-style-type: none"><li>▪ Up status: Active</li><li>▪ Down status: Continue-Pending, Pause-Pending, Paused</li></ul> <p> This channel is the primary channel by default.</p>

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

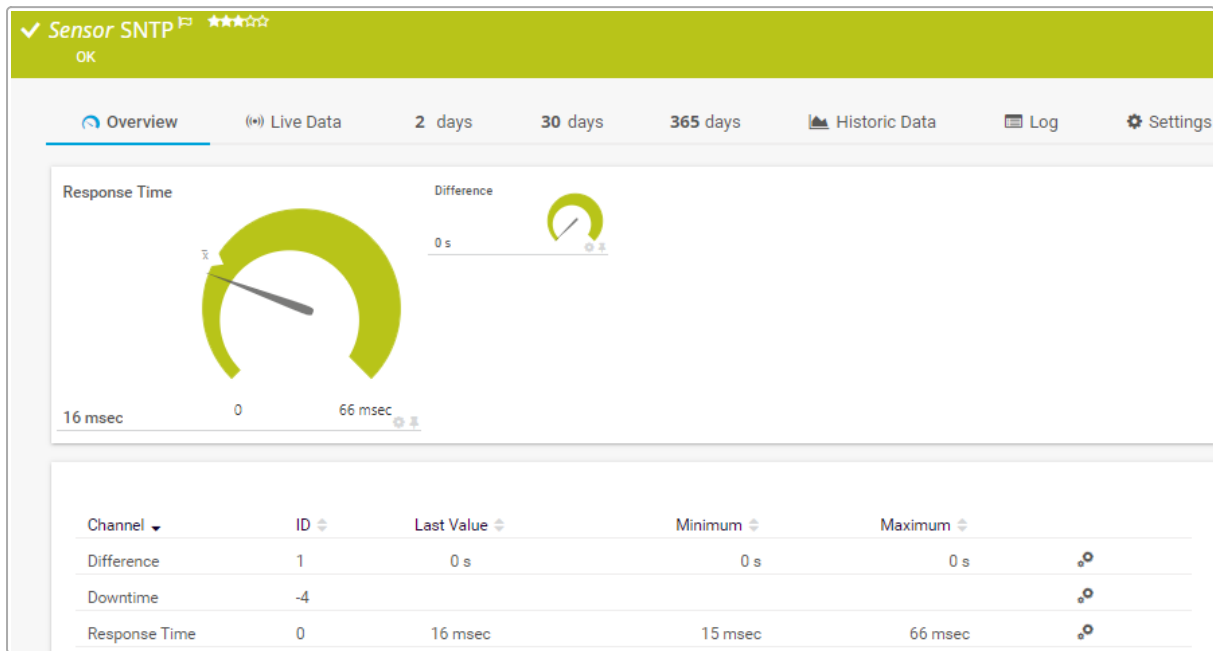
My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

## 7.8.242 SNTP Sensor

The SNTP sensor monitors a Simple Network Time Protocol (SNTP) server.

- ❶ The sensor tries to get a valid time stamp from the server up to three times per scan until it reports an error.



SNTP Sensor

- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SNTP
- French: SNTP
- German: SNTP
- Japanese: SNTP
- Portuguese: SNTP
- Russian: SNTP
- Simplified Chinese: SNTP
- Spanish: SNTP

### Remarks

Consider the following [remarks](#) and requirements for this sensor:



Remark	Description
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>low</b> performance impact.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- sntpsensord

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Specific

#### Sensor Specific

**Timeout (Sec.)** ⓘ 60

Sensor Specific

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p>ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Difference	The time difference in comparison to the local system time
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Response Time	The response time  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

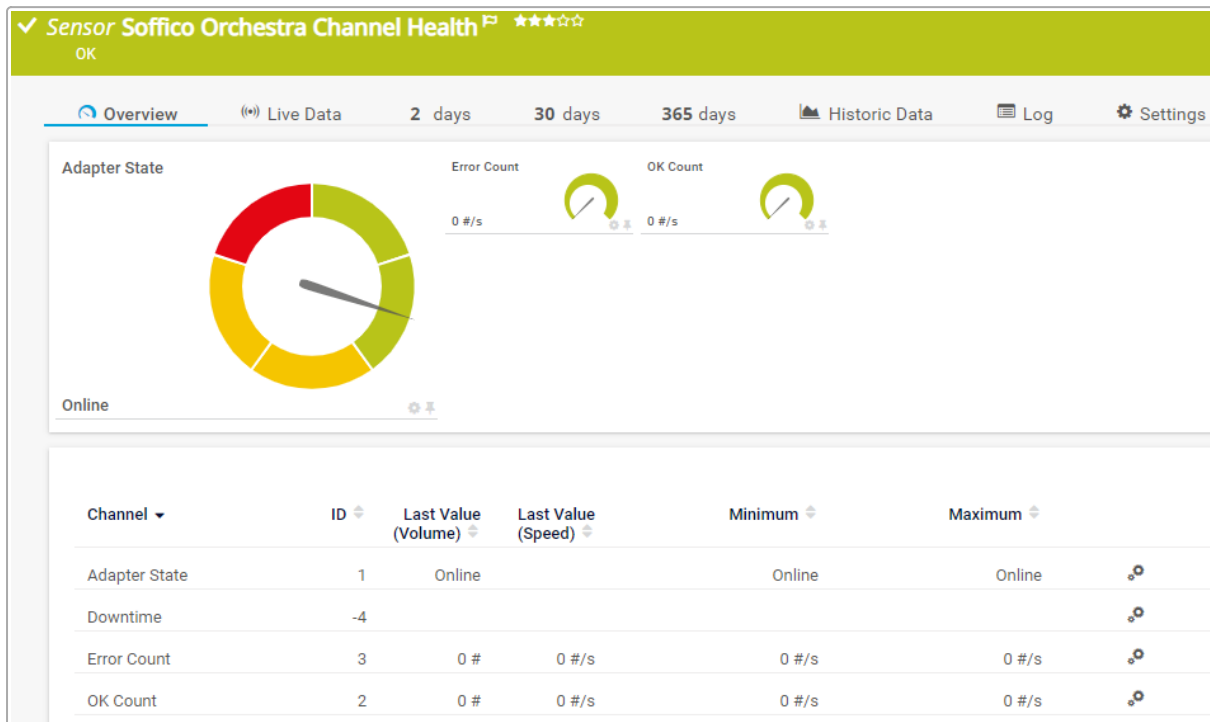
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.243 Soffico Orchestra Channel Health Sensor

The Soffico Orchestra Channel Health sensor monitors the state and the overall number of successful or unsuccessful channel calls.

**i** The sensor supports inbound and outbound channels.



Soffico Orchestra Channel Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>2234</sup>.

### Sensor in Other Languages

- Dutch: Soffico Orchestra Kanaal Gezondheid
- French: Soffico Orchestra état de canal
- German: Soffico Orchestra Channel-Zustand
- Japanese: Soffico Orchestra チャンネルの正常性
- Portuguese: Funcionamento do canal do Soffico Orchestra
- Russian: Работоспособность канала Soffico Orchestra
- Simplified Chinese: Soffico Orchestra 通道运行状况
- Spanish: Salud del canal Orchestra Soffico

### Remarks

Consider the following [remarks](#)<sup>2230</sup> and requirements for this sensor:

Remark	Description
Soffico license and Orchestra version	This sensor requires a Soffico license and as of Orchestra 4.8.2.5.
Credentials	This sensor requires <a href="#">credentials for Soffico Orchestra</a> in the settings of the parent device.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Scanning interval	The recommended scanning interval of this sensor is <a href="#">5 minutes</a> .
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- orchestra
- orchestrachannelhealth
- soffico

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Orchestra Channel Specific

**Orchestra Channel Specific**

**Channel Name** ⓘ *DicomWorklistTest\_ORM/CH\_ORM\_IN*

**Channel Type** ⓘ *MLLP.Inbound*

Orchestra Channel Specific

Setting	Description
Channel Name	The name of the Orchestra channel that this sensor monitors. ⓘ The channel name consists of the Orchestra scenario, a slash, and the Orchestra channel name.
Channel Type	The type of the Orchestra channel that this sensor monitors.

## Sensor Display

**Sensor Display**

**Primary Channel** ⓘ *Downtime*

**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.
Graph Type	Define how this sensor shows different channels: <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a> ).

Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options

**Debug Options**

Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><span style="font-size: 0.8em;">☁</span> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><span style="font-size: 0.8em;">ⓘ</span> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Adapter State	<p>The adapter status</p> <ul style="list-style-type: none"> <li>▪ Up status: Offline, Online</li> <li>▪ Warning status: Not Installed, Unknown</li> <li>▪ Down status: Online With Error</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Error Count	<p>The number of errors</p>
OK Count	<p>The number of OKs</p>

## More

### ■ KNOWLEDGE BASE

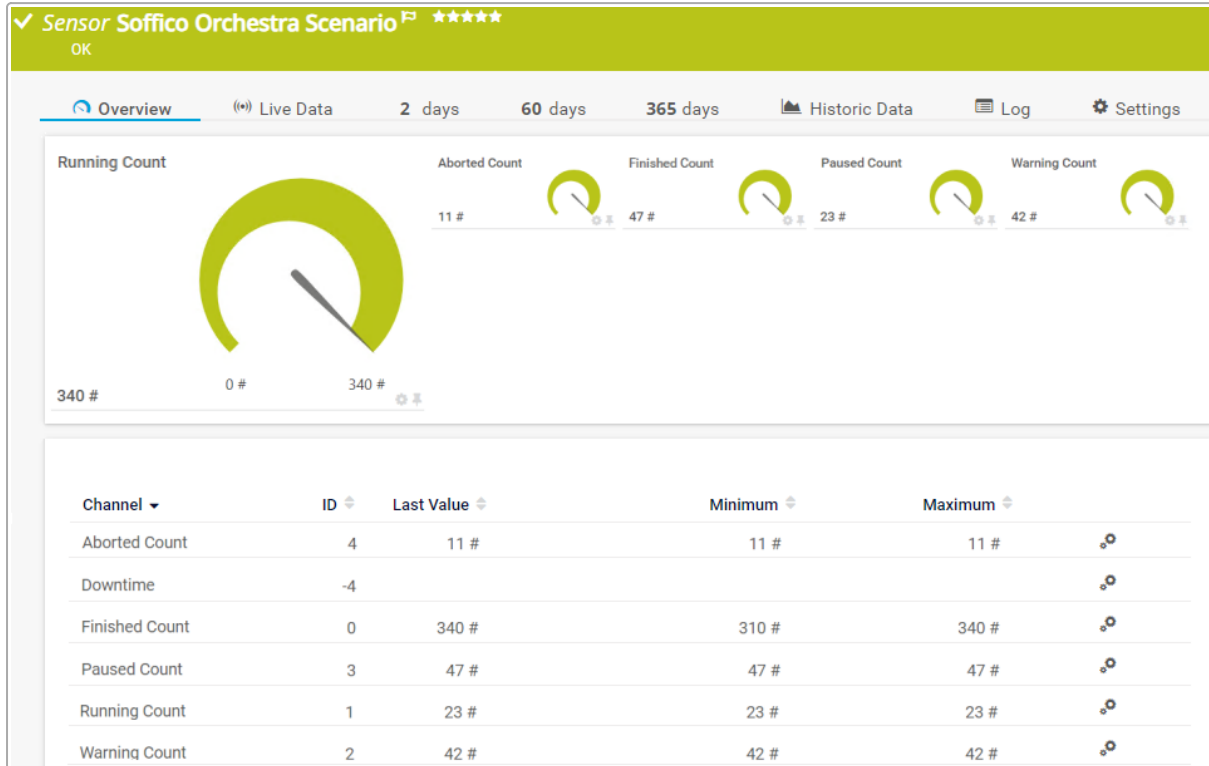
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>



## 7.8.244 Soffico Orchestra Scenario Sensor

The Soffico Orchestra Scenario sensor monitors the status of processes within an Orchestra scenario.



Soffico Orchestra Scenario Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Soffico Orchestra Scenario
- French: Scénario Soffico Orchestra
- German: Soffico Orchestra-Szenario
- Japanese: Soffico Orchestra シナリオ
- Portuguese: Cenário do Soffico Orchestra
- Russian: Сценарий Soffico Orchestra
- Simplified Chinese: Soffico Orchestra 场景
- Spanish: Escenario Soffico Orchestra

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Soffico license and Orchestra version	This sensor requires a Soffico license and as of Orchestra 4.8.2.5.
Credentials	This sensor requires <a href="#">credentials for Soffico Orchestra</a> in the settings of the parent device.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <b>1 minute</b>.</li> <li>▪ The recommended scanning interval of this sensor is <b>1 minute</b>.</li> </ul>
Multi-platform probe	You can add this sensor to a multi-platform probe.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ

**Priority** ⓘ

Example Name

exampletag

✕ +

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- orchestra
- orchestrascenario
- soffico

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Orchestra Scenario Specific

**Orchestra Scenario Specific**

**Base Path** ⓘ */Orchestra/Example Scenario*

**Scenario Name** ⓘ *Example Scenario*

Orchestra Scenario Specific

Setting	Description
Base Path	The base path of the Orchestra scenario that this sensor monitors.
Scenario Name	The name of the Orchestra scenario that this sensor monitors.

## Sensor Display

**Sensor Display**

**Primary Channel** ⓘ Downtime

**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

## Debug Options


**Debug Options**

**Result Handling** ⓘ  Discard result (default)   
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result: Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Aborted Count	The number of aborted processes
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Finished Count	The number of finished processes
Paused Count	The number of paused processes
Running Count	The number of running processes <b>i</b> This channel is the primary channel by default.
Warning Count	The number of processes with a warning status

## More

### ■ KNOWLEDGE BASE

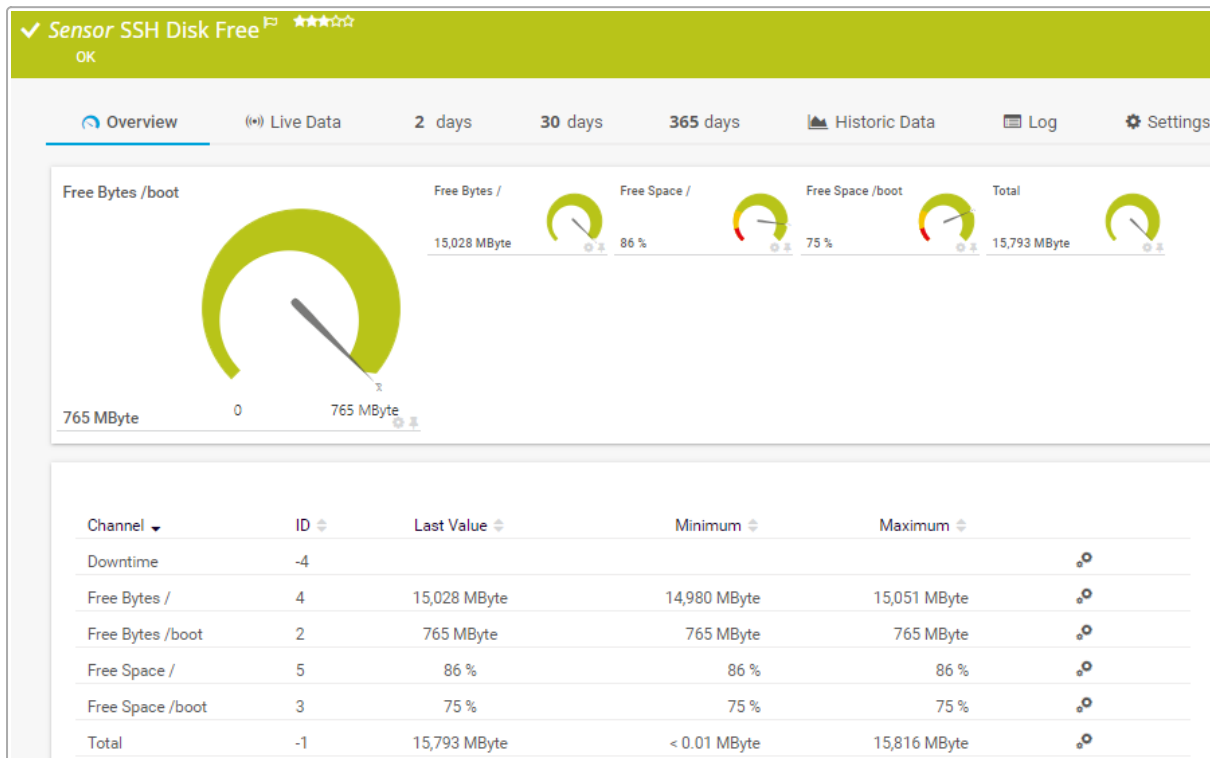
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.245 SSH Disk Free Sensor

The SSH Disk Free sensor monitors the free space on disks of a Linux/Unix system using Secure Shell (SSH).

- ❶ The free space that this sensor returns shows the available disk space of the volume, minus a reserve defined for this volume (for example, for redundancy purposes). So, this sensor shows the disk space that is actually available for use. You can define the size of the reserved disk space with `tune2fs`. For more information, see the Knowledge Base: [Why do SSH Disk Free and SNMP Linux Disk Free show different values for my target Linux system?](#)



SSH Disk Free Sensor

- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) [2248].

### Sensor in Other Languages

- Dutch: SSH Disk vrij
- French: Espace disponible disque (SSH)
- German: SSH Laufwerkskapazität
- Japanese: SSH ディスク空き容量
- Portuguese: Disco livre (SSH)
- Russian: Свободное пространство диска по SSH
- Simplified Chinese: SSH 磁盘可用空间
- Spanish: Espacio libre en disco (SSH)

## Remarks

Consider the following [remarks](#)<sup>[2241]</sup> and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for Linux/Solaris/macOS (SSH/WBEM) systems in the settings of the parent device.
Distributions	This sensor does not support all Linux/Unix and macOS distributions.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
IPv4	This sensor only supports IPv4.
Add Sensor dialog	You can select up to 100 disks in the Add Sensor dialog. If you select more disks, you cannot create the sensor. Add the sensor multiple times to monitor more than 100 disks with several sensors.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">Which encryption algorithms do PRTG SSH sensors support?</a></li> <li>Knowledge Base: <a href="#">SSH and SFTP sensors in Unknown status</a></li> </ul>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ

**Priority** ⓘ

Example Name

exampletag ✕ +

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- diskfreesensor
- sshdiskfreesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## SSH Specific

### SSH Specific

**Connection Timeout (Sec.)** ⓘ 60

---

**Shell Timeout (Sec.)** ⓘ 10

---

**SSH Port Inheritance** ⓘ  Inherit port from parent device (default)  
 Do not inherit port (enter a custom SSH port)





**SSH Engine** ⓘ  Inherit from parent device (default)  
 Default  
 Compatibility mode (deprecated)

**Result Handling** ⓘ  Discard result (default)  
 Store result  
 Store result in case of error

SSH Specific

Setting	Description
Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time that the sensor waits to establish a connection to the host. Keep this value as low as possible. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p>ⓘ Make sure that the connection timeout is a value that is higher than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (for example, <a href="#">cat /proc/loadavg</a>). The maximum value is 300 seconds (5 minutes). Enter an integer.</p> <p>ⓘ Make sure that the shell timeout is a value that is lower than the connection timeout to avoid potential errors.</p>
SSH Port Inheritance	<p>Define which port this sensor uses for the SSH connection:</p> <ul style="list-style-type: none"> <li>▪ Inherit port from parent device (default): Use the port number as defined in the <a href="#">Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems</a> section of the parent device settings.</li> <li>▪ Do not inherit port (enter a custom SSH port): Define a custom port number below and do not use the port number from the parent device settings.</li> </ul>



Setting	Description
Custom SSH Port	<p>This setting is only visible if you select Do not inherit port (enter a custom SSH port) <a href="#">above</a>.</p> <p>Enter the port number (between 1 and 65535) that this sensor uses for the SSH connection. Enter an integer.</p>
SSH Engine	<p>Select the SSH engine that you want to use to <a href="#">access data with this SSH sensor</a>:</p> <ul style="list-style-type: none"> <li>▪ Inherit from parent device (default): Use the SSH engine that you defined in the parent device settings or higher up in the <a href="#">object hierarchy</a>. If you have not changed the SSH engine, this is the recommended option.</li> <li>▪ Default: This is the default SSH engine. It provides the best performance and security. It is set by default in objects that are higher up in the hierarchy, so usually you can keep the Inherit from parent device (default) option.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default SSH engine does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions. It is deprecated. We will remove this legacy mode soon, so try to get your SSH sensors to run with the default SSH engine.</li> </ul> <p> We strongly recommend that you use the default SSH engine.</p> <p> The option you select here overrides the selection of the SSH engine in a higher object: a parent device, group, probe, or root.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID] (SSHv2).txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> <li>▪ Store result in case of error: Store the last sensor result only if the sensor shows the Down status.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Set Limits Checked for ALL Disks

In this section, you can set limits that are valid for all channels and all drives. By entering limits, you can define when the sensor shows the Warning or the Down [status](#), depending on the data provided by all drives that this sensor monitors. If you want to individually define limits for separate channels, use the limit settings in the [channel settings](#).

**i** All limits that you define here are valid in addition to the limits defined in the particular Channel settings. The limits are valid simultaneously, so the first limit that is breached applies.

**Set Limits Checked For ALL Disks** Use the channel settings to set separate error limits or warning limits for each disk.

Percentage Limit Check ?  Only use the limits in the settings of the percentage channels  
 Use the limits of both the sensor and the channel settings (default)

Upper Error Limit ?

Upper Warning Limit ?

Lower Warning Limit ?





Lower Error Limit ?

Size Limit Check ?  Only use the limits in the settings of the byte size channels (default)  
 Use the limits of both the sensor and the channel settings

Alarm on Missing/Removed Disk ?  Deactivate alarm (default)  
 Activate alarm

Set Limits Checked for ALL Disks

Setting	Description
Percentage Limit Check	<p>By default, the sensor enables percentage limits with a lower warning limit and a lower error limit. Enable or disable a limit check for the free space in percentage channels of all drives:</p> <ul style="list-style-type: none"> <li>Only use the limits in the settings of the percentage channels: Do not define sensor limits that are valid for all percentage channels. The sensor only uses the limits that you define in the settings of the particular "free space in percent" channels to determine the status.</li> <li>Use the limits of both the sensor and the channel settings (default): Define sensor limits that are valid for all percentage channels. Additional fields appear below. The sensor shows the Warning or the Down status when free space limits are above or below the limits.</li> </ul>
Upper Error Limit	<p><b>This setting is only visible if you select Use the limits of both the sensor and the channel settings (default) above.</b></p> <p>Specify an upper limit in percent for the Down status. If the free disk space of one of your drives exceeds this value, the sensor changes to the Down status. Enter an integer or leave the field empty.</p>

Setting	Description
	<p> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Upper Warning Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings (default) <a href="#">above</a>.</p> <p>Specify an upper limit in percent for the Warning status. If the free disk space of one of your drives exceeds this value, the sensor changes to the Warning status. Enter an integer or leave the field empty.</p> <p> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Lower Warning Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings (default) <a href="#">above</a>.</p> <p>Specify a lower limit in percent for the Warning status. If the free disk space of one of your drives falls below this value, the sensor changes to the Warning status. Enter an integer or leave the field empty.</p> <p> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Lower Error Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings (default) <a href="#">above</a>.</p> <p>Specify a lower limit in percent for the Down status. If the free disk space of one of your drives falls below this value, the sensor changes to the Down status. Enter an integer or leave the field empty.</p> <p> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Size Limit Check	<p>Enable or disable a limit check for the free bytes channels of all drives:</p> <ul style="list-style-type: none"> <li>▪ Only use the limits in the settings of the byte size channels (default): Do not define sensor limits that are valid for all byte size channels. The sensor only uses limits that you define in the settings of the particular free space in bytes channels to determine the status.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Use the limits of both the sensor and the channel settings: Define limits for the sensor that are valid for all byte size channels. Additional fields appear below. The sensor shows the Warning or Down status when free space limits are above or below the value.</li> </ul> <p><b>i</b> By default, byte size limits are not enabled for drives.</p>
Upper Error Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings <b>above</b>.</p> <p>Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (the default unit is <b>MB</b>). If the free disk space of one of your drives exceeds this value, the sensor changes to the Down status. Enter an integer or leave the field empty.</p> <p><b>i</b> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Upper Warning Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings <b>above</b>.</p> <p>Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (the default unit is <b>MB</b>). If the free disk space of one of your drives exceeds this value, the sensor changes to the Warning status. Enter an integer or leave the field empty.</p> <p><b>i</b> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Lower Warning Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings <b>above</b>.</p> <p>Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (the default unit is <b>MB</b>). If the free disk space of one of your drives falls below this value, the sensor changes to the Warning status. Enter an integer or leave the field empty.</p> <p><b>i</b> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Lower Error Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings <b>above</b>.</p>

Setting	Description
	<p>Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (the default unit is <a href="#">MB</a>). If the free disk space of one of your drives falls below this value, the sensor changes to the Down status. Enter an integer or leave the field empty.</p> <p><b>i</b> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Alarm on Missing/Removed Disk	<p>If a monitored disk is removed or not found, the sensor sets the values to zero. Select the alarm approach in this case:</p> <ul style="list-style-type: none"> <li>▪ Deactivate alarm (default): Do not send an alert for a removed disk.</li> <li>▪ Activate alarm: Send an alert if a monitored disk is removed or not found.</li> </ul>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---


Graph Type ⓘ 
 Show channels independently (default)
   
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>

Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other above.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Bytes [ <a href="#">Mounted Partition</a> ]	The free space
Free Space [ <a href="#">Mounted Partition</a> ]	The free space (%)
Total	The total space

## More

### ■ KNOWLEDGE BASE

Why do SSH Disk Free and SNMP Linux Disk Free show different values for my target Linux system?

- <https://kb.paessler.com/en/topic/43183>

Which encryption algorithms do PRTG SSH sensors support?

- <https://kb.paessler.com/en/topic/90689>

SSH and SFTP sensors in Unknown status

- <https://kb.paessler.com/en/topic/79174>

What security features does PRTG include?

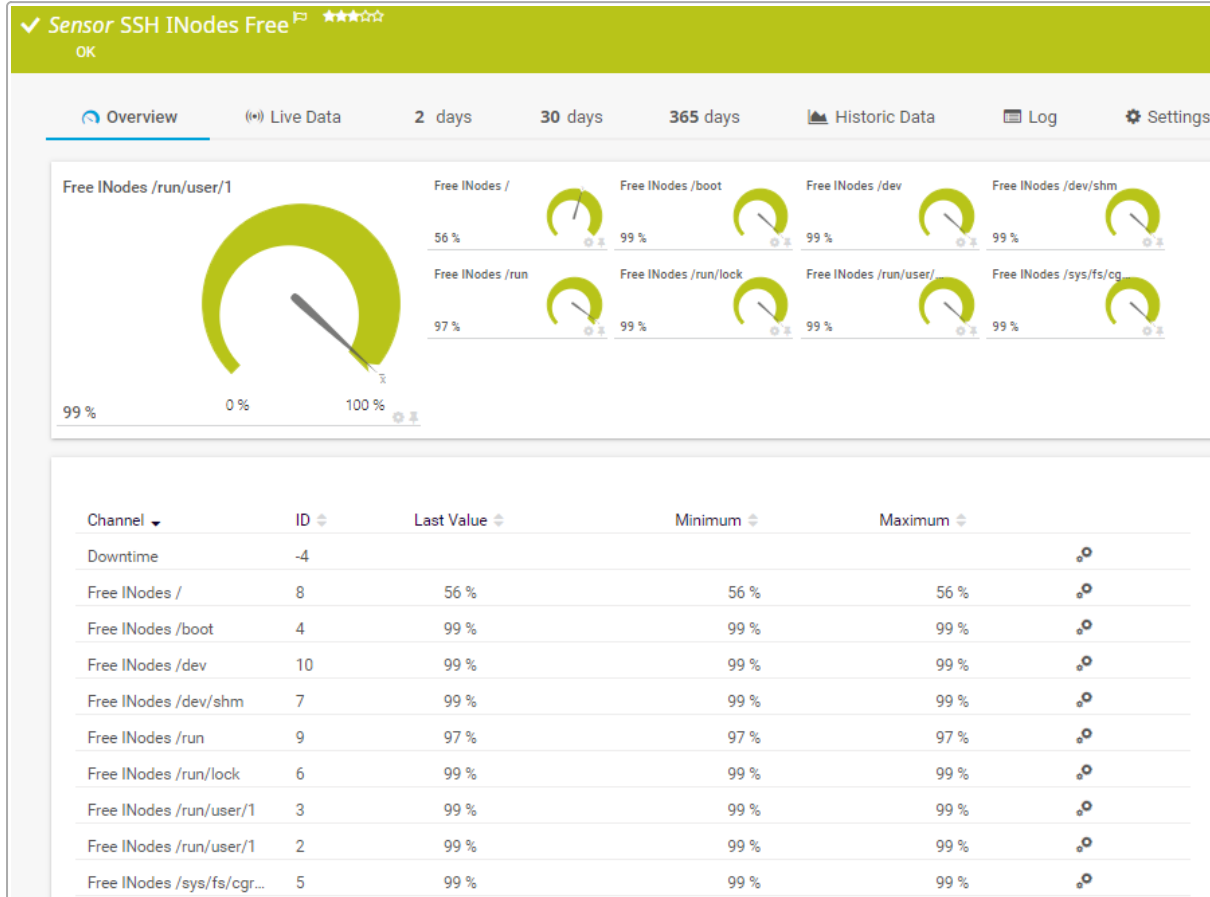
- <https://kb.paessler.com/en/topic/61108>

How do I set up SSH sensors with my AWS Linux instances?

- <https://kb.paessler.com/en/topic/79569>

## 7.8.246 SSH INodes Free Sensor

The SSH INodes Free sensor monitors the free index nodes on disks of Linux/Unix and macOS systems via Secure Shell (SSH).



SSH INodes Free Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) [2254].

### Sensor in Other Languages

- Dutch: SSH INodes Vrij
- French: INodes disponibles (SSH)
- German: SSH Freie INodes
- Japanese: SSH inode の空き領域
- Portuguese: INodes livre (SSH)
- Russian: Свободные узлы INodes по SSH
- Simplified Chinese: SSH INode 可用空间
- Spanish: INodes libres (SSH)



## Remarks

Consider the following [remarks](#)<sup>2251</sup> and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for Linux/Solaris/macOS (SSH/WBEM) systems in the settings of the parent device.
Distributions	This sensor does not support all Linux/Unix and macOS distributions.
ESX(i) hosts	This sensor does not support ESX(i) hosts.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
IPv4	This sensor only supports IPv4.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">Which encryption algorithms do PRTG SSH sensors support?</a></li> <li>Knowledge Base: <a href="#">SSH and SFTP sensors in Unknown status</a></li> </ul>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

**Tags** ⓘ exampletag X +

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- sshinodesfreesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## SSH Specific

**SSH Specific**

Connection Timeout (Sec.) ⓘ 60

---

Shell Timeout (Sec.) ⓘ 10

---





SSH Port Inheritance ⓘ  Inherit port from parent device (default)  
 Do not inherit port (enter a custom SSH port)

SSH Engine ⓘ  Inherit from parent device (default)  
 Default  
 Compatibility mode (deprecated)

Result Handling ⓘ  Discard result (default)  
 Store result  
 Store result in case of error

SSH Specific

Setting	Description
Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time that the sensor waits to establish a connection to the host. Keep this value as low as possible. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p>ⓘ Make sure that the connection timeout is a value that is higher than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (for example, <a href="#">cat /proc/loadavg</a>). The maximum value is 300 seconds (5 minutes). Enter an integer.</p> <p>ⓘ Make sure that the shell timeout is a value that is lower than the connection timeout to avoid potential errors.</p>
SSH Port Inheritance	<p>Define which port this sensor uses for the SSH connection:</p> <ul style="list-style-type: none"> <li>▪ Inherit port from parent device (default): Use the port number as defined in the <a href="#">Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems</a> section of the parent device settings.</li> <li>▪ Do not inherit port (enter a custom SSH port): Define a custom port number below and do not use the port number from the parent device settings.</li> </ul>

Setting	Description
Custom SSH Port	<p>This setting is only visible if you select Do not inherit port (enter a custom SSH port) <a href="#">above</a>.</p> <p>Enter the port number (between 1 and 65535) that this sensor uses for the SSH connection. Enter an integer.</p>
SSH Engine	<p>Select the SSH engine that you want to use to <a href="#">access data with this SSH sensor</a>:</p> <ul style="list-style-type: none"> <li>▪ Inherit from parent device (default): Use the SSH engine that you defined in the parent device settings or higher up in the <a href="#">object hierarchy</a>. If you have not changed the SSH engine, this is the recommended option.</li> <li>▪ Default: This is the default SSH engine. It provides the best performance and security. It is set by default in objects that are higher up in the hierarchy, so usually you can keep the Inherit from parent device (default) option.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default SSH engine does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions. It is deprecated. We will remove this legacy mode soon, so try to get your SSH sensors to run with the default SSH engine.</li> </ul> <p> We strongly recommend that you use the default SSH engine.</p> <p> The option you select here overrides the selection of the SSH engine in a higher object: a parent device, group, probe, or root.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID] (SSHv2).txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> <li>▪ Store result in case of error: Store the last sensor result only if the sensor shows the Down status.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free INodes [ <a href="#">Mount</a> ]	<p>The free index nodes for the mount (%)</p> <p><b>i</b> UNIX file systems only allow a limited number of index nodes. If the limit is exceeded, no more data can be stored, although free space might still be available. This sensor informs you before one of your drives runs out of INodes.</p>

## More

### ■ KNOWLEDGE BASE

Which encryption algorithms do PRTG SSH sensors support?

- <https://kb.paessler.com/en/topic/90689>

SSH and SFTP sensors in Unknown status

- <https://kb.paessler.com/en/topic/79174>

What security features does PRTG include?

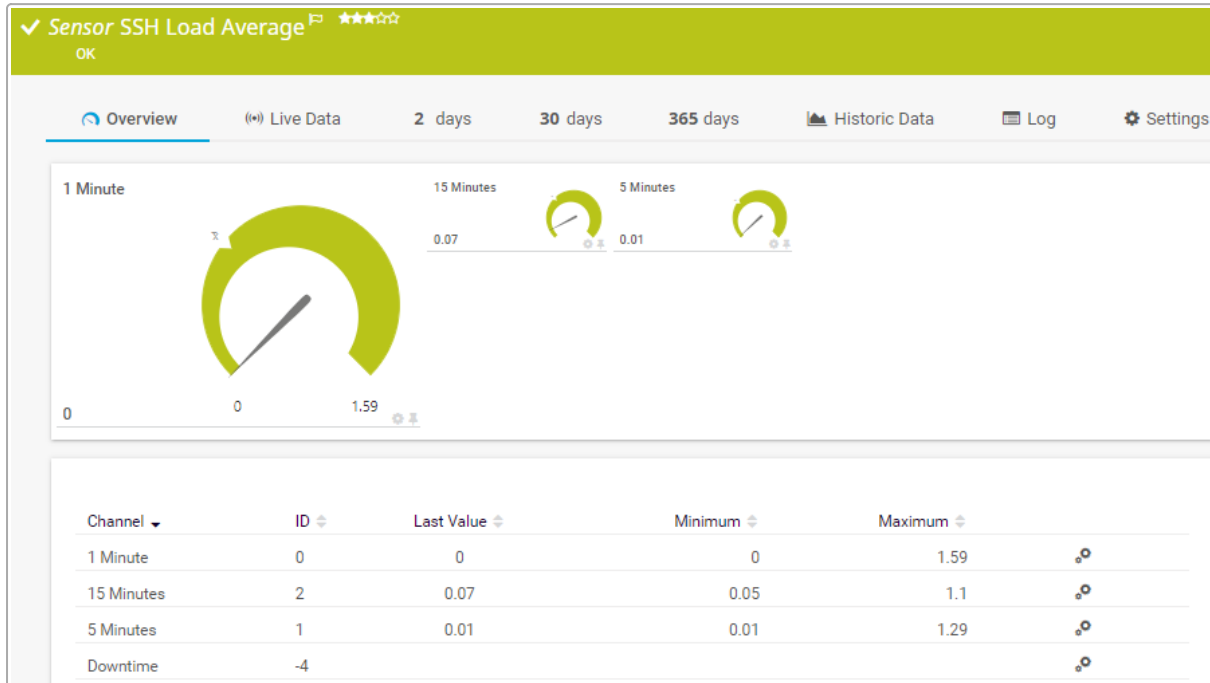
- <https://kb.paessler.com/en/topic/61108>

How do I set up SSH sensors with my AWS Linux instances?

- <https://kb.paessler.com/en/topic/79569>

## 7.8.247 SSH Load Average Sensor

The SSH Load Average sensor monitors the load average of a Linux/Unix system using Secure Shell (SSH).



SSH Load Average Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SSH Gemiddelde belasting
- French: Charge moyenne (SSH)
- German: SSH Durchschnittliche Last
- Japanese: SSH 負荷平均
- Portuguese: Carga média (SSH)
- Russian: Средняя загрузка по SSH
- Simplified Chinese: SSH 负载平均值
- Spanish: Promedio de carga (SSH)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for Linux/Solaris/macOS (SSH/WBEM) systems in the settings of the parent device.
Distributions	This sensor does not support all Linux/Unix and macOS distributions.
Performance impact	This sensor has a <b>medium</b> performance impact.
IPv4	This sensor only supports IPv4.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">Which encryption algorithms do PRTG SSH sensors support?</a></li> <li>Knowledge Base: <a href="#">SSH and SFTP sensors in Unknown status</a></li> </ul>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- sshloadavgsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## SSH Specific

**SSH Specific**

Connection Timeout (Sec.) ⓘ 60

---

Shell Timeout (Sec.) ⓘ 10

---

SSH Port Inheritance ⓘ  Inherit port from parent device (default)  
 Do not inherit port (enter a custom SSH port)





SSH Engine ⓘ  Inherit from parent device (default)  
 Default  
 Compatibility mode (deprecated)

Result Handling ⓘ  Discard result (default)  
 Store result  
 Store result in case of error

SSH Specific

Setting	Description
Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time that the sensor waits to establish a connection to the host. Keep this value as low as possible. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p> ⓘ Make sure that the connection timeout is a value that is higher than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (for example, <a href="#">cat /proc/loadavg</a>). The maximum value is 300 seconds (5 minutes). Enter an integer.</p> <p> ⓘ Make sure that the shell timeout is a value that is lower than the connection timeout to avoid potential errors.</p>
SSH Port Inheritance	<p>Define which port this sensor uses for the SSH connection:</p> <ul style="list-style-type: none"> <li>▪ Inherit port from parent device (default): Use the port number as defined in the <a href="#">Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems</a> section of the parent device settings.</li> <li>▪ Do not inherit port (enter a custom SSH port): Define a custom port number below and do not use the port number from the parent device settings.</li> </ul>



Setting	Description
Custom SSH Port	<p>This setting is only visible if you select Do not inherit port (enter a custom SSH port) <a href="#">above</a>.</p> <p>Enter the port number (between 1 and 65535) that this sensor uses for the SSH connection. Enter an integer.</p>
SSH Engine	<p>Select the SSH engine that you want to use to <a href="#">access data with this SSH sensor</a>:</p> <ul style="list-style-type: none"> <li>▪ Inherit from parent device (default): Use the SSH engine that you defined in the parent device settings or higher up in the <a href="#">object hierarchy</a>. If you have not changed the SSH engine, this is the recommended option.</li> <li>▪ Default: This is the default SSH engine. It provides the best performance and security. It is set by default in objects that are higher up in the hierarchy, so usually you can keep the Inherit from parent device (default) option.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default SSH engine does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions. It is deprecated. We will remove this legacy mode soon, so try to get your SSH sensors to run with the default SSH engine.</li> </ul> <p> We strongly recommend that you use the default SSH engine.</p> <p> The option you select here overrides the selection of the SSH engine in a higher object: a parent device, group, probe, or root.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID] (SSHv2).txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> <li>▪ Store result in case of error: Store the last sensor result only if the sensor shows the Down status.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
1 Minute	The average system load within a 1-minute interval <i>i</i> This channel is the primary channel by default.
5 Minutes	The average system load within a 5-minute scanning interval
15 Minutes	The average system load within a 15-minute interval
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

## More

### ■ KNOWLEDGE BASE

Which encryption algorithms do PRTG SSH sensors support?

- <https://kb.paessler.com/en/topic/90689>

SSH and SFTP sensors in Unknown status

- <https://kb.paessler.com/en/topic/79174>

What security features does PRTG include?

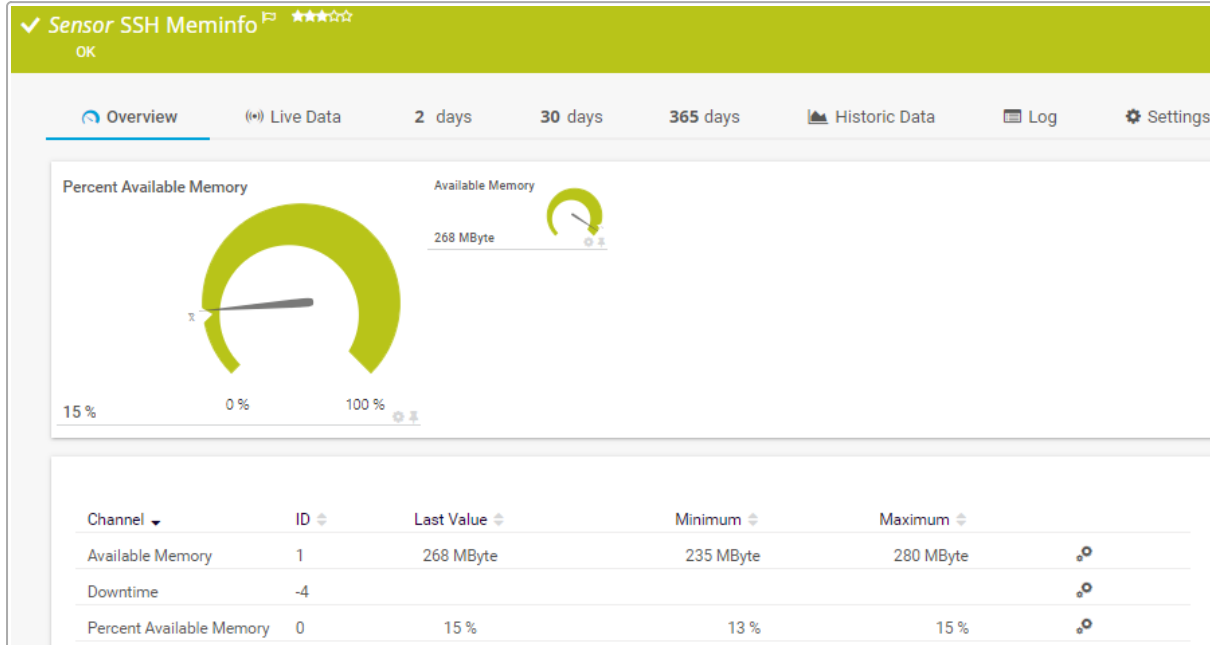
- <https://kb.paessler.com/en/topic/61108>

How do I set up SSH sensors with my AWS Linux instances?

- <https://kb.paessler.com/en/topic/79569>

## 7.8.248 SSH Meminfo Sensor

The SSH Meminfo sensor monitors the memory usage of a Linux/Unix system using Secure Shell (SSH).



SSH Meminfo Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SSH Meminfo
- French: Information mémoire (SSH)
- German: SSH Speicherinfo
- Japanese: SSH メモリ情報
- Portuguese: Meminfo (SSH)
- Russian: Meminfo no SSH
- Simplified Chinese: SSH 内存信息
- Spanish: Meminfo (SSH)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Credentials	This sensor requires credentials for Linux/Solaris/macOS (SSH/WBEM) systems in the settings of the parent device.
Distributions	<ul style="list-style-type: none"> <li>▪ This sensor does not support all Linux/Unix distributions.</li> <li>▪ This sensor does not support any macOS distributions.</li> </ul>
Performance impact	This sensor has a <b>medium</b> performance impact.
IPv4	This sensor only supports IPv4.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">Which encryption algorithms do PRTG SSH sensors support?</a></li> <li>▪ Knowledge Base: <a href="#">SSH and SFTP sensors in Unknown status</a></li> </ul>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag X +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- memorysensor
- sshmeminfosensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## SSH Specific

**SSH Specific**

Connection Timeout (Sec.) ⓘ 60

---

Shell Timeout (Sec.) ⓘ 10

---





SSH Port Inheritance ⓘ  Inherit port from parent device (default)  
 Do not inherit port (enter a custom SSH port)

SSH Engine ⓘ  Inherit from parent device (default)  
 Default  
 Compatibility mode (deprecated)

Result Handling ⓘ  Discard result (default)  
 Store result  
 Store result in case of error

SSH Specific

Setting	Description
Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time that the sensor waits to establish a connection to the host. Keep this value as low as possible. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p>ⓘ Make sure that the connection timeout is a value that is higher than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (for example, <a href="#">cat /proc/loadavg</a>). The maximum value is 300 seconds (5 minutes). Enter an integer.</p> <p>ⓘ Make sure that the shell timeout is a value that is lower than the connection timeout to avoid potential errors.</p>
SSH Port Inheritance	<p>Define which port this sensor uses for the SSH connection:</p> <ul style="list-style-type: none"> <li>▪ Inherit port from parent device (default): Use the port number as defined in the <a href="#">Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems</a> section of the parent device settings.</li> <li>▪ Do not inherit port (enter a custom SSH port): Define a custom port number below and do not use the port number from the parent device settings.</li> </ul>

Setting	Description
Custom SSH Port	<p>This setting is only visible if you select Do not inherit port (enter a custom SSH port) <a href="#">above</a>.</p> <p>Enter the port number (between 1 and 65535) that this sensor uses for the SSH connection. Enter an integer.</p>
SSH Engine	<p>Select the SSH engine that you want to use to <a href="#">access data with this SSH sensor</a>:</p> <ul style="list-style-type: none"> <li>▪ Inherit from parent device (default): Use the SSH engine that you defined in the parent device settings or higher up in the <a href="#">object hierarchy</a>. If you have not changed the SSH engine, this is the recommended option.</li> <li>▪ Default: This is the default SSH engine. It provides the best performance and security. It is set by default in objects that are higher up in the hierarchy, so usually you can keep the Inherit from parent device (default) option.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default SSH engine does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions. It is deprecated. We will remove this legacy mode soon, so try to get your SSH sensors to run with the default SSH engine.</li> </ul> <p> We strongly recommend that you use the default SSH engine.</p> <p> The option you select here overrides the selection of the SSH engine in a higher object: a parent device, group, probe, or root.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID] (SSHv2).txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> <li>▪ Store result in case of error: Store the last sensor result only if the sensor shows the Down status.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.



Channel	Description
Available Memory	The available memory
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Percent Available Memory	The available memory (%) <b>i</b> This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

Which encryption algorithms do PRTG SSH sensors support?

- <https://kb.paessler.com/en/topic/90689>

SSH and SFTP sensors in Unknown status

- <https://kb.paessler.com/en/topic/79174>

What security features does PRTG include?

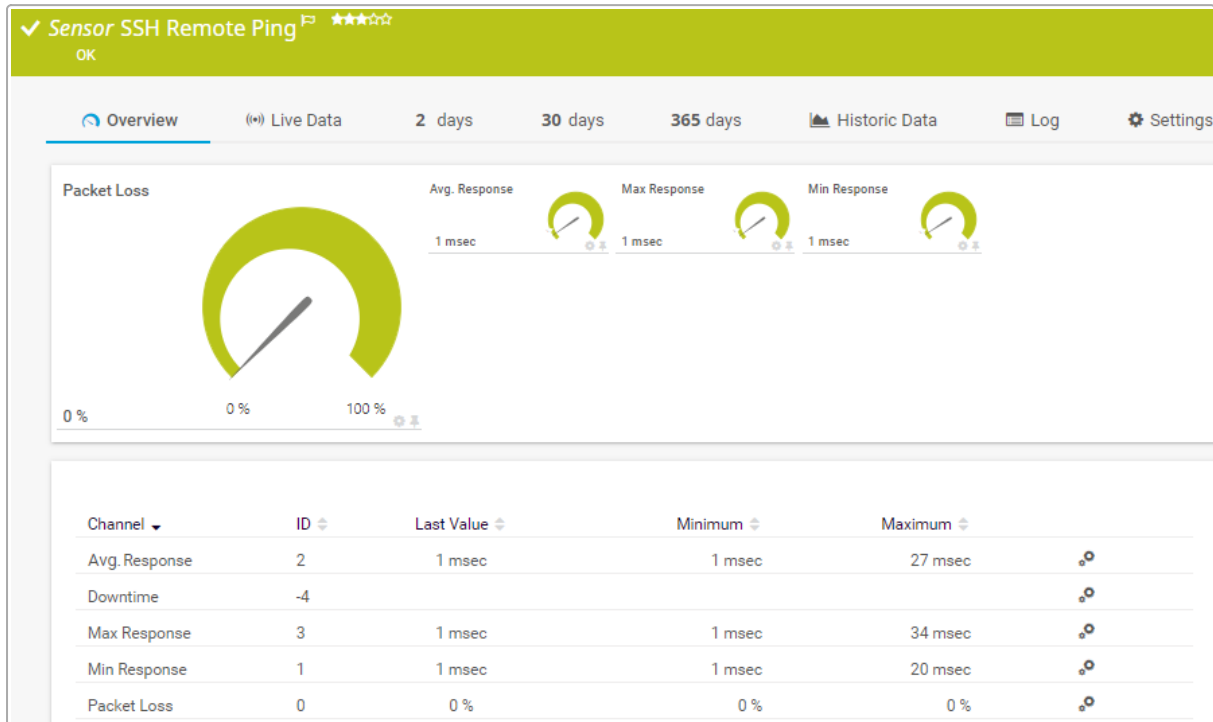
- <https://kb.paessler.com/en/topic/61108>

How do I set up SSH sensors with my AWS Linux instances?

- <https://kb.paessler.com/en/topic/79569>

## 7.8.249 SSH Remote Ping Sensor

The SSH Remote Ping sensor remotely monitors the connectivity between a system running Linux/macOS X and another device, using Internet Control Message Protocol (ICMP) echo requests ("ping") and Secure Shell (SSH).



SSH Remote Ping Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>2273</sup>.

### Sensor in Other Languages

- Dutch: SSH Remote Ping
- French: Ping distant (SSH)
- German: SSH Remote Ping
- Japanese: SSH リモート Ping 実行
- Portuguese: Ping remoto (SSH)
- Russian: Удаленный пинг по SSH
- Simplified Chinese: SSH 远程 Ping
- Spanish: Ping remoto (SSH)

### Remarks

Consider the following [remarks](#)<sup>2268</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <b>high</b> performance impact. We recommend that you use no more than <b>200</b> of this sensor on each probe.
Credentials	This sensor requires credentials for Linux/Solaris/macOS (SSH/WBEM) systems in the settings of the parent device.
Distributions	This sensor does not support all Linux/Unix and macOS distributions.
IPv4	This sensor only supports IPv4.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">Which encryption algorithms do PRTG SSH sensors support?</a></li> <li>Knowledge Base: <a href="#">SSH and SFTP sensors in Unknown status</a></li> </ul>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  x +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- pingsensor
- remotepingsensor
- sshremotepingsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## SSH Remote Ping Configuration

SSH Remote Ping Configuration	Target ⓘ	192.0.2.0
	Packet Size (Bytes) ⓘ	32
	Packet Count ⓘ	2
	Custom Parameters ⓘ	

SSH Remote Ping Configuration

Setting	Description
Target	Enter the Domain Name System (DNS) name or IP address of the target device the ping is sent to. The sensor remotely connects to the parent device it is created on via SSH, then performs a ping request from this remote device to the target device or server. Enter a string.
Packet Size (Bytes)	Enter the packet size for the ping in bytes. You can enter any value between 1 and 10000. Enter an integer.  ⓘ We recommend that you use the default value.
Packet Count	Enter the number of packets that the sensor sends with each scanning interval.
Custom Parameter	Optionally, enter additional parameters that the sensor adds at the end of the ping command. Enter a string or leave the field empty.  ⓘ Do not use parameters that change the output format of the result to make sure that it can still be parsed. You cannot enter an additional command.

## SSH Specific

**SSH Specific**

Connection Timeout (Sec.) ⓘ 60

---

Shell Timeout (Sec.) ⓘ 10

---





SSH Port Inheritance ⓘ  Inherit port from parent device (default)  
 Do not inherit port (enter a custom SSH port)

SSH Engine ⓘ  Inherit from parent device (default)  
 Default  
 Compatibility mode (deprecated)

Result Handling ⓘ  Discard result (default)  
 Store result  
 Store result in case of error

SSH Specific

Setting	Description
Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time that the sensor waits to establish a connection to the host. Keep this value as low as possible. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p> ⓘ Make sure that the connection timeout is a value that is higher than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (for example, <a href="#">cat /proc/loadavg</a>). The maximum value is 300 seconds (5 minutes). Enter an integer.</p> <p> ⓘ Make sure that the shell timeout is a value that is lower than the connection timeout to avoid potential errors.</p>
SSH Port Inheritance	<p>Define which port this sensor uses for the SSH connection:</p> <ul style="list-style-type: none"> <li>▪ Inherit port from parent device (default): Use the port number as defined in the <a href="#">Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems</a> section of the parent device settings.</li> <li>▪ Do not inherit port (enter a custom SSH port): Define a custom port number below and do not use the port number from the parent device settings.</li> </ul>

Setting	Description
Custom SSH Port	<p>This setting is only visible if you select Do not inherit port (enter a custom SSH port) <a href="#">above</a>.</p> <p>Enter the port number (between 1 and 65535) that this sensor uses for the SSH connection. Enter an integer.</p>
SSH Engine	<p>Select the SSH engine that you want to use to <a href="#">access data with this SSH sensor</a>:</p> <ul style="list-style-type: none"> <li>▪ Inherit from parent device (default): Use the SSH engine that you defined in the parent device settings or higher up in the <a href="#">object hierarchy</a>. If you have not changed the SSH engine, this is the recommended option.</li> <li>▪ Default: This is the default SSH engine. It provides the best performance and security. It is set by default in objects that are higher up in the hierarchy, so usually you can keep the Inherit from parent device (default) option.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default SSH engine does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions. It is deprecated. We will remove this legacy mode soon, so try to get your SSH sensors to run with the default SSH engine.</li> </ul> <p> We strongly recommend that you use the default SSH engine.</p> <p> The option you select here overrides the selection of the SSH engine in a higher object: a parent device, group, probe, or root.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID] (SSHv2).txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> <li>▪ Store result in case of error: Store the last sensor result only if the sensor shows the Down status.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Avg. Response	The average response time measured from the remote device
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Max Response	The maximum response time measured from the remote device
Min Response	The minimum response time measured from the remote device
Packet Loss	The packet loss (%)   This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

Which encryption algorithms do PRTG SSH sensors support?

- <https://kb.paessler.com/en/topic/90689>

SSH and SFTP sensors in Unknown status

- <https://kb.paessler.com/en/topic/79174>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How do I set up SSH sensors with my AWS Linux instances?

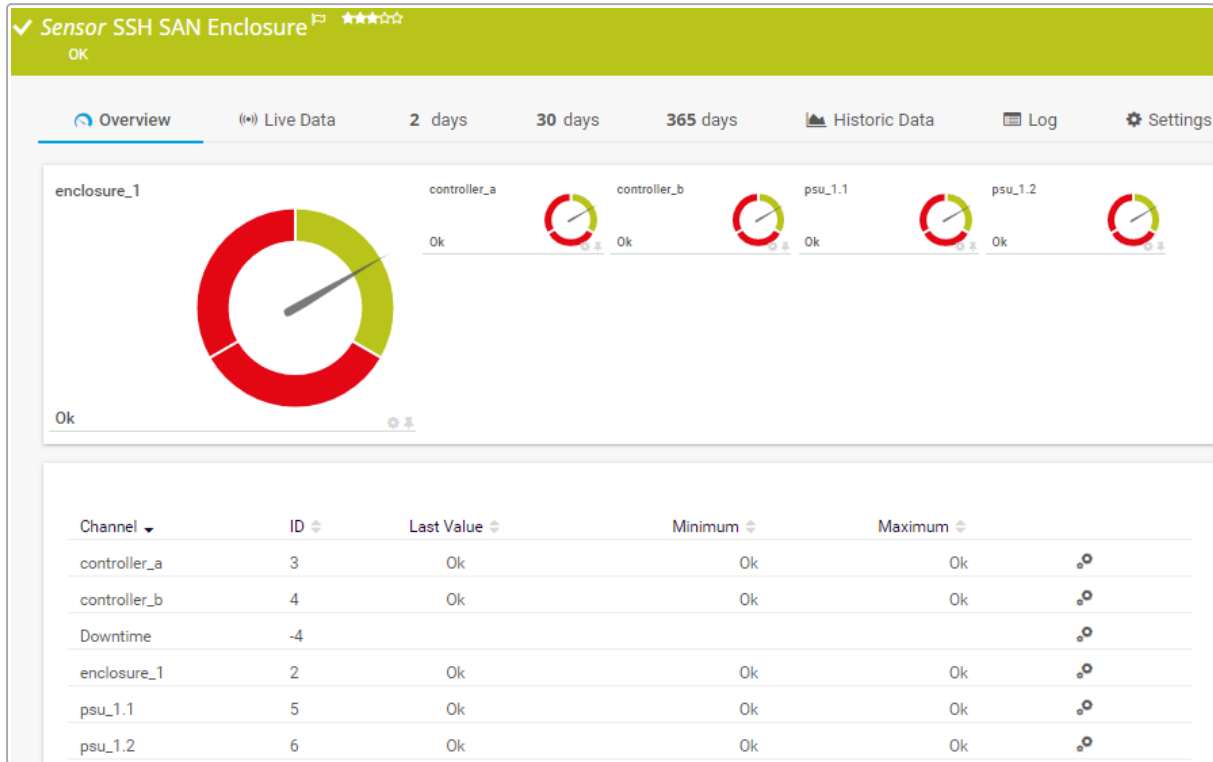
- <https://kb.paessler.com/en/topic/79569>



## 7.8.250 SSH SAN Enclosure Sensor

The SSH SAN Enclosure sensor monitors a storage area network (SAN) enclosure via Secure Shell (SSH).

**i** The SAN must provide a command-line interface (CLI) for this purpose.



SSH SAN Enclosure Sensor

■ For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>2280</sup>.

### Sensor in Other Languages

- Dutch: SSH SAN behuizing
- French: SAN boîtier (SSH)
- German: SSH SAN Enclosure
- Japanese: SSH SAN エンクロージャ
- Portuguese: Gabinete SAN (SSH)
- Russian: Корпус SAN по SSH
- Simplified Chinese: SSH SAN 机箱
- Spanish: Gabinete SAN (SSH)

### Remarks

Consider the following [remarks](#)<sup>2278</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Credentials	This sensor requires <a href="#">credentials for Linux/Solaris/macOS (SSH/WBEM) systems</a> in the settings of the parent device.
SAN support	This sensor does not support every SAN, even if it provides a CLI. This sensor only works with specific devices, for example, the <a href="#">HPE P2000</a> .
Scanning interval	If the controller of the target system breaks down, increase the scanning interval to discharge the controller and try again.
Firmware update	After a firmware update of the target system, this sensor might show incorrect channel values. Add this sensor anew in this case.
IPv4	This sensor only supports IPv4.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Device status	Sometimes the devices you monitor with this sensor return status values that are not officially documented so that the shown sensor status in PRTG differs from the "real" device status. For more information, see the Knowledge Base: <a href="#">Why does my SSH SAN sensor show a wrong status?</a>
Knowledge Base	Knowledge Base: <a href="#">Which encryption algorithms do PRTG SSH sensors support?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- enclosure

- sshsan
- sshsanenclosure

For more information about basic sensor settings, see section [Sensor Settings](#).

### SSH SAN Enclosure Settings

#### SSH SAN Enclosure Settings

Storage Enclosure ⓘ 0

Durable ID ⓘ

Name ⓘ

WWN ⓘ

SSH SAN Enclosure Settings

Setting	Description
Storage Enclosure	The identifier of the storage enclosure that this sensor monitors.
Durable ID	The durable identifier of the storage enclosure that this sensor monitors.
Name	The name of the storage enclosure that this sensor monitors.
WWN	The World Wide Name (WWN) of the storage enclosure that this sensor monitors.

## SSH Specific

**SSH Specific**

Connection Timeout (Sec.) ⓘ 60

---

Shell Timeout (Sec.) ⓘ 10

---





SSH Port Inheritance ⓘ  Inherit port from parent device (default)  
 Do not inherit port (enter a custom SSH port)

SSH Engine ⓘ  Inherit from parent device (default)  
 Default  
 Compatibility mode (deprecated)

Result Handling ⓘ  Discard result (default)  
 Store result  
 Store result in case of error

SSH Specific

Setting	Description
Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time that the sensor waits to establish a connection to the host. Keep this value as low as possible. Enter an integer.</p> <p>ⓘ This sensor has a fixed timeout of 300 seconds. If you change the value, it does not have an effect on the timeout.</p> <p>ⓘ Make sure that the connection timeout is a value that is higher than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (for example, <code>cat /proc/loadavg</code>). The maximum value is 300 seconds (5 minutes). Enter an integer.</p> <p>ⓘ This sensor has a fixed timeout of 300 seconds. If you change the value, it does not have an effect on the timeout.</p> <p>ⓘ Make sure that the shell timeout is a value that is lower than the connection timeout to avoid potential errors.</p>
SSH Port Inheritance	<p>Define which port this sensor uses for the SSH connection:</p> <ul style="list-style-type: none"> <li>Inherit port from parent device (default): Use the port number as defined in the <a href="#">Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems</a> section of the parent device settings.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Do not inherit port (enter a custom SSH port): Define a custom port number below and do not use the port number from the parent device settings.</li> </ul>
Custom SSH Port	<p>This setting is only visible if you select Do not inherit port (enter a custom SSH port) <a href="#">above</a>.</p> <p>Enter the port number (between 1 and 65535) that this sensor uses for the SSH connection. Enter an integer.</p>
SSH Engine	<p>Select the SSH engine that you want to use to <a href="#">access data with this SSH sensor</a>:</p> <ul style="list-style-type: none"> <li>Inherit from parent device (default): Use the SSH engine that you defined in the parent device settings or higher up in the <a href="#">object hierarchy</a>. If you have not changed the SSH engine, this is the recommended option.</li> <li>Default: This is the default SSH engine. It provides the best performance and security. It is set by default in objects that are higher up in the hierarchy, so usually you can keep the Inherit from parent device (default) option.</li> <li>Compatibility mode (deprecated): Use this only if the default SSH engine does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions. It is deprecated. We will remove this legacy mode soon, so try to get your SSH sensors to run with the default SSH engine.</li> </ul> <p> We strongly recommend that you use the default SSH engine.</p> <p> The option you select here overrides the selection of the SSH engine in a higher object: a parent device, group, probe, or root.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID] (SSHv2).txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> <li>Store result in case of error: Store the last sensor result only if the sensor shows the Down status.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Controller[#]	<p>The controller status</p> <ul style="list-style-type: none"> <li>▪ Up status: Ok</li> <li>▪ Down status: Fault, Not Available</li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Enclosure[#]	<p>The overall enclosure status</p> <ul style="list-style-type: none"> <li>▪ Up status: Ok</li> <li>▪ Down status: Fault, Not Available</li> </ul> <p> This channel is the primary channel by default.</p>
PSU[#]	<p>The power supplies status</p> <ul style="list-style-type: none"> <li>▪ Up status: Ok</li> <li>▪ Down status: Fault, Not Available</li> </ul>

## More

### KNOWLEDGE BASE

Which encryption algorithms do PRTG SSH sensors support?

- <https://kb.paessler.com/en/topic/90689>

Why does my SSH SAN sensor show a wrong status?

- <https://kb.paessler.com/en/topic/60145>

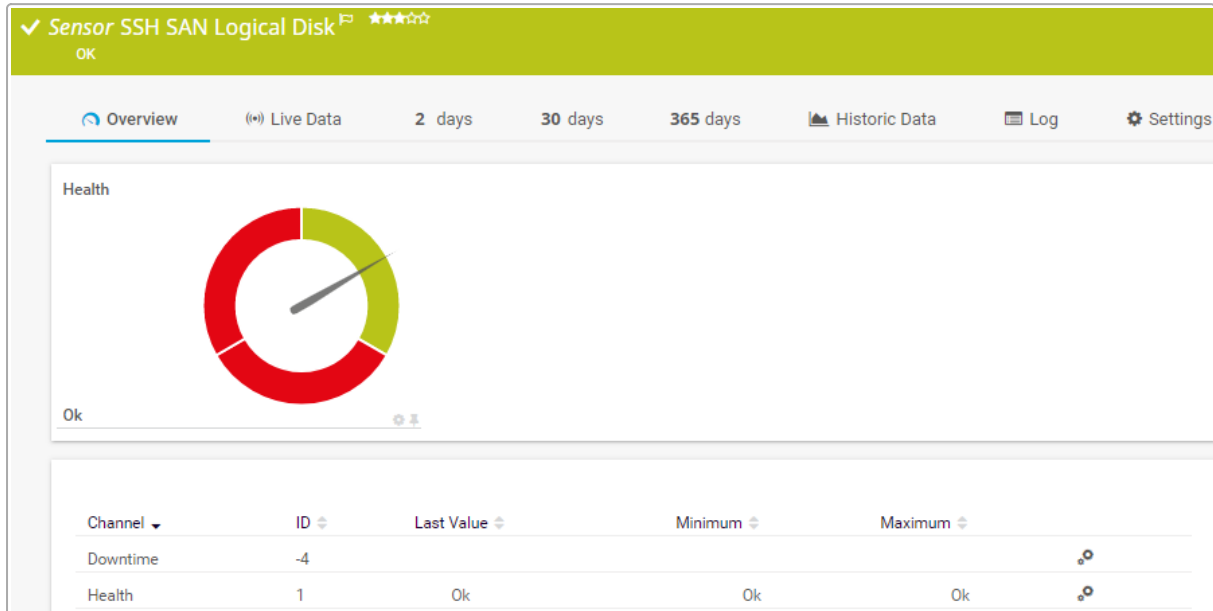
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.251 SSH SAN Logical Disk Sensor

The SSH SAN Logical Disk sensor monitors a logical disk on a storage area network (SAN) via Secure Shell (SSH).

**i** The SAN must provide a command-line interface (CLI) for this purpose.



SSH SAN Logical Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SSH SAN Logische Schijf
- French: SAN disque logique (SSH)
- German: SSH SAN Logisches Laufwerk
- Japanese: SSH SAN 論理ディスク
- Portuguese: Disco lógico SAN (SSH)
- Russian: Логический диск SAN по SSH
- Simplified Chinese: SSH SAN 逻辑磁盘
- Spanish: Disco lógico SAN (SSH)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:



Remark	Description
Credentials	This sensor requires <a href="#">credentials for Linux/Solaris/macOS (SSH/WBEM) systems</a> in the settings of the parent device.
SAN support	This sensor does not support every SAN, even if it provides a CLI. This sensor only works with specific devices, for example, the <a href="#">HPE P2000</a> .
Scanning interval	If the controller of the target system breaks down, increase the scanning interval to discharge the controller and try again.
Firmware update	After a firmware update of the target system, this sensor might show incorrect channel values. Add this sensor anew in this case.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
IPv4	This sensor only supports IPv4.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Device status	Sometimes the devices you monitor with this sensor return status values that are not officially documented so that the shown sensor status in PRTG differs from the "real" device status. For more information, see the Knowledge Base: <a href="#">Why does my SSH SAN sensor show a wrong status?</a>
Knowledge Base	Knowledge Base: <a href="#">Which encryption algorithms do PRTG SSH sensors support?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- logicaldisk
- sshsan

- sshsanlogicaldisk

For more information about basic sensor settings, see section [Sensor Settings](#) [667].

## SSH Specific

**SSH Specific**

Connection Timeout (Sec.) ⓘ 60

---

Shell Timeout (Sec.) ⓘ 10

---




SSH Port Inheritance ⓘ  Inherit port from parent device (default)  
 Do not inherit port (enter a custom SSH port)

SSH Engine ⓘ  Inherit from parent device (default)  
 Default  
 Compatibility mode (deprecated)

Result Handling ⓘ  Discard result (default)  
 Store result  
 Store result in case of error

SSH Specific

Setting	Description
Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time that the sensor waits to establish a connection to the host. Keep this value as low as possible. Enter an integer.</p> <p> ⓘ This sensor has a fixed timeout of 300 seconds. If you change the value, it does not have an effect on the timeout.</p> <p> ⓘ Make sure that the connection timeout is a value that is higher than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (for example, <code>cat /proc/loadavg</code>). The maximum value is 300 seconds (5 minutes). Enter an integer.</p> <p> ⓘ This sensor has a fixed timeout of 300 seconds. If you change the value, it does not have an effect on the timeout.</p> <p> ⓘ Make sure that the shell timeout is a value that is lower than the connection timeout to avoid potential errors.</p>
SSH Port Inheritance	Define which port this sensor uses for the SSH connection:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Inherit port from parent device (default): Use the port number as defined in the <a href="#">Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems</a> section of the parent device settings.</li> <li>▪ Do not inherit port (enter a custom SSH port): Define a custom port number below and do not use the port number from the parent device settings.</li> </ul>
Custom SSH Port	<p><b>This setting is only visible if you select Do not inherit port (enter a custom SSH port) above.</b></p> <p>Enter the port number (between 1 and 65535) that this sensor uses for the SSH connection. Enter an integer.</p>
SSH Engine	<p>Select the SSH engine that you want to use to <a href="#">access data with this SSH sensor</a>:</p> <ul style="list-style-type: none"> <li>▪ Inherit from parent device (default): Use the SSH engine that you defined in the parent device settings or higher up in the <a href="#">object hierarchy</a>. If you have not changed the SSH engine, this is the recommended option.</li> <li>▪ Default: This is the default SSH engine. It provides the best performance and security. It is set by default in objects that are higher up in the hierarchy, so usually you can keep the Inherit from parent device (default) option.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default SSH engine does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions. It is deprecated. We will remove this legacy mode soon, so try to get your SSH sensors to run with the default SSH engine.</li> </ul> <p> We strongly recommend that you use the default SSH engine.</p> <p> The option you select here overrides the selection of the SSH engine in a higher object: a parent device, group, probe, or root.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID] (SSHv2).txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> <li>▪ Store result in case of error: Store the last sensor result only if the sensor shows the Down status.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### SSH SAN Logical Disk Settings

#### SSH SAN Logical Disk Settings

Volume **i** *Volume01*

Size **i**

Command Mode **i**
 Basic (default)
  Advanced

SSH SAN Logical Disk Settings

Setting	Description
Volume	The volume that this sensor monitors.
Size	The size of the volume that this sensor monitors.
Command Mode	<p>Define the command set that the sensor uses on the device to get monitoring data:</p> <ul style="list-style-type: none"> <li>▪ Basic (default): Use the basic command set. We recommend that you use the basic command set for best sensor performance. This setting is appropriate for most scenarios.</li> <li>▪ Advanced: Monitor additional data on the target device like IOs and bandwidth.</li> </ul> <p><b>i</b> Because this setting results in higher usage of system resources and so might cause sensor instabilities, we strongly recommend that you only select this option if this data is crucial for the volume that you monitor.</p>


### Sensor Display

#### Sensor Display


Primary Channel **i** *Downtime*


Graph Type **i**
 Show channels independently (default)
  Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Health	The disk health status <ul style="list-style-type: none"><li>▪ Up status: Ok</li><li>▪ Down status: Fault, Not Available</li></ul> <p> This channel is the primary channel by default.</p>
Total IOs	The total number of I/O operations
Transferred	The data transferred

## More

### KNOWLEDGE BASE

Which encryption algorithms do PRTG SSH sensors support?

- <https://kb.paessler.com/en/topic/90689>

Why does my SSH SAN sensor show a wrong status?

- <https://kb.paessler.com/en/topic/60145>

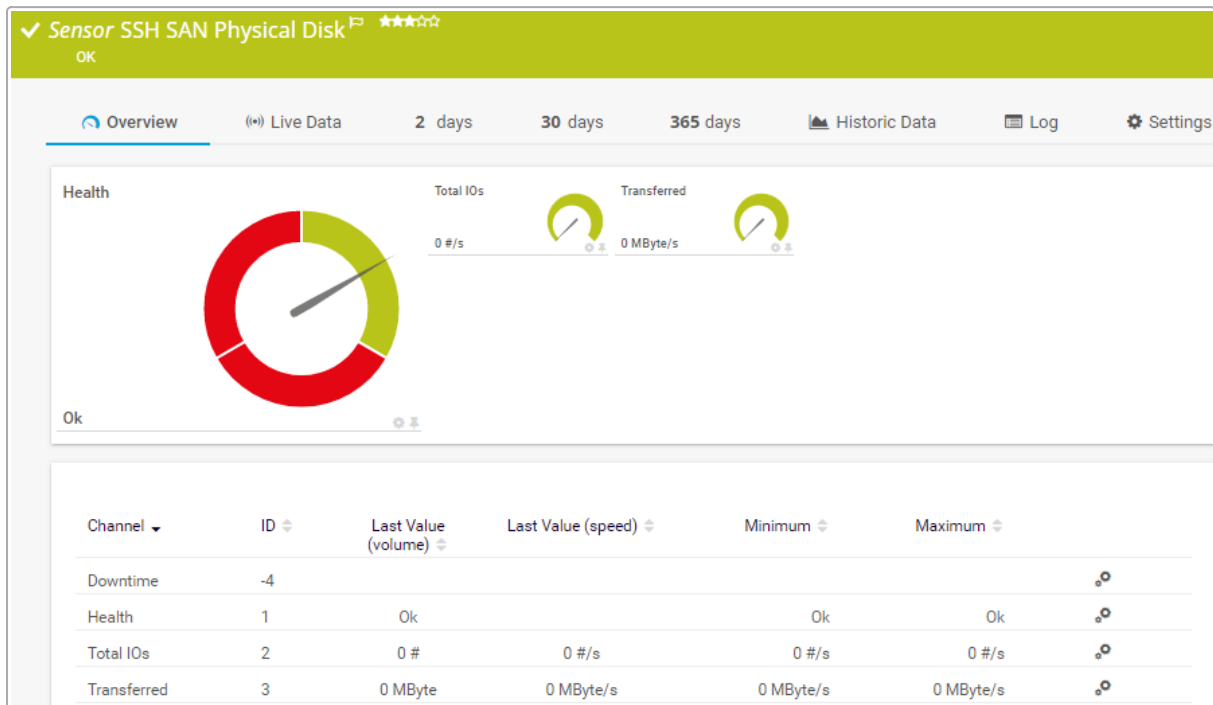
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.252 SSH SAN Physical Disk Sensor

The SSH SAN Physical Disk sensor monitors a physical disk on a storage area network (SAN) via Secure Shell (SSH).

**i** The SAN must provide a command-line interface (CLI) for this purpose.



SSH SAN Physical Disk Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SSH SAN Fysieke Schijf
- French: SAN disque physique (SSH)
- German: SSH SAN Physikalisches Laufwerk
- Japanese: SSH SAN 物理ディスク
- Portuguese: Disco físico SAN (SSH)
- Russian: Физический диск SAN по SSH
- Simplified Chinese: SSH SAN 物理磁盘
- Spanish: Disco físico SAN (SSH)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Credentials	This sensor requires <a href="#">credentials for Linux/Solaris/macOS (SSH/WBEM) systems</a> in the settings of the parent device.
SAN support	This sensor does not support every SAN, even if it provides a CLI. This sensor only works with specific devices, for example, the <a href="#">HPE P2000</a> .
Scanning interval	If the controller of the target system breaks down, increase the scanning interval to discharge the controller and try again.
Firmware update	After a firmware update of the target system, this sensor might show incorrect channel values. Add this sensor anew in this case.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
IPv4	This sensor only supports IPv4.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Device status	Sometimes the devices you monitor with this sensor return status values that are not officially documented so that the shown sensor status in PRTG differs from the "real" device status. For more information, see the Knowledge Base: <a href="#">Why does my SSH SAN sensor show a wrong status?</a>
Knowledge Base	Knowledge Base: <a href="#">Which encryption algorithms do PRTG SSH sensors support?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- physicaldisk
- sshsan



- sshsanphysicaldisk

For more information about basic sensor settings, see section [Sensor Settings](#) <sup>[667]</sup>.

## SSH Specific

**SSH Specific**

Connection Timeout (Sec.) ⓘ 60

---

Shell Timeout (Sec.) ⓘ 10

---




SSH Port Inheritance ⓘ  Inherit port from parent device (default)  
 Do not inherit port (enter a custom SSH port)

SSH Engine ⓘ  Inherit from parent device (default)  
 Default  
 Compatibility mode (deprecated)

Result Handling ⓘ  Discard result (default)  
 Store result  
 Store result in case of error

SSH Specific

Setting	Description
Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time that the sensor waits to establish a connection to the host. Keep this value as low as possible. Enter an integer.</p> <p> ⓘ This sensor has a fixed timeout of 300 seconds. If you change the value, it does not have an effect on the timeout.</p> <p> ⓘ Make sure that the connection timeout is a value that is higher than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (for example, <code>cat /proc/loadavg</code>). The maximum value is 300 seconds (5 minutes). Enter an integer.</p> <p> ⓘ This sensor has a fixed timeout of 300 seconds. If you change the value, it does not have an effect on the timeout.</p> <p> ⓘ Make sure that the shell timeout is a value that is lower than the connection timeout to avoid potential errors.</p>
SSH Port Inheritance	Define which port this sensor uses for the SSH connection:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Inherit port from parent device (default): Use the port number as defined in the <a href="#">Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems</a> section of the parent device settings.</li> <li>▪ Do not inherit port (enter a custom SSH port): Define a custom port number below and do not use the port number from the parent device settings.</li> </ul>
Custom SSH Port	<p>This setting is only visible if you select Do not inherit port (enter a custom SSH port) <a href="#">above</a>.</p> <p>Enter the port number (between 1 and 65535) that this sensor uses for the SSH connection. Enter an integer.</p>
SSH Engine	<p>Select the SSH engine that you want to use to <a href="#">access data with this SSH sensor</a>:</p> <ul style="list-style-type: none"> <li>▪ Inherit from parent device (default): Use the SSH engine that you defined in the parent device settings or higher up in the <a href="#">object hierarchy</a>. If you have not changed the SSH engine, this is the recommended option.</li> <li>▪ Default: This is the default SSH engine. It provides the best performance and security. It is set by default in objects that are higher up in the hierarchy, so usually you can keep the Inherit from parent device (default) option.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default SSH engine does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions. It is deprecated. We will remove this legacy mode soon, so try to get your SSH sensors to run with the default SSH engine.</li> </ul> <p> We strongly recommend that you use the default SSH engine.</p> <p> The option you select here overrides the selection of the SSH engine in a higher object: a parent device, group, probe, or root.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID] (SSHv2).txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> <li>▪ Store result in case of error: Store the last sensor result only if the sensor shows the Down status.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### SSH SAN Physical Disk Settings

#### SSH SAN Physical Disk Settings

**Disk** i 1.1

**Name** i disk\_1.1

**Size** i 450.0GB

**Command Mode** i  Basic (default)  
 Advanced

**Request Mode** i  Request all historical data (default)  
 Request actual counters

SSH SAN Physical Disk Settings

Setting	Description
Disk	The physical disk that this sensor monitors.
Name	The name of the physical disk that this sensor monitors.
Size	The size of the physical disk that this sensor monitors.
Command Mode	<p>Define the command set that the sensor uses on the device to get monitoring data:</p> <ul style="list-style-type: none"> <li>▪ <b>Basic (default):</b> Use the basic command set. We recommend that you use the basic command set for best sensor performance. This setting is appropriate for most scenarios.</li> <li>▪ <b>Advanced:</b> Monitor additional data on the target device like IOs and bandwidth. <ul style="list-style-type: none"> <li><b>i</b> Because this setting results in higher usage of system resources and so might cause sensor instabilities, we strongly recommend that you only select this option if this data is crucial for the volume that you monitor.</li> </ul> </li> </ul>
Request Mode	Define the which type of data the sensor requests:

Setting	Description
	<ul style="list-style-type: none"> <li>Request all historical data (default): Use this mode to possibly deliver better data.</li> <li>Request actual counters: Use this mode if the device does not support Request all historical data (default). This mode might result in incorrect data and spikes in graphs.</li> </ul>

## Sensor Display

**Sensor Display**


Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Health	<p>The disk health status</p> <ul style="list-style-type: none"> <li>▪ Up status: Ok</li> <li>▪ Down status: Fault, Not Available</li> </ul> <p> This channel is the primary channel by default.</p>
Total IOs	The total number of I/O operations
Transferred	The data transferred

## More

### ■ KNOWLEDGE BASE

Which encryption algorithms do PRTG SSH sensors support?

- <https://kb.paessler.com/en/topic/90689>

Why does my SSH SAN sensor show a wrong status?

- <https://kb.paessler.com/en/topic/60145>

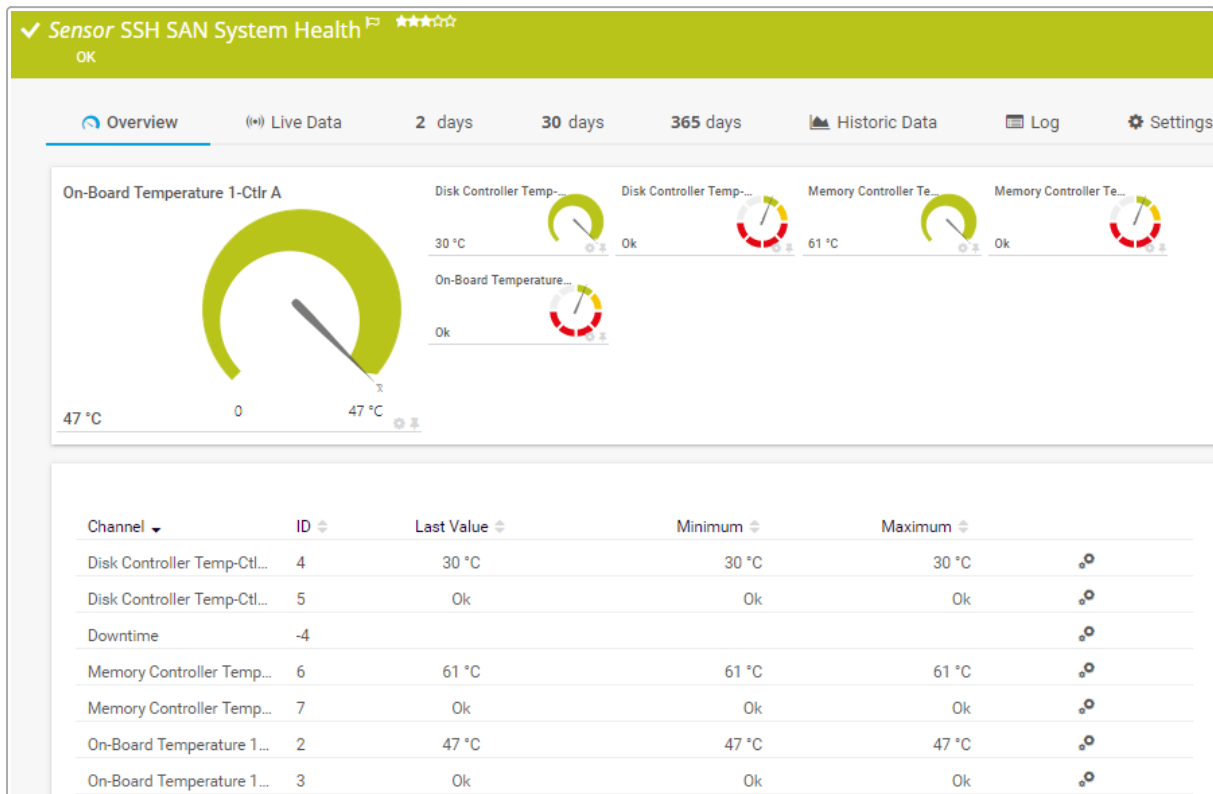
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.253 SSH SAN System Health Sensor

The SSH SAN System Health sensor monitors the system health of a storage area network (SAN) via Secure Shell (SSH).

**i** The SAN must provide a command-line interface (CLI) for this purpose.



SSH SAN System Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[230]</sup>.

### Sensor in Other Languages

- Dutch: SSH SAN Systeemstatus
- French: SAN état du système (SSH)
- German: SSH SAN Systemzustand
- Japanese: SSH SAN システムの正常性
- Portuguese: Saúde do sistema SAN (SSH)
- Russian: Работоспособность системы SAN по SSH
- Simplified Chinese: SSH SAN 系统健康状况
- Spanish: Salud de sistema SAN (SSH)

### Remarks

Consider the following [remarks](#)<sup>[229]</sup> and requirements for this sensor:

Remark	Description
Credentials	This sensor requires <a href="#">credentials for Linux/Solaris/macOS (SSH/WBEM) systems</a> in the settings of the parent device.
SAN support	This sensor does not support every SAN, even if it provides a CLI. This sensor only works with specific devices, for example, the <a href="#">HPE P2000</a> .
Scanning interval	If the controller of the target system breaks down, increase the scanning interval to discharge the controller and try again.
Firmware update	After a firmware update of the target system, this sensor might show incorrect channel values. Add this sensor anew in this case.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
IPv4	This sensor only supports IPv4.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Device status	Sometimes the devices you monitor with this sensor return status values that are not officially documented so that the shown sensor status in PRTG differs from the "real" device status. For more information, see the Knowledge Base: <a href="#">Why does my SSH SAN sensor show a wrong status?</a>
Knowledge Base	Knowledge Base: <a href="#">Which encryption algorithms do PRTG SSH sensors support?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- sshsan
- sshsansystemhealth

- systemhealth

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## SSH SAN Specific

SSH SAN Specific
Metric ⓘ Metric1

Monitoring Mode ⓘ

- Automatic detection
- Firmware before June 2015
- Firmware as of June 2015

SSH SAN Specific

Setting	Description
Metric	The metric that this sensor monitors.
Monitoring Mode	<p>Define how the sensor requests data from the target device:</p> <ul style="list-style-type: none"> <li>▪ Automatic detection: Automatically detect the firmware version and use the appropriate mode. We recommend that you use this option and only explicitly define the firmware date if errors occur.</li> <li>▪ Firmware before June 2015: Use the mode that is appropriate for firmware versions before June 2015.</li> <li>▪ Firmware as of June 2015: Use the mode that is appropriate for firmware versions as of June 2015.</li> </ul> <p>ⓘ The required mode depends on the firmware version of the target device. The sensor automatically detects the firmware version and uses the appropriate mode in most cases. If errors occur, explicitly define the firmware version.</p> <p>ⓘ We recommend that you use the default value.</p>



## SSH Specific

**SSH Specific**

Connection Timeout (Sec.) ⓘ 60

---

Shell Timeout (Sec.) ⓘ 10

---





SSH Port Inheritance ⓘ  Inherit port from parent device (default)  
 Do not inherit port (enter a custom SSH port)

SSH Engine ⓘ  Inherit from parent device (default)  
 Default  
 Compatibility mode (deprecated)

Result Handling ⓘ  Discard result (default)  
 Store result  
 Store result in case of error

SSH Specific

Setting	Description
Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time that the sensor waits to establish a connection to the host. Keep this value as low as possible. Enter an integer.</p> <p> ⓘ This sensor has a fixed timeout of 300 seconds. If you change the value, it does not have an effect on the timeout.</p> <p> ⓘ Make sure that the connection timeout is a value that is higher than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (for example, <code>cat /proc/loadavg</code>). The maximum value is 300 seconds (5 minutes). Enter an integer.</p> <p> ⓘ This sensor has a fixed timeout of 300 seconds. If you change the value, it does not have an effect on the timeout.</p> <p> ⓘ Make sure that the shell timeout is a value that is lower than the connection timeout to avoid potential errors.</p>
SSH Port Inheritance	<p>Define which port this sensor uses for the SSH connection:</p> <ul style="list-style-type: none"> <li>▪ Inherit port from parent device (default): Use the port number as defined in the <a href="#">Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems</a> section of the parent device settings.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Do not inherit port (enter a custom SSH port): Define a custom port number below and do not use the port number from the parent device settings.</li> </ul>
Custom SSH Port	<p>This setting is only visible if you select Do not inherit port (enter a custom SSH port) <a href="#">above</a>.</p> <p>Enter the port number (between 1 and 65535) that this sensor uses for the SSH connection. Enter an integer.</p>
SSH Engine	<p>Select the SSH engine that you want to use to <a href="#">access data with this SSH sensor</a>:</p> <ul style="list-style-type: none"> <li>Inherit from parent device (default): Use the SSH engine that you defined in the parent device settings or higher up in the <a href="#">object hierarchy</a>. If you have not changed the SSH engine, this is the recommended option.</li> <li>Default: This is the default SSH engine. It provides the best performance and security. It is set by default in objects that are higher up in the hierarchy, so usually you can keep the Inherit from parent device (default) option.</li> <li>Compatibility mode (deprecated): Use this only if the default SSH engine does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions. It is deprecated. We will remove this legacy mode soon, so try to get your SSH sensors to run with the default SSH engine.</li> </ul> <p> We strongly recommend that you use the default SSH engine.</p> <p> The option you select here overrides the selection of the SSH engine in a higher object: a parent device, group, probe, or root.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID] (SSHv2).txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> <li>Store result in case of error: Store the last sensor result only if the sensor shows the Down status.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Capacitor Cell [#] Voltage [Controller]	The capacitor cell voltage
Capacitor Cell [#] Voltage [Controller] Status	<p>The capacitor cell voltage status</p> <ul style="list-style-type: none"> <li>▪ Up status: Ok</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Error, Unavailable, Unknown, Unrecoverable</li> <li>▪ Unknown status: Not Installed, Unsupported</li> </ul>
Capacitor Pack Voltage [Controller]	The capacitor pack voltage
Capacitor Pack Voltage [Controller] Status	<p>The capacitor pack voltage status</p> <ul style="list-style-type: none"> <li>▪ Up status: Ok</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Error, Unavailable, Unknown, Unrecoverable</li> <li>▪ Unknown status: Not Installed, Unsupported</li> </ul>
Disk Controller Temp [Controller]	The disk controller temperature
Disk Controller Temp [Controller] Status	<p>The disk controller temperature status</p> <ul style="list-style-type: none"> <li>▪ Up status: Ok</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Error, Unavailable, Unknown, Unrecoverable</li> <li>▪ Unknown status: Not Installed, Unsupported</li> </ul>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Overall Unit Status	<p>The overall unit status</p> <ul style="list-style-type: none"> <li>▪ Up status: Ok</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Error, Unavailable, Unknown, Unrecoverable</li> <li>▪ Unknown status: Not Installed, Unsupported</li> </ul>

Channel	Description
Memory Controller Temp [Controller]	The memory controller temperature
Memory Controller Temp [Controller] Status	<p>The memory controller temperature status</p> <ul style="list-style-type: none"> <li>▪ Up status: Ok</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Error, Unavailable, Unknown, Unrecoverable</li> <li>▪ Unknown status: Not Installed, Unsupported</li> </ul>
On-Board Temperature [Controller]	The on-board temperature
On-Board Temperature [Controller] Status	<p>The on-board temperature status</p> <ul style="list-style-type: none"> <li>▪ Up status: Ok</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Error, Unavailable, Unknown, Unrecoverable</li> <li>▪ Unknown status: Not Installed, Unsupported</li> </ul>

## More

### ■ KNOWLEDGE BASE

Which encryption algorithms do PRTG SSH sensors support?

- <https://kb.paessler.com/en/topic/90689>

Why does my SSH SAN sensor show a wrong status?

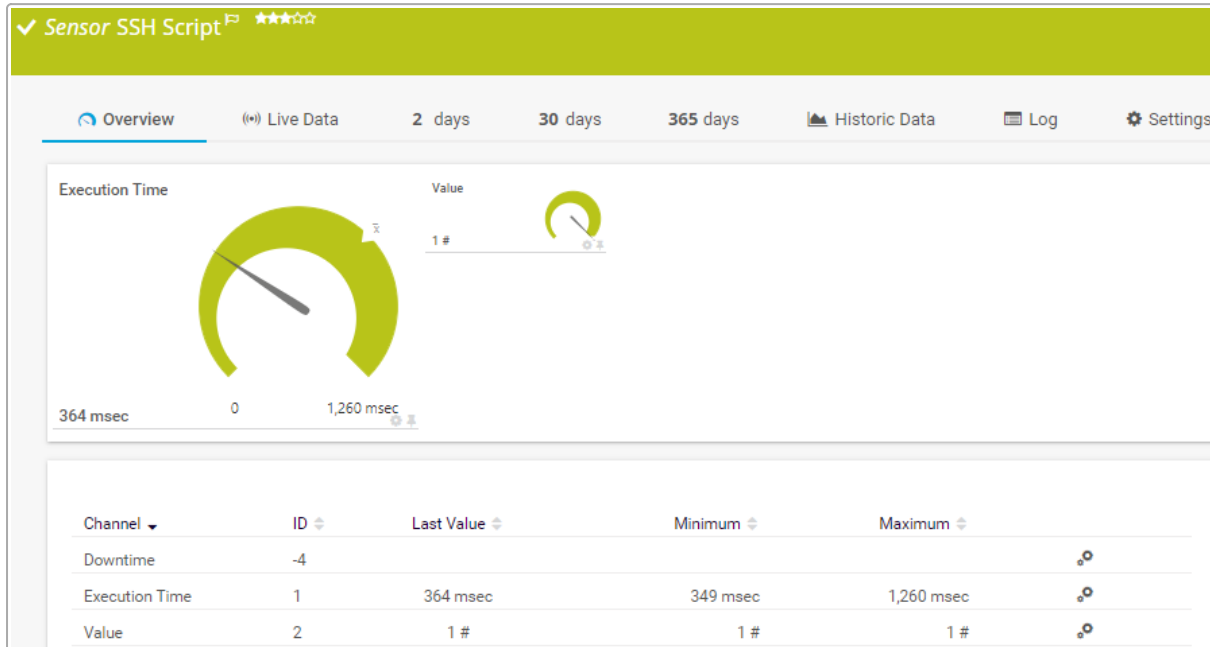
- <https://kb.paessler.com/en/topic/60145>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.254 SSH Script Sensor

The SSH Script sensor connects to a Linux/Unix system via Secure Shell (SSH) and executes a script file that is located on the target system. This option is available as part of the PRTG API.



SSH Script Sensor

■ For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2312]</sup>.

### Sensor in Other Languages

- Dutch: SSH Script
- French: Script (SSH)
- German: SSH-Skript
- Japanese: SSH スクリプト
- Portuguese: Script (SSH)
- Russian: Скрипт SSH
- Simplified Chinese: SSH 脚本
- Spanish: Script (SSH)

### Remarks

Consider the following [remarks](#)<sup>[2304]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
File storage	For security reasons, this sensor requires that you store your script file in the /var/prtg/scripts directory on the target system. Make sure that the script has executable rights. If the script is not available or was deleted from the directory, you get the error message <a href="#">Script not found (237)</a> .
Credentials	This sensor requires credentials for Linux/Solaris/macOS (SSH/WBEM) systems in the settings of the parent device.
Distributions	This sensor does not support all Linux/Unix and macOS distributions.
IPv4	This sensor only supports IPv4.
Return format	For more information about the return value format, see the <a href="#">PRTG Manual: Custom Sensors</a> .
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">Which encryption algorithms do PRTG SSH sensors support?</a></li> <li>▪ Knowledge Base: <a href="#">SSH and SFTP sensors in Unknown status</a></li> </ul>

## Add Sensor

Setting	Description
Channel Name	<p>Enter a name for the channel. Enter a string. This is for display purposes only.</p> <p><b>i</b> You can change this value later in the <a href="#">channel settings</a> of this sensor.</p>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- sshscript

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Credentials for Script Sensors

Click to interrupt the [inheritance](#).

### Credentials for Script Sensors

inherit from

**Placeholder 1 Description** ⓘ

**Placeholder 1** ⓘ

Credentials for Script Sensors

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder1</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.



Setting	Description
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder2</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder3</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder4</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder5</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.

## Sensor Settings

**Sensor Settings**

The sensor executes the script on the parent device. The working directory for the script is the parent directory on the target Linux/Unix system.

Script

Character Encoding  UTF-8 (default)  ASCII

Parameters











Mutex Name

Unit String

Value Type

If Value Changes  Ignore (default)  Trigger 'change' notification

Sensor Settings

Setting	Description
Script	<p>Select a script file from the dropdown list. It shows all script files that are available in the /var/prtg/scripts directory on the target Linux/Unix system. For a script file to appear in this list, store the target file in this directory.</p> <ul style="list-style-type: none"> <li> Make sure that the script has executable rights.</li> <li> To show the expected sensor value and <a href="#">status</a>, your file must use the correct format for the returned values. In this case, it is <a href="#">exitcode:value:message</a> to standard output <a href="#">stdout</a>. The exit code determines the sensor status.</li> <li> For more information on how to create custom sensors and for the return format, see section <a href="#">Custom Sensors</a>.</li> <li> For more information and an example script, see the Knowledge Base: <a href="#">Is there a shell script example for the SSH Script sensor?</a></li> <li> You cannot change this value after sensor creation.</li> </ul>
Character Encoding	<p>Define the character encoding that you use in your script to correctly display the sensor message:</p> <ul style="list-style-type: none"> <li>▪ UTF-8 (default)</li> <li>▪ ASCII</li> </ul>
Parameters	<p>If your script file catches command-line parameters, define them here. You can also use placeholders. Enter a string or leave the field empty.</p> <ul style="list-style-type: none"> <li> For a full list of all placeholders, see section <a href="#">Custom Sensors</a>.</li> <li> You need to escape special characters and whitespaces in your parameters and surround them with double quotation marks ("). See section <a href="#">Escape Special Characters and Whitespaces in Parameters</a> for details.</li> <li> In SSH scripts, you can use alphanumeric characters and the special characters ".", "_", "-", "=", and "/" outside of quoted strings.</li> </ul>
Mutex Name	<p>Define a mutual exclusion (mutex) name for the process. Enter a string or leave the field empty.</p> <ul style="list-style-type: none"> <li> PRTG runs all custom script sensors that have the same mutex name serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes that run running at the same time.</li> <li> See the Knowledge Base: <a href="#">What is the Mutex Name in the EXE/Script sensor settings?</a></li> </ul>
Unit String	<p>Define a unit for the channel value. Enter a string. This is for display purposes only and is the default unit for a new channel. You can change the unit after sensor creation in the sensor's channel settings.</p>

Setting	Description
Value Type	<p>Define the type of the values that your executable or script file returns:</p> <ul style="list-style-type: none"> <li>▪ Integer: An integer is expected as return value. If the script returns a float, PRTG displays the value 0.</li> <li>▪ Float: A float is expected as return value, with a dot (.) between the predecimal position and the decimal places. <ul style="list-style-type: none"> <li>ⓘ The sensor also displays integers unless they produce a buffer overflow.</li> </ul> </li> <li>▪ Counter: Your script returns an integer that increases. PRTG shows the difference between the values of two sensor scans. <ul style="list-style-type: none"> <li>ⓘ A counter <b>must</b> return an integer. It does not support float values.</li> </ul> </li> </ul> <p>ⓘ The sensor does not support string values.</p> <p>ⓘ You cannot change this value after sensor creation.</p>
If Value Changes	<p>Define what the sensor does when its value changes:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> <li>▪ Trigger 'change' notification: Send an internal message that indicates a change. <ul style="list-style-type: none"> <li>ⓘ In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</li> </ul> </li> </ul>

## SSH Specific

SSH Specific

Connection Timeout (Sec.) ⓘ 60

---

Shell Timeout (Sec.) ⓘ 10

---




SSH Port Inheritance ⓘ  Inherit port from parent device (default)  
 Do not inherit port (enter a custom SSH port)

SSH Engine ⓘ  Inherit from parent device (default)  
 Default  
 Compatibility mode (deprecated)

Result Handling ⓘ  Discard result (default)  
 Store result  
 Store result in case of error


SSH Specific

Setting	Description
Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time that the sensor waits to establish a connection to the host. Keep this value as low as possible. Enter an integer.</p> <p><b>i</b> Make sure that the connection timeout is a value that is higher than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (for example, <code>cat /proc/loadavg</code>). The maximum value is 300 seconds (5 minutes). Enter an integer.</p> <p><b>i</b> Make sure that the shell timeout is a value that is lower than the connection timeout to avoid potential errors.</p>
SSH Port Inheritance	<p>Define which port this sensor uses for the SSH connection:</p> <ul style="list-style-type: none"> <li>▪ Inherit port from parent device (default): Use the port number as defined in the <a href="#">Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems</a> section of the parent device settings.</li> <li>▪ Do not inherit port (enter a custom SSH port): Define a custom port number below and do not use the port number from the parent device settings.</li> </ul>
Custom SSH Port	<p><b>This setting is only visible if you select Do not inherit port (enter a custom SSH port) above.</b></p> <p>Enter the port number (between 1 and 65535) that this sensor uses for the SSH connection. Enter an integer.</p>
SSH Engine	<p>Select the SSH engine that you want to use to <a href="#">access data with this SSH sensor</a>:</p> <ul style="list-style-type: none"> <li>▪ Inherit from parent device (default): Use the SSH engine that you defined in the parent device settings or higher up in the <a href="#">object hierarchy</a>. If you have not changed the SSH engine, this is the recommended option.</li> <li>▪ Default: This is the default SSH engine. It provides the best performance and security. It is set by default in objects that are higher up in the hierarchy, so usually you can keep the Inherit from parent device (default) option.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default SSH engine does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions. It is deprecated. We will remove this legacy mode soon, so try to get your SSH sensors to run with the default SSH engine.</li> </ul> <p><b>i</b> We strongly recommend that you use the default SSH engine.</p>


Setting	Description
	<p> The option you select here overrides the selection of the SSH engine in a higher object: a parent device, group, probe, or root.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID] (SSHv2).txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> <li>▪ Store result in case of error: Store the last sensor result only if the sensor shows the Down status.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display



**Sensor Display**


Primary Channel  Downtime

---


Graph Type   Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>



## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Execution Time	<p>The execution time</p> <p> This channel is the primary channel by default.</p>
[Value]	<p>The value that the script file returns in one channel</p> <p> For more information about the return value format, see section <a href="#">Custom Sensors</a>.</p>

## More

### ■ KNOWLEDGE BASE

Which encryption algorithms do PRTG SSH sensors support?

- <https://kb.paessler.com/en/topic/90689>

SSH and SFTP sensors in Unknown status

- <https://kb.paessler.com/en/topic/79174>

Is there a shell script example for the SSH Script sensor?

- <https://kb.paessler.com/en/topic/39513>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

What is the Mutex Name in the EXE/Script sensor settings?

- <https://kb.paessler.com/en/topic/6673>

How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- <https://kb.paessler.com/en/topic/11283>

How can I show special characters with EXE/Script sensors?

- <https://kb.paessler.com/en/topic/64817>

Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

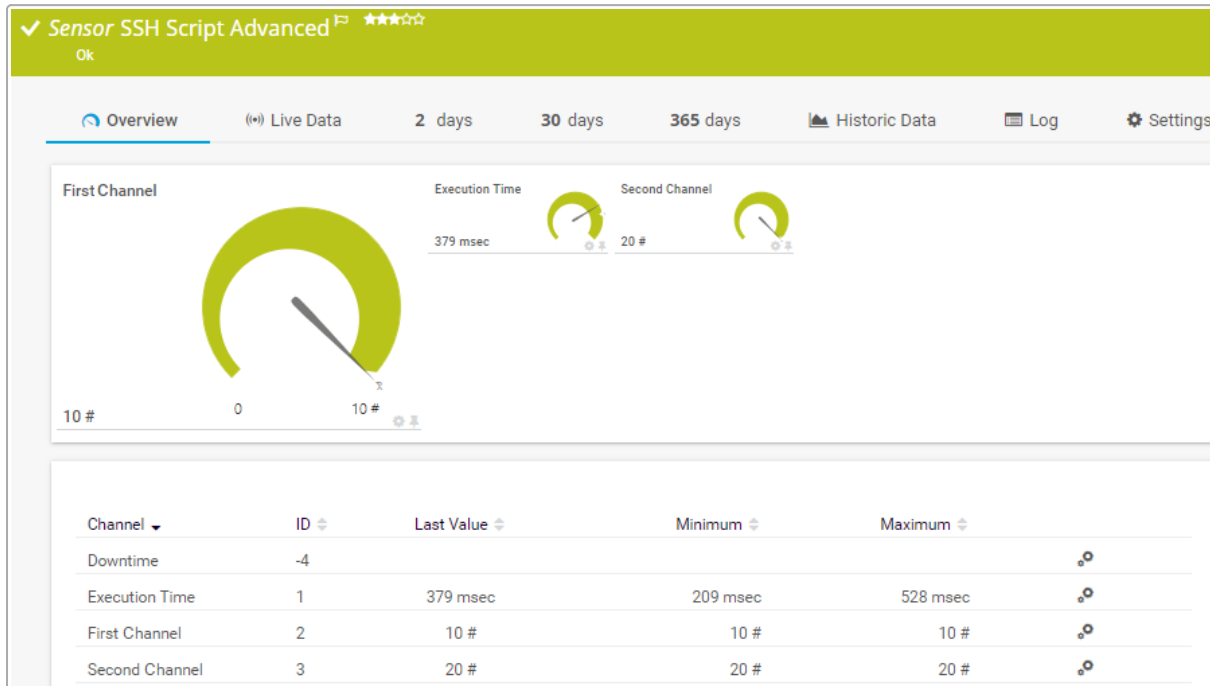
- <https://kb.paessler.com/en/topic/75372>

For which sensor types do you recommend at least Windows Server 2016 and why?

- <https://kb.paessler.com/en/topic/64331>

## 7.8.255 SSH Script Advanced Sensor

The SSH Script Advanced sensor connects to a Linux/Unix system via Secure Shell (SSH) and executes a script file that is located on the target system. This option is available as part of the PRTG API.



SSH Script Advanced Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SSH Script Geavanceerd
- French: Script avancé (SSH)
- German: SSH-Skript (Erweitert)
- Japanese: SSH スクリプト (詳細)
- Portuguese: Script (avançado) (SSH)
- Russian: Расширенный скрипт SSH
- Simplified Chinese: 高级 SSH 脚本
- Spanish: Script (avanzado) (SSH)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:



Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
File storage	For security reasons, this sensor requires that you store the script file in the /var/prtg/scriptsxml directory on the target system. Make sure that the script has executable rights.
Credentials	This sensor requires credentials for Linux/Solaris/macOS (SSH/WBEM) systems in the settings of the parent device.
Distributions	This sensor does not support all Linux/Unix and macOS distributions.
Channels	This sensor does not officially support more than <b>50 channels</b> .
IPv4	This sensor only supports IPv4.
Return format	For more information about the return value format, see the <a href="#">PRTG Manual: Custom Sensors</a> .
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">Which encryption algorithms do PRTG SSH sensors support?</a></li> <li>Knowledge Base: <a href="#">SSH and SFTP sensors in Unknown status</a></li> </ul>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:


- sshscript


■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>[667]</sup>.

## Credentials for Script Sensors


Click  to interrupt the [inheritance](#).

### Credentials for Script Sensors

 inherit from

Placeholder 1 Description 

---

Placeholder 1 

---

Credentials for Script Sensors

Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder1</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder2</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder3</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder4</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.

Setting	Description
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add <code>%scriptplaceholder5</code> in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.

## Sensor Settings

**Sensor Settings**

**Important:** The script is executed on the device the sensor is created on. The working directory for the script is the script's parent directory on the target Linux/Unix system.

Script

Parameters

Mutex Name

Sensor Settings

Setting	Description
Script	<p>Select a script file from the dropdown list. It shows all script files that are available in the <code>/var/prtg/scriptsxml</code> directory on the target Linux/Unix system. For a script file to appear in this list, store the target file in this directory.</p> <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> Make sure that the script has executable rights.</li> <li><span style="color: red;">❗</span> To show the expected sensor value and <a href="#">status</a>, your files must return the expected XML or JSON format to standard output <code>stdout</code>. The values and message must be embedded in the XML or JSON.</li> <li><span style="color: blue;">■</span> For more information on how to create custom sensors and for the return format, see section <a href="#">Custom Sensors</a>.</li> <li><span style="color: gray;">❗</span> You cannot change this value after sensor creation.</li> </ul>
Parameters	<p>If your script file catches command-line parameters, define them here. You can also use placeholders. Enter a string or leave the field empty.</p> <ul style="list-style-type: none"> <li><span style="color: blue;">■</span> For a full list of all placeholders, see section <a href="#">Custom Sensors</a>.</li> <li><span style="color: red;">❗</span> You need to escape special characters and whitespaces in your parameters and surround them with double quotation marks (<code>"</code>). See section <a href="#">Escape Special Characters and Whitespaces in Parameters</a> for details.</li> <li><span style="color: gray;">❗</span> In SSH scripts, you can use alphanumeric characters and the special characters <code>.", "_", "-", "=", and "/"</code> outside of quoted strings.</li> </ul>
Mutex Name	Define a mutual exclusion (mutex) name for the process. Enter a string or leave the field empty.

Setting	Description
	<p><b>i</b> PRTG runs all custom script sensors that have the same mutex name serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes that run running at the same time.</p> <p><b>■</b> See the Knowledge Base: <a href="#">What is the Mutex Name in the EXE/Script sensor settings?</a></p>

## SSH Specific

**SSH Specific**

Connection Timeout (Sec.) **i**

---

Shell Timeout (Sec.) **i**

---

SSH Port Inheritance **i**  Inherit port from parent device (default)  
 Do not inherit port (enter a custom SSH port)

SSH Engine **i**  Inherit from parent device (default)  
 Default  
 Compatibility mode (deprecated)

Result Handling **i**  Discard result (default)  
 Store result  
 Store result in case of error

SSH Specific

Setting	Description
Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time that the sensor waits to establish a connection to the host. Keep this value as low as possible. Enter an integer.</p> <p><b>i</b> Make sure that the connection timeout is a value that is higher than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (for example, <code>cat /proc/loadavg</code>). The maximum value is 300 seconds (5 minutes). Enter an integer.</p> <p><b>i</b> Make sure that the shell timeout is a value that is lower than the connection timeout to avoid potential errors.</p>

Setting	Description
SSH Port Inheritance	<p>Define which port this sensor uses for the SSH connection:</p> <ul style="list-style-type: none"> <li>▪ Inherit port from parent device (default): Use the port number as defined in the <a href="#">Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems</a> section of the parent device settings.</li> <li>▪ Do not inherit port (enter a custom SSH port): Define a custom port number below and do not use the port number from the parent device settings.</li> </ul>
Custom SSH Port	<p><b>This setting is only visible if you select</b> Do not inherit port (enter a custom SSH port) <b>above</b>.</p> <p>Enter the port number (between 1 and 65535) that this sensor uses for the SSH connection. Enter an integer.</p>
SSH Engine	<p>Select the SSH engine that you want to use to <a href="#">access data with this SSH sensor</a>:</p> <ul style="list-style-type: none"> <li>▪ Inherit from parent device (default): Use the SSH engine that you defined in the parent device settings or higher up in the <a href="#">object hierarchy</a>. If you have not changed the SSH engine, this is the recommended option.</li> <li>▪ Default: This is the default SSH engine. It provides the best performance and security. It is set by default in objects that are higher up in the hierarchy, so usually you can keep the Inherit from parent device (default) option.</li> <li>▪ Compatibility mode (deprecated): Use this only if the default SSH engine does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions. It is deprecated. We will remove this legacy mode soon, so try to get your SSH sensors to run with the default SSH engine.</li> </ul> <p><b>i</b> We strongly recommend that you use the default SSH engine.</p> <p><b>i</b> The option you select here overrides the selection of the SSH engine in a higher object: a parent device, group, probe, or root.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID] (SSHv2).txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> <li>▪ Store result in case of error: Store the last sensor result only if the sensor shows the Down status.</li> </ul>

Setting	Description
	<p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**


Primary Channel ⓘ Downtime

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Execution Time	The execution time
[Value]	The values that the script file returns in several channels ■ For more information about the return value format, see section <a href="#">Custom Sensors</a> .

## More

### ■ KNOWLEDGE BASE

Which encryption algorithms do PRTG SSH sensors support?

- <https://kb.paessler.com/en/topic/90689>

SSH and SFTP sensors in Unknown status

- <https://kb.paessler.com/en/topic/79174>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

What is the Mutex Name in the EXE/Script sensor settings?

- <https://kb.paessler.com/en/topic/6673>

How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- <https://kb.paessler.com/en/topic/11283>

How can I show special characters with EXE/Script sensors?

- <https://kb.paessler.com/en/topic/64817>

Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

For which sensor types do you recommend at least Windows Server 2016 and why?

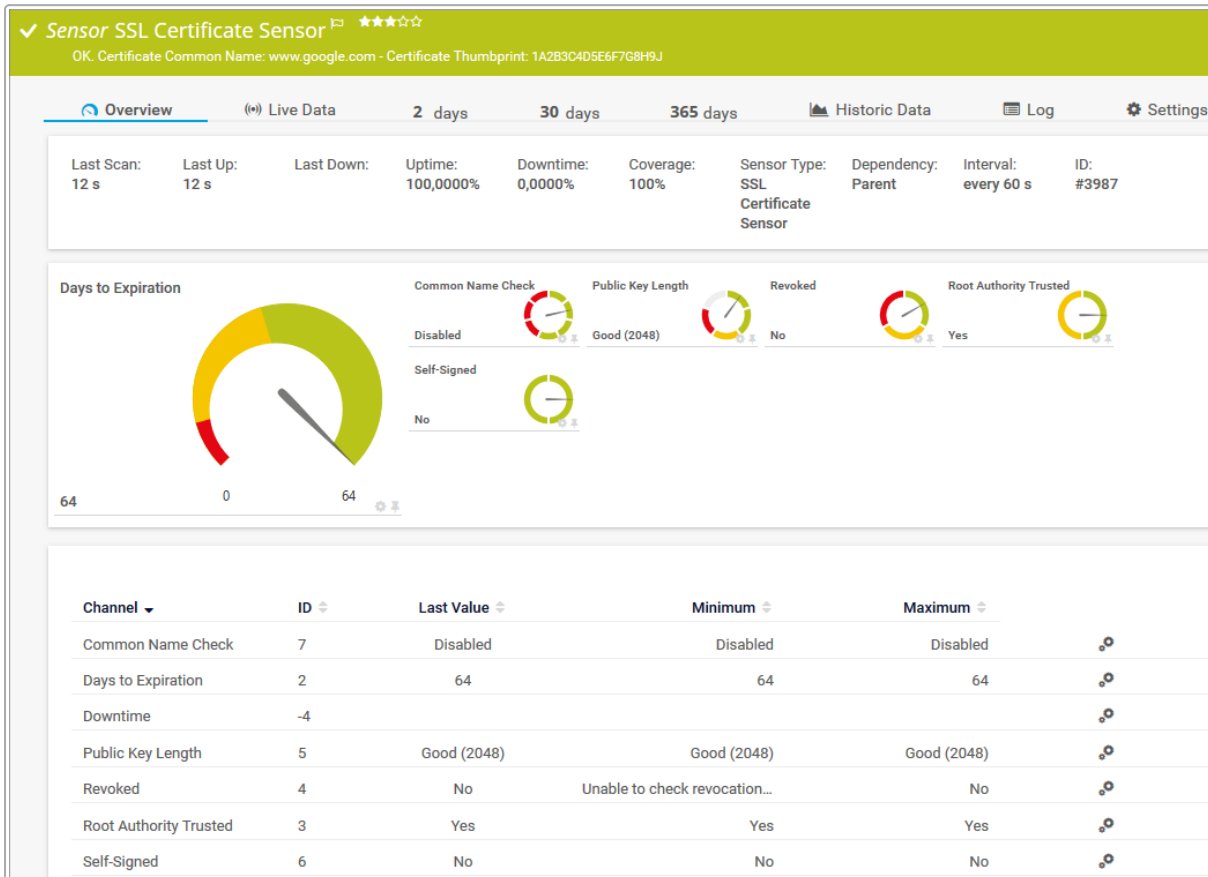
- <https://kb.paessler.com/en/topic/64331>



## 7.8.256 SSL Certificate Sensor

The SSL Certificate sensor monitors the certificate of a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.

- ❶ The sensor also shows the certificate common name and the certificate thumbprint in the sensor message.



SSL Certificate Sensor

- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2323]</sup>.

### Sensor in Other Languages

- Dutch: SSL Certificaat
- French: SSL certificat
- German: SSL-Zertifikat
- Japanese: SSL 証明書
- Portuguese: Certificado SSL
- Russian: Сертификат SSL
- Simplified Chinese: SSL 证书
- Spanish: Certificado SSL

## Remarks

Consider the following [remarks](#)<sup>[2324]</sup> and requirements for this sensor:

Remark	Description
DNS name	Enter the Domain Name System (DNS) name in the <a href="#">settings of the parent device</a> exactly as it is written in your certificate. You can also use <a href="#">wildcards</a> <sup>[2328]</sup> .
Revocation status	To check the revocation status of a certificate, the sensor uses WinHTTP to auto-detect the proxy server to use. You can also manually define a server. If you do not define a proxy server, PRTG uses the default WinHTTP proxy settings. For more information, see the Knowledge Base: <a href="#">How can I configure the WinHTTP proxy settings for the SSL Certificate sensor?</a>
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ  ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- certificate
- ssl
- sslcertificate

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## SSL Certificate Specific

SSL Certificate Specific

Port

Virtual Host (SNI Domain)

Certificate Name Validation  Do not compare common name (CN) with device address or SNI (default)  
 Compare and show down status if common name (CN) and address/SNI do not match  
 Compare and show down status if common name (CN)/alternative names (SAN) and address/SNI do not match

SSL Certificate Specific

Setting	Description
Port	Enter the number of the port to which this sensor connects. Enter an integer. The default port is <a href="#">443</a> .
Virtual Host (SNI Domain)	<p>Define the host name that the sensor tries to query if your server has multiple certificates on the same IP address and port combination. Enter a string.</p> <p><b>i</b> In the case of virtual hosting, you must identify the specific certificate for a specific domain while all domains use the same IP address, you can use SNI, which is an extension of TLS.</p> <p><b>i</b> If you select a Certificate Name Validation option below, the sensor compares the common name and optionally alternative names with the SNI. Leave this field empty to validate the common name with the host address of the parent device.</p>
Certificate Name Validation	<p>Define if you want the sensor to validate the certificate name:</p> <ul style="list-style-type: none"> <li>▪ Do not compare common name (CN) with device address or SNI (default): Do not check if the certificate name is valid by comparing it with the address of the parent device or the defined SNI.</li> <li>▪ Compare and show down status if common name (CN) and address/SNI do not match: Check the common name to validate the certificate name. If you define an SNI above, the sensor compares the common name with the SNI. If you do not define an SNI, the sensor uses the host address of the parent device. If the common name and the checked address/SNI do not match, the sensor shows the <a href="#">Down status</a>.</li> <li>▪ Compare and show down status if common name (CN)/alternative names (SAN) and address/SNI do not match: Check the common name and the <a href="#">Subject Alternative Names (SAN)</a> to validate the certificate. If you define an SNI domain above, the sensor compares the common name and alternative names with the SNI. If you do not define an SNI, the sensor uses the host address of the parent device. If the common name or alternative names and the checked address/SNI do not match, the sensor shows the Down status.</li> </ul>

## Connection Specific

**Connection Specific**

Use SOCKS Proxy (v5 only) ⓘ   
  Do not use SOCKS proxy (default)   
  Use SOCKS proxy

Connection Specific

Setting	Description
Use SOCKS Proxy (v5 only)	<p>Define if the sensor uses a SOCKS proxy server for the sensor connection:</p> <ul style="list-style-type: none"> <li>▪ Do not use SOCKS proxy(default): Directly connect to the target host without using a SOCKS proxy.</li> <li>▪ Use SOCKS proxy: Connect using <b>SOCKS5</b>. Provide data for the SOCKS connection below.               <ul style="list-style-type: none"> <li>ⓘ Other SOCKS versions are not supported.</li> </ul> </li> </ul> <p>ⓘ This sensor only supports SOCKS5 proxies. It does not support HTTP proxies.</p>
Server	<p><i>This setting is only visible if you select Use SOCKS proxy above.</i></p> <p>Enter the IP address or host name of the proxy server that the sensor uses for connection.</p>
Port	<p><i>This setting is only visible if you select Use SOCKS proxy above.</i></p> <p>Enter the port number of the proxy server that the sensor uses for connection.</p>
User Name	<p><i>This setting is only visible if you select Use SOCKS proxy above.</i></p> <p>If the proxy server requires authentication, enter a user name.</p>
Password	<p><i>This setting is only visible if you select Use SOCKS proxy above.</i></p> <p>If the proxy server requires authentication, enter the password for the user you specified above.</p>

## Debug Options

**Debug Options**

**Result Handling** ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result to the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].Data.txt, Result of Sensor [ID] (Certificate 0 in Certificate Chain).cer, Result of Sensor [ID] (Certificate 1 in Certificate Chain).cer, Result of Sensor [ID] (Certificate 2 in Certificate Chain).cer, Result of Sensor [ID] (Certificate Chain).txt, and Result of Sensor [ID] (Certificate).cer. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

ⓘ You can use the debug option to get a log file with information about the certificate chain. Additionally, certificates in the certificate chain are stored in the log folder (.cer files). This can help you, for example, if you have issues with the Root Authority Trusted channel of this sensor.

## Sensor Display

**Sensor Display**


**Primary Channel** ⓘ Downtime

**Graph Type** ⓘ


Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are

Setting	Description
	<p>available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Using Wildcards

You can use wildcards in the IP Address/DNS Name in the [device settings](#). Wildcards that apply to only one level of the domain name are supported.

Example	Result
<a href="#">*.wildcard.com</a> for <a href="#">www.wildcard.com</a>	Works
<a href="#">api.wildcard.com</a> for <a href="#">api.wildcard.com</a>	Works

Example	Result
contoso.com for contoso.com	Works
*.subapi.subapi2.wildcard.com for de.subapi.subapi2.wildcard.com	Works
*. *.wildcard.com for www.de.wildcard.com	Not supported
*.wildcard.com for de.subapi.wildcard.com	Doesn't work
www.contoso.com for contoso.com	Doesn't work
subapi.*.wildcard.com for subapi.dns.wildcard.com	Doesn't work

## Channel List

- i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Common Name Check	<p>If the common name or subject-alternative names match the host address or SNI (if you select a Certificate Name Validation option)</p> <ul style="list-style-type: none"> <li>▪ Up status: CN/SAN Match, Disabled, Matches Device Address, Matches SNI</li> <li>▪ Down status: CN/SAN Do Not Match SNI, Does Not Match Device Address, Does Not Match SNI</li> </ul>
Days to Expiration	<p>The days to expiration with a predefined lower warning limit (28 days) and lower error limit (7 days)</p> <p><b>i</b> This channel is the primary channel by default.</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: <b>7</b></li> <li>▪ Lower warning limit: <b>28</b></li> </ul>

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Public Key Length	<p>The public key length</p> <ul style="list-style-type: none"> <li>▪ Up status: <ul style="list-style-type: none"> <li>▫ RSA keys: For 2048-bit keys (<b>good</b> security) and longer (<b>perfect</b> security)</li> <li>▫ ECC keys: For 128-bit and 192-bit keys (<b>good</b> security) and longer (<b>perfect</b> security)</li> </ul> </li> <li>▪ Warning status: For <b>weak</b> security</li> <li>▪ Down status: For shorter keys (<b>unsecure</b>)</li> <li>▪ Unknown status: Unknown</li> </ul>
Revoked	<p>If the certificate has been revoked</p> <ul style="list-style-type: none"> <li>▪ Up status: No</li> <li>▪ Warning status: Unable To Check Revocation Status</li> <li>▪ Down status: Yes</li> </ul>
Root Authority Trusted	<p>If the certificate is trusted as root authority</p> <ul style="list-style-type: none"> <li>▪ Up status: Yes</li> <li>▪ Warning status: No</li> </ul>
Self-Signed	<p>If a self-signed certificate is used</p> <ul style="list-style-type: none"> <li>▪ Up status: Yes, No</li> </ul>

## More

### ■ KNOWLEDGE BASE

How can I configure the WinHTTP proxy settings for the SSL Certificate sensor?

- <https://kb.paessler.com/en/topic/86280>

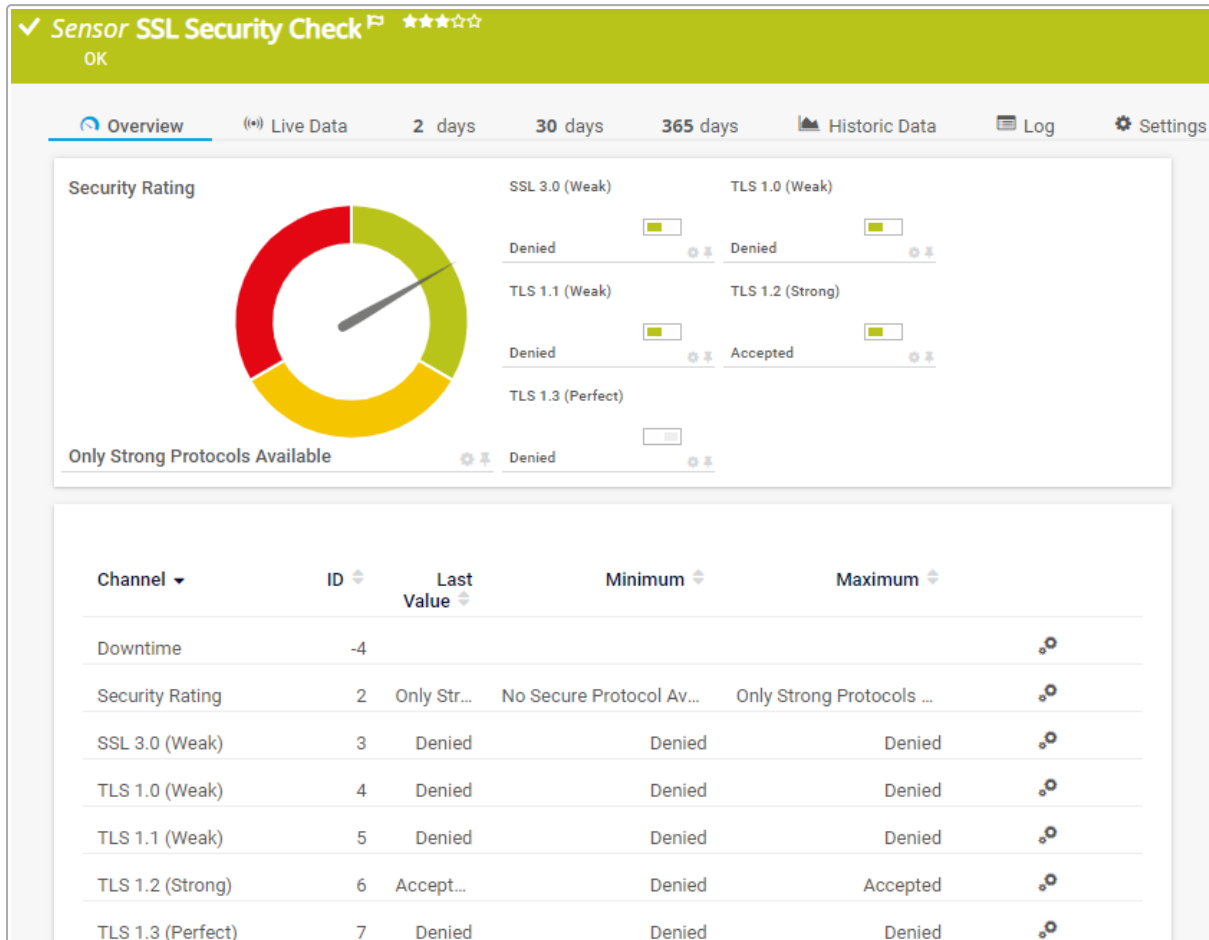
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>



## 7.8.257 SSL Security Check Sensor

The SSL Security Check sensor monitors Secure Sockets Layer (SSL)/Transport Layer Security (TLS) connectivity to the port of a device. It tries to connect to the specified TCP/IP port number of a device with different SSL/TLS versions and shows if the device supports a particular protocol.



SSL Security Check Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: SSL Security Check
- French: SSL vérification de sécurité
- German: SSL-Sicherheitsüberprüfung
- Japanese: SSL セキュリティーチェック
- Portuguese: Verificação de segurança SSL
- Russian: Проверка безопасности SSL
- Simplified Chinese: SSL 安全检查
- Spanish: Comprobación de seguridad SSL

## Remarks

Consider the following [remarks](#)<sup>[2332]</sup> and requirements for this sensor:

Remark	Description
Protocols	This sensor only checks accepted protocols. It does not consider the used ciphers.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Knowledge Base	Knowledge Base: <a href="#">How do you determine the protocol security ratings of the SSL Security Check sensor?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ

**Priority** ⓘ

Example Name

---

exampletag ✕ +

---

★★★★☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- sslsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

### SSL Security Specific

**SSL Security Specific**

Timeout (Sec.) ⓘ

Port ⓘ

Virtual Host (SNI Domain) ⓘ

SSL Security Specific

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is 900 seconds (15 minutes).</p> <p> ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>
Port	<p>Enter the number of the port to which this sensor connects. Enter an integer. The default port is 443.</p>
Virtual Host (SNI Domain)	<p>Enter the host name that the sensor queries. The sensor uses this host for the connection if the target server has multiple certificates on the same IP address and IP port when using Server Name Indication (SNI).</p>

### Connection Specific

**Connection Specific**

Use SOCKS Proxy (v5 only) ⓘ
  Do not use SOCKS proxy (default)
  Use SOCKS proxy

Connection Specific

Setting	Description
Use SOCKS Proxy (v5 only)	<p>Define if the sensor uses a SOCKS proxy server for the sensor connection:</p> <ul style="list-style-type: none"> <li>▪ Do not use SOCKS proxy(default): Directly connect to the target host without using a SOCKS proxy.</li> <li>▪ Use SOCKS proxy: Connect using SOCKS5. Provide data for the SOCKS connection below.</li> </ul> <p> ⓘ Other SOCKS versions are not supported.</p>

Setting	Description
	<p><b>i</b> This sensor only supports SOCKS5 proxies. It does not support HTTP proxies.</p>
Server	<p>This setting is only visible if you select Use SOCKS proxy above.</p> <p>Enter the IP address or host name of the proxy server that the sensor uses for connection.</p>
Port	<p>This setting is only visible if you select Use SOCKS proxy above.</p> <p>Enter the port number of the proxy server that the sensor uses for connection.</p>
User Name	<p>This setting is only visible if you select Use SOCKS proxy above.</p> <p>If the proxy server requires authentication, enter a user name.</p>
Password	<p>This setting is only visible if you select Use SOCKS proxy above.</p> <p>If the proxy server requires authentication, enter the password for the user you specified above.</p>

## Sensor Display

**Sensor Display**


Primary Channel **i**    Downtime

---


Graph Type **i**     Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>+</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>


Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Security Rating	<p>The security of the connection to the defined port</p> <ul style="list-style-type: none"> <li>Up status: Only Strong Protocols Available</li> <li>Warning status: Weak Protocols Available</li> <li>Down status: No Secure Protocol Available</li> </ul> <p> This channel is the primary channel by default.</p>
SSL 2.0 (Deprecated)	No longer available

Channel	Description
SSL 3.0 (Weak)	The status of connections using SSL v3 <ul style="list-style-type: none"> <li>▪ Up status: Denied</li> <li>▪ Warning status: Accepted</li> </ul>
TLS 1.0 (Weak)	The status of connections using TLS 1.0 <ul style="list-style-type: none"> <li>▪ Up status: Denied</li> <li>▪ Warning status: Accepted</li> </ul>
TLS 1.1 (Weak)	The status of connections using TLS 1.1 <ul style="list-style-type: none"> <li>▪ Up status: Accepted</li> <li>▪ Unknown status: Denied</li> </ul>
TLS 1.2 (Strong)	The status of connections using TLS 1.2 <ul style="list-style-type: none"> <li>▪ Up status: Accepted</li> <li>▪ Unknown status: Denied</li> </ul>
TLS 1.3 (Perfect)	The status of connections using TLS 1.3 <ul style="list-style-type: none"> <li>▪ Up status: Accepted</li> <li>▪ Unknown status: Denied</li> </ul>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

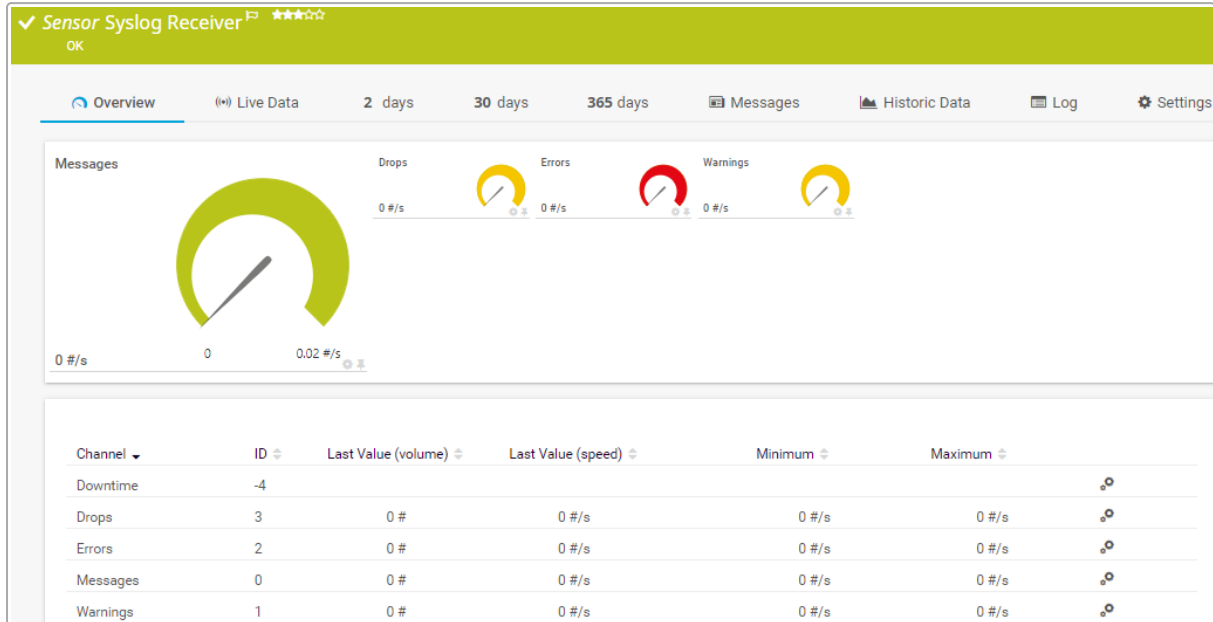
- <https://kb.paessler.com/en/topic/61108>

How do you determine the protocol security ratings of the SSL Security Check sensor?

- <https://kb.paessler.com/en/topic/71566>

## 7.8.258 Syslog Receiver Sensor

The Syslog Receiver sensor receives and analyzes Syslog messages.



Syslog Receiver Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).



### Sensor in Other Languages

- Dutch: Syslog ontvanger
- French: Récepteur Syslog
- German: Syslog-Empfänger
- Japanese: Syslog レシーバー
- Portuguese: Receptor de Syslog
- Russian: Приемник Syslog
- Simplified Chinese: Syslog 接收程序
- Spanish: Receptor de Syslog

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.

Remark	Description
UDP	This sensor only supports the User Datagram Protocol (UDP).
Cluster probe	This sensor does not support cluster probes. You can only set it up on local probes or remote probes.
IPv6	This sensor supports IPv6.
Probe device	<p>Add this sensor to the probe device to receive all messages of the remote probe system.</p> <p> If you add the sensor to a device other than a probe device, the IP address or Domain Name System (DNS) name of the parent device must match the proper sender. For example, if you want to receive messages from a storage area network (SAN), you might need to add a device with the IP address of a specific array member that sends the messages. Providing a DNS name that points to the IP address of a whole group might not work for SANs.</p>
Filter options	You can use the filter options to define which types of messages the sensor considers for monitoring, and which messages it categorizes as warnings or errors.
Specific device	Add this sensor to a specific device to directly receive all messages from this device. This is faster than using source filters.
Placeholders	You can use <a href="#">placeholders</a> in email <a href="#">notification templates</a> to see messages when you receive email notifications.
Sensor states	The <a href="#">sensor states</a> of this sensor persist for one scanning interval only. After showing the Warning or the Down status, and if there is no warning or error message in the next scanning interval, the sensor shows the Up status again. For more information on a workaround, see the Knowledge Base: <a href="#">How can I configure sensors using speed limits to keep the status for more than one interval?</a>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.



## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- syslogsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Syslog Specific

### Syslog Specific

**Port** ⓘ 514

---

**Purge Messages After** ⓘ 32 days (default)

Syslog Specific

Setting	Description
Port	Enter the number of the port on which the sensor listens for Syslog messages. The default port is <a href="#">514</a> . Enter an integer.  ⓘ We recommend that you use the default value.
Purge Messages After	Define how long PRTG stores received Syslog messages for analysis. Select a period of time from the dropdown list.

## Filter

■ For more information, see section [Filter Rules](#)<sup>[2343]</sup>.

**Filter**

*Filters are formulas using AND, OR, NOT, brackets and the following fields:*

Field	Parameters	Examples
source[ip]	Enter a UDP source IP, IP range, or IP hostmask	source[10.0.23.50], source[10.0.23.10-50], source[10.0.23.10/24]
facility[number]	Enter a number or range of the facility code, between 0 and 23	facility[2], facility[5-7]
severity[number]	Enter a single number or range of the severity code, between 0 (Emergency) and 7 (Debug)	severity[4], severity[1-3]
hostname[text]	Enter the hostname string to match (exact, case sensitive)	hostname[www.paessler.com]
tag[text]	Enter the tag string to match (exact, case sensitive)	tag[su]
appname[text]	Enter the app name string to match (exact, case sensitive)	appname[myproc]
procid[text]	Enter the process ID string to match (exact, case sensitive)	procid[8710]
msgid[text]	Enter the message ID string to match (exact, case sensitive)	msgid[ID47]
message[parttext]	Enter a substring to match the message field (partial, case insensitive)	message[Error]
data[parttext] data[id,param] data[id,param,value]	Enter a substring to match on structured data as displayed in the table (partial, case sensitive); or enter an ID and a parameter (comma separated) to check if the parameter exists in the ID element; or enter an ID, a parameter, and a value (comma separated) to match on a structured data value (RFC 5424)	data[exampleSDID@32473], data[exampleSDID@32473, eventSource], data[exampleSDID@32473, eventSource,Application]

Include Filter ⓘ severity[0-6]

Exclude Filter ⓘ

Warning Filter ⓘ severity[4]

Error Filter ⓘ severity[0-3]

Filter

Setting	Description
Include Filter	Define if you want to filter Syslog messages. If you leave this field empty or use the keyword <b>any</b> , the sensor processes all data. To only include specific types of messages, define filters using a special syntax.
Exclude Filter	Define which types of Syslog messages the sensor discards and does not process. To exclude specific types of messages, define filters using a special syntax.
Warning Filter	Define which types of Syslog messages count for the Warnings channel. To categorize received messages as warning messages, define filters using a special syntax.

Setting	Description
	<p><b>i</b> The sensor collects messages until a scanning interval ends. As long as the scanning interval is running, the sensor does not change its status. By default, the sensor changes to the Warning <a href="#">status</a> after a scanning interval finishes and there was at least one warning message (and no error message) during this scanning interval. The sensor shows the Warning at least until the succeeding scanning interval finishes. If the sensor does not receive any warning or error message in this scanning interval, its status changes to the Up status again with the start of the next scanning interval.</p>
Error Filter	<p>Define which types of Syslog messages count for the Errors channel. To categorize received messages as error messages, define filters using a special syntax.</p> <p><b>i</b> The sensor collects messages until a scanning interval ends. As long as the scanning interval is running, the sensor does not change its status. By default, the sensor changes to the Down status after a scanning interval finishes and there was at least one error message during this scanning interval. The sensor shows the Down status at least until the succeeding scanning interval finishes. If the sensor does not receive any warning or error message in this scanning interval, its status changes to the Up status again with the start of the next scanning interval.</p>

## Sensor Display

**Sensor Display**


Primary Channel **ⓘ** Downtime

---


Graph Type **ⓘ**  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⚙</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


### Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).


### Debug Options

**Debug Options**

Result Handling 

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\debug subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is UDP Debug Port [Port]_[Date].log. This setting is for debugging purposes.                             <ul style="list-style-type: none"> <li> Use with caution. We recommend that you only use this setting for a short time because it can create huge data files.</li> </ul> </li> </ul>

## Filter Rules

Filter rules are used for the include, exclude, warning, and error definition fields of the Syslog Receiver sensor. They are based on the following format:

```
field[filter]
```

You can use various filters suitable to your needs. Include and exclude filters define which messages to monitor. Warning and error filters define how to categorize received messages. Provide these filters in the sensor settings as formulas. Formulas are fields that you can combine with boolean operators ([AND](#), [OR](#), [NOT](#)) and brackets.

Field	Parameter	Example
source[ip]	Enter an IP address where the messages come from. IP masks and ranges are also possible.	<ul style="list-style-type: none"> <li>▪ source[10.0.23.50]</li> <li>▪ source[10.0.23.10-50]</li> <li>▪ source[10.0.23.10/24]</li> </ul>
facility[number]	Enter any number or range from 0 to 23 specifying the program type that sends the message.	<ul style="list-style-type: none"> <li>▪ facility[2]</li> <li>▪ facility[5-7]</li> <li>▪ facility[5] OR facility[6]</li> </ul>
severity[number]	Enter any number or range from 0 (emergency) to 7 (debug) specifying the message type.	<ul style="list-style-type: none"> <li>▪ severity[4]</li> <li>▪ severity[1-3]</li> <li>▪ severity[1] AND severity[2]</li> </ul>
hostname[text]	Enter any string that specifies the hostname of a device in the message.	<ul style="list-style-type: none"> <li>▪ hostname[www.example.com]</li> </ul>
tag[text]	Enter any string that specifies the tag of a program or process in the message.	<ul style="list-style-type: none"> <li>▪ tag[su]</li> </ul>
appname[text]	Enter any string that specifies the appname part of the message.	<ul style="list-style-type: none"> <li>▪ appname[myproc]</li> <li>▪ appname[demo] AND msgid[m42]</li> </ul>
procid[text]	Enter any string that specifies the process identifier part of the message.	<ul style="list-style-type: none"> <li>▪ procid[1860]</li> </ul>
msgid[text]	Enter any string that specifies the message identifier part of the message.	<ul style="list-style-type: none"> <li>▪ msgid[ID47]</li> </ul>
message[parttext]	Enter any string that specifies the message part of the message. (Any substring matches. This value is not case-sensitive.)	<ul style="list-style-type: none"> <li>▪ message[Error]</li> </ul>

Field	Parameter	Example
data [id,param,value]	This checks the SD-ID block of the message's structured data for a parameter matching the specified value.	▪ data[exampleSDID@12345,eventSource,Application]
data[parttext]	This checks if the specified substring matches structured data as displayed in the corresponding table.	▪ data[exampleSDID@1234]
data[id,param]	This checks if the parameter exists in the specified ID element.	▪ data[exampleSDID@1234,eventSource]

- ❗ String parameters (except the substring in message) must **exactly** match the particular parts of the message. They are case-sensitive.

## Messages Tab: Review and Analyze Syslog Messages


PRTG stores received Syslog messages as common files in the \Syslog Database subfolder of the PRTG data directory. To review and analyze all received messages, you can directly access the most recent data in a [table list](#) on the PRTG web interface. You can access this list via the sensor's Overview tab.

- ❗ Received Syslog messages are only shown in the table on the Overview tab after an (automatic) page refresh following a sensor scan. The default value for [auto refresh](#) is 30 seconds.

For more details and further filter options, click the Messages tab of the Syslog Receiver sensor. You see all received messages in a table list. On the top, you have display filter options to drill down into the data for specific events of your interest. The filters are the same as those available in the sensor settings, but you can define them without using formulas. Provide the desired parameters and PRTG automatically loads the filtered list.

- ❗ You can automatically add a filter by clicking the content of a column.

### Advanced Filter Settings

You can open advanced filter settings by clicking  in the Filter row. The Advanced Filter appears in a popup window. In the text field, you can define a filter using the syntax as specified in section [Filter Rules](#) <sup>2343</sup>.

If you provided filter parameters on the Messages tab, the advanced filter already includes them as a corresponding formula with the correct syntax. You can adjust this filter to your needs. You can also copy the automatically created and manually adjusted formula for usage in the filter fields of the sensor settings.

### Channel List

- ❗ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Drops	The number of dropped packets on the syslog port ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper warning limit: <a href="#">0.00000001</a></li> </ul>
Errors	The number of messages categorized as "error" ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper error limit: <a href="#">0.00000001</a></li> </ul>
Messages	The number of received Syslog messages ⓘ This channel is the primary channel by default.
Warnings	The number of messages categorized as "warning" ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper warning limit: <a href="#">0.00000001</a></li> </ul>

## More

### ■ KNOWLEDGE BASE

How can I configure sensors using speed limits to keep the status for more than one interval?

- <https://kb.paessler.com/en/topic/73212>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

### ▶ VIDEO TUTORIAL

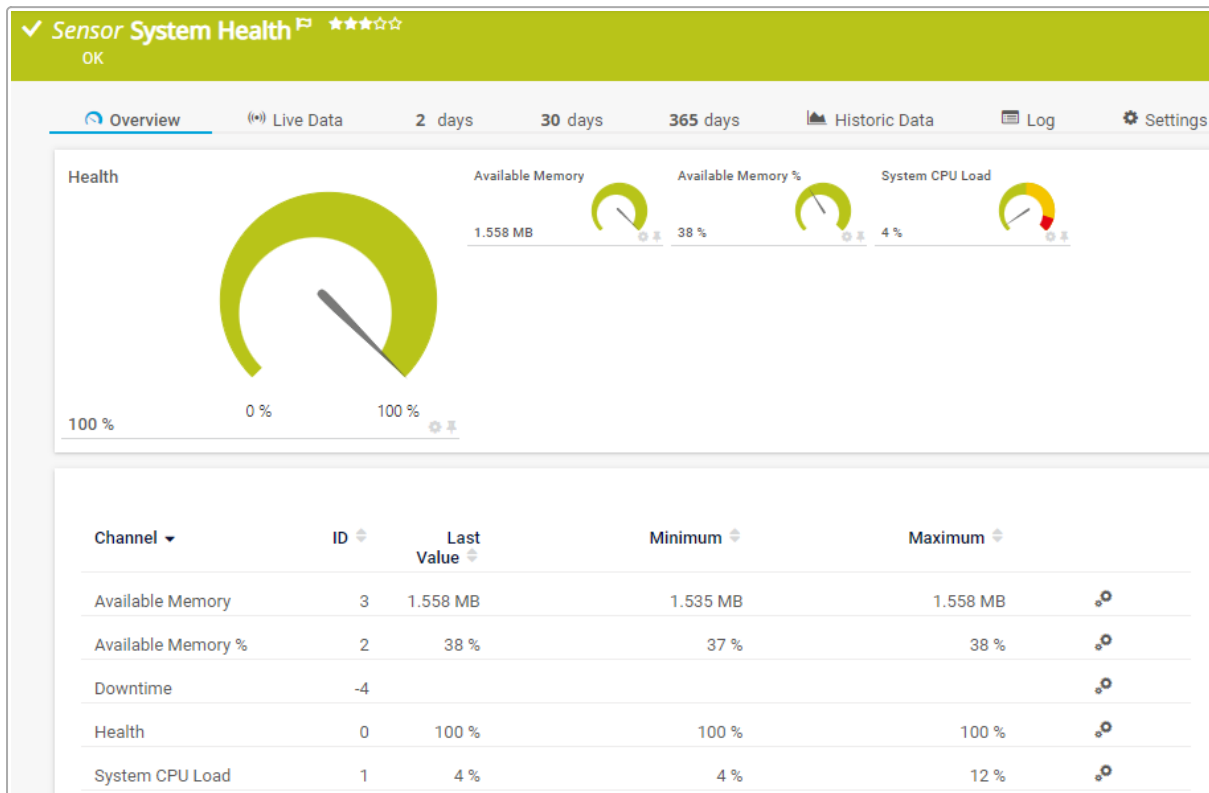
SNMP Trap receiver and syslog receiver sensors

- <https://www.paessler.com/support/videos-and-webinars/videos/syslog-receiver>

## 7.8.259 System Health Sensor

The System Health sensor monitors the status of the probe system. It checks various system parameters that can affect the quality of the monitoring results.

- ❶ PRTG automatically creates this sensor. You cannot delete the sensor if it was created automatically. If you manually create the sensor, you can delete it.



System Health Sensor

- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2348]</sup>.

### Sensor in Other Languages

- Dutch: Systemstatus
- French: État du système
- German: Systemzustand
- Japanese: システム正常性
- Portuguese: Saúde do sistema
- Russian: Работоспособность системы
- Simplified Chinese: 系统健康状况
- Spanish: Salud de sistema



## Remarks

Consider the following [remarks](#)<sup>[2347]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <b>very low</b> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- systemhealthsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Sensor Display

### Sensor Display

**Primary Channel** ⓘ


**Graph Type** ⓘ

Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.

Setting	Description
	<p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Available Memory	The amount of free memory available on the system. This value should not fall below 500 MB. This way, PRTG can still request resources during report generation or auto-discoveries, for example.
Available Memory %	The available memory (%)
System CPU Load	The CPU load (%). Extensive CPU load can lead to false, incomplete, and incorrect monitoring results. This value should usually stay below 50%.

Channel	Description
	<p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: 90%</li> <li>▪ Upper warning limit: 50%</li> </ul>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Health	<p>The sum of the system status as a value between 100% (healthy) and 0% (failing). Investigate frequent or repeated health values below 100%.</p> <p><b>i</b> This channel is the primary channel by default.</p>

More

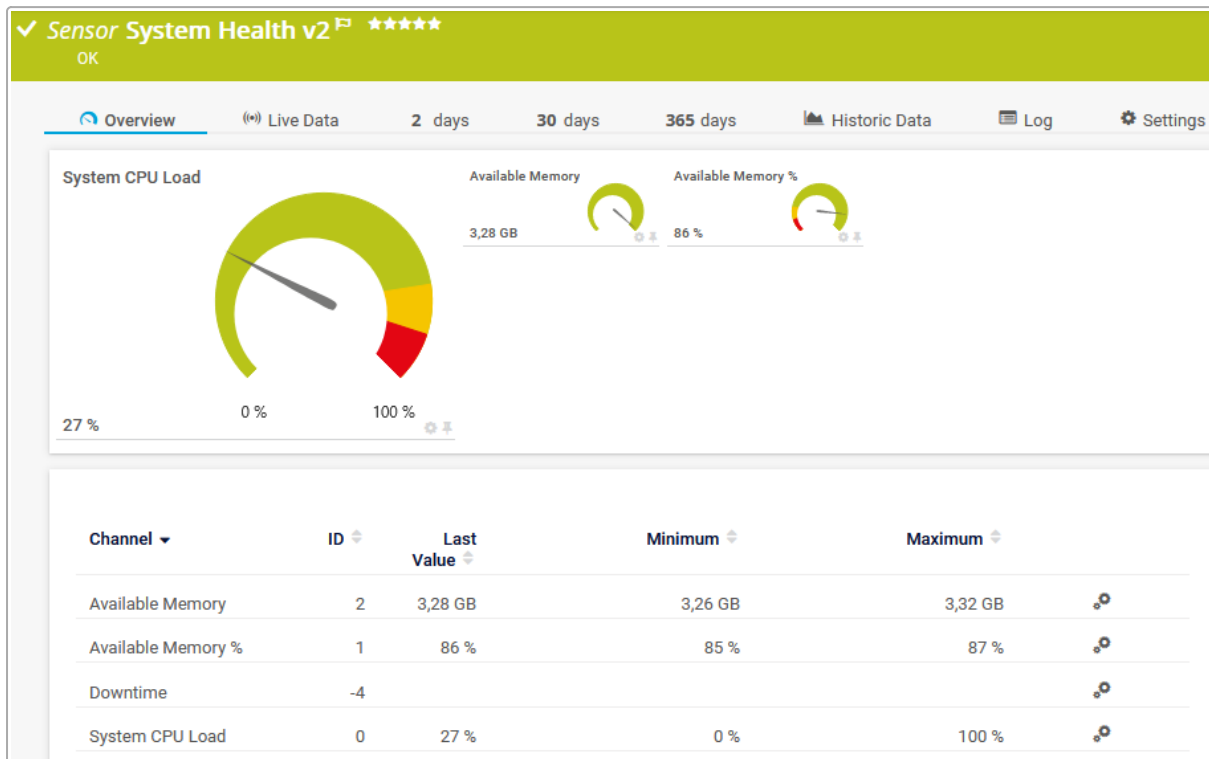
**■** KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.260 System Health v2 Sensor

The System Health v2 sensor monitors the health of a Linux system that the PRTG core server runs on.



For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2353]</sup>.

### Sensor in Other Languages

- Dutch: Systeemstatus v2
- French: État du système v2
- German: Systemzustand v2
- Japanese: システム正常性 v2
- Portuguese: Saúde do sistema v2
- Russian: Работоспособность системы v2
- Simplified Chinese: 系统健康状况 v2
- Spanish: Salud del sistema v2

### Remarks

Consider the following [remarks](#)<sup>[2350]</sup> and requirements for this sensor:

Remark	Description
Sensor creation	PRTG automatically creates this sensor. You cannot delete it. If you manually create the sensor, you can delete it.
Probe device	You can create this sensor only on a <a href="#">probe device</a> .
Windows OS	This sensor does not support Windows operating systems.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">low</a> performance impact.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Scanning interval	The recommended scanning interval of this sensor is <a href="#">1 minute</a> .
Multi-platform probe	You can add this sensor to a multi-platform probe.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- systemhealthsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings



By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Available Memory	The amount of free memory available on the system. This value should not fall below 500 MB. This way, PRTG can still request resources during report generation or auto-discoveries, for example.
Available Memory %	<p>The available memory (%)</p> <p>ⓘ This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: <a href="#">10%</a></li> <li>▪ Lower warning limit: <a href="#">20%</a></li> </ul>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
System CPU Load	<p>The CPU load (%).</p> <p>Extensive CPU load can lead to false, incomplete, and incorrect monitoring results. This value should usually stay below 50%.</p> <p> This channel has default limits:</p> <ul style="list-style-type: none"><li>▪ Upper error limit: <a href="#">90%</a></li><li>▪ Upper warning limit: <a href="#">80%</a></li></ul> <p> This channel is the primary channel by default.</p>

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

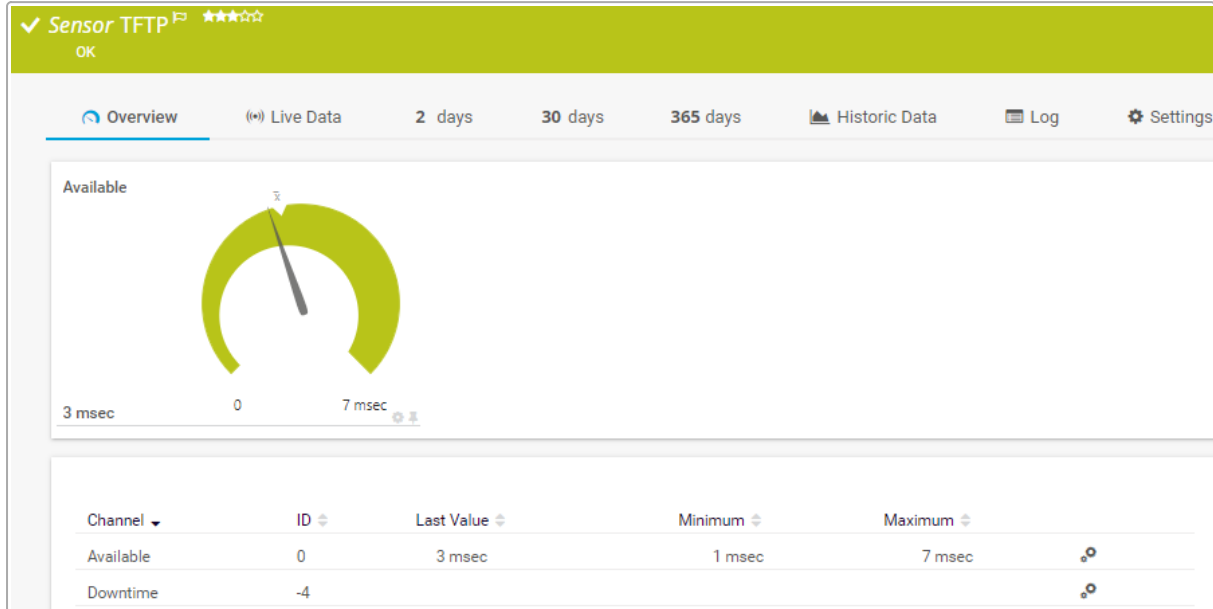
What is the multi-platform probe and how can I use it?

- <https://kb.paessler.com/en/topic/90140>



## 7.8.261 TFTP Sensor

The TFTP sensor monitors a Trivial File Transfer Protocol (TFTP) server and checks if a certain file is available for download.



TFTP Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: TFTP
- French: TFTP
- German: TFTP
- Japanese: TFTP
- Portuguese: TFTP
- Russian: TFTP
- Simplified Chinese: TFTP
- Spanish: TFTP

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
IPv4	This sensor only supports IPv4.

Remark	Description
Performance impact	This sensor has a <b>medium</b> performance impact.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- trivialftpsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Specific

#### Sensor Specific

**Timeout (Sec.)** ⓘ 5

---

**Port** ⓘ 69

---

**File Name** ⓘ tftp.c

Sensor Specific

Setting	Description
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>ⓘ</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

Setting	Description
Port	Enter the number of the port that the TFTP service runs on. The sensor connects to this port. Enter an integer.
File Name	Enter the name of the file that this sensor checks. If the file is not available on the server, the sensor shows the Down <a href="#">status</a> . Enter a string.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Available	The response time  This channel is the primary channel by default.
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

## More

### ■ KNOWLEDGE BASE

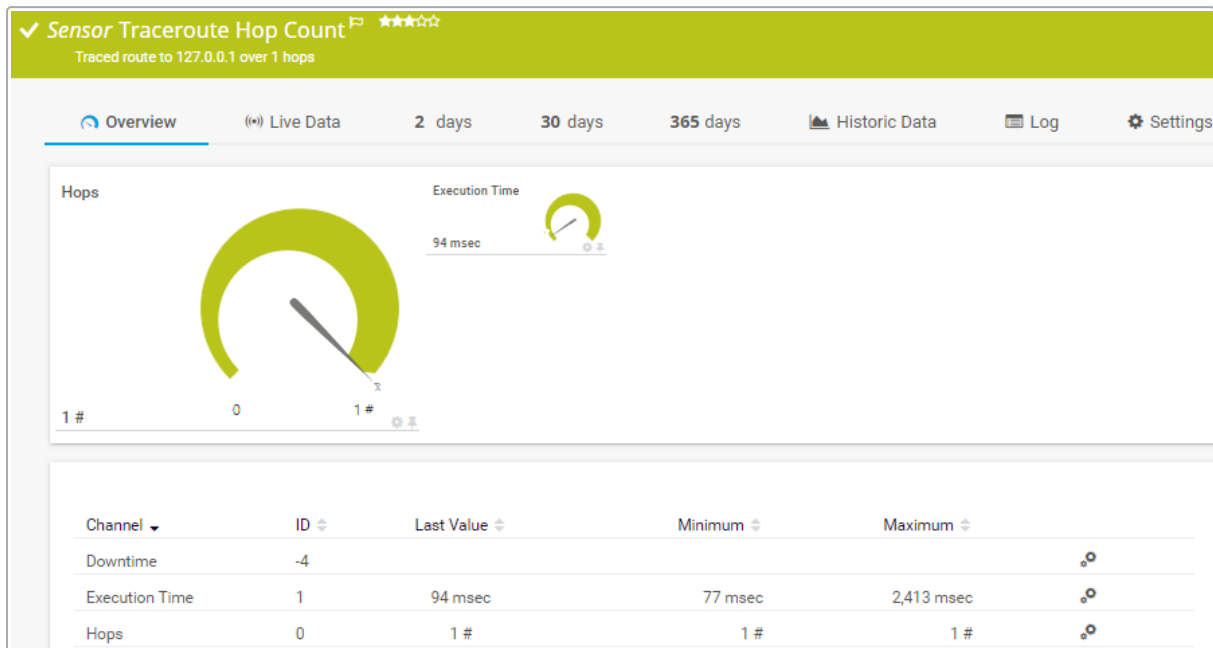
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.262 Traceroute Hop Count Sensor

The Traceroute Hop Count sensor traces the number of hops from the probe system to the IP Address/DNS Name of the parent device.

**i** If the number of hops (the route) changes, you can additionally define a different [sensor status](#).



Traceroute Hop Count Sensor



For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Traceroute Hop Count
- French: Compteur de hop Traceroute
- German: Traceroute Hop-Anzahl
- Japanese: Traceroute ホップ数
- Portuguese: Contagem de hops em traceroute
- Russian: Кол-во переходов трассировки маршрута
- Simplified Chinese: Traceroute 跳跃计数
- Spanish: Recuento de saltos traceroute

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node. If the sensor shows the error PE087, additionally install .NET 3.5 on the probe system.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Windows Server	We recommend Windows Server 2016 on the probe system for best performance of this sensor.
IPv6	This sensor supports IPv6.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- ptfsensor

 For more information about basic sensor settings, see section [Sensor Settings](#) .

### Sensor Settings

#### Sensor Settings

**If Route Changes** ⓘ

Ignore (default)

Set sensor to warning status

Set sensor to down status

Sensor Settings

Setting	Description
If Route Changes	<p>Define what to do if the route has changed since the last check:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> <li>▪ Set sensor to warning status: Show the Warning status if the route changes.</li> <li>▪ Set sensor to down status: Show the Down status if the route changes.</li> </ul>

## Debug Options

**Debug Options**

**Result Handling** ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display


**Sensor Display**

**Primary Channel** ⓘ Downtime  



---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.


 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status



Channel	Description
Execution Time	The execution time
Hops	The number of hops  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

Which .NET version does PRTG require?

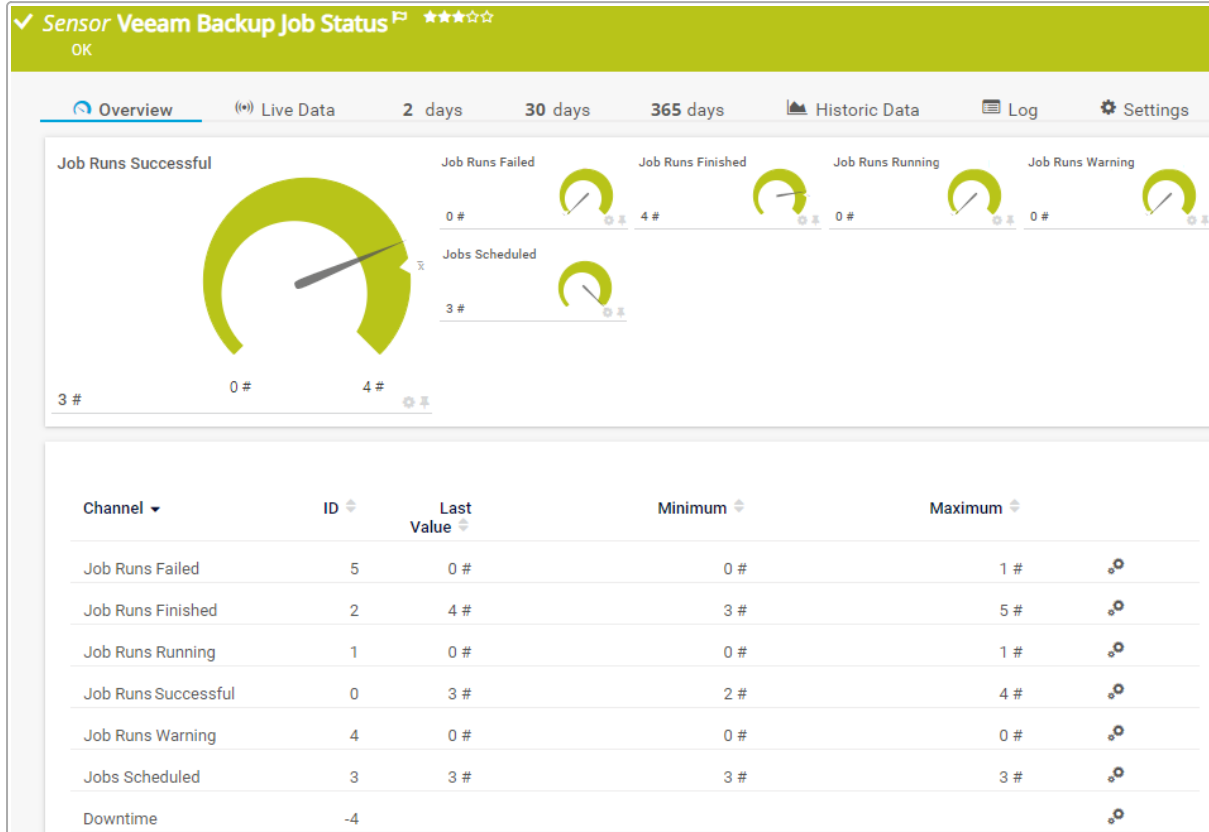
- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.263 Veeam Backup Job Status Sensor

The Veeam Backup Job Status sensor monitors the status of all backup job runs on the Veeam Backup Enterprise Manager in the last 24 hours.



Veeam Backup Job Status Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Veeam Backup Taak Status
- French: Veeam statut de tâche de sauvegarde
- German: Veeam Backupjob-Status
- Japanese: Veeam バックアップジョブのステータス
- Portuguese: Status da tarefa de backup do Veeam
- Russian: Состояние задания резервного копирования Veeam
- Simplified Chinese: Veeam 备份作业状态
- Spanish: Estado del trabajo de copia de seguridad Veeam

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Veeam version	This sensor requires that the <a href="#">Veeam Backup Enterprise Manager 10, 11, or 12</a> with the <a href="#">Enterprise Plus</a> license are installed.
Credentials	This sensor requires credentials for Veeam.
Backup jobs	This sensor does not support the following backup job types: <a href="#">Tape</a> , <a href="#">Sure Backup</a> , <a href="#">NAS Backup Copy</a> , and <a href="#">Agent Backup Copy</a> .
Veeam agent	This sensor does not support <a href="#">Veeam Agent Backup Jobs</a> if they are managed by a <a href="#">Veeam Agent</a> .
REST API	This sensor only supports version <a href="#">1.5</a> of the Representational State Transfer (REST) application programming interface (API).
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">5 minutes</a>.</li> </ul>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- veeam
- veeambackup
- veeamenterprisemanager

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Job Runs Failed	<p>The number of failed job runs (sessions)</p> <p>ⓘ This channel has a default limit:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: 0</li> </ul> <p>ⓘ The Job Runs Failed channel shows the total number of all failed job runs.</p>
Job Runs Finished	The number of finished job runs

Channel	Description
	<p><b>i</b> The Job Runs Finished channel shows the total number of all finished job runs with status <b>Success</b>, <b>Warning</b>, and <b>Failed</b>.</p>
Job Runs Running	The number of running job runs
Job Runs Successful	<p>The number of successful job runs</p> <p><b>i</b> The Job Runs Successful channel shows the total number of all finished job runs with status <b>Success</b>.</p> <p><b>i</b> This channel is the primary channel by default.</p>
Job Runs Warning	<p>The number of job runs in the warning status</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>▪ Upper warning limit: <b>0</b></li> </ul>
Jobs Scheduled	The number of scheduled backup jobs

## More

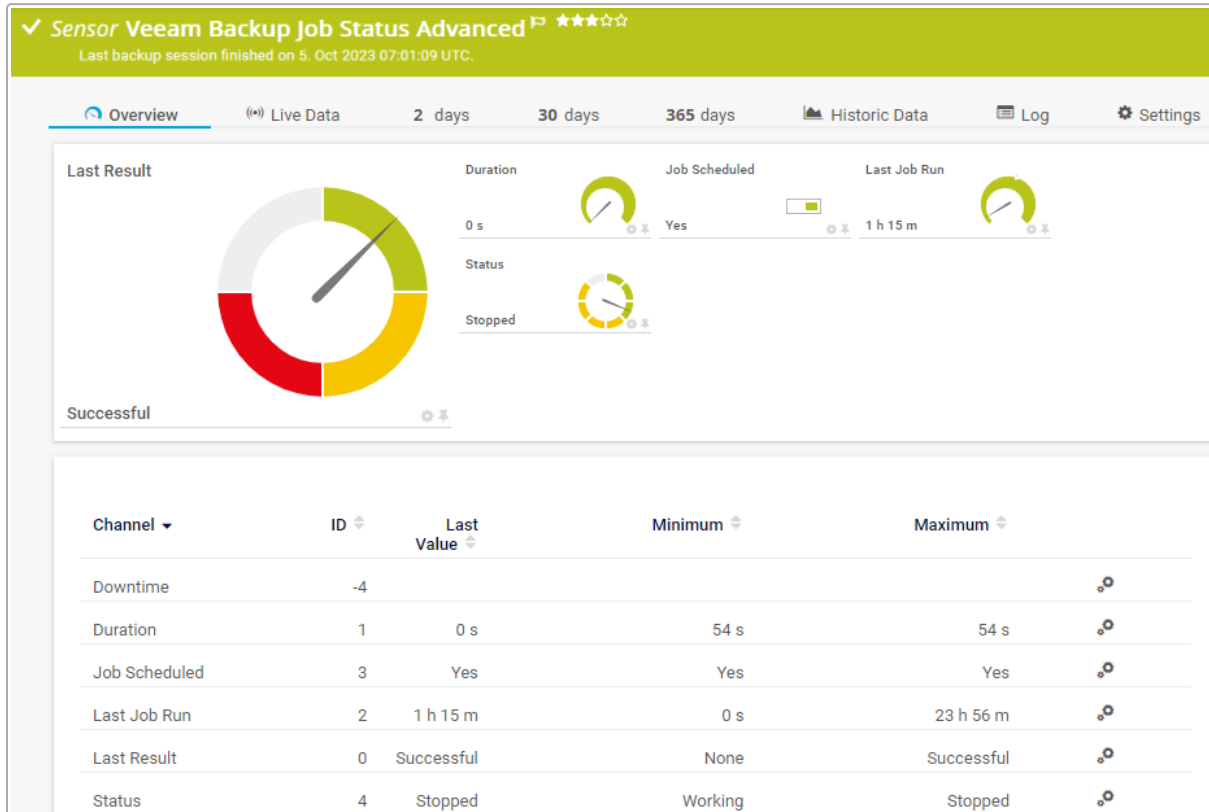
### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.264 Veeam Backup Job Status Advanced Sensor

The Veeam Backup Job Status Advanced sensor monitors the status of a specific backup job that runs on the Veeam Backup Enterprise Manager.



Veeam Backup Job Status Advanced Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>2373</sup>.

### Sensor in Other Languages

- Dutch: Veeam Backup Taakstatus Geavanceerd
- French: Veeam statut de tâche de sauvegarde avancée
- German: Veeam Backupjob-Status (Erweitert)
- Japanese: Veeam バックアップジョブステータス詳細
- Portuguese: Status da tarefa de backup do Veeam (Avançado)
- Russian: Расширенное состояние задания резервного копирования Veeam
- Simplified Chinese: Veeam 备份作业状态高级
- Spanish: Estado del trabajo de Veeam Backup (avanzado)

### Remarks

Consider the following [remarks](#)<sup>2369</sup> and requirements for this sensor:

Remark	Description
Veeam version	This sensor requires that the <a href="#">Veeam Backup Enterprise Manager 10, 11, or 12</a> with the <a href="#">Enterprise Plus</a> license are installed.
Credentials	This sensor requires credentials for Veeam.
Backup jobs	This sensor does not support the following backup job types: <a href="#">Tape</a> , <a href="#">Sure Backup</a> , <a href="#">NAS Backup Copy</a> , and <a href="#">Agent Backup Copy</a> .
Veeam agent	This sensor does not support <a href="#">Veeam Agent Backup Jobs</a> if they are managed by a <a href="#">Veeam Agent</a> .
REST API	This sensor only supports version <a href="#">1.5</a> of the Representational State Transfer (REST) application programming interface (API).
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <a href="#">1 minute</a>.</li> <li>▪ The recommended scanning interval of this sensor is <a href="#">5 minutes</a>.</li> </ul>
Knowledge Base	Knowledge Base: <a href="#">How can I change the status of my Veeam sensors based on whether a job is scheduled or not?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ exampletag ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Example Name

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- veeam



- veeambackup
- veeamenterprisemanager

For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Veeam Specific

**Veeam Specific**

**Job Name** ⓘ *Example Job*

**Job Type** ⓘ *Backup*

**Platform** ⓘ *VMware*

**Job Description** ⓘ *Created by EXAMPLE/johnqpublic at 11/6/2020 7:44 AM.*

Veeam Specific

Setting	Description
Job Name	The name of the backup job that this sensor monitors.
Job Type	The type of backup job that this sensor monitors.
Platform	The platform on which the backup job runs.
Job Description	The description of the backup job that this sensor monitors.

## Sensor Display


**Sensor Display**

**Primary Channel** ⓘ *Downtime*

**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>



Setting	Description
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

**Result Handling** 
 Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>



## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Duration	The duration of the backup job run
Job Scheduled	<p>If the backup job is scheduled</p> <ul style="list-style-type: none"> <li>▪ Up status: No, Yes. Which status the sensor actually shows depends on the <a href="#">lookup file</a> that you choose in the channel settings. <ul style="list-style-type: none"> <li> For more information, see the Knowledge Base: <a href="#">How can I change the status of my Veeam sensors based on whether a job is scheduled or not?</a></li> </ul> </li> <li>▪ Down status: No</li> </ul>
Last Job Run	The time since the last backup job run
Last Result	<p>The last backup job run status</p> <ul style="list-style-type: none"> <li>▪ Up status: Successful</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Failed</li> <li>▪ Unknown status: None</li> </ul> <p> This channel is the primary channel by default.</p>
Status	<p>The backup job run status</p> <ul style="list-style-type: none"> <li>▪ Up status: Starting, Working, Stopped</li> </ul>

Channel	Description
	<ul style="list-style-type: none"><li>▪ Warning status: Stopping, Pausing, Resuming, Never Started, Postprocessing</li><li>▪ Unknown status: Idle</li></ul>

## More

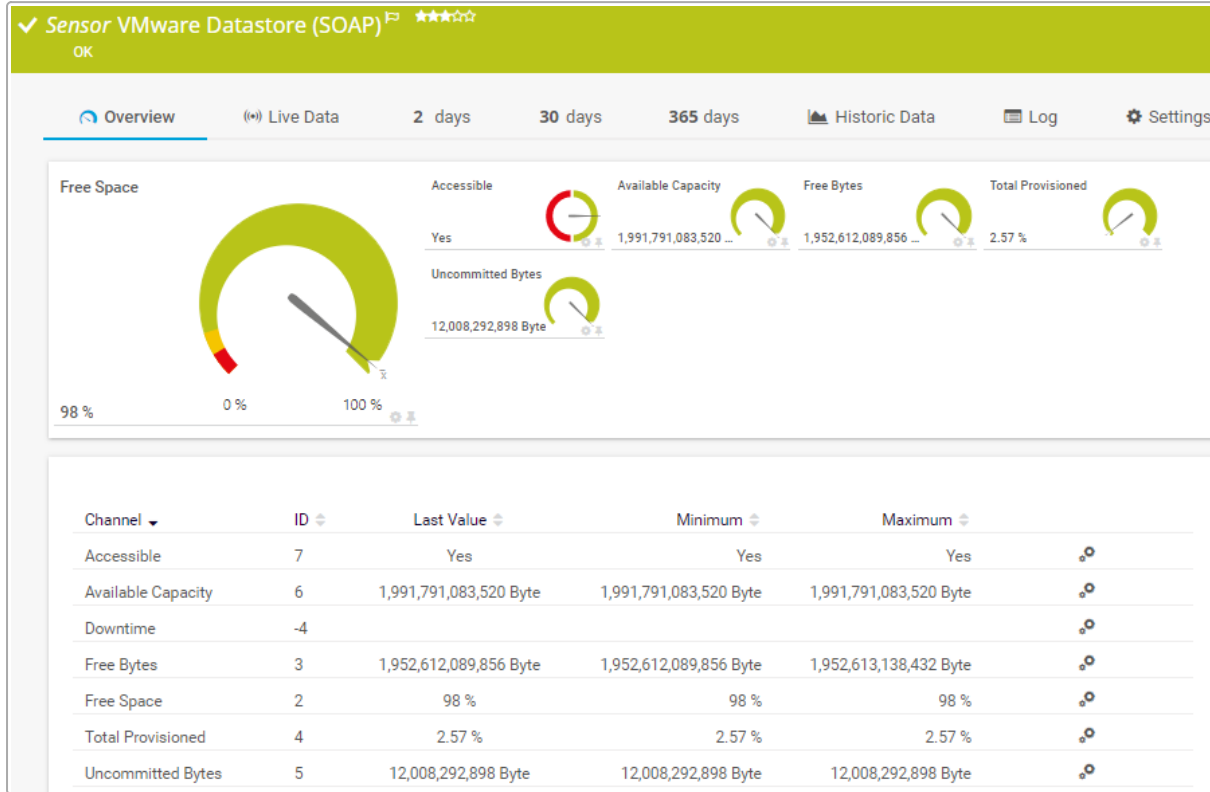
### KNOWLEDGE BASE

How can I change the status of my Veeam sensors based on whether a job is scheduled or not?

- <https://kb.paessler.com/en/topic/89136>

## 7.8.265 VMware Datastore (SOAP) Sensor

The VMware Datastore (SOAP) sensor monitors the disk usage of a VMware datastore using the Simple Object Access Protocol (SOAP).



VMware Datastore (SOAP) Sensor



For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2379]</sup>.

### Sensor in Other Languages

- Dutch: VMware Datastore (SOAP)
- French: VMware Datastore (SOAP)
- German: VMware Datastore (SOAP)
- Japanese: VMware Datastore( SOAP)
- Portuguese: Armazenamento de dados VMware (SOAP)
- Russian: Хранилище данных VMware (SOAP)
- Simplified Chinese: VMware 数据存储 (SOAP)
- Spanish: Almacén de datos VMware (SOAP)


### Remarks

Consider the following [remarks](#)<sup>[2379]</sup> and requirements for this sensor:

Remark	Description
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Windows Server	We recommend Windows Server 2016 on the probe system for best performance of this sensor.
Parent device	This sensor requires that the parent device is a VMware ESXi server as of version 5.2 or vCenter.
Credentials	This sensor requires credentials for VMware/XenServer in the settings of the parent device. Enter a user with sufficient access rights to obtain statistics (read-only usually works).
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">very low</a> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?</a></li> <li>▪ Knowledge Base: <a href="#">Why are my VMware sensors not working after upgrading to VCSA 6.5 U1?</a></li> </ul>

## Settings on VMware Host System

If you set up this sensor on different probes (for example, when using [remote probes](#) or when running a [failover cluster](#)), you might need to change the settings of your VMware host so that it accepts more incoming connections. Otherwise, you might get connection timeouts when running plenty of VMware sensors with a short scanning interval.

 For more information, see the Knowledge Base: [How can I increase the connection limit on VMware systems? PE121.](#)

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- vmwaredatastoreexternsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Datstore Settings

### Datstore Settings

**Managed Object Identifier (MOID)** ⓘ

**Result Handling** ⓘ

Discard result (default)

Store result

Datstore Settings

Setting	Description
Managed Object Identifier (MOID)	The managed object identifier (MOID) of the datastore that this sensor monitors.
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **ⓘ** Downtime

---

Graph Type **ⓘ**
 Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click **🔒** under the corresponding setting name to disable the inheritance and to display its options.



■ For more information, see section [Inheritance of Settings](#).

## Channel List

❗ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Accessible	The accessibility of the datastore <ul style="list-style-type: none"> <li>▪ Up status: Yes</li> <li>▪ Down status: No</li> </ul>
Available Capacity	The available capacity (the physically or virtually available size of the datastore)
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Bytes	The free space (the disk space that is not used by VMs. Used disk space can be either thick-provisioned or used by thin-provisioned virtual disks)
Free Space	The free space (%) (the disk space that is not used by VMs. Used disk space can be either thick-provisioned or used by thin-provisioned virtual disks) <p>❗ This channel is the primary channel by default.</p>
Total Provisioned	The total provisioned disk space (%) (the sum of all potentially used disk space of thin-provisioned and thick-provisioned VM hard drives, that is, the uncommitted bytes plus used bytes)
Uncommitted Bytes	The uncommitted bytes (the disk space that is provisioned for thin-provisioned VMs but not used yet)

## More

### ■ KNOWLEDGE BASE

I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?

- <https://kb.paessler.com/en/topic/66794>

Why are my VMware sensors not working after upgrading to VCSA 6.5 U1?

- <https://kb.paessler.com/en/topic/78274>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

How can I increase the connection limit on VMware systems? PE121

- <https://kb.paessler.com/en/topic/30643>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Monitoring VMware ESXi 5.5 does not work. What can I do?

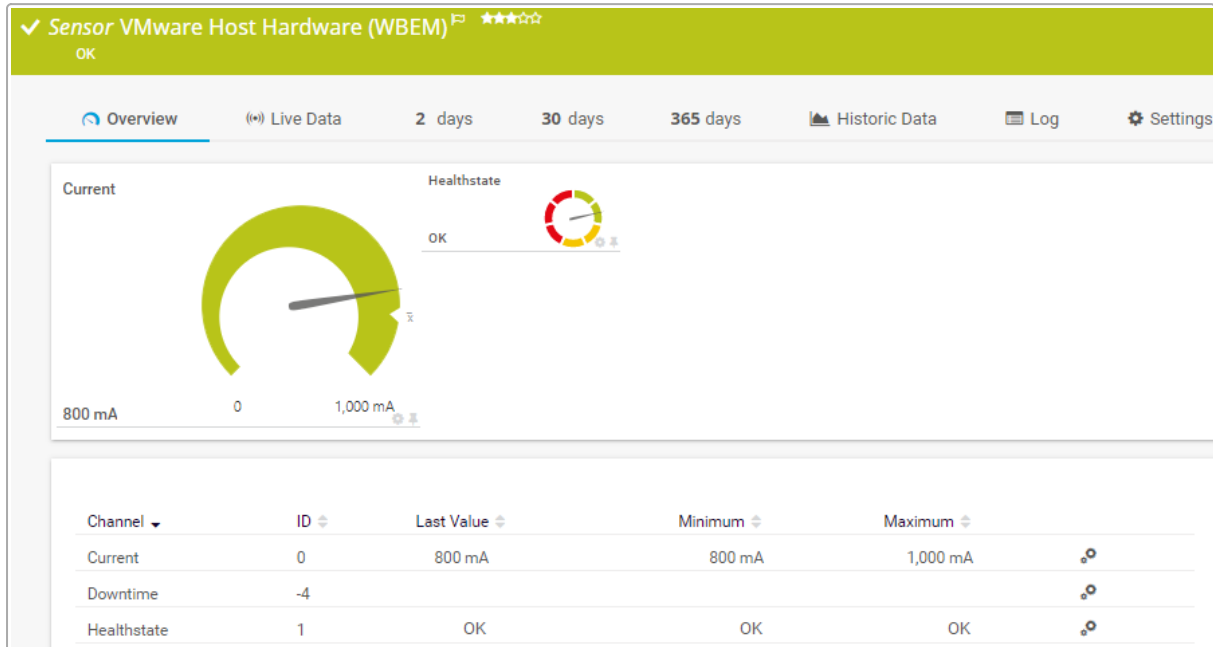
- <https://kb.paessler.com/en/topic/59173>

For which sensor types do you recommend at least Windows Server 2016 and why?

- <https://kb.paessler.com/en/topic/64331>

## 7.8.266 VMware Host Hardware (WBEM) Sensor

The VMware Host Hardware (WBEM) sensor monitors information about the hardware of an ESXi server using Web-based Enterprise Management (WBEM).



VMware Host Hardware (WBEM) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2384]</sup>.

### Sensor in Other Languages

- Dutch: VMware Host Hardware (WBEM)
- French: VMware matériel du serveur hôte (WBEM)
- German: VMware Host Hardware (WBEM)
- Japanese: VMware ホストハードウェア (WBEM)
- Portuguese: Hardware de host VMware (WBEM)
- Russian: Аппаратные средства узла VMware (WBEM)
- Simplified Chinese: VMware 主机硬件 (WBEM)
- Spanish: Hardware de host VMware (WBEM)

### Remarks

Consider the following [remarks](#)<sup>[2381]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Enabled CIM Interface on ESXi Host	This sensor requires that the CIM interface is enabled on the ESXi host. As of ESXi 6.5, you must manually enable CIM.  ■ For more information, see the Knowledge Base: <a href="#">How do I enable the CIM interface on VMware ESXi 6.5?</a>
Windows Server	We recommend Windows Server 2016 on the probe system for best performance of this sensor.
Credentials	This sensor requires credentials for Linux/Solaris/macOS (SSH/WBEM) systems in the settings of the parent device.
Parent device	This sensor requires that the parent device is a VMware ESXi server as of version 5.2.
IPv4	This sensor only supports IPv4.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Knowledge Base	Knowledge Base: <a href="#">Why are my VMware sensors not working after upgrading to VCSA 6.5 U1?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- esxshealthsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## ESXi Server Elements

**ESXi Server Elements**

Hardware Element <sup>ⓘ</sup> *Power Supply 1 Current 1*

This sensor monitors the health of an element as reported by the ESXi server. The sensor can automatically change to a Warning status when the ESXi server returns Degraded/Warning for this particular element. It can change to a Down status when the server reports any of the following errors: Minor / Major / Critical / Non recoverable.

Automatic Sensor Status <sup>ⓘ</sup>

- Set sensor to warning or down status (default)
- Report the current reading

Result Handling <sup>ⓘ</sup>

- Discard result (default)
- Store result

ESXi Server Elements

Setting	Description
Hardware Element	The hardware element that this sensor monitors.
Automatic Sensor Status	<p>Define if the sensor changes its <a href="#">status</a> depending on the health status reading:</p> <ul style="list-style-type: none"> <li>▪ Set sensor to warning or down status (default): Set the sensor to the Warning or the Down status when the server returns respective values. The sensor also changes to the Down status if the connection to the server fails.</li> <li>▪ Report the current reading: Never change the sensor's status dependent on the values returned by the server. The sensor only changes to the Down status if the connection to the server fails.</li> </ul>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Current	The current
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Healthstate	The health status <ul style="list-style-type: none"> <li>▪ Up status: OK Unknown</li> <li>▪ Warning status: Degraded, Minor</li> <li>▪ Down status: Critical, Major, Non Recoverable Error</li> </ul>
Power	The average host power usage
Rotational Speed	The fan RPM
Temperature	The temperature

## More

### ■ KNOWLEDGE BASE

Why are my VMware sensors not working after upgrading to VCSA 6.5 U1?

- <https://kb.paessler.com/en/topic/78274>

How do I enable the CIM interface on VMware ESXi 6.5?

- <https://kb.paessler.com/en/topic/76255>

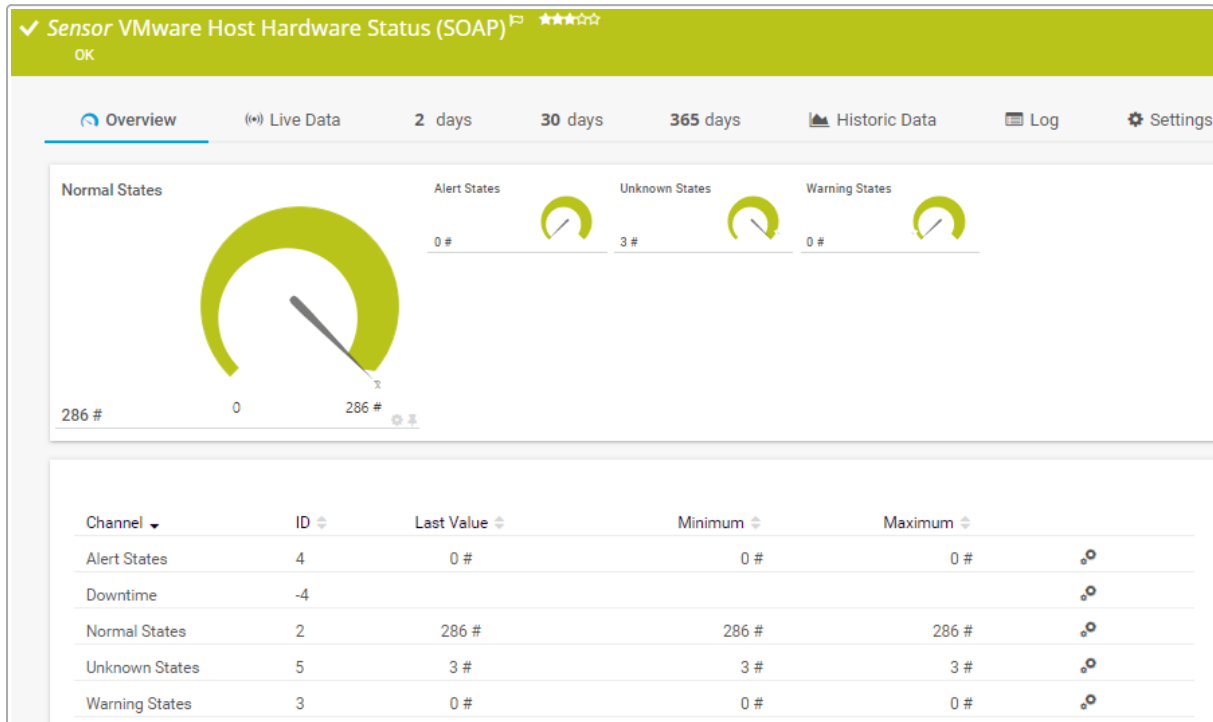
What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.267 VMware Host Hardware Status (SOAP) Sensor

The VMware Host Hardware Status (SOAP) sensor monitors the hardware status of a VMware host server using the Simple Object Access Protocol (SOAP). It gives you a general status overview of the host.

**i** The sensor also shows any states other than **normal** in the sensor message.



VMware Host Hardware Status (SOAP) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).



### Sensor in Other Languages

- Dutch: VMware Host Hardware Status (SOAP)
- French: VMware statut du matériel du serveur hôte (SOAP)
- German: VMware Hostserver Hardware-Zustand (SOAP)
- Japanese: VMware ホストハードウェアの状態 (SOAP)
- Portuguese: Status do hardware de host VMware (SOAP)
- Russian: Состояние аппаратных средств узла VMware (SOAP)
- Simplified Chinese: VMware 主机硬件状态 (SOAP)
- Spanish: Estado de hardware host VMware (SOAP)

### Remarks


Consider the following [remarks](#) and requirements for this sensor:



Remark	Description
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Windows Server	We recommend Windows Server 2016 on the probe system for best performance of this sensor.
Credentials	This sensor requires credentials for VMware/XenServer in the settings of the parent device. Enter a user with sufficient access rights to obtain statistics (read-only usually works).
Parent device	This sensor requires that the parent device is a VMware ESXi server as of version 5.2. We recommend that you do not use this sensor on your vCenter. Reliable hardware information can only be provided when this sensor is created on your physical host server as parent device.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <a href="#">medium</a> performance impact.
Sensors	This sensor only shows items that report an actual state, so you might see more "sensors" in your vSphere client than the number of states available in the channels of this sensor
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?</a></li> <li>▪ Knowledge Base: <a href="#">Why are my VMware sensors not working after upgrading to VCSA 6.5 U1?</a></li> </ul>

## Settings on VMware Host System

If you set up this sensor on different probes (for example, when using [remote probes](#) or when running a [failover cluster](#)), you might need to change the settings of your VMware host so that it accepts more incoming connections. Otherwise, you might get connection timeouts when running plenty of VMware sensors with a short scanning interval.

 For more information, see the Knowledge Base: [How can I increase the connection limit on VMware systems? PE121.](#)

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- esxserverhosthealthsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## VMware Host Settings

### VMware Host Settings

**Managed Object Identifier (MOID)** ⓘ

**Known Warnings** ⓘ

**Known Errors** ⓘ

**Handling of Unknown States** ⓘ

Show unknown states (default)

Do not show unknown states

**Result Handling** ⓘ

Discard result (default)

Store result

VMware Host Settings

Setting	Description
Managed Object Identifier (MOID)	The managed object identifier of the host that this sensor monitors.
Known Warnings	<p>Enter one or more warning messages from the VMware host that you want to ignore. Use semicolons (;) as separators, for example, <a href="#">Power Supply 7</a>; <a href="#">Power Supply 8</a>. Enter a string or leave the field empty.</p> <p> ⓘ Warning messages that you enter do not affect the <a href="#">sensor status</a>.</p>

Setting	Description
	<p><b>i</b> We strongly recommend that you use this filter for known issues only. For example, for states that systems return because of errors in the vendors' CIM extensions. Because of this, the sensor might never show the Up status although the vSphere client does not show any warnings.</p>
Known Errors	<p>Enter one or more error messages from the VMware host that you want to ignore. Use semicolons (;) as separators, for example, <a href="#">Power Supply 7</a>; <a href="#">Power Supply 8</a>. Enter a string or leave the field empty.</p> <p><b>i</b> Error messages that you enter do not affect the sensor status.</p> <p><b>i</b> We strongly recommend that you use this filter for known issues only. For example, for states that systems return because of errors in the vendors' CIM extensions. Because of this, the sensor might never show the Up status although the vSphere client does not show any errors.</p>
Handling of Unknown States	<p>Define the sensor behavior when the vSphere client reports unknown states:</p> <ul style="list-style-type: none"> <li>▪ Show unknown states (default): Show unknown states in the status message and set the sensor to the Warning status.</li> <li>▪ Do not show unknown states: Do not show unknown states in the status message and do not change the sensor status.</li> </ul>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display


**Sensor Display**

Primary Channel **i** Downtime


---


Graph Type **i** 
 Show channels independently (default)
   
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Alert States	The total number of items in the <a href="#">alert</a> status as the vSphere client reports

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Normal States	The total number of items in the <b>normal</b> status as the vSphere client reports   This channel is the primary channel by default.
Unknown States	The total number of items in the <b>unknown</b> status as the vSphere client reports
Warning States	The total number of items in the <b>warning</b> status as the vSphere client reports

## More

### ■ KNOWLEDGE BASE

I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?

- <https://kb.paessler.com/en/topic/66794>

Why are my VMware sensors not working after upgrading to VCSA 6.5 U1?

- <https://kb.paessler.com/en/topic/78274>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

How can I increase the connection limit on VMware systems? PE121

- <https://kb.paessler.com/en/topic/30643>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Monitoring VMware ESXi 5.5 does not work. What can I do?

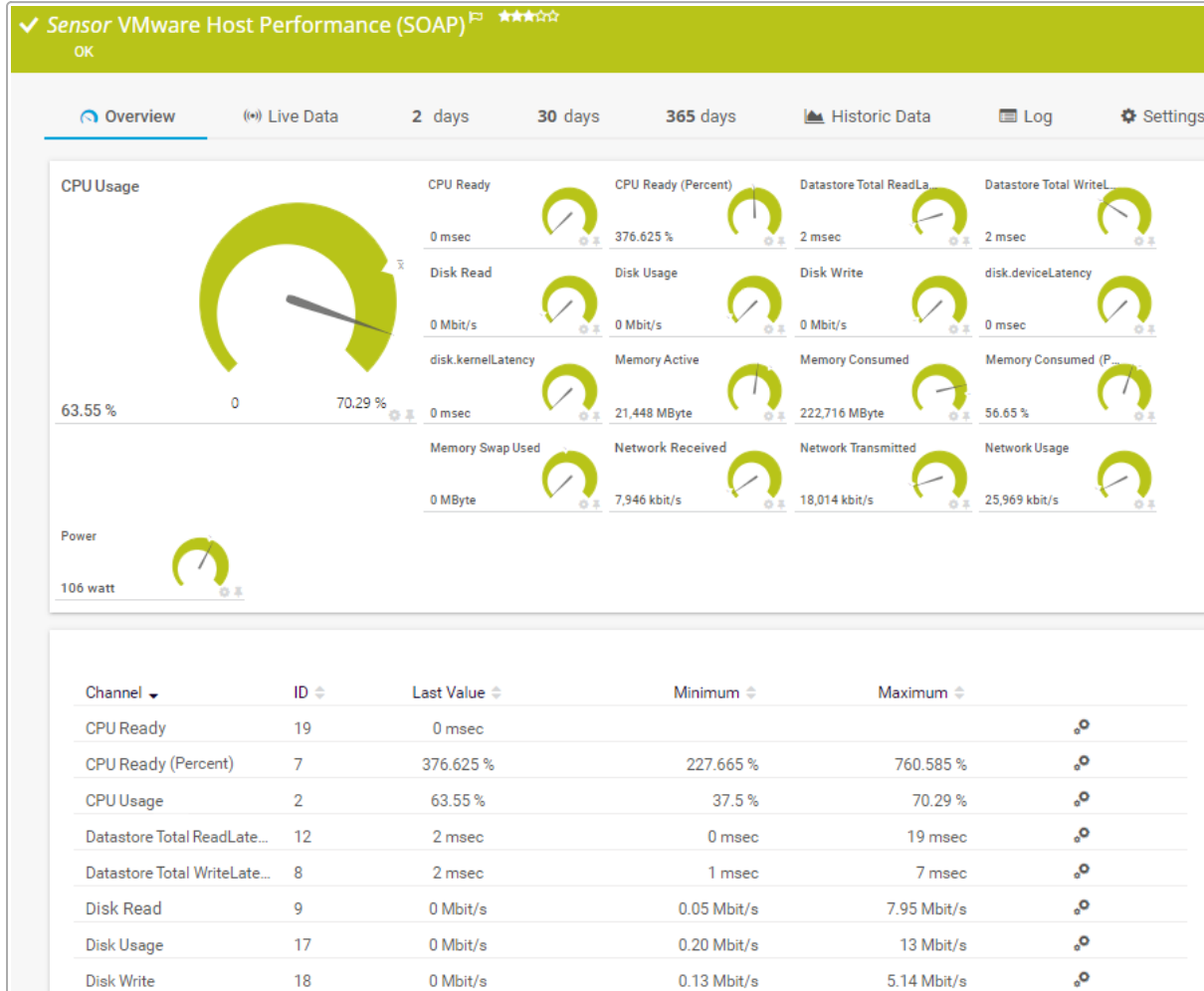
- <https://kb.paessler.com/en/topic/59173>

For which sensor types do you recommend at least Windows Server 2016 and why?

- <https://kb.paessler.com/en/topic/64331>

## 7.8.268 VMware Host Performance (SOAP) Sensor

The VMware Host Performance (SOAP) sensor monitors a VMware host server using the Simple Object Access Protocol (SOAP).



VMware Host Performance (SOAP) Sensor



For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: VMware Host Prestaties (SOAP)
- French: VMware performances du serveur hôte (SOAP)
- German: VMware Hostserver Leistung (SOAP)
- Japanese: VMware ホストパフォーマンス (SOAP)
- Portuguese: Performance do host VMware (SOAP)
- Russian: Работа узла VMware (SOAP)
- Simplified Chinese: VMware 主机性能 (SOAP)
- Spanish: Rendimiento de host VMware (SOAP)


## Remarks

Consider the following [remarks](#) <sup>2393</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
.NET 4.7.2 or later	This sensor requires <b>.NET 4.7.2 or later</b> from Microsoft on the probe system. In a cluster, install it on every cluster node.   If the framework is missing, you cannot create this sensor.   For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a>
Windows Server	We recommend Windows Server 2016 on the probe system for best performance of this sensor.
Parent device	This sensor requires that the parent device is a VMware ESXi server as of version 5.2. We recommend that you do not use this sensor on your vCenter. Reliable hardware information can only be provided when this sensor is created on your physical host server as parent device.
Credentials	This sensor requires credentials for VMware/XenServer in the settings of the parent device. Enter a user with sufficient access rights to obtain statistics (read-only usually works).
IPv6	This sensor supports IPv6.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?</a></li> <li>▪ Knowledge Base: <a href="#">Why are my VMware sensors not working after upgrading to VCSA 6.5 U1?</a></li> </ul>

## Settings on VMware Host System

If you set up this sensor on different probes (for example, when using [remote probes](#) or when running a [failover cluster](#)), you might need to change the settings of your VMware host so that it accepts more incoming connections. Otherwise, you might get connection timeouts when running plenty of VMware sensors with a short scanning interval.

 For more information, see the Knowledge Base: [How can I increase the connection limit on VMware systems? PE121.](#)

## Basic Sensor Settings

Basic Sensor Settings

Sensor Name ⓘ Example Name

---

Tags ⓘ exampletag ✕ +

---

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- esxserverhostsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## VMware Host Settings

VMware Host Settings

Managed Object Identifier (MOID) ⓘ 1a2b3d4c

---

Result Handling ⓘ  Discard result (default)  
 Store result

VMware Host Settings

Setting	Description
Managed Object Identifier (MOID)	The managed object identifier of the host that this sensor monitors.
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>



Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime


---

Graph Type **i**  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>+</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CPU Ready (Percent)	The CPU readiness (%)
CPU Usage	The CPU usage <b>i</b> This channel is the primary channel by default.
Datastore Total ReadLatency	The datastore total read latency
Datastore Total WriteLatency	The datastore total write latency
Disk Read	The disk read speed
Disk Usage	The disk usage
Disk Write	The disk write speed
Disk.DeviceLatency	The disk device latency
Disk.KernelLatency	The disk kernel latency
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Memory Active	The active memory
Memory Consumed	The consumed memory
Memory Consumed (Percent)	The memory consumed (%)
Memory Swap Used	The used memory swap
Network Received	The received bytes

Channel	Description
Network Transmitted	The transmitted bytes
Network Usage	The total network usage
Power	The average host power usage

## More

### ■ KNOWLEDGE BASE

I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?

- <https://kb.paessler.com/en/topic/66794>

Why are my VMware sensors not working after upgrading to VCSA 6.5 U1?

- <https://kb.paessler.com/en/topic/78274>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

How can I increase the connection limit on VMware systems? PE121

- <https://kb.paessler.com/en/topic/30643>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Monitoring VMware ESXi 5.5 does not work. What can I do?

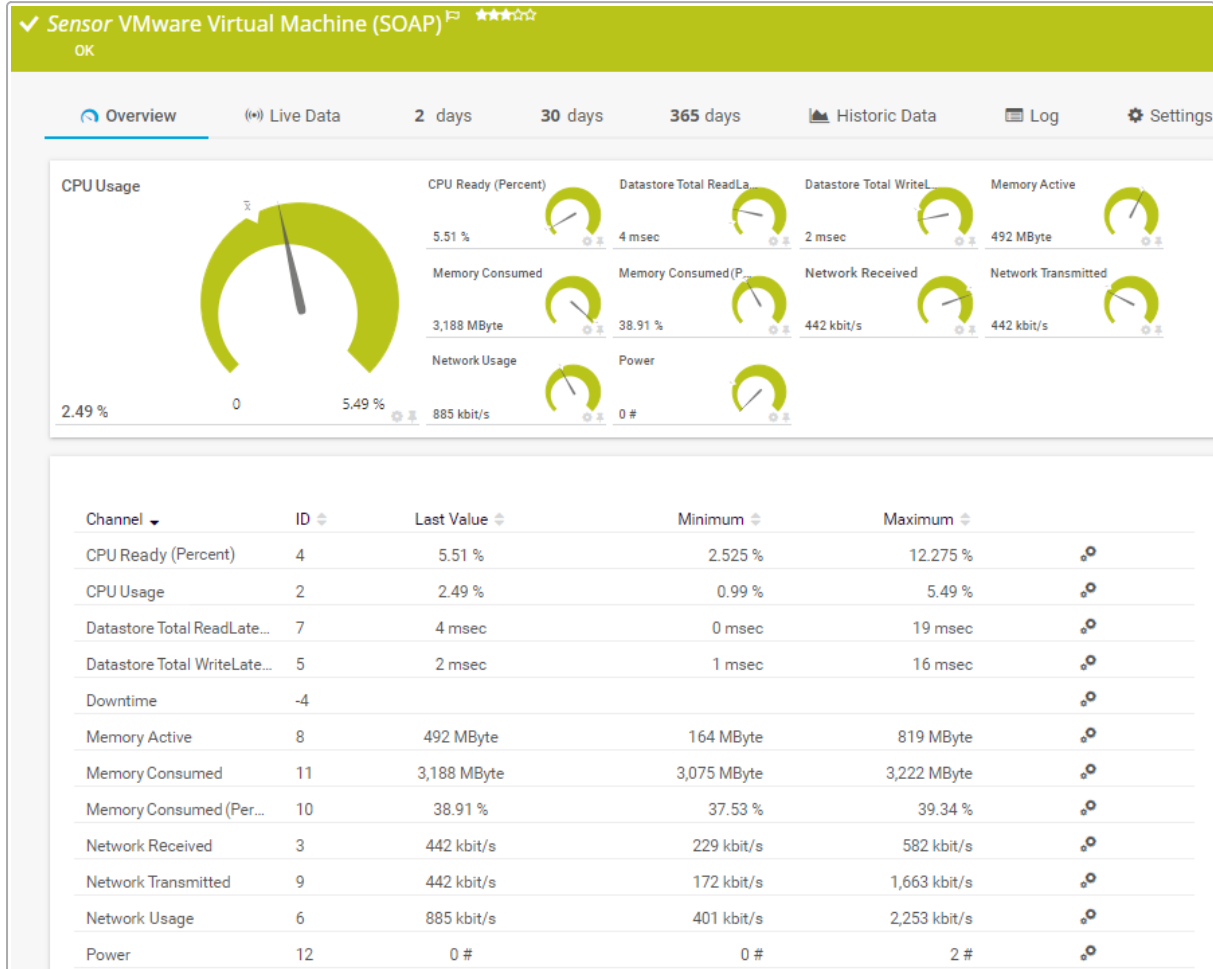
- <https://kb.paessler.com/en/topic/59173>

For which sensor types do you recommend at least Windows Server 2016 and why?

- <https://kb.paessler.com/en/topic/64331>

## 7.8.269 VMware Virtual Machine (SOAP) Sensor

The VMware Virtual Machine (SOAP) sensor monitors a virtual machine (VM) on a VMware host server using the Simple Object Access Protocol (SOAP).



VMware Virtual Machine (SOAP) Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: VMware Virtuele Machine (SOAP)
- French: VMware machine virtuelle (SOAP)
- German: VMware Virtual Machine (SOAP)
- Japanese: VMware 仮想マシン (SOAP)
- Portuguese: Máquina virtual VMware (SOAP)
- Russian: Виртуальная машина VMware (SOAP)
- Simplified Chinese: VMware 虚拟机 (SOAP)
- Spanish: Máquina virtual VMware (SOAP)

## Remarks

Consider the following [remarks](#) <sup>[2399]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
.NET 4.7.2 or later	This sensor requires <b>.NET 4.7.2 or later</b> from Microsoft on the probe system. In a cluster, install it on every cluster node.   If the framework is missing, you cannot create this sensor.   For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a>
Windows Server	We recommend Windows Server 2016 on the probe system for best performance of this sensor.
Credentials	This sensor requires credentials for VMware/XenServer in the settings of the parent device. Enter a user with sufficient access rights to obtain statistics (read-only usually works).
Parent device	We recommend that you use <b>vCenter</b> as parent device. If the monitored VM changes the host server via <b>vMotion</b> , PRTG can still continue monitoring. The sensor can monitor VMware ESXi server as of version 5.2.
VMs	For VMware virtual machines, disk usage channels are only available as of virtual hardware version 8.   PRTG requests a full list of all VMs configured on the target device (also those that do not run). Because of this, it might take a few seconds before the dialog appears.
IPv6	This sensor supports IPv6.
Knowledge Base	<ul style="list-style-type: none"> <li>▪ Knowledge Base: <a href="#">I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?</a></li> <li>▪ Knowledge Base: <a href="#">Why are my VMware sensors not working after upgrading to VCSA 6.5 U1?</a></li> </ul>

## Settings on VMware Host System

If you set up this sensor on different probes (for example, when using [remote probes](#) or when running a [failover cluster](#)), you might need to change the settings of your VMware host so that it accepts more incoming connections. Otherwise, you might get connection timeouts when running plenty of VMware sensors with a short scanning interval.

For more information, see the Knowledge Base: [How can I increase the connection limit on VMware systems? PE121](#).

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- esxservermsensor

For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### VMware Virtual Machine Settings

#### VMware Virtual Machine Settings

**Managed Object Identifier (MOID)** ⓘ 2

---

**Powered-Off VM Handling** ⓘ  Alarm when VM is powered off (default)  
 Ignore powered-off state

---

**Result Handling** ⓘ  Discard result (default)  
 Store result

VMware Virtual Machine Settings

Setting	Description
Managed Object Identifier (MOID)	The managed object identifier (MOID) of the VM that this sensor monitors.
Powered-Off VM Handling	<p>Define how the sensor reacts to VMs that are powered off:</p> <ul style="list-style-type: none"> <li>▪ Alarm when VM is powered off (default): Change to the Down <a href="#">status</a> if the VM is powered off.</li> </ul> <p>ⓘ If the sensor is in the Down status, it does not record any data in any of its channels.</p> <ul style="list-style-type: none"> <li>▪ Ignore powered off state: Do not change to the Down status if the VM is powered off. The sensor reports zero values instead.</li> </ul>

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p> <p>ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CPU Ready (Percent)	The CPU readiness (%)
CPU Usage	The CPU usage  This channel is the primary channel by default.
Datastore Total Read Latency	The datastore total read latency
Datastore Total Write Latency	The datastore total write latency
Disk Read	The disk read speed
Disk Usage	The disk usage
Disk Write	The disk write speed
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status



Channel	Description
Memory Active	The active memory
Memory Consumed	The consumed memory
Memory Consumed (Percent)	The memory consumed (%)
Network Received	The received bytes
Network Transmitted	The transmitted bytes
Network Usage	The total network usage
Power	The average host power usage

## More

### ■ KNOWLEDGE BASE

I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?

- <https://kb.paessler.com/en/topic/66794>

Why are my VMware sensors not working after upgrading to VCSA 6.5 U1?

- <https://kb.paessler.com/en/topic/78274>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

How can I increase the connection limit on VMware systems? PE121

- <https://kb.paessler.com/en/topic/30643>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Monitoring VMware ESXi 5.5 does not work. What can I do?

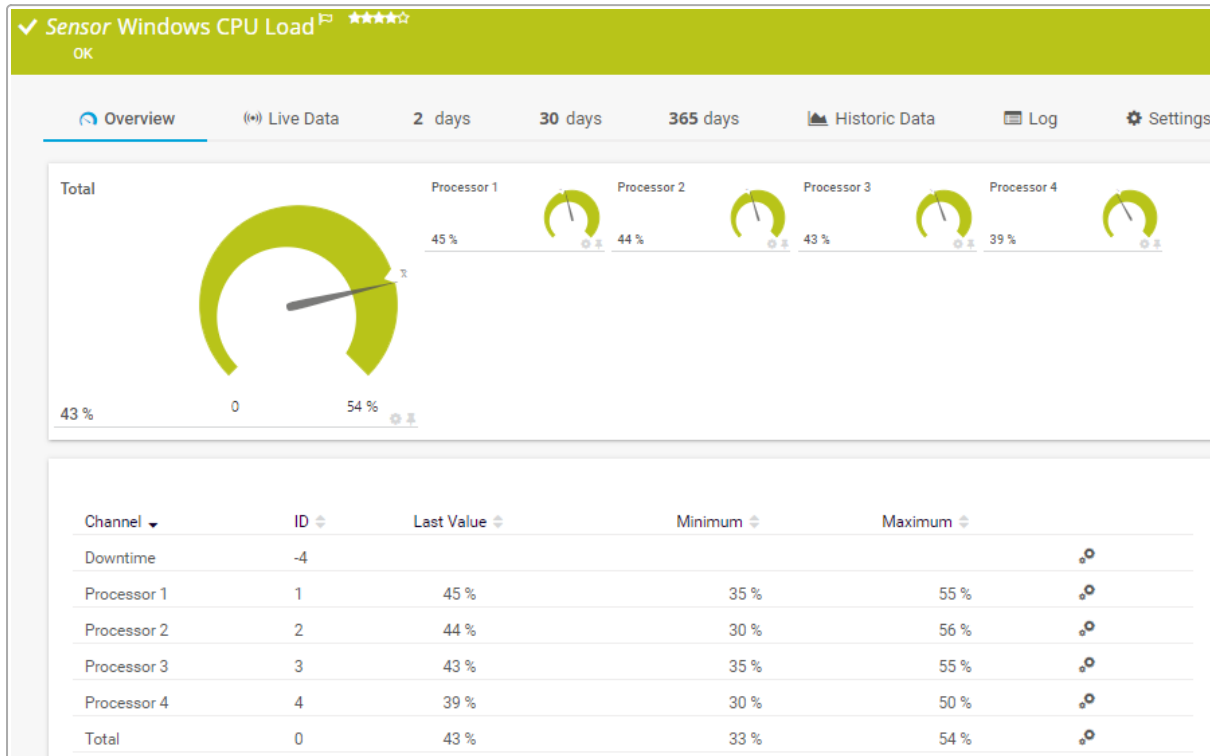
- <https://kb.paessler.com/en/topic/59173>

For which sensor types do you recommend at least Windows Server 2016 and why?

- <https://kb.paessler.com/en/topic/64331>

## 7.8.270 Windows CPU Load Sensor

The Windows CPU Load sensor monitors the CPU load on a system via Windows Management Instrumentation (WMI) or Windows performance counters, as configured in the [Windows Compatibility Options](#) of the parent device.



Windows CPU Load Sensor






For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2408]</sup>.

### Sensor in Other Languages


- Dutch: Windows Processor Belasting
- French: Windows charge CPU
- German: Windows CPU-Last
- Japanese: Windows CPU 負荷
- Portuguese: Carga de CPU Windows
- Russian: Загрузка ЦП Windows
- Simplified Chinese: Windows CPU 负载
- Spanish: Carga de CPU Windows

### Remarks

Consider the following [remarks](#)<sup>[2404]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Windows version	This sensor requires <a href="#">at least Windows Server 2008 R2</a> on the probe system (on every cluster node, if on a cluster probe).   <b>WoW64</b> must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the PRTG probe service only runs with 32-bit support. Without it, WMI sensors do not work.
Remote Registry Windows service	This sensor requires that the <a href="#">Remote Registry</a> Windows service runs on the target system.   If this service does not run, a connection via performance counters is not possible. However, WMI connections might still work.   To enable the service, log in to the respective system and open the services manager (for example, via <code>services.msc</code> ). In the list, find the respective service and set its Start Type to Automatic.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.   We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system.  Otherwise, a connection via performance counters is not possible. However, WMI connections might still work.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Hybrid Approach: Performance Counters and WMI

 By default, this sensor uses WMI to request monitoring data. You can change the default behavior to a [hybrid approach](#) in the Windows Compatibility Options of the parent [device's settings](#) on which you create this sensor: if you choose this option, the sensor first tries to query data via [Windows performance counters](#) and uses WMI as a fallback if performance counters are not available. When running in fallback mode, the sensor tries to connect via performance counters again after 24 hours.

**i** Sensors that use the WMI protocol have a high impact on the system performance. Try to stay below 200 WMI sensors per [probe](#). Above this number, consider using multiple [remote probes](#) for load balancing.

**i** For a general introduction to the technology behind WMI, see section [Monitoring via WMI](#).

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- cpuloadsensor
- wmicpuloadsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>[667]</sup>.

## Debug Options

### Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Alternative WMI Query

**Alternative WMI Query**

WMI sensors use the most efficient and accurate WMI queries possible. However, different Windows versions and even different patch levels on the target systems can lead to changes in some WMI classes. These changes often result in errors like *class not valid* or *invalid data*. If these errors persist, try the option *Use the alternative WMI query method*.

Query Method <sup>?</sup>  Use the default WMI query method (default)  
 Use the alternative WMI query method

Alternative WMI Query

Setting	Description
Query Method	<p>Select the method that the sensor uses to query via WMI:</p> <ul style="list-style-type: none"> <li>▪ Use the default WMI query method (default): Use the standard method to query WMI. We recommend that you use this option.</li> <li>▪ Use the alternative WMI query method: Use an alternative method to query WMI for better compatibility if WMI sensors return errors such as <a href="#">class not valid</a> or <a href="#">invalid data</a>.</li> </ul>

## Sensor Display

**Sensor Display**

Primary Channel <sup>?</sup> Downtime


Graph Type <sup>?</sup>  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><sup>i</sup> You can set a different primary channel later by clicking <sup>?</sup> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><sup>i</sup> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>

Setting	Description
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Processor [#]	The CPU load of the processor (%)
Total	<p>The total CPU load (%)</p> <p> This channel is the primary channel by default.</p>

## More

### KNOWLEDGE BASE

What security features does PRTG include?

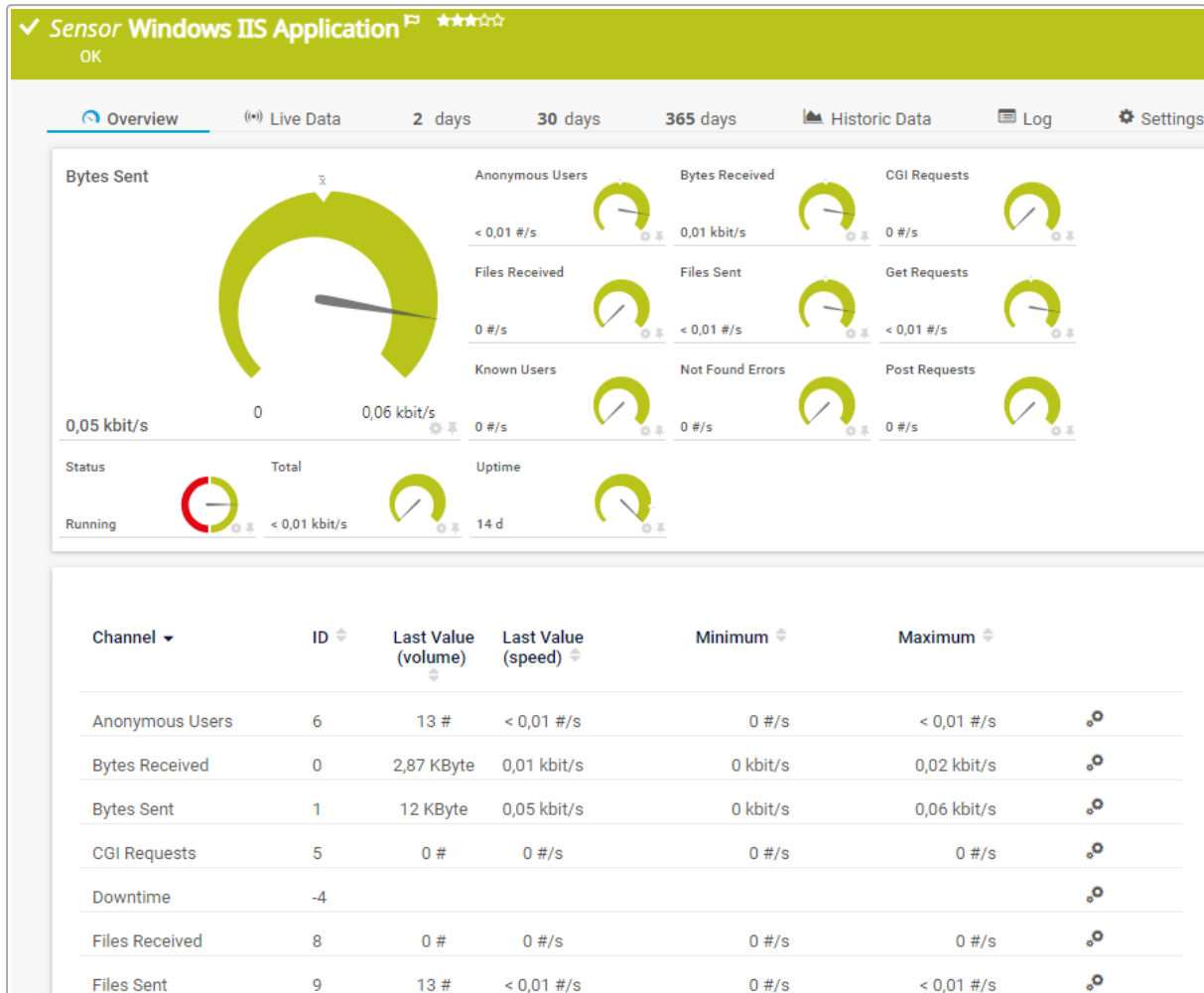
- <https://kb.paessler.com/en/topic/61108>

My Windows sensors do not work when using direct performance counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>

## 7.8.271 Windows IIS Application Sensor

The Windows IIS Application sensor monitors a Microsoft Internet Information Services (IIS) server via Windows Management Instrumentation (WMI). It can also monitor applications that use IIS, such as Microsoft SharePoint or Microsoft Reporting Services (SSRS).



Windows IIS Application Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).


### Sensor in Other Languages

- Dutch: Windows IIS Toepassing
- French: Windows IIS application
- German: Windows IIS-Anwendung
- Japanese: Windows IIS アプリケーション
- Portuguese: Aplicativo Windows IIS
- Russian: Приложение Windows IIS
- Simplified Chinese: Windows IIS 应用程序

- Spanish: Aplicación IIS Windows

## Remarks

Consider the following [remarks](#) <sup>2410</sup> and requirements for this sensor:

Remark	Description
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
Performance counters	The sensor cannot return data for the channels Status, Uptime, and Total when using performance counters. We recommend that you use WMI only (default) as Preferred Data Source in the <a href="#">Windows Compatibility Options</a> of the parent device.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>medium</b> performance impact.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiis

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.



## Windows Internet Information Services

Windows Internet Information Services
Instance ⓘ *\_Total*

Windows Internet Information Services

Setting	Description
Instance	The unique instance name of the web service that this sensor monitors.

## Debug Options

Debug Options
Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display


Sensor Display

Primary Channel ⓘ Downtime


---


Graph Type ⓘ
 Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Anonymous Users	The number of anonymous users
Bytes Received	The number of bytes received

Channel	Description
Bytes Sent	The number of bytes sent <b>i</b> This channel is the primary channel by default.
CGI Requests	The number of CGI requests
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Files Received	The number of files received
Files Sent	The number of files sent
Get Requests	The number of GET requests
Known Users	The number of known users
Not Found Errors	The number of not found errors
Post Requests	The number of POST requests
Status	The web service status <ul style="list-style-type: none"> <li>▪ Up status: Running</li> <li>▪ Down status: Stopped</li> </ul>
Total	The total
Uptime	The uptime

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

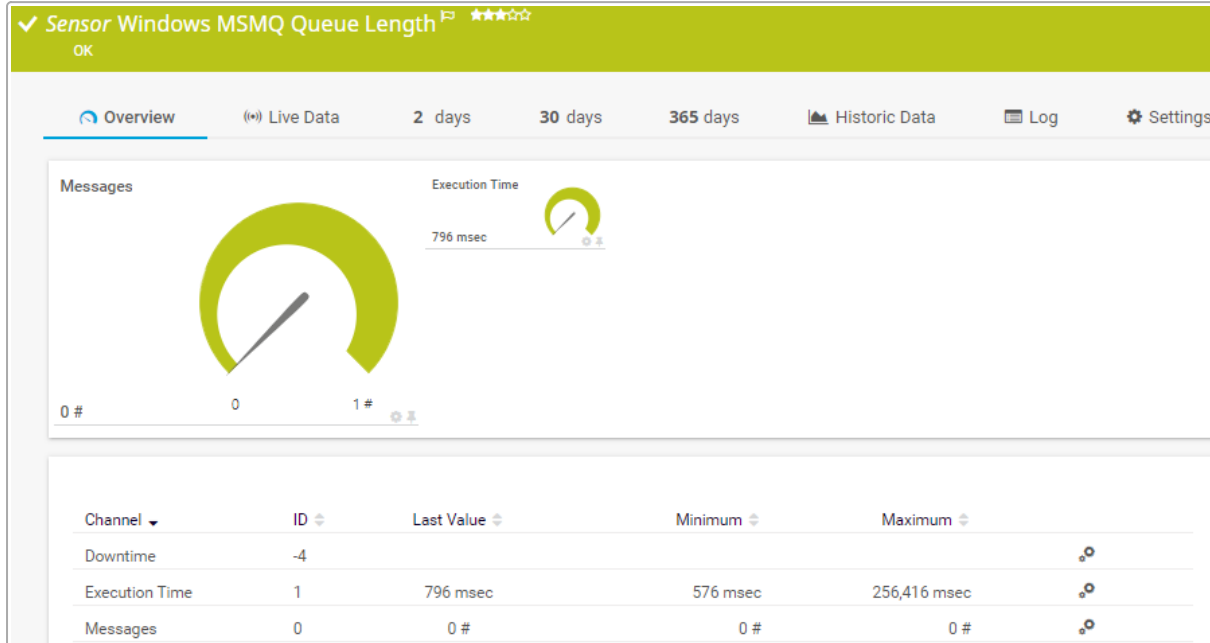
- <https://kb.paessler.com/en/topic/61108>

My Windows sensors do not work when using direct performance counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>

## 7.8.272 Windows MSMQ Queue Length Sensor

The Windows MSMQ Queue Length sensor reads the number of messages in a Microsoft message queue of the parent device.



Windows MSMQ Queue Length Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2418]</sup>.

### Sensor in Other Languages

- Dutch: Windows MSMQ wachtrijlengte
- French: Windows MSMQ longueur de la file d'attente
- German: Windows MSMQ Queue-Länge
- Japanese: Windows MSMQ キュー長
- Portuguese: Comprimento da fila MSMQ Windows
- Russian: Длина очереди Windows MSMQ
- Simplified Chinese: Windows MSMQ 队列长度
- Spanish: Longitud de cola MSMQ Windows

### Remarks

Consider the following [remarks](#)<sup>[2414]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
MSMQ service	<p>This sensor requires that the <a href="#">Microsoft Message Queuing (MSMQ)</a> service runs on both the probe system and the target system. Depending on your Windows version, you might first need to install the <a href="#">MSMQ Server</a>.</p> <p><b>i</b> To enable the service, log in to the respective system and open the services manager (for example, via <code>services.msc</code>). In the list, find the respective service and set its Start Type to Automatic.</p> <p><b>i</b> When installing MSMQ Server, make sure that you install it including the <a href="#">Directory Service</a>. Depending on your Windows installation, this might have a different name, such as:</p> <ul style="list-style-type: none"> <li>▫ MSMQ Active Directory Domain Service Integration</li> <li>▫ Directory Service Integration</li> <li>▫ Active Directory Integration</li> </ul> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">How do I activate Message Queuing in my Windows installation?</a></p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node. If the sensor shows the error PE087, additionally install .NET 3.5 on the probe system.</p> <p><b>i</b> If the framework is missing, you cannot create this sensor.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Windows Server	We recommend Windows Server 2016 on the probe system for best performance of this sensor.
Credentials	<p>This sensor requires credentials for Windows systems.</p> <p><b>i</b> We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system. Otherwise, the sensor cannot correctly connect.</p>
Subqueues	This sensor cannot monitor subqueues.
Add Sensor dialog	If no message queues are available in the Add Sensor dialog, you see a corresponding message.
IPv6	This sensor supports IPv6.

Remark	Description
Knowledge Base	Knowledge Base: <a href="#">How do I activate Message Queuing in my Windows installation?</a>
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

**Tags** ⓘ  ✕ ⊕

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- ptfsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Sensor Settings

#### Sensor Settings

**Message Queue** ⓘ *All Outgoing Queues*

**Message Queue Type** ⓘ *OUTGOING*

**Minimum Message Age** ⓘ \_\_\_\_\_

**If Value Changes** ⓘ

Ignore (default)

Trigger 'change' notification

Sensor Settings

Setting	Description
Message Queue	The name of the message queue that this sensor monitors.
Message Queue Type	The type of the message queue that this sensor monitors.
Minimum Message Age	Optionally define an age in minutes that the message must be for the sensor to count it. If you set a minimum message age, the sensor does not regard messages that are younger than this age. If you leave this field empty, the sensor does not check for the message age. Enter an integer or leave the field empty.
If Value Changes	<p>Define what the sensor does when its value changes:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> <li>▪ Trigger 'change' notification: Send an internal message that indicates a change.</li> </ul> <p><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</p>

## Debug Options

**Debug Options**

Result Handling **i**

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.



Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Execution Time	The execution time
Messages	The total number of messages in the queue  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

How do I activate Message Queuing in my Windows installation?

- <https://kb.paessler.com/en/topic/25963>

Which .NET version does PRTG require?

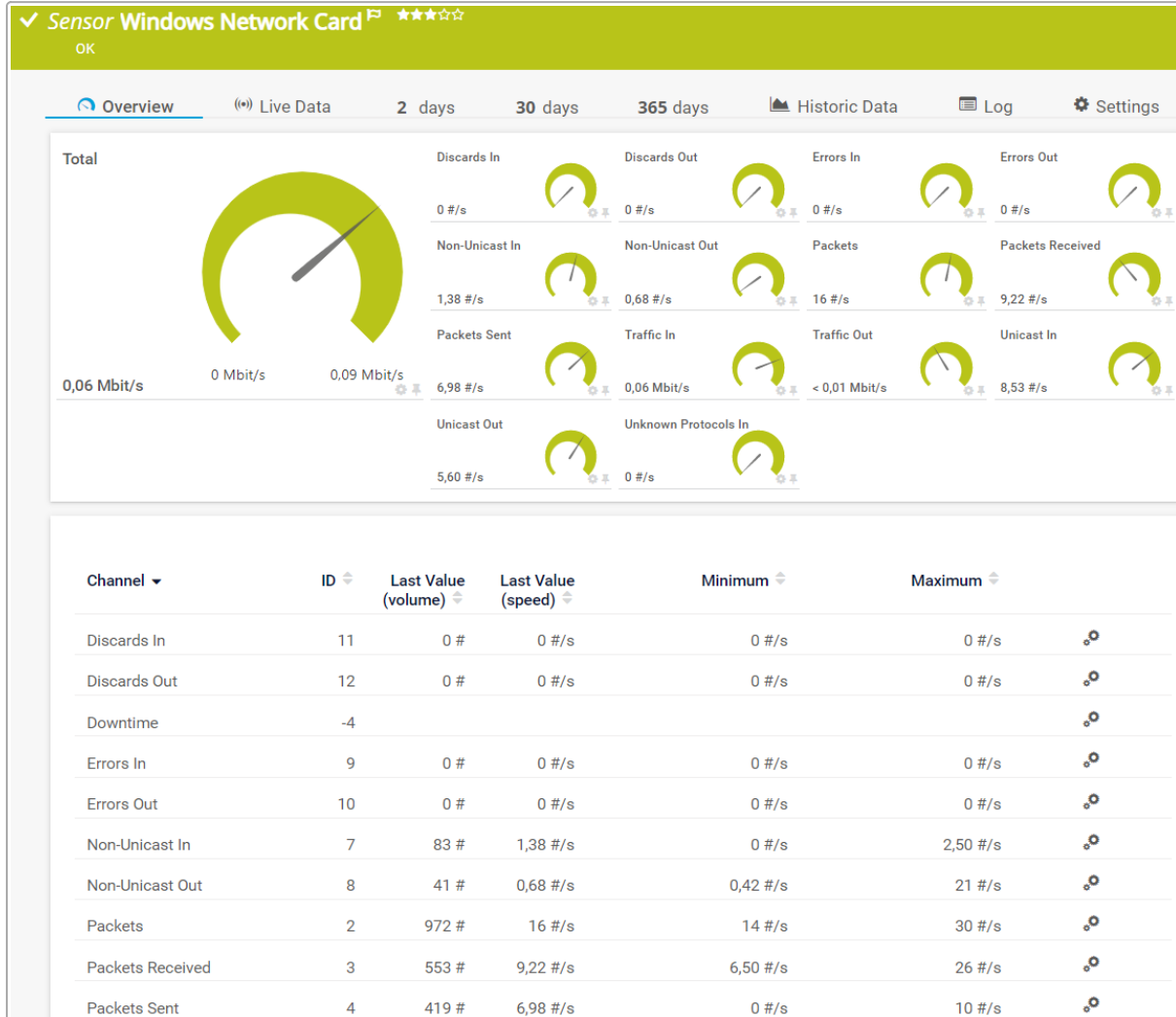
- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.273 Windows Network Card Sensor

The Windows Network Card sensor monitors the bandwidth usage and traffic of a network interface via Windows Management Instrumentation (WMI) or Windows performance counters, as configured in the [Windows Compatibility Options](#) of the parent device.



Windows Network Card Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2424]</sup>.

### Sensor in Other Languages

- Dutch: Windows Netwerkkkaart
- French: Windows carte réseau
- German: Windows Netzwerkadapter
- Japanese: Windows ネットワークカード
- Portuguese: Adaptador de rede Windows
- Russian: Сетевой адаптер Windows

- Simplified Chinese: Windows 网卡
- Spanish: Tarjeta de red Windows

## Remarks

Consider the following [remarks](#) <sup>[2421]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Windows version	<p>This sensor requires <a href="#">at least Windows Server 2008 R2</a> on the probe system to work with Windows performance counters.</p> <p><b>i</b> WoW64 must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the PRTG probe service only runs with 32-bit support. Without it, WMI sensors do not work.</p> <p><b>i</b> This sensor requires at least Windows Server 2008 R2 or Windows 7 to monitor 64-bit counters of the class <a href="#">Network Adapter</a> (virtual network interfaces). On older target systems, the sensor can only monitor 32-bit counters of the class <a href="#">Network Interface</a> (the physical interface) and shows fewer channels.</p>
Remote Registry Windows service	<p>This sensor requires that the <a href="#">Remote Registry</a> Windows service runs on the target system.</p> <p><b>i</b> If this service does not run, a connection via performance counters is not possible. However, WMI connections might still work.</p> <p><b>i</b> To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.</p>
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	<p>This sensor requires credentials for Windows systems.</p> <p><b>i</b> We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system.</p> <p>Otherwise, a connection via performance counters is not possible. However, WMI connections might still work.</p>
Teamed network adapters	This sensor supports teamed network adapters ("network interface card (NIC) teaming") on Windows Server 2016.

Remark	Description
IPv6	This sensor supports IPv6.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Hybrid Approach: Performance Counters and WMI

**i** By default, this sensor uses WMI to request monitoring data. You can change the default behavior to a [hybrid approach](#) in the Windows Compatibility Options of the parent [device's settings](#) on which you create this sensor: if you choose this option, the sensor first tries to query data via [Windows performance counters](#) and uses WMI as a fallback if performance counters are not available. When running in fallback mode, the sensor tries to connect via performance counters again after 24 hours.

**i** Sensors that use the WMI protocol have a high impact on the system performance. Try to stay below 200 WMI sensors per [probe](#). Above this number, consider using multiple [remote probes](#) for load balancing.

**i** For a general introduction to the technology behind WMI, see section [Monitoring via WMI](#).

## Basic Sensor Settings

**Basic Sensor Settings**

Sensor Name ⓘ Example Name

---

Tags ⓘ  X +

---

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- bandwidthsensor
- wmibandwidthsensor

**■** For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Specific

**Sensor Specific** Network Card ⓘ Gigabit-Netzwerkverbindung Intel[R] 82574L

Sensor Specific

Setting	Description
Network Card	The name of the network card that this sensor monitors.

## Debug Options

**Debug Options** Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options


Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display


**Sensor Display** Primary Channel ⓘ Downtime

**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> <li>▪ Show in and out traffic as positive and negative area graph: Show channels for incoming and outgoing traffic as positive and negative area graph. This visualizes your traffic in a clear way. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the channel settings). Manual scaling is not possible if you choose this option.</li> <li><b>i</b> You cannot show a positive/negative graph for a channel if you choose to display its data in percent of maximum (available in the channel settings).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Discards In	The number of incoming discards
Discards Out	The number of outgoing discards
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Errors In	The number of incoming errors
Errors Out	The number of outgoing errors
Non-Unicast In	The number of incoming non-unicast packets
Non-Unicast Out	The number of outgoing non-unicast packets
Packets	The total number of packets
Packets Received	The number of packets received
Packets Sent	The number of packets sent
Total	The total traffic <b>i</b> This channel is the primary channel by default.
Traffic In	The incoming traffic
Traffic Out	The outgoing traffic
Unicast In	The number of incoming unicast packets
Unicast Out	The number of outgoing unicast packets
Unknown Protocols In	The number of unknown protocols

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

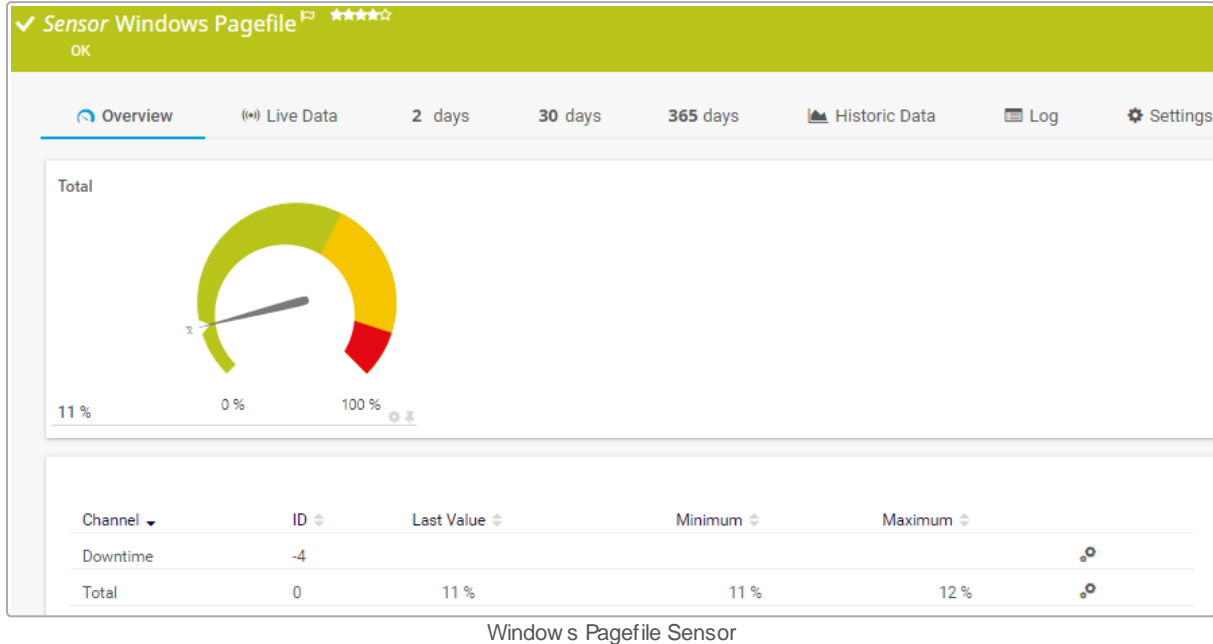
My Windows sensors do not work when using direct performance counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>



## 7.8.274 Windows Pagefile Sensor

The Windows Pagefile sensor monitors the Windows pagefile usage via Windows Management Instrumentation (WMI) or Windows performance counters, as configured in the [Windows Compatibility Options](#) of the parent device.









For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Windows Wisselbestand
- French: Windows fichier d'échange
- German: Windows Auslagerungsdatei
- Japanese: Windows ページファイル
- Portuguese: Arquivo de Paginação (Pagefile) Windows
- Russian: Файл подкачки Windows
- Simplified Chinese: Windows 页面文件
- Spanish: Archivo de página Windows

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Windows version	<p>This sensor requires <a href="#">at least Windows Server 2008 R2</a> on the probe system (on every cluster node, if on a cluster probe).</p> <ul style="list-style-type: none"> <li> <b>WoW64</b> must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the PRTG probe service only runs with 32-bit support. Without it, WMI sensors do not work.</li> <li> This sensor does not work with Windows 2000 because the respective WMI class does not exist on this operating system.</li> </ul>
Remote Registry Windows service	<p>This sensor requires that the <a href="#">Remote Registry</a> Windows service runs on the target system.</p> <ul style="list-style-type: none"> <li> If this service does not run, a connection via performance counters is not possible. However, WMI connections might still work.</li> <li> To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.</li> </ul>
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	<p>This sensor requires credentials for Windows systems.</p> <ul style="list-style-type: none"> <li> We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system.</li> </ul> <p>Otherwise, a connection via performance counters is not possible. However, WMI connections might still work.</p>
IPv6	This sensor supports IPv6.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Hybrid Approach: Performance Counters and WMI

**i** By default, this sensor uses WMI to request monitoring data. You can change the default behavior to a [hybrid approach](#) in the Windows Compatibility Options of the parent [device's settings](#) on which you create this sensor: if you choose this option, the sensor first tries to query data via [Windows performance counters](#) and uses WMI as a fallback if performance counters are not available. When running in fallback mode, the sensor tries to connect via performance counters again after 24 hours.

**i** Sensors that use the WMI protocol have a high impact on the system performance. Try to stay below 200 WMI sensors per [probe](#). Above this number, consider using multiple [remote probes](#) for load balancing.

**i** For a general introduction to the technology behind WMI, see section [Monitoring via WMI](#).

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- pagefilesensor
- wmi pagefilesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Debug Options

### Debug Options

**Result Handling** ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ <b>Store result:</b> Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---


Graph Type **i**  Show channels independently (default)

Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ <b>Show channels independently (default):</b> Show a graph for each channel.</li> <li>▪ <b>Stack channels on top of each other:</b> Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>



## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Total	<p>The total pagefile usage (%)</p> <p> This channel is the primary channel by default.</p> <p> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Upper error limit: 90%</li> <li>▪ Upper warning limit: 60%</li> </ul>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

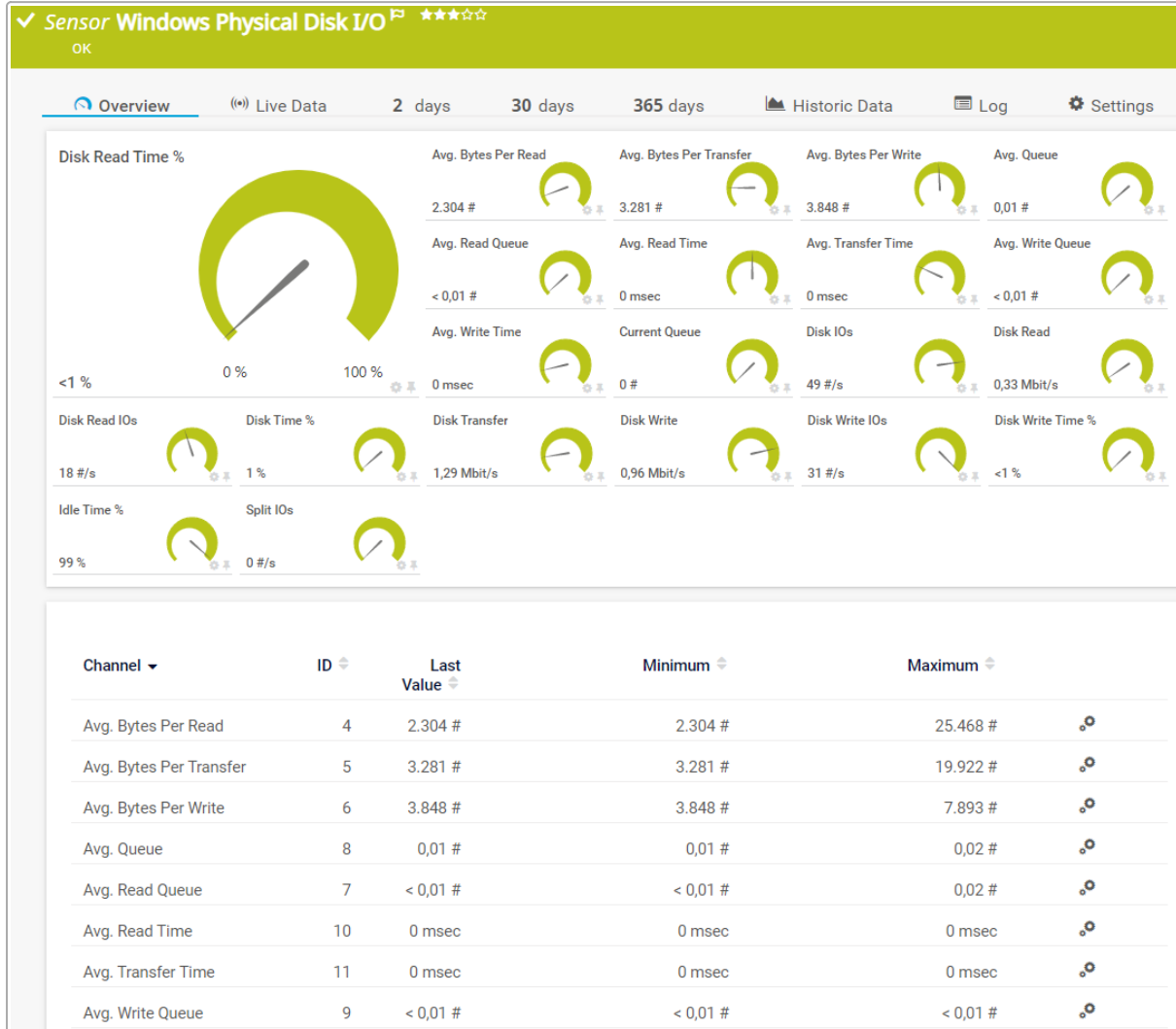
- <https://kb.paessler.com/en/topic/61108>

My Windows sensors do not work when using direct performance counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>

## 7.8.275 Windows Physical Disk I/O Sensor

The Windows Physical Disk I/O sensor monitors the input/output (I/O) parameters of a hard disk on a Windows system via Windows Management Instrumentation (WMI) or Windows performance counters, as configured in the [Windows Compatibility Options](#) of the parent device.



Windows Physical Disk I/O Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).






### Sensor in Other Languages

- Dutch: Windows Fysieke Schijf I/O
- French: Windows disque physique E/S
- German: Windows Physikalischer Datenträger E/A
- Japanese: Windows 物理ディスク I/O
- Portuguese: E/S de disco físico Windows
- Russian: Ввод-вывод физического диска Windows

- Simplified Chinese: Windows 物理磁盘 I/O
- Spanish: E/S de disco físico Windows

## Remarks

Consider the following [remarks](#)<sup>[2433]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <b>high</b> performance impact. We recommend that you use no more than <b>200</b> of this sensor on each probe.
Windows version	This sensor requires <b>at least Windows Server 2008 R2</b> on the probe system (on every cluster node, if on a cluster probe).   WoW64 must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the PRTG probe service only runs with 32-bit support. Without it, WMI sensors do not work.
Remote Registry Windows service	This sensor requires that the <b>Remote Registry</b> Windows service runs on the target system.   If this service does not run, a connection via performance counters is not possible. However, WMI connections might still work.   To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.   We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system.  Otherwise, a connection via performance counters is not possible. However, WMI connections might still work.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Hybrid Approach: Performance Counters and WMI

- i** By default, this sensor uses WMI to request monitoring data. You can change the default behavior to a [hybrid approach](#) in the Windows Compatibility Options of the parent [device's settings](#) on which you create this sensor: if you choose this option, the sensor first tries to query data via [Windows performance counters](#) and uses WMI as a fallback if performance counters are not available. When running in fallback mode, the sensor tries to connect via performance counters again after 24 hours.
- i** Sensors that use the WMI protocol have a high impact on the system performance. Try to stay below 200 WMI sensors per [probe](#). Above this number, consider using multiple [remote probes](#) for load balancing.
- i** For a general introduction to the technology behind WMI, see section [Monitoring via WMI](#).

## Basic Sensor Settings

**Basic Sensor Settings**

Sensor Name ⓘ Example Name

---

Tags ⓘ  x +

---

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiphysicaldisksensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Windows Physical Disk Specific

**Windows Physical Disk Specific**

Disk ⓘ *\_Total*

Windows Physical Disk Specific

Setting	Description
Disk	The physical disk that this sensor monitors.



## Debug Options

**Debug Options**

**Result Handling** ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p> ⓘ PRTG only stores the result of this sensor if you select WMI only (default) as Preferred Data Source in the <a href="#">Windows Compatibility Options</a> of the parent device.</p> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

**Primary Channel** ⓘ Downtime


---

**Graph Type** ⓘ


Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Avg. Bytes Per Read	The average number of bytes per read
Avg. Bytes Per Transfer	The average number of bytes per transfer
Avg. Bytes Per Write	The average number of bytes per write
Avg. Queue	The average number of items in the queue
Avg. Read Queue	The average number of items in the read queue
Avg. Read Time	The average read time

Channel	Description
Avg. Transfer Time	The average transfer time
Avg. Write Queue	The average number of items in the write queue
Avg. Write Time	The average write time
Current Queue	The current number of items in the queue
Disk IOs	The number of disk I/O operations
Disk Read	The disk read speed
Disk Read IOs	The number of disk read I/O operations
Disk Read Time %	The disk read time (%) <b>i</b> This channel is the primary channel by default.
Disk Time %	The disk time (%)
Disk Transfer	The disk transfer speed
Disk Write	The disk write speed
Disk Write IOs	The number of disk write I/O operations
Disk Write Time %	The disk write time (%)
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Idle Time %	The idle time (%)
Split IOs	The number of split I/O operations

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

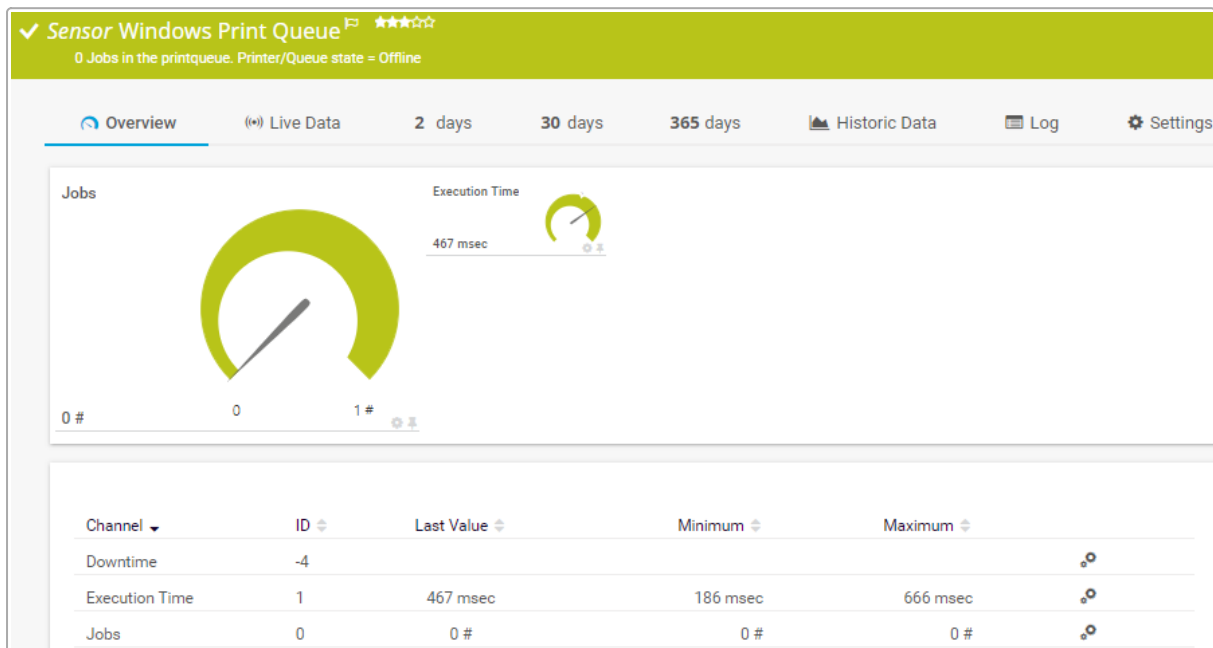
My Windows sensors do not work when using direct performance counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>

## 7.8.276 Windows Print Queue Sensor

The Windows Print Queue sensor reads the print queue on the parent device and returns the number of jobs in the print queue. It can monitor queues for all printers that are locally installed.

- ❶ You can use this sensor to monitor all print queues on your Windows print server and to retrieve information about all available jobs that are in the queue longer than defined.
- ❷ Additionally, this sensor can change to a defined status if there is a printer problem. See section [Sensor Settings](#) <sup>[2441]</sup> for available parameters.



Windows Print Queue Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) <sup>[2448]</sup>.


### Sensor in Other Languages

- Dutch: Windows Print Queue
- French: Windows file d'attente d'impression
- German: Windows Druckwarteschlange
- Japanese: Windows プリントキュー
- Portuguese: Fila de impressão Windows
- Russian: Очередь печати Windows
- Simplified Chinese: Windows 打印队列
- Spanish: Cola de impresión Windows

### Remarks

Consider the following [remarks](#) <sup>[2439]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Print Spooler Windows service	This sensor requires that the <a href="#">Print Spooler</a> Windows service runs on the target device and the probe system.   To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.
.NET 4.7.2 or later	This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node. If the sensor shows the error PE087, additionally install .NET 3.5 on the probe system.   If the framework is missing, you cannot create this sensor.   For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a>
Windows Server	We recommend Windows Server 2016 on the probe system for best performance of this sensor.
Credentials	This sensor requires credentials for Windows systems.   We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system.  Otherwise, the sensor cannot correctly connect.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

 You can add a [change trigger](#) to this sensor to get a notification when the number of jobs in the queue changes.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★★★★☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- ptfsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Settings

### Sensor Settings

**Print Queue** ⓘ

**Advanced Status Options** ⓘ  Do not define sensor states for specific return messages (default)  
 Define sensor states for specific return messages

**Minimum Print Job Age (Sec.)** ⓘ

Sensor Settings

Setting	Description
Print Queue	<p>Select the print queues that you want to monitor. PRTG creates one sensor for each print queue that you select.</p> <ul style="list-style-type: none"> <li>ⓘ If no print queues are available, you see a corresponding message.</li> <li>ⓘ If a printer name changes after sensor creation, you need to add the sensor anew.</li> <li>ⓘ You cannot change this value after sensor creation.</li> </ul>
Advanced Status Options	<p>Optionally define specific <a href="#">sensor states</a> for several return messages of the printer that this sensor monitors:</p> <ul style="list-style-type: none"> <li>▪ Do not define sensor states for specific return messages (default): Do not define sensor states for specific return messages.</li> <li>▪ Define sensor states for specific return messages: Define sensor states for various messages that the printer reports.</li> </ul>

Setting	Description
	<p><b>i</b> Not all printer types properly support Advanced Status Options, which might lead to false alerts. If the printer does not support a property, this property is always <b>false</b>. This means that the sensor cannot display the state or detect if the printer supports the property. Even if the printer can report a property, it can only do so if a print job is sent to the printer.</p>
<p>Door Open</p>	<p><b>This setting is only visible if you select</b> Define sensor states for specific return messages <b>above</b>.</p> <p>For each problem that the printer reports, define the status that the sensor shows:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Stay the same if the printer reports this message.</li> <li>▪ Warning: Show the Warning status if the printer reports this message.</li> <li>▪ Down: Show the Down status if the printer reports this message.</li> </ul>
<p>Manual Feed Required</p>	<p><b>This setting is only visible if you select</b> Define sensor states for specific return messages <b>above</b>.</p> <p>For each problem that the printer reports, define the status that the sensor shows:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Stay the same if the printer reports this message.</li> <li>▪ Warning: Show the Warning status if the printer reports this message.</li> <li>▪ Down: Show the Down status if the printer reports this message.</li> </ul>
<p>Needs User Intervention</p>	<p><b>This setting is only visible if you select</b> Define sensor states for specific return messages <b>above</b>.</p> <p>For each problem that the printer reports, define the status that the sensor shows:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Stay the same if the printer reports this message.</li> <li>▪ Warning: Show the Warning status if the printer reports this message.</li> <li>▪ Down: Show the Down status if the printer reports this message.</li> </ul>
<p>Offline</p>	<p><b>This setting is only visible if you select</b> Define sensor states for specific return messages <b>above</b>.</p> <p>For each problem that the printer reports, define the status that the sensor shows:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Stay the same if the printer reports this message.</li> <li>▪ Warning: Show the Warning status if the printer reports this message.</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ Down: Show the Down status if the printer reports this message.</li> </ul>
Out of Memory	<p><a href="#">This setting is only visible if you select</a> Define sensor states for specific return messages <a href="#">above</a>.</p> <p>For each problem that the printer reports, define the status that the sensor shows:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Stay the same if the printer reports this message.</li> <li>▪ Warning: Show the Warning status if the printer reports this message.</li> <li>▪ Down: Show the Down status if the printer reports this message.</li> </ul>
Out of Paper	<p><a href="#">This setting is only visible if you select</a> Define sensor states for specific return messages <a href="#">above</a>.</p> <p>For each problem that the printer reports, define the status that the sensor shows:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Stay the same if the printer reports this message.</li> <li>▪ Warning: Show the Warning status if the printer reports this message.</li> <li>▪ Down: Show the Down status if the printer reports this message.</li> </ul>
Paper Jammed	<p><a href="#">This setting is only visible if you select</a> Define sensor states for specific return messages <a href="#">above</a>.</p> <p>For each problem that the printer reports, define the status that the sensor shows:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Stay the same if the printer reports this message.</li> <li>▪ Warning: Show the Warning status if the printer reports this message.</li> <li>▪ Down: Show the Down status if the printer reports this message.</li> </ul>
Paper Problem	<p><a href="#">This setting is only visible if you select</a> Define sensor states for specific return messages <a href="#">above</a>.</p> <p>For each problem that the printer reports, define the status that the sensor shows:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Stay the same if the printer reports this message.</li> <li>▪ Warning: Show the Warning status if the printer reports this message.</li> <li>▪ Down: Show the Down status if the printer reports this message.</li> </ul>

Setting	Description
Paused	<p><a href="#">This setting is only visible if you select</a> Define sensor states for specific return messages <a href="#">above</a>.</p> <p>For each problem that the printer reports, define the status that the sensor shows:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Stay the same if the printer reports this message.</li> <li>▪ Warning: Show the Warning status if the printer reports this message.</li> <li>▪ Down: Show the Down status if the printer reports this message.</li> </ul>
Printer Error	<p><a href="#">This setting is only visible if you select</a> Define sensor states for specific return messages <a href="#">above</a>.</p> <p>For each problem that the printer reports, define the status that the sensor shows:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Stay the same if the printer reports this message.</li> <li>▪ Warning: Show the Warning status if the printer reports this message.</li> <li>▪ Down: Show the Down status if the printer reports this message.</li> </ul>
Printer Not Available	<p><a href="#">This setting is only visible if you select</a> Define sensor states for specific return messages <a href="#">above</a>.</p> <p>For each problem that the printer reports, define the status that the sensor shows:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Stay the same if the printer reports this message.</li> <li>▪ Warning: Show the Warning status if the printer reports this message.</li> <li>▪ Down: Show the Down status if the printer reports this message.</li> </ul>
Toner Low	<p><a href="#">This setting is only visible if you select</a> Define sensor states for specific return messages <a href="#">above</a>.</p> <p>For each problem that the printer reports, define the status that the sensor shows:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Stay the same if the printer reports this message.</li> <li>▪ Warning: Show the Warning status if the printer reports this message.</li> <li>▪ Down: Show the Down status if the printer reports this message.</li> </ul>
Toner Out	<p><a href="#">This setting is only visible if you select</a> Define sensor states for specific return messages <a href="#">above</a>.</p>

Setting	Description
	<p>For each problem that the printer reports, define the status that the sensor shows:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Stay the same if the printer reports this message.</li> <li>▪ Warning: Show the Warning status if the printer reports this message.</li> <li>▪ Down: Show the Down status if the printer reports this message.</li> </ul>
Minimum Print Job Age (Sec.)	Optionally define the age of the print job in seconds. If you define a minimum print job age, the sensor does not regard jobs that are younger than this value. If you leave this field empty, the sensor does not check for the print job age. Enter an integer or leave the field empty.

### Debug Options

**Debug Options**

**Result Handling** ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### Sensor Display


**Sensor Display**

**Primary Channel** ⓘ Downtime


---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Execution Time	The execution time
Jobs	The number of jobs in the queue  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

Which .NET version does PRTG require?

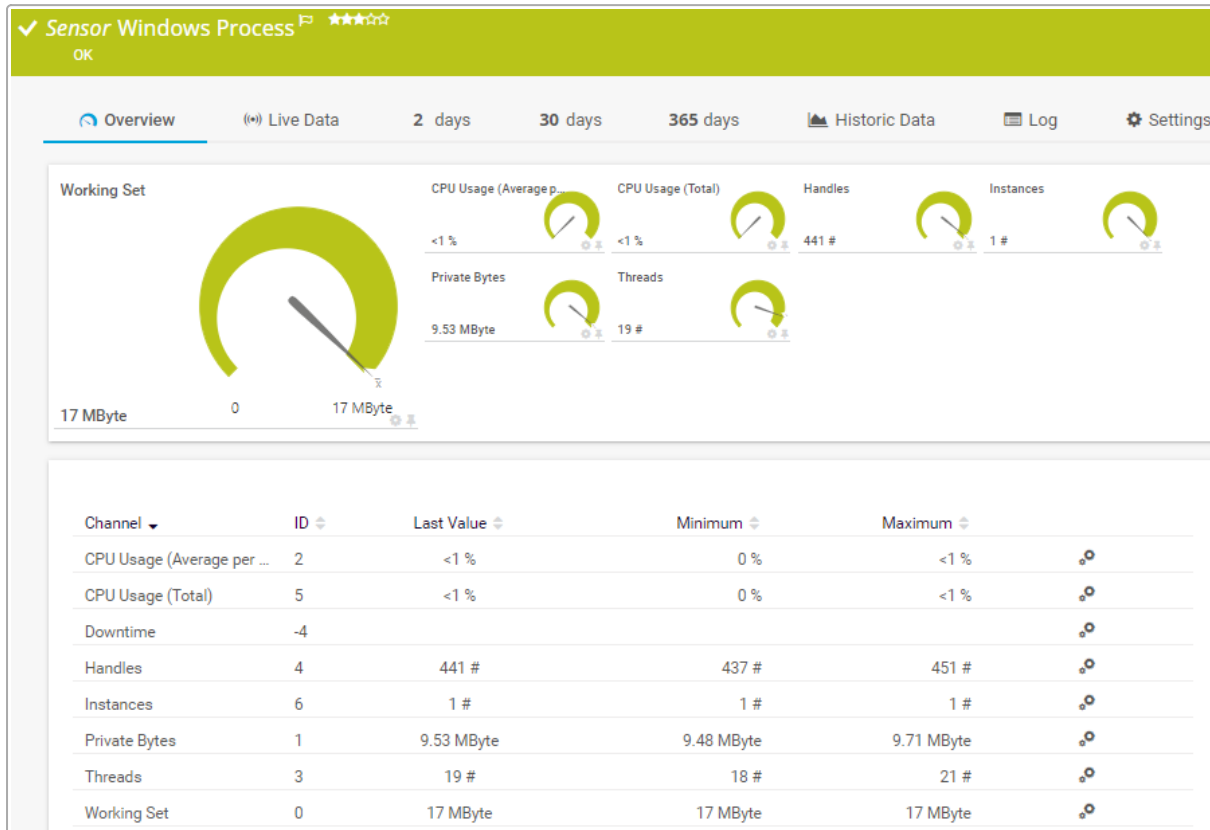
- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.8.277 Windows Process Sensor

The Windows Process sensor monitors a Windows process via Windows Management Instrumentation (WMI) or Windows performance counters, as configured in the [Windows Compatibility Options](#) of the parent device.



Windows Process Sensor






For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: Windows Proces
- French: Windows processus
- German: Windows Prozess
- Japanese: Windows プロセス
- Portuguese: Processo Windows
- Russian: Процесс Windows
- Simplified Chinese: Windows 进程
- Spanish: Proceso Windows

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Windows version	This sensor requires <a href="#">at least Windows Server 2008 R2</a> on the probe system (on every cluster node, if on a cluster probe).   <b>WoW64</b> must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the PRTG probe service only runs with 32-bit support. Without it, WMI sensors do not work.
Remote Registry Windows service	This sensor requires that the <a href="#">Remote Registry</a> Windows service runs on the target system.   If this service does not run, a connection via performance counters is not possible. However, WMI connections might still work.   To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.   We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system.  Otherwise, a connection via performance counters is not possible. However, WMI connections might still work.
Performance counters	The sensor cannot show values above 4 GB for 64-bit processes if you use performance counters.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Hybrid Approach: Performance Counters and WMI

**i** By default, this sensor uses WMI to request monitoring data. You can change the default behavior to a [hybrid approach](#) in the Windows Compatibility Options of the parent [device's settings](#) on which you create this sensor: if you choose this option, the sensor first tries to query data via [Windows performance counters](#) and uses WMI as a fallback if performance counters are not available. When running in fallback mode, the sensor tries to connect via performance counters again after 24 hours.

**i** Sensors that use the WMI protocol have a high impact on the system performance. Try to stay below 200 WMI sensors per [probe](#). Above this number, consider using multiple [remote probes](#) for load balancing.

**i** For a general introduction to the technology behind WMI, see section [Monitoring via WMI](#).

## Basic Sensor Settings

The screenshot shows the 'Basic Sensor Settings' configuration window. It includes the following elements:

- Sensor Name:** A text input field containing 'Example Name'.
- Tags:** A list of tags with 'exampletag' currently selected. There are 'x' and '+' icons for removing and adding tags.
- Priority:** A star rating system showing 5 stars.

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiprocesssensor

**■** For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Windows Process Monitor

The screenshot shows the 'Windows Process Monitor' configuration window. It includes the following element:

- Executable:** A text input field containing 'firefox'.

Windows Process Monitor

Setting	Description
Executable	<p>Enter the name of the process that you want to monitor. Provide the name of an executable file without the <code>.exe</code> extension (for example, enter <a href="#">firefox</a> to monitor <code>firefox.exe</code>).</p> <p><b>i</b> The sensor shows the Down <a href="#">status</a> if the process is not active on the target device.</p>



## Debug Options

**Debug Options**

**Result Handling** ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

**Primary Channel** ⓘ Downtime


---

**Graph Type** ⓘ


Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>



## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CPU Usage (Average per Instance)	<p>The average CPU usage (%) (if multiple instances are running)</p> <p> For this value, the summed up CPU usage value is divided by the number of all instances. It shows the average CPU usage of a single instance of the process on one CPU.</p>
CPU Usage (Total)	<p>The total CPU usage (%)</p> <p> For this value of a process, all CPU usage values are summed up. The total is divided by the number of all CPUs and the maximum value is <b>100%</b>. This corresponds to the CPU usage of all instances of this specific process.</p>

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Handles	The number of handles
Instances	The number of instances
Private Bytes	The private bytes
Threads	The number of threads
Working Set	The working set  This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My Windows sensors do not work when using direct performance counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>

## 7.8.278 Windows SMTP Service Received Sensor

The Windows SMTP Service Received sensor monitors the number of received emails of a Windows Simple Mail Transfer Protocol (SMTP) service via Windows Management Instrumentation (WMI) or Windows performance counters, as configured in the [Windows Compatibility Options](#) of the parent device.

■ For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2457]</sup>.



### Sensor in Other Languages

- Dutch: Windows SMTP Service Ontvangen
- French: Service Windows SMTP reçu
- German: Windows SMTP-Dienst Empfangen
- Japanese: Windows SMTP サービスが受信
- Portuguese: Serviço Windows SMTP recebido
- Russian: Получено пакетов службы Windows SMTP
- Simplified Chinese: 已接收 Windows SMTP 服务
- Spanish: Servicio SMTP de Windows recibidos


### Remarks


Consider the following [remarks](#)<sup>[2454]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Windows version	This sensor requires <a href="#">at least Windows Server 2008 R2</a> on the probe system (on every cluster node, if on a cluster probe).  <span style="color: red;">❗</span> WoW64 must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the PRTG probe service only runs with 32-bit support. Without it, WMI sensors do not work.
Remote Registry Windows service	This sensor requires that the <a href="#">Remote Registry</a> Windows service runs on the target system.  <span style="color: red;">❗</span> If this service does not run, a connection via performance counters is not possible. However, WMI connections might still work.  <span style="color: red;">❗</span> To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Remark	Description
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.   We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system. Otherwise, a connection via performance counters is not possible. However, WMI connections might still work.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Hybrid Approach: Performance Counters and WMI

 By default, this sensor uses WMI to request monitoring data. You can change the default behavior to a [hybrid approach](#) in the Windows Compatibility Options of the parent [device's settings](#) on which you create this sensor: if you choose this option, the sensor first tries to query data via [Windows performance counters](#) and uses WMI as a fallback if performance counters are not available. When running in fallback mode, the sensor tries to connect via performance counters again after 24 hours.

 Sensors that use the WMI protocol have a high impact on the system performance. Try to stay below 200 WMI sensors per [probe](#). Above this number, consider using multiple [remote probes](#) for load balancing.

 For a general introduction to the technology behind WMI, see section [Monitoring via WMI](#).

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiissmtpreceivedsensor

For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Debug Options

**Debug Options**

Result Handling ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ

Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	Define how this sensor shows different channels:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li>❗ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

❗ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Message Bytes Received	The number of bytes in received messages
Messages Received	<p>The number of received messages</p> <p>❗ This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My Windows sensors do not work when using direct performance counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>



## 7.8.279 Windows SMTP Service Sent Sensor

The Windows SMTP Service Sent sensor monitors the number of sent emails on a Windows Simple Mail Transfer Protocol (SMTP) service via Windows Management Instrumentation (WMI) or Windows performance counters, as configured in the [Windows Compatibility Options](#) of the parent device.

■ For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2462]</sup>.



### Sensor in Other Languages

- Dutch: Windows SMTP Service Verzonden
- French: Service Windows SMTP envoyé
- German: Windows SMTP-Dienst Versendet
- Japanese: Windows SMTP サービスが送信
- Portuguese: Serviço Windows SMTP enviado
- Russian: Отправлено пакетов службы Windows SMTP
- Simplified Chinese: 已发送 Windows SMTP 服务
- Spanish: Servicio SMTP de Windows enviados


### Remarks


Consider the following [remarks](#)<sup>[2459]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
Windows version	This sensor requires <a href="#">at least Windows Server 2008 R2</a> on the probe system (on every cluster node, if on a cluster probe).  <span style="color: red;">❗</span> WoW64 must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the PRTG probe service only runs with 32-bit support. Without it, WMI sensors do not work.
Remote Registry Windows service	This sensor requires that the <a href="#">Remote Registry</a> Windows service runs on the target system.  <span style="color: red;">❗</span> If this service does not run, a connection via performance counters is not possible. However, WMI connections might still work.  <span style="color: red;">❗</span> To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.

Remark	Description
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.   We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system. Otherwise, a connection via performance counters is not possible. However, WMI connections might still work.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Hybrid Approach: Performance Counters and WMI

 By default, this sensor uses WMI to request monitoring data. You can change the default behavior to a [hybrid approach](#) in the Windows Compatibility Options of the parent [device's settings](#) on which you create this sensor: if you choose this option, the sensor first tries to query data via [Windows performance counters](#) and uses WMI as a fallback if performance counters are not available. When running in fallback mode, the sensor tries to connect via performance counters again after 24 hours.

 Sensors that use the WMI protocol have a high impact on the system performance. Try to stay below 200 WMI sensors per [probe](#). Above this number, consider using multiple [remote probes](#) for load balancing.

 For a general introduction to the technology behind WMI, see section [Monitoring via WMI](#).

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiissmtpsentsensor

For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Debug Options

### Debug Options

**Result Handling** ⓘ
  Discard result (default)
   
 Store result

Debug Options

Setting	Description
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>


## Sensor Display

### Sensor Display


**Primary Channel** ⓘ Downtime
   
**Graph Type** ⓘ
  Show channels independently (default)
   
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor. <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	Define how this sensor shows different channels:

Setting	Description
	<ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Message Bytes Sent	The number of bytes in sent messages
Message Send Retries	The number of retries per second for sent messages
Messages Sent	<p>The number of sent messages</p> <p> This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

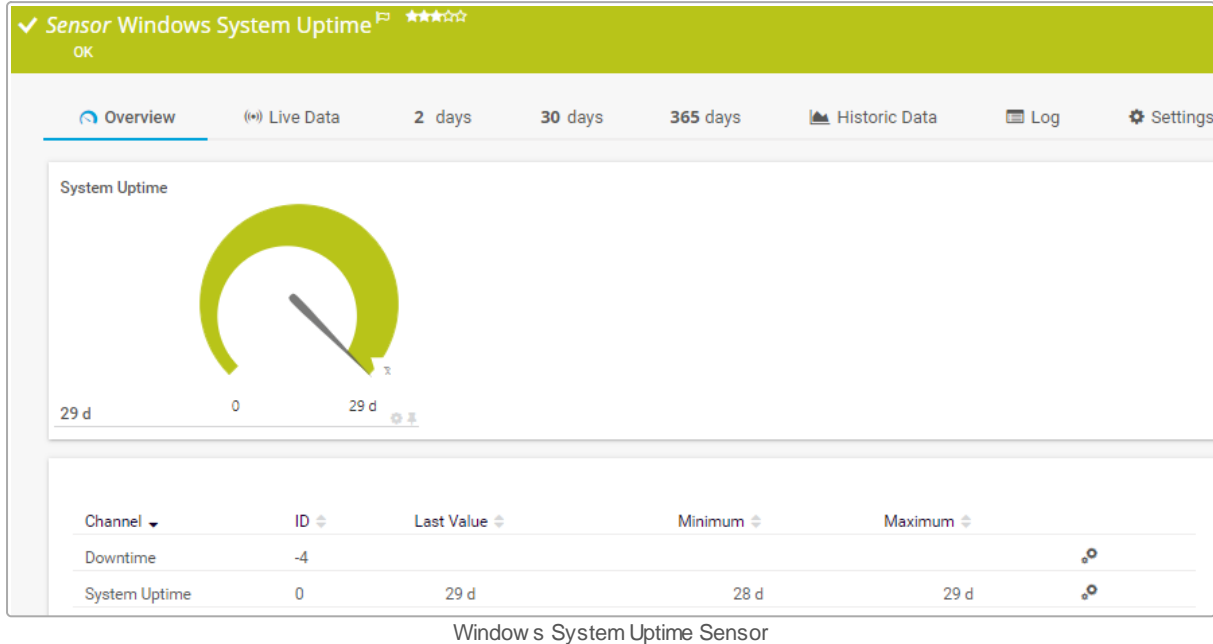
- <https://kb.paessler.com/en/topic/61108>

My Windows sensors do not work when using direct performance counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>

## 7.8.280 Windows System Uptime Sensor

The Windows System Uptime sensor monitors the uptime of a Windows system via Windows Management Instrumentation (WMI) or Windows performance counters, as configured in the [Windows Compatibility Options](#) of the parent device.



For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2467]</sup>.

### Sensor in Other Languages

- Dutch: Windows System Uptime
- French: Windows disponibilité du système
- German: Windows-Systemlaufzeit
- Japanese: Windows システムアップタイム
- Portuguese: Tempo de atividade do sistema Windows
- Russian: Время бесперебойной работы системы Windows
- Simplified Chinese: Windows 系统正常运行时间
- Spanish: Tiempo activo del sistema Windows

### Remarks

Consider the following [remarks](#)<sup>[2464]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact.

Remark	Description
Windows version	<p>This sensor requires <a href="#">at least Windows Server 2008 R2</a> on the probe system (on every cluster node, if on a cluster probe).</p> <p><b>i</b> WoW64 must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the PRTG probe service only runs with 32-bit support. Without it, WMI sensors do not work.</p>
Remote Registry Windows service	<p>This sensor requires that the <a href="#">Remote Registry</a> Windows service runs on the target system.</p> <p><b>i</b> If this service does not run, a connection via performance counters is not possible. However, WMI connections might still work.</p> <p><b>i</b> To enable the service, log in to the respective system and open the services manager (for example, via services.msc). In the list, find the respective service and set its Start Type to Automatic.</p>
WoW64	<p>This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.</p>
Credentials	<p>This sensor requires credentials for Windows systems.</p> <p><b>i</b> We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system.</p> <p>Otherwise, a connection via performance counters is not possible. However, WMI connections might still work.</p>
IPv6	<p>This sensor supports IPv6.</p>
Hosted probe	<p> You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.</p>

## Hybrid Approach: Performance Counters and WMI

**i** By default, this sensor uses WMI to request monitoring data. You can change the default behavior to a [hybrid approach](#) in the Windows Compatibility Options of the parent [device's settings](#) on which you create this sensor: if you choose this option, the sensor first tries to query data via [Windows performance counters](#) and uses WMI as a fallback if performance counters are not available. When running in fallback mode, the sensor tries to connect via performance counters again after 24 hours.

**i** Sensors that use the WMI protocol have a high impact on the system performance. Try to stay below 200 WMI sensors per [probe](#). Above this number, consider using multiple [remote probes](#) for load balancing.

**i** For a general introduction to the technology behind WMI, see section [Monitoring via WMI](#).

### Basic Sensor Settings

Basic Sensor Settings

Sensor Name **i**

Tags **i**
 ✕ +

Priority **i**
★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiuptimesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Debug Options

Debug Options

Result Handling **i**

Discard result (default)
   
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>



## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
System Uptime	The uptime  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My Windows sensors do not work when using direct performance counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>

## 7.8.281 Windows Updates Status (PowerShell) Sensor

The Windows Updates Status (PowerShell) sensor monitors the status of Windows updates on a computer and counts the available and installed Windows updates that are either from Microsoft or from the local Windows Server Update Services (WSUS) server.

- ❶ You can find the updates that the sensor considers in the [Server Manager \(WSUS\)](#) under Roles | Windows Server Update Services | Update Services | Computers | Reports.



Windows Updates Status (PowerShell) Sensor

- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2474]</sup>.

### Sensor in Other Languages


- Dutch: Windows Updates Status (PowerShell)

- French: Windows statut des mises à jour (PowerShell)
- German: Windows Updates Status (PowerShell)
- Japanese: Windows アップデートステータス( PowerShell)
- Portuguese: Status de atualizações do Windows (PowerShell)
- Russian: Статус обновления Windows (PowerShell)
- Simplified Chinese: Windows 更新状态 (PowerShell)
- Spanish: Estado de actualizaciones Windows (PowerShell)

## Remarks

Consider the following [remarks](#)<sup>2470</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
Remote PowerShell	<p>This sensor requires that <a href="#">Remote PowerShell</a> is enabled on the target system and <a href="#">PowerShell 3.0</a> on both the probe system and the target system.</p> <p><b>i</b> Also make sure that you have at least <a href="#">PowerShell 3.0</a> installed on both the probe system and the target system. If you receive an error message regarding issues with the WinRM connection, make sure that remote commands have been enabled in PowerShell. For more information, see the Knowledge Base: <a href="#">How do I enable and use remote commands in Windows PowerShell?</a></p>
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node.</p> <p><b>i</b> If the framework is missing, you cannot create this sensor.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Credentials	This sensor requires credentials for Windows systems.
Scanning interval	<p>This sensor has a fixed minimum scanning interval for performance reasons. You cannot use a shorter scanning interval. Consequently, shorter scanning intervals in the <a href="#">Monitoring</a> settings are not available for this sensor.</p> <ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <b>1 hour</b>.</li> <li>▪ The recommended scanning interval of this sensor is <b>12 hours</b>. We recommend this scanning interval to limit the load on the server that this sensor monitors.</li> </ul>

Remark	Description
IPv6	This sensor supports IPv6.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Initial data	In certain cases, it might take some time until the sensor receives data for the first time.
Time Since Last Update channel	If the sensor cannot determine any values for the Time Since Last Update channel (for example, because the list of updates is empty), it shows the value <b>-1s</b> and changes to the Warning <a href="#">status</a> .
Roaming Profiles	When monitoring a <a href="#">Remote Desktop Server (RDS) system</a> with the option Roaming Profiles enabled, this sensor creates a temporary user profile folder for each scanning interval. To minimize this effect, we recommend that you set the sensor's scanning interval to at least 7 days.
Severity	This sensor displays the severity member <a href="#">Unspecified</a> as <b>None</b> . If the severity member is missing, this sensor displays it as <b>None</b> .
Knowledge Base	Knowledge Base: <a href="#">Where can I find more information about PowerShell sensors?</a>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag × +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- windowsupdatesstatus

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Sensor Specific

**Sensor Specific**

Port ⓘ 5985

---

Port in SPN ⓘ  Exclude port in SPN (default)  
 Include port in SPN

Authentication Method ⓘ  Kerberos authentication (default)  
 Negotiate authentication

Sensor Specific

Setting	Description
Port	Enter the number of the port to which this sensor connects. Enter an integer. The default port is <a href="#">5985</a> .
Port in SPN	<p>Define whether to include the port number in the Service Principal Name (SPN) used for Kerberos authentication, for example, on devices where Microsoft Internet Information Services (IIS) or similar services are installed:</p> <ul style="list-style-type: none"> <li>▪ Exclude port in SPN (default): Do not include the port number in the SPN.</li> <li>▪ Include port in SPN: Include the port number in the SPN.</li> </ul> <p> ⓘ With this option, a client that uses a non-default SPN can authenticate against a remote computer that uses Kerberos authentication.</p>
Authentication Method	<p>Select the authentication method for the connection to the host via PowerShell:</p> <ul style="list-style-type: none"> <li>▪ Kerberos authentication (default): The sensor uses Kerberos authentication.</li> <li>▪ Negotiate authentication: The sensor uses Negotiate authentication. <span style="color: #0070C0;">■</span> For more information about Negotiate authentication, see the Knowledge Base: <a href="#">Facing issues with the Windows Updates Status (PowerShell) sensor - can you help me?</a></li> </ul>

## Debug Options

**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>+</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.





## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Time Since Last Update	<p>The time passed since the last update</p> <ul style="list-style-type: none"> <li> This channel is the primary channel by default.</li> <li> The sensor always creates the channel Time Since Last Update. All other channels are optional and only show up if the sensor can retrieve respective data.</li> <li> This channel has default limits: <ul style="list-style-type: none"> <li>▪ Upper warning limit: <a href="#">2592000</a></li> <li>▪ Lower warning limit: <a href="#">0</a></li> </ul> </li> </ul>
Updates (Severity Critical) Hidden	<p>The number of hidden updates with critical severity</p> <ul style="list-style-type: none"> <li> This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper error limit: <a href="#">0.2</a></li> </ul> </li> </ul>
Updates (Severity Critical) Installed	The number of installed updates with critical severity



Channel	Description
Updates (Severity Critical) Missing	The number of missing updates with critical severity ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper error limit: <a href="#">0.2</a></li> </ul>
Updates (Severity Important) Hidden	The number of hidden updates with important severity ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper warning limit: <a href="#">0.2</a></li> </ul>
Updates (Severity Important) Installed	The number of installed updates with important severity
Updates (Severity Important) Missing	The number of missing updates with important severity ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper error limit: <a href="#">0.2</a></li> </ul>
Updates (Severity Low) Hidden	The number of hidden updates with low severity
Updates (Severity Low) Installed	The number of installed updates with low severity
Updates (Severity Low) Missing	The number of missing updates with low severity ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper warning limit: <a href="#">0.2</a></li> </ul>
Updates (Severity Moderate) Hidden	The number of hidden updates with moderate severity
Updates (Severity Moderate) Installed	The number of installed updates with moderate severity
Updates (Severity Moderate) Missing	The number of missing updates with moderate severity ⓘ This channel has a default limit: <ul style="list-style-type: none"> <li>▪ Upper warning limit: <a href="#">0.2</a></li> </ul>
Updates (Unclassified) Hidden	The number of hidden updates with unclassified severity

Channel	Description
Updates (Unclassified) Installed	The number of installed updates with unclassified severity
Updates (Unclassified) Missing	<p>The number of missing updates with unclassified severity</p> <p><b>i</b> This channel has a default limit:</p> <ul style="list-style-type: none"> <li>Upper warning limit: <a href="#">0.2</a></li> </ul>

## More

### ■ KNOWLEDGE BASE

Where can I find more information about PowerShell sensors?

- <https://kb.paessler.com/en/topic/62451>

Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

I have problems with the PowerShell Exchange sensors, what can I do?

- <https://kb.paessler.com/en/topic/54353>

My PowerShell sensor returns an error message. What can I do?

- <https://kb.paessler.com/en/topic/59473>

I get the error "WinRM cannot process the request" when I try to use a PowerShell sensor

- <https://kb.paessler.com/en/topic/59745>

How can I increase memory for Remote PowerShell?

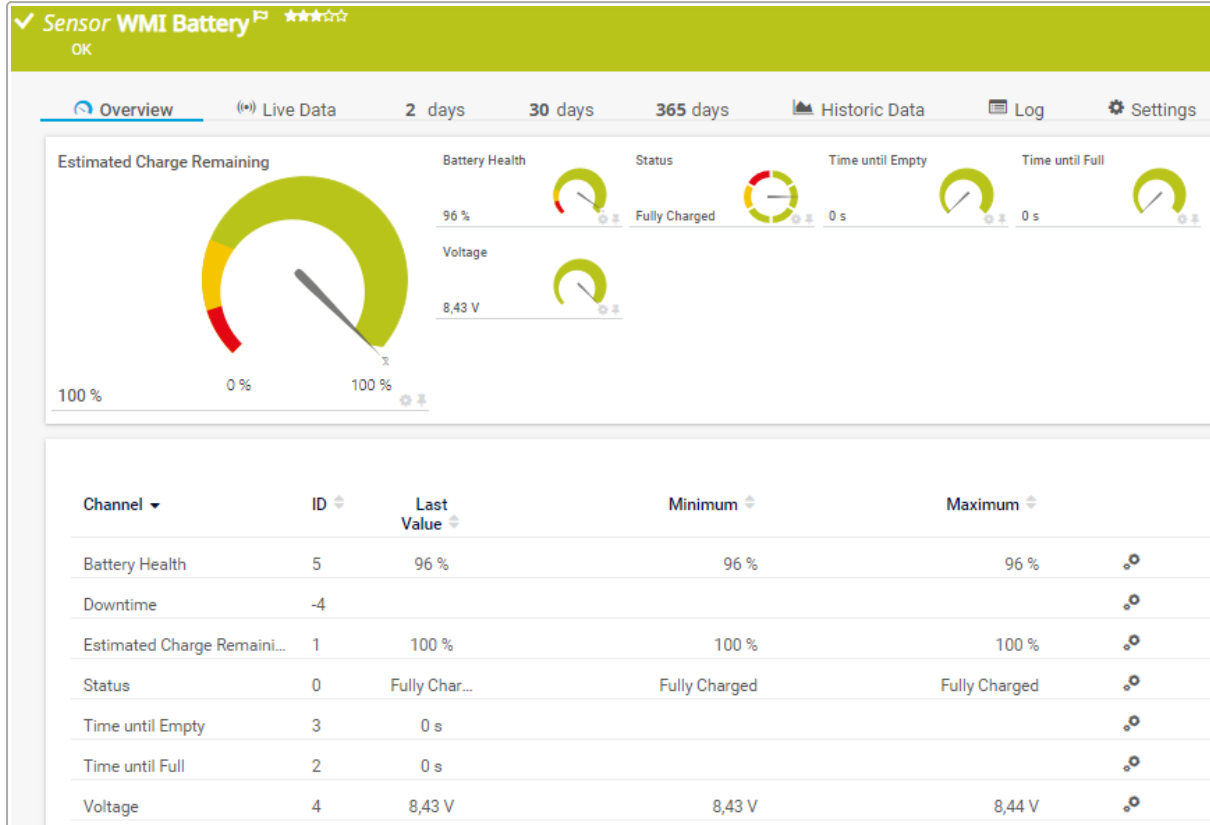
- <https://kb.paessler.com/en/topic/61922>

Facing issues with the Windows Updates Status (PowerShell) sensor - can you help me?

- <https://kb.paessler.com/en/topic/71899>

## 7.8.282 WMI Battery Sensor

The WMI Battery sensor monitors the available capacity and the state of connected batteries or uninterruptible power supplies (UPSs) of a Windows-based device via Windows Management Instrumentation (WMI).



WMI Battery Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: WMI batterij
- French: Batterie (WMI)
- German: WMI Batterie
- Japanese: WMI バッテリー
- Portuguese: Bateria (WMI)
- Russian: Аккумулятор WMI
- Simplified Chinese: WMI 电池
- Spanish: Batería (WMI)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- batterysensor
- wmbatterysensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### WMI Battery Specific

WMI Battery Specific
Name ⓘ *DELL DD9VF0A*

WMI Battery Specific

Setting	Description
Name	The name of the battery or the UPS that this sensor monitors.

### Debug Options

Debug Options
Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>


### Sensor Display

Sensor Display
Primary Channel ⓘ Downtime



---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Battery Health	The battery health (%)

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Estimated Charge Remaining	<p>The estimated remaining charge (%)</p> <ul style="list-style-type: none"> <li><b>i</b> This channel is the primary channel by default.</li> <li><b>i</b> This channel has default limits: <ul style="list-style-type: none"> <li>▪ Lower error limit: 10%</li> <li>▪ Lower warning limit: 25%</li> </ul> </li> </ul>
Status	<p>The battery status</p> <ul style="list-style-type: none"> <li>▪ Up status: Charging, Discharging, Fully Charged, Unknown</li> <li>▪ Warning status: Critical But Charging</li> <li>▪ Down status: Critical But Discharging</li> </ul>
Time Until Empty	The time until the battery is empty
Time Until Full	The time until the battery is fully charged
Voltage	The voltage

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

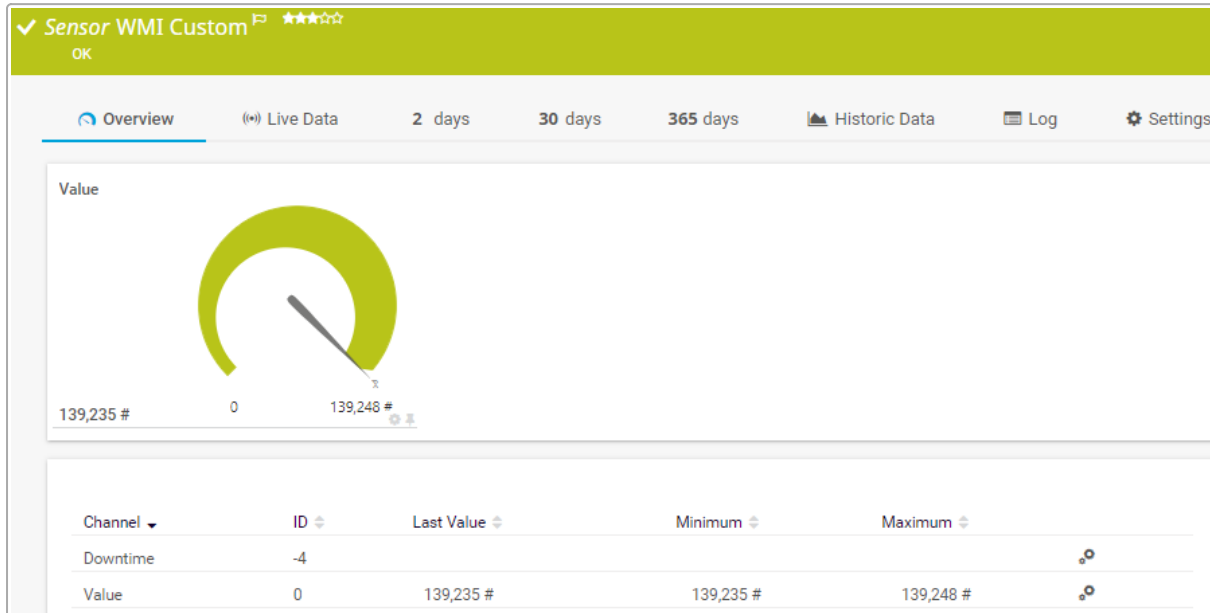
My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.283 WMI Custom Sensor

The WMI Custom sensor performs a custom query via Windows Management Instrumentation (WMI) and monitors numeric values (integers and floats).

**i** If the WQL query returns strings, use the [WMI Custom String](#) <sup>[2488]</sup> sensor.



WMI Custom Sensor

**■** For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) <sup>[2487]</sup>.


### Sensor in Other Languages

- Dutch: WMI (Klant Specifiek)
- French: Requête personnalisée (WMI)
- German: WMI (Benutzerdef.)
- Japanese: WMI カスタム
- Portuguese: WMI (customizado)
- Russian: Нестандартный WMI
- Simplified Chinese: WMI 自定义
- Spanish: WMI (personalizado)


### Remarks

Consider the following [remarks](#) <sup>[2482]</sup> and requirements for this sensor:




Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a></li> <li>Knowledge Base: <a href="#">How do I create a WMI Custom sensor?</a></li> </ul>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.


### Add Sensor


Setting	Description
Channel Name	<p>Enter a name for the channel in which PRTG shows the received data. PRTG shows this name in graphs and tables. Enter a string.</p> <p> You can change this value later in the <a href="#">channel settings</a> of this sensor.</p>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** 

**Tags** 

**Priority** 

Example Name

exampletag ✕ +

★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmicustomsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

### Custom Query Specific

**Custom Query Specific**

Namespace ⓘ

WQL File ⓘ

Placeholder <#PH1> ⓘ

Placeholder <#PH2> ⓘ

Placeholder <#PH3> ⓘ

If Value Changes ⓘ  Ignore (default)  
 Trigger 'change' notification

Unit String ⓘ

Multiplication ⓘ

Division ⓘ

Custom Query Specific

Setting	Description
Namespace	Enter the WMI namespace for the query.
WQL File	<p>Select a .wql file. The sensor executes it with every scanning interval.</p> <p>The list contains WQL scripts that are available in the \Custom Sensors\WMI WQL scripts subfolder of the <a href="#">PRTG program directory</a> on the probe system. Store your script there. If used on a cluster probe, you must store the file on all cluster nodes.</p> <p> ⓘ Your query must return an integer or float value. Strings are not supported. Use the <a href="#">WMI Custom String</a><sup>[2488]</sup> sensor in this case.</p> <p> ⓘ You cannot change this value after sensor creation.</p>
Placeholder <#PH1>	In your WQL script, you can use up to three placeholders to which you can assign a value in this field. Enter a string for variable <#PH1> or leave the field empty.

Setting	Description
Placeholder <#PH2>	In your WQL script, you can use up to three placeholders to which you can assign a value in this field. Enter a string for variable <#PH2> or leave the field empty.
Placeholder <#PH3>	In your WQL script, you can use up to three placeholders to which you can assign a value in this field. Enter a string for variable <#PH3> or leave the field empty.
If Value Changes	<p>Define what the sensor does when its value changes:</p> <ul style="list-style-type: none"> <li>Ignore (default): Do nothing.</li> <li>Trigger 'change' notification: Send an internal message that indicates a change. <ul style="list-style-type: none"> <li><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</li> </ul> </li> </ul>
Unit String	Enter a unit for the data that the sensor receives from your script. This is for display purposes only. The unit is displayed in graphs and tables. Enter a string.
Multiplication	Define a multiplier for the received values. The default value <b>1</b> does not change received values. Enter an integer.
Division	Define a divisor for the received values. The default value <b>1</b> does not change received values. Enter an integer.

## Debug Options

**Debug Options**

Result Handling **i**

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **ⓘ** Downtime

---

Graph Type **ⓘ**
 Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⚙</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click **🔒** under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

❗ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Value]	The retrieved numeric value ❗ This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

How do I create a WMI Custom sensor?

- <https://kb.paessler.com/en/topic/2743>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How do I properly configure a WMI custom sensor?

- <https://kb.paessler.com/en/topic/163>

Which WQL queries are used by the PRTG WMI sensors?

- <https://kb.paessler.com/en/topic/8783>

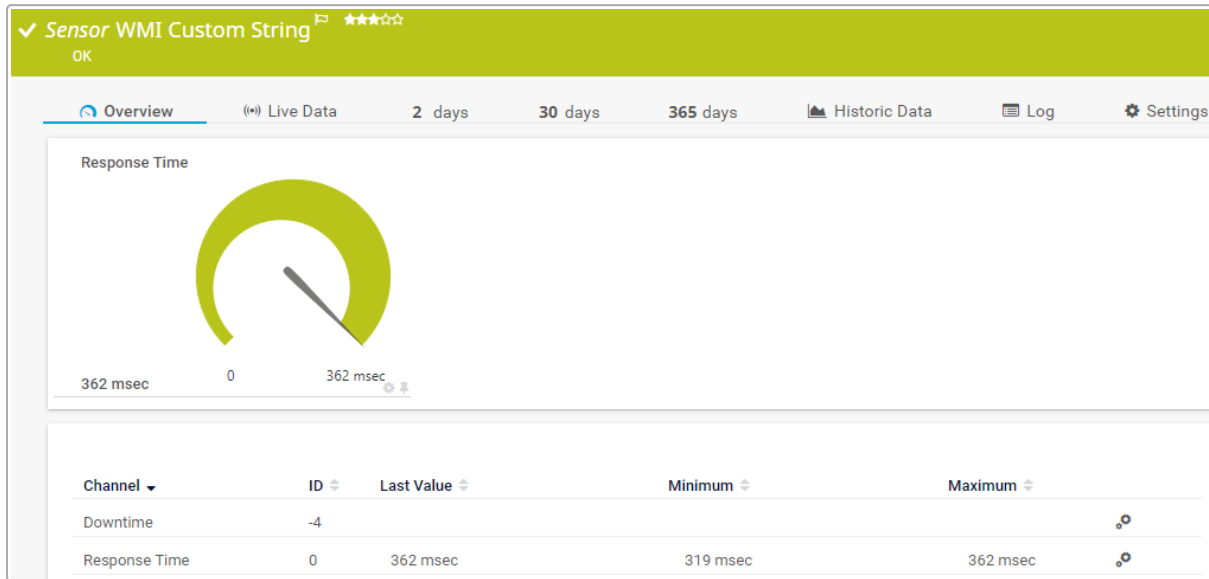
My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.284 WMI Custom String Sensor

The WMI Custom String sensor performs a custom string query via Windows Management Instrumentation (WMI).

- ❶ The sensor can also show the retrieved string value in the sensor message.
- ❶ If the WQL query returns numeric values, use the [WMI Custom](#) <sup>[2482]</sup> sensor.



WMI Custom String Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) <sup>[2493]</sup>.

### Sensor in Other Languages

- Dutch: WMI Aangepaste Tekenreeks
- French: Chaîne personnalisée (WMI)
- German: WMI Text (benutzerdef.)
- Japanese: WMI カスタム文字列
- Portuguese: Sequência de caracteres (customizado) (WMI)
- Russian: Нестандартная строка WMI
- Simplified Chinese: WMI 自定义字符串
- Spanish: Cadena (personalizado) (WMI)

### Remarks

Consider the following [remarks](#) <sup>[2488]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?</a></li> <li>Knowledge Base: <a href="#">How do I create a WMI Custom sensor?</a></li> </ul>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ exampletag ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Example Name

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmicustomsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Custom Query Specific

**Custom Query Specific**

**Namespace** ⓘ root\CIMV2

---

**WQL File** ⓘ Demo WQL Script - Get Win32LogicalDiscFreeMB.wql

**Placeholder <#PH1>** ⓘ

---

**Placeholder <#PH2>** ⓘ

---

**Placeholder <#PH3>** ⓘ

---

**Unit String** ⓘ #

---

**If Value Changes** ⓘ  Ignore (default)  
 Trigger 'change' notification

---

**Response Must Include (Down Status If Not Included)** ⓘ

**Search Method** ⓘ  Simple string search (default)  
 Regular expression

---

**Response Must Not Include (Down Status if Included)** ⓘ

**Search Method** ⓘ  Simple string search (default)  
 Regular expression

---

**Maximum String Length** ⓘ

---

**Numeric Value Extraction** ⓘ  Do not use extraction (default)  
 Use a regular expression for extraction

---









**Result Handling** ⓘ  Discard result (default)  
 Store result

Custom Query Specific

Setting	Description
Namespace	Enter the WMI namespace for the query. .
WQL File	Select a .wql file. The sensor executes it with every scanning interval.



Setting	Description
	<p>The list contains WQL scripts that are available in the \Custom Sensors\WMI WQL scripts subfolder of the <a href="#">PRTG program directory</a> on the probe system. Store your script there. If used on a cluster probe, you must store the file on all cluster nodes.</p> <p><b>i</b> If the WQL query returns integers or floats, use the <a href="#">WMI Custom</a> <small>2482</small> sensor to not only show the returned value in the sensor message, but to also monitor the value in a channel.</p> <p><b>i</b> You cannot change this value after sensor creation.</p>
Placeholder <#PH1>	In your WQL script, you can use up to three placeholders to which you can assign a value in this field. Enter a string for variable <#PH1> or leave the field empty.
Placeholder <#PH2>	In your WQL script, you can use up to three placeholders to which you can assign a value in this field. Enter a string for variable <#PH2> or leave the field empty.
Placeholder <#PH3>	In your WQL script, you can use up to three placeholders to which you can assign a value in this field. Enter a string for variable <#PH3> or leave the field empty.
Unit String	Enter a unit for the data that the sensor receives from your script. This is for display purposes only. The unit is displayed in graphs and tables. Enter a string.
If Value Changes	<p>Define what the sensor does when its value changes:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> <li>▪ Trigger 'change' notification: Send an internal message that indicates a change. <ul style="list-style-type: none"> <li><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</li> </ul> </li> </ul>
Response Must Include (Down Status if Not Included)	<p>Define the search string that must be part of the data that is received from the WMI object. You can enter a simple string in plain text or a <a href="#">regular expression</a>.</p> <p><b>i</b> The search string must be case-sensitive.</p> <p><b>i</b> If the data does <b>not</b> include the search pattern, the sensor shows the Down status.</p>
Response Must Not Include (Down Status if Included)	<p>Define the search string that must <b>not</b> be part of the data that is received from the WMI object. You can enter a simple string in plain text or a regular expression.</p>

Setting	Description
	<ul style="list-style-type: none"> <li> The search string must be case-sensitive.</li> <li> If the data does include the search pattern, the sensor shows the Down status.</li> </ul>
Search Method	<p>Define the method with which you want to provide the search string:</p> <ul style="list-style-type: none"> <li>▪ Simple string search (default): Search for a simple string in plain text.</li> </ul> <p> The characters <code>*</code> and <code>?</code> work as placeholders. <code>*</code> stands for no number or any number of characters and <code>?</code> stands for exactly one character. You cannot change this behavior. The literal search for these characters is only possible with a regex.</p> <ul style="list-style-type: none"> <li>▪ Regular expression: Search with a regular expression (regex).</li> </ul> <p> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</p>
Maximum String Length	<p>Define the maximum allowed length of the string that is received from the WMI object. If it is longer than this value, the sensor shows the Down status. Enter an integer or leave the field empty.</p>
Numeric Value Extraction	<p>Define if you want to filter out a numeric value from the string received from the WMI object:</p> <ul style="list-style-type: none"> <li>▪ Do not use extraction (default): Do not extract a float value. Use the result as a string value.</li> <li>▪ Use a regular expression for extraction: Use a regex to identify a numeric value in the string and convert it to a float value. Define below. <ul style="list-style-type: none"> <li> See also the <a href="#">example</a> <sup>2494</sup>.</li> </ul> </li> </ul> <p> You can convert this into a float value to use it with <a href="#">channel limits</a>.</p>
Regular Expression	<p><b>This setting is only visible if you select</b> Use a regular expression for extraction <a href="#">above</a>.</p> <p>Enter a regex to identify the numeric value you want to extract from the string returned by the WMI object. You can use capturing groups here.</p> <ul style="list-style-type: none"> <li> Make sure that the expression returns numbers only (including decimal and thousands separators). The result is further refined by the settings below.</li> <li> PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section <a href="#">Regular Expressions</a>.</li> </ul>

Setting	Description
Index of Capturing Group	<p><b>This setting is only visible if you select</b> Use a regular expression for extraction <a href="#">above</a>.</p> <p>If your regex uses capturing groups, specify which one captures the number. Enter an integer or leave the field empty.</p>
Decimal Separator	<p><b>This setting is only visible if you select</b> Use a regular expression for extraction <a href="#">above</a>.</p> <p>Define the character for the decimal separator of the number. Enter a string or leave the field empty.</p>
Thousands Separator	<p><b>This setting is only visible if you select</b> Use a regular expression for extraction <a href="#">above</a>.</p> <p>Define the character for the thousands separator of the number. Enter a string or leave the field empty.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> </ul> <p>Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</p> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display


**Sensor Display**

Primary Channel ⓘ Downtime


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p>


Setting	Description
	<p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Number Extraction with Regular Expression

 If you want to extract a number in the response string via a regex, note that the index for captures in this sensor is based on 1 (not on 0). Furthermore, capturing groups are not automatically created. The example below illustrates this issue.

Consider the following string as returned by a request for CPU usage:

```
5 Sec (3.49%), 1 Min (3.555%), 5 Min (3.90%)
```

Assuming you would like to filter for the number [3.555](#), this is the percentage in the second parentheses. Enter the following regex in the Regular Expression field:

```
(\d+\.\d+).*?(\d+\.\d+).*?(\d+\.\d+)
```

As Index of Capturing Group, enter [3](#). This extracts the desired number [3.555](#).

The index must be 3 in this case because the capturing groups here are the following:

- Group 1 contains [3.49%](#), [1 Min \(3.555\)](#), [5 Min \(3.90\)](#)

- Group 2 contains [3.49](#)
- Group 3 contains [3.555](#)
- Group 4 contains [3.90](#)

Keep this note about index and capturing groups in mind when using number extraction.

- ❗ It is not possible to match an empty string with the PRTG regex sensor search.
- ❗ PRTG supports Perl Compatible Regular Expression (PCRE) regex. For more information, see section [Regular Expressions](#).

## Channel List

- ❗ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Response Time	The response time ❗ This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

How do I create a WMI Custom sensor?

- <https://kb.paessler.com/en/topic/2743>

What security features does PRTG include?

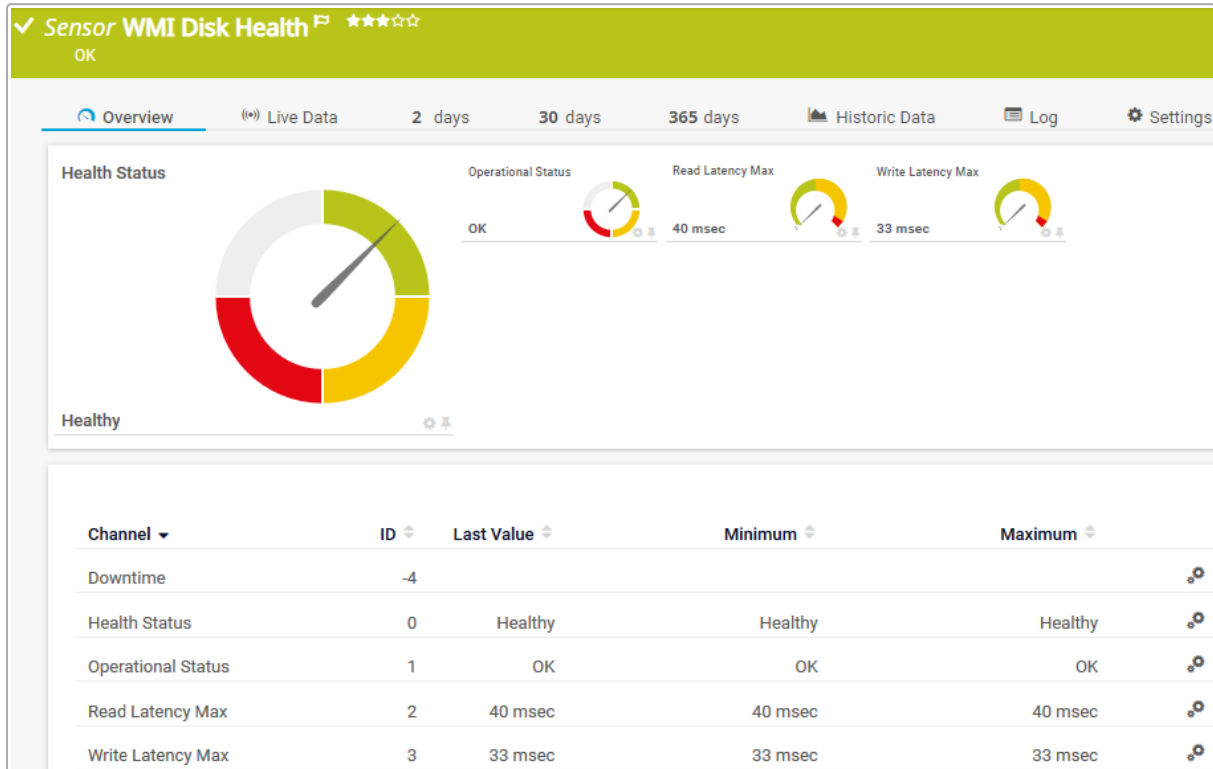
- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.285 WMI Disk Health Sensor

The WMI Disk Health sensor monitors the health of a physical disk on a Windows system via Windows Management Instrumentation (WMI).



WMI Disk Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: WMI schijfstatus
- French: État du disque (WMI)
- German: WMI Laufwerkszustand
- Japanese: WMI ディスクの正常性
- Portuguese: Funcionamento do disco (WMI)
- Russian: Работоспособность диска WMI
- Simplified Chinese: WMI 磁盘运行状况
- Spanish: Salud de disco (WMI)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
Windows version	This sensor supports Windows versions as of Windows 10 or Windows Server 2016 on the target system.
IPv6	This sensor supports IPv6.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- diskhealthsensor
- wmidiskhealthsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## WMI Disk Health Specific

**WMI Disk Health Specific**

Friendly Name ⓘ *SK hynix SC300 M.2 2280 256GB, 0*

Timeout (Sec.) ⓘ

WMI Disk Health Specific

Setting	Description
Friendly Name	The user-friendly name for the physical disk that this sensor monitors.
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p> ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

## Debug Options

**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>



## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Flush Latency Max	The maximum flush latency
Health Status	<p>The health status</p> <ul style="list-style-type: none"> <li>▪ Up status: Healthy</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Unhealthy</li> <li>▪ Unknown status: Unknown</li> </ul> <p> This channel is the primary channel by default.</p>
Operational Status	<p>The operational status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Error</li> <li>▪ Unknown status: Starting</li> </ul>
Read Latency Max	The maximum read latency
Write Latency Max	The maximum write latency

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

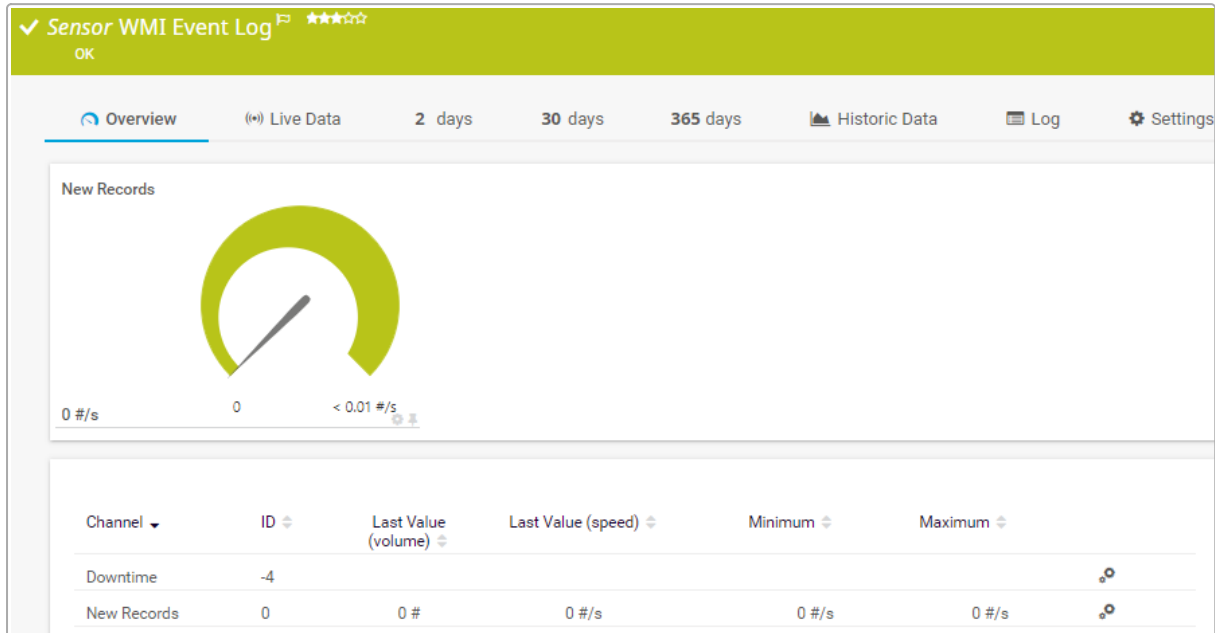
My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.286 WMI Event Log Sensor

The WMI Event Log sensor monitors a Windows log file via Windows Management Instrumentation (WMI).

**i** You can individually set the sensor to a specific status according to a new event log entry.



WMI Event Log Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: WMI Logboek
- French: Journal des événements (WMI)
- German: WMI Ereignisprotokoll
- Japanese: WMI イベントログ
- Portuguese: Log de eventos (WMI)
- Russian: Журнал событий WMI
- Simplified Chinese: WMI 事件日志
- Spanish: Registro de eventos (WMI)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a very high performance impact. We recommend that you use no more than <b>50</b> of this sensor on each probe.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Knowledge Base	<ul style="list-style-type: none"> <li>Knowledge Base: <a href="#">My Event Log sensor ignores changes in the event log. What can I do?</a></li> <li>Knowledge Base: <a href="#">How can I configure sensors using speed limits to keep the status for more than one interval?</a></li> </ul>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  x +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmieventlogsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## WMI Event Log Monitor

WMI Event Log Monitor
Log File ⓘ *Application*

Result Handling ⓘ

Discard result (default)
 

Store result

WMI Event Log Monitor

Setting	Description
Log File	The Windows log file that this sensor monitors.
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Filter Event Log Entries

- For more information and how to find out the correct filter, see the Knowledge Base: [My Event Log sensor ignores changes in the event log. What can I do?](#)

## Filter Event Log Entries

- Event Type ⓘ
- Any (default)
  - Error
  - Warning
  - Information
  - Security Audit Success
  - Security Audit Failure

- Filter by Source ⓘ
- Disable (default)
  - Enable

- Filter by ID ⓘ
- Disable (default)
  - Enable

- Filter by Category ⓘ
- Disable (default)
  - Enable

- Filter by User ⓘ
- Disable (default)
  - Enable

- Filter by Computer ⓘ
- Disable (default)
  - Enable

- Filter by Message ⓘ
- Disable (default)
  - Enable

Filter Event Log Entries

Setting	Description
Event Type	<p>Specify the type of event that this sensor processes:</p> <ul style="list-style-type: none"> <li>▪ Any</li> <li>▪ Error</li> <li>▪ Warning</li> <li>▪ Information</li> <li>▪ Security Audit Success</li> <li>▪ Security Audit Failure</li> </ul> <p> ⓘ The sensor cannot process other event types.</p>

Setting	Description
Filter by Source	<p>Filter all received events for a certain event source:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not filter events.</li> <li>▪ Enable: Filter events. <ul style="list-style-type: none"> <li>ⓘ The sensor only processes messages that match the value that you define below.</li> </ul> </li> </ul>
Filter Type	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Select the filter type:</p> <ul style="list-style-type: none"> <li>▪ Include filter: Include the specified value and disregard all other values.</li> <li>▪ Exclude filter: Exclude the specified value and regard all other values.</li> </ul>
Match String (Event Source)	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Enter an event source that you want to filter for. Depending on the kind of filter, the sensor either processes the event source (Include filter option) or it does not process it (Exclude filter option). Enter a string.</p>
Filter by ID	<p>Filter all received events for a certain event ID:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not filter events.</li> <li>▪ Enable: Filter events. <ul style="list-style-type: none"> <li>ⓘ The sensor only processes messages that match the value that you define below.</li> </ul> </li> </ul>
Filter Type	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Select the filter type:</p> <ul style="list-style-type: none"> <li>▪ Include filter: Include the specified value and disregard all other values.</li> <li>▪ Exclude filter: Exclude the specified value and regard all other values.</li> </ul>
Match Values (Event ID)	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Enter an event ID that you want to filter for. Depending on the kind of filter, the sensor either processes the event ID (Include filter option) or it does not process it (Exclude filter option).</p> <ul style="list-style-type: none"> <li>ⓘ The WMI Event Log supports more than one event ID. You can enter a comma-separated list of event IDs to filter for more than one ID. For example, <a href="#">1100,4627,4747,4884,5050,6422</a>.</li> </ul>
Filter by Category	<p>Filter all received events for a certain event category:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not filter events.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Enable: Filter events.</li> <li>ⓘ The sensor only processes messages that match the value that you define below.</li> </ul>
Filter Type	<p>This setting is only visible if you select Enable above.</p> <p>Select the filter type:</p> <ul style="list-style-type: none"> <li>▪ Include filter: Include the specified value and disregard all other values.</li> <li>▪ Exclude filter: Exclude the specified value and regard all other values.</li> </ul>
Match String (Event Category)	<p>This setting is only visible if you select Enable above.</p> <p>Enter a category that you want to filter for. Depending on the kind of filter, the sensor either processes the event category (Include filter option) or it does not process it (Exclude filter option). Enter a string.</p>
Filter by User	<p>Filter all received events for a certain event user:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not filter events.</li> <li>▪ Enable: Filter events.</li> <li>ⓘ The sensor only processes messages that match the value that you define below.</li> </ul>
Filter Type	<p>This setting is only visible if you select Enable above.</p> <p>Select the filter type:</p> <ul style="list-style-type: none"> <li>▪ Include filter: Include the specified value and disregard all other values.</li> <li>▪ Exclude filter: Exclude the specified value and regard all other values.</li> </ul>
Match String (Event User)	<p>This setting is only visible if you select Enable above.</p> <p>Enter a user name that you want to filter for. Depending on the kind of filter, the sensor either processes the event user (Include filter option) or it does not process it (Exclude filter option). Enter a string.</p>
Filter by Computer	<p>Filter all received events for a certain event computer:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not filter events.</li> <li>▪ Enable: Filter events.</li> <li>ⓘ The sensor only processes messages that match the value that you define below.</li> </ul>
Filter Type	<p>This setting is only visible if you select Enable above.</p>



Setting	Description
	<p>Select the filter type:</p> <ul style="list-style-type: none"> <li>▪ Include filter: Include the specified value and disregard all other values.</li> <li>▪ Exclude filter: Exclude the specified value and regard all other values.</li> </ul>
Match String (Event Computer)	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Enter a computer name that you want to filter for. Depending on the kind of filter, the sensor either processes the event computer (Include filter option) or it does not process it (Exclude filter option). Enter a string.</p>
Filter by Message	<p>Filter all received events for a certain event message:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): Do not filter events.</li> <li>▪ Enable: Filter events. <ul style="list-style-type: none"> <li>ⓘ The sensor only processes messages that match the value that you define below.</li> </ul> </li> </ul>
Filter Type	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Select the filter type:</p> <ul style="list-style-type: none"> <li>▪ Include filter: Include the specified value and disregard all other values.</li> <li>▪ Exclude filter: Exclude the specified value and regard all other values.</li> </ul>
Match String (Event Message)	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Enter a message that you want to filter for. Depending on the kind of filter, the sensor either processes the event message (Include filter option) or it does not process it (Exclude filter option). Enter a string.</p> <p>ⓘ You must use the percent sign (%) as wildcard for any or no character if you want to check if the string is part of the message. Otherwise, the whole event message must match the string. For example, you can enter %RAS% for any event message that contains the string RAS.</p>

## Sensor Display


**Sensor Display**

Primary Channel ⓘ Downtime


---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
New Records	The number of new records  This channel is the primary channel by default.

## More

### KNOWLEDGE BASE

My Event Log sensor ignores changes in the event log. What can I do?

- <https://kb.paessler.com/en/topic/59803>

How can I configure sensors using speed limits to keep the status for more than one interval?

- <https://kb.paessler.com/en/topic/73212>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

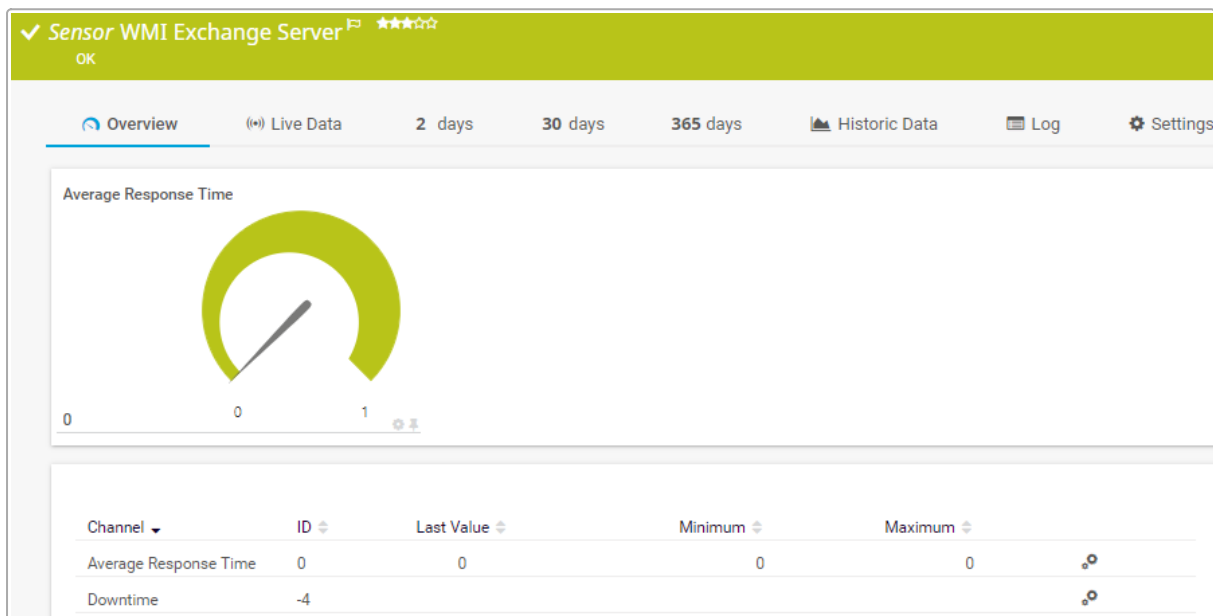
## 7.8.287 WMI Exchange Server Sensor

The WMI Exchange Server sensor monitors a Microsoft Exchange Server as of version 2016 via Windows Management Instrumentation (WMI).

You might be able to monitor aspects regarding:

- SMTP Server: Queue Lengths
- MExchangeIS Mailbox: Queue Sizes, Delivery Times, Operations, Messages
- MExchangeIS Public: Queue Sizes, Delivery Times, Operations, Messages
- MExchangeIS: Packets, Operations, Clients, Latency, Requests, Users
- MExchange RPC Client Access: Active User Count, User Count, Connection Count
- MExchange OWA: Current Unique Users, Average Response Time

**i** Depending on your Exchange server version, not all counters might be available.



WMI Exchange Server Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: WMI Exchange Server
- French: Exchange serveur (WMI)
- German: WMI Exchange-Server
- Japanese: WMI Exchange サーバー
- Portuguese: Servidor Exchange (WMI)
- Russian: WMI Exchange Server

- Simplified Chinese: WMI Exchange 服务器
- Spanish: Servidor Exchange (WMI)

## Remarks

Consider the following [remarks](#)<sup>[2511]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiexchangeserversensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

## Exchange Server Data Readings Accessible Using WMI

**Exchange Server Data Readings Accessible Using WMI**

**Display Name** ⓘ *MSEExchange OWA: Average Response Time*

**Instance** ⓘ

**WMI Class** ⓘ *Win32\_PerfRawData\_MSEExchangeOWA\_MSEExchangeOWA*

**Counter** ⓘ *AverageResponseTime*

**Time Stamp** ⓘ

**Time Frequency** ⓘ

**Counter Type** ⓘ *PERF\_COUNTER\_RAWCOUNT*

**Result Handling** ⓘ

Discard result (default)  
 Store result

Exchange Server Data Readings Accessible Using WMI

Setting	Description
Display Name	The display name that the sensor uses to query data from the target device.
Instance	The instance that the sensor uses to query data from the target device.
WMI Class	The WMI class that the sensor uses to query data from the target device.
Counter	The counter that the sensor uses to query data from the target device.
Time Stamp	The time stamp that the sensor uses to query data from the target device.
Time Frequency	The time frequency that the sensor uses to query data from the target device.
Counter Type	The counter type that the sensor uses to query data from the target device.
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **ⓘ** Downtime

---

Graph Type **ⓘ**
 Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⚙</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click **🔒** under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

❗ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Active User Count	The number of active users
Average Response Time	The average response time (OWA)
Connection Count	The number of connections
Current Unique Users	The number of current unique users (OWA)
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
RPC Requests Failed	The number of failed RPC requests
RPC Requests Outstanding	The number of outstanding RPC requests
RPC Requests Sent	The number of sent RPC requests
RPC Slow Requests	The number of slow RPC requests
User Count	The number of users

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

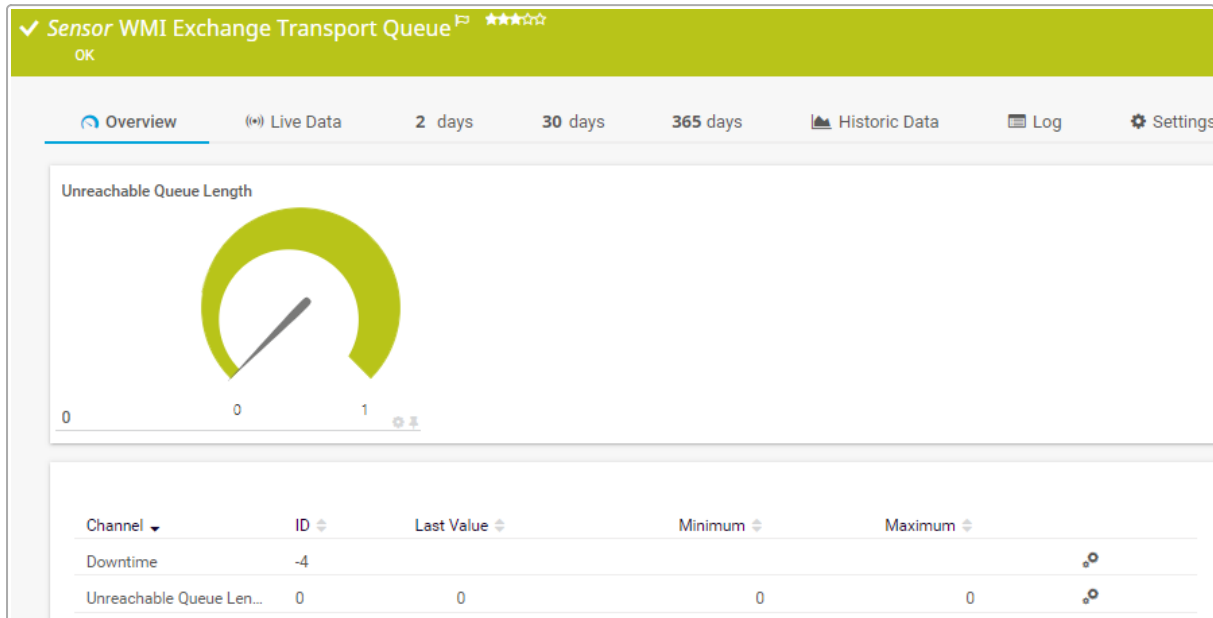
My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>



## 7.8.288 WMI Exchange Transport Queue Sensor

The WMI Exchange Transport Queue sensor monitors the length of transport queues of a Microsoft Exchange Server as of version 2016 via Windows Management Instrumentation (WMI). It shows the same information as in Windows System Monitor [perfmon](#).



WMI Exchange Transport Queue Sensor


- For more information and an explanation of transport queue types, see the Knowledge Base: [What types of Exchange transport queues are there?](#)
- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2519]</sup>.

### Sensor in Other Languages



- Dutch: WMI Exchange Transport Wachtrij
- French: Exchange file d'attente de transport (WMI)
- German: WMI Exchange Transportwarteschlange
- Japanese: WMI Exchange 転送キュー
- Portuguese: Fila de transporte Exchange (WMI)
- Russian: Очередь транспорта WMI Exchange
- Simplified Chinese: WMI Exchange 传输队列
- Spanish: Cola de transporte Exchange (WMI)

### Remarks

Consider the following [remarks](#)<sup>[2519]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Knowledge Base	Knowledge Base: <a href="#">What types of Exchange transport queues are there?</a>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Add Sensor

Setting	Description
Transport Queue	<p>Select the transport queues that you want to monitor. PRTG creates one sensor for each transport queue that you select.</p> <p> The available options depend on your Exchange server configuration. PRTG shows all possible queues with names and instance descriptions (if available).</p> <p> For performance reasons, we recommend that you only select necessary items.</p>

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiexchangeservertransportqueuesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## WMI Exchange Transport Queue Specific

**WMI Exchange Transport Queue Specific**

**Display Name** ⓘ *Active Mailbox Delivery Queue Length*

**Instance** ⓘ *\_total*

**WMI Class** ⓘ *Win32\_PerfRawData\_MSExchangeTransportQueues\_MSExchangeTransportQueues*

**Counter** ⓘ *ActiveMailboxDeliveryQueueLength*

**Time Stamp** ⓘ

**Time Frequency** ⓘ

**Counter Type** ⓘ *PERF\_COUNTER\_RAWCOUNT*

**Result Handling** ⓘ  Discard result (default)  
 Store result

WMI Exchange Transport Queue Specific

Setting	Description
Display Name	The display name that the sensor uses to query data from the target device.
Instance	The instance that the sensor uses to query data from the target device.
WMI Class	The WMI class that the sensor uses to query data from the target device.
Counter	The counter that the sensor uses to query data from the target device.
Time Stamp	The time stamp that the sensor uses to query data from the target device.
Time Frequency	The time frequency that the sensor uses to query data from the target device.
Counter Type	The counter type that the sensor uses to query data from the target device.
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **ⓘ** Downtime

---


Graph Type **ⓘ**  Show channels independently (default)

Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Active Mailbox Delivery Queue Length	The number of items in the active mailbox delivery queue
Active Non-SMTP Delivery Queue Length	The number of items in the non-SMTP delivery queue
Active Remote Delivery Queue Length	The number of items in the active remote delivery queue
Aggregate Delivery Queue Length (All Queues)	The number of items in the aggregate delivery queue (all queues)
Aggregate Shadow Queue Length	The number of items in the aggregate shadow queue
Categorizer Job Availability	The categorizer job availability
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Items Completed Delivery Per Second	The number of items with completed delivery
Items Completed Delivery Total	The number of items with completed delivery in total
Items Deleted By Admin Total	The number of items deleted by the admin in total

Channel	Description
Items Queued For Delivery Expired Total	The number of items expired queued for delivery in total
Items Queued for Delivery Per Second	The number of items queued for delivery
Items Queued For Delivery Total	The number of items queued for delivery in total
Items Resubmitted Total	The number of items resubmitted in total
Largest Delivery Queue Length	The largest number of items in the delivery queue
Messages Completed Delivery Per Second	The number of messages with completed delivery
Messages Completed Delivery Total	The number of messages with completed delivery in total
Messages Completing Categorization	The number of messages completing categorization
Messages Deferred Due To Local Loop	The number of messages deferred due to local loop
Messages Deferred During Categorization	The number of messages deferred during categorization
Messages Queued For Delivery	The number of messages queued for delivery
Messages Queued for Delivery Per Second	The number of messages queued for delivery per second
Messages Queued For Delivery Total	The number of messages queued for delivery in total
Messages Submitted Per Second	The number of messages submitted
Messages Submitted Total	The number of messages submitted in total

Channel	Description
Poison Queue Length	The number of items in the poison queue
Retry Mailbox Delivery Queue Length	The number of items in the retry mailbox delivery queue
Retry Non-SMTP Delivery Queue Length	The number of items in the retry non-SMTP delivery queue
Retry Remote Delivery Queue Length	The number of items in the retry remote delivery queue
Shadow Queue Auto Discards Total	The number of auto discards in the shadow queue in total
Submission Queue Items Expired Total	The number of items expired in the submission queue in total
Submission Queue Length	The number of items in the submission queue
Unreachable Queue Length	The number of items in the unreachable queue

## More

### ■ KNOWLEDGE BASE

What types of Exchange transport queues are there?

- <https://kb.paessler.com/en/topic/55413>

What security features does PRTG include?

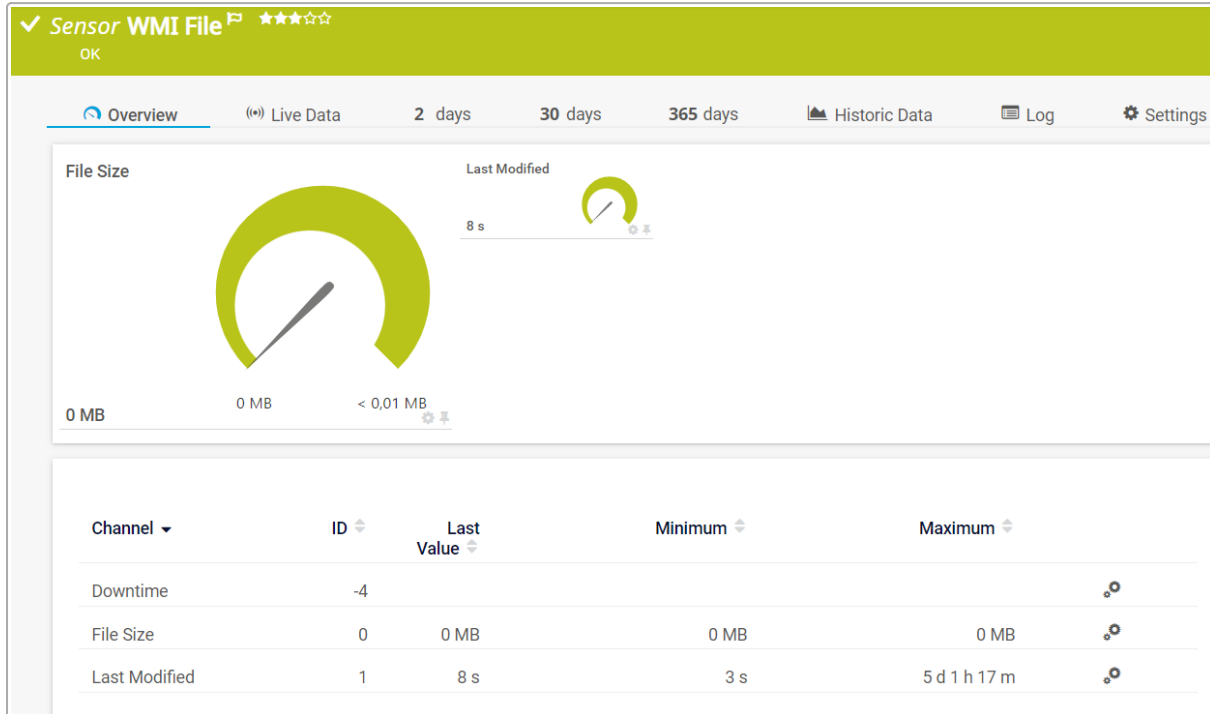
- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.289 WMI File Sensor

The WMI File sensor monitors a file via Windows Management Instrumentation (WMI).



WMI File Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).


### Sensor in Other Languages

- Dutch: WMI Bestand
- French: Fichier (WMI)
- German: WMI Datei
- Japanese: WMI ファイル
- Portuguese: Arquivo (WMI)
- Russian: Файл WMI
- Simplified Chinese: WMI 文件
- Spanish: Archivo (WMI)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:



Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmifilesensor

 For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### WMI File Monitor

#### WMI File Monitor

**File Name** ⓘ C:\Windows\regedit.exe

---

**If Time Stamp Changes** ⓘ  Ignore (default)  
 Trigger 'change' notification

WMI File Monitor

Setting	Description
File Name	<p>Enter the name of the file that you want to monitor. Enter the full local path. The file must exist on the probe system.</p> <p><b>i</b> The sensor does not support Universal Naming Convention (UNC) paths.</p>
If Time Stamp Changes	<p>Define what the sensor does if the time stamp of the file changes:</p> <ul style="list-style-type: none"> <li>Ignore (default): Do nothing.</li> <li>Trigger 'change' notification: Send an internal message that indicates a change.</li> </ul> <p><b>i</b> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</p>

## Debug Options

**Debug Options**

**Result Handling** ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display


**Sensor Display**

**Primary Channel** ⓘ Downtime


---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings


By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
File Size	The file size  This channel is the primary channel by default.
Last Modified	The time since the last modification of the file

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

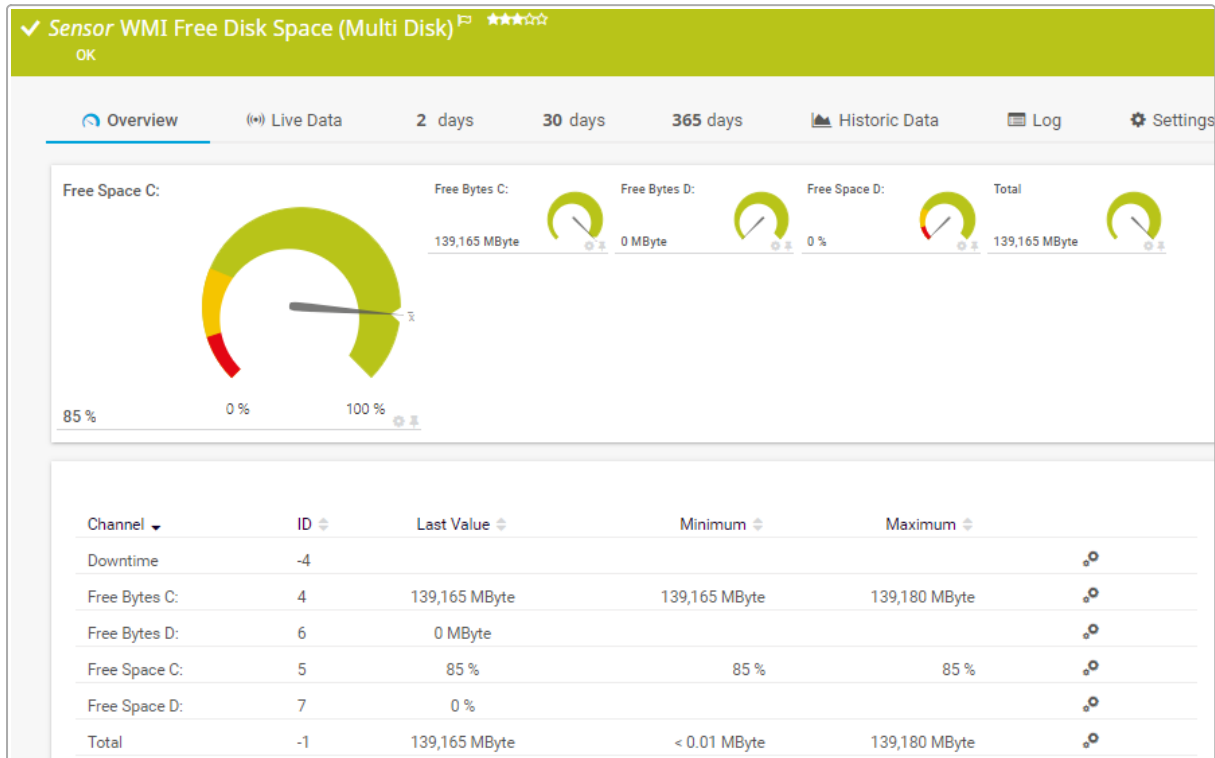
My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.290 WMI Free Disk Space (Multi Disk) Sensor

The WMI Free Disk Space (Multi Disk) sensor monitors the free disk space of one or more drives via Windows Management Instrumentation (WMI).

- ① The sensor monitors logical partitions of a hard or fixed disk drive. PRTG identifies logical disks by their drive letter, such as C.



WMI Free Disk Space (Multi Disk) Sensor


- For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2533]</sup>.

### Sensor in Other Languages

- Dutch: WMI Vrije Schijfruimte (Multi Schijf)
- French: Espace disponible de multiples disques (WMI)
- German: WMI Laufwerkskapazität (mehrf.)
- Japanese: WMI ディスク空き領域 (複数ドライブ)
- Portuguese: Espaço livre em disco (vários discos) (WMI)
- Russian: Свободное дисковое пространство WMI (на нескольких дисках)
- Simplified Chinese: WMI 磁盘可用空间 (多个磁盘)
- Spanish: Espacio libre en disco (discos múltiples) (WMI)

### Remarks

Consider the following [remarks](#)<sup>[2527]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- diskspacesensor
- wmidiskspacesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Drive Selection

#### Drive Selection

**Drives** ⓘ All

Drive Selection

Setting	Description
Drives	The drives that this sensor monitors. This is either <a href="#">All</a> or a specific drive letter.

## Set Limits Checked for ALL Disks

In this section, you can set limits that are valid for all channels and all drives. By entering limits, you can define when the sensor shows the Warning or the Down [status](#), depending on the data provided by all drives that this sensor monitors. If you want to individually define limits for separate channels, use the limit settings in the [channel settings](#).

**i** All limits that you define here are valid in addition to the limits defined in the particular channel settings. The limits are valid simultaneously, so the first limit that is breached applies.

**Set Limits Checked For ALL Disks** Use the channel settings to set separate error limits or warning limits for each disk.

Percentage Limit Check ?  Only use the limits in the settings of the percentage channels  
 Use the limits of both the sensor and the channel settings (default)

Upper Error Limit ?

Upper Warning Limit ?

Lower Warning Limit ?





Lower Error Limit ?

Size Limit Check ?  Only use the limits in the settings of the byte size channels (default)  
 Use the limits of both the sensor and the channel settings

Alarm on Missing/Removed Disk ?  Deactivate alarm (default)  
 Activate alarm

Set Limits Checked for ALL Disks

Setting	Description
Percentage Limit Check	<p>By default, the sensor enables percentage limits with a lower warning limit and a lower error limit. Enable or disable a limit check for the free space in percentage channels of all drives:</p> <ul style="list-style-type: none"> <li>▪ Only use the limits in the settings of the percentage channels: Do not define sensor limits that are valid for all percentage channels. The sensor only uses the limits that you define in the settings of the particular "free space in percent" channels to determine the status.</li> <li>▪ Use the limits of both the sensor and the channel settings (default): Define sensor limits that are valid for all percentage channels. Additional fields appear below. The sensor shows the Warning or the Down status when free space limits are above or below the limits.</li> </ul>

Setting	Description
Upper Error Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings (default) <a href="#">above</a>.</p> <p>Specify an upper limit in percent for the Down status. If the free disk space of one of your drives exceeds this value, the sensor changes to the Down status. Enter an integer or leave the field empty.</p> <p> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Upper Warning Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings (default) <a href="#">above</a>.</p> <p>Specify an upper limit in percent for the Warning status. If the free disk space of one of your drives exceeds this value, the sensor changes to the Warning status. Enter an integer or leave the field empty.</p> <p> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Lower Warning Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings (default) <a href="#">above</a>.</p> <p>Specify a lower limit in percent for the Warning status. If the free disk space of one of your drives falls below this value, the sensor changes to the Warning status. Enter an integer or leave the field empty.</p> <p> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Lower Error Limit	<p>Specify a lower limit in percent for the Down status. If the free disk space of one of your drives falls below this value, the sensor changes to the Down status. Enter an integer or leave the field empty.</p> <p> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Size Limit Check	<p>Enable or disable a limit check for the free bytes channels of all drives:</p>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ Only use the limits in the settings of the byte size channels (default): Do not define sensor limits that are valid for all byte size channels. The sensor only uses limits that you define in the settings of the particular free space in bytes channels to determine the status.</li> <li>▪ Use the limits of both the sensor and the channel settings: Define limits for the sensor that are valid for all byte size channels. Additional fields appear below. The sensor shows the Warning or Down status when free space limits are above or below the value.</li> </ul> <p><b>i</b> By default, byte size limits are not enabled for drives.</p>
Upper Error Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings <a href="#">above</a>.</p> <p>Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (the default unit is <b>MB</b>). If the free disk space of one of your drives exceeds this value, the sensor changes to the Down status. Enter an integer or leave the field empty.</p> <p><b>i</b> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Upper Warning Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings <a href="#">above</a>.</p> <p>Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (the default unit is <b>MB</b>). If the free disk space of one of your drives exceeds this value, the sensor changes to the Warning status. Enter an integer or leave the field empty.</p> <p><b>i</b> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Lower Warning Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings <a href="#">above</a>.</p> <p>Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (the default unit is <b>MB</b>). If the free disk space of one of your drives falls below this value, the sensor changes to the Warning status. Enter an integer or leave the field empty.</p> <p><b>i</b> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>

Setting	Description
Lower Error Limit	<p><b>This setting is only visible if you select</b> Use the limits of both the sensor and the channel settings <a href="#">above</a>.</p> <p>Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (the default unit is <b>MB</b>). If the free disk space of one of your drives falls below this value, the sensor changes to the Down status. Enter an integer or leave the field empty.</p> <p><b>i</b> The limits that you set here are valid for all channels of this sensor. You can additionally set individual limits for each channel in the channel settings. Both the limits that you set here and in the channel settings are valid simultaneously.</p>
Alarm on Missing/Removed Disk	<p>If a monitored disk is removed or not found, the sensor sets the values to zero. Select the alarm approach in this case:</p> <ul style="list-style-type: none"> <li>▪ Deactivate alarm (default): Do not send an alert for a removed disk.</li> <li>▪ Activate alarm: Send an alert if a monitored disk is removed or not found.</li> </ul>

## Debug Options

**Debug Options**

Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Bytes C:	The free space
Free Bytes D:	The free space
Free Space C:	The free space (%)
Free Space D:	The free space (%)
Total	The total disk space

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

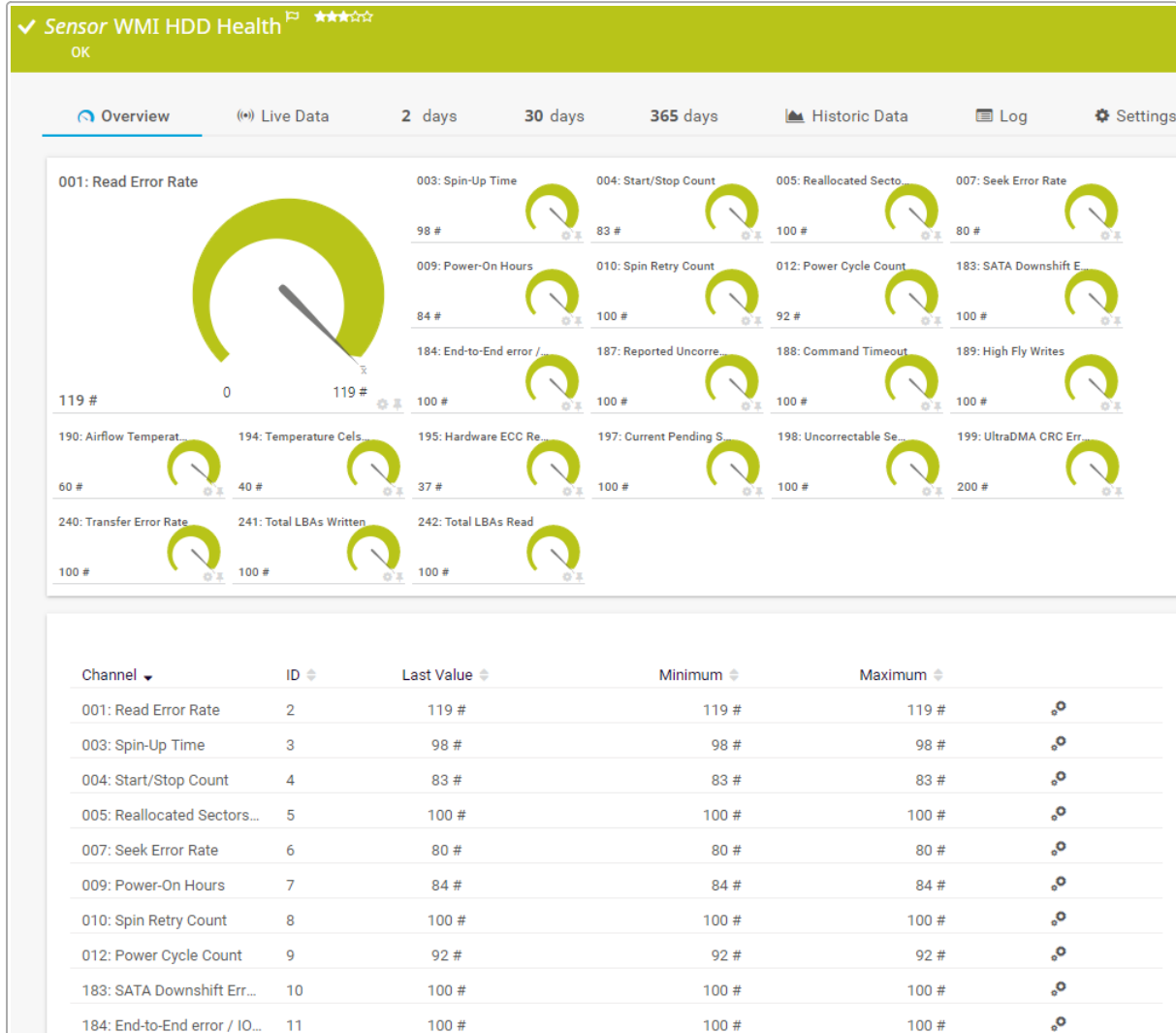
- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.291 WMI HDD Health Sensor

The WMI HDD Health sensor connects to the parent device via Windows Management Instrumentation (WMI) and monitors the health of integrated development environment (IDE) disk drives on the target system using Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.).



WMI HDD Health Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#) [2539].

### Sensor in Other Languages

- Dutch: WMI HDD Status
- French: État du disque dur (WMI)
- German: WMI Laufwerkszustand
- Japanese: WMI HDD 正常性
- Portuguese: Funcionamento do HDD (WMI)
- Russian: Работоспособность жесткого диска WMI

- Simplified Chinese: WMI 硬盘健康状况
- Spanish: Salud HDD (WMI)

## Remarks

Consider the following [remarks](#) <sup>[2536]</sup> and requirements for this sensor:

Remark	Description
Windows version	This sensor requires at least Windows 7 on the target system that holds the hard disk drives you want to monitor. The sensor might not work reliably if the target system runs on Windows 2003, Windows XP, or Windows Vista. Because of a known bug in those systems, the sensor might not detect available hard disk drives.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv4	This sensor only supports IPv4.
Performance impact	This sensor has a <b>medium</b> performance impact.
Sensor values	The values that this sensor shows can vary depending on how a vendor handles S.M.A.R.T. values. See the respective vendor's documentation for more information.
Add Sensor dialog	The items in the list in the Add Sensor dialog are specific to the parent device.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- smartsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### S.M.A.R.T. Specific

#### S.M.A.R.T. Specific

Serial Number ⓘ	12345ABCDE
Size (GB) ⓘ	978
Name ⓘ	\\.\PHYSICALDRIVE0
Timeout (Sec.) ⓘ	60

S.M.A.R.T. Specific

Setting	Description
Serial Number	The serial number of the disk that this sensor monitors.
Size (GB)	The size of the disk that this sensor monitors.
Name	The name of the disk that this sensor monitors.
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p><b>i</b> If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

### Debug Options

#### Debug Options

Result Handling ⓘ	<input checked="" type="radio"/> Discard result (default) <input type="radio"/> Store result
-------------------	---

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)

Stack channels on top of each other


Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p>



Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).


## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

The channel names indicate the ID of the S.M.A.R.T. attribute, followed by a colon, and the typical meaning of the channel. The sensor can also show other attributes that the target device returns, but some channels have the name Unknown Channel. This happens if PRTG cannot match the ID of a found attribute with an internally defined channel name.

 Some vendors do not agree on attribute definitions and define meanings other than the common ones.

Every attribute of a disk assumes a value. PRTG shows these attributes as channels with their last, minimum, and maximum value. These channel values change over time and indicate the disk health. Higher values correspond to a better health. The disk's attributes come with a threshold, defined by the manufacturer of the drive. If a channel value is lower than this threshold, the sensor automatically shows the Warning [status](#). This indicates that the S.M.A.R.T. status of the HDD might break soon.

 For some attributes, there are no thresholds defined and because of this, they cannot be categorized for a status other than the Up status. You can define [lookups](#) and use them with affected channels to get the desired status for a return value.

Channel	Description
Average Erase Count And Maximum Erase Count	The average erase count and the maximum erase count
Command Timeout	The command timeout count

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Erase Fail Count	The erase fail count
G-Sense Error Rate	The G-sense error rate count
Hardware ECC Recovered	The hardware ECC recovered count
Power Cycle Count	The power cycle count
Power Loss Protection Failure	The power loss protection failure count
Power-On Hours	The power-on hours count
Program Fail Count Total	The program fail count total
Read Error Rate	The read error rate count  This channel is the primary channel by default.
Read Error Retry Rate	The read error retry rate count
Reallocated Sectors Count	The reallocated sectors count
Reported Uncorrectable Errors	The reported uncorrectable errors count
SATA Downshift Error Count	The SATA downshift error count
Soft ECC Correction	The soft ECC correction count
Soft Read Error Rate	The soft read error rate count
SSD Erase Fail Count	The SSD erase fail count
SSD Life Left	The SSD life left count

Channel	Description
SSD Program Fail Count	The SSD program fail count
Unexpected Power Loss Count	The unexpected power loss count
Unknown Channel	PRTG cannot match the ID of a found attribute with an internally defined channel name
Unused Reserved Block Count Total	The total unused reserved block count
Used Reserved Block Count Total	The total used reserved block count
Temperature Celsius	The temperature
Total LBAs Read	The total LBAs read
Total LBAs Written	The total LBAs written
Wear Range Delta	The wear range delta

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

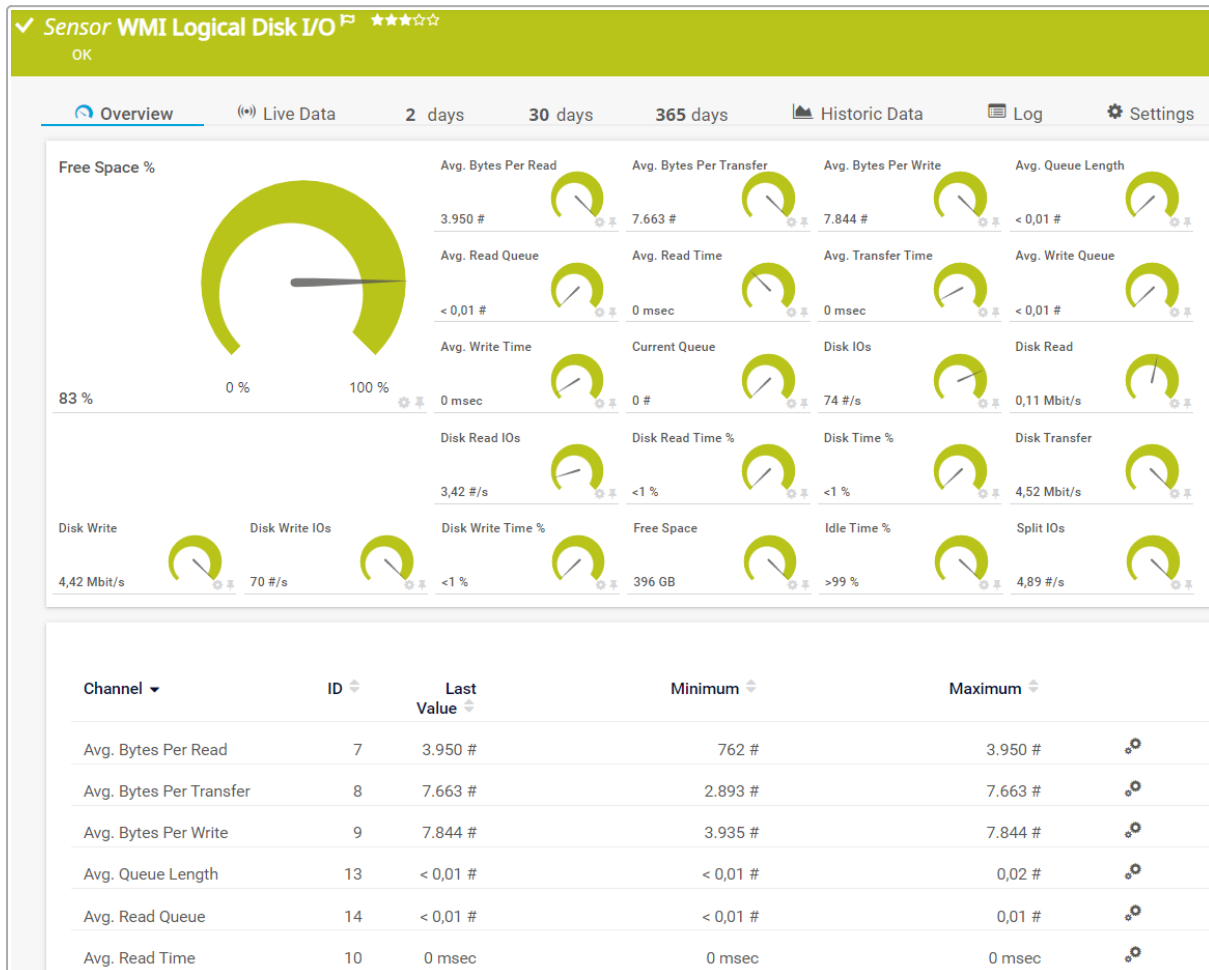
My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.292 WMI Logical Disk I/O Sensor

The WMI Logical Disk I/O sensor monitors the disk usage of a logical disk or mount point on a Windows system via Windows Management Instrumentation (WMI).

**i** The sensor shows performance data of counters that monitor logical partitions of a hard drive. The system monitor identifies logical disk instances by their identifier, such as C:, and the sensor reads the logical disk object in the system monitor and returns the values.



WMI Logical Disk I/O Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: WMI Logische Schijf I/O
- French: Disque logique E/S (WMI)
- German: WMI Logischer Datenträger E/A
- Japanese: WMI 論理ディスク I/O
- Portuguese: E/S do disco lógico (WMI)
- Russian: Ввод-вывод логического диска WMI

- Simplified Chinese: WMI 逻辑磁盘 I/O
- Spanish: E/S de disco lógico (WMI)

## Remarks

Consider the following [remarks](#)<sup>[2543]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Windows version	This sensor requires at least Windows Server 2008 R2. It does not work on previous Windows versions (Windows Server 2008 or earlier).
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

**Basic Sensor Settings**

Sensor Name ⓘ Example Name

Tags ⓘ  X +

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmilogicalsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>[667]</sup>.

### WMI Logical Disk I/O Specific

WMI Logical Disk Specific
Disk ⓘ *\_Total*

WMI Logical Disk I/O Specific

Setting	Description
Disk	The logical disk or mount point that this sensor monitors.

### Debug Options

Debug Options
Result Handling ⓘ

Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### Sensor Display


Sensor Display

Primary Channel ⓘ Downtime


Graph Type ⓘ

Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).


## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Avg. Bytes Per Read	The average number of bytes per read
Avg. Bytes Per Transfer	The average number of bytes per transfer

Channel	Description
Avg. Bytes Per Write	The average number of bytes per write
Avg. Queue Length	The average number of items in the queue
Avg. Read Queue	The average number of items in the read queue
Avg. Read Time	The average read time
Avg. Transfer Time	The average transfer time
Avg. Write Queue	The average number of items in the write queue
Avg. Write Time	The average write time
Current Queue	The current number of items in the queue
Disk IOs	The number of disk I/O operations
Disk Read	The disk read speed
Disk Read IOs	The number of disk read I/O operations
Disk Read Time %	The disk read time (%)
Disk Time %	The disk time (%)
Disk Transfer	The disk transfer speed
Disk Write	The disk write speed
Disk Write IOs	The number of disk write I/O operations
Disk Write Time %	The disk write time (%)
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Space	The free space
Free Space %	The free space (%)



Channel	Description
	 This channel is the primary channel by default.
Idle Time %	The idle time (%)
Split IOs	The number of split I/O operations

## More

### KNOWLEDGE BASE

What security features does PRTG include?

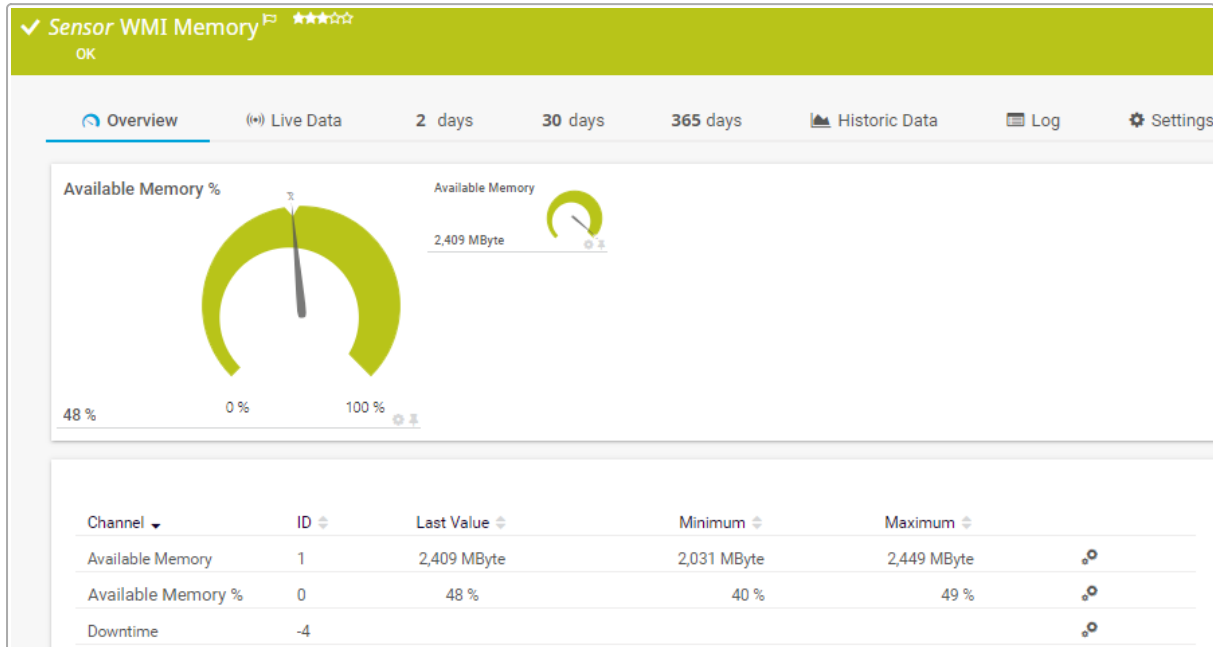
- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.293 WMI Memory Sensor

The WMI Memory sensor monitors available (free) system memory on Windows systems via Windows Management Instrumentation (WMI).



WMI Memory Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>2551</sup>.

### Sensor in Other Languages

- Dutch: WMI Geheugen
- French: Mémoire (WMI)
- German: WMI Arbeitsspeicher
- Japanese: WMI メモリ
- Portuguese: Memória (WMI)
- Russian: Память WMI
- Simplified Chinese: WMI 内存
- Spanish: Memoria (WMI)

### Remarks

Consider the following [remarks](#)<sup>2548</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- memmysensor
- wmmemmysensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Debug Options

#### Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### Alternative WMI Query

**Alternative WMI Query**

WMI sensors use the most efficient and accurate WMI queries possible. However, different Windows versions and even different patch levels on the target systems can lead to changes in some WMI classes. These changes often result in errors like class not valid or invalid data. If these errors persist, try the option Use the alternative WMI query method.

Query Method **i**

Use the default WMI query method (default)

Use the alternative WMI query method

Alternative WMI Query

Setting	Description
Query Method	<p>Select the method that the sensor uses to query via WMI:</p> <ul style="list-style-type: none"> <li>▪ Use the default WMI query method (default): Use the standard method to query WMI. We recommend that you use this option.</li> <li>▪ Use the alternative WMI query method: Use an alternative method to query WMI for better compatibility if WMI sensors return errors such as <a href="#">class not valid</a> or <a href="#">invalid data</a>.</li> </ul>

### Sensor Display

**Sensor Display**

Primary Channel **i** Downtime


---

Graph Type **i**


Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings



By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

**i** Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Available Memory	The available memory
Available Memory %	The available memory (%)

Channel	Description
	<p> This channel is the primary channel by default.</p> <p> This channel has a default limit:</p> <ul style="list-style-type: none"><li>▪ Lower warning limit: <a href="#">30%</a></li></ul>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.294 WMI Microsoft SQL Server 2005 Sensor (Deprecated)

### Important Notice

This sensor is deprecated.

Monitoring of Microsoft SQL Server 2005 using PRTG is discontinued. Microsoft SQL Server 2005 cannot be monitored with PRTG anymore with the latest updates of SQL Server 2005. The reason for this is a software update delivered by Microsoft in August 2012. The following updates cause this issue:

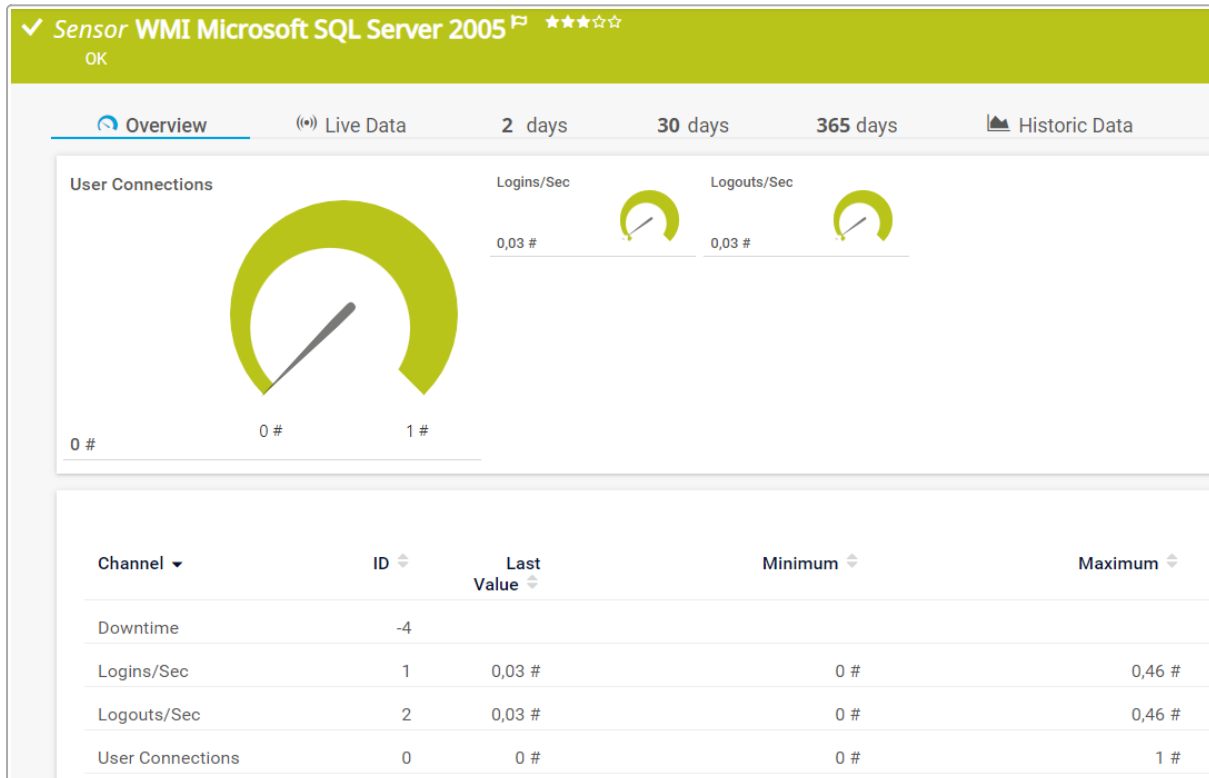
- Security Update for SQL Server 2005 Service Pack 4 (KB2716429)
- Security Update for SQL Server 2005 Service Pack 4 (KB2716427)

We have made reasonable effort to fix this from our side but we were unable to do so. We do not have instructions to circumvent this issue at this time. Please ask the vendor to fix this.

### More

Knowledge Base: [Why does my WMI Microsoft SQL Server 2005 sensor not work anymore?](#)

The WMI Microsoft SQL Server 2005 sensor monitors the performance of a Microsoft SQL Server via Windows Management Instrumentation (WMI).



WMI Microsoft SQL Server 2005 Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

## Sensor in Other Languages

- Dutch: WMI Microsoft SQL Server 2005
- French: Microsoft SQL serveur 2005 (WMI)
- German: WMI Microsoft SQL Server 2005
- Japanese: WMI Microsoft SQL Server 2005
- Portuguese: Microsoft SQL Server 2005 (WMI)
- Russian: WMI Microsoft SQL Server 2005
- Simplified Chinese: WMI Microsoft SQL Server 2005
- Spanish: Microsoft SQL Server 2005 (WMI)

## Remarks

Consider the following [remarks](#) <sup>2554</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
Target system	You can only add this sensor to a target system that runs a Microsoft SQL database.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.



## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmisqlserversensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## SQL Server Settings

### SQL Server Settings

**Service** ⓘ MSSQLSERVER

**Name** ⓘ SQL Server (MSSQLSERVER)

**Naming Method** ⓘ  Automatically determine the WMI class name (default)  
 Manually enter the WMI class name

**Result Handling** ⓘ  Discard result (default)  
 Store result

SQL Server Settings

Setting	Description
Service	The service that this sensor monitors. <span style="font-size: 1.2em;">ⓘ</span> The service name is provided as returned by the SQL server.
Name	The name of the server instance that this sensor monitors. <span style="font-size: 1.2em;">ⓘ</span> The display name is provided as returned by the SQL server.
Naming Method	Select whether PRTG automatically selects the name of the WMI class used for monitoring:

Setting	Description
	<ul style="list-style-type: none"> <li>Automatically determine the WMI class name (default): Automatically select WMI class. We recommend this setting.</li> <li>Manually enter the WMI class name: Manually enter a WMI class name. Select this option if your server instance returns an error code in automatic mode.</li> </ul>
WMI Class	<p><b>This setting is only visible if you select</b> Manually enter the WMI class name <a href="#">above</a>.</p> <p>Enter the WMI class name that the sensor uses to monitor the server instance.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>Discard result (default): Do not store the sensor result.</li> <li>Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## SQL Counter Specific

SQL Counter Specific

Performance Counters i
General Statistics

SQL Counter Specific

Setting	Description
Performance Counters	<p>You see a list of different groups of performance counters that the sensor can monitor for the instances that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counters you select here.</p> <ul style="list-style-type: none"> <li>General Statistics: Read general performance counters. This shows the number of user connections and the number of logins and logouts per second.</li> <li>Access Methods: Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second).</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ <b>Buffer Manager:</b> Read buffer manager counters. This shows the buffer cache hit ratio in percent and the number of database pages and stolen pages.</li> <li>▪ <b>Memory Manager:</b> Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb).</li> <li>▪ <b>Locks:</b> Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time.</li> <li>▪ <b>SQL Statistics:</b> Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second).</li> </ul> <p>Depending on your selection, PRTG creates a sensor with the specified channels.</p> <p><b>i</b> To monitor more than one of the listed groups of performance counters, add the sensor several times for the respective instances.</p> <p><b>i</b> After sensor creation, this setting shows the performance counter that this sensor monitors.</p>

## Sensor Display

**Sensor Display**


**Primary Channel** ⓘ Downtime

---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ <b>Show channels independently (default):</b> Show a graph for each channel.</li> </ul>


Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Average Wait Time	The average amount of wait time for each lock request that resulted in a wait
Batch Requests/Sec	The number of Transact-SQL command batches received. This statistic is affected by all constraints (such as input/output, number of users, cache size, or complexity of requests). High batch requests mean good throughput.
Buffer Cache Hit Ratio	The percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little.

Channel	Description
	Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.
Connection Memory (KB)	The total amount of dynamic memory the server is using for maintaining connections
Database Pages	The number of pages in the buffer pool with database content
Number of Deadlocks/Sec	The number of lock requests that resulted in a deadlock
Full Scans/Sec	The number of unrestricted full scans. These can be either base-table or full-index scans.
Lock Requests/Sec	The number of new locks and lock conversions requested from the lock manager
Logins/Sec	The total number of logins started
Logouts/Sec	The total number of logout operations started
Optimizer Memory (KB)	The total amount of dynamic memory the server is using for query optimization
Page Life Expectancy	The number of seconds a page stays in the buffer pool without references
Page Splits/Sec	The number of page splits that occur as the result of overflowing index pages
SQL Cache Memory (KB)	The total amount of dynamic memory the server is using for the dynamic SQL cache
SQL Compilations/Sec	The number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles because of recompiles. After the SQL Server user activity is stable, this value reaches a steady state.
SQL Recompilations/Sec	The number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.
Stolen Pages	The number of pages used for miscellaneous server purposes (including procedure cache)

Channel	Description
Table Lock Escalations/Sec	The number of times that locks on a table were escalated
Target Server Memory (KB)	The total amount of dynamic memory the server can consume
Total Server Memory (KB)	The total amount of dynamic memory that the server is using
User Connections	The number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.

## More

### ■ KNOWLEDGE BASE

Why does my WMI Microsoft SQL Server 2005 sensor not work anymore?

- <https://kb.paessler.com/en/topic/44713>

What security features does PRTG include?

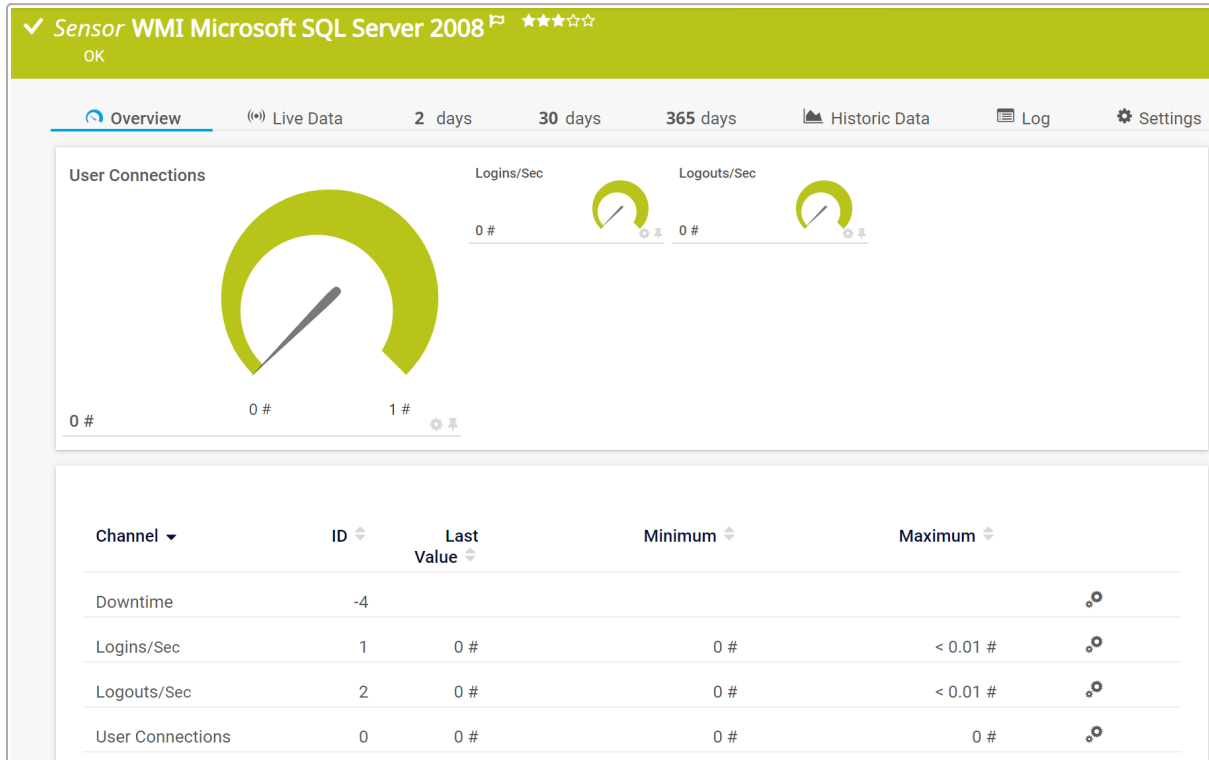
- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.295 WMI Microsoft SQL Server 2008 Sensor

The WMI Microsoft SQL Server 2008 sensor monitors the performance of a Microsoft SQL Server via Windows Management Instrumentation (WMI).



WMI Microsoft SQL Server 2008 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: WMI Microsoft SQL Server 2008
- French: Microsoft SQL serveur 2008 (WMI)
- German: WMI Microsoft SQL Server 2008
- Japanese: WMI Microsoft SQL Server 2008
- Portuguese: Microsoft SQL Server 2008 (WMI)
- Russian: WMI Microsoft SQL Server 2008
- Simplified Chinese: WMI Microsoft SQL Server 2008
- Spanish: Microsoft SQL Server 2008 (WMI)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
Target system	You can only add this sensor to a target system that runs a Microsoft SQL database.
IPv6	This sensor supports IPv6.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiqlserversensor
- wmiqlserversensor2008

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.



## SQL Server Settings

### SQL Server Settings

**Service** ⓘ *MSSQLSERVER*

**Name** ⓘ *SQL Server (MSSQLSERVER)*

**Naming Method** ⓘ  Automatically determine the WMI class name (default)  
 Manually enter the WMI class name

**Result Handling** ⓘ  Discard result (default)  
 Store result

SQL Server Settings

Setting	Description
Service	The service that this sensor monitors. ⓘ The service name is provided as returned by the SQL server.
Name	The name of the server instance that this sensor monitors. ⓘ The display name is provided as returned by the SQL server.
Naming Method	Select whether PRTG automatically selects the name of the WMI class used for monitoring: <ul style="list-style-type: none"> <li>▪ Automatically determine the WMI class name (default): Automatically select WMI class. We recommend this setting.</li> <li>▪ Manually enter the WMI class name: Manually enter a WMI class name. Select this option if your server instance returns an error code in automatic mode.</li> </ul>
WMI Class	<b>This setting is only visible if you select Manually enter the WMI class name above.</b>  Enter the WMI class name that the sensor uses to monitor the server instance.
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### SQL Counter Specific

**SQL Counter Specific** Performance Counters ⓘ *General Statistics*

SQL Counter Specific

Setting	Description
Performance Counters	<p>You see a list of different groups of performance counters that the sensor can monitor for the instances that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counters you select here.</p> <ul style="list-style-type: none"> <li>▪ <b>General Statistics:</b> Read general performance counters. This shows the number of user connections and the number of logins and logouts per second.</li> <li>▪ <b>Access Methods:</b> Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second).</li> <li>▪ <b>Buffer Manager:</b> Read buffer manager counters. This shows the buffer cache hit ratio in percent and the number of database pages and stolen pages.</li> <li>▪ <b>Memory Manager:</b> Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb).</li> <li>▪ <b>Locks:</b> Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time.</li> <li>▪ <b>SQL Statistics:</b> Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second).</li> </ul> <p>Depending on your selection, PRTG creates a sensor with the specified channels.</p> <p><b>i</b> To monitor more than one of the listed groups of performance counters, add the sensor several times for the respective instances.</p> <p><b>i</b> After sensor creation, this setting shows the performance counter that this sensor monitors.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Average Wait Time	The average amount of wait time for each lock request that resulted in a wait
Batch Requests/Sec	The number of Transact-SQL command batches received. This statistic is affected by all constraints (such as input/output, number of users, cache size, or complexity of requests). High batch requests mean good throughput.
Buffer Cache Hit Ratio	<p>The percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little.</p> <p>Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.</p>
Connection Memory (KB)	The total amount of dynamic memory the server is using for maintaining connections
Database Pages	The number of pages in the buffer pool with database content
Number of Deadlocks/Sec	The number of lock requests that resulted in a deadlock
Full Scans/Sec	The number of unrestricted full scans. These can be either base-table or full-index scans.
Lock Requests/Sec	The number of new locks and lock conversions requested from the lock manager
Logins/Sec	The total number of logins started
Logouts/Sec	The total number of logout operations started
Optimizer Memory (KB)	The total amount of dynamic memory the server is using for query optimization
Page Life Expectancy	The number of seconds a page stays in the buffer pool without references
Page Splits/Sec	The number of page splits that occur as the result of overflowing index pages

Channel	Description
SQL Cache Memory (KB)	The total amount of dynamic memory the server is using for the dynamic SQL cache
SQL Compilations/Sec	The number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles because of recompiles. After the SQL Server user activity is stable, this value reaches a steady state.
SQL Recompilations/Sec	The number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.
Stolen Pages	The number of pages used for miscellaneous server purposes (including procedure cache)
Table Lock Escalations/Sec	The number of times that locks on a table were escalated
Target Server Memory (KB)	The total amount of dynamic memory the server can consume
Total Server Memory (KB)	The total amount of dynamic memory that the server is using
User Connections	The number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

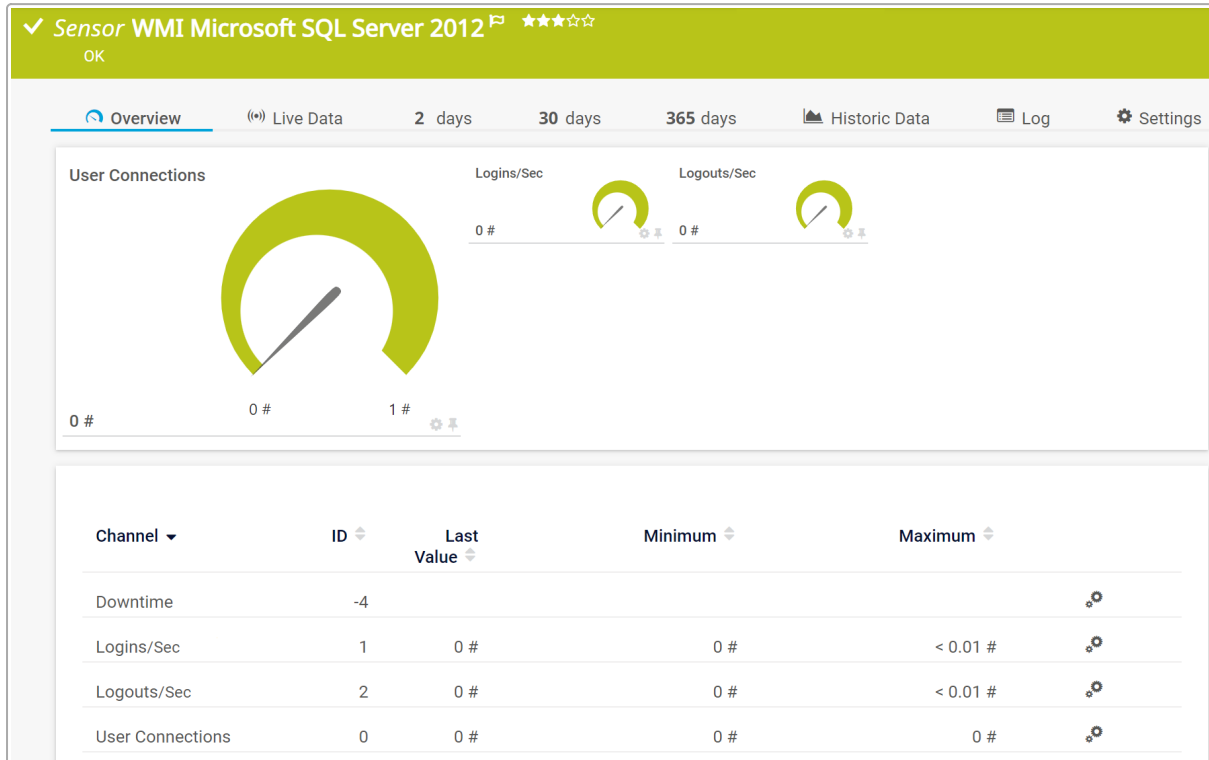
- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.296 WMI Microsoft SQL Server 2012 Sensor

The WMI Microsoft SQL Server 2012 sensor monitors the performance of a Microsoft SQL Server via Windows Management Instrumentation (WMI).



WMI Microsoft SQL Server 2012 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2572]</sup>.

### Sensor in Other Languages

- Dutch: WMI Microsoft SQL Server 2012
- French: Microsoft SQL serveur 2012 (WMI)
- German: WMI Microsoft SQL Server 2012
- Japanese: WMI Microsoft SQL Server 2012
- Portuguese: Microsoft SQL Server 2012 (WMI)
- Russian: WMI Microsoft SQL Server 2012
- Simplified Chinese: WMI Microsoft SQL Server 2012
- Spanish: Microsoft SQL Server 2012 (WMI)

### Remarks

Consider the following [remarks](#)<sup>[2568]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
Target system	You can only add this sensor to a target system that runs a Microsoft SQL database.
IPv6	This sensor supports IPv6.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

**Basic Sensor Settings**

Sensor Name ⓘ Example Name

Tags ⓘ  ✕ ⊕

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiqlserversensor
- wmiqlserversensor2012

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## SQL Server Settings

### SQL Server Settings

**Service** ⓘ *MSSQLSERVER*

**Name** ⓘ *SQL Server (MSSQLSERVER)*

**Naming Method** ⓘ  Automatically determine the WMI class name (default)  
 Manually enter the WMI class name

**Result Handling** ⓘ  Discard result (default)  
 Store result

SQL Server Settings

Setting	Description
Service	The service that this sensor monitors. ⓘ The service name is provided as returned by the SQL server.
Name	The name of the server instance that this sensor monitors. ⓘ The display name is provided as returned by the SQL server.
Naming Method	Select whether PRTG automatically selects the name of the WMI class used for monitoring: <ul style="list-style-type: none"> <li>▪ Automatically determine the WMI class name (default): Automatically select WMI class. We recommend this setting.</li> <li>▪ Manually enter the WMI class name: Manually enter a WMI class name. Select this option if your server instance returns an error code in automatic mode.</li> </ul>
WMI Class	<b>This setting is only visible if you select Manually enter the WMI class name above.</b>  Enter the WMI class name that the sensor uses to monitor the server instance.
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul>



Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### SQL Counter Specific

**SQL Counter Specific** Performance Counters ⓘ *General Statistics*

SQL Counter Specific

Setting	Description
Performance Counters	<p>You see a list of different groups of performance counters that the sensor can monitor for the instances that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counters you select here.</p> <ul style="list-style-type: none"> <li>▪ <b>General Statistics:</b> Read general performance counters. This shows the number of user connections and the number of logins and logouts per second.</li> <li>▪ <b>Access Methods:</b> Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second).</li> <li>▪ <b>Buffer Manager:</b> Read buffer manager counters. This shows the buffer cache hit ratio in percent and the number of database pages and stolen pages.</li> <li>▪ <b>Memory Manager:</b> Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb).</li> <li>▪ <b>Locks:</b> Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time.</li> <li>▪ <b>SQL Statistics:</b> Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second).</li> </ul> <p>Depending on your selection, PRTG creates a sensor with the specified channels.</p> <p><b>i</b> To monitor more than one of the listed groups of performance counters, add the sensor several times for the respective instances.</p> <p><b>i</b> After sensor creation, this setting shows the performance counter that this sensor monitors.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p>ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Average Wait Time	The average amount of wait time for each lock request that resulted in a wait
Batch Requests/Sec	The number of Transact-SQL command batches received. This statistic is affected by all constraints (such as input/output, number of users, cache size, or complexity of requests). High batch requests mean good throughput.
Buffer Cache Hit Ratio	<p>The percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little.</p> <p>Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.</p>
Connection Memory (KB)	The total amount of dynamic memory the server is using for maintaining connections
Database Pages	The number of pages in the buffer pool with database content
Number of Deadlocks/Sec	The number of lock requests that resulted in a deadlock
Full Scans/Sec	The number of unrestricted full scans. These can be either base-table or full-index scans.
Lock Requests/Sec	The number of new locks and lock conversions requested from the lock manager
Logins/Sec	The total number of logins started
Logouts/Sec	The total number of logout operations started
Optimizer Memory (KB)	The total amount of dynamic memory the server is using for query optimization
Page Life Expectancy	The number of seconds a page stays in the buffer pool without references
Page Splits/Sec	The number of page splits that occur as the result of overflowing index pages

Channel	Description
SQL Cache Memory (KB)	The total amount of dynamic memory the server is using for the dynamic SQL cache
SQL Compilations/Sec	The number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles because of recompiles. After the SQL Server user activity is stable, this value reaches a steady state.
SQL Recompilations/Sec	The number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.
Stolen Pages	The number of pages used for miscellaneous server purposes (including procedure cache)
Table Lock Escalations/Sec	The number of times that locks on a table were escalated
Target Server Memory (KB)	The total amount of dynamic memory the server can consume
Total Server Memory (KB)	The total amount of dynamic memory that the server is using
User Connections	The number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

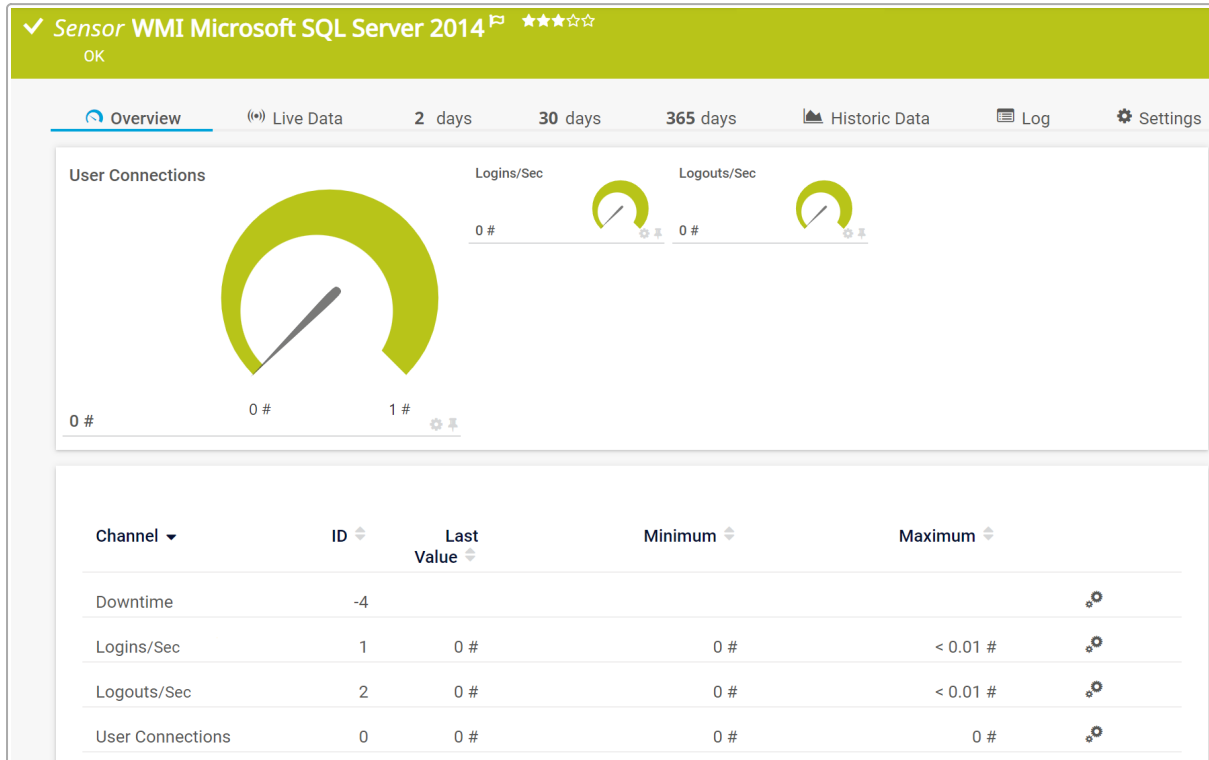
- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.297 WMI Microsoft SQL Server 2014 Sensor

The WMI Microsoft SQL Server 2014 sensor monitors the performance of a Microsoft SQL Server via Windows Management Instrumentation (WMI).



WMI Microsoft SQL Server 2014 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: WMI Microsoft SQL Server 2014
- French: Microsoft SQL serveur 2014 (WMI)
- German: WMI Microsoft SQL Server 2014
- Japanese: WMI Microsoft SQL Server 2014
- Portuguese: Microsoft SQL Server 2014 (WMI)
- Russian: WMI Microsoft SQL Server 2014
- Simplified Chinese: WMI Microsoft SQL Server 2014
- Spanish: Microsoft SQL Server 2014 (WMI)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
Target system	You can only add this sensor to a target system that runs a Microsoft SQL database.
IPv6	This sensor supports IPv6.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiqlserversensor
- wmiqlserversensor2014

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## SQL Server Settings

### SQL Server Settings

**Service** ⓘ *MSSQLSERVER*

**Name** ⓘ *SQL Server (MSSQLSERVER)*

**Naming Method** ⓘ  Automatically determine the WMI class name (default)  
 Manually enter the WMI class name

**Result Handling** ⓘ  Discard result (default)  
 Store result

SQL Server Settings

Setting	Description
Service	The service that this sensor monitors. ⓘ The service name is provided as returned by the SQL server.
Name	The name of the server instance that this sensor monitors. ⓘ The display name is provided as returned by the SQL server.
Naming Method	Select whether PRTG automatically selects the name of the WMI class used for monitoring: <ul style="list-style-type: none"> <li>▪ Automatically determine the WMI class name (default): Automatically select WMI class. We recommend this setting.</li> <li>▪ Manually enter the WMI class name: Manually enter a WMI class name. Select this option if your server instance returns an error code in automatic mode.</li> </ul>
WMI Class	<b>This setting is only visible if you select Manually enter the WMI class name above.</b>  Enter the WMI class name that the sensor uses to monitor the server instance.
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### SQL Counter Specific

**SQL Counter Specific** Performance Counters **i** *General Statistics*

SQL Counter Specific

Setting	Description
Performance Counters	<p>You see a list of different groups of performance counters that the sensor can monitor for the instances that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counters you select here.</p> <ul style="list-style-type: none"> <li>▪ <b>General Statistics:</b> Read general performance counters. This shows the number of user connections and the number of logins and logouts per second.</li> <li>▪ <b>Access Methods:</b> Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second).</li> <li>▪ <b>Buffer Manager:</b> Read buffer manager counters. This shows the buffer cache hit ratio in percent and the number of database pages and stolen pages.</li> <li>▪ <b>Memory Manager:</b> Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb).</li> <li>▪ <b>Locks:</b> Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time.</li> <li>▪ <b>SQL Statistics:</b> Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second).</li> </ul> <p>Depending on your selection, PRTG creates a sensor with the specified channels.</p> <p><b>i</b> To monitor more than one of the listed groups of performance counters, add the sensor several times for the respective instances.</p> <p><b>i</b> After sensor creation, this setting shows the performance counter that this sensor monitors.</p>



## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Average Wait Time	The average amount of wait time for each lock request that resulted in a wait
Batch Requests/Sec	The number of Transact-SQL command batches received. This statistic is affected by all constraints (such as input/output, number of users, cache size, or complexity of requests). High batch requests mean good throughput.
Buffer Cache Hit Ratio	<p>The percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little.</p> <p>Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.</p>
Connection Memory (KB)	The total amount of dynamic memory the server is using for maintaining connections
Database Pages	The number of pages in the buffer pool with database content
Number of Deadlocks/Sec	The number of lock requests that resulted in a deadlock
Full Scans/Sec	The number of unrestricted full scans. These can be either base-table or full-index scans.
Lock Requests/Sec	The number of new locks and lock conversions requested from the lock manager
Logins/Sec	The total number of logins started
Logouts/Sec	The total number of logout operations started
Optimizer Memory (KB)	The total amount of dynamic memory the server is using for query optimization
Page Life Expectancy	The number of seconds a page stays in the buffer pool without references
Page Splits/Sec	The number of page splits that occur as the result of overflowing index pages

Channel	Description
SQL Cache Memory (KB)	The total amount of dynamic memory the server is using for the dynamic SQL cache
SQL Compilations/Sec	The number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles because of recompiles. After the SQL Server user activity is stable, this value reaches a steady state.
SQL Recompilations/Sec	The number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.
Stolen Pages	The number of pages used for miscellaneous server purposes (including procedure cache)
Table Lock Escalations/Sec	The number of times that locks on a table were escalated
Target Server Memory (KB)	The total amount of dynamic memory the server can consume
Total Server Memory (KB)	The total amount of dynamic memory that the server is using
User Connections	The number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

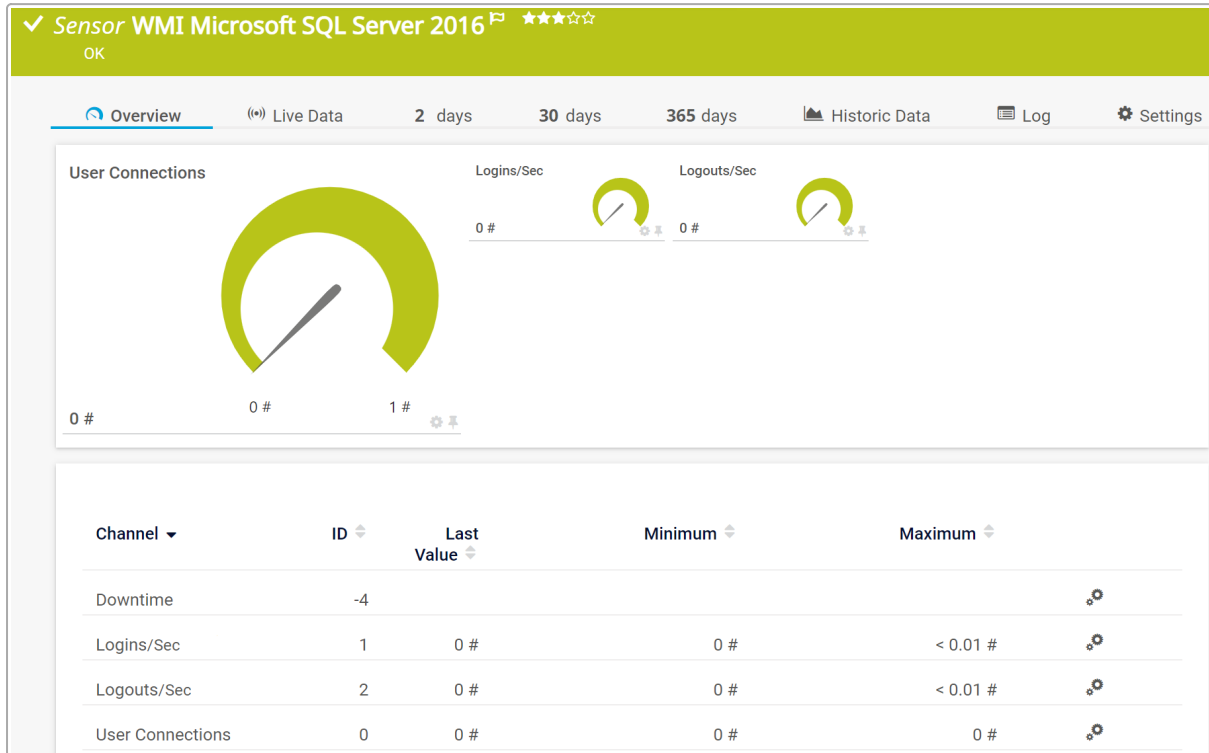
- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.298 WMI Microsoft SQL Server 2016 Sensor

The WMI Microsoft SQL Server 2016 sensor monitors the performance of a Microsoft SQL Server via Windows Management Instrumentation (WMI).



WMI Microsoft SQL Server 2016 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2587]</sup>.

### Sensor in Other Languages

- Dutch: WMI Microsoft SQL Server 2016
- French: Microsoft SQL serveur 2016 (WMI)
- German: WMI Microsoft SQL Server 2016
- Japanese: WMI Microsoft SQL Server 2016
- Portuguese: Microsoft SQL Server 2016 (WMI)
- Russian: WMI Microsoft SQL Server 2016
- Simplified Chinese: WMI Microsoft SQL Server 2016
- Spanish: Microsoft SQL Server 2016 (WMI)

### Remarks

Consider the following [remarks](#)<sup>[2582]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
Target system	You can only add this sensor to a target system that runs a Microsoft SQL database.
IPv6	This sensor supports IPv6.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiqlserversensor
- wmiqlserversensor2016

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## SQL Server Settings

**SQL Server Settings**

**Service** ⓘ *MSSQLSERVER*

**Name** ⓘ *SQL Server (MSSQLSERVER)*

**Naming Method** ⓘ  Automatically determine the WMI class name (default)  
 Manually enter the WMI class name

**Result Handling** ⓘ  Discard result (default)  
 Store result

SQL Server Settings

Setting	Description
Service	<p>The service that this sensor monitors.</p> <p> ⓘ The service name is provided as returned by the SQL server.</p> <p> ⓘ You cannot change this value after sensor creation.</p>
Name	<p>The name of the server instance that this sensor monitors.</p> <p> ⓘ The display name is provided as returned by the SQL server.</p>
Naming Method	<p>Select whether PRTG automatically selects the name of the WMI class used for monitoring:</p> <ul style="list-style-type: none"> <li>▪ Automatically determine the WMI class name (default): Automatically select WMI class. We recommend this setting.</li> <li>▪ Manually enter the WMI class name: Manually enter a WMI class name. Select this option if your server instance returns an error code in automatic mode.</li> </ul>
WMI Class	<p><b>This setting is only visible if you select</b> Manually enter the WMI class name <b>above</b>.</p> <p>Enter the WMI class name that the sensor uses to monitor the server instance.</p>
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ <b>Store result:</b> Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## SQL Counter Specific

SQL Counter Specific

Performance Counters i
General Statistics

SQL Counter Specific

Setting	Description
Performance Counters	<p>You see a list of different groups of performance counters that the sensor can monitor for the instances that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counters you select here.</p> <ul style="list-style-type: none"> <li>▪ <b>General Statistics:</b> Read general performance counters. This shows the number of user connections and the number of logins and logouts per second.</li> <li>▪ <b>Access Methods:</b> Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second).</li> <li>▪ <b>Buffer Manager:</b> Read buffer manager counters. This shows the buffer cache hit ratio in percent and the number of database pages and stolen pages.</li> <li>▪ <b>Memory Manager:</b> Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb).</li> <li>▪ <b>Locks:</b> Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time.</li> <li>▪ <b>SQL Statistics:</b> Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second).</li> </ul> <p>Depending on your selection, PRTG creates a sensor with the specified channels.</p> <p><b>i</b> To monitor more than one of the listed groups of performance counters, add the sensor several times for the respective instances.</p>

Setting	Description
	<p><b>i</b> After sensor creation, this setting shows the performance counter that this sensor monitors.</p>

## Sensor Display

**Sensor Display**

Primary Channel **ⓘ** Downtime

---

Graph Type **ⓘ**
 Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⚙</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click **🔒** under the corresponding setting name to disable the inheritance and to display its options.



■ For more information, see section [Inheritance of Settings](#).

## Channel List

❗ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Average Wait Time	The average amount of wait time for each lock request that resulted in a wait
Batch Requests/Sec	The number of Transact-SQL command batches received. This statistic is affected by all constraints (such as input/output, number of users, cache size, or complexity of requests). High batch requests mean good throughput.
Buffer Cache Hit Ratio	<p>The percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little.</p> <p>Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.</p>
Connection Memory (KB)	The total amount of dynamic memory the server is using for maintaining connections
Database Pages	The number of pages in the buffer pool with database content
Number of Deadlocks/Sec	The number of lock requests that resulted in a deadlock
Full Scans/Sec	The number of unrestricted full scans. These can be either base-table or full-index scans.
Lock Requests/Sec	The number of new locks and lock conversions requested from the lock manager
Logins/Sec	The total number of logins started
Logouts/Sec	The total number of logout operations started
Optimizer Memory (KB)	The total amount of dynamic memory the server is using for query optimization

Channel	Description
Page Life Expectancy	The number of seconds a page stays in the buffer pool without references
Page Splits/Sec	The number of page splits that occur as the result of overflowing index pages
SQL Cache Memory (KB)	The total amount of dynamic memory the server is using for the dynamic SQL cache
SQL Compilations/Sec	The number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles because of recompiles. After the SQL Server user activity is stable, this value reaches a steady state.
SQL Recompilations/Sec	The number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.
Stolen Pages	The number of pages used for miscellaneous server purposes (including procedure cache)
Table Lock Escalations/Sec	The number of times that locks on a table were escalated
Target Server Memory (KB)	The total amount of dynamic memory the server can consume
Total Server Memory (KB)	The total amount of dynamic memory that the server is using
User Connections	The number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

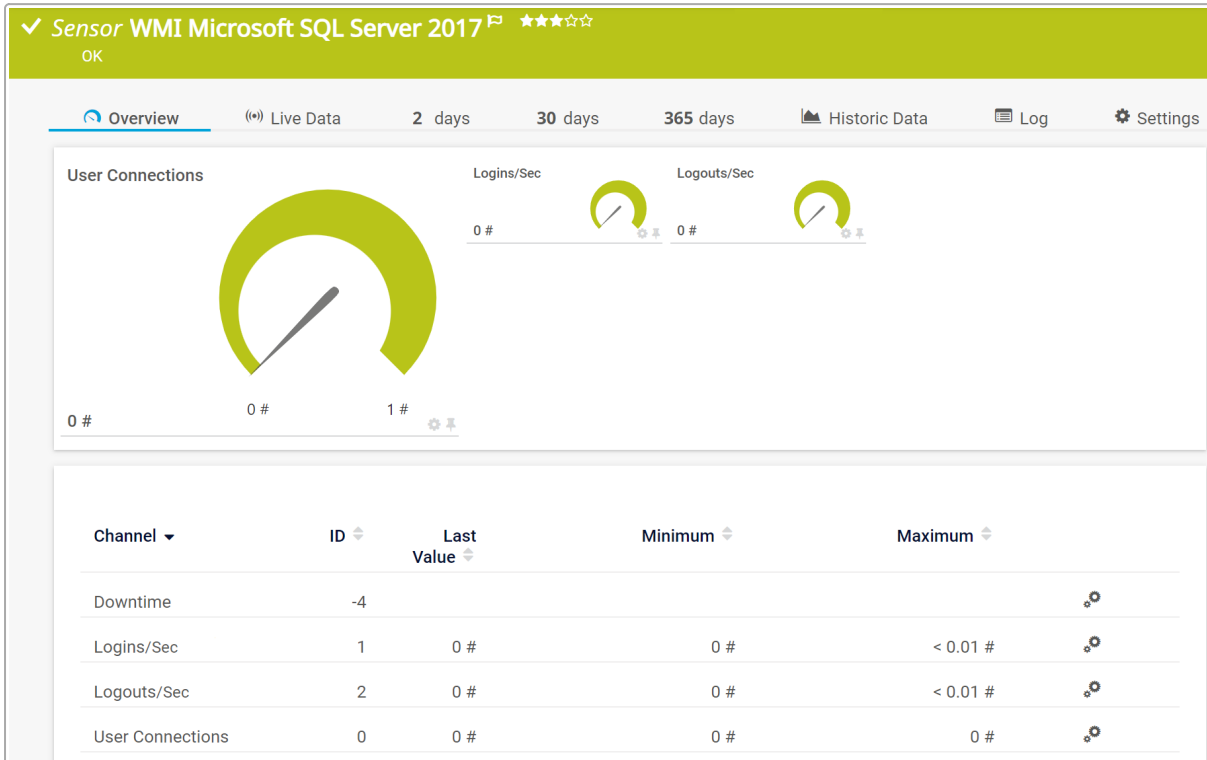
- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.299 WMI Microsoft SQL Server 2017 Sensor

The WMI Microsoft SQL Server 2017 sensor monitors the performance of a Microsoft SQL Server via Windows Management Instrumentation (WMI).



WMI Microsoft SQL Server 2017 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: WMI Microsoft SQL Server 2017
- French: Microsoft SQL serveur 2017 (WMI)
- German: WMI Microsoft SQL Server 2017
- Japanese: WMI Microsoft SQL Server 2017
- Portuguese: Microsoft SQL Server 2017 (WMI)
- Russian: WMI Microsoft SQL Server 2017
- Simplified Chinese: WMI Microsoft SQL Server 2017
- Spanish: Microsoft SQL Server 2017 (WMI)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
Target system	You can only add this sensor to a target system that runs a Microsoft SQL database.
IPv6	This sensor supports IPv6.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiqlserversensor
- wmiqlserversensor2017

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## SQL Server Settings

### SQL Server Settings

**Service** ⓘ *MSSQLSERVER*

**Name** ⓘ *SQL Server (MSSQLSERVER)*

**Naming Method** ⓘ  Automatically determine the WMI class name (default)  
 Manually enter the WMI class name

**Result Handling** ⓘ  Discard result (default)  
 Store result

SQL Server Settings

Setting	Description
Service	The service that this sensor monitors. ⓘ The service name is provided as returned by the SQL server.
Name	The name of the server instance that this sensor monitors. ⓘ The display name is provided as returned by the SQL server.
Naming Method	Select whether PRTG automatically selects the name of the WMI class used for monitoring: <ul style="list-style-type: none"> <li>▪ Automatically determine the WMI class name (default): Automatically select WMI class. We recommend this setting.</li> <li>▪ Manually enter the WMI class name: Manually enter a WMI class name. Select this option if your server instance returns an error code in automatic mode.</li> </ul>
WMI Class	<b>This setting is only visible if you select Manually enter the WMI class name above.</b>  Enter the WMI class name that the sensor uses to monitor the server instance.
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### SQL Counter Specific

**SQL Counter Specific** Performance Counters ⓘ General Statistics

SQL Counter Specific

Setting	Description
Performance Counters	<p>You see a list of different groups of performance counters that the sensor can monitor for the instances that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counters you select here.</p> <ul style="list-style-type: none"> <li>▪ <b>General Statistics:</b> Read general performance counters. This shows the number of user connections and the number of logins and logouts per second.</li> <li>▪ <b>Access Methods:</b> Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second).</li> <li>▪ <b>Buffer Manager:</b> Read buffer manager counters. This shows the buffer cache hit ratio in percent and the number of database pages and stolen pages.</li> <li>▪ <b>Memory Manager:</b> Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb).</li> <li>▪ <b>Locks:</b> Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time.</li> <li>▪ <b>SQL Statistics:</b> Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second).</li> </ul> <p>Depending on your selection, PRTG creates a sensor with the specified channels.</p> <p><b>i</b> To monitor more than one of the listed groups of performance counters, add the sensor several times for the respective instances.</p> <p><b>i</b> After sensor creation, this setting shows the performance counter that this sensor monitors.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Average Wait Time	The average amount of wait time for each lock request that resulted in a wait
Batch Requests/Sec	The number of Transact-SQL command batches received. This statistic is affected by all constraints (such as input/output, number of users, cache size, or complexity of requests). High batch requests mean good throughput.
Buffer Cache Hit Ratio	<p>The percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little.</p> <p>Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.</p>
Connection Memory (KB)	The total amount of dynamic memory the server is using for maintaining connections
Database Pages	The number of pages in the buffer pool with database content
Number of Deadlocks/Sec	The number of lock requests that resulted in a deadlock
Full Scans/Sec	The number of unrestricted full scans. These can be either base-table or full-index scans.
Lock Requests/Sec	The number of new locks and lock conversions requested from the lock manager
Logins/Sec	The total number of logins started
Logouts/Sec	The total number of logout operations started
Optimizer Memory (KB)	The total amount of dynamic memory the server is using for query optimization
Page Life Expectancy	The number of seconds a page stays in the buffer pool without references
Page Splits/Sec	The number of page splits that occur as the result of overflowing index pages



Channel	Description
SQL Cache Memory (KB)	The total amount of dynamic memory the server is using for the dynamic SQL cache
SQL Compilations/Sec	The number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles because of recompiles. After the SQL Server user activity is stable, this value reaches a steady state.
SQL Recompilations/Sec	The number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.
Stolen Pages	The number of pages used for miscellaneous server purposes (including procedure cache)
Table Lock Escalations/Sec	The number of times that locks on a table were escalated
Target Server Memory (KB)	The total amount of dynamic memory the server can consume
Total Server Memory (KB)	The total amount of dynamic memory that the server is using
User Connections	The number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

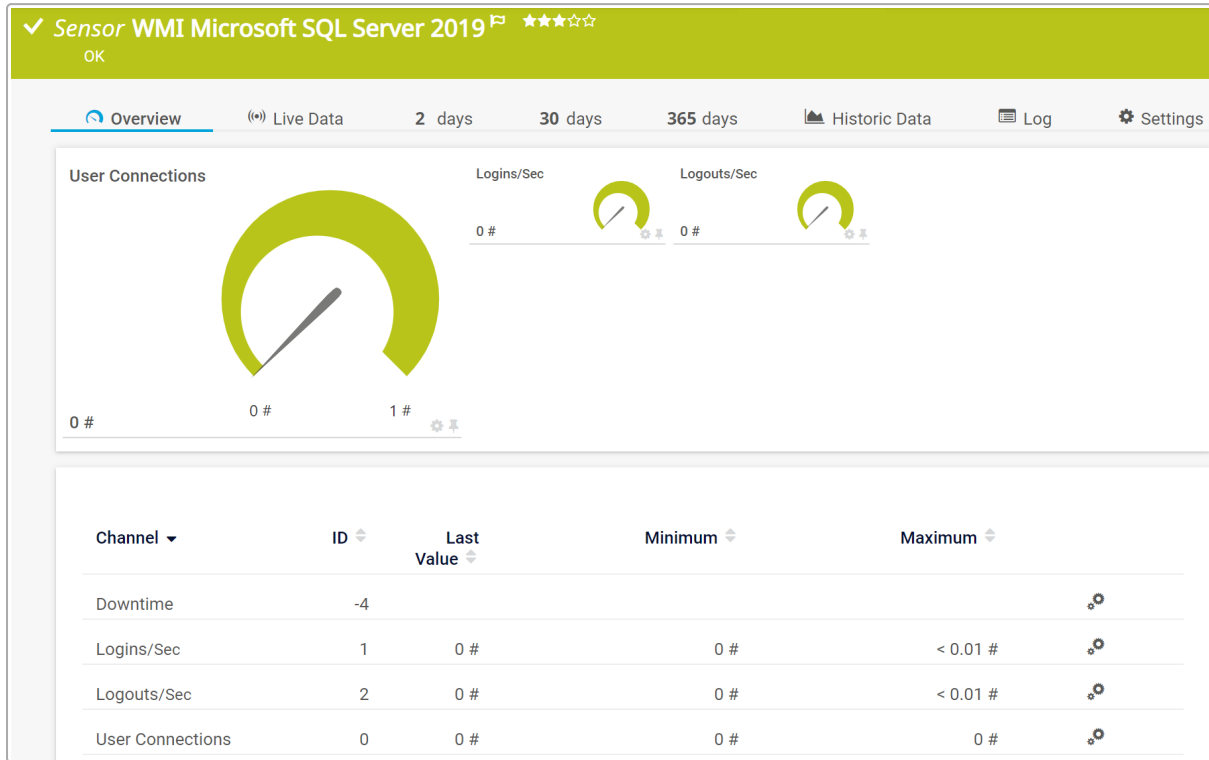
- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.300 WMI Microsoft SQL Server 2019 Sensor

The WMI Microsoft SQL Server 2019 sensor monitors the performance of a Microsoft SQL Server via Windows Management Instrumentation (WMI).



WMI Microsoft SQL Server 2019 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: WMI Microsoft SQL Server 2019
- French: Microsoft SQL serveur 2019 (WMI)
- German: WMI Microsoft SQL Server 2019
- Japanese: WMI Microsoft SQL Server 2019
- Portuguese: Microsoft SQL Server 2019 (WMI)
- Russian: WMI Microsoft SQL Server 2019
- Simplified Chinese: WMI Microsoft SQL Server 2019
- Spanish: Microsoft SQL Server 2019 (WMI)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
Target system	You can only add this sensor to a target system that runs a Microsoft SQL database.
IPv6	This sensor supports IPv6.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiqlserversensor
- wmiqlserversensor2019

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## SQL Server Settings

### SQL Server Settings

**Service** ⓘ *MSSQLSERVER*

**Name** ⓘ *SQL Server (MSSQLSERVER)*

**Naming Method** ⓘ  Automatically determine the WMI class name (default)  
 Manually enter the WMI class name

**Result Handling** ⓘ  Discard result (default)  
 Store result

SQL Server Settings

Setting	Description
Service	The service that this sensor monitors. ⓘ The service name is provided as returned by the SQL server.
Name	The name of the server instance that this sensor monitors. ⓘ The display name is provided as returned by the SQL server.
Naming Method	Select whether PRTG automatically selects the name of the WMI class used for monitoring: <ul style="list-style-type: none"> <li>▪ Automatically determine the WMI class name (default): Automatically select WMI class. We recommend this setting.</li> <li>▪ Manually enter the WMI class name: Manually enter a WMI class name. Select this option if your server instance returns an error code in automatic mode.</li> </ul>
WMI Class	<b>This setting is only visible if you select Manually enter the WMI class name above.</b>  Enter the WMI class name that the sensor uses to monitor the server instance.
Result Handling	Define what PRTG does with the sensor result: <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

### SQL Counter Specific

**SQL Counter Specific** Performance Counters **i** *General Statistics*

SQL Counter Specific

Setting	Description
Performance Counters	<p>You see a list of different groups of performance counters that the sensor can monitor for the instances that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counters you select here.</p> <ul style="list-style-type: none"> <li>▪ <b>General Statistics:</b> Read general performance counters. This shows the number of user connections and the number of logins and logouts per second.</li> <li>▪ <b>Access Methods:</b> Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second).</li> <li>▪ <b>Buffer Manager:</b> Read buffer manager counters. This shows the buffer cache hit ratio in percent and the number of database pages and stolen pages.</li> <li>▪ <b>Memory Manager:</b> Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb).</li> <li>▪ <b>Locks:</b> Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time.</li> <li>▪ <b>SQL Statistics:</b> Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second).</li> </ul> <p>Depending on your selection, PRTG creates a sensor with the specified channels.</p> <p><b>i</b> To monitor more than one of the listed groups of performance counters, add the sensor several times for the respective instances.</p> <p><b>i</b> After sensor creation, this setting shows the performance counter that this sensor monitors.</p>

## Sensor Display


**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Average Wait Time	The average amount of wait time for each lock request that resulted in a wait
Batch Requests/Sec	The number of Transact-SQL command batches received. This statistic is affected by all constraints (such as input/output, number of users, cache size, or complexity of requests). High batch requests mean good throughput.
Buffer Cache Hit Ratio	<p>The percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little.</p> <p>Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.</p>
Connection Memory (KB)	The total amount of dynamic memory the server is using for maintaining connections
Database Pages	The number of pages in the buffer pool with database content
Number of Deadlocks/Sec	The number of lock requests that resulted in a deadlock
Full Scans/Sec	The number of unrestricted full scans. These can be either base-table or full-index scans.
Lock Requests/Sec	The number of new locks and lock conversions requested from the lock manager
Logins/Sec	The total number of logins started
Logouts/Sec	The total number of logout operations started
Optimizer Memory (KB)	The total amount of dynamic memory the server is using for query optimization
Page Life Expectancy	The number of seconds a page stays in the buffer pool without references
Page Splits/Sec	The number of page splits that occur as the result of overflowing index pages

Channel	Description
SQL Cache Memory (KB)	The total amount of dynamic memory the server is using for the dynamic SQL cache
SQL Compilations/Sec	The number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles because of recompiles. After the SQL Server user activity is stable, this value reaches a steady state.
SQL Recompilations/Sec	The number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.
Stolen Pages	The number of pages used for miscellaneous server purposes (including procedure cache)
Table Lock Escalations/Sec	The number of times that locks on a table were escalated
Target Server Memory (KB)	The total amount of dynamic memory the server can consume
Total Server Memory (KB)	The total amount of dynamic memory that the server is using
User Connections	The number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

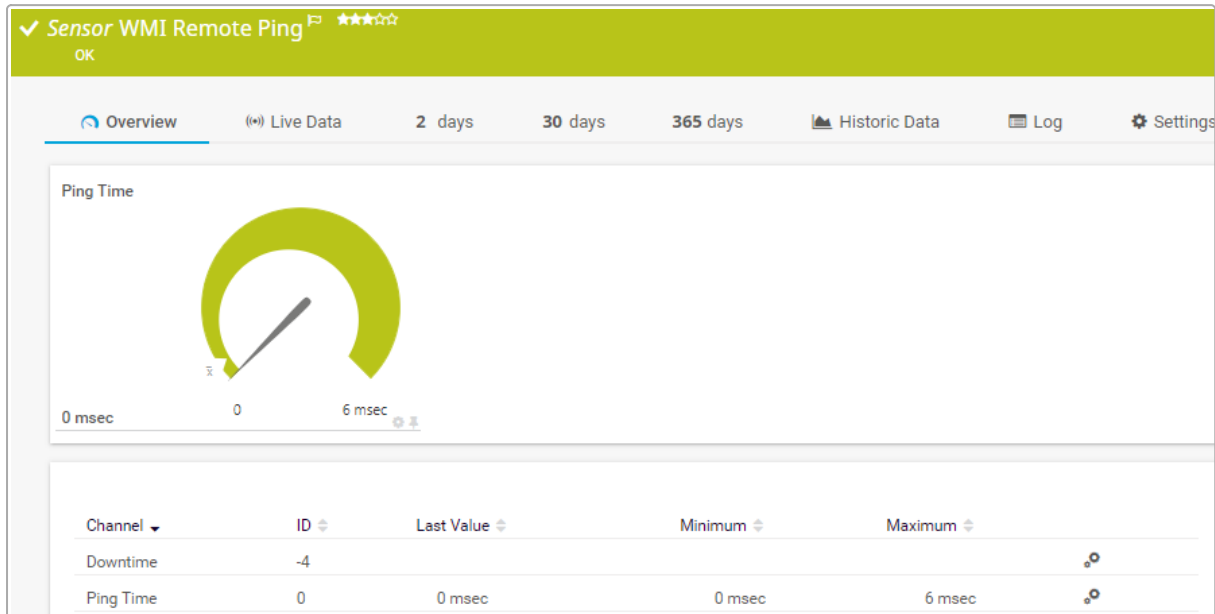
My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>



## 7.8.301 WMI Remote Ping Sensor

The WMI Remote Ping sensor remotely connects to a Windows system via Windows Management Instrumentation (WMI) and performs an Internet Control Message Protocol (ICMP) echo request ("ping") from this device to a specified target.



WMI Remote Ping Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: WMI Remote Ping
- French: Ping distant (WMI)
- German: WMI Remote Ping
- Japanese: WMI リモート Ping 実行
- Portuguese: Ping remoto (WMI)
- Russian: Удаленный пинг по WMI
- Simplified Chinese: WMI 远程 Ping
- Spanish: Ping remoto (WMI)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- pingsensor
- remotepingsensor
- wmisensor
- wmipingsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## WMI Remote Ping Configuration

### WMI Remote Ping Configuration

**Target** ⓘ 192.0.2.0

---

**Timeout (Sec.)** ⓘ 5

---

**Packet Size (Bytes)** ⓘ 32

---

WMI Remote Ping Configuration

Setting	Description
Target	Enter the Domain Name System (DNS) name or IP address of the target device that you want to ping. The sensor remotely connects to its parent device via WMI. Then it performs a ping request from this remote device to the target device or server. Enter a string.
Timeout (Sec.)	Enter a timeout in seconds for the ping. If the reply takes longer than this value, PRTG cancels the request and shows an error message. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).
Packet Size (Bytes)	Enter the packet size for the ping in bytes. You can enter any value between <b>1</b> and <b>10000</b> . Enter an integer.  ⓘ We recommend that you use the default value.

## Debug Options

### Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul>

Setting	Description
	<p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**
 Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⚙</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click **🔒** under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Ping Time	The ping time from the remote device to the target device ⓘ This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

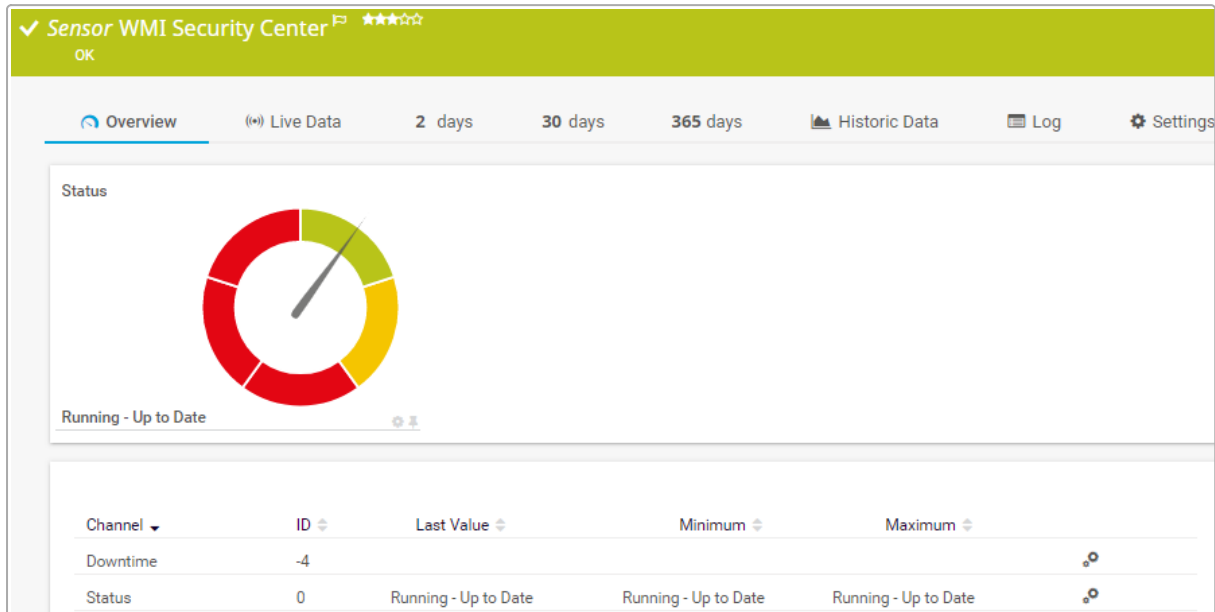
- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.302 WMI Security Center Sensor

The WMI Security Center sensor monitors the security status of a Windows client system via Windows Management Instrumentation (WMI). It can monitor all security products that are controlled by Windows Security Center / Windows Action Center.



WMI Security Center Sensor



For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: WMI Security Center
- French: Centre de sécurité (WMI)
- German: WMI Sicherheits-Center
- Japanese: WMI セキュリティーセンター
- Portuguese: Centro de segurança (WMI)
- Russian: Центр безопасности WMI
- Simplified Chinese: WMI 安全中心
- Spanish: Centro de seguridad (WMI)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Windows version	This sensor requires at least Windows Vista on the target system.  This sensor does not run on Windows Server operating systems because the Windows Security Center / Windows Action Center is only available on client Windows versions.
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Add Sensor

### WMI Security Center Specific

Setting	Description
Security Center Product	Select the security center products that you want to monitor. PRTG creates one sensor for each product that you select.  You see a list showing the Name and Type of all security products that the sensor finds in the Windows Security Center on the target device. If there are no products, you see a corresponding message.

## Basic Sensor Settings

Basic Sensor Settings

Sensor Name ⓘ Example Name

---

Tags ⓘ exampletag ✕ +

---

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- WMI Security Center

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## WMI Security Center Specific

WMI Security Center Specific

Display Name ⓘ *Windows Defender*

---

Type ⓘ *Antivirus*

WMI Security Center Specific

Setting	Description
Display Name	The display name of the security center product that this sensor monitors.
Type	The type of the security center product that this sensor monitors.

## Debug Options

Debug Options

Result Handling ⓘ

Discard result (default)

Store result

Debug Options



Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Status	<p>The status code of the security product</p> <ul style="list-style-type: none"> <li>▪ Up status: Running - Up To Date (status code 4)</li> <li>▪ Warning status: Running - Out Of Date (status code 2)</li> <li>▪ Down status: Not Running - Out Of Date (status code 1), Not Running - Up To Date (status code 3), Unknown (status code 0)</li> </ul> <p> This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

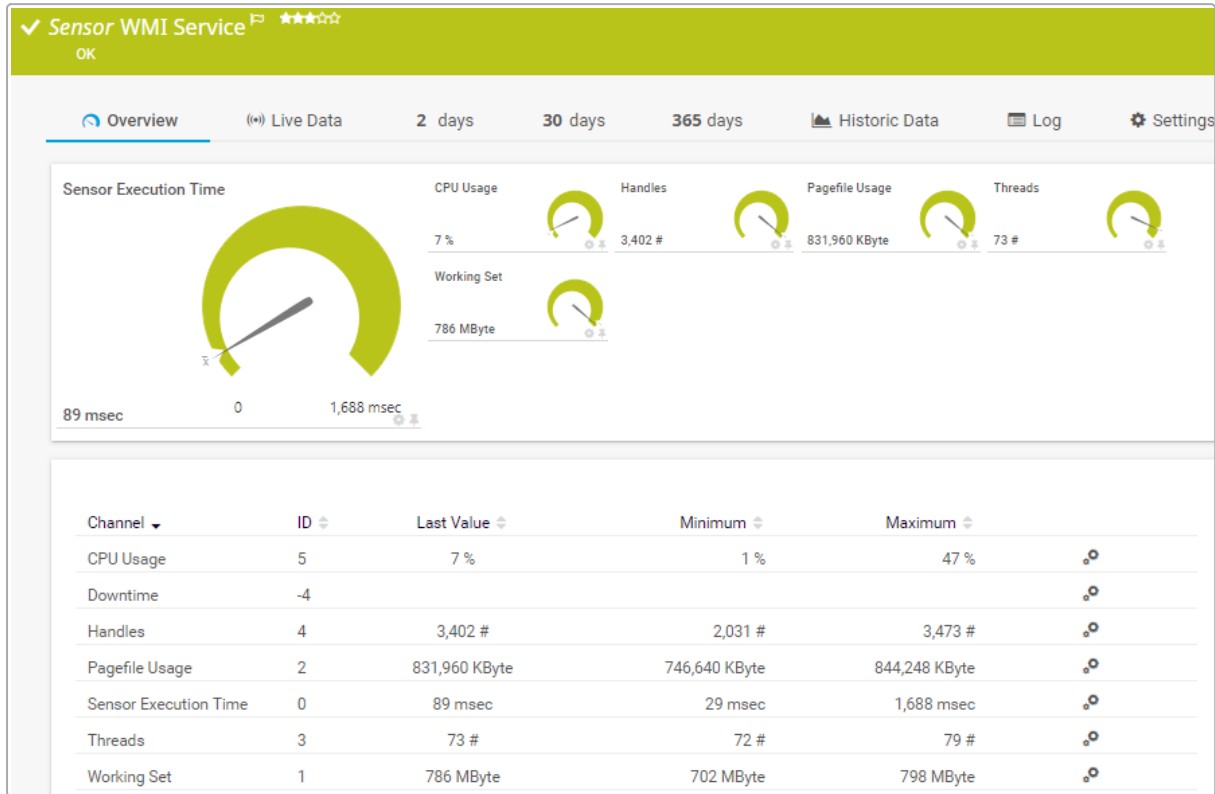
My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.303 WMI Service Sensor

The WMI Service sensor monitors a Windows service via Windows Management Instrumentation (WMI).

**i** After creation, the sensor shows the Down [status](#) if the service does not run.



WMI Service Sensor


■ For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2617]</sup>.

### Sensor in Other Languages

- Dutch: WMI Service
- French: Service (WMI)
- German: WMI Dienst
- Japanese: WMI サービス
- Portuguese: Serviço (WMI)
- Russian: Служба WMI
- Simplified Chinese: WMI 服务
- Spanish: Servicio (WMI)

### Remarks

Consider the following [remarks](#)<sup>[2613]</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Add Sensor dialog	The name and description of the service in the Add Sensor dialog appear in the language of the device's Windows installation.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- servicesensor
- wmiservicesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>[667]</sup>.

## WMI Service Monitor

**WMI Service Monitor**

If Service is Not Running <sup>ⓘ</sup>  Start/Restart service (default)  
 Do not start/restart service

Extended Monitoring <sup>ⓘ</sup>  Only check if the service is running (default)  
 Monitor other performance counters

Service <sup>ⓘ</sup> *Print Spooler*

Description <sup>ⓘ</sup> *This service spools print jobs and handles interaction with the printer. If you turn off this service, you won't be able to print or see your printers.*

Result Handling <sup>ⓘ</sup>  Discard result (default)  
 Store result

WMI Service Monitor

Setting	Description
If Service is Not Running	<p>Select whether you want PRTG to start or restart the service if it is stopped or paused:</p> <ul style="list-style-type: none"> <li>▪ Start/Restart service (default): PRTG tries to start the service if it is not running when the device is scanned. In combination with a <a href="#">change trigger</a>, you can use this mechanism to <a href="#">trigger a notification</a> whenever PRTG (re)starts the service.</li> <li>▪ Do not start/restart service: PRTG does not automatically start any service on the device.</li> </ul> <p><sup>ⓘ</sup> If you select the Start/Restart service (default) option and the sensor detects that the service does not run, PRTG tries to restart the service during this scan and postpones the next sensor scan for one interval. With the following scan, the sensor checks if the service runs now. If starting the service was not successful or if the service fails again, the sensor shows the Down status and does not try to start the service again. If the service runs after a (re)start attempt, the sensor continues monitoring as usual.</p>
If Service is Restarted	<p><b>This setting is only visible if you select Start/Restart service (default) above.</b></p> <p>Define what the sensor does if PRTG restarts the service:</p> <ul style="list-style-type: none"> <li>▪ Ignore (default): Do nothing.</li> <li>▪ Trigger 'change' notification: Send an internal message that indicates a change.</li> </ul> <p><sup>ⓘ</sup> In combination with a <a href="#">change trigger</a>, you can use this to <a href="#">trigger a notification</a> if a change occurs.</p>
Extended Monitoring	<p>Select whether you want to monitor CPU usage and other performance counters:</p>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Only check if the service is running (default): PRTG only monitors the channel Sensor Execution Time.</li> <li>▪ Monitor other performance counters: PRTG also monitors other performance counters.</li> </ul> <p><b>i</b> Extended monitoring might cause a <a href="#">class not found</a> error on some Windows systems.</p>
Service	The Windows service that this sensor monitors.
Description	The description of the Windows service that this sensor monitors.
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last result of the requested data in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID]-A.txt, and Result of Sensor [ID].Data.txt. This setting is for debugging purposes, especially in combination with content checks. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **ⓘ** Downtime

---


Graph Type **ⓘ** 
 Show channels independently (default)
   
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⚑</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	Define how this sensor shows different channels:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.                             <ul style="list-style-type: none"> <li>❗ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

❗ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
CPU Usage	<p>The CPU usage</p> <p>❗ Enable Monitor other performance counters in the sensor settings to show this parameter.</p>
Downtime	<p>In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status</p>
Handles	<p>The number of handles</p> <p>❗ Enable Monitor other performance counters in the sensor settings to show this parameter.</p>

Channel	Description
Pagefile Usage	The pagefile usage ⓘ Enable Monitor other performance counters in the sensor settings to show this parameter.
Sensor Execution Time	The execution time of the monitoring request ⓘ This channel is the primary channel by default.
Threads	The number of threads ⓘ Enable Monitor other performance counters in the sensor settings to show this parameter.
Working Set	The working set ⓘ Enable Monitor other performance counters in the sensor settings to show this parameter.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

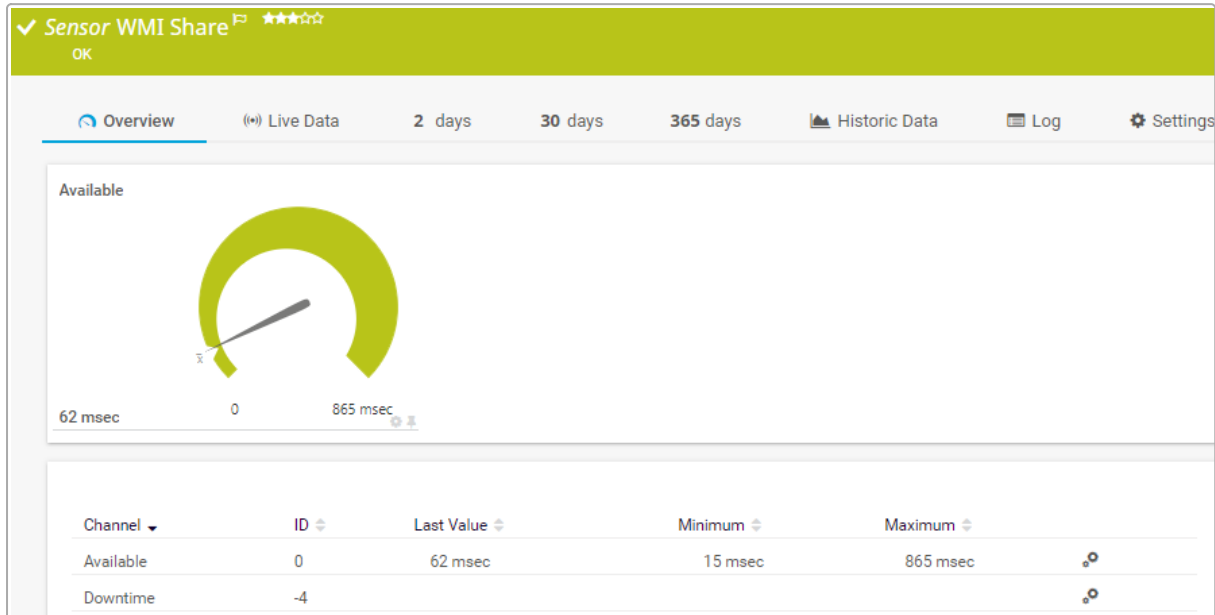
- <https://kb.paessler.com/en/topic/1043>



## 7.8.304 WMI Share Sensor

The WMI Share sensor monitors a shared resource on a Windows system via Windows Management Instrumentation (WMI).

**i** You can set the sensor to the Down [status](#) for different share status messages.



WMI Share Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: WMI Share
- French: Partage (WMI)
- German: WMI Freigabe
- Japanese: WMI 共有
- Portuguese: Compartilhamento (WMI)
- Russian: Pecыc WMI
- Simplified Chinese: WMI 共享
- Spanish: Recurso compartido (WMI)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
LanmanServer service	To provide any shares, the <a href="#">LanmanServer</a> "Server" Windows service must run on the target system. If it does not run, there are no shares and you see a <a href="#">No Share available</a> message.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmisharesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## WMI Shared Resource

**WMI Shared Resource**

Shared Resource ⓘ *Transfer*

Description ⓘ

Type ⓘ *Disk Drive*

TypeID ⓘ *0*

WMI Shared Resource

Setting	Description
Shared Resource	Information about the shared resource that this sensor monitors.
Description	The description of the shared resource that this sensor monitors.
Type	The type of the shared resource that this sensor monitors.
TypeID	The typeID of the shared resource that this sensor monitors.

### Trigger Down Status on Following Conditions

Select under which conditions the sensor shows the Down status. As long as the share returns **OK**, the sensor status shows the Up status. Enable the check box in front of the respective line to select a Down condition. Select none, one, or several of the following conditions.

ⓘ If the sensor is in the Down status, it does not record any data in any of its channels.

### Trigger Down Status on Following Conditions

- Error <sup>?</sup>  Alert on this condition <sup>?</sup>
- Degraded <sup>?</sup>  Alert on this condition <sup>?</sup>
- Unknown <sup>?</sup>  Alert on this condition <sup>?</sup>
- Pred Fail <sup>?</sup>  Alert on this condition <sup>?</sup>
- Starting <sup>?</sup>  Alert on this condition <sup>?</sup>
- Stopping <sup>?</sup>  Alert on this condition <sup>?</sup>
- Service <sup>?</sup>  Alert on this condition <sup>?</sup>
- Stressed <sup>?</sup>  Alert on this condition <sup>?</sup>
- Nonrecover <sup>?</sup>  Alert on this condition <sup>?</sup>
- NoContact <sup>?</sup>  Alert on this condition <sup>?</sup>
- LostComm <sup>?</sup>  Alert on this condition <sup>?</sup>

Trigger Down Status on Following Conditions

Condition	Description
Error	Set the sensor to the Down status if the share returns an <b>error</b> status. A share in this status is not operational.  <sup>?</sup> This condition is enabled by default.
Degraded	Set the sensor to the Down status if the share returns a <b>degraded</b> status. A share in this status is still operational.  <sup>?</sup> This condition is enabled by default.
Unknown	Set the sensor to the Down status if the share returns an <b>unknown</b> status.

Condition	Description
Pred Fail	<p>Set the sensor to the Down status if the share returns a <b>predicted fail</b> status. This indicates that an element works properly but predicts a failure (for example, a SMART-enabled hard drive). A share in this status is still operational.</p> <p><b>i</b> This condition is enabled by default.</p>
Starting	<p>Set the sensor to the Down status if the share returns a <b>starting</b> status. A share in this status is not operational.</p>
Stopping	<p>Set the sensor to the Down status if the share returns a <b>stopping</b> status. A share in this status is not operational.</p>
Service	<p>Set the sensor to the Down status if the share returns a <b>service</b> status. This can apply during disk mirror-resilvering, reloading a user permissions list, or other administrative work on the device that this sensor monitors. Not all such work is done online, but the managed element is neither OK nor has one of the other states. A share in this status is not operational.</p>
Stressed	<p>Set the sensor to the Down status if the share returns a <b>stressed</b> status.</p>
Nonrecover	<p>Set the sensor to the Down status if the share returns a <b>non recover</b> status.</p> <p><b>i</b> This condition is enabled by default.</p>
NoContact	<p>Set the sensor to the Down status if the share returns a <b>no contact</b> status.</p> <p><b>i</b> This condition is enabled by default.</p>
LostComm	<p>Set the sensor to the Down status if the share returns a <b>lost communication</b> status.</p> <p><b>i</b> This condition is enabled by default.</p>

## Debug Options

**Debug Options**

**Result Handling** **i**
 Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⚙</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Available	The availability of the share  This channel is the primary channel by default.
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

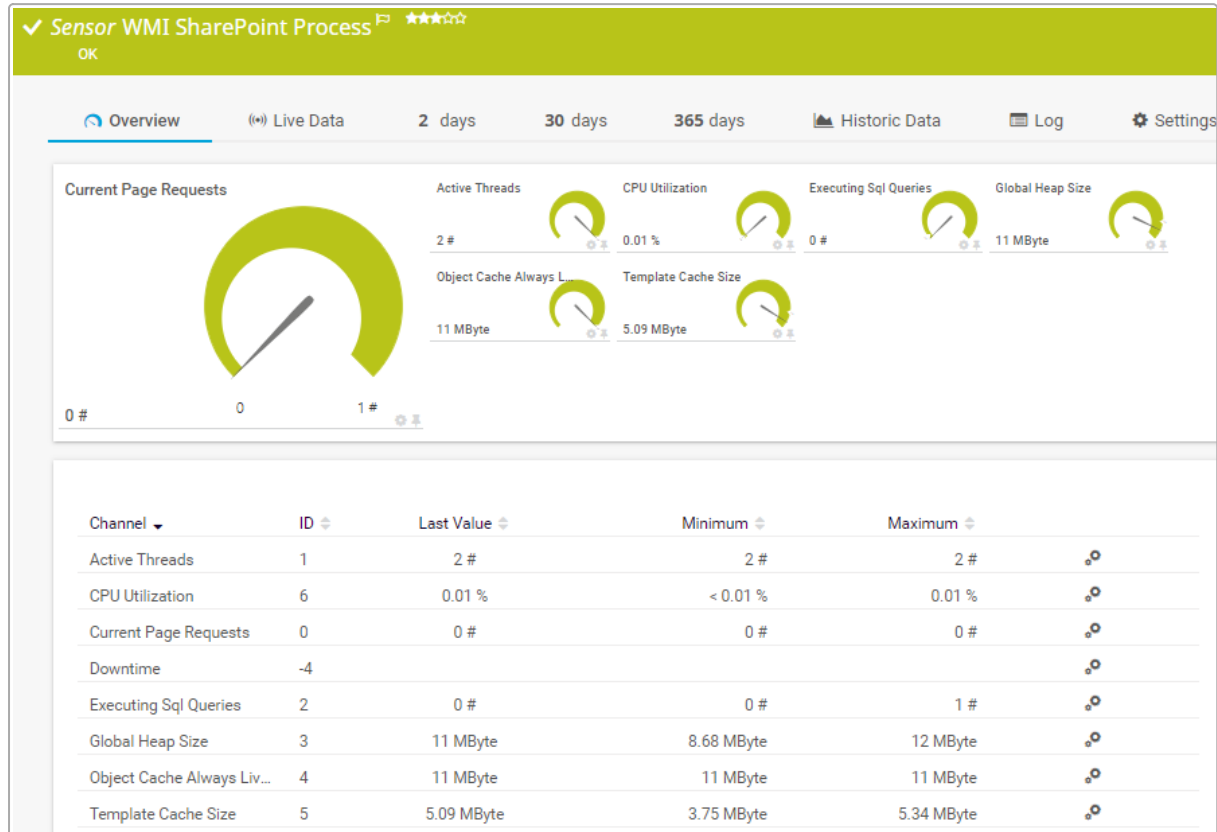
- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.305 WMI SharePoint Process Sensor

The WMI SharePoint Process sensor monitors a Microsoft SharePoint server via Windows Management Instrumentation (WMI).



WMI SharePoint Process Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).


### Sensor in Other Languages

- Dutch: WMI SharePoint Proces
- French: SharePoint processus (WMI)
- German: WMI SharePoint-Prozess
- Japanese: WMI SharePoint プロセス
- Portuguese: Processo SharePoint (WMI)
- Russian: Процесс SharePoint WMI
- Simplified Chinese: WMI SharePoint 进程
- Spanish: Proceso SharePoint (WMI)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:



Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

Basic Sensor Settings

Sensor Name ⓘ Example Name

---

Tags ⓘ  ✕ +

---

Priority ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiprocesssensor
- wmiendpointprocesssensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### WMI Process Monitor

WMI Process Monitor

SharePoint Process ⓘ *\_Total*

WMI Process Monitor

Setting	Description
SharePoint Process	The name of the SharePoint process that this sensor monitors.

## Debug Options

**Debug Options**

**Result Handling** ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**


**Primary Channel** ⓘ Downtime  


---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>


Setting	Description
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>Show channels independently (default): Show a graph for each channel.</li> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> <li> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</li> </ul> </li> </ul>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Active Threads	The number of active threads
CPU Utilization	The CPU usage
Current Page Requests	<p>The number of current page requests</p> <p> This channel is the primary channel by default.</p>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status

Channel	Description
Executing SQL Queries	The number of SQL queries being executed
Global Heap Size	The global heap size
Object Cache Always Live Size	The object cache always live size
Template Cache Size	The template cache size

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

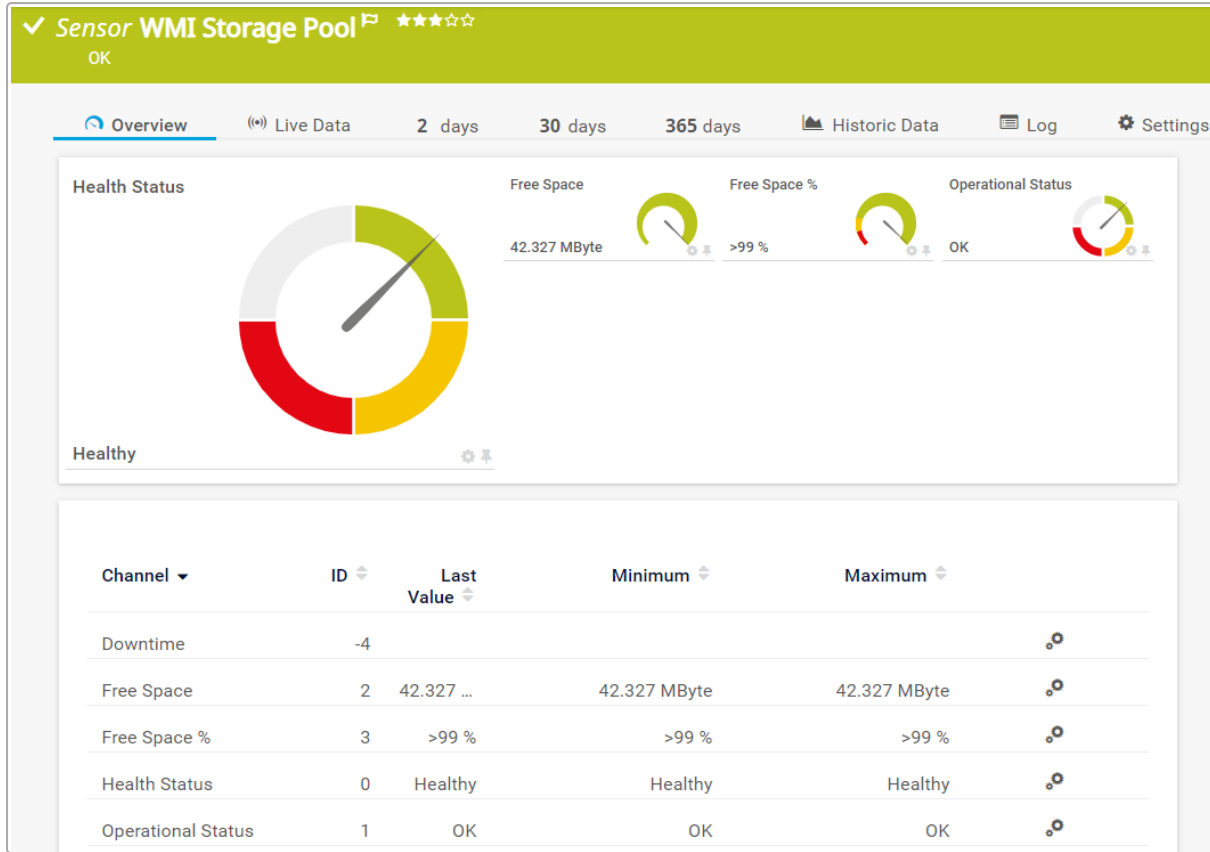
- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.306 WMI Storage Pool Sensor

The WMI Storage Pool sensor monitors a storage pool via Windows Management Instrumentation (WMI).



WMI Storage Pool Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: WMI opslagpool
- French: Pool de stockage (WMI)
- German: WMI Speicherpool
- Japanese: WMI ストレージプール
- Portuguese: Pool de armazenamento (WMI)
- Russian: Пул хранения WMI
- Simplified Chinese: WMI 存储池
- Spanish: Grupo de almacenamiento (WMI)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
Windows version	This sensor supports Windows versions as of Windows 10 or Windows Server 2016 on the target system.
IPv6	This sensor supports IPv6.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- storagepoolsensor
- wmistoragepoolsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### WMI Storage Pool Specific

**WMI Storage Pool Specific**

Friendly Name ⓘ *Storage Pool*

Timeout (Sec.) ⓘ

WMI Storage Pool Specific

Setting	Description
Friendly Name	The user-friendly name for the storage pool that this sensor monitors.
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>900</b> seconds (15 minutes).</p> <p> ⓘ If the reply takes longer than this value, the sensor cancels the request and shows a corresponding error message.</p>

### Debug Options

**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime


---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.



Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Space	The free space
Free Space %	<p>The free space (%)</p> <p><b>i</b> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: 10%</li> <li>▪ Lower warning limit: 20%</li> </ul>
Health Status	<p>The health status</p> <ul style="list-style-type: none"> <li>▪ Up status: Healthy</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Unhealthy</li> <li>▪ Unknown status: Unknown</li> </ul> <p><b>i</b> This channel is the primary channel by default.</p>
Operational Status	<p>The operational status</p> <ul style="list-style-type: none"> <li>▪ Up status: OK</li> <li>▪ Warning status: Warning</li> <li>▪ Down status: Error</li> <li>▪ Unknown status: Starting</li> </ul>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

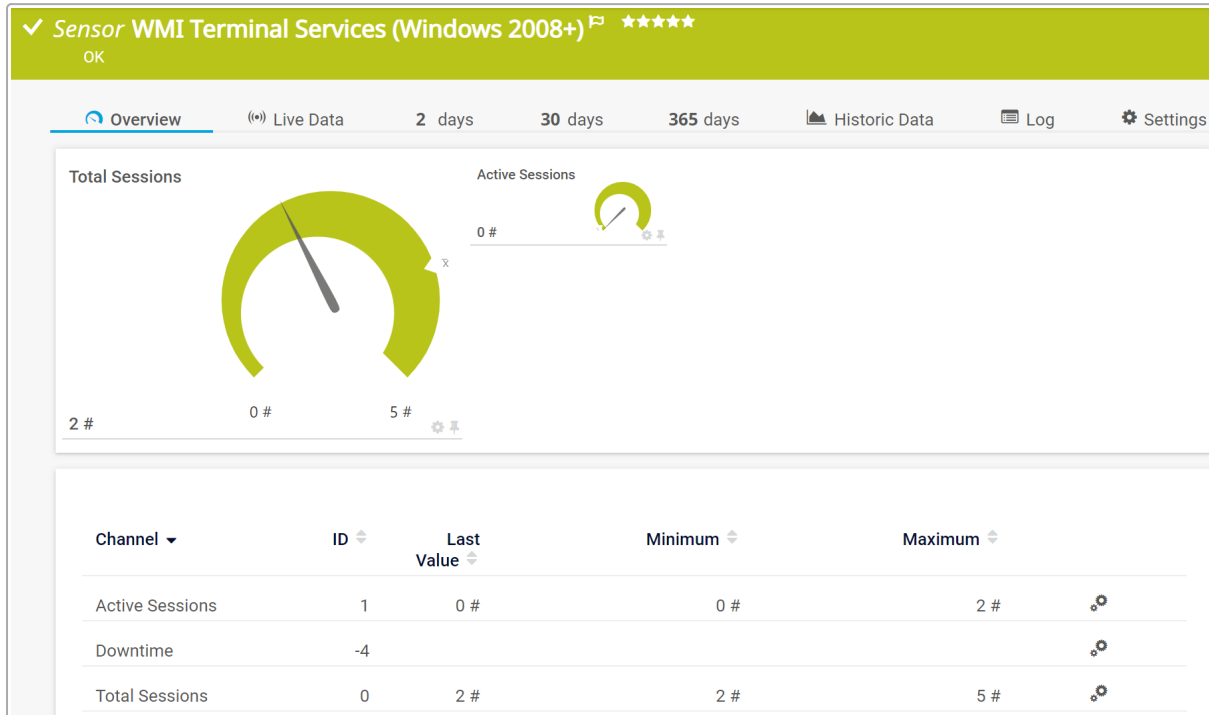
My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.307 WMI Terminal Services (Windows 2008+) Sensor

The WMI Terminal Services (Windows 2008+) sensor monitors the number of sessions on a Windows Terminal Services (Remote Desktop Services) server via Windows Management Instrumentation (WMI).

**i** The sensor supports Windows 2008 R2 and later.



WMI Terminal Services (Windows 2008+) Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: WMI Terminal Services (Windows 2008+)
- French: Windows (2008+) Terminal Services (WMI)
- German: WMI Terminaldienste (Windows 2008+)
- Japanese: WMI ターミナルサービス (Windows 2008 以降)
- Portuguese: Serviços de terminal (Windows 2008+) (WMI)
- Russian: WMI служб терминалов (Windows 2008 и последующая)
- Simplified Chinese: WMI 终端服务 (Windows 2008+)
- Spanish: Terminal Services (Windows 2008+) (WMI)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiterminalservicessensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Debug Options

#### Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.



## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Active Sessions	The number of active sessions: sessions with a logged in user, including used published applications
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Total Sessions	<p>The total number of sessions (including inactive sessions): inactive sessions can be sessions with a disconnected user that has not logged out or system services using a session</p> <p> For the Total Sessions channel, the sensor returns the number of active and inactive sessions, plus two additional sessions: one for the console, and one for the services. So, the number of total sessions might actually be higher than expected.</p> <p> This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

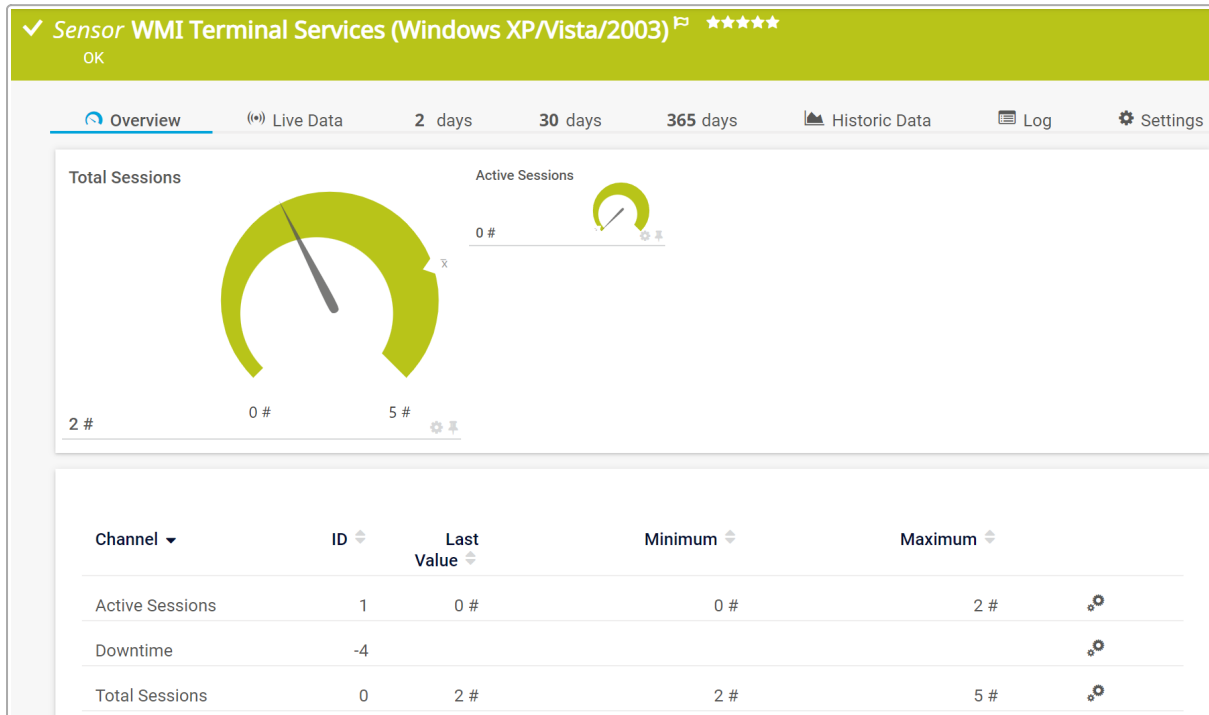
My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.308 WMI Terminal Services (Windows XP/Vista/2003) Sensor

The WMI Terminal Services (Windows XP/Vista/2003) sensor monitors the number of sessions on a Windows Terminal Services (Remote Desktop Services) server via Windows Management Instrumentation (WMI).

**i** The sensor supports Windows XP, Vista, or 2003.



WMI Terminal Services (Windows XP/Vista/2003) Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: WMI Terminal Services (Windows XP/Vista/2003)
- French: Windows (XP/Vista/2003) Terminal Services (WMI)
- German: WMI Terminaldienste (Windows XP/Vista/2003)
- Japanese: WMI ターミナルサービス (Windows XP/Vista/2003)
- Portuguese: Serviços de terminal (Windows XP/Vista/2003) (WMI)
- Russian: WMI служб терминалов (Windows XP/Vista/2003)
- Simplified Chinese: WMI 终端服务 (Windows XP/Vista/2003)
- Spanish: Terminal Services (Windows XP/Vista/2003) (WMI)

### Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmiterminalservicessensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Debug Options

#### Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options



Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>+</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.



## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Active Sessions	The number of active sessions: sessions with a logged in user, including used published applications
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Total Sessions	<p>The total number of sessions (including inactive sessions): inactive sessions can be sessions with a disconnected user that has not logged out or system services using a session</p> <p> For the Total Sessions channel, the sensor returns the number of active and inactive sessions, plus two additional sessions: one for the console, and one for the services. So, the number of total sessions might actually be higher than expected.</p> <p> This channel is the primary channel by default.</p>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

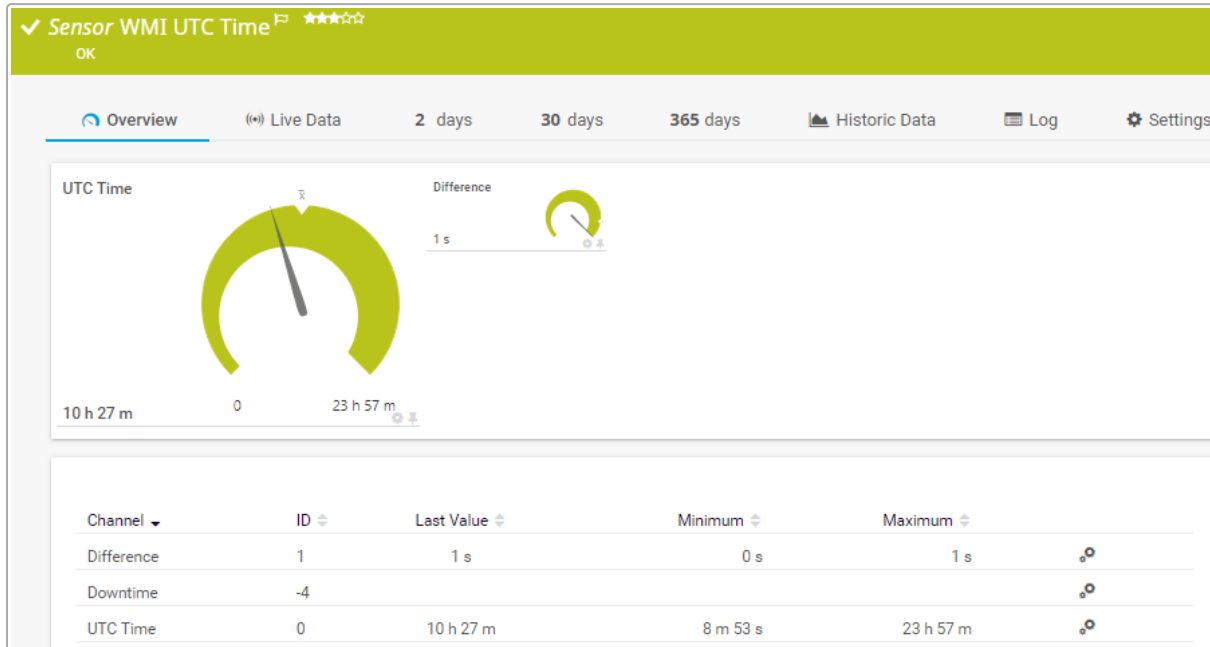
- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.309 WMI UTC Time Sensor

The WMI UTC Time sensor monitors the Coordinated Universal Time (UTC) time of a target device via Windows Management Instrumentation (WMI).



WMI UTC Time Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>[2649]</sup>.

### Sensor in Other Languages

- Dutch: WMI UTC Tijd
- French: Heure UTC (WMI)
- German: WMI UTC-Zeit
- Japanese: WMI UTC 時間
- Portuguese: Tempo UTC (WMI)
- Russian: Время WMI UTC
- Simplified Chinese: WMI UTC 时间
- Spanish: Tiempo UTC (WMI)

### Remarks

Consider the following [remarks](#)<sup>[2646]</sup> and requirements for this sensor:

Remark	Description
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv4	This sensor only supports IPv4.
Performance impact	This sensor has a <b>low</b> performance impact.
Hosted probe	☁ You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

### Basic Sensor Settings

#### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ ⊕

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following **default tags** that are automatically predefined in the sensor's settings when you add the sensor:

- wmiutctimesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

### Debug Options

#### Debug Options

**Result Handling** ⓘ

Discard result (default)

Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.


## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Difference	The time difference between the PRTG core server system time and the target device
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
UTC Time	The UTC time of the target device  This channel is the primary channel by default.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

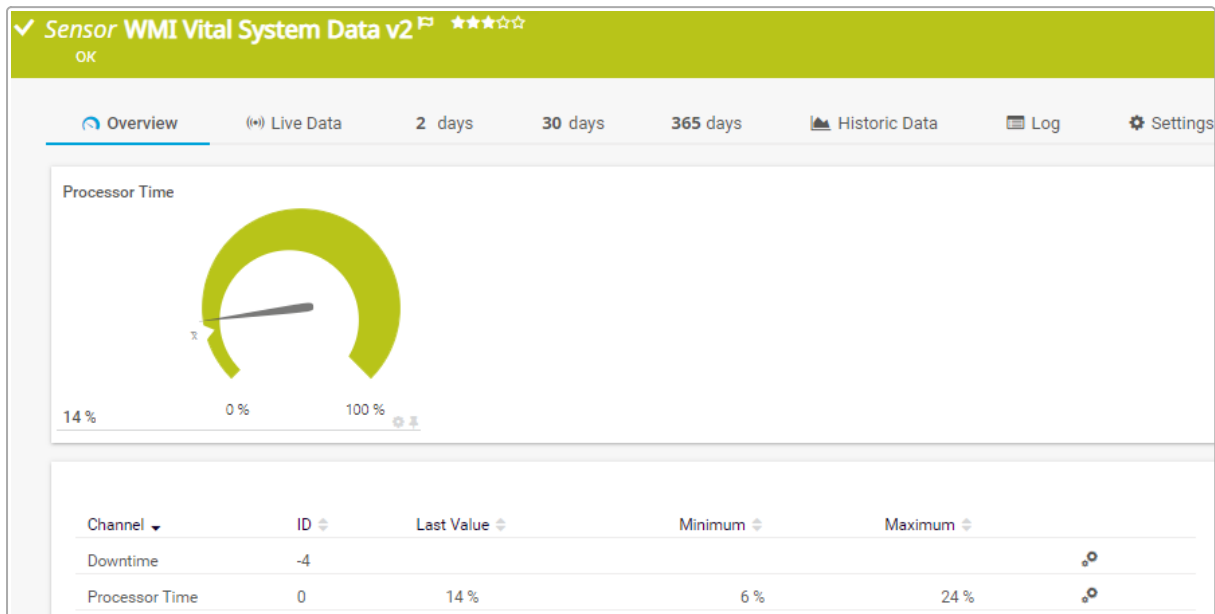
My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.310 WMI Vital System Data v2 Sensor

The WMI Vital System Data v2 sensor monitors vital system parameters via Windows Management Instrumentation (WMI).

**i** The sensor can monitor CPU, thread, memory, network, or pagefile, for example.



WMI Vital System Data v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#)<sup>2654</sup>.


### Sensor in Other Languages

- Dutch: WMI Vitale Systeem Gegevens V2
- French: Données système vitales v2 (WMI)
- German: WMI Wichtige Systemdaten v2
- Japanese: WMI バイタルシステムデータ (V2)
- Portuguese: Dados vitais do sistema (WMI) v2
- Russian: Важные системные данные WMI v2
- Simplified Chinese: WMI 关键系统数据 v2
- Spanish: Datos vitales de sistema (WMI) v2

### Remarks

Consider the following [remarks](#)<sup>2650</sup> and requirements for this sensor:



Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
IPv6	This sensor supports IPv6.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Add Sensor

Setting	Description
Performance Counter	<p>Select the performance counters that you want to monitor. PRTG creates one sensor for each counter that you select.</p> <p>You see a list of available vital system data values the sensor can monitor on the target device. The available options depend on your configuration. PRTG shows all possible performance counters with the name and instance description (if available).</p> <p>Choose from the following counters:</p> <ul style="list-style-type: none"> <li>▪ CPU</li> <li>▪ Thread</li> <li>▪ Memory</li> <li>▪ Network</li> <li>▪ Pagefile</li> </ul>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★★☆☆☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- wmvitalsystemdatasensor

■ For more information about basic sensor settings, see section [Sensor Settings](#) <sup>667</sup>.

## Vital System Data Readings Accessible Using WMI

### Vital System Data Readings Accessible Using WMI

**Display Name** ⓘ CPU: Percent User Time

**Instance** ⓘ \_Total

**WMI Class** ⓘ Win32\_PerfRawData\_PerfOS\_Processor

**Counter** ⓘ PercentUserTime

**Time Stamp** ⓘ Timestamp\_Sys100NS

**Time Frequency** ⓘ

**Counter Type** ⓘ PERF\_100NSEC\_TIMER

**Result Handling** ⓘ  Discard result (default)  
 Store result

Vital System Data Readings Accessible Using WMI

Setting	Description
Display Name	The display name that the sensor uses to query data from the target device.
Instance	The instance that the sensor uses to query data from the target device.

Setting	Description
WMI Class	The WMI class that the sensor uses to query data from the target device.
Counter	The counter that the sensor uses to query data from the target device.
Time Stamp	The time stamp that the sensor uses to query data from the target device.
Time Frequency	The time frequency that the sensor uses to query data from the target device.
Counter Type	The counter type that the sensor uses to query data from the target device.
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**


Primary Channel ⓘ Downtime

---


Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking  below a channel gauge on the sensor's Overview tab.</p>
Graph Type	Define how this sensor shows different channels:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select</b> Stack channels on top of each other <b>above</b>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Bytes In All Heaps	The CLR memory bytes in all heaps
Bytes Total/Sec	The total number of bytes per second
Committed	The committed bytes
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Excepts	The number of thrown CLR exceptions

Channel	Description
Free Physical Memory	The free physical memory
Packets Outbound Errors	The number of outbound packet errors
Queue Length	The CPU queue length
Total Visible Memory	The total visible memory
User Time	The CPU user time (%)

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

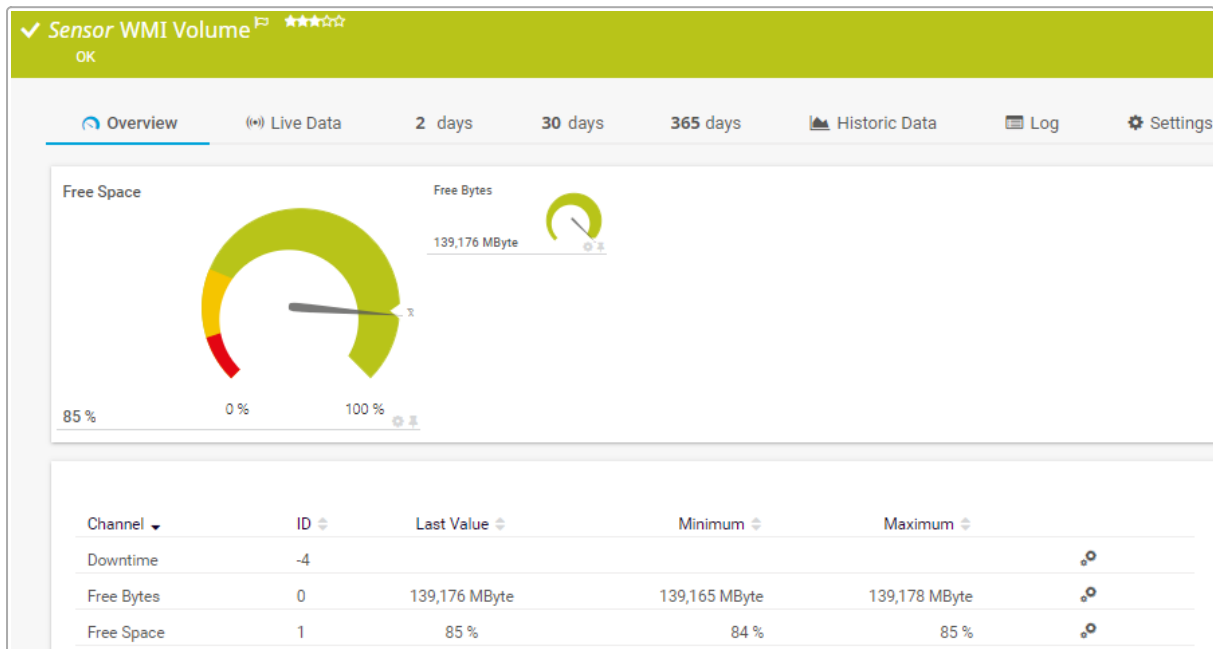
My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.311 WMI Volume Sensor

The WMI Volume sensor monitors the free disk space on a drive, logical volume, or mount point via Windows Management Instrumentation (WMI).

- i The sensor does not support disk drive management.
- i The sensor monitors an area of storage on a hard disk. It can monitor local volumes that are formatted, unformatted, mounted, or offline. A volume is formatted by using a file system such as file allocation table (FAT) or New Technology File System (NTFS), and might have a drive letter assigned to it. One hard disk can have multiple volumes, and volumes can span multiple physical disks.



WMI Volume Sensor


For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

### Sensor in Other Languages

- Dutch: WMI Volume
- French: Espace disponible du disque (WMI)
- German: WMI Datenträger
- Japanese: WMI ボリューム
- Portuguese: Volume (WMI)
- Russian: Том WMI
- Simplified Chinese: WMI 卷
- Spanish: Volumen (WMI)

## Remarks

Consider the following [remarks](#)<sup>2657</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. Stay below 200 WMI sensors per <a href="#">probe</a> . Above this number, consider using multiple <a href="#">remote probes</a> for load balancing.
WoW64	This sensor requires WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
Credentials	This sensor requires credentials for Windows systems.
Windows version	This sensor does not support Windows XP and earlier.
IPv6	This sensor supports IPv6.
Limits	This sensor has predefined <a href="#">limits</a> for several metrics.
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ exampletag ✕ +

---

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- diskspacesensor
- wmvolumesensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## WMI Volume Specific

### WMI Volume Specific

**DeviceID** ⓘ \\?\Volume{1111aaaa-22bb-33cc-44dd-555555eeeeee}\

**Drive Type** ⓘ *Unknown*

**ID Selection** ⓘ  Use system device ID (default)  
 Use drive letter

WMI Volume Specific

Setting	Description
DeviceID	The unique identifier of the volume (drive, logical volume, mount point) that this sensor monitors.
Drive Type	The type of disk drive that this sensor monitors.
ID Selection	Define how the sensor identifies the volume: <ul style="list-style-type: none"> <li>▪ Use system device ID (default): Use the system device ID. This is usually the best option for this sensor because the device ID does not change when the volume is renamed.</li> <li>▪ Use drive letter: Use the drive letter. In a Microsoft cluster environment, the device ID changes when the cluster is switched to a different node. We recommend that you select this option in this case.</li> </ul>
Drive Letter	<p><b>This setting is only visible if you select Use drive letter above.</b></p> Enter the letter of the drive that you want to monitor followed by a colon, for example, C:

## Debug Options

### Debug Options

**Result Handling** ⓘ  Discard result (default)  
 Store result

Debug Options



Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p><b>i</b> In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**

Primary Channel **i** Downtime

---

Graph Type **i**  Show channels independently (default)


Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p><b>i</b> You can set a different primary channel later by clicking <b>⌵</b> below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p><b>i</b> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p>

Setting	Description
	Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.



## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Free Bytes	The free space
Free Space	<p>The free space (%)</p> <p> This channel is the primary channel by default.</p> <p> This channel has default limits:</p> <ul style="list-style-type: none"> <li>▪ Lower error limit: <a href="#">10%</a></li> <li>▪ Lower warning limit: <a href="#">25%</a></li> </ul>

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

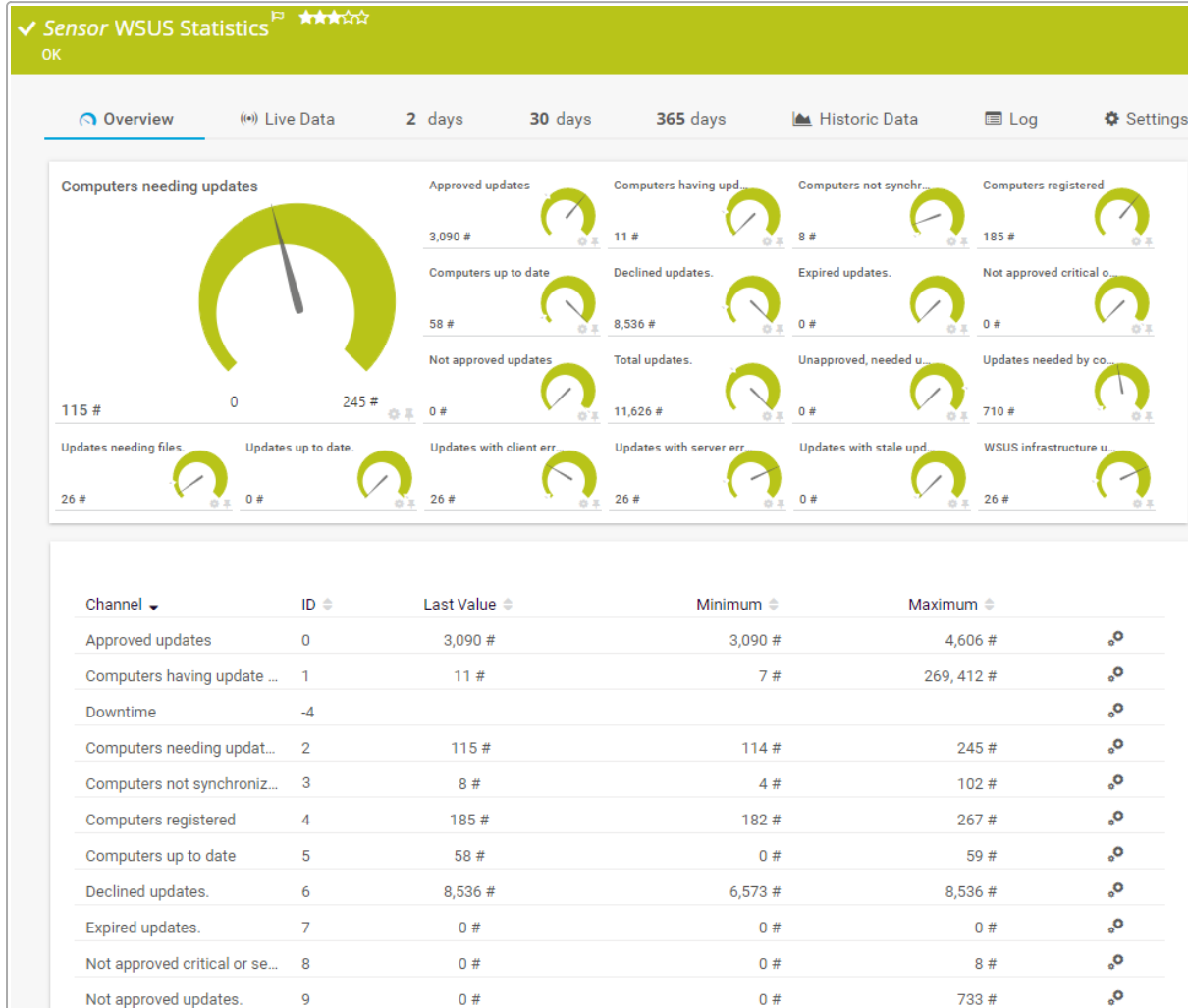
- <https://kb.paessler.com/en/topic/61108>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

## 7.8.312 WSUS Statistics Sensor

The WSUS Statistics sensor monitors various statistics on a Windows Server Update Services (WSUS) server via Windows Management Instrumentation (WMI).



WSUS Statistics Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).





### Sensor in Other Languages

- Dutch: WSUS Statistieken
- French: WSUS statistiques
- German: WSUS-Statistiken
- Japanese: WSUS 統計情報
- Portuguese: Estatísticas WSUS
- Russian: Статистика WSUS
- Simplified Chinese: WSUS 统计

- Spanish: Estadísticas WSUS

## Remarks

Consider the following [remarks](#) <sup>2662</sup> and requirements for this sensor:

Remark	Description
Performance impact	This sensor has a <a href="#">high</a> performance impact. We recommend that you use no more than <a href="#">200</a> of this sensor on each probe.
WSUS 3.0 Administration Console	This sensor requires the Microsoft <a href="#">WSUS 3.0 Administration Console</a> on the probe system. In a cluster, it must be installed on every cluster node.
.NET 4.7.2 or later	<p>This sensor requires <a href="#">.NET 4.7.2 or later</a> from Microsoft on the probe system. In a cluster, install it on every cluster node. If the sensor shows the error PE087, additionally install .NET 3.5 on the probe system.</p> <p> If the framework is missing, you cannot create this sensor.</p> <p> For more information, see the Knowledge Base: <a href="#">Which .NET version does PRTG require?</a></p>
Windows Server	We recommend Windows Server 2016 on the probe system for best performance of this sensor.
Credentials	<p>This sensor requires credentials for Windows systems.</p> <p> We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system. Otherwise, the sensor cannot correctly connect.</p>
IPv6	This sensor supports IPv6.
Knowledge Base	Knowledge Base: <a href="#">Can I encrypt connections to my WSUS server?</a>
Hosted probe	 You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ

**Tags** ⓘ  ✕ +

**Priority** ⓘ ★ ★ ★ ☆ ☆

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- ptfsensor

■ For more information about basic sensor settings, see section [Sensor Settings](#)<sup>667</sup>.

## Sensor Settings

### Sensor Settings

**WSUS Server Port** ⓘ

**Connection Security** ⓘ  Use SSL/TLS  
 Do not use connection security (default)

Sensor Settings

Setting	Description
WSUS Server Port	Enter the number of the port the WSUS server service runs on. The default value is <a href="#">8530</a> . Enter an integer.
Connection Security	<p>Define if you want to use Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for the connection to the WSUS server or if you prefer unsecured connections:</p> <ul style="list-style-type: none"> <li>▪ Use SSL/TLS</li> <li>▪ Do not use connection security (default)</li> </ul> <p><span style="color: #0070C0;">■</span> If you want to use SSL/TLS, you must configure the WSUS server accordingly. For more information, see the Knowledge Base: <a href="#">Can I encrypt connections to my WSUS server?</a></p>

## Debug Options

**Debug Options**

**Result Handling** ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval.</li> </ul> <p> ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.</p>

## Sensor Display

**Sensor Display**


**Primary Channel** ⓘ Downtime

---


**Graph Type** ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⓘ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p>This setting is only visible if you select Stack channels on top of each other <a href="#">above</a>.</p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

 For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Approved Updates	The number of approved updates
Computers Having Update Errors	The number of computers that have update errors
Computers Needing Updates	The number of computers that need updates
Computers Not Synchronized for 7 Days	The number of computers that have not synchronized for seven days
Computers Registered	The number of computers that are registered

Channel	Description
Computers Up To Date	The number of computers that are up to date
Declined Updates	The number of updates that were declined
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Expired Updates	The number of updates that are expired
Not Approved Critical Or Security Updates	The number of critical or security updates that were not approved
Not Approved Updates	The number of updates that were not approved
Total Updates	The total number of updates
Unapproved, Needed Updates	The number of updates that are unapproved but needed
Updates Needed By Computers	The number of updates that computers need
Updates Needing Files	The number of updates that need files
Updates Up To Date	The number of updates that are up to date
Updates With Client Errors	The number of updates that have client errors
Updates With Server Errors	The number of updates that have server errors
Updates With Stale Update Approvals	The number of updates that have stale update approvals
WSUS Infrastructure Updates Not Approved For Install	The number of WSUS infrastructure updates that were not approved for installation

## More

 KNOWLEDGE BASE



Can I encrypt connections to my WSUS server?

- <https://kb.paessler.com/en/topic/63611>

Which .NET version does PRTG require?

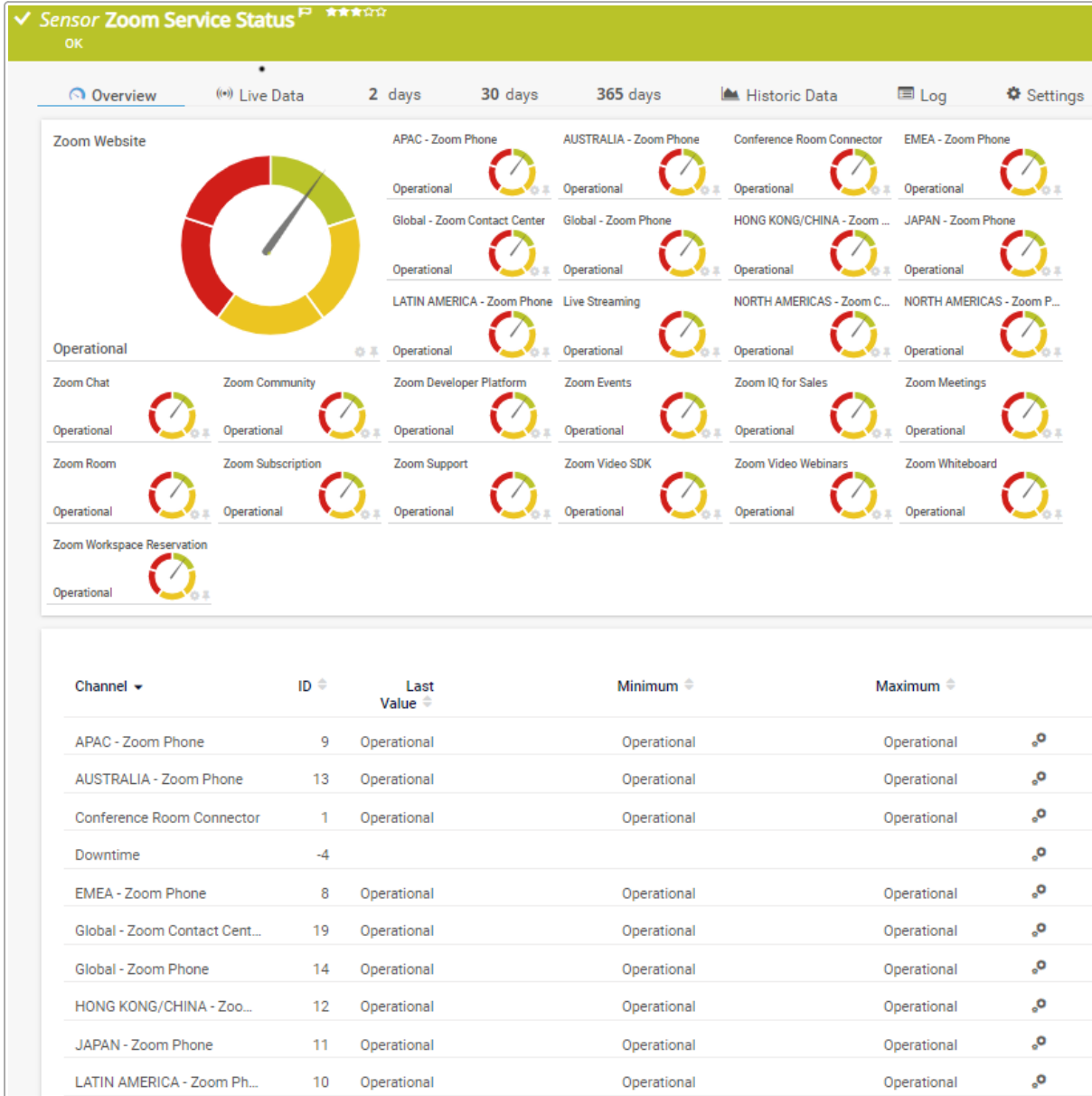
- <https://kb.paessler.com/en/topic/60543>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

### 7.8.313 Zoom Service Status Sensor

The Zoom Service Status sensor monitors the overall status of Zoom groups based on the status of their components.



Zoom Service Status Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section [Channel List](#).

#### Sensor in Other Languages

- Dutch: Zoom Service Status
- French: Zoom statut des services
- German: Zoom-Dienste-Status
- Japanese: Zoom サービスステータス

- Portuguese: Status do serviço do Zoom
- Russian: Состояние службы Zoom
- Simplified Chinese: Zoom 服务状态
- Spanish: Estado del servicio de Zoom

## Remarks

Consider the following [remarks](#) and requirements for this sensor:

Remark	Description
Internet proxies	This sensor is not compatible with internet proxies.
IPv6	This sensor supports IPv6.
Performance impact	This sensor has a <b>very low</b> performance impact.
Lookups	This sensor uses <a href="#">lookups</a> to determine the status values of one or more channels.
Scanning interval	<ul style="list-style-type: none"> <li>▪ The minimum scanning interval of this sensor is <b>1 minute</b>.</li> <li>▪ The recommended scanning interval of this sensor is <b>5 minutes</b>.</li> </ul>
Knowledge Base	Knowledge Base: <a href="#">How can I apply Zoom Service Status sensors and Modbus sensors via device templates?</a>

## Basic Sensor Settings

### Basic Sensor Settings

**Sensor Name** ⓘ Example Name

---

**Tags** ⓘ  X +

---

**Priority** ⓘ ★★★★★

Basic Sensor Settings

The sensor has the following [default tags](#) that are automatically predefined in the sensor's settings when you add the sensor:

- zoom
- zoomsensor

For more information about basic sensor settings, see section [Sensor Settings](#).

## Sensor Display

**Sensor Display**

Primary Channel ⓘ Downtime

---

Graph Type ⓘ  Show channels independently (default)  
 Stack channels on top of each other

Sensor Display

Setting	Description
Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, PRTG displays the last value of the primary channel below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> ⓘ You can set a different primary channel later by clicking ⚙ below a channel gauge on the sensor's Overview tab.</p>
Graph Type	<p>Define how this sensor shows different channels:</p> <ul style="list-style-type: none"> <li>▪ Show channels independently (default): Show a graph for each channel.</li> <li>▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic.</li> </ul> <p> ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the <a href="#">channel settings</a>).</p>
Stack Unit	<p><b>This setting is only visible if you select Stack channels on top of each other above.</b></p> <p>Select a unit from the list. PRTG stacks all channels with this unit on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

## Debug Options


**Debug Options**

Result Handling ⓘ  Discard result (default)  
 Store result

Debug Options

Setting	Description
Result Handling	<p>Define what PRTG does with the sensor result:</p> <ul style="list-style-type: none"> <li>▪ Discard result (default): Do not store the sensor result.</li> <li>▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the <a href="#">PRTG data directory</a> on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval.</li> </ul> <p>☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance.</p>

## Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the [root group settings](#) if necessary. To change a setting for this object only, click  under the corresponding setting name to disable the inheritance and to display its options.

■ For more information, see section [Inheritance of Settings](#).

## Channel List

 Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
APAC - Zoom Phone	<p>The status of the group 'APAC - Zoom Phone' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
AUSTRALIA - Zoom Phone	<p>The status of the group 'AUSTRALIA - Zoom Phone' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Conference Room Connector	<p>The status of the group 'Conference Room Connector' based on its components</p>

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
EMEA - Zoom Phone	<p>The status of the group 'EMEA - Zoom Phone' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Global - Zoom Contact Center	<p>The status of the group 'Global - Zoom Contact Center' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Global - Zoom Phone	<p>The status of the group 'Global - Zoom Phone' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
HONG KONG/CHINA - Zoom Phone	<p>The status of the group 'HONG KONG/CHINA - Zoom Phone' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
JAPAN - Zoom Phone	<p>The status of the group 'JAPAN - Zoom Phone' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
LATIN AMERICA - Zoom Phone	<p>The status of the group 'LATIN AMERICA - Zoom Phone' based on its components</p>

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Live Streaming	<p>The status of Live Streaming</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
NORTH AMERICAS - Zoom Contact Center	<p>The status of the group 'NORTH AMERICAS - Zoom Contact Center' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
NORTH AMERICAS - Zoom Phone	<p>The status of the group 'NORTH AMERICAS - Zoom Phone' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Zoom Chat	<p>The status of the group 'Zoom Chat' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Zoom Community	<p>The status of Zoom Community</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Zoom Developer Platform	<p>The status of the group 'Zoom Developer Platform' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> </ul>

Channel	Description
	<ul style="list-style-type: none"> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Zoom Events	<p>The status of Zoom Events</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Zoom IQ for Sales	<p>The status of the group 'Zoom IQ for Sales' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Zoom Meetings	<p>The status of the group 'Zoom Meetings' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul> <p> This channel is the primary channel by default.</p>
Zoom Room	<p>The status of the group 'Zoom Room' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Zoom Subscription	<p>The status of Zoom Subscription</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Zoom Support	<p>The status of the group 'Zoom Support' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Zoom Video SDK	<p>The status of the group 'Zoom Video SDK' based on its components</p>



Channel	Description
	<ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Zoom Video Webinars	<p>The status of the group 'Zoom Video Webinars' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Zoom Website	<p>The status of the group 'Zoom Website' based on its components</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Zoom Whiteboard	<p>The status of Zoom Whiteboard</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>
Zoom Workspace Reservation	<p>The status of Zoom Workspace Reservation</p> <ul style="list-style-type: none"> <li>▪ Up status: Operational</li> <li>▪ Warning status: Degraded Performance, Under Maintenance</li> <li>▪ Down status: Major Outage, Partial Outage</li> </ul>

## More

### ■ KNOWLEDGE BASE

How can I apply Zoom Service Status sensors and Modbus sensors via device templates?

- <https://kb.paessler.com/en/topic/89684>

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 7.9 Additional Sensor Types (Custom Sensors)

You can create and use your own custom sensors in PRTG to extend the standard sensor set. You can create your own sensors by using Windows Management Instrumentation Query Language (WQL), visual basic scripting, PowerShell, batch scripting, Structured Query Language (SQL) queries, by compiling an .exe file, by running Python scripts, or by translating JavaScript Object Notation (JSON) and Extensible Markup Language (XML) responses of a Representational State Transfer (REST) application programming interface (API) into sensor values.

☁ You cannot use custom sensors on hosted probes in PRTG Hosted Monitor (except SSH sensors). If you want to use custom sensors, add them to a remote probe device.

### Basics

For a general introduction, see the sections about EXE/Script sensors and section [Custom Sensors](#)<sup>[8213]</sup>, which contain details about the necessary return format for these sensors.

ⓘ WMI Custom sensors allow you to execute WQL requests. Additionally, some types of SQL sensors execute script files with SQL queries.

### Custom Sensors in PRTG

After you install PRTG, you can find a selection of custom EXE/Script, Python, and WMI WQL script sensors in the [PRTG program directory](#)<sup>[8213]</sup>, as well as scripts with SQL queries for specific database sensors, REST configuration files in the JSON template (\*.template) format for the REST Custom sensor, and .hl7 message files for the HL7 sensor. Many of the files are sample projects that you can edit and improve for your needs.

Subfolder of the PRTG Program Directory	Custom Sensors
\Custom Sensors\EXE	<p>The following custom sensors are available by default:</p> <ul style="list-style-type: none"> <li>▪ Demo Batchfile - Returns 200.bat</li> <li>▪ Demo Batchfile - Set sensorstate to error.bat</li> <li>▪ Demo Batchfile - Set sensorstate to warning.bat</li> <li>▪ Demo Cmd - Returns 200.cmd</li> <li>▪ Demo EXE - Returns a random integer.exe</li> <li>▪ Demo EXE - Returns number of files in folder (parameter).exe</li> <li>▪ Demo EXE - Returns user of process.exe</li> <li>▪ Demo Powershell Script - Available MB via WMI.ps1</li> <li>▪ Demo Powershell Script - InterruptsPerSec via WMI.ps1</li> <li>▪ Demo Powershell Script - Powershell Version.ps1</li> <li>▪ Demo Powershell Script - Returns a fixed integer.ps1</li> <li>▪ Demo Powershell Script - Returns a random integer.ps1</li> </ul>

<p>Subfolder of the PRTG Program Directory</p>	<p>Custom Sensors</p>
	<ul style="list-style-type: none"> <li>▪ Demo Powershell Script - Returns Random Integer and Warnings.ps1</li> <li>▪ Demo VBScript - InterruptsPerSec via WMI.vbs</li> <li>▪ Demo VBScript - Multiplies two integers(2 parameters).vbs</li> <li>▪ Demo VBScript - Returns a fixed float value.vbs</li> <li>▪ Demo VBScript - Returns a fixed integer.vbs</li> <li>▪ Demo VBScript - Returns a random value.vbs</li> <li>▪ Demo VBScript - Returns number of svchost processes.vbs</li> <li>▪ Demo VBScript - Returns user of process.vbs</li> <li>▪ Demo VBScript - Returns warning depending on number of svchost processes.vbs</li> <li>▪ Demo VBScript - Timezone via WMI.vbs</li> <li>▪ Demo VBScript - UTCTime via WMI.vbs</li> <li>▪ Load_Test_CPU_1_Mio_Primes.exe</li> <li>▪ Load_Test_CPU_10_Mio_Primes.exe</li> <li>▪ Load_Test_Disk_Write_Read_1000_files.exe</li> <li>▪ Load_Test_Disk_Write_Read_10000_files.exe</li> <li>▪ Load_Test_Memory_Allocate_And_Free_400MB.exe</li> </ul> <p>To create a new sensor based on one of these files, create a new EXE/Script sensor and choose the respective file from the EXE/Script list in the sensor settings.</p> <p><b>i</b> We recommend that you not edit the demo files. Create your own new files and make sure to give them unique names that do not start with <a href="#">Demo</a>, for example.</p>
<p>\\Custom Sensors\\EXEXML</p>	<p>The following custom sensor is available by default:</p> <ul style="list-style-type: none"> <li>▪ Demo Batchfile - Returns static values in four channels.bat</li> </ul> <p>To create a new sensor based on one of these files, create a new EXE/Script Advanced sensor and choose the respective file from the EXE/Script list in the sensor settings.</p>
<p>\\Custom Sensors\\hl7</p>	<p>The following custom sensors are available by default:</p> <ul style="list-style-type: none"> <li>▪ ADT_A08.hl7</li> <li>▪ ORM_O01.hl7</li> </ul>

Subfolder of the PRTG Program Directory	Custom Sensors
	<p>Each file contains an HL7 message that is conform to the HL7 message format. To create a new sensor based on one of these files, create a new HL7 sensor and choose the respective file from the HL7 Messages list in the sensor settings. You can override certain message headers in the files via the sensor settings.</p>
\Custom Sensors\python	<p>The following custom sensor is available by default:</p> <ul style="list-style-type: none"> <li>▪ sensor_example.py</li> </ul> <p>This Python example script only returns fixed values in two channels to demonstrate the usage. To create a new sensor based on this file, create a new Python Script Advanced sensor and choose the file from the Script list in the sensor settings.</p>
\Custom Sensors\rest	<p>The following custom sensors are available by default:</p> <ul style="list-style-type: none"> <li>▪ kemp.loadbalancer.template: maps values returned by the RESTful API of a KEMP load balancer to channels, for example, CPU usage, memory usage, traffic</li> <li>▪ prtg-sensor-stats.template: maps values returned by the PRTG API to channels that show the count of each sensor status on the local probe</li> <li>▪ windows.docker.container.stats.template: maps values returned by the Docker Engine API to channels, for example, CPU usage, memory usage, traffic, input/output (I/O)</li> <li>▪ wunderground.template: maps values returned by the Weather Underground API to channels, for example, temperature, dew point, pressure, wind speed, wind direction</li> </ul> <p>To create a new sensor based on one of these files, create a new REST Custom sensor on the device that provides the REST API and choose the file from the REST Configuration list in the sensor settings.</p>
\Custom Sensors\scripts\examples\python	<p>The following example scripts are available by default:</p> <ul style="list-style-type: none"> <li>▪ dice_roll.py</li> <li>▪ dropbox_space_free.py</li> <li>▪ hybrid_parameters_ping.py</li> <li>▪ remote_ssh_linux_network.py</li> <li>▪ remote_ssh_linux_system_load.py</li> </ul> <p>To use the example scripts, copy them to the \Custom Sensors\scripts subfolder of the PRTG program directory. To create a new sensor based on one of these files, create a new Script v2 sensor and choose one or more Python scripts from the list in the script specific settings. PRTG creates one sensor for each script that you select.</p>

Subfolder of the PRTG Program Directory	Custom Sensors
\Custom Sensors\sql\[dbms]	<p>The following custom sensor is available by default:</p> <ul style="list-style-type: none"> <li>▪ Demo Serveruptime.sql</li> </ul> <p>You can find this demo SQL query script in each subfolder for each supported <a href="#">database management system (DBMS)</a>: \adosql, \mssql, \mysql, \oracle, \postgresql</p> <p>To create a new sensor that uses one of the scripts in the dbms folders, create the according sensor (<a href="#">see above for supported sensors</a><sup>2676</sup>) and choose the respective file from the SQL Query File list in the sensor settings.</p>
\Custom Sensors\WMI WQL scripts	<p>The following custom sensors are available by default:</p> <ul style="list-style-type: none"> <li>▪ Demo WQL Script - Get Win32LogicalDiscFreeMB.wql</li> <li>▪ Demo WQL Script - Get Win32OsBuildnumber.wql</li> <li>▪ Demo WQL Script - Get Win32PercentProcessorIdleTime.wql</li> <li>▪ Demo WQL Script - Get Win32PercentProcessorTime.wql</li> </ul> <p>To create a new sensor based on one of these files, create a new WMI Custom sensor and choose the respective file from the WQL File list in the sensor settings.</p>

## Download Custom Sensors

Good resources to find custom sensors that other users and we from Paessler share are the [PRTG Sensor Hub](#) and our Knowledge Base. In the Knowledge Base, search for the tag [custom-script-exe](#) to find a lot of custom sensors.

## More

### ■ KNOWLEDGE BASE

Guide for PowerShell-based custom sensors

- <https://kb.paessler.com/en/topic/71356>

Custom sensors

- <https://kb.paessler.com/en/tags/custom-script-exe>

How can I share my self-written PRTG script/program with other PRTG users?

- <https://kb.paessler.com/en/topic/63737>

How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- <https://kb.paessler.com/en/topic/11283>

Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

I want to use the Script v2 sensor example scripts. What do I need to know?

- <https://kb.paessler.com/en/topic/91349>



#### ■ PAESSLER WEBSITE

You can find useful scripts for sensors in the PRTG Sensor Hub

- <https://www.paessler.com/sensor-hub>

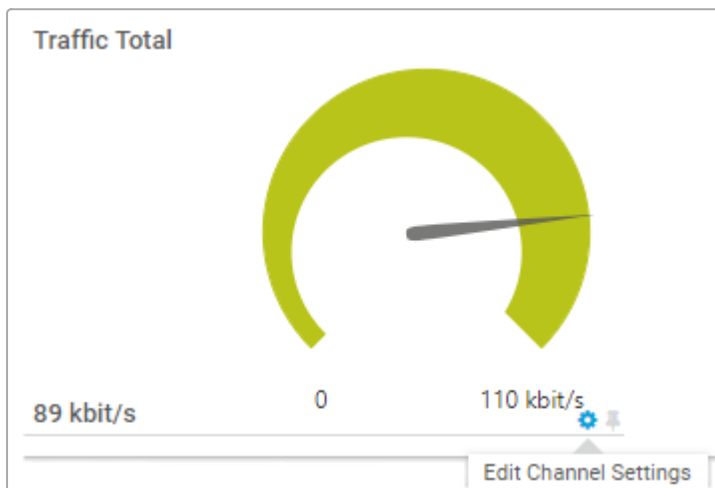
## 7.10 Channel Settings

A sensor has one or more channels in which it handles the actual monitoring data. In the channel settings, you can define how to display the data from the sensor's different channels displayed in graphs, gauges, and tables. Additionally, the channel data can determine the [sensor status](#). Use the limit settings to define desired sensor states for values.

On the sensor's Overview tab, click  below a gauge to change the channel's settings. Click  below a gauge to make this channel the primary channel of the selected sensor.

You can also open the settings of a channel by clicking  in the channels data table.

**i** For [lookup](#) channels, we recommend that you stay below 120 lookup values to get expressive gauges. For non-primary lookup channels, the upper limit is around 40 lookup values.



The Gear Icon of an SNMP Traffic Total Channel to Open Channel Settings

The available options are nearly the same for all sensors. An exception applies to the Downtime channel, which PRTG automatically calculates and which does not offer all settings. Channels with [absolute](#) values additionally have an option to define the Value Mode. Custom channels have a Lookups and Limits setting to distinguish between alerting by lookups or numeric limits.

You can choose a different channel via the dropdown list at the top of the channel settings list.

**Edit Channel**
✕

---

Free Space (ID 0)
▼

---

**Edit Channel "Free Space"**

**Name** ⓘ

Free Space

---

**ID** ⓘ

0

**Limits** ⓘ

Disable limits

Enable alerting based on limits

**Graph Rendering** ⓘ

Show in graphs

Hide in graphs

**Table Rendering** ⓘ

Show in tables

Hide in tables

**Line Color** ⓘ

Automatic

Manual

**Line Width** ⓘ

1

---

**Value Mode** ⓘ

Average

Minimum

Maximum

**Decimal Places** ⓘ

Apply
OK
Cancel

Channel Settings for a Disk Sensor

## Edit Channel

Setting	Description
Name	<p>Enter a name for the channel. The name appears in graphs and tables.</p> <p> ⓘ You can automatically add the sensor's ID to the name by using the placeholder <code>[#id]</code>.</p> <p> ⓘ You cannot edit the name for script sensors after sensor creation.</p>



Setting	Description
	<p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Unit	<p><b>This setting is only visible for custom sensors.</b></p> <p>Enter the unit for the values that this sensor returns. Enter a string.</p> <p><b>i</b> PRTG uses the unit string for display purposes and shows it in graphs, data tables, and gauges.</p>
Scaling Multiplication	<p><b>This setting is only visible for channels with a custom unit.</b></p> <p>If you want to multiply the received raw data by a certain value, enter the multiplier. Otherwise, use the default value <b>1</b> to not change the received value. Enter an integer.</p> <p>For example, the following sensors provide the scaling factor for received values with custom units in their settings:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Sensor Factory</a> sensor (you can use multiplication and division in the channel definition)</li> <li>▪ <a href="#">SNMP APC Hardware</a> sensor</li> <li>▪ <a href="#">SNMP Custom</a> sensor</li> <li>▪ <a href="#">SNMP Dell Hardware</a> sensor</li> <li>▪ <a href="#">WMI Custom</a> sensor</li> </ul> <p><b>i</b> If the channel uses lookups, the scaling factor does not modify the values that are defined in the lookups. Any applied lookup always uses the raw value as it is retrieved from the target device. If you use a scaling factor for such a channel, you notice the scaling in data graphs, but the channel value appears unmodified in data tables.</p>
Scaling Division	<p><b>This setting is only visible for channels with a custom unit.</b></p> <p>If you want to divide the received raw data by a certain value, enter the divisor here. Otherwise, use the default value <b>1</b> to not change the received value. Enter an integer.</p> <p>For example, the following sensors provide the scaling factor for received values with custom units in their settings:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Sensor Factory</a> sensor (you can use multiplication and division in the channel definition)</li> <li>▪ <a href="#">SNMP APC Hardware</a> sensor</li> <li>▪ <a href="#">SNMP Custom</a> sensor</li> <li>▪ <a href="#">SNMP Dell Hardware</a> sensor</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ <a href="#">WMI Custom</a> sensor</li> </ul> <p><b>i</b> If the channel uses lookups, the scaling factor does not modify the values that are defined in the lookups. Any applied lookup always uses the raw value as it is retrieved from the target device. If you use a scaling factor for such a channel, you notice the scaling in data graphs, but the channel value appears unmodified in data tables.</p>
ID	<p>Shows the ID of the channel. PRTG uses it for unique identification. For example, you need the ID for Sensor Factory sensors.</p> <p>There are a few special, fixed channel IDs.</p> <ul style="list-style-type: none"> <li>▪ <b>-1</b> is for sum channels of traffic sensors (for example, of the <a href="#">SNMP Traffic</a> sensor).</li> <li>▪ <b>-4</b> is for the Downtime channel (you can use it, for example, for an uptime percentage calculation in a Sensor Factory sensor).</li> <li>▪ <b>-2</b> (coverage) and <b>-3</b> (error) are internally used.</li> </ul> <p><b>i</b> This setting is for your information only. You cannot change it.</p>
Limits	<p><b>This setting is not available for custom channels.</b></p> <p>Define if you want to set limits for this channel:</p> <ul style="list-style-type: none"> <li>▪ <b>Disable limits:</b> Do not use the channel data to define the sensor status.</li> <li>▪ <b>Enable alerting based on limits:</b> Define limits for the numeric values that are returned by the device. The sensor of which this channel is a part of shows the Warning status or the Down status when limits fall below the defined value or when limits are exceeded.</li> </ul> <p><b>i</b> The channel can affect the <a href="#">status of the sensor</a> that it is a part of. By setting limits, you can define when the sensor shows the Warning status or the Down status, depending on the channel data. For example, you can use limits to set a traffic sensor (that is usually never in the Down status) to show the Down status when the monitored values reach critical limits.</p> <p><b>i</b> Enable alerting based on limits is not available for the Downtime channel.</p> <p><b>i</b> You can show limits in graphs (highlighted in yellow or red) if you select exactly one channel with a limit in a graph.</p>
Lookups and Limits	<p><b>This setting is only available for custom channels.</b></p> <p>Define when the sensor shows the Down status and alerts you, either based on the lookup definition or based on limits for returned values:</p>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Enable alerting based on lookups: Use the lookup definition of the channel to define the sensor status. Make sure that the channel uses a proper Lookup if you use this option. Select the lookup file either in the channel settings or in the sensor settings, depending on the sensor. If you do not want to use the channel data to define the sensor status, select None as Lookup.</li> <li>▪ Enable alerting based on limits: Define limits for numeric values returned by the device. The sensor of which this channel is a part of shows the Warning status or the Down status when limits fall below the defined value or when limits are exceeded.</li> </ul> <p><b>i</b> Only the option you choose applies. If you choose limit-based alerting, errors and warnings that you have defined in the lookup file do not apply.</p>
Lookup	<p>This setting is only visible for custom sensors and if you select lookups-based alerting.</p> <p>Select the lookup file that you want to use with this channel.</p> <p><b>i</b> Do not use this option for sensors that provide the unit Lookup in the sensor settings. The channel setting is overwritten with the next sensor scan. Define the lookup file that you want to use with this channel on the Settings tab of the sensor. Select the option Lookup for the setting Channel #x Unit (where x is the number of the channel) and define the desired lookup file under Channel #x Lookup. See section <a href="#">Define Lookups</a> for affected sensors.</p> <p><b>i</b> If you choose None, alerting by lookups and limits is disabled and channels do not appear as lookups. If you want to keep the lookup representation without alerting, define the states accordingly in the lookup file.</p>
Upper Error Limit ([unit])	<p>This setting is only visible if you select Enable alerting based on limits above.</p> <p>Specify an upper limit for the Down status. If the channel values exceed this value, the sensor shows the Down status. Enter a valid number into at least one of the limit fields.</p> <p><b>i</b> The value that you enter here must match the type of value that the device returns, either an integer or a float. See also <a href="#">Absolute Values and Delta Values for Limits</a>.</p> <p><b>i</b> While a sensor shows the Down status because of a limit, it still receives data in its channels.</p>
Upper Warning Limit ([unit])	<p>This setting is only visible if you select Enable alerting based on limits above.</p>

Setting	Description
	<p>Specify an upper limit for the Warning status. If the channel values exceed this value, the sensor shows the Warning status. Enter a valid number into at least one of the limit fields.</p> <p><b>i</b> The value that you enter here must match the type of value that the device returns, either an integer or a float. See also <a href="#">Absolute Values and Delta Values for Limits</a> <sup>2690</sup>.</p>
Lower Warning Limit ([unit])	<p><b>This setting is only visible if you select</b> Enable alerting based on limits above.</p> <p>Specify a lower limit for the Warning status. If the channel values fall below this value, the sensor shows the Warning status. Enter a valid number into at least one of the limit fields.</p> <p><b>i</b> The value that you enter here must match the type of value that the device returns, either an integer or a float. See also <a href="#">Absolute Values and Delta Values for Limits</a> <sup>2690</sup>.</p>
Lower Error Limit ([unit])	<p><b>This setting is only visible if you select</b> Enable alerting based on limits above.</p> <p>Specify a lower limit for the Down status. If the channel values fall below this value, the sensor shows the Down status. Enter a valid number into at least one of the limit fields.</p> <p><b>i</b> The value that you enter here must match the type of value that the device returns, either an integer or a float. See also <a href="#">Absolute Values and Delta Values for Limits</a> <sup>2690</sup>.</p> <p><b>i</b> While a sensor shows the Down status because of a limit, it still receives data in its channels.</p>
Error Limit Message	<p><b>This setting is only visible if you select</b> Enable alerting based on limits above.</p> <p>Enter an additional message. PRTG adds it to the sensor message when the sensor shows the Down status. Enter a string or leave the field empty.</p>
Warning Limit Message	<p><b>This setting is only visible if you select</b> Enable alerting based on limits above.</p> <p>Enter an additional message. PRTG adds it to the sensor message when the sensor shows the Warning status. Enter a string or leave the field empty.</p>
Graph Rendering	Select if you want to show this channel in data graphs:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Show in graphs: Sensor graphs contain the data of this channel.</li> <li>▪ Hide in graphs: Sensor graphs do not contain data of this channel.</li> </ul> <p><b>i</b> If you choose to hide this channel in graphs, it also does not appear in the graphs of <a href="#">reports</a><sup>[2754]</sup> or <a href="#">maps</a><sup>[2776]</sup>.</p> <p><b>■</b> For more information about data graphs, see the Knowledge Base: <a href="#">What options do I have to review my monitoring data in detail?</a></p>
Table Rendering	<p>Select if you want to show this channel in data tables:</p> <ul style="list-style-type: none"> <li>▪ Show in tables: Sensor data tables contain the data of this channel.</li> <li>▪ Hide in tables: Sensor data tables do not contain the data of this channel. This option hides the gauge as well, but the channel is still available in the data table of the sensor's Overview tab.</li> </ul> <p><b>i</b> If you choose to hide this channel in data tables, PRTG also does not use it for the calculation of the Total channel of a sensor. It also does not appear in data tables of a report.</p> <p><b>■</b> For more information about data tables, see the Knowledge Base: <a href="#">What options do I have to review my monitoring data in detail?</a></p>
Line Color	<p>Select the color of the channel display in graphs:</p> <ul style="list-style-type: none"> <li>▪ Automatic: PRTG automatically sets the color of this channel in graphs.</li> <li>▪ Manual: Individually define the color of this channel. You can enter the desired color code below.</li> </ul>
Color (#rrggbb)	<p><b>This setting is only visible if you select Manual above.</b></p> <p>Enter a color in hexadecimal notation as in .html and .css files, or choose a color from the visual color selector. The field with the hexadecimal color value automatically changes to the color you select.</p>
Line Width	<p>Enter the width of the channel line in graphs. Enter an integer in pixels. The maximum line width is <b>25</b>, but we recommend that you only use values between <b>1</b> and <b>7</b> to get optimal results.</p>
Data	<p>This setting is available for most channels. Define how to display data:</p> <ul style="list-style-type: none"> <li>▪ Display actual values in <b>[unit]</b>: Display the values in the shown unit.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Display in percent of maximum: Calculate and show percent values based on a maximum value. Enter a maximum below.               <ul style="list-style-type: none"> <li>❗ If you choose this option, you cannot display the data of traffic sensors as a positive and negative area graph.</li> <li>❗ If you choose this option, values in the Limits section are counted as percent values.</li> </ul> </li> </ul>
Maximum ([unit])	<p><b>This setting is only visible if you select</b> Display in percent of maximum above.</p> <p>Enter a value to use as the maximum. Consider the unit. PRTG calculates all percent values based on this value. Enter an integer.</p>
Value Mode	<p><b>This setting is only available for channels that return</b> absolute values.</p> <p>Define which value type you want to display in historic data graphs and tables:</p> <ul style="list-style-type: none"> <li>▪ Average: The channel shows average values.</li> <li>▪ Minimum: The channel shows the minimum values.</li> <li>▪ Maximum: The channel shows the maximum values.</li> </ul> <p>❗ This setting is not available for sensors that show difference values, such as traffic channels.</p> <p>■ For more information about value modes, see the Knowledge Base: <a href="#">What is the Value Mode in channel settings?</a></p>
Decimal Places	<p>Define how many decimal places of the channel's data that you want to display in graphs and tables:</p> <ul style="list-style-type: none"> <li>▪ Automatic: PRTG automatically defines how many decimal places to use for optimal viewing results.               <ul style="list-style-type: none"> <li>❗ PRTG rounds values between 10 and -10 to two decimal places. It rounds values that are very close to an integer to the integer, for example, it rounds 3.001 to 3.</li> </ul> </li> <li>▪ All: Display all available decimal places.</li> <li>▪ Custom: Manually define the number of decimal places. If you choose this option, an additional field appears. Enter an integer.</li> </ul>
Spike Filter	<p>You can use a spike filter to correct faulty monitoring data. Sometimes, sensors report values that are enormously high or far too low. This can be because of an error in data transmission, or because of incompatibilities of the physical device you are monitoring. This can make graphs unreadable. A spike filter can compensate for these flaws.</p> <p>Define if you want to filter incoming data:</p>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ <b>Disable filtering:</b> Display all data as it is received. Do not filter out spikes.</li> <li>▪ <b>Enable filtering:</b> Enable a filter to remove spike values. PRTG disregards values that are above and below a certain limit in the monitoring data for graphs and tables. Additional fields appear below. <ul style="list-style-type: none"> <li>ⓘ This does not change monitoring data itself but only the presentation of the data. This setting is valid for all data of this channel, including historic data.</li> </ul> </li> </ul> <p>ⓘ Use the spike filter with care. For overflow values in SNMP sensors, check the <a href="#">SNMP Compatibility Options</a> before.</p> <p>ⓘ The spike filter option is not available for the channel Downtime.</p>
Spike Filter Max. Value ([unit])	<p>This setting is only visible if you select <a href="#">Enable filtering</a> above.</p> <p>Enter the maximum value to show in the channel data. PRTG disregards all data above this value in graphs and tables. Enter an integer or leave the field empty.</p>
Spike Filter Min. Value ([unit])	<p>This setting is only visible if you select <a href="#">Enable filtering</a> above.</p> <p>Enter the minimum value to show in the channel data. PRTG disregards all data below this value in graphs and tables. Enter an integer or leave the field empty.</p>
Vertical Axis Scaling	<p>Define how to display the vertical axis for the channel in graphs:</p> <ul style="list-style-type: none"> <li>▪ <b>Automatic scaling:</b> PRTG automatically uses the optimum scaling. Usually the scaling ranges from the minimum to the maximum value. PRTG uses one single scale for each unit label only.</li> <li>▪ <b>Manual scaling:</b> Manually define the scaling. Additional fields appear below. If you define manual axis scaling, it can make low values better visible in your graph, but it might result in a graph with multiple vertical axes for the same unit label.</li> </ul> <p>ⓘ PRTG ignores settings for this option if you select <a href="#">Stack channels on top of each other</a> under Graph Type on the sensor's Settings tab.</p>
Vertical Axis Maximum ([unit])	<p>This setting is only visible if you select <a href="#">Manual scaling</a> above.</p> <p>Enter the maximum value to use on the vertical axis for the channel. Enter an integer.</p>
Vertical Axis Minimum ([unit])	<p>This setting is only visible if you select <a href="#">Manual scaling</a> above.</p>

Setting	Description
	Enter the minimum value to use on the vertical axis for the channel. Enter an integer.

**i** Click OK to save your settings and to close the settings window. Click Apply to save the changed settings while the Edit Channel window remains open, for example if you want to change the settings of other channels of the current sensor as well. You can select a different channel via the dropdown list above the settings. You can close the settings window without saving by clicking Cancel.

**i** If you change any settings and either click Cancel or select a different channel via the dropdown list, PRTG asks you to confirm this step. Click Save to apply the changes or click Discard Changes to ignore the changes. PRTG closes the window or shows the settings of the selected channel respectively.

#### Absolute Values and Delta Values for Limits

The value type that you need to configure for limits depends on the type of data that the channel delivers:

Value Type	Description
Absolute values	For channels that measure absolute values, for example, for free disk space, you must set limits with absolute values like <a href="#">20</a> .
Delta values	For channels that measure delta values, that is, measurements per second (x.xx/sec), you must set delta values according to the formula <a href="#">number of errors/scanning interval in seconds</a> .

For example, you have an SNMP Traffic sensor and want to receive an alert when the sensor reports errors:

- Set the sensor to the Warning status when [1](#) error occurs.
- Set the sensor to the Down status when [30](#) errors occur.

The following screenshot shows how to configure the limits for delta channels. You could set the following limits for the channel Errors In with a standard scanning interval of 60 seconds:



### Edit Channel "Errors in"

**Name** ⓘ  
Errors in

---

**ID** ⓘ  
10

**Limits** ⓘ  
 Disable limits  
 Enable alerting based on limits

**Upper Error Limit (#/s)** ⓘ  
0.5

---

**Upper Warning Limit (#/s)** ⓘ  
0.1

---

**Lower Warning Limit (#/s)** ⓘ

---

**Lower Error Limit (#/s)** ⓘ

---

**Error Limit Message** ⓘ

---

**Warning Limit Message** ⓘ

---

**Graph Rendering** ⓘ  
 Show in Graphs  
 Hide from Graphs

**Table Rendering** ⓘ  
 Show in Tables

---

**Apply** **Ok** **Cancel**

Setting Channel Limits with Delta Values

Because this channel uses per second (delta) measurements, the sensor reports a single error that occurs over a standard 60-second scanning interval as 0.016 # per second. So the warning limit for one single error within a scanning interval is 0.1 (errors/sec). To get an alert when there are 30 errors within a scanning interval, the limit needs to be 0.5 (errors/sec).

- ❗ If no new errors occur in the next scanning interval, the sensor shows the Up status again. To make sure that you do not miss any notifications for this sensor, set a notification trigger with 0 seconds.

## Channel List Status

Under the channel gauge view on a sensor overview page, there is a channel list showing the active channels of a sensor listed alphabetically and data from each channel. The Downtime channel never shows any values. Sensors in the Paused status display **No data** in place of all data values or remain blank, regardless of whether there is historic data available. The data values are displayed again when the sensor is no longer paused.

Channel ▾	ID ↕	Last Value ↕	Minimum ↕	Maximum ↕
-----------	------	--------------	-----------	-----------

Channel List

Table Header	Description
Channel	The name of the channel.
ID	The ID of the channel.  ❗ This setting is for your information only. You cannot change it.
Last Value	The most recent value of the channel recorded by the sensor.
Minimum	The lowest historic value recorded by the sensor.
Maximum	The highest historic value recorded by the sensor.

The Minimum and Maximum values remain the same until one of two events take place:

- The value is replaced by another value that is less than or greater than the original, respectively.
- A PRTG cache recalculation is prompted, refreshing all values.

These values are cached and are not affected by [historic data purges](#)<sup>[2899]</sup>, making it possible to have a minimum or maximum value that is no longer recorded in the historic data.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

What is the Value Mode in channel settings?

- <https://kb.paessler.com/en/topic/60238>

## 7.11 Notification Triggers Settings

You can use changes in a sensor's status or in the sensor's data to trigger notifications.

The screenshot shows the 'Notification Triggers' tab for a sensor. The interface includes a navigation bar with options like Overview, Live Data, and Settings. The main content area is divided into three sections:

- Notification Triggers:** A table with columns for Type, Rule, and Actions. It lists three triggers based on sensor state (Down for at least 900 seconds, Down for at least 3600 seconds, and no longer Down).
- Notification triggers that can be inherited from parent objects:** Radio buttons to select inheritance options. Below is a table of inherited triggers from the 'Root' object.
- Notification triggers that are defined in libraries:** A section indicating that no triggers are currently defined in libraries.

Notification Triggers Tab

Although sensors activate notification triggers, you can set notification triggers in the settings of objects that are higher in the [object hierarchy](#)<sup>[132]</sup>. This allows you to use the [inheritance of settings](#)<sup>[136]</sup> to define notification triggers for multiple sensors. Objects that inherit notification triggers show them on the Notification Triggers tab.

■ For more information, see section [Triggers That Can Be Inherited from Parent Objects](#)<sup>[2703]</sup>.

You can also define notification triggers in [libraries](#)<sup>[2738]</sup>. If a sensor is in a library that has notification triggers, the sensor shows them on the Notification Triggers tab.

■ For more information, see section [Triggers That Are Defined in Libraries](#)<sup>[2704]</sup>.

ⓘ You can also directly edit notification templates on the Notification Triggers tab. To do so, click  next to name of a notification template.

### Note

You must take the following four steps to set up and use notifications:

1. Check and set up the [notification delivery](#)<sup>[2877]</sup> settings if you use PRTG Network Monitor. These settings define how PRTG sends messages.
2. Check and set up [notification contacts](#)<sup>[2842]</sup> for the user accounts. These contacts define the recipients to which PRTG sends notifications.

3. Check and set up several [notification templates](#)<sup>[2808]</sup>. These templates define the notification methods and their content.

**i** You can also check or edit notification templates via the Notification Triggers tab. For more information, see section [Notification Triggers Settings](#)<sup>[2693]</sup>.

4. Check and set up [notification triggers settings](#)<sup>[2693]</sup> for objects. These triggers define when PRTG sends notifications.

**i** Usually, there are three successive attempts to deliver a notification. If all of these attempts fail, the notification is lost. To never miss a notification, we recommend that you always set up at least two notifications with different notification methods for a notification trigger, for example, one email notification and one SMS notification. If delivery via email fails, PRTG can still notify you via smartphone as a fallback. For example, use the latency setting of a [state trigger](#)<sup>[2694]</sup> to choose a notification with a different notification method than in the first trigger condition, or set up a second trigger with a different notification method for the corresponding object.

■ For a detailed step-by-step guide, see the Paessler website: [How to set up notifications via the PRTG web interface](#).

■ Custom notification scripts are also available in the [PRTG Sensor Hub](#).

## Notification Triggers



Select the Notification Triggers tab of an object to add or edit notification triggers. You can set up one or more of the following notification triggers:

- [State Trigger](#)<sup>[2694]</sup>
- [Speed Trigger](#)<sup>[2696]</sup>
- [Volume Trigger](#)<sup>[2699]</sup>
- [Threshold Trigger](#)<sup>[2700]</sup>
- [Change Trigger](#)<sup>[2702]</sup>

Different options are available for every notification trigger. You see the Type of notification trigger and the notification Rule that the sensor executes once it activates a notification trigger.

**i** Which notification triggers are available on the Notification Triggers tab depends on the kind of object you select.

## State Trigger

The state trigger performs a notification when a sensor changes its status. Hover over  and select Add State Trigger from the menu to add a new state trigger or click  next to a state trigger to change it.


State Trigger      When sensor state is Down      for at least 60 seconds, perform no notification



When sensor state is Down for at least 300 seconds, perform no notification and repeat every 0 minutes

When sensor state is no longer Down, perform no notification

Add State Trigger



**i** PRTG includes a state trigger for the [root group](#)<sup>132</sup> by default. This notification trigger performs the notification Email and push notification to admin if any sensor is in the Down [status](#)<sup>181</sup> for at least 10 minutes.

Setting	Description
When sensor status is [...]	<p>Select the status that triggers a notification:</p> <ul style="list-style-type: none"> <li>▪ Down: Trigger a notification if a sensor changes to the Down status.</li> <li>▪ Warning: Trigger a notification if a sensor changes to the Warning status.</li> <li>▪ Unusual: Trigger a notification if a sensor changes to the Unusual status.</li> <li>▪ Down (Partial): Trigger a notification if a sensor changes to the Down (Partial) status. This status is only possible in a <a href="#">failover cluster</a><sup>128</sup>.</li> <li>▪ Up: Trigger a notification if a sensor changes to the Up status.</li> <li>▪ Unknown: Trigger a notification if a sensor changes to the Unknown status.</li> </ul>
for at least [...] seconds,	<p>Enter the time in seconds that PRTG waits before it sends a notification (<a href="#">latency</a>). This can avoid false alarms if, for example, a sensor changes to the Down status for only a few seconds. Enter an integer.</p> <p><b>i</b> Do not define a latency that is shorter than the scanning interval of a sensor that uses this trigger. The notification trigger might not work as expected in this case.</p>
perform [...]	<p>Select the notification that PRTG sends if the sensor is in the selected status <a href="#">and</a> if the defined latency is over. You see all notification templates that you have defined under Setup   Account Settings   Notification Templates. Use the search box to filter for notification templates. You can also select no notification to not send a notification in this case.</p> <p><b>i</b> You can also directly create and use new notification templates by clicking  in the dropdown list.</p>
When sensor status is [...] for at least [...] seconds	<p>Enter the escalation latency in seconds that PRTG waits before it sends an escalation notification. Use this to automatically escalate a notification if a problem exists for a longer time. Enter an integer.</p> <p><b>i</b> PRTG automatically fills in the selected status.</p>
perform [...]	<p>Select the notification that PRTG sends if the sensor is still in the selected status <a href="#">and</a> if the defined escalation latency is over. You see all notification templates that you have defined under Setup   Account Settings   Notification Templates. Use the search box to filter for notification templates. You can also select no notification to not send a notification in this case.</p>

Setting	Description
	<p><b>i</b> Select a notification with a different delivery method than in the first trigger condition to make sure that you receive a notification in case the first notification could not be sent.</p> <p><b>i</b> You can also directly create and use new notification templates by clicking  in the dropdown list.</p>
and repeat every [...] minutes	<p>Enter the interval in minutes after which PRTG sends the escalation notification again. Enter an integer.</p> <p><b>i</b> If you enter 0, PRTG does not send the escalation notification again.</p>
When sensor status is no longer [...], perform [...]	<p>Select the notification that PRTG sends if the sensor is <b>no longer</b> in the selected status <b>and</b> if the defined latency is over. You see all notification templates that you have defined under Setup   Account Settings   Notification Templates. Use the search box to filter for notification templates. You can also select no notification to not send a notification in this case.</p> <p><b>i</b> PRTG automatically fills in the selected status.</p> <p><b>i</b> You can also directly create and use new notification templates by clicking  in the dropdown list.</p>

Click  to save your settings or click  to undo your changes.


## Speed Trigger



The speed trigger performs a notification if the speed that a sensor monitors changes. Hover over  and select Add Speed Trigger from the menu to add a new speed trigger or click  next to a speed trigger to change it.








Speed Trigger    When **Other**  channel is **Above**  **0** **bit**  / **second**  for at least **60** seconds, perform **no notification**

When condition clears, perform **no notification**

[Add Speed Trigger](#)

Setting	Description
When [...] channel	<p>Select the <b>channel</b>  whose data PRTG uses for the speed comparison. At root, probe, group, or device level or in libraries, the following channels are available:</p> <ul style="list-style-type: none"> <li>Primary: Use the data of the primary channel of the sensor for the comparison.</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ Total: Use the data of the Total channel of the sensor for the comparison.</li> <li>▪ Traffic In: Use the data of the Traffic In channel of the sensor for the speed comparison.</li> <li>▪ Traffic Out: Use the data of the Traffic Out channel of the sensor for the speed comparison.</li> </ul> <p>At sensor level, the available channels depend on the type of sensor you select.</p> <p> If you set notification triggers at root, probe, group, or device level and you want to know which sensors the notification triggers apply to, see section <a href="#">Available Sensor Types</a><sup>[3232]</sup>.</p>
is [...]	<p>Select the condition that triggers the notification:</p> <ul style="list-style-type: none"> <li>▪ Above: Trigger the notification if the value of the selected channel exceeds a defined value.</li> <li>▪ Below: Trigger the notification if the value of the selected channel falls below a defined value.</li> <li>▪ Equal to: Trigger the notification if the value of the selected channel is the same as a defined value.</li> <li>▪ Not equal to: Trigger the notification if the value of the selected channel is different than a defined value.</li> </ul>
[value]	<p>Enter the value to which PRTG compares the channel data. Enter an integer.</p>
[scale]	<p>Select the unit for the [value]:</p> <ul style="list-style-type: none"> <li>▪ bit</li> <li>▪ kbit</li> <li>▪ Mbit</li> <li>▪ Gbit</li> <li>▪ Tbit</li> <li>▪ Byte</li> <li>▪ KB</li> <li>▪ MB</li> <li>▪ GB</li> <li>▪ TB</li> </ul> <p> The available units depend on the type of sensor you select.</p>

Setting	Description
	<p> [scale] and [time] define the unit for [value]. If the channel data has a different unit, PRTG internally converts the values.</p>
[time]	<p>Select the time for the scale to create a scale per time unit:</p> <ul style="list-style-type: none"> <li>▪ second</li> <li>▪ minute</li> <li>▪ hour</li> <li>▪ day</li> </ul> <p> [scale] and [time] define the unit for [value]. If the channel data has a different unit, PRTG internally converts the values.</p>
for at least [...] seconds,	<p>Enter the time in seconds that PRTG waits before it sends a notification (<a href="#">latency</a>). This can avoid false alarms if, for example, a sensor changes to the Down status for only a few seconds.. Enter an integer.</p> <p> Do not define a latency that is shorter than the scanning interval of a sensor that uses this trigger. The notification trigger might not work as expected in this case.</p>
perform [...]	<p>Select the notification that PRTG sends if the defined [value], [scale], and [time] are true <b>and</b> the defined latency is over. You see all notification templates that you have defined under Setup   Account Settings   Notification Templates. Use the search box to filter for notification templates. You can also select no notification to not send a notification in this case.</p> <p> You can also directly create and use new notification templates by clicking  in the dropdown list.</p>
When condition clears, perform [...]	<p>Select the notification that PRTG sends if the defined [value], [scale], and [time] are <b>no longer</b> true <b>and</b> the defined latency is over. You see all notification templates that you have defined under Setup   Account Settings   Notification Templates. Use the search box to filter for notification templates. You can also select no notification to not send a notification in this case.</p> <p> You can also directly create and use new notification templates by clicking  in the dropdown list.</p>

Click  to save your settings or click  to undo your changes.






## Volume Trigger

The volume trigger performs a notification if a sensor reaches a certain volume in a specific time. Hover over  and select Add Volume Trigger from the menu to add a new volume trigger or click  next to a volume trigger to change it.

Volume Trigger    When Other ▾ channel reaches 0    Byte ▾ per Hour ▾, perform no notification ▾


Add Volume Trigger

Setting	Description
When [...] channel	<p>Select the channel whose data PRTG uses for the volume comparison. At root, probe, group, or device level or in libraries, the following channels are available:</p> <ul style="list-style-type: none"> <li>▪ Primary: Use the data of the primary channel of the sensor for the comparison.</li> <li>▪ Total: Use the data of the Total channel of the sensor for the comparison.</li> <li>▪ Traffic In: Use the data of the Traffic In channel of the sensor for the speed comparison.</li> <li>▪ Traffic Out: Use the data of the Traffic Out channel of the sensor for the speed comparison.</li> </ul> <p>At sensor level, the available channels depend on the type of sensor you select.</p> <p> If you set notification triggers at root, probe, group, or device level and you want to know which sensors the notification triggers apply to, see section <a href="#">Available Sensor Types</a> <sup>[3232]</sup>.</p>
reaches [value]	Enter the value to which PRTG compares the channel data. Enter an integer.
[scale]	<p>Select the unit for the [value]:</p> <ul style="list-style-type: none"> <li>▪ Byte</li> <li>▪ KB</li> <li>▪ MB</li> <li>▪ GB</li> <li>▪ TB</li> </ul> <p> [scale] and [time] define the unit for [value]. If the channel data has a different unit, PRTG internally converts the values.</p>
per [time],	Select the time for the scale to create a scale per time unit:

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Hour</li> <li>▪ Day</li> <li>▪ Week</li> <li>▪ Month</li> </ul> <p><b>i</b> [scale] and [time] define the unit for [value]. If the channel data has a different unit, PRTG internally converts the values.</p>
perform [...]	<p>Select the notification that PRTG sends if the defined [value], [scale], and [time] are true. You see all notification templates that you have defined under Setup   Account Settings   Notification Templates. Use the search box to filter for notification templates. You can also select no notification to not send a notification in this case.</p> <p><b>i</b> You can also directly create and use new notification templates by clicking  in the dropdown list.</p>

Click  to save your settings or click  to undo your changes.

## Threshold Trigger



The threshold trigger performs a notification if a sensor reaches specific values. Hover over  and select Add Threshold Trigger from the menu to add a new threshold trigger, or click  next to a threshold trigger to change it.

Threshold Trigger    When Last Sync Result (#)    v channel is Above    v 0    for at least 60 seconds, perform no notification v

When condition clears, perform no notification v

Add Threshold Trigger

Setting	Description
When [...] channel	<p>Select the channel whose data PRTG uses for the threshold comparison. At root, probe, group, or device level or in libraries, the following channels are available:</p> <ul style="list-style-type: none"> <li>▪ Primary: Use the data of the primary channel of the sensor for the comparison.</li> <li>▪ Total: Use the data of the Total channel of the sensor for the comparison.</li> </ul> <p>At sensor level, the available channels depend on the type of sensor you select.</p>

Setting	Description
	<p> The threshold trigger for a Total channel that you define at group or device level or in libraries only applies to the Total channel of traffic sensors. This channel has the ID <b>-1</b>. The threshold trigger works with the Total channel of the following sensors:</p> <ul style="list-style-type: none"> <li>▪ IPFIX</li> <li>▪ IPFIX (Custom)</li> <li>▪ jFlow v5</li> <li>▪ jFlow v5 (Custom)</li> <li>▪ NetFlow v5</li> <li>▪ NetFlow v5 (Custom)</li> <li>▪ NetFlow v9</li> <li>▪ NetFlow v9 (Custom)</li> <li>▪ Packet Sniffer</li> <li>▪ Packet Sniffer (Custom)</li> <li>▪ sFlow</li> <li>▪ sFlow (Custom)</li> <li>▪ SMTP&amp;IMAP Round Trip</li> <li>▪ SMTP&amp;POP3 Round Trip</li> <li>▪ SNMP Traffic (channel Traffic Total)</li> <li>▪ Windows Network Card</li> </ul> <p> If you set notification triggers at root, probe, group, or device level and you want to know which sensors the notification triggers apply to, see section <a href="#">Available Sensor Types</a> <small>[3232]</small>.</p>
is [...]	<p>Select the condition that triggers the notification:</p> <ul style="list-style-type: none"> <li>▪ Above: Trigger the notification if the value of the selected channel exceeds a defined value.</li> <li>▪ Below: Trigger the notification if the value of the selected channel falls below a defined value.</li> <li>▪ Equal to: Trigger the notification if the value of the selected channel is the same as a defined value.</li> <li>▪ Not equal to: Trigger the notification if the value of the selected channel is different than a defined value.</li> </ul>
[value]	<p>Enter the value to which PRTG compares the channel data. Enter values in the smallest (base) unit that is possible, for example, in <a href="#">bytes</a>, <a href="#">milliseconds</a>, or <a href="#">percent</a>. Enter an integer.</p>

Setting	Description
for at least [...] seconds,	<p>Enter the time in seconds that PRTG waits before it sends a notification (<b>latency</b>). This can avoid false alarms if, for example, a sensor changes to the Down status for only a few seconds. Enter an integer.</p> <p><b>i</b> Do not define a latency that is shorter than the scanning interval of a sensor that uses this trigger. The notification trigger might not work as expected in this case.</p>
perform [...]	<p>Select the notification that PRTG sends if the defined channel condition is true <b>and</b> the defined latency is over. You see all notification templates that you have defined under Setup   Account Settings   Notification Templates. Use the search box to filter for notification templates. You can also select no notification to not send a notification in this case.</p> <p><b>i</b> You can also directly create and use new notification templates by clicking <b>+</b> in the dropdown list.</p>
When condition clears, perform [...]	<p>Select the notification that PRTG sends if the defined channel condition is <b>no longer</b> true <b>and</b> the defined latency is over. You see all notification templates that you have defined under Setup   Account Settings   Notification Templates. Use the search box to filter for notification templates. You can also select no notification to not send a notification in this case.</p> <p><b>i</b> You can also directly create and use new notification templates by clicking <b>+</b> in the dropdown list.</p>

Click  to save your settings or click  to undo your changes.



## Change Trigger

**i** Before you set up a change trigger, make sure that you select Trigger 'change' notification in the sensor's settings, otherwise PRTG never sends the notification.

**If Content Changes** **i**     Ignore changes


Trigger 'change' notification


Trigger 'Change' Notification

The change trigger performs a notification if a compatible sensor's value changes. Hover over  and select Add Change Trigger from the menu to add a new change trigger, or click  next to a change trigger to change it.

Change Trigger    When sensor changes, perform **no notification** ▼

Add Change Trigger

Setting	Description
When sensor changes, perform [...]	<p>Select the notification that PRTG sends if a compatible sensor triggers a 'change' notification. You can enable this option in the <a href="#">settings</a> of compatible sensors. You see all notification templates that you have defined under Setup   Account Settings   Notification Templates. Use the search box to filter for notification templates. You can also select no notification to not send a notification in this case.</p> <p><b>i</b> You can also directly create and use new notification templates by clicking  in the dropdown list.</p>




Click  to save your settings or click  to undo your changes.

### Triggers That Can Be Inherited from Parent Objects

You see a list of all notification triggers that the selected object inherits from parent objects. The list is empty and shows the message [\(no triggers defined\)](#) if you have not set any notification triggers for objects that are higher in the [object hierarchy](#) <sup>132</sup>.

Notification triggers that can be inherited from parent objects

Inherit all notification triggers from parent objects and use the notification triggers defined above  
 Only use the notification triggers defined above

Type ^	Rule	Inherited from
State Trigger	When sensor state is Down for at least 600 seconds, perform @ ► Email and push notification to admin (paused) 	 Root
	When sensor state is Down for at least 900 seconds, perform no notification and repeat every 0 minutes	
	When sensor state is no longer Down, perform @ ► Email and push notification to admin (paused) 	

Trigger Inheritance

Setting	Description
Trigger Inheritance	<p>Select the notification triggers that you want to use for the selected object:</p> <ul style="list-style-type: none"> <li>▪ Inherit all triggers from parent objects and use the triggers defined above: Use the inherited notification triggers in section Triggers that can be inherited from parent objects <b>and</b> use the specific triggers for this object in section Notification Triggers. To change settings of the inherited notification triggers, click the name of the monitoring object in the column Inherited from to open its Overview tab and then open the Notification Triggers tab.</li> <li>▪ Only use the triggers defined above: Do not use the inherited notification triggers in section Triggers that can be inherited from parent objects. Only use the triggers that you define for this object in section Notification Triggers.</li> </ul> <p><b>i</b> This setting is valid for all notification triggers that you see here. It is not possible to select only some of the notification triggers.</p>

Setting	Description
	<p><b>i</b> You can also click a notification template to edit its settings or click the object under Inherited from to go to the object's Overview tab.</p>

## Triggers That Are Defined in Libraries

You see a list of all notification triggers that are set in libraries <sup>2738</sup> that contain the selected sensor. The list is empty and shows the message **(no triggers defined)** if you have not set any notification triggers in libraries that contain the selected sensor.

Notification triggers that are defined in libraries

Type <sup>▲</sup>	Rule	Inherited from
State Trigger	When sensor state is Down for at least 60 seconds, perform no notification When sensor state is Down for at least 300 seconds, perform no notification and repeat every 0 minutes When sensor state is no longer Down, perform no notification	All disk space sensors

If you want to change these notification triggers, remove the sensor from the library or edit the notification triggers on the library's Notification Triggers tab.

Triggers in Libraries

Click a notification template to change its settings. Click a library in the column Inherited from to view the library.

**i** You cannot disable notification trigger usage from a library here. If you do not want to use notification triggers from a library for the selected sensor, open the library and remove the sensor from it or edit the notification triggers on the Notification Triggers <sup>2749</sup> tab of the library.
















# Part 8

# Advanced Procedures

## 8 Advanced Procedures

The following sections introduce more advanced features and procedures of PRTG.

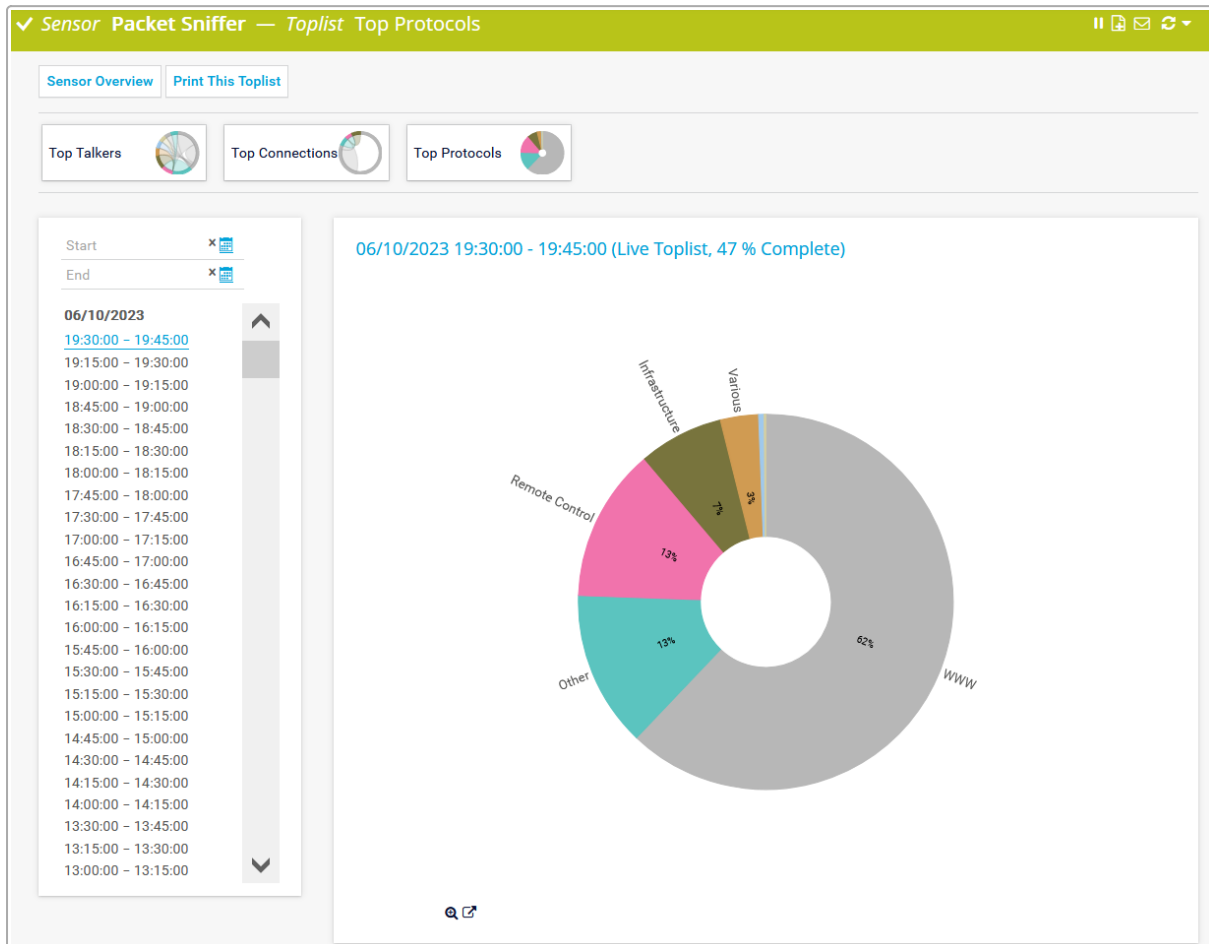
In this section:

- [Toplists](#) 
- [Move Objects](#) 
- [Clone Object](#) 
- [Multi-Edit](#) 
- [Create Device Template](#) 
- [Show Dependencies](#) 
- [Geo Maps](#) 
- [Notifications](#) 
- [Libraries](#) 
  - [Library Management](#) 
  - [Libraries and Node Settings](#) 
  - [Library Context Menus](#) 
- [Reports](#) 
  - [Run Reports](#) 
  - [Report Settings](#) 
- [Maps](#) 
  - [Map Designer](#) 
  - [Maps Settings](#) 
  - [Map Rotation](#) 
- [Setup](#) 
  - [Account Settings](#) 
  - [System Administration](#) 
  - [PRTG Status](#) 
  - [License Information](#) 
  - [Auto-Update](#) 
  - [Optional Downloads](#) 
  - [Help and Support Center](#) 
  - [Contact Support](#) 



## 8.1 Toplists

Packet Sniffer sensors and Flow (NetFlow, jFlow, sFlow, IPFIX) sensors not only measure the total bandwidth usage, but also break down traffic by IP address, port, protocol, and other parameters. This way, PRTG can tell which IP address, connection, or protocol uses the most bandwidth. PRTG shows the results in [Toplists](#).



Toplist Top Protocols for a Packet Sniffer Sensor

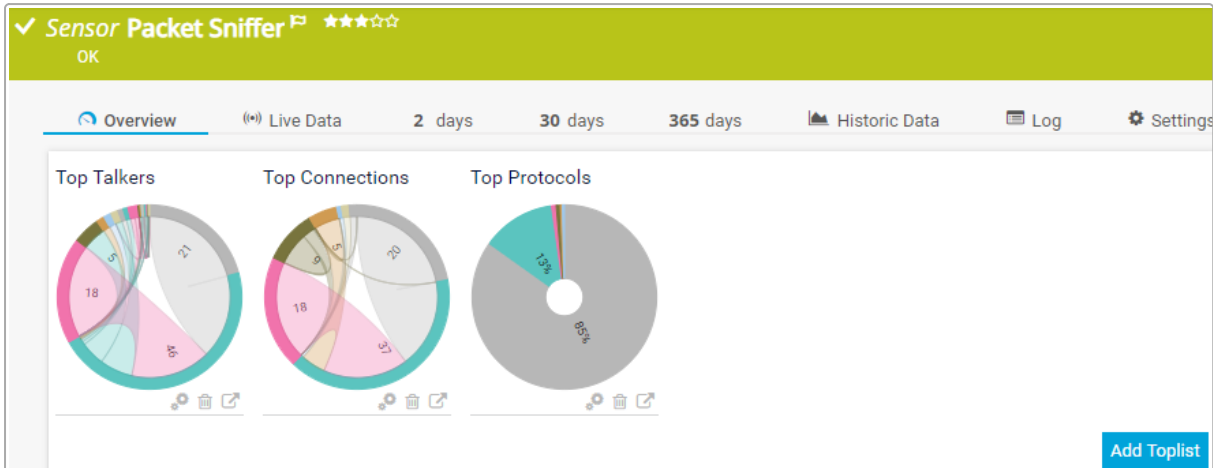
### Toplist Storage

PRTG looks at all network packets and collects the bandwidth information for all IP addresses, ports, and protocols. This creates a huge amount of analysis data. To reduce the amount of data that is actually stored, PRTG only stores the top 100 entries of each Toplist in the database at the end of a specified Toplist period by default.

### Toplist Overview

Toplists are only available for [Flow and Packet Sniffer sensors](#) <sup>[3232]</sup>. PRTG displays Toplist on the sensor's Overview tab.

■ For more information about the Overview tab, see the Knowledge Base: [What options do I have to review my monitoring data in detail?](#)




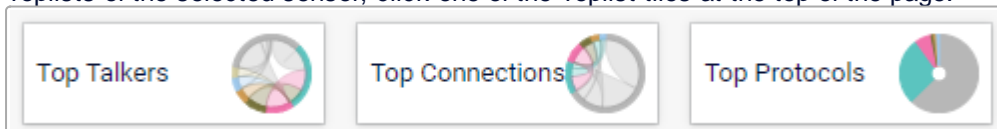
Toplist Overview for a Packet Sniffer Sensor

By default, there are three preconfigured Toplists:

Toplist	Description
Top Talkers	Shows bandwidth usage by IP address.
Top Connections	Shows bandwidth usage by connection.
Top Protocols	Shows bandwidth usage by protocol.

### Working with Toplists

- Click one of the Toplist names on the sensor's Overview tab or click  below a Toplist to view a distribution chart and a list of source IP addresses and destination IP addresses, source ports and destination ports, protocols, or kinds of traffic in different channels, for example. What kind of information is available depends on the selected Toplist.
  - Click an entry in the Toplist periods list on the left side to view data for a specific time period. The default value is 15 minutes. You can also manually define the start and end time of the Toplist period that you want to view. Use the date time picker to enter the date and time. Additionally, several [table list options](#) <sup>[218]</sup> are available.
  - Click Print This Toplist to view a printer-friendly version of your Toplist and use the print dialog of your browser to print the Toplist.
  - Click Sensor Overview to return to the selected sensor's Overview tab. For a quick selection of other Toplists of the selected sensor, click one of the Toplist tiles at the top of the page.









Toplist Tiles

- Click Add Toplist on the sensor's Overview tab to create a new Toplist. The available options are the same as when you [edit](#) <sup>[2709]</sup> a Toplist.

- Click  below a Toplist on the sensor's Overview tab and confirm with Delete to delete the Toplist.

## Edit Toplists

Click  below a Toplist on the sensor's Overview tab to modify a Toplist.

Setting	Description
Name	<p>Enter a name to identify the Toplist.</p> <p> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Toplist Type	<p>Select the type of Toplist:</p> <ul style="list-style-type: none"> <li>▪ Top Talkers (IP address): Shows bandwidth usage by IP address.</li> <li>▪ Top Connections: Shows bandwidth usage by connection.</li> <li>▪ Top Protocols: Shows bandwidth usage by protocol.</li> <li>▪ Custom: Create your own Toplist by selecting one or more Toplist fields.</li> </ul>
Toplist Fields	<p><a href="#">This setting is only visible if you select Custom above.</a></p> <p>Select the fields that you want to add to the Toplist by enabling the check box in front of the respective field name. The available options depend on the sensor. They are different for Packet Sniffer, NetFlow v5, NetFlow v9, IPFIX, and sFlow sensors.</p> <p> For performance reasons, only select the fields that you really need to monitor.</p> <p> For more information, see section <a href="#">Performance Considerations</a> <sup>2710</sup>.</p>
Toplist Period (Minutes)	<p>Define the time span that a Toplist period covers in minutes. Enter an integer. When a Toplist period is finished, PRTG stores the top results and starts a new Toplist period.</p> <p> To avoid load problems on the probe system, do not set this time period too long. The default value is 15 minutes.</p> <p> For more information, see section <a href="#">Performance Considerations</a> <sup>2710</sup>.</p>
Top Count	<p>Define the length of your Toplist. PRTG stores only this number of entries for each Toplist period. Enter an integer.</p> <p> To avoid load problems on the probe system, set this value as low as possible. The default setting is 100 to store the top 100 entries for each Toplist period.</p>

Setting	Description
	<p>■ For more information, see section <a href="#">Performance Considerations</a> <small>2710</small>.</p>
Reverse DNS Lookup	<p>Define if you want to do a reverse Domain Name System (DNS) lookup for IP addresses that are stored in the Toplist:</p> <ul style="list-style-type: none"> <li>▪ Reverse DNS lookup for IP addresses: Determine the domain name that is associated with an IP address and show it in the Toplist.</li> <li>▪ No reverse DNS lookup: Only show IP addresses. Select this option to increase performance.</li> </ul>
Data Transfer	<p>Define how the probe sends the Toplist data set to the PRTG core server:</p> <ul style="list-style-type: none"> <li>▪ According to scanning interval (default): Send data in the scanning interval defined in the settings of the sensor for which you create this Toplist. <ul style="list-style-type: none"> <li>ⓘ This setting can create a lot of bandwidth usage and CPU load if you have many Packet Sniffer sensors, complex traffic, or long Toplists.</li> </ul> </li> <li>▪ At end of Toplist period: Send data once a Toplist period is finished. <ul style="list-style-type: none"> <li>ⓘ This setting creates less bandwidth usage and CPU load, but you cannot see the data of the <b>current</b> Toplist in the PRTG web interface. You can only see Toplists with finished time periods.</li> </ul> </li> </ul> <p>■ For more information, see section <a href="#">Performance Considerations</a> <small>2710</small>.</p>
Memory Limit (MB)	<p>Define the maximum amount of memory (in megabytes) that the probe uses to collect the different connection information. Every Toplist adds its amount of used memory to the probe's memory consumption. Increase this value if the number of captured connections is not sufficient. Enter an integer.</p>

ⓘ Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

## Performance Considerations

If you create Toplists for data lines with considerable usage (for example, steady bandwidth over 10 megabits per second) or if the traffic is very diverse (for example, many IP addresses or ports with only little traffic each), consider the following aspects:

- The probe gathers all information that is needed for the Toplist in RAM during each Toplist period. By default, only the top 100 entries are transferred to the PRTG core server. Depending on the Toplist type and the traffic patterns, the required memory can consume many megabytes.
- Define Toplist periods that are as short as possible to minimize memory usage. This is especially important when the traffic is highly diverse.

- Memory requirements can grow almost exponentially with each Toplist field that you use in the Toplist definition (depending on the traffic pattern). Avoid complex Toplists for high and diverse traffic. For example, the Toplist Top Connections with 5 Toplist fields needs a lot more memory than the Toplist Top Talkers with 1 Toplist field.
- If you notice a high bandwidth usage between the PRTG core server and the probe, try the At end of Toplist period option in the [Toplist settings](#)<sup>[2709]</sup>.
- If you get [Data incomplete, memory limit was exceeded](#) messages, try to increase the memory limit in the Toplist settings but keep an eye on the memory usage of the probe process.
- To increase the performance of a Toplist, disable the reverse DNS lookup setting.

## Notes

- When you work with Toplists, be aware that privacy issues can come up for certain configurations of this feature. Using Toplists, you can track all single connections of an individual system to the outside world and you must make sure that it is legal for you to configure PRTG like this.
- Keep in mind that Toplists can be viewed in the PRTG web interface. You might not want to show lists of domains that are used in your network to others, so restrict [access rights](#)<sup>[145]</sup> to sensors that have Toplists.
- Toplist charts, for example for top connections, are not meant to be used for detailed analysis. Instead, they should indicate if there is an uncommon, bigger change in this Toplist.

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

What options do I have to review my monitoring data in detail?

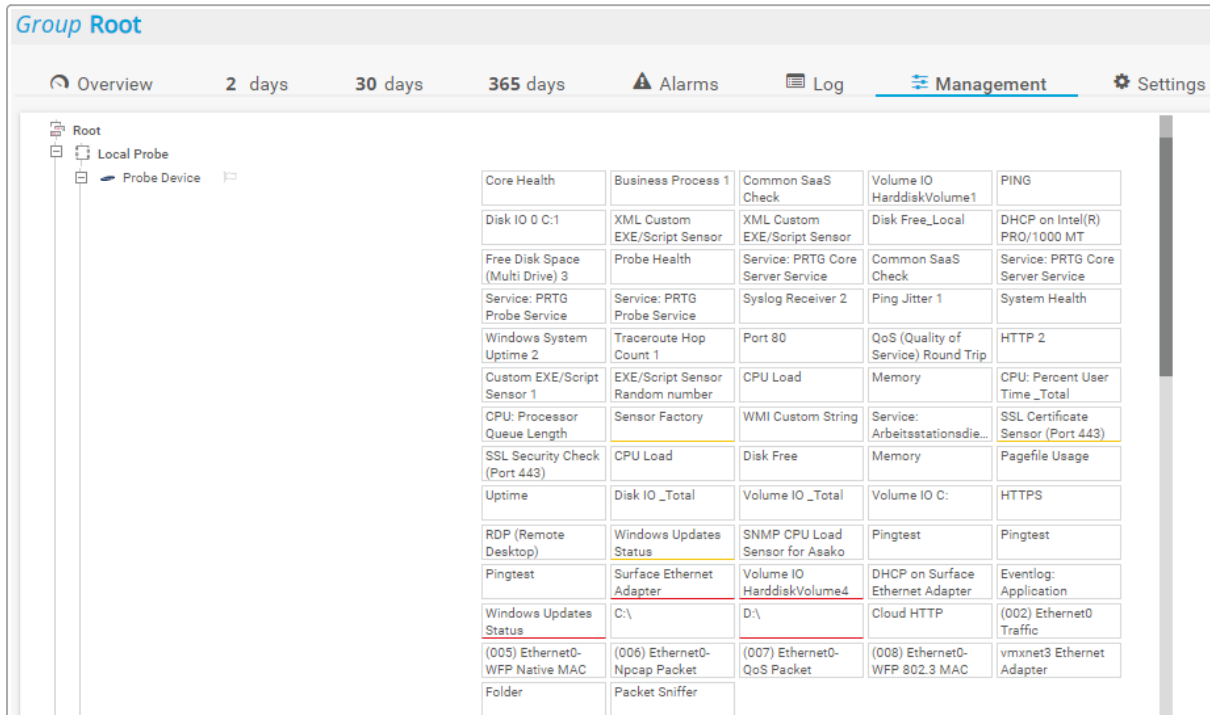
- <https://kb.paessler.com/en/topic/90007>

## 8.2 Move Objects

There are several options for moving objects in the device tree or for moving objects from one probe or group to a different probe or group.

### Probes or Groups: Management Tab

The Management tab is available when you view probes or groups. After you click this tab, you can directly move devices and sensors in the device tree via drag-and-drop.



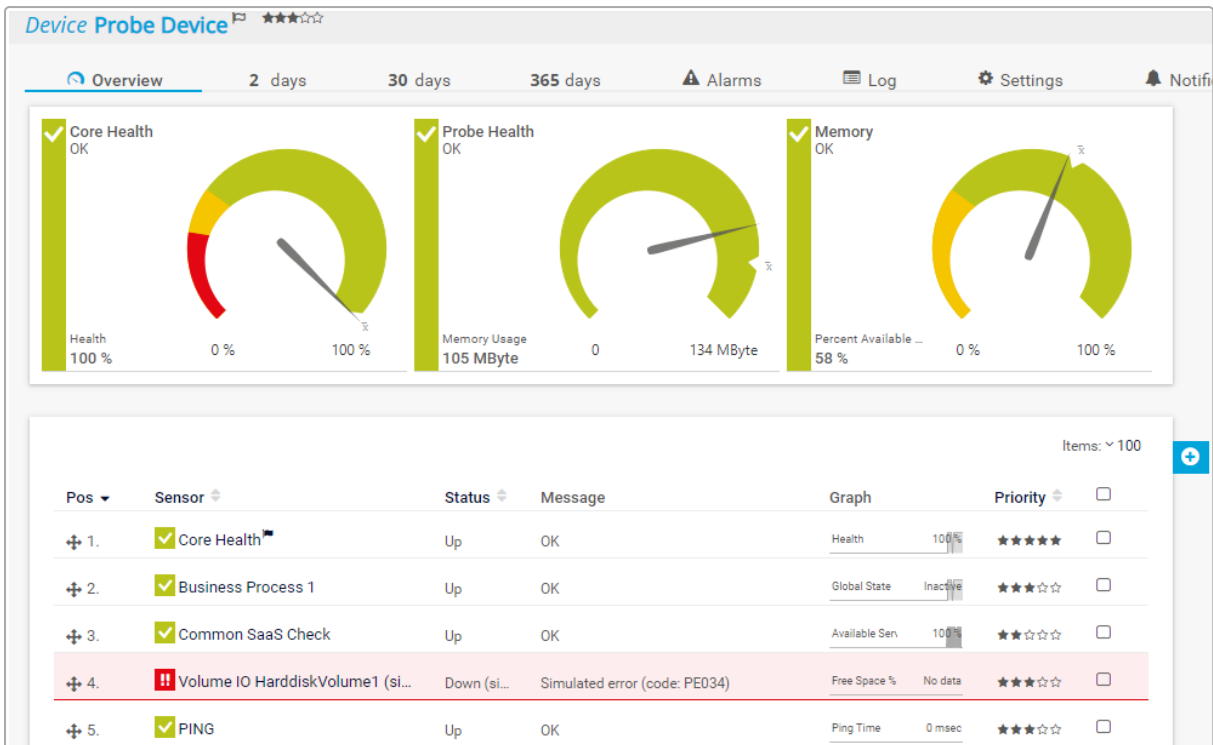
Move Objects on a Probe or Group

**i** If it is not possible to move an object, PRTG automatically starts a [clone](#) process.

**■** For more information, see section [Manage Device Tree](#).

### Devices: Overview Tab

When you view the Overview tab of a device, you see a list of all sensors on the device.

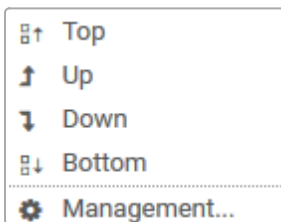


Move Sensors on a Device

Click the column headers Pos, Sensor, Status, or Priority to sort the sensor list. To change a sensor's position, click **+** at the beginning of the row, drag the sensor to the new position, and drop it.

### Context Menu: Move Option

Right-click any object in the device tree to show its [context menu](#). Hover over Move to open the Move menu. The following actions are available:



Move Context Menu

- Top: Move the object to the top of the parent object.
- Up: Move the object one entry up.
- Down: Move the object one entry down.
- Bottom: Move the object to the bottom of the parent object.
- Open the Management [tab](#) of the object. This setting is only available for probes and groups.

## 8.3 Clone Object

If you want to duplicate an object with the same settings, you can clone it. Cloning is available for groups, devices, and sensors.

### Rules

The following rules for cloning apply:

- The new object takes over all settings of the original object. This means, for example, that an [auto-discovery](#)<sup>[254]</sup> starts automatically on a cloned device if this setting is enabled on the original device.
- A cloned device contains all objects of the original device, regardless of whether they produce working sensors or not. This often depends on the settings of the cloned device.  
① This behavior is different from [creating a device template](#)<sup>[2725]</sup>.
- Cloned sensors initially show the Paused [status](#)<sup>[227]</sup> to give you the chance to change any settings before monitoring starts. Check the settings and [resume](#)<sup>[227]</sup> monitoring.
- You cannot clone [fixed](#) objects such as the root group, a probe device, or PRTG system-internal sensors.
- The [user account](#)<sup>[2901]</sup> that clones an object must have at least [read access](#)<sup>[145]</sup> to this object and all objects underneath in the [object hierarchy](#)<sup>[132]</sup>. The user group to which this user account belongs must have the [permission](#)<sup>[2914]</sup> to create all sensors that run on the device or group that they want to clone.

### Clone an Object

Right-click an object in the device tree and select Clone from the [context menu](#)<sup>[229]</sup> to open an assistant.

① If you want to clone a [sensor](#), a faster way is to manage the [manage device tree](#)<sup>[418]</sup>.





## Duplicate Sensors by Cloning

To duplicate a sensor by creating a clone of the sensor, select a parent device and enter a new name for the sensor.



**Note:** After you clone a sensor, PRTG sets the new sensor to the **Paused** status so that you can edit the sensor's settings before you actually start monitoring.

### Sensor to Be Cloned


Parent Probe

 Local Probe (Local Probe) 

Parent Group

 Local Probe (Local Probe) 

Parent Device

 Probe Device

Sensor


Business Process

### Name for New Sensor

New Sensor Name

Clone of Business Process

### Parent Device for New Sensor

Select the device to which you want to add the sensor clone.  



Cancel

Continue

Clone Dialog for a Sensor

## Clone Object Settings

[Object] To Be Cloned

Several fields show information about the object that you want to clone. The available information varies depending on whether you clone a group, a device, or a sensor.

Name for New [Object]

Enter information for the new object as described below.

Field	Description
New [Object] Name	<p>Enter a name for the new object to identify it later, for example, in the device tree or in table lists. By default, PRTG uses the old name with the prefix <a href="#">Clone of</a>.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({}). For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
New IP Address/DNS Name	<p><a href="#">This setting is only available when you clone a device.</a></p> <p>Enter the IP address or Domain Name System (DNS) name for the new device.</p>
Service URL	<p><a href="#">This setting is only available when you clone a device.</a></p> <p>Specify a URL that you want to open directly when you select Device Tools   Go to Service URL from the context menu of the device. For example, you can configure this option to call the address <a href="http://www.example.com/service.html">http://www.example.com/service.html</a>. Enter a valid URL or leave the field empty.</p>

Parent [Object] for New [Object]

Use the [object selector](#)<sup>[222]</sup> to select the object to which you want to add the cloned object. If you clone a group or a device, select a group. If you clone a sensor, select a device.

Click Continue to clone the object.

## Results

After you clone an object, you can see the following:

- If you clone a sensor, the Overview tab of the new sensor opens.
- For more information about the Overview tab, see the Knowledge Base: [What options do I have to review my monitoring data in detail?](#)
- If you clone a group or a device, you stay on the same page.
- Cloned sensors initially show the Paused [status](#)<sup>[227]</sup> to give you the chance to change any settings before monitoring starts. Check the settings and [resume](#)<sup>[227]</sup> monitoring.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## 8.4 Multi-Edit

[Table lists](#) <sup>[218]</sup> offer the multi-edit feature. With this, you can bulk edit the properties of many objects. Multi-edit is also available on the Management tab of probes or groups when you hold down the Ctrl key to select multiple objects. See also section [Manage Device Tree](#) <sup>[418]</sup>.

**i** You cannot change every setting with multi-edit. PRTG only displays settings that all selected objects have in common.

Log Entries					
Date Time	Parent	Type	Object	Status	Message
05/10/2023 14:08:58	Probe Device	Local Folder (BETA)	Local Folder	Up	0 #
05/10/2023 14:08:53	Probe Device	FortiGate VPN Overview (...)	FortiGate VPN Overview	Down	The sensor could not authenticate again
05/10/2023 14:07:21	Example Device 1	SNMP Traffic 32bit	(019) Ethernet0-WFP 802.3 MAC Layer ...	Up	0,04 Mbit/s
05/10/2023 14:07:19	192.0.2.0	SNMP Traffic 32bit	(019) Ethernet0-WFP 802.3 MAC Layer ...	Up	0,34 Mbit/s
05/10/2023 14:07:18	Probe Device	System Health	System Health	Up	100 %
05/10/2023 14:07:16	Example Device 2	SNMP Traffic 32bit	(018) Ethernet0-QoS Packet Scheduler...	Up	0,34 Mbit/s
05/10/2023 14:07:15	Example Device 3	SNMP Traffic 32bit	(018) Ethernet0-QoS Packet Scheduler...	Up	0,04 Mbit/s
05/10/2023 14:07:13	Probe Device	Windows Network Card	vmxnet3 Ethernet Adapter	Up	0,08 Mbit/s
05/10/2023 14:07:03	192.0.2.0	SSL Certificate	SSL Certificate Sensor (Port 443)	Down	-92 # (Days to Expiration) is below the t...
05/10/2023 14:07:00	Example Device 1	SNMP Traffic 32bit	(016) Ethernet0-WFP Native MAC Layer...	Up	0,04 Mbit/s

### Multi-Edit in Table Lists

In a table list, you can select several objects by enabling the check boxes on the right. You can also select all objects on the page at once by enabling the check box in the table header.

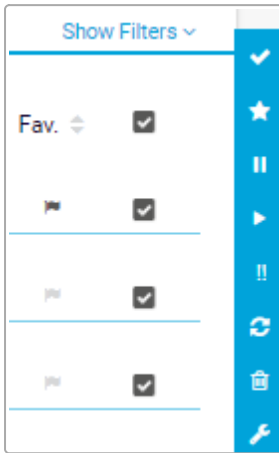
**i** Selecting all objects via the check box in the table header does not select all objects across multiple pages. It only selects all objects on the first page in most cases.

Sensors									
Sensor	Probe Group Device	Status	Last Value	Message	Graph	Priority	Fav.	Perf. Impact	<input type="checkbox"/>
<input checked="" type="checkbox"/> (001) Alias 1 Traffic	Local Probe (Local Probe) Sensors » 192.0.2.0	Up	92 kbit/s	OK	Traffic Total 92 kbit/s	★★★★★	F3		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Cluster Health	Cluster Probe Devi...	Up	0 #	OK	Outbound Clu 0 #	★★★★★	F3		<input type="checkbox"/>
<input checked="" type="checkbox"/> Core Health	Local Probe (Local Probe) Probe Device	Up	100 %	OK	Health 100 %	★★★★★	F3		<input type="checkbox"/>
<input checked="" type="checkbox"/> Core Health	Cluster Probe » Cluster Probe Devi...	Up	100 %	OK	Health 100 %	★★★★★	F3		<input type="checkbox"/>
<input checked="" type="checkbox"/> Memory	Local Probe (Local Probe) Probe Device	Up	42 %	OK	Percent Avail: 42 %	★★★★★	F3		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Ping	Local Probe (Local Probe) Group Auto » Example	Up	1 msec	OK	Ping Time 1 msec	★★★★★	F3		<input checked="" type="checkbox"/>

Example of a Table List with Some Selected Objects

Use the Items option in the upper-right corner to view more items per page.

When you select one or more objects, the multi-edit menu appears in which different functions are available. The available menu options depend on the selected objects. For sensor lists, for example, some frequently used functions are Pause (⏸), Resume (▶), Scan Now (🔄), Delete (🗑), or Settings (⚙). Click a button to apply the respective function to all selected objects.



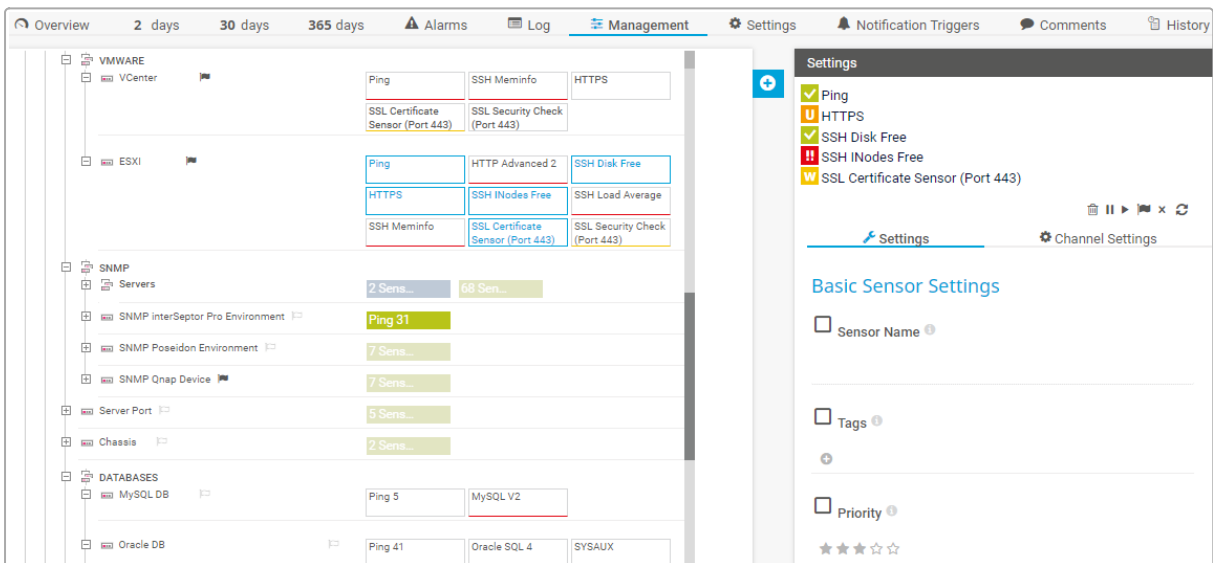
Multi-Edit Menu

### Multi-Edit on the Management Tab

The Management tab is available for probes and groups.


You can use multi-edit for object settings:

- Hold down the Ctrl key and select multiple objects of the same type, for example, multiple groups, devices, or sensors.
- In the dialog that appears, select the properties that you want to edit, change the respective settings, and click Save. The changes are applied to all selected objects.



Multi-Edit on the Management Tab

## Edit Object Settings

Click  in the multi-edit menu to open the Edit Multiple Objects dialog. This dialog shows most of the settings that the selected objects have in common. For example, you can edit the name, tags, priority, scanning interval, or access rights. The available options depend on the selected objects.

### Editing 2 Objects ✕

#### Edit Multiple Objects

Here you can edit one or more settings for selected objects of the same type, for example, groups, devices, or sensors. Enable the check box next to the settings that you want to change for all selected objects and enter or select a new value.

You are editing 2 objects (Show all objects):

#### Basic Device Settings

Device Name ⓘ

---

Monitoring Status ⓘ

Started (default)

Paused

IP Version ⓘ

IPv4 (default)

IPv6

IPv4 Address/DNS Name ⓘ

---

IPv6 Address/DNS Name ⓘ

---

Tags ⓘ

+


---


Priority ⓘ


★ ★ ★ ☆ ☆


#### Additional Device Information


Device Icon ⓘ

























































Cancel OK

Example of Device Settings in Multi-Edit Mode

To change a property, enable the check box in front of the respective setting and then change the setting. New settings are applied to all selected objects. All properties with a disabled check box remain unchanged.

 If you multi-edit tags, PRTG overwrites existing tags.

 Click OK to save your settings. If you close the dialog without saving, all changes to the settings are lost.

## Edit Channel Settings

The Channel Settings tab in the Edit Multiple Objects dialog is only available when you edit multiple sensors. The available settings depend on the selected sensors. You can edit the settings of all channels that the selected sensors have in common. Select a channel name from the Channel list. You can then edit display settings, colors, scaling, and limits, for example.



**Editing 2 Objects**
✕

---

### Edit Multiple Objects

This page allows to edit one or more settings for a selection of objects (groups, devices, sensors, etc.). First enable the checkbox in the first column for each setting that you want to change for all selected objects. Then enter/select your new value.

You are editing 2 objects (Show all objects):

⚙ Settings
← Channel Settings

### Select Channel

Channel

- Downtime (ID -4)
- Ping Time (ID 0)
- Minimum (ID 1)
- Maximum (ID 2)
- Packet Loss (ID 3)

---

### Edit Channel ""

- Graph Rendering** ⓘ
  - Show in Graphs
  - Hide from Graphs
- Table Rendering** ⓘ
  - Show in Tables
  - Hide from Tables
- Line Color** ⓘ
  - Automatic
  - Manual
- Line Width** ⓘ
  - 1

Cancel
OK

Example of Channel Settings in Multi-Edit Mode

To change a property, enable the check box in front of the respective setting and then change the setting. New settings are applied to all selected objects. All properties with a disabled check box remain unchanged.

❗ Click OK to save your settings. If you close the dialog without saving, all changes to the settings are lost.

## More

### ■ KNOWLEDGE BASE

Why are my credentials suddenly resulting in an error?

- <https://kb.paessler.com/en/topic/91883>

## 8.5 Create Device Template

To add a specific device several times, you can create a device template from this device. When you create a device template, PRTG saves information for nearly all sensors on this device to a template file that you can later use in combination with the [auto-discovery](#) (restrictions apply for a few sensors). Custom device templates are also available in the [PRTG Sensor Hub](#).

In the device template, PRTG saves all relevant [sensor settings](#) except for settings that you set on other objects, such as [schedules](#), [notification triggers](#), and [access rights](#). PRTG automatically sets these settings to inherited settings.

To create a device template, right-click a device in your device tree. From the [context menu](#), select Create Device Template to open the Create Device Template dialog.

**Create Device Template for Probe Device**
✕

### Create Device Template

To create a device template that you can use for auto-discovery, you have to provide a template name in clear text. PRTG uses this name in the template list in the auto-discovery assistant. A device template contains an entry for every sensor of the selected device. This entry includes all relevant sensor settings except settings that refer to other objects like schedules, triggers, or access rights. PRTG reverts these settings to inherited settings when you create a sensor via a device template.

**Note:** There are sensors that you cannot save in a device template. For a list of these sensors, see the [PRTG Manual: Create Device Template](#).

### Enter Template Name

Template Name ⓘ

You can exclude sensors from the device template. Enable the check box in front of a sensor that you want to exclude.

**Note:** Sensors that you cannot save in a device template do not appear in this list.

**Note:** Sensors that dynamically scan for available monitoring items when you add the sensor to a device do not appear in this list. PRTG automatically includes these sensors in the device template if they support the device template functionality. You cannot exclude these sensors from the device template.

Exclude Sensors

🔍

▲ Sensors

---

✔ CPU Load

✔ Disk Free

✔ HTTPS

✔ Memory

✔ Pagefile Usage

Cancel
OK

Create Device Template Assistant

## Template Settings

Setting	Description
Template Name	<p>Enter a display name to identify the device template.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Exclude Sensors	<p>Enable the check box in front of the sensors that you want to exclude from the device template.</p> <p><b>i</b> Sensors that you cannot save in device templates do not appear in this list.</p> <p><b>i</b> Sensors that dynamically scan for available monitoring items when you add the sensor to a device do not appear in this list. PRTG automatically includes these sensors in the device template if they support the device template functionality. You cannot exclude these sensors from the device template.</p>

**i** Click OK to save your settings. If you close the dialog without saving, all changes to the settings are lost.

**i** Device templates only save the sensors on the device and the sensors' settings including the [channel settings](#)<sup>[26831]</sup>. They do not save the device itself or the device's settings. To successfully create a device template, you must add sensors to the device (either [manually](#)<sup>[414]</sup> or via the auto-discovery) and the sensors must be [device template capable](#)<sup>[2727]</sup>.

After you save your device template file, you see a message where you can review the sensors that the new device template contains. Click OK to finish. PRTG stores the device template in the \devicetemplates subfolder of the [PRTG program directory](#)<sup>[3213]</sup>. Your device template file contains all sensors of the original device, including the sensors' settings.

Before the next auto-discovery, choose the Auto-discovery with specific device templates setting and select the name of your new device template from the list. PRTG then tries to discover the stored sensors. If the physical device answers to a sensor request, the sensor is added to the respective device in PRTG.

**■** For more information, see section [Auto-Discovery](#)<sup>[254]</sup>.

## Restrictions

There are a few settings that you cannot save in a device template so PRTG uses the default settings:

- The Dependency Type setting Master sensor for parent in the Schedules, Dependencies, and Maintenance Window section,
- The Result Handling setting Store result because this setting is only intended for debugging purposes,
- Settings in the Access Rights section to avoid security flaws, and

- Notification triggers settings that you set on other objects, for example, a device or group. PRTG saves, however, notification triggers settings that you set directly on a sensor.
- ⓘ In general, you cannot save all sensor settings and channel settings (for example, channel limits of dynamically created channels) of sensors that dynamically scan for available monitoring items when you add the sensor.

Furthermore, because of internal restrictions, PRTG does not save every sensor in a device template.

- For an overview list of all sensors, including their device template capability see section [Available Sensor Types](#) <sup>B232</sup>.

## Device Template Updates

Once a device template is created, it is not possible to add additional sensors to it via the PRTG web interface. If you want to create a device template with an extended set of sensors, you need to create a new template.

- ⓘ When you save a new device template, PRTG updates all internal sensor IDs in this template. Because of this, PRTG creates all sensors that the new device template contains anew on the device to which you apply the template, even if the same sensors have already been created on this device with a different device template.

- ⓘ You cannot delete device templates via the PRTG web interface.

- ☁ You cannot edit device template files in PRTG Hosted Monitor but you can upload the updated device template again. For more information, see section [Manage a PRTG Hosted Monitor Subscription](#).

## Device Template Filtering

You can include and exclude sensors from existing device templates. For more information, see the Knowledge Base: [How can I include and exclude sensors from device templates?](#)

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

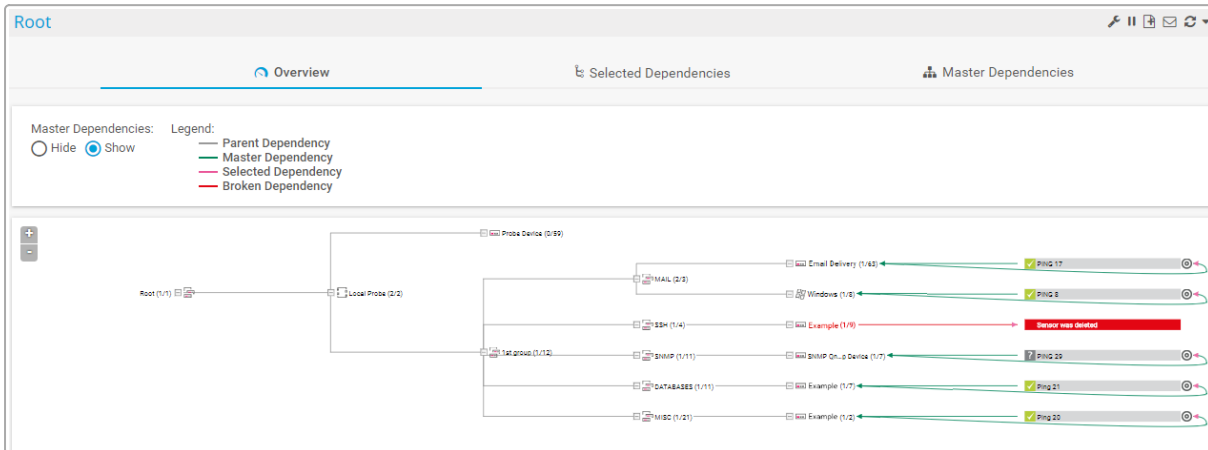
How can I include and exclude sensors from device templates?

- <https://kb.paessler.com/en/topic/89025>

## 8.6 Show Dependencies

The [Dependencies](#) <sup>140</sup> feature gives an overview of the dependencies that are configured for the objects in your setup.

To see an object's dependencies, select Devices | Dependencies from the [main menu bar](#) <sup>238</sup>.



Dependencies Graph View





Tab	Description
Overview	Shows the <a href="#">dependencies graph</a> <sup>2728</sup> . This is a visualization of device, group, and sensor dependencies. <b>i</b> To show the dependencies graph, you need to access the PRTG web interface as an administrator.
Selected Dependencies	Shows a table list of manually set dependencies (see the Dependency setting in section Schedules, Dependencies, and Maintenance Window in any object's settings).
Master Dependencies	Shows a table list of master dependencies.

### Dependencies Graph

The Overview [tab](#) <sup>170</sup> shows the device tree in the dependencies graph view. The lines in the dependencies graph symbolize dependencies between the monitoring objects in the device tree. Additionally, PRTG uses different [line colors](#) <sup>2729</sup> for the dependencies. You can also view the dependencies in different table lists on the Selected Dependencies tab or the Master Dependencies tab.

**i** To show the dependencies graph, you need to access the PRTG web interface as an administrator.

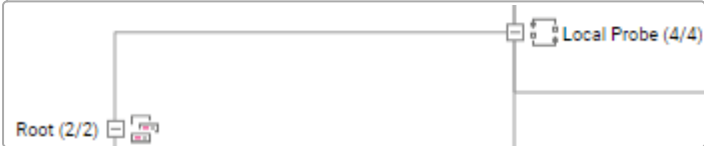


The following actions are available:


- Enable the Show or Hide option to show or hide master dependencies. Hide is enabled by default to only show parent dependencies, selected dependencies, and broken dependencies.
  - ⓘ For technical reasons, the Show and Hide radio buttons are not available in Internet Explorer. Use Google Chrome 75 or Mozilla Firefox 67 instead.
- Click  or  in the upper-left corner to zoom in or out of the dependencies graph.
- Click probe and group nodes to show the respective dependencies.
- Click device or sensor nodes to open the corresponding Overview tab.
- Click  or  to expand or collapse probe and group nodes.
- The numbers in parentheses indicate how many child nodes of an object are shown.

### Legend of Dependencies Graph

The line's colors show the kind and source of a dependency. This represents the Dependency Type as defined in the Schedules, Dependencies, and Maintenance Window settings of a [probe](#)<sup>[514]</sup>, [group](#)<sup>[588]</sup>, [device](#)<sup>[659]</sup>, or [sensor](#).

ⓘ You can also find the legend for the line colors in the graph header bar.

Color	Description
Gray	<p>Gray lines show a dependency by inheritance (Use parent (default) setting). The source of the dependency is the parent object on the left end of the line, for example, <a href="#">Root</a> is the parent of <a href="#">Local Probe</a>.</p>  <p style="text-align: center;">Gray Line for Parent Dependency</p>
Green	<p>Green lines show a master dependency for a device (Master sensor for parent setting). The sensor that is set as the master points to the dependent device with a green arrow head at the line's end. The arrow head from the dependent device to its master sensor is pink.</p>  <p style="text-align: center;">Green Line for Master Dependency</p>
Pink	<p>Pink lines show a dependency that you set manually (Select a sensor setting). The source of the dependency points to the dependant with a pink arrow at the line's end.</p>  <p style="text-align: center;">Pink Line for Selected Dependency</p>

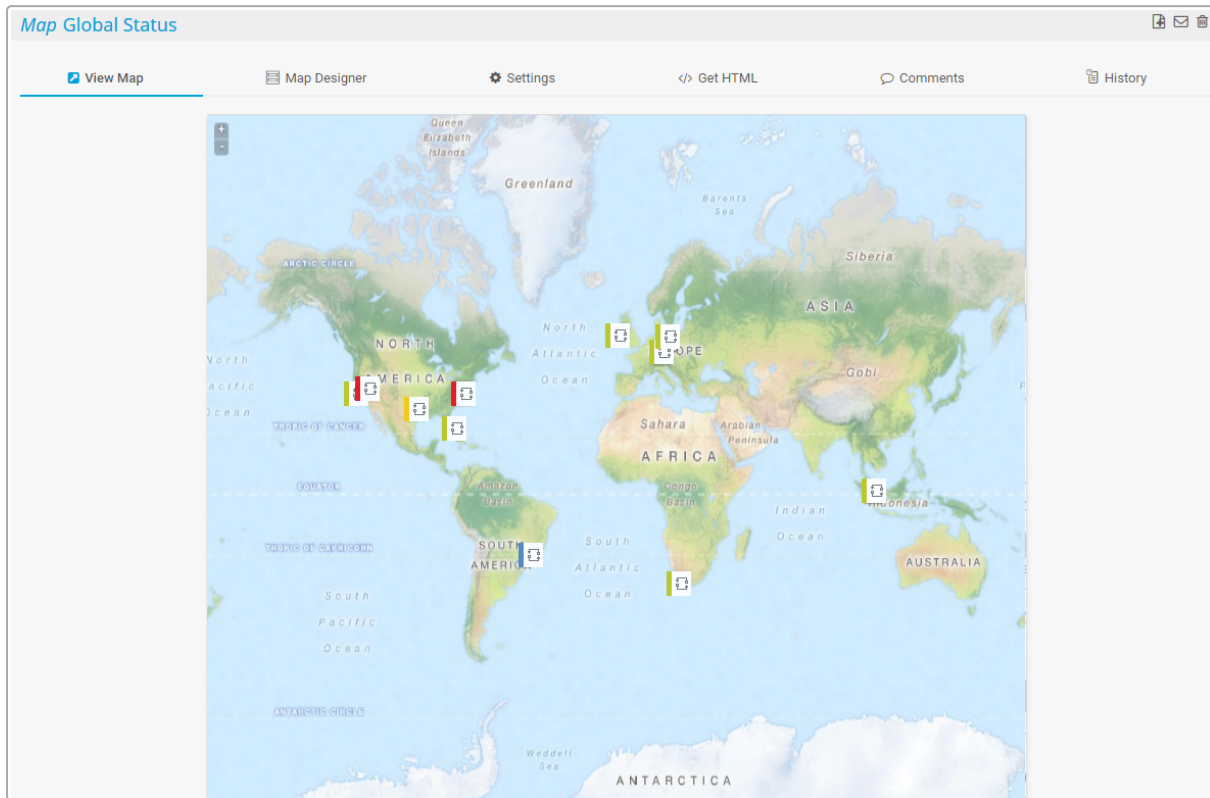
Color	Description
Red	<p>Red lines indicate broken dependencies, for example, if the master sensor is not available.</p>  <p>Red Line for Broken Dependency</p>



## 8.7 Geo Maps

With the [Geo Maps](#) feature, you can visualize geographical information about monitored objects that are located at different sites worldwide on one page. You can display the location of probes, groups, and devices in a geographical map on the Overview tab of an object or in [Maps](#)<sup>[2776]</sup>.

■ For more information about the Overview tab, see the Knowledge Base: [What options do I have to review my monitoring data in detail?](#)



Global Status of a Network in a Geographical Map

### Prerequisites


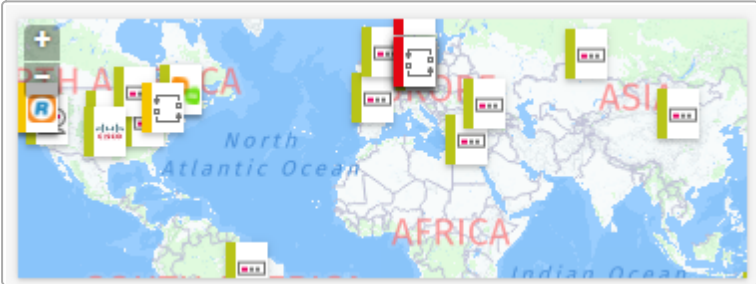
To use geographical maps and view them in the PRTG web interface, make sure that your PRTG core server has access to the internet to obtain map tiles. If a proxy is mandatory in your network, configure the according proxy settings.

■ For more information, see section [Core & Probes](#)<sup>[2888]</sup>.

■ For more information about map tile server domains, see the Knowledge Base: [Which domains and ports does the Geo Maps feature use?](#)

### Geo Maps Concepts

The Geo Maps feature works as follows:

Concept	Description
Location information	<p>Enter Location (for Geo Maps) information, for example, a city name, an address, or coordinates, for each probe, group, or device in the <a href="#">object's settings</a> [201]. The PRTG core server resolves your location specification to global geographical coordinates with the help of an external map service provider. PRTG uses this information to query a geographical map that shows your objects.</p> <p><b>i</b> You can use the first line of the location information field to <a href="#">label</a> [2732] your locations.</p>
Geo Maps settings	<p>Select a map service provider and the type of map that you want to view in the <a href="#">User Interface</a> [2659] settings in section Geo Maps. You can also disable the integration of Geo Maps there.</p> <p>PRTG connects to the specified maps service provider to get map tiles. These map tiles provide the geographical background map. PRTG then marks defined locations with a corresponding location marker that consists of an object icon and the object's <a href="#">status color</a> [2734].</p>  <p>Object Marker for a Group</p>
Geographical maps display	<p>You can display geographical maps in the device tree on an object's Overview tab. PRTG automatically adjusts the zoom level of a geographical map so that it can show all locations of a selected object.</p>  <p>Geographical Map on an Object's Overview Tab</p> <p>You can also add geographical maps to Maps. To do so, open the <a href="#">Map Designer</a> [2780] and click Geo Maps in the properties menu on the right.</p>

## Location Labels

You can define your own labels for locations of objects. To do so, enter the desired label in the [first line](#) of the Location (for Geo Maps) field in an object's settings and provide the geo coordinates of the location in the [second line](#). The object appears with the defined label in geographical maps. It is also possible to define the same label for different locations as long as the coordinates differ from each other.

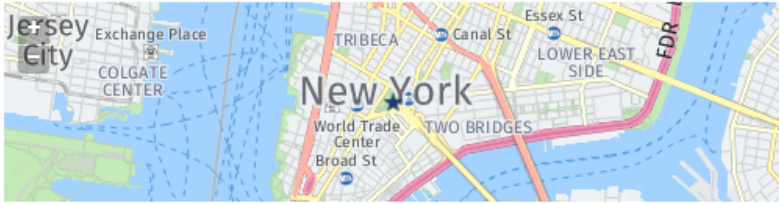
For example, enter the following information:

Big Apple  
40.712778,-74.005833

**Location**

inherit from

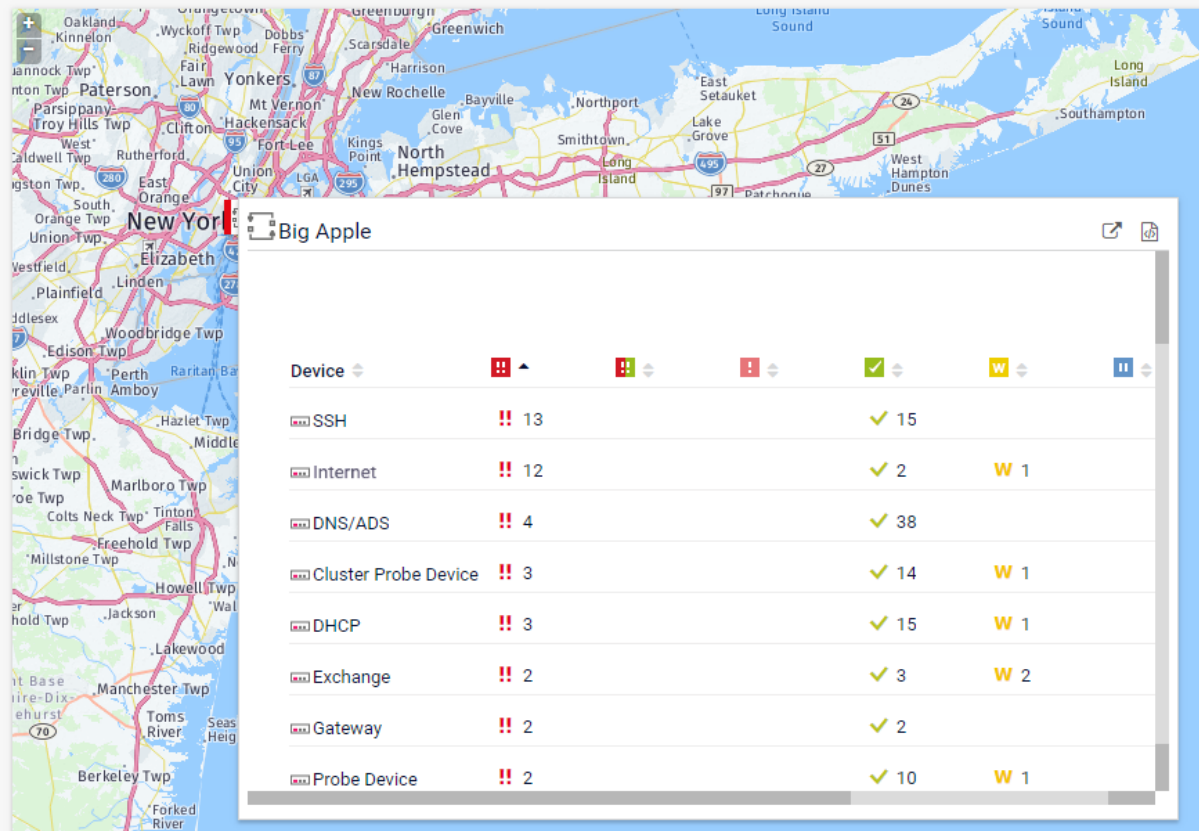
**Location (for Geo Maps) <sup>1</sup>**



Location New York with Geo Coordinates and Label Big Apple

The location **New York** appears on the geographical map with the label **Big Apple**:

**Geo Map for Root**



Device	!!	!	✓	W	
SSH	13		15		
Internet	12		2	1	
DNS/ADS	4		38		
Cluster Probe Device	3		14	1	
DHCP	3		15	1	
Exchange	2		3	2	
Gateway	2		2		
Probe Device	2		10	1	

Location New York with Label Big Apple

## Status Color of Location Markers

The location markers use different colors to show the overall monitoring status at this location.

 For an overview of the colors and their states, see section [Sensor States](#) <sup>181</sup>.

## More

### KNOWLEDGE BASE

Which domains and ports does the Geo Maps feature use?

- <https://kb.paessler.com/en/topic/35823>

Which provider should I use for the Geo Maps feature of PRTG?

- <https://kb.paessler.com/en/topic/34603>

Why does my street not appear on the Geo Map shown in PRTG?

- <https://kb.paessler.com/en/topic/35653>

How do I get a Google Maps API key for use in PRTG?

- <https://kb.paessler.com/en/topic/32363>

Which limitations apply when using the Google Maps API in PRTG?

- <https://kb.paessler.com/en/topic/7913>

My geo maps are displayed without background. What can I do?

- <https://kb.paessler.com/en/topic/63608>

What options do I have to review my monitoring data in detail?

- <https://kb.paessler.com/en/topic/90007>

## 8.8 Notifications

PRTG uses notifications to send you an alert, for example, whenever PRTG discovers a defined [sensor status](#) <sup>[181]</sup> or when channels breach specific limits. You can define an unlimited number of notifications using one or more [notification methods](#) <sup>[2735]</sup>. PRTG sends notifications to a user's [notification contacts](#) <sup>[2842]</sup> that you can define for each user account.

▶ For more information, see the video tutorial: [Notifications](#).

### Overview








PRTG sends a notification when a defined event triggers it. The following events can trigger notifications:

Event	Examples
Sensor status change	<ul style="list-style-type: none"> <li>A sensor changes from the Up status to the Down or the Warning status because responses are slow.</li> <li>A sensor changes to the Unusual status.</li> </ul>
Sensor value threshold breach	<ul style="list-style-type: none"> <li>A sensor shows a request time that is higher than 1,000 ms for more than 30 minutes.</li> <li>Free disk space is below 10%.</li> </ul>
Speed threshold breach	A traffic sensor shows more than 1 Mbit/s for more than 5 minutes.
Volume threshold breach	A traffic sensor shows more than 1 GB transferred in 24 hours.
Sensor value change	A specific value changes, for example, when the sensor monitors files on a hard disk drive.

### Notification Methods

A notification can use one or more of the following notification methods:

- [Send Email](#) <sup>[2815]</sup>
- [Add Entry to Event Log](#) <sup>[2818]</sup>
- [Send SMS/Pager Message](#) <sup>[2819]</sup>
- [Execute HTTP Action](#) <sup>[2821]</sup>
- [Execute Program](#) <sup>[2823]</sup>
- [Send Syslog Message](#) <sup>[2824]</sup>
- [Send SNMP Trap](#) <sup>[2825]</sup>

- [Send Amazon Simple Notification Service Message](#) 
  - [Assign Ticket](#) 
  - [Send Push Notification](#) 
  - [Send Microsoft Teams Message](#) 
  - [Send Slack Message](#) 
  - [Send MQTT Publish Notification](#) 
  - [Send OPC UA Notification](#) 
- For more information, see section [Notification Templates](#) .

## Placeholders






Notifications can contain valuable sensor information that you can define via placeholders, for example:


- Last error message
- Last successful or failed request
- Total downtime
- Total uptime
- Recent sensor history
- A direct link to the PRTG web interface

■ For available placeholders, see section [Placeholders for Notifications](#) .

## Notifications Setup

You must take the following four steps to set up and use notifications:

1. Check and set up the [notification delivery](#)  settings if you use PRTG Network Monitor. These settings define how PRTG sends messages.
2. Check and set up [notification contacts](#)  for the user accounts. These contacts define the recipients to which PRTG sends notifications.
3. Check and set up several [notification templates](#) . These templates define the notification methods and their content.
  - ① You can also check or edit notification templates via the Notification Triggers tab. For more information, see section [Notification Triggers Settings](#) .
4. Check and set up [notification triggers settings](#)  for objects. These triggers define when PRTG sends notifications.

① Usually, there are three successive attempts to deliver a notification. If all of these attempts fail, the notification is lost. To never miss a notification, we recommend that you always set up at least two notifications with different notification methods for a notification trigger, for example, one email notification and one SMS notification. If delivery via email fails, PRTG can still notify you via smartphone as a fallback. For example, use the latency setting of a [state trigger](#)  to choose a notification with a different notification method than in the first trigger condition, or set up a second trigger with a different notification method for the corresponding object.

- For a detailed step-by-step guide, see the Paessler website: [How to set up notifications via the PRTG web interface](#).
- Custom notification scripts are also available in the [PRTG Sensor Hub](#).

## More

### ■ KNOWLEDGE BASE

Notifications based on priority or favorites

- <https://kb.paessler.com/en/topic/31243>

### ▶ VIDEO TUTORIAL

Notifications

- <https://www.paessler.com/support/videos-and-webinars/videos/notifications>

### ■ PAESSLER WEBSITE

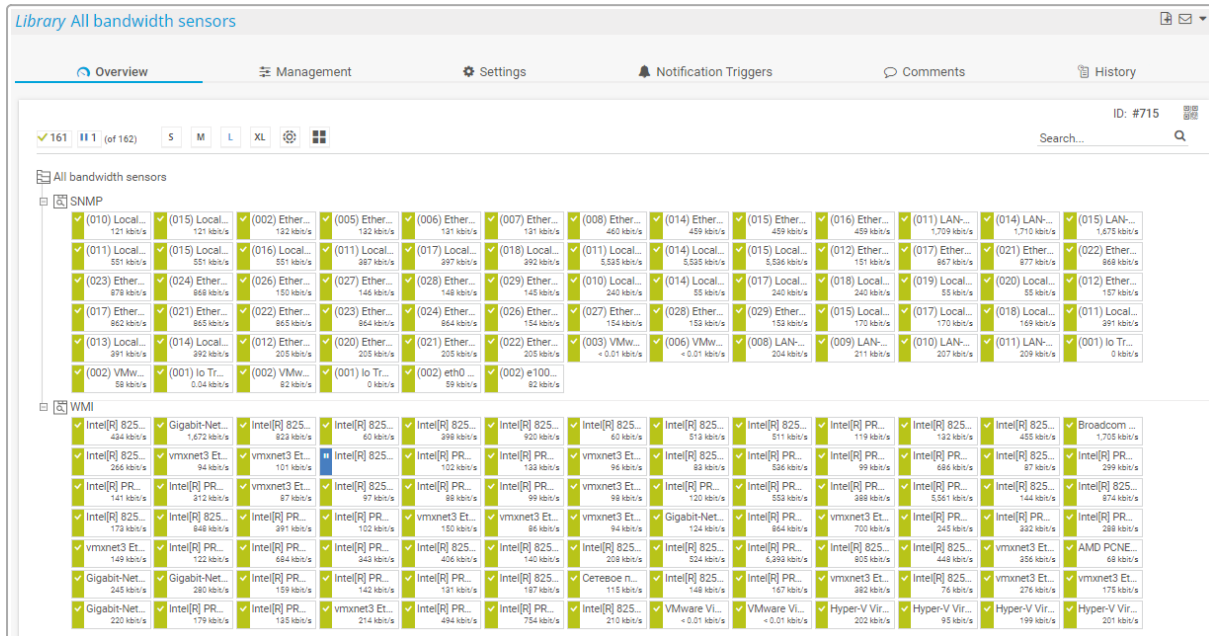
You can find custom notification scripts in the PRTG Sensor Hub

- <https://www.paessler.com/sensor-hub>

## 8.9 Libraries

With the **Libraries** feature, you can create additional, customized views of your device tree.

▶ For more information, see the video tutorial: [Libraries in PRTG](#)



Example of a Library

In this section:

- [Introduction](#) <sup>2738</sup>
- [Preconfigured Libraries](#) <sup>2739</sup>
- [Libraries Menu](#) <sup>2739</sup>
- [Libraries List](#) <sup>2740</sup>
- [Working with Libraries](#) <sup>2740</sup>

### Introduction

With libraries, you can create custom device tree views of your network's status and monitoring data. PRTG updates these views in the same interval as your device tree. The library views display the same monitoring data, but arranged the way you want, for example, based on target groups or a specific use case. For example, you can create a library that contains an overview of all your bandwidth monitoring sensors, regardless of the device that they run on.

The Libraries feature includes the following options:

- Create libraries that contain library nodes with objects from your entire configuration.
- Show data from different probes in one library.
- Show different branches of your device tree right next to each other.
- Arrange sensors in a tree-like view regardless of the device that they run on.



- Filter your entire device tree or parts of it by sensor type, status, or tag, and only show matching sensors.

## Preconfigured Libraries

PRTG provides several preconfigured libraries that you can also edit or delete.

- ① Preconfigured libraries are only visible to administrators.



Object ▾	Security Context ⓘ	<input type="checkbox"/>
All bandwidth sensors	PRTG System Administrator	<input type="checkbox"/>
All CPU load sensors	PRTG System Administrator	<input type="checkbox"/>
All diskspace sensors	PRTG System Administrator	<input type="checkbox"/>
All memory sensors	PRTG System Administrator	<input type="checkbox"/>
All sensors grouped by state	PRTG System Administrator	<input type="checkbox"/>
All VMware sensors	PRTG System Administrator	<input type="checkbox"/>
Sensors grouped by priority	PRTG System Administrator	<input type="checkbox"/>

Preconfigured Libraries

The following libraries are automatically created when you install PRTG for the first time. Some of these libraries are initially empty, but as you add more sensors, PRTG automatically fills them according to the filter settings defined for the library nodes:

- All bandwidth sensors
- All CPU load sensors
- All diskspace sensors
- All memory sensors
- All sensors grouped by state
- All VMware sensors
- Sensors grouped by priority

- ① Sensors that you add to libraries do not count against the maximum number of sensors of your license.

## Libraries Menu

Click Libraries in the [main menu bar](#) <sup>[240]</sup> to open an overview list of all libraries. Hover over Libraries to show other options.

Option	Description
All	Open the Libraries list where you can view or add custom device tree views of your network status and monitoring data.
Add Library	Open a dialog to create a new library.
Select Library	Open a library. Hover over Select Library to show more options. Follow the alphabetical menu path that is specific to your setup to view your libraries. Click a library to open it.

## Libraries List

In the All view, you see a list of all libraries. Enable the check box next to a library and use the quick action buttons:

- Used by (👤): Show which objects use this library.
- Clone (📄): Create a [clone](#)<sup>[2714]</sup> of this library.
- Delete (🗑️): Delete this library.
- Settings (⚙️): Open this library and change the [settings](#)<sup>[2744]</sup> of the library and its library nodes.

To add a new library, hover over  and select Add Library from the menu.

■ See also sections [Working with Table Lists](#)<sup>[218]</sup> and [Multi-Edit](#)<sup>[2718]</sup>.

## Working with Libraries

For more information on how to work with libraries, see the following sections:

- [Library Management](#)<sup>[2741]</sup>
- [Libraries and Node Settings](#)<sup>[2744]</sup>
- [Library Context Menus](#)<sup>[2751]</sup>

## More

### ■ PAESSLER WEBSITE

How to use libraries in PRTG in 4 steps

- <https://www.paessler.com/support/how-to/libraries>

### ▶ VIDEO TUTORIAL

Libraries in PRTG

- <https://www.paessler.com/support/videos-and-webinars/videos/libraries>

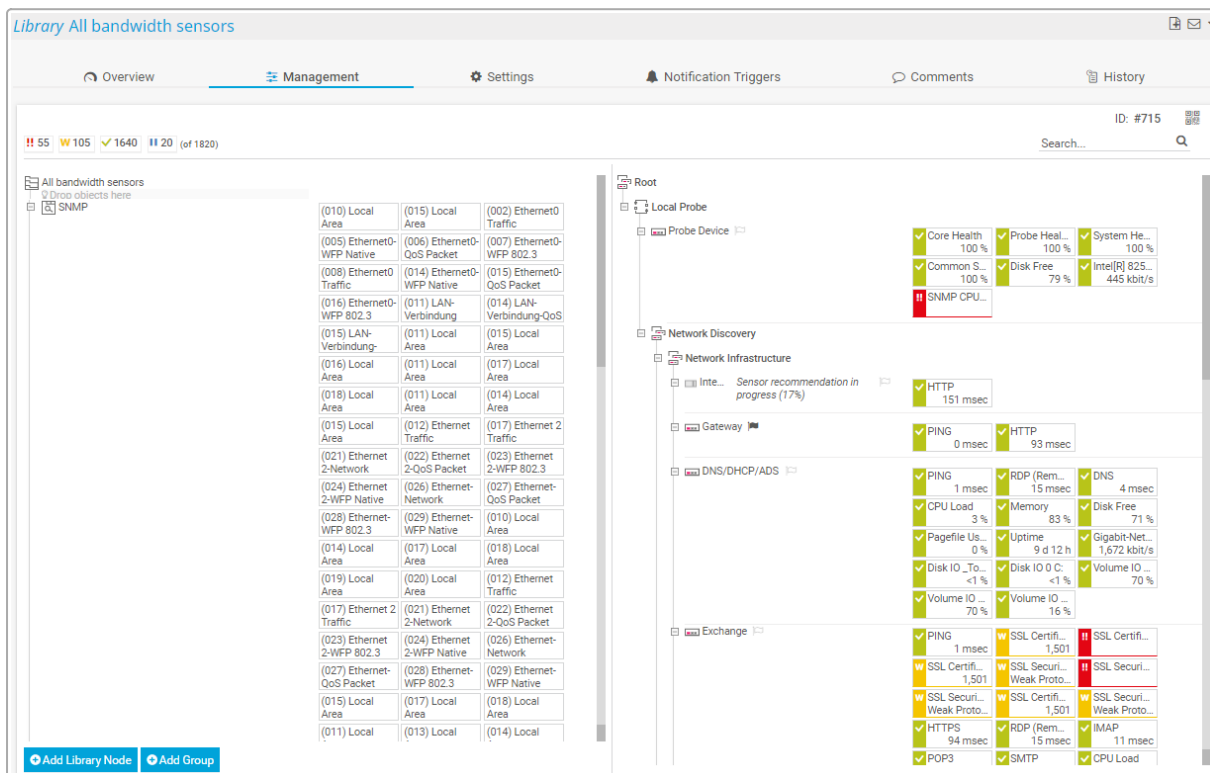
## 8.9.1 Library Management

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

You can manage your libraries by adding and editing library nodes and by defining which objects you want to see on a library node.

Click the Management tab. You see a split screen:

- On the left side, you can see your library. If you create a new library, it is empty in the beginning.
- On the right side, you see your device tree.



Bandwidth Library in Management Mode

### Add and Change Library Nodes

From the device tree on the right side, drag objects and drop them on the library on the left side. Each dropped object is immediately added as a new library node. Repeat this procedure as often as you wish until you have added all desired items to the library.

**i** Library nodes can contain up to 1,000 sensors. However, if you add single sensors to the library via the Management tab, there can only be one sensor in one library node.

Click Add Library Node or Add Group in the bottom-left corner of the split screen to create nested library nodes.

Drag and drop library nodes to change their position. If you want to change the monitoring object that is associated with a library node, you can change the Linked Object in the library node's settings.

## Set Library Node Display Settings

Right-click the name of a library node and select Edit | Settings from the [context menu](#) to change the Library Node Display Settings. In the dialog that appears, you can change the name of the library and its tags, as well as the linked object, the library node view, and filters. These settings are available for each library node.

**Edit Object NetFlow**
✕

---

### Basic Library Node Settings

**Library Node Name** ⓘ

NetFlow

---

**Security Context** ⓘ

PRTG System Administrator ▾

---

**Tags** ⓘ

bandwidthsensor ✕ netflow ✕ +

---

### Library Node Display Settings

**Linked Object** ⓘ

📁 Root » 🔍

---

**Library Node View** ⓘ

Show a subtree of the device tree (default)

Show a collection of filtered sensors

---

**Filter by Sensor Type** ⓘ

Show all sensor types (default)

Show only specific sensor types

---

**Sensor Types** ⓘ

Search... 🔍

Name

---

Active Directory Replication E...

---

Cancel
OK

Edit Library Node Display Settings

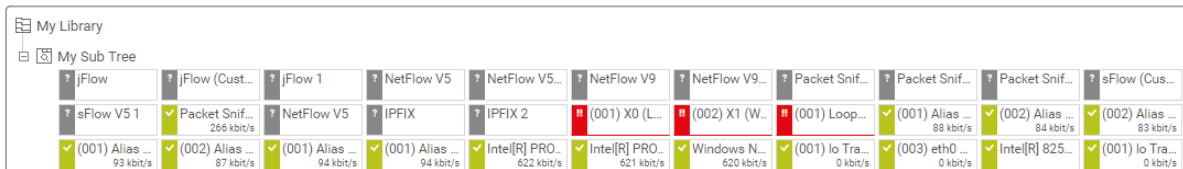
You can either show the Linked Object as a subtree of your device tree including probes, groups, and devices, or you can view all sensors underneath the Linked Object.

- When you select Show a subtree of the device tree (default), the library node called **My Sub Tree**, for example, looks like a branch in your device tree.



Library with One Node that Shows a Branch of the Device Tree

- When you select Show a collection of filtered sensors, PRTG only shows the sensors that are underneath the Linked Object in the device tree without probes, groups, and devices. You can additionally filter for certain sensor types, states, and tags. PRTG then only shows matching sensors. In the example screenshot, you can see the library node **My Sub Tree** where only bandwidth sensors are shown.



Library with One Node that Only Shows a Collection of Bandwidth Sensors

For more information, see section [Libraries and Node Settings](#) <sup>[2744]</sup>.

## Context Menu

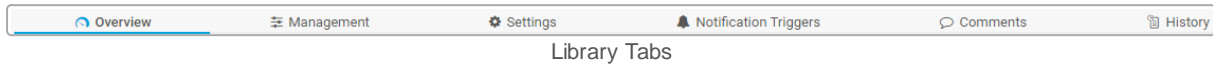
You can right-click any object on a library's Overview tab or Management tab to open its context menu.

For more information, see section [Library Context Menus](#) <sup>[2751]</sup>.

## 8.9.2 Libraries and Node Settings

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

Use the library tabs to access all functionalities and settings of a library.



### Overview

Click the Overview tab to show the status of your library.

### Management

Click the Management tab to edit the contents of your library, for example, to add items to the library via drag-and-drop.

**■** For more information, see section [Library Management](#)<sup>[2741]</sup>.

### Library Node Settings

To change the settings of a library node, go to a library's Overview tab and click the name of a library node. You can also open the library node settings on the Management tab via the library node's [context menu](#)<sup>[2751]</sup>.


**i** You can only change the settings of a library node if it already contains monitoring objects like groups, devices, or sensors.

### Basic Library Node Settings

Setting	Description
Library Node Name	<p>Enter a name to identify the library node.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Security Context	<p>Define the security context for the Overview tab of the library. Select a user account from the dropdown list to define which objects are visible. All users with access to the library can only see the objects that the selected user account has the rights to view.</p> <p><b>i</b> Only sensors that are visible in the library trigger a <a href="#">notification</a><sup>[2735]</sup>.</p>

Setting	Description
	<p><b>i</b> Basically, the security context defines the minimum access rights to objects like libraries, reports, or maps, that a user account has. If the security context of an object is <a href="#">PRTG System Administrator</a>, for example, every user sees all objects in a library, in a report, or on a map, no matter what the particular user access rights are.</p>
Tags	<p>Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically <a href="#">inherited</a><sup>[138]</sup>.</p> <p><b>i</b> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (&lt;&gt;).</p> <p><b>i</b> For performance reasons, it can take some minutes until you can filter for new tags that you added.</p>

### Library Node Display Settings

Setting	Description
Linked Object	<p>Click  and use the <a href="#">object selector</a><sup>[222]</sup> to change the object in the device tree that the library node references.</p>
Library Node View	<p>Select how you want to view the objects that PRTG shows underneath the library node:</p> <ul style="list-style-type: none"> <li>Show a subtree of the device tree (default): View all objects underneath the linked object as you can see them in the device tree, including probes, groups, and devices.</li> <li>Show a collection of filtered sensors: Only view the sensors underneath the linked object without probes, groups, and devices. You can use filters to show only specific sensors.</li> </ul> <p><b>i</b> The library node can show up to 1,000 sensors. PRTG discards further sensors.</p>
Filter by Sensor Type	<p><b>This setting is only visible if you select</b> Show a collection of filtered sensors <a href="#">above</a>.</p> <p>Select if you want to filter the displayed sensors by specific sensor types:</p> <ul style="list-style-type: none"> <li>Show all sensor types (default): Do not filter by sensor types.</li> <li>Show only specific sensor types: Filter the displayed sensors by specific sensor types.</li> </ul>

Setting	Description
	<p><b>i</b> PRTG applies this filter in real time. If the configuration underneath the linked object changes, the library node accordingly shows matching sensors.</p>
<p>Sensor Types</p>	<p><b>This setting is only visible if you select</b> Show only specific sensor types <a href="#">above</a>.</p> <p>You can see a list of all sensor types. PRTG displays sensors that are in use in bold print.</p> <p>Enable the check box in front of a sensor type that you want to include in the library node view.</p> <p><b>i</b> You can also select all items or cancel the selection by using the check box in the table header.</p> <p><b>i</b> PRTG applies this filter in real time. If the configuration underneath the linked object changes, the library node accordingly shows matching sensors.</p> <p><b>i</b> You cannot filter for sensor types that are defined in mini probes.</p>
<p>Filter by Sensor Status</p>	<p><b>This setting is only visible if you select</b> Show a collection of filtered sensors <a href="#">above</a>.</p> <p>Select if you want to filter the displayed sensors by specific sensor states:</p> <ul style="list-style-type: none"> <li>▪ Show all sensor states: Do not filter by sensor status.</li> <li>▪ Show only sensors in specific states: Filter the displayed sensors by specific sensor states.</li> </ul>
<p>Sensor States</p>	<p><b>This setting is only visible if you select</b> Show only sensors in specific states <a href="#">above</a>.</p> <p>You can see a list of all sensor states. Enable the check box in front of a sensor status to include all sensors that show this status in the library node view:</p> <ul style="list-style-type: none"> <li>▪ Unknown</li> <li>▪ Up</li> <li>▪ Warning</li> <li>▪ Down</li> <li>▪ Paused by user</li> <li>▪ Unusual</li> <li>▪ Down (Acknowledged)</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ Down (Partial)</li> </ul> <p><b>i</b> You can also select all items or cancel the selection by using the check box in the table header.</p> <p><b>i</b> PRTG applies this filter in real time. If the configuration underneath the linked object changes, the library node accordingly shows matching sensors.</p>
Filter by Tag	<p><b>This setting is only visible if you select</b> Show a collection of filtered sensors <a href="#">above</a>.</p> <p>Select if you want to filter the displayed sensors by specific tags:</p> <ul style="list-style-type: none"> <li>▪ Show all tags: Do not filter by tag.</li> <li>▪ Show only sensors with specific tags: Filter the displayed sensors by specific tags.</li> </ul>
Tags	<p><b>This setting is only visible if you select</b> Show only sensors with specific tags <a href="#">above</a>.</p> <p>Enter one or more tags for sensors that you want to include in the library node view. You can also use the plus sign (+) or the minus sign (-) to categorize tags as <b>must have</b> or <b>must not have</b>, for example, <b>+snmp;-wmi</b> (must have the tag <b>snmp</b> and must not have the tag <b>wmi</b>).</p> <p><b>i</b> The tag of a sensor can also be inherited from a parent object.</p> <p><b>i</b> For performance reasons, it can take some minutes until you can filter for new tags that you added.</p> <p><b>i</b> PRTG applies this filter in real time. If the configuration underneath the linked object changes, the library node accordingly shows matching sensors.</p>
Filter by Priority	<p><b>This setting is only visible if you select</b> Show a collection of filtered sensors <a href="#">above</a>.</p> <p>Select if you want to filter the displayed sensors by specific <a href="#">priorities</a> <sup>224</sup>:</p> <ul style="list-style-type: none"> <li>▪ Show all priorities: Do not filter by priority.</li> <li>▪ Show only sensors with specific priorities: Filter the displayed sensors by specific priorities.</li> </ul> <p><b>i</b> PRTG ignores the priority settings of a parent object. It only regards the priority setting of the sensor itself.</p>
Priorities	<p><b>This setting is only visible if you select</b> Show only sensors with specific priorities <a href="#">above</a>.</p>

Setting	Description
	<p>You can see a list of all available priorities. Enable the check box in front of a priority to include all sensors that have this priority in the library node view:</p> <ul style="list-style-type: none"> <li>▪ ***** (highest priority)</li> <li>▪ ****</li> <li>▪ ***</li> <li>▪ **</li> <li>▪ * (lowest priority)</li> </ul> <p><b>i</b> PRTG applies this filter in real time. If the configuration underneath the linked object changes, the library node accordingly shows matching sensors.</p>

**i** Click OK to save your settings. If you close the dialog without saving, all changes to the settings are lost.

**i** After you apply filters, it might take several seconds for the changes to become visible. This is because of internal filter processes that run in the background.

## Settings

Click the Settings tab to open a library's general settings.

### Basic Library Node Settings

Setting	Description
Library Node Name	<p>Enter a name to identify the library.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Security Context	<p>Define the security context for the Overview tab of the library. Select a user account from the dropdown list to define which objects are visible. All users with access to the library can only see the objects that the selected user account has the rights to view.</p> <p><b>i</b> Only sensors that are visible in the library trigger a <a href="#">notification</a><sup>2735</sup>.</p> <p><b>i</b> Basically, the security context defines the minimum access rights to objects like libraries, reports, or maps, that a user account has. If the security context of an object is <a href="#">PRTG System Administrator</a>, for example, every user sees all objects in a library, in a report, or on a map, no matter what the particular user access rights are.</p>

Setting	Description
Tags	<p>Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically <a href="#">inherited</a><sup>138</sup>.</p> <p><b>i</b> For performance reasons, it can take some minutes until you can filter for new tags that you added.</p>

## Access Rights

Setting	Description
User Group Access	<p>Define the user groups that have access to the object. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights:</p> <ul style="list-style-type: none"> <li>▪ No access: Users in this user group cannot see or edit the object. The object does not show up in lists.</li> <li>▪ Read access: Users in this user group can see the object and view its settings.</li> <li>▪ Write access: Users in this user group can see the object and view and edit its settings. However, they cannot edit the object's access rights settings.</li> <li>▪ Full access: Users in this user group can see the object, view and edit its settings, and edit its access rights settings.</li> </ul> <p><b>i</b> You can create new user groups in the <a href="#">User Groups</a><sup>2912</sup> settings.</p>

**i** When you give access rights to a user group, all user group members can see the objects in the respective library.

**i** Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

## Notification Triggers

You can define notification triggers for any kind of library, also for dynamic libraries that can change with every scanning interval, for example, when you filter a library by sensor status or priority.

## Comments

On the Comments tab, you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

## History

On the History tab, all changes in the settings of an object are logged with a time stamp, the name of the user who made the change, and a message. The history log retains the last 100 entries.

## Delete

You can delete the entire library at any time. Right-click a library's name and select Delete from the context menu.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

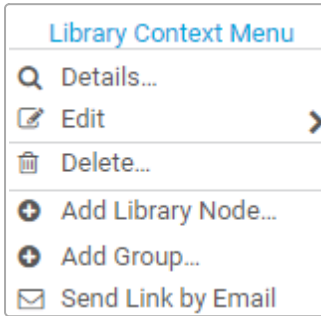
- <https://kb.paessler.com/en/topic/61108>

### 8.9.3 Library Context Menus

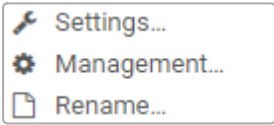
Right-click a library or a library node on a library's Overview tab or Management tab to show its context menu.

#### Library Context Menu

The Library Context Menu contains actions for your libraries.



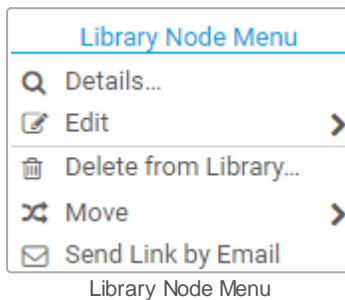
Library Context Menu






Action	Description
Details	<p>Show the Overview tab of the object.</p> <p>■ For more information about the Overview tab, see the Knowledge Base: <a href="#">What options do I have to review my monitoring data in detail?</a></p>
Edit	<p>Hover over Edit to show the Edit menu. The following actions are available:</p>  <p>Edit Context Menu</p> <ul style="list-style-type: none"> <li>▪ Settings: Open a dialog to edit the <a href="#">library settings</a><sup>[2748]</sup>.</li> <li>▪ Management: Open the Management <a href="#">tab</a><sup>[2741]</sup> of the library.</li> <li>▪ Rename: Open a dialog to edit the name of the object.</li> </ul>
Delete	<p>Delete the object. PRTG asks for confirmation before it actually deletes an object.</p>
Add Library Node	<p>Add a new library node to the library.</p>
Add Group	<p>Add a group to the library to create nested library nodes.</p>

Action	Description
Send Link by Email	Send a link to the object by email. Click to create a new email with your system's standard email client. The email contains a direct link to the Overview tab of the object.

## Library Node Menu

The Library Node Menu contains actions for your library nodes.



Action	Description
Details	Show the Overview tab of the object.  ■ For more information about the Overview tab, see the Knowledge Base: <a href="#">What options do I have to review my monitoring data in detail?</a>
Edit	Hover over Edit to show the Edit menu. The following actions are available: <ul style="list-style-type: none"> <li>▪ Settings: Open a dialog to edit the <a href="#">library node settings</a> .</li> <li>▪ Rename: Open a dialog to edit the name of the object.</li> </ul>
Delete from Library	Delete the object. PRTG asks for confirmation before it actually deletes an object.
Move	Hover over Move to open the Move menu. The following actions are available: <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <ul style="list-style-type: none"> <li> Top</li> <li> Up</li> <li> Down</li> <li> Bottom</li> </ul> </div> <p style="text-align: center; margin: 0;">Move Context Menu</p> <ul style="list-style-type: none"> <li>▪ Top: Move the library node to the top of the library.</li> </ul>

Action	Description
	<ul style="list-style-type: none"><li>▪ Up Move the library node one entry up.</li><li>▪ Down: Move the library node one entry down.</li><li>▪ Bottom Move the library node to the bottom of the library.</li></ul>
Send Link by Email	Send a link to the object by email. Click to create a new email with your system's standard email client. The email contains a direct link to the Overview tab of the object.

## More

### KNOWLEDGE BASE

What options do I have to review my monitoring data in detail?

- <https://kb.paessler.com/en/topic/90007>

## 8.10 Reports

With the [Reports](#) feature, you can view and analyze historic monitoring results for a specific period of time or for your system configuration. You can create reports for all sensors or only for specific sensors.



Example of a Report

**i** The report above shows the report data for devices on a local probe. You can see graphs for the preceding week and data tables with numeric results.

In this section:

- [Introduction](#) <sup>[2755]</sup>
- [Reports Menu](#) <sup>[2755]</sup>
- [Reports List](#) <sup>[2756]</sup>
- [Configuration Reports](#) <sup>[2757]</sup>



- [Automatic Averaging](#)<sup>[2757]</sup>

## Introduction

You can generate reports on demand or via schedules in HTML and PDF format, as well as in comma-separated values (CSV) and Extensible Markup Language (XML) format. Furthermore, you can create reports for a single sensor or for a whole range of sensors. It is also possible to [create HTML reports of your system configuration](#)<sup>[2757]</sup>.

Report templates define the overall look of your report and in which detail the report shows monitoring data.

## Preconfigured Reports

PRTG provides several preconfigured reports that you can also edit or delete:

- Summary report for all sensors
- Top 100 Busy/Idle Processor Sensors
- Top 100 Fastest/Slowest HTTP Sensors
- Top 100 Fastest/Slowest Ping Sensors
- Top 100 Free/Full Disk Space Sensors
- Top 100 Most/Least Used Bandwidth Sensors
- Top 100 Most/Least Used Memory Sensors
- Top 100 Uptime/Downtime Report

## Reports Menu

Click Reports in the [main menu bar](#)<sup>[245]</sup> to open an overview list of all reports about monitoring data. Hover over Reports to show other options.

Option	Description
All	Open the Reports list where you can view or add reports about your monitoring data.
Add Report	Open a dialog to create a new report.
Select Report	Hover over Select Report to show a list of your reports about monitoring data. Click a report to open it.
Configuration Reports	Hover over Configuration Reports to see the available <a href="#">configuration reports</a> <sup>[2757]</sup> . Select an item to create reports for maps, reports, users and user groups, and system configuration to document changes to the configuration.

## Reports List

In the All view, you see a list of all reports about monitoring data.

Reports					
Object ▾	Template ▾	Security Context ▾	Period ▾	Schedule ▾	
<input checked="" type="checkbox"/> Summary report for all sensors	List of sensors (with 1 h graph)	PRTG System Admi...	Day	None	
<input checked="" type="checkbox"/> Top 100 Busy/Idle Processor Sensors	Top 100 highest and lowest (5 ...	PRTG System Admi...	Day	None	
<input checked="" type="checkbox"/> Top 100 Fastest/Slowest HTTP Sensors	Top 100 highest and lowest (5 ...	PRTG System Admi...	Day	None	
<input checked="" type="checkbox"/> Top 100 Fastest/Slowest Ping Sensors	Top 100 highest and lowest (5 ...	PRTG System Admi...	Day	None	
<input checked="" type="checkbox"/> Top 100 Free/Full Disk Space Sensors	Top 100 highest and lowest (5 ...	PRTG System Admi...	Day	None	
<input checked="" type="checkbox"/> Top 100 Most/Least Used Bandwidth S...	Top 100 highest and lowest (5 ...	PRTG System Admi...	Day	None	
<input checked="" type="checkbox"/> Top 100 Most/Least Used Memory Sen...	Top 100 highest and lowest (5 ...	PRTG System Admi...	Day	None	
<input checked="" type="checkbox"/> Top 100 Uptime/Downtime Report	Top 100 uptime and downtime...	PRTG System Admi...	Day	None	

List of Reports



Section	Description
Object	Shows the name of the report.
Template	Shows the name of the template that this report uses.
Security Context	Shows the user account that PRTG uses to run the report. This user account defines which objects are visible in the report. For more information, see section <a href="#">Report Settings</a> <sup>2764</sup> .
Period	Shows the time span that the report covers.
Schedule	Shows if you set a schedule to automatically run the report in a regular interval. For more information, see section <a href="#">Report Settings</a> <sup>2764</sup> .
Email	Shows the email address to which PRTG automatically sends the report if you set a schedule <b>and</b> entered an email address in the report settings.
Status	Shows the status of the report.

Section	Description
Next Run	Shows the date and time at which PRTG runs the report the next time if you set a schedule in the report settings.
Last Run	Shows the date and time at which PRTG ran the report the last time if you set a schedule in the report settings.
# Sensors in Last Run	Shows the number of sensors whose data was included when PRTG last ran the report.

Click the name of a report about monitoring data to open the Run Now tab.

**i** You can only run configuration reports via the main menu bar.

Enable the check box next to a report and use the quick action buttons:

- Clone (clone<sup>[2714]</sup> of this report.
- Delete (settings<sup>[2764]</sup>.

To add a new report, hover over  and select Add Report from the menu.

 See also sections [Working with Table Lists](#)<sup>[218]</sup> and [Multi-Edit](#)<sup>[2718]</sup>.

## Configuration Reports

Configuration reports show the PRTG configuration. They are available for Maps, Reports, Users & User Groups, and System Configuration. PRTG directly displays a configuration report in a new browser window as an HTML page. You can use configuration reports, for example, to file and document changes to the PRTG configuration.

Configuration reports contain the same information as you can see on the [Maps](#)<sup>[2776]</sup> overview, the [Reports](#)<sup>[2754]</sup> overview, and on the [User Accounts](#)<sup>[2901]</sup> and [User Groups](#)<sup>[2912]</sup> tabs of the system administration settings. The configuration report System Configuration includes the system administration settings of the [User Interface](#)<sup>[2855]</sup>, [Monitoring](#)<sup>[2869]</sup>, [Notification Delivery](#)<sup>[2877]</sup>, [Core & Probes](#)<sup>[2887]</sup>, and [Cluster](#)<sup>[2923]</sup> tabs.

**i** Configuration reports are interactive. You can click available links to go to the corresponding pages in the PRTG web interface.

## Automatic Averaging

For performance reasons, PRTG automatically averages monitoring data when it calculates data for large periods of time.

Period of Time in Report	Minimum Level of Detail (Averaging Interval)
Up to 40 days	Any
40 to 500 days	60 minutes/1 hour or longer

**i** Reports for periods that are longer than 500 days are not possible. If you enter a longer period, PRTG automatically shortens it to 365 days.

**i** In some cases, the generated report might contain a period of time that differs from the defined start and end date for the report because of internal averaging processes. When averaging intervals are longer than 1 hour and do not equal 24 hours, and when they are combined with specific periods of time, the resulting data points might be asynchronous to the periods of time. Consider this behavior particularly if you use [application programming interface \(API\) calls](#) <sup>3084</sup> to generate reports.

## More

**■** PAESSLER WEBSITE

How to set up reports in PRTG in 5 easy steps

- <https://www.paessler.com/support/how-to/reports>

## 8.10.1 Run Reports

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

### Run Now

On the Run Now tab, you can immediately run a report with the settings that you defined before.

**i** When you set up or run a report, also keep in mind the [remarks for reports](#) <sup>2762</sup>.

Run Report on Demand

### Report Period

Setting	Description
Period	<p>Define the time span that the report covers:</p> <ul style="list-style-type: none"> <li>Current period: This week [date range]: Use monitoring data of the current period. The actual time span depends on the report period that you define in the <a href="#">report settings</a> <sup>2764</sup>. It can be today, this week, this month, or this year.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Previous period: Last week [<a href="#">date range</a>]: Use monitoring data of the previous period. The actual time span depends on the report period that you define in the report settings. It can be yesterday, last week, last month, or last year.</li> <li>▪ Select a predefined date range: Use monitoring data of a predefined period other than the current or the previous period. Select from a list of date ranges below.</li> <li>▪ Define a custom date range: Use monitoring data of a custom period. Set the start and end date below or choose from several quick range buttons.</li> </ul>
Date Range	<p><a href="#">This setting is only visible if you select</a> Select a predefined date range <a href="#">above</a>.</p> <p>From the list, select a date range for which PRTG generates the report. The shown time spans depend on the available monitoring data and on the report period that you define in the report settings. It can be days, weeks, months, or years.</p>
Start Date	<p><a href="#">This setting is only visible if you select</a> Define a custom date range <a href="#">above</a>.</p> <p>Set the start date of the time span for which PRTG generates the report. Use the date time picker to enter the date and time. Make sure that you define a valid period.</p>
End Date	<p><a href="#">This setting is only visible if you select</a> Define a custom date range <a href="#">above</a>.</p> <p>Set the end date of the time span for which PRTG generates the report. Use the date time picker to enter the date and time. Make sure that you define a valid period.</p>
Quick Range	<p><a href="#">This setting is only visible if you select</a> Define a custom date range <a href="#">above</a>.</p> <p>Use the buttons to quickly set the start and end dates for the report:</p> <ul style="list-style-type: none"> <li>▪ Today</li> <li>▪ Yesterday</li> <li>▪ Last Week (Mo-Su)</li> <li>▪ Last Week (Su-Sa)</li> <li>▪ Last Month</li> <li>▪ 2 Months</li> <li>▪ 6 Months</li> <li>▪ 12 Months</li> </ul>

Setting	Description
	<p><b>i</b> PRTG sets the <a href="#">date range</a> <sup>[220]</sup> to the last matching period. It starts at 00:00 and ends at 00:00 of the following day.</p>

## Report Processing

**i** This section is not visible for read-only users.

Setting	Description
File Format and Delivery	<p>Define how you want to view the report:</p> <ul style="list-style-type: none"> <li>▪ View report as HTML: Directly view the report in a new browser window or tab.</li> <li>▪ Create and store .pdf and data files: Create a .pdf file and, depending on the <a href="#">Data Files</a> <sup>[2772]</sup> setting, create data files of the report and store it. You find the stored report files on the Stored Reports tab. You also receive a ToDo ticket. By default, PRTG sends out a notification email to administrators in this case.</li> <li>▪ Create and store .pdf and data files and send them by email: Create a .pdf file and, depending on the Data Files setting, create data files of the report, store the files, and send them via email to the email address that you define below. You can find the stored report files on the Stored Reports tab.</li> </ul> <p><b>i</b> PRTG only generates .csv and .xml data files for report templates that include data tables.</p> <p><b>i</b> To create .pdf files, make sure that the print spooler service runs on the PRTG core server system.</p> <p><b>i</b> Some special characters, for example, 4-byte unicode characters, might not be displayed correctly in PDF reports. As a workaround, we recommend that you generate an HTML report and save it as a .pdf file.</p> <p><b>i</b> If you generate reports with Internet Explorer 11, we recommend that you use one of the PDF options for optimal results.</p>
Target Email Address	<p><b>This setting is only visible if you select</b> Create and store .pdf and data files and send them by email <b>above</b>.</p> <p>Enter one or more valid email addresses to which PRTG sends the report. Use commas to separate email addresses.</p> <p><b>i</b> PRTG sends an email to all recipients. All recipients appear in the To field of the email.</p>

Setting	Description
	<p><b>i</b> You can change the configuration for outgoing emails in the <a href="#">Notification Delivery</a> settings.</p>
File Compression	<p>This setting is only visible if you select Create and store .pdf and data files and send them by email above.</p> <p>Define if PRTG compresses the attached report files before it sends them:</p> <ul style="list-style-type: none"> <li>▪ Send files without compression: PRTG sends the report files by email in their original size.</li> <li>▪ Compress files in a .zip file: PRTG compresses the report files to a .zip file before they are sent by email.</li> </ul>

Click Run Report to start the report generation. Depending on the number of selected sensors, this might take a while. If it takes a long time to generate HTML reports, consider using one of the PDF options.

## Remarks for Reports

- Any sensor graph in your report only shows channels that you select via the Show in graphs option in the [channel settings](#).
- Reports show statistics for the uptime (the Up and Down [states](#) in percent) and for requests (Good and Failed in percent). PRTG rounds values between 5% and 95%, as well as 100% and 0%, to whole numbers without decimal places. Other values are shown with 3 decimal places.
- Because PRTG rounds values, the statistics in the report section Sensor Status History can differ from the values in the report section Uptime Stats by a few seconds.
- PRTG limits data reporting to 5 requests per minute.
- Reports cannot show uptime or downtime data for the [Sensor Factory](#) sensor.
- Create reports that include an appropriate amount of data. Reports might not work as expected if PRTG has to process too many sensors with short scanning intervals. Adjust your report size and the time span that the report covers, if necessary.

## Stored Reports

On the Stored Reports tab, you can view all PDF reports and data files that you created and stored.

Click a name to open the report. PRTG stores reports until they are deleted according to the [data purging settings](#) of your PRTG configuration.

## Other Tabs

For all other tabs, see section [Report Settings](#).



## More

### ■ KNOWLEDGE BASE

Why is there missing data in historic data reports?

- <https://kb.paessler.com/en/topic/61382>

Creating a PDF report does not work. What can I do?

- <https://kb.paessler.com/en/topic/87084>

## 8.10.2 Report Settings

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

In this section:

- [Settings](#)<sup>[2764]</sup>
- [Basic Report Settings](#)<sup>[2764]</sup>
- [Included Sensors](#)<sup>[2766]</sup>
- [Report Schedule](#)<sup>[2768]</sup>
- [Report Period](#)<sup>[2770]</sup>
- [Percentile Handling](#)<sup>[2771]</sup>
- [Data Files](#)<sup>[2772]</sup>
- [Report Comments](#)<sup>[2773]</sup>
- [Access Rights](#)<sup>[2773]</sup>
- [Select Sensors Manually](#)<sup>[2774]</sup>
- [Sensors Selected by Tag](#)<sup>[2775]</sup>
- [Comments](#)<sup>[2775]</sup>

### Settings

Click the Settings tab to open the settings of a report.

**i** When you set up or run a report, also keep in mind the [remarks for reports](#)<sup>[2762]</sup>.

### Basic Report Settings

Setting	Description
Report Name	<p>Enter a name to identify the report. PRTG uses the name in <a href="#">reports lists</a><sup>[245]</sup> and as the title of generated reports.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Tags	<p>Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically <a href="#">inherited</a><sup>[138]</sup>.</p>

Setting	Description
	<ul style="list-style-type: none"> <li data-bbox="488 387 1294 454">❗ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (&lt;&gt;).</li> <li data-bbox="488 488 1294 555">❗ For performance reasons, it can take some minutes until you can filter for new tags that you added.</li> </ul>
Report Template	<p data-bbox="488 613 1342 707">Templates define the overall look of your report and in which detail the report shows monitoring data. PRTG includes several preconfigured report templates. Select a template for the report from the dropdown list:</p> <ul style="list-style-type: none"> <li data-bbox="488 730 1342 857">▪ Graph with data table (data files available): Create a report with graphs and data tables. Choose from different intervals. Reports that use one of these templates also generate .csv and .xml files if you select the respective setting in the Data Files section.</li> <li data-bbox="488 880 1342 1008">▪ Data table only (data files available): Create a report with data tables. Choose from different intervals. Reports that use one of these templates also generate .csv and .xml files if you select the respective setting in the Data Files section.</li> <li data-bbox="488 1030 1342 1124">▪ Graph only (data files not available): Create a report with graphs. Choose from different intervals. Reports that use one of these templates cannot generate .csv or .xml files.</li> <li data-bbox="488 1146 1342 1240">▪ List of sensors (data files not available): Create a report in a compact sensor list style. The list is available with and without graphs. Reports that use one of these templates cannot generate .csv or .xml files.</li> <li data-bbox="488 1263 1342 1391">▪ Top 100 highest and lowest (data files not available): Create a report with up to 100 objects with the highest and lowest average values. Choose from different intervals. Reports that use one of these templates cannot generate .csv or .xml files.</li> <li data-bbox="488 1413 1342 1541">▪ Top 10 uptime and downtime (data files not available): Create a report with up to 10 objects with the highest uptime and downtime for each object. You can choose between data in percent and hours. Reports that use one of these templates cannot generate .csv or .xml files.</li> <li data-bbox="488 1563 1342 1691">▪ Top 100 uptime and downtime (data files not available): Create a report with up to 100 objects with the highest uptime and downtime for each object. You can choose between data in percent and hours. Reports that use one of these templates cannot generate .csv or .xml files.</li> </ul> <p data-bbox="488 1713 1318 1736">❗ PRTG <a href="#">automatically averages</a><sup>27571</sup> monitoring data within an interval.</p>
Security Context	<p data-bbox="488 1800 1326 1957">Define the security context that the report uses for access to monitoring data. Select a user account from the dropdown list to define which objects are visible in the report. The report only contains objects that the selected user has the <a href="#">access rights</a><sup>1451</sup> to view. By default, the security context is the user account that creates the report.</p>

Setting	Description
	<p><b>i</b> Basically, the security context defines the minimum access rights to objects like libraries, reports, or maps, that a user account has. If the security context of an object is <a href="#">PRTG System Administrator</a>, for example, every user sees all objects in a library, in a report, or on a map, no matter what the particular user access rights are.</p>
Time Zone	Select a time zone from the dropdown list. PRTG uses this time zone for all date-specific settings in the report.
Page Format	<p>Define the page size in which PRTG creates .pdf files:</p> <ul style="list-style-type: none"> <li>▪ None: Do not specify a page format. PRTG automatically sets a size.</li> <li>▪ DIN A4: Use the German DIN A4 format.</li> <li>▪ DIN A3: Use the DIN A3 format.</li> <li>▪ DIN A2: Use the DIN A2 format.</li> <li>▪ Legal: Use the North American legal page format.</li> <li>▪ Letter: Use the North American letter page format.</li> <li>▪ Ledger: Use the North American ledger page format.</li> </ul>
Page Orientation	<p>Define the page orientation for the data in PDF reports:</p> <ul style="list-style-type: none"> <li>▪ Portrait: Use the portrait orientation.</li> <li>▪ Landscape: Use the landscape orientation to show data tables of sensors with many channels. Other parts of the report remain in the portrait orientation and do not resize to the landscape orientation.</li> </ul>

## Included Sensors

Setting	Description
Cluster Node	<p><a href="#">This setting is only visible if you run PRTG in a failover cluster</a><sup>[128]</sup>.</p> <p>Select the cluster node from which the report takes monitoring data from the dropdown list. The available options are specific to your configuration.</p> <p>By default, the master node is set. Select All cluster nodes to create a report that includes data from all of your cluster nodes.</p> <p><b>i</b> A report for all cluster nodes only includes data for the primary channels. Be careful with big reports for all cluster nodes because the report generation might significantly slow down your monitoring.</p>

Setting	Description
	<p><b>i</b> If you select a failover node, report and data files do not show data from the local probe or from a remote probe and might be empty or show 0 values.</p> <p><b>i</b> You can generate .csv and .xml data files only for a single failover node. If you select the option All cluster nodes, the report does not create data files.</p>
Sensors by Tag	<p>Select the sensors that you want to include in the report by tag. Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically <a href="#">inherited</a><sup>[138]</sup>. The report covers all sensors that have at least one of the tags. You can also leave the field empty.</p> <p>You can also use the plus sign (+) or the minus sign (-) to categorize tags as <b>must have</b> or <b>must not have</b>, for example, <b>+snmp -wmi</b> (must have the tag <b>snmp</b> and must not have the tag <b>wmi</b>).</p> <p><b>i</b> For performance reasons, it can take some minutes until you can filter for new tags that you added.</p> <p><b>i</b> The report automatically includes all channels of sensors that you add by tag, unless you run a cluster and select All cluster nodes in the Cluster Node setting above.</p> <p><b>i</b> If you want to manually select the sensors to include in the report, save your settings and go to the <a href="#">Select Sensors Manually</a><sup>[2774]</sup> tab.</p>
Filter Included Sensors by Tag	<p>Filter the included sensors further. Use this option, for example, if you manually add entire probes, groups, or devices to the report and do not want to include all sensors that have these objects as their parent objects. PRTG then only includes the sensors in the report that have at least one of the tags that you enter here.</p> <p>Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically <a href="#">inherited</a><sup>[138]</sup>. You can also leave the field empty.</p> <p>You can also use the plus sign (+) or the minus sign (-) to categorize tags as <b>must have</b> or <b>must not have</b>, for example, <b>+snmp -wmi</b> (must have the tag <b>snmp</b> and must not have the tag <b>wmi</b>).</p> <p><b>i</b> For performance reasons, it can take some minutes until you can filter for new tags that you added.</p>


## Report Schedule

Setting	Description
Schedule	<p>Define the time at which you want to automatically run the report:</p> <ul style="list-style-type: none"> <li>▪ No schedule (default): Only use the options on the Run Now tab to manually start the report generation.</li> <li>▪ Every full hour: Run the report every 60 minutes.</li> <li>▪ Every day at a specific hour: Run the report every 24 hours. Specify the exact time below.</li> <li>▪ Every specific day of the week: Run the report every 7 days. Specify the exact time below.</li> <li>▪ Every specific day of the month: Run the report on a specific day every month. Specify the exact time below.</li> <li>▪ First day after the quarter: Run the report on the first day after the end of the quarter. This means, for example, on April 1st for the first quarter of the year (January 1st - March 31st).</li> <li>▪ Every specific date: Run the report on a specific date every year. Specify the exact date below.</li> </ul>
Specific Hour	<p><a href="#">This setting is only visible if you select</a> Every day at a specific hour <a href="#">above</a>.</p> <p>From the list, select the hour at which you want to run the report.</p>
Specify Day	<p><a href="#">This setting is only visible if you select</a> Every specific day of the week <a href="#">above</a>.</p> <p>From the list, select a day of the week or a day of the month for which you want to run the report.</p> <p><b>i</b> If you select Last, the report always runs on the last day of the month, regardless of how many days the month has. If you select a date that does not exist in every month, for example, <b>30th</b>, PRTG automatically runs the report on the last day of the month.</p>
Specific Date	<p><a href="#">This setting is only visible if you select</a> Every specific date <a href="#">above</a>.</p> <p>Enter a valid date in the format <b>DD.MM.</b>, for example, <b>31.12</b>. The report runs on this date every year.</p>
Report Handling	<p><a href="#">This setting is only visible if you select one of the schedule options above</a>.</p> <p>Define what you want to do with a finished report:</p>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ Store report and send it by email: Create a .pdf file and, depending on the Data Files setting, create data files of the report, store the files, and send them via email to the email address that you define below. You can find the stored report files on the Stored Reports tab.</li> <li>▪ Store report (default): Create a .pdf file and, depending on the <a href="#">Data Files</a> setting, create data files of the report and store it. You find the stored report files on the Stored Reports tab. You also receive a ToDo ticket. By default, PRTG sends out a notification email to administrators in this case.</li> <li>▪ Send report by email: Create a .pdf file and, depending on the Data Files setting, create data files of the report and send them via email to the email address that you define below. PRTG does not permanently store the report files.</li> </ul> <ul style="list-style-type: none"> <li>ⓘ PRTG only generates .csv and .xml data files for report templates that include data tables.</li> <li>ⓘ To create .pdf files, make sure that the print spooler service runs on the PRTG core server system.</li> <li>ⓘ Some special characters, for example, 4-byte unicode characters, might not be displayed correctly in PDF reports. As a workaround, we recommend that you generate an HTML report and save it as a .pdf file.</li> </ul>
<p>Target Email Address</p>	<p><a href="#">This setting is only visible if you select one of the email options above.</a></p> <p>Enter one or more valid email addresses to which PRTG sends the report. Use commas to separate email addresses.</p> <ul style="list-style-type: none"> <li>ⓘ PRTG sends an email to all recipients. All recipients appear in the To field of the email.</li> <li>ⓘ You can change the configuration for outgoing emails in the <a href="#">Notification Delivery</a> settings.</li> </ul>
<p>Email to User Group</p>	<p><a href="#">This setting is only visible if you select one of the email options above.</a></p> <p>From the list, select a user group to which you send an email with the report. All members of this group receive the email. You can edit user groups in the <a href="#">User Groups</a> settings.</p> <ul style="list-style-type: none"> <li>ⓘ If you define both individual email addresses and select a user group, PRTG sends the report to the individual email addresses as well as to the members of the selected user group.</li> <li>ⓘ PRTG sends an email to all recipients. All recipients appear in the To field of the email.</li> </ul>

Setting	Description
File Compression	<p>This setting is only visible if you select one of the email options above.</p> <p>Define if PRTG compresses the attached report files before it sends them:</p> <ul style="list-style-type: none"> <li>▪ Disable (default): PRTG sends the report files by email in their original size.</li> <li>▪ Enable: PRTG compresses the report files to a .zip file before they are sent by email.</li> </ul>


## Report Period

Setting	Description
Report Period Type	<p>Define the type of period for which you want to create the report:</p> <ul style="list-style-type: none"> <li>▪ Current period: Use monitoring data of the current period.</li> <li>▪ Previous period: Use monitoring data of the previous period.</li> </ul> <p> This setting works in combination with the Period setting below. For example, Previous period means <a href="#">yesterday</a> if you select the Day option.</p>
Period	<p>Define the period that the report covers:</p> <ul style="list-style-type: none"> <li>▪ Day</li> <li>▪ Week</li> <li>▪ Month</li> <li>▪ Quarter of year</li> <li>▪ Year</li> </ul>
Day Period	<p>This setting is only visible if you select Day above.</p> <p>From the list, select the hours at which a day starts and ends. The default setting is 0:00-23:59.</p>
Week Period	<p>This setting is only visible if you select Week above.</p> <p>From the list, select the days of the week when the week starts and ends:</p> <ul style="list-style-type: none"> <li>▪ Monday-Sunday: A reported week starts on the Monday and ends on the Sunday of the week.</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ <a href="#">[Day-Day]</a>: A reported week starts on the <a href="#">[Day]</a> of the week and ends on the <a href="#">[Day]</a> of the following week.</li> </ul>
Month Period	<p><a href="#">This setting is only visible if you select Month above.</a></p> <p>From the list, select the days of the month when the month starts and ends:</p> <ul style="list-style-type: none"> <li>▪ first-last day: A reported month starts on the first day and ends on the last day of the month.</li> <li>▪ <a href="#">[15.-14.]</a>: A reported month starts on the 15th of the month and ends on the 14th of the following month.</li> </ul>
Year Period	<p><a href="#">This setting is only visible if you select Year above.</a></p> <p>From the list, select when the year starts and ends:</p> <ul style="list-style-type: none"> <li>▪ 1/1-12/31: A reported year starts on January 1st and ends on December 31st.</li> <li>▪ 7/1-6/30: A reported year starts on July 1st and ends on June 30th the following year.</li> </ul>
Report Schedule	<p>From the list, select a specific time span for which you want to generate the report. The report only includes monitoring data for specific hours or weekdays within the defined period.</p> <p>Select None to include all available monitoring data in the report, or choose a schedule, for example Weekdays, to exclude all weekends from the report. The available schedules depend on your configuration.</p> <p> For more information, see section <a href="#">Schedules</a> .</p>

## Percentile Handling

Setting	Description
Percentile Results	<p>Define if you want to include an additional <a href="#">percentile calculation</a>  of your data in the report:</p> <ul style="list-style-type: none"> <li>▪ Do not show percentiles: PRTG does not use a percentile formula to calculate your monitoring results. It only shows the standard values.</li> <li>▪ Show percentiles: PRTG displays an overview table with the percentiles of <a href="#">each</a> channel for the whole report period, and the percentiles of the <a href="#">primary</a> channel in the table for each scanning interval.</li> </ul>

Setting	Description
	<p><b>i</b> Percentiles are not available for all report templates. If a template does not support percentiles, they do not show up in the report, even if you enable this setting.</p> <p><b>i</b> Percentiles are also not available for a cluster if you select All cluster nodes in the Cluster Node setting in section Included Sensors. Select a failover node to include percentiles.</p>
Percentile Type	<p><b>This setting is only visible if you select Show percentiles above.</b></p> <p>Enter the percentile type that you want PRTG to use for the calculation. If you choose, for example, to calculate the 95th percentile, enter <b>95</b> here and 5% of peak values are discarded. Enter an integer.</p>
Percentile Averaging Interval	<p><b>This setting is only visible if you select Show percentiles above.</b></p> <p>Enter a value to define the averaging interval on which PRTG bases the percentile calculation. The default value is <b>300</b> seconds (5 minutes). This means that PRTG takes 5-minute averages as basic values for the percentile calculation. Enter an integer.</p>
Percentile Mode	<p><b>This setting is only visible if you select Show percentiles above.</b></p> <p>Select the mode for percentile calculation:</p> <ul style="list-style-type: none"> <li>▪ Discrete: PRTG takes discrete values to calculate percentile results.</li> <li>▪ Continuous: PRTG interpolates between discrete values and bases the calculation on interpolated values.</li> </ul>

## Data Files

Setting	Description
Files in CSV / XML Format	<p>Define if you want to generate .csv and .xml files for data tables in the report in addition to the .pdf file:</p> <ul style="list-style-type: none"> <li>▪ Do not include data files: PRTG does not generate .csv or .xml files for the report. It only creates a .pdf file.</li> <li>▪ Include only .csv files: PRTG generates and stores .csv files in addition to the .pdf file. The data files are only generated if the report uses a report template that includes data tables.</li> <li>▪ Include only .xml files: PRTG generates and stores .xml files in addition to the .pdf file. The data files are only generated if the report uses a report template that includes data tables.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Include all data files: PRTG generates and stores .csv and .xml files in addition to the .pdf file. The data files are only generated if the report uses a report template that includes data tables.</li> </ul> <p><b>i</b> If you run PRTG in a cluster, the report does not generate data files if you select All cluster nodes in the Cluster Node setting. Select a failover node to get data files.</p>

### Report Comments

Setting	Description
Introductory Comment	Enter a custom text that the report displays at the top of the first page. Enter a string or leave the field empty.
Final Comment	Enter a custom text that the report displays below the last data table or graph on the last page. Enter a string or leave the field empty.

### Access Rights

Setting	Description
User Group Access	<p>Define the user groups that have access to the object. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights:</p> <ul style="list-style-type: none"> <li>▪ No access: Users in this user group cannot see or edit the object. The object does not show up in lists.</li> <li>▪ Read access: Users in this user group can see the object and view its settings.</li> <li>▪ Write access: Users in this user group can see the object and view and edit its settings. However, they cannot edit the object's access rights settings.</li> <li>▪ Full access: Users in this user group can see the object, view and edit its settings, and edit its access rights settings.</li> </ul> <p><b>i</b> You can create new user groups in the <a href="#">User Groups</a> settings.</p>

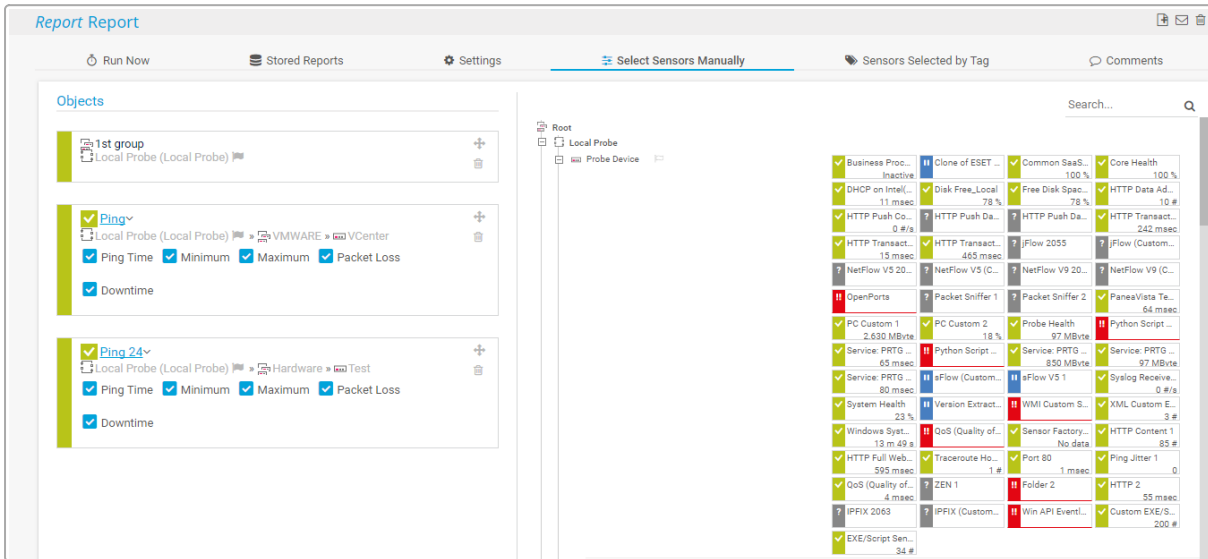
**i** Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

## Select Sensors Manually

Click the Select Sensors Manually tab to manually add sensors that you want to include in the report.

You see a split screen: On the left side, there is a list of objects that the report already contains, and on the right side, you see your device tree. You can add objects to the report via drag-and-drop.




**i** You can also add a report via the [context menu](#) of an object. In this case, the selected object is automatically included in the report.



Select Sensors Manually Tab

The following actions are available:

Action	Description
Add items	<p>From the device tree on the right side, drag objects and drop them onto the list on the left side. You can add entire probes, groups, devices, or single sensors. PRTG adds each dropped object as a new list item.</p> <p><b>i</b> The objects you drop on the left side are always added to the end of the list, you cannot directly add objects in a different order.</p>
Select channels	<p>If you add a sensor to the selection, you can specify the channels that the report includes. By default, PRTG selects all channels. To exclude a channel from the report, disable the check box in front of a channel name.</p> <p><b>i</b> If you run PRTG in a cluster, you can only choose between single channels if you select a specific Cluster Node in the report settings. If you select All cluster nodes, the report contains only the <b>primary</b> channel of each sensor.</p>

Action	Description
Change order	You can change the order of list items on the left side via drag-and-drop. Click  in the upper-right corner of a selected object, drag it to the desired position, and drop it there.
Remove	To remove any objects from the report, click  next to the respective list item, or select several list items while holding down the Ctrl key, then click  .

 PRTG automatically saves your selection. There is no undo function.

 The final report includes both manually selected sensors and sensors selected by tag.

## Sensors Selected by Tag

Click the Sensors Selected by Tag tab to view all sensors that you added to the report by tag in section Included Sensors of the report settings. This is for your information only, you cannot change sensors here.

To edit the sensor selection, go to the Settings tab of the report and change the tags that the report uses to include sensors. Additionally, you can also exclude sensors with specific tags there.

For sensors that you add by tag, PRTG automatically includes all channels in the report unless you use a cluster and select All cluster nodes in the Cluster Node setting of the report. In this case, the report only includes the [primary](#) channel of each sensor.

 The final report includes both manually selected sensors and sensors selected by tag.

## Comments

On the Comments tab, you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

## More

### KNOWLEDGE BASE

What security features does PRTG include?

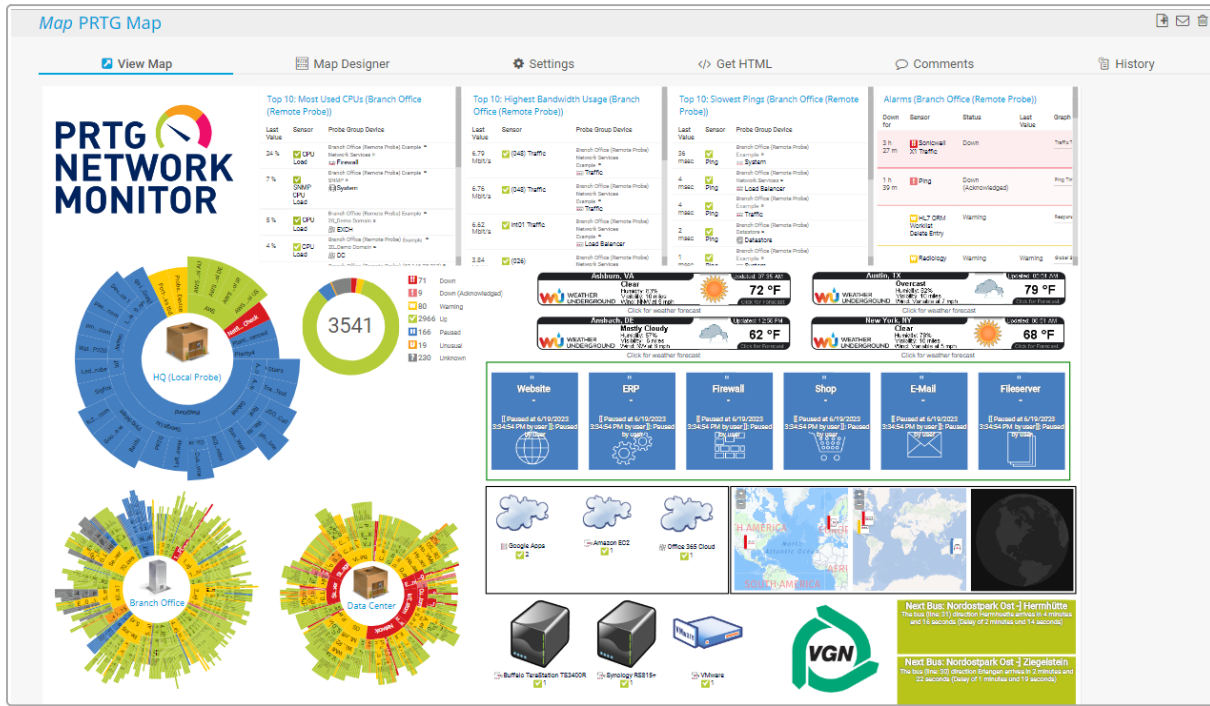
- <https://kb.paessler.com/en/topic/61108>

Creating a PDF report does not work. What can I do?

- <https://kb.paessler.com/en/topic/87084>

## 8.11 Maps

With the [Maps](#) feature, you can create dashboards with monitoring information in a customizable layout. You can also make live data overviews publicly available.



Example of a Map

In this section:

- [Introduction](#)<sup>[2776]</sup>
- [Maps Menu](#)<sup>[2777]</sup>
- [Maps List](#)<sup>[2777]</sup>
- [Home Menu](#)<sup>[2778]</sup>
- [Working with Maps](#)<sup>[2778]</sup>

### Introduction

There are a lot of different options for the implementation of maps:

- Create network maps with status icons for each device.
- Create views of your network that can be shown on network operations center screens.
- Create network overviews that you can publish on the intranet for colleagues or the management.
- Create custom views of the most important sensors in your monitoring setup.
- Create Top 10 lists of the sensors of a specific group or device.

### Map Technology

In technical terms, a map is a common HTML web page. A map can consist of the following elements:

- Map items including device icons, sensor status icons, graphs, data tables, sensor lists, connection lines, geographical maps, or custom HTML code.
- An optional background image in JPG, PNG, or GIF format, for example, your company logo or a graphical view of your network.

### Preconfigured Map

PRTG provides the preconfigured map [Sample Dashboard](#) that you can also edit or delete. The map is only visible to administrators. Define a lower [priority](#)<sup>[224]</sup> for the map to not show it under Home in the [main menu bar](#)<sup>[237]</sup>.




## Maps Menu

Click Maps in the main menu bar to open an overview list of all maps. Hover over Maps to show other options.

Option	Description
All	Open the Maps list where you can view or add custom views of your network status and monitoring data.
Add Map	Open a dialog to create a new map.
Select Map	Hover over Select Map to show a list of your maps. Click a map to open it.

## Maps List

In the All view, you see a list of all maps. Click the name of a map to view it. Enable the check box next to a map and use the quick action buttons:

- Map Rotation (Rotate<sup>[2797]</sup> between maps.
- Clone (clone<sup>[2714]</sup> of this map.
- Delete (settings<sup>[2792]</sup>.

Hover over  and select Add Map from the menu to add a new map.

You can also define the priority of a map. Maps with a 5-star priority ( ★★★★★ ) appear in the main menu bar under Home so that you can directly select them. PRTG can show up to 10 entries in the Home menu.

 For more information, see section [Home Menu](#)<sup>[2778]</sup>.

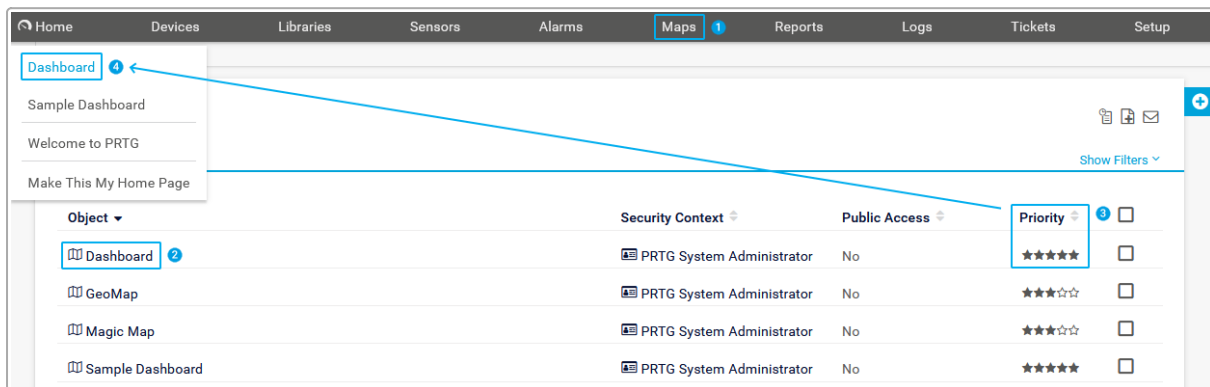
 See also sections [Working with Table Lists](#)<sup>[218]</sup> and [Multi-Edit](#)<sup>[2718]</sup>.

## Home Menu

You can add any map to the Home menu in the main menu bar of the PRTG web interface. This way, you can gain quick access to your most important maps.

**i** If you open a map via the Home menu, it appears as a dashboard without the tabs that are available when you open a map via the Maps menu. Furthermore, in contrast to a map that you open via a URL, the map is embedded in the PRTG web interface with the global header area and page footer.

You can define whether a map appears in the Home menu via the priority setting:



Add Map to Home Menu

1. Open the Maps overview via the main menu bar (1).
2. In the overview list, look for the map that you want to add to the Home menu (2).
3. In the Priority column, select ★★★★★ for the desired map (3).

The map appears in the Home menu (4). To immediately see the change, manually refresh the page with **F5**.

- i** You can include up to 10 map entries in the Home menu.
- i** Every map with a 5-star priority (★★★★★) appears as a menu item under Home.
- i** PRTG provides a sample dashboard in the Home menu by default. You can remove the sample dashboard and other dashboards from the menu by changing their priority to ★★★☆☆ or lower.

## Working with Maps

For more information on how to work with maps and on how to make the maps available to other people, see the following sections:

- [Map Designer](#)<sup>2780</sup>
- [Maps Settings](#)<sup>2792</sup>
- [Map Rotation](#)<sup>2797</sup>




## More

### ■ PAESSLER WEBSITE

How to create dashboards in PRTG with the Maps feature in 5 steps










- <https://www.paessler.com/support/how-to/map-designer>

## 8.11.1 Map Designer

 This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

With the [Map Designer](#) feature, you can create custom web pages as maps, or dashboards, that represent your network.

In this section:

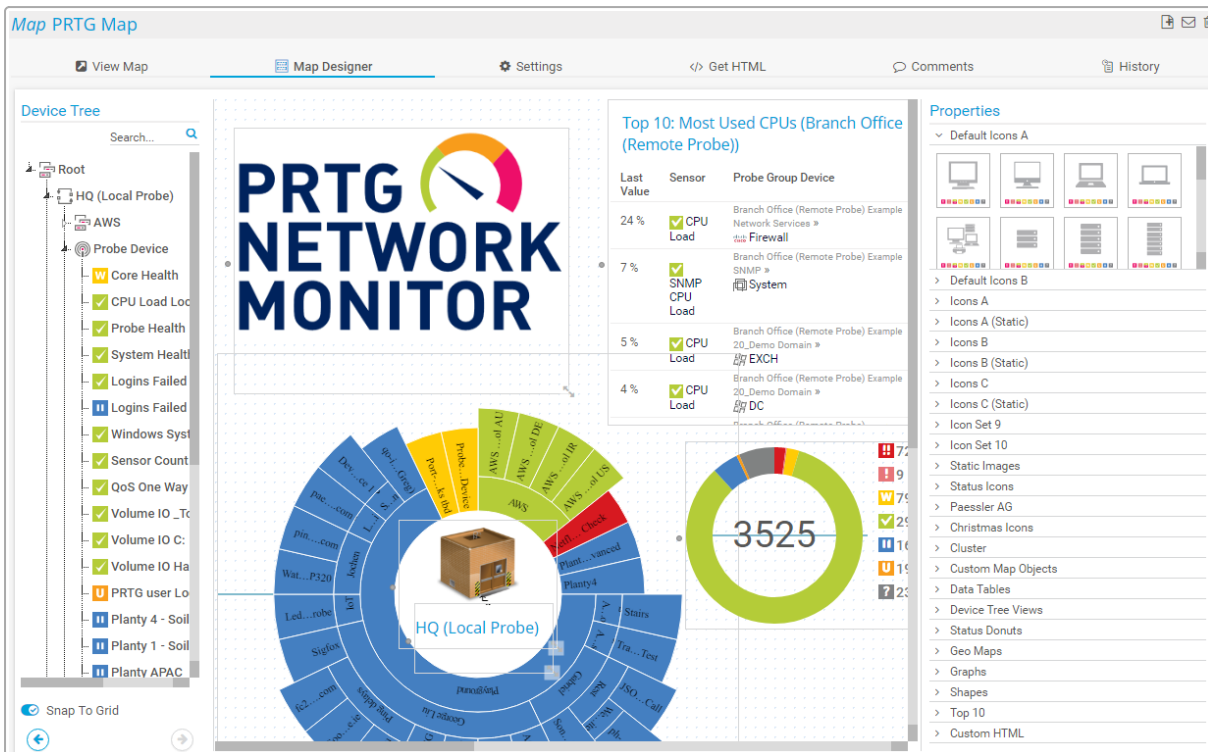
- [Browser Compatibility](#)  2780
- [Basic Design Concept](#)  2780
- [Device Tree Section](#)  2781
- [Properties Section](#)  2783
- [Properties Object Types](#)  2784
- [Edit Map Items](#)  2786
- [Draw Connection Lines Between Items](#)  2789
- [Snap To Grid](#)  2791
- [Undo and Redo](#)  2791

### Browser Compatibility

Because of the map designer's extensive scripting capability, it is important that you use a compatible browser when you edit maps. We recommend that you use Google Chrome 75. You can also use Mozilla Firefox 67 or Microsoft Edge 79. The map designer is **not** fully compatible with earlier versions of Internet Explorer or Opera browsers.

### Basic Design Concept

Click the Map Designer tab to open the map editor. It might take a few moments to load. Here, you can add or change map items to create your individual map.



Map Designer General Layout

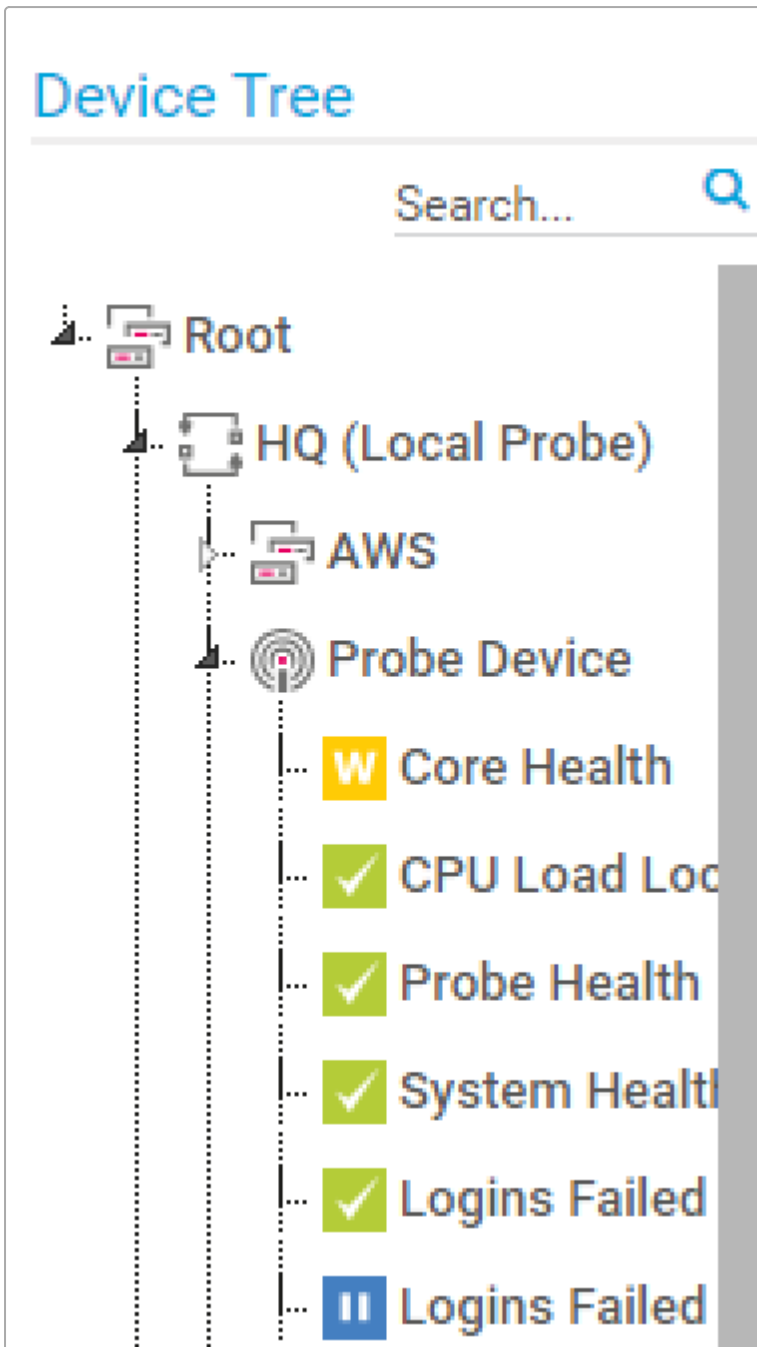
The map designer consists of three main sections:

- The Device Tree section on the left side. Here you can select the object whose data you want to show on the map.
- The map design area in the middle that has the size in pixels that you specified in the [map settings](#) [2793].
- The Properties section on the right side. Here you can define how a map item is displayed, for example, as an icon or a data table.

Drag and drop any object from either side onto the map, or double-click an object. You always see all changes immediately.

## Device Tree Section

Use the Device Tree section to select the object whose data you want to show on the map. This can be a probe, a group, a device, or a single sensor.



Device Tree Section in the Map Designer

The following actions are available:

Action	Description
Find an object	<p>To find the desired object, you have the following options:</p> <ul style="list-style-type: none"> <li>Click <b>▶</b> at the beginning of a line to expand objects in the device tree and show objects below probes, groups, and devices. Click <b>▲</b> to collapse the object again.</li> </ul>

Action	Description
	<ul style="list-style-type: none"> <li>Enter a few characters into the Search box to search for names or parts of names of objects in your configuration. You immediately get the search results. Click <b>x</b> to clear your search.</li> </ul>
Drag-and-drop	<p>You can always drag any object from the device tree onto a free area of the map to create a new map item.</p> <p>If you drag the object onto an existing map item, the displayed device tree object is replaced while the property and size stay the same.</p>
Double-click	<p>Double-click an object in the device tree to add a new map item.</p> <p>If you select a map item and double-click an object in the device tree, the map designer replaces the map item.</p>
Change size	<p>You can adapt the size of the Device Tree section. Drag the right border to the left to make the section smaller. To enlarge the section, drag the right border to the right.</p>

## Properties Section

Use the Properties section to define how to display the map item, for example, as an icon, a map, a table, or a graph. Select the appearance of a map item from different categories.

Properties
> Default Icons A
> Default Icons B
> Icons A
> Icons A (Static)
> Icons B
> Icons B (Static)
> Icons C
> Icons C (Static)
> Static Images
> Status Icons
> Cluster
> Data Tables
> Device Tree Views
> Status Donuts
> Geo Maps
> Graphs
> Shapes
> Top 10 Lists
> Custom HTML

Properties Section in the Map Designer







The following actions are available:

- Hover over an object to get a live preview of it, if available.
- Drag an object onto a free area of the map to create a new map item. If you drag the object onto an existing map item, the property is replaced while the device tree object attributes and size stay the same.
- Double-click an object to add it to the map, or select an existing map item and double-click an object to replace the map item.

**i** If a specific Properties object is not available for a selected Device Tree object, you see a corresponding note in the live preview of the Properties object.

## Properties Object Types

Many different object types are available. Click one of the categories to show all available types.

Object Type	Description
Default Icons A, Default Icons B	Choose from various icons that represent typical network devices in the style of the PRTG web interface. Default icons from category A also display object data. You can see the object name and a sensor overview for the object. This indicates how many sensors show a specific status. For some sensors, a mini graph is shown as well.
Icons A, Icons B, Icons C	Choose from various icons that represent typical network devices. Icons from this category also display object data. You can see the object name and a sensor overview for the object. This indicates how many sensors show a specific status. For some sensors, a mini graph is shown as well.
Icons A (Static), Icons B (Static), Icons C (Static)	Choose from the same icons as in the category described above. Here, only the icon is displayed without additional object data.
Static Images	<p>Choose from various free or public domain geographical maps from different sources.</p> <ul style="list-style-type: none"> <li> Use the category Geo Maps if you want to show geographical maps that include monitoring locations.</li> <li> The items in this category are independent from the selected objects in the device tree.</li> </ul>
Status Icons	<p>Choose from various sensor status icons in different styles. You can see the object name and a sensor overview for the object. This indicates how many sensors show a specific status. For some sensors, a mini graph is shown as well. Additionally, you can add traffic lights or the QR code of an object to your map. A map item for an audible alert that plays a sound when the number of alarms of the monitored object is &gt; 0 is also available.</p> <ul style="list-style-type: none"> <li> Your browser must support playing embedded sounds for the status icon that includes an audible alert.</li> <li> For more information, see the Knowledge Base: <a href="#">Which audible notifications are available in the PRTG web interface and in the PRTG app for desktop?</a></li> <li> If you experience issues with audible notifications in Google Chrome, see the Knowledge Base: <a href="#">Why are audible alerts in public maps not working in Chrome?</a></li> </ul>
Cluster	<p>These map items are only available if you run PRTG in a <a href="#">failover cluster</a><sup>128</sup>. Choose between a map and a status table.</p> <ul style="list-style-type: none"> <li> The Map item does not scale automatically. You need to manually enlarge the item in the map design area.</li> </ul>

Object Type	Description
	<p><b>i</b> If you do not have a cluster, you only see white boxes instead of map previews.</p>
Data Tables	Choose from various <a href="#">table lists</a> <sup>[218]</sup> that show sensors for the selected object. You can also choose from several lists that only show sensors in a specific status.
Device Tree Views	Choose from various <a href="#">device tree views</a> <sup>[174]</sup> , including gauges for the selected object.
Status Donuts	Choose from various status donuts that either show all alarms or all sensor states for the selected object. These are the same status donuts that you see on the Welcome <a href="#">page</a> <sup>[157]</sup> .
Geo Maps	<p>These map items are only available if you enable the <a href="#">Geo Maps</a><sup>[2731]</sup> feature and enter location information in the selected device tree object's settings. Choose between a globe and a geographical map.</p> <p><b>i</b> If the Geo Maps feature is disabled, you only see white boxes instead of map previews.</p>
Graphs	Choose from various graph styles that differ in font size and detail. You can also select graphs that include a legend or sensor states.
Shapes	<p>Choose from various geometrical shapes.</p> <p><b>i</b> The items in this category are independent from the selected objects in the device tree.</p>
Top 10 Lists	<p>Choose from various tables that show the top 10 sensors in specific categories like the highest bandwidth usage or the best availability.</p> <p><b>i</b> The items in this category are independent from the selected objects in the device tree.</p>
Custom HTML	<p>Use this property, for example, to add <a href="#">custom text</a><sup>[2789]</sup>, external images, or applets to your map.</p> <p>Drag the item to the map design area and select it to <a href="#">edit</a><sup>[2786]</sup> it. You can then copy your custom code into the HTML Before and HTML After fields.</p>

## Edit Map Items

### Properties Section



Click a map item to select it. You can then edit its attributes in the upper part of the Properties section.

### Properties

Top:	Left:	Width:	Height:	Layer:
100	50	350	460	2

External Link: Select object

---

HTML Before:

HTML After:

Edit Map Items in the Properties Section

Property	Description
Top Left	<p>Enter position values to directly position the item on the map. Enter a positive integer.</p> <p><b>i</b> You can also use the mouse to move a map item.</p>
Width Height	<p>Enter size values to give the item a predefined size. Enter a positive integer.</p> <p><b>i</b> You can also use the mouse to resize a map item.</p>
Layer	<p>Enter a layer value that defines if an item appears in front of or behind a different item if the items overlap. The item with the higher value appears in front. Enter a positive integer.</p> <p><b>i</b> You can also use the <a href="#">context buttons</a> <sup>[2788]</sup> of a map item to bring it an item to the front (⬆) or send it back one layer (⬇).</p>
External Link	<p>Enter the address of any web page. If you click the map item while you view the map, PRTG opens the web page in a browser window. Enter the full URL of an external website, for example, <a href="https://www.paessler.com">https://www.paessler.com</a>, or the address of a subpage of your PRTG installation, for example, <a href="#">devices.htm</a>.</p> <p><b>i</b> To make a map interactive, you need to define a suitable <a href="#">public access</a> <sup>[2794]</sup> setting for the map.</p>

Property	Description
HTML Before HTML After	Enter custom HTML code to embed an object in the map. Any HTML code you enter in these fields is added before or after the map item and your HTML object is inserted into the map. For example, you can enter <code>&lt;img src="https://media.paessler.com/common/img/logoclaim_r1.gif"&gt;</code> to insert an image of a Paessler logo.

**i** Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

### Context Buttons

Hover over a map item to show its context buttons.



Edit Map Items via Context Buttons

Context Button	Description
Bring to front	Move this item one layer to the front. This is useful when you add several items to a map that overlap each other.
Send to back	Move the item one layer to the back. This is useful when you add several items to a map that overlap each other.
Delete	Delete the item. <b>i</b> The item is immediately deleted without notice. You cannot undo this action. <b>i</b> You can also select the item and press the Delete key on your keyboard.
Drop Connections	Delete all <a href="#">connection lines</a> <small>(2789)</small> to the item.

## Cursor Keys

Select a map item and use the cursor keys to move the item one pixel at a time. Hold down the Shift key in combination with the cursor keys to move the object 10 pixels at a time.

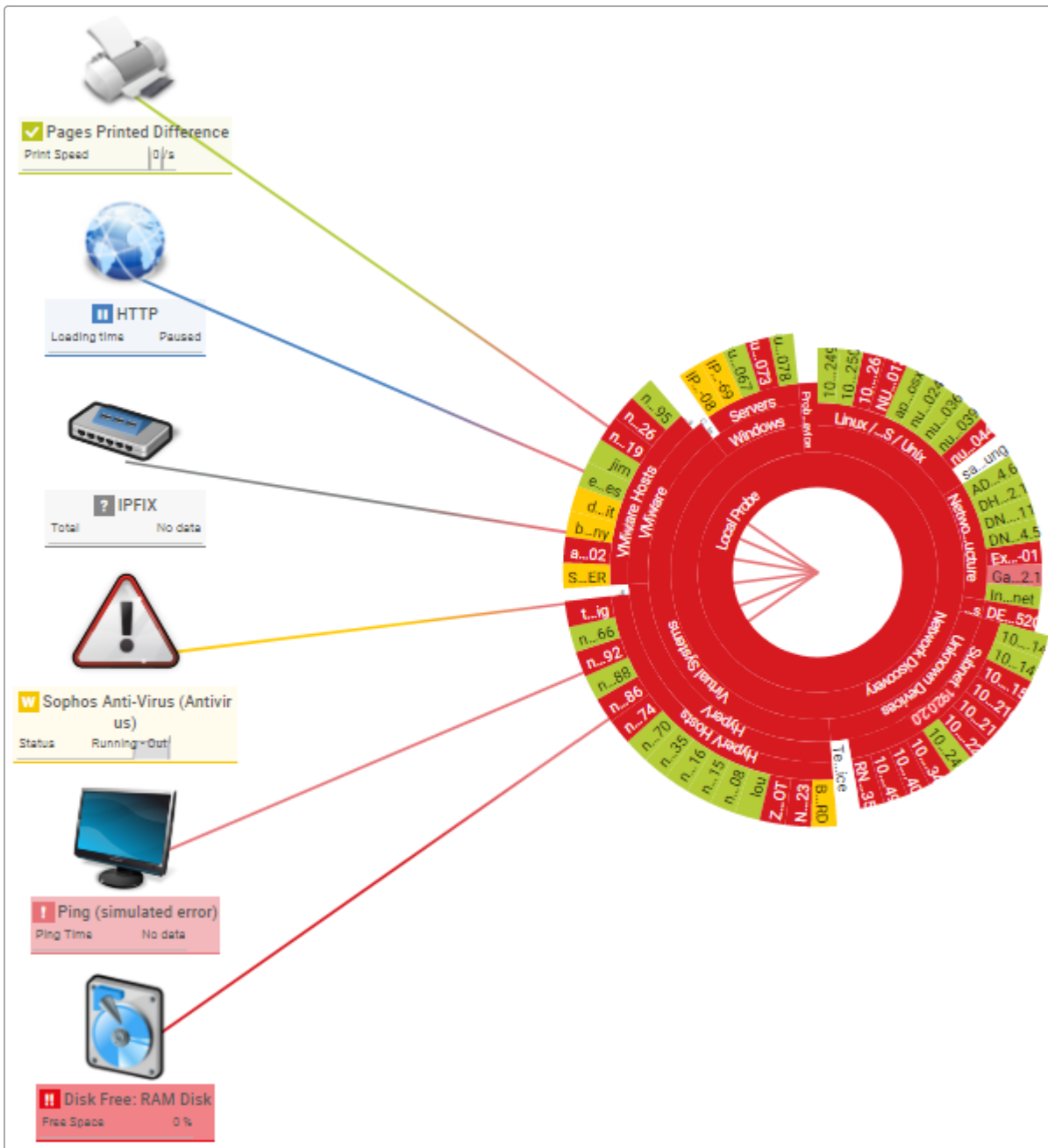
## Add Custom Text

You can add custom text with individual styling to your map with the Custom HTML Element.

■ For more information, see the Knowledge Base: [How to add text to a map?](#)

## Draw Connection Lines Between Items

You can draw connection lines between any map items via drag-and-drop to indicate, for example, network connections or a logical coherence between two items.





Map with Connection Lines



- Click the gray handle to the left of an item and drag it onto the item with which you want to create a connection to create a connection line.
  - Hover over a connection line and click ✂ to delete it.
- ⓘ The map designer dynamically colors the lines between items depending on the [status](#) <sup>181</sup> of the linked objects. A line is red, for example, if the linked objects both show the Down status. Connection lines can also have two colors. For example, if one linked object shows the Down status and the second linked object shows the Warning status, one half of the line is red and the other half is yellow.

## Snap To Grid

With the Snap To Grid setting, you can define how map items are positioned when you add or remove them via drag-and-drop.

Click  at the bottom of the Device Tree section to enable Snap To Grid so that you can only place items aligned with the grid. Click  to disable Snap To Grid to place map objects freely.

## Undo and Redo

You can undo previous changes to the map and its items by clicking  (Ctrl+Z) at the bottom of the Device Tree section. To redo actions, click  (Ctrl+Y). You can undo and redo up to 50 changes when you work on a map. Because PRTG saves changes persistently in your configuration, you can even revert changes at a later point in time.

 Both buttons are only available if they can apply, otherwise they are grayed out.

## More

### KNOWLEDGE BASE

Which audible notifications are available in the PRTG web interface and in the PRTG app for desktop?

- <https://kb.paessler.com/en/topic/26303>

Why are audible alerts in public maps not working in Chrome?

- <https://kb.paessler.com/en/topic/83142>

How to add text to a map?

- <https://kb.paessler.com/en/topic/11523>

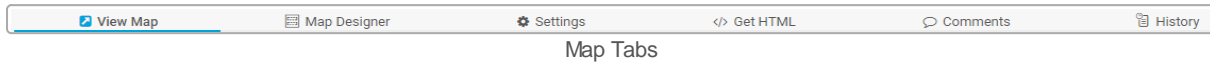
Why does my browser show an unresponsive script warning while loading the Map Designer?

- <https://kb.paessler.com/en/topic/19483>

## 8.11.2 Maps Settings

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

Use the maps tabs to access all functionalities and settings of a map.



### Settings

Click the Settings tab to open the general settings of a map.

**i** In the Add Map dialog, not all of these settings are available. You can change the settings later via the Settings tab.

### Basic Map Settings

Setting	Description
Map Name	<p>Enter a name to identify the map.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Tags	<p>Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically <a href="#">inherited</a><sup>[138]</sup>.</p> <p><b>i</b> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (&lt;&gt;).</p> <p><b>i</b> For performance reasons, it can take some minutes until you can filter for new tags that you added.</p>
Security Context and Color Mode	<p>Define the security context that the map uses for access to monitoring data. Select a user account from the dropdown list to define which objects are visible on the map. The map only contains objects that the selected user has the <a href="#">access rights</a><sup>[145]</sup> to view. By default, the security context is the user account that creates the map.</p> <p><b>i</b> Basically, the security context defines the minimum access rights to objects like libraries, reports, or maps, that a user account has. If the security context of an object is <a href="#">PRTG System Administrator</a>, for example, every user sees all objects in a library, in a report, or on a map, no matter what the particular user access rights are.</p>

Setting	Description
	<p><b>i</b> This setting also affects the <a href="#">color mode</a> (2805) of <a href="#">public maps</a> (2794). PRTG takes the color mode setting of the security context user account.</p>
Time Zone	Define the time zone that the map uses for all date-related settings. Select a time zone from the dropdown list.
Filter by Tag	<p>This setting applies to table map objects. Enter one or more tags separated by a space or comma to include sensors in map data tables. Only sensors that have one of the specified tags appear in the tables, including sensors that <a href="#">inherit</a> (136) tags from parent objects. Enter a string or leave the field empty.</p> <p><b>i</b> For performance reasons, it can take some minutes until you can filter for new tags that you added.</p> <p><b>i</b> For some map objects, for example for sunburst and treemap objects, the tag filter applies only to probes, groups, and devices. If you only enter tags of sensors, these map objects do not appear on the map. Filtering sunburst and treemap objects with multiple tags might not work properly and is not officially supported.</p> <p><b>i</b> Use this setting with caution because it affects all tables of the map.</p>

## Map Layout

Setting	Description
Map Width	Define the width of the map in pixels. Enter an integer.
Map Height	Define the height of the map in pixels. Enter an integer.
Automatic Scaling	<p>Define if you want the map to automatically adapt to your screen size:</p> <ul style="list-style-type: none"> <li>▪ Scale map view to fit browser size: The size of the map automatically adapts to the size of your screen. We recommend that you use this option if you display the map on different screens with different resolutions. <ul style="list-style-type: none"> <li><b>i</b> This setting does not apply to the map designer.</li> </ul> </li> <li>▪ Do not automatically scale map view: The map always uses the specified width and height settings.</li> </ul>
Background Image	<p>Define if you want to use a background image for the map:</p> <ul style="list-style-type: none"> <li>▪ Use a background image: Use a custom background image, for example, your company logo.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>Do not use a background image: Use a background that shows the color that you define in the Background Color setting.</li> </ul>
Custom Image	<p>This setting is only visible if you select Use a background image <a href="#">above</a>.</p> <p>Click Select File and select an image from your system or network.</p> <p><b>i</b> PRTG only supports images in JPG, PNG, and GIF format. The file size must be smaller than <b>20 MB</b>.</p>
Background Color	<p>Select a background color for this map. Either enter a hex color code or choose a color from the color selector. The hex color code field always displays the defined color.</p>

## Map Access

Setting	Description
Public Access	<p>Define who can view the map:</p> <ul style="list-style-type: none"> <li>No public access: Do not allow public access to the map. Users who want to view the map first need to log in to PRTG. They also need sufficient access rights to the map.</li> <li>Allow public access: Allow access to the map via a unique URL. The URL contains a secret key that you can change. The map is an interactive public map.</li> <li>Allow public access but disable all links except for Geo Maps: Allow access to the map via a unique URL. The URL contains a secret key that you can change. If you select this option, all links on the map are disabled so that you get a non-interactive public map. <ul style="list-style-type: none"> <li><b>i</b> It is not possible to disable the links in map objects that contain an embedded <a href="#">geographical map</a><sup>[2731]</sup>. As a workaround, place an empty, transparent square object over the Geo Map object and link it to an unrelated URL.</li> <li><b>i</b> PRTG displays maps with public access in the color mode defined for the security context user account.</li> </ul> </li> </ul>
Secret Key	<p>This setting is only visible if you select Allow public access or Allow public access but disable all links except for Geo Maps <a href="#">above</a>.</p> <p>The secret key is automatically generated. It is part of the public URL for the map. You can also enter a customized string.</p>



Setting	Description
	<p><b>i</b> We recommend that you use the default value.</p> <p><b>■</b> For more information on public access, see section <a href="#">Get HTML</a><sup>2795</sup>.</p> <p><b>i</b> The characters comma (,) and colon (:) are not allowed in the secret key field.</p>

## Access Rights

Setting	Description
User Group Access	<p>Define the user groups that have access to the object. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights:</p> <ul style="list-style-type: none"> <li>▪ No access: Users in this user group cannot see or edit the object. The object does not show up in lists.</li> <li>▪ Read access: Users in this user group can see the object and view its settings.</li> <li>▪ Write access: Users in this user group can see the object and view and edit its settings. However, they cannot edit the object's access rights settings.</li> <li>▪ Full access: Users in this user group can see the object, view and edit its settings, and edit its access rights settings.</li> </ul> <p><b>i</b> You can create new user groups in the <a href="#">User Groups</a><sup>2912</sup> settings.</p>

**i** Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

## Get HTML

Your map is a standard HTML page. You can make it available to other people via a unique URL. Depending on the map's Public Access [setting](#)<sup>2794</sup>, a visitor needs to provide login credentials for PRTG to view the map, or they immediately see the map.

You have different options to link to the map:

- Option 1: Link To The Map With Required Login  
A user who wants to view the map via the shown URL first needs to log in to PRTG.
  - i** In the URL, PRTG usually specifies the IP address under which the page is reachable. If a network address translation (NAT) is set in your firewall, or if you want to use a domain name or a name from a dynamic Domain Name System (DNS) service for public access, customize the URL according to your needs.

- Option 2: Link To The Map Without A Login  
People who want to view the map via the shown URL do not need login credentials. Allow public access to the map to make it available to the public.
- ⓘ In the URL, PRTG usually specifies the IP address under which the page is reachable. If a NAT is set in your firewall, or if you want to use a domain name or a name from a dynamic DNS service for public access, customize the URL according to your needs.
- Option 3: Show the Map on Other Webpages via an Iframe  
Here you can find the HTML code to embed an [iframe](#) in your web page. It includes a URL for direct access to the map. Allow public access to the map to make it available to the public.
- ⓘ In the URL, PRTG usually specifies the IP address under which the page is reachable. If a NAT is set in your firewall, or if you want to use a domain name or a name from a dynamic DNS service for public access, customize the URL according to your needs.

## Comments

On the Comments tab, you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

## History

On the History tab, all changes in the settings of an object are logged with a time stamp, the name of the user who made the change, and a message. The history log retains the last 100 entries.

## Delete

You can delete a map at any time. To do so, click  in the upper-right corner of the screen.

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

### 8.11.3 Map Rotation



With the [Map Rotation](#) feature, you can rotate between several maps on one page. This is similar to a slide show.

#### Map Rotation Setup

To configure your custom map rotation, take the following steps:

Object	Security Context	Public Access	Priority	
Magic Map	PRTG System Administrator	No	★★★★☆	<input checked="" type="checkbox"/>
Map	PRTG System Administrator	No	★★★★☆	<input type="checkbox"/>
Map 1	PRTG System Administrator	Yes	★★★★☆	<input checked="" type="checkbox"/>
Map 2	PRTG System Administrator	No	★★★★★	<input type="checkbox"/>
Map 3	PRTG System Administrator	No	★★★★☆	<input checked="" type="checkbox"/>
Global Status	PRTG System Administrator	No	★★★★☆	<input type="checkbox"/>
My Map	PRTG System Administrator	No	★★★★☆	<input type="checkbox"/>
Sample Dashboard	PRTG System Administrator	No	★★★★☆	<input type="checkbox"/>

Map Rotation Setup

1. Open the Maps overview from the main menu bar.
2. Select the maps that you want to rotate by enabling the check box next to the respective maps. The [multi-edit](#) menu appears.
3. Click .
4. PRTG now rotates the selected maps on a new page in a specific interval.
5. You can change the interval until a new map appears. Hover over  in the lower-right corner and choose from 10s, 30s, 60s (seconds), 10m (minutes), and Refresh (now).

 To view the maps that you specified for the map rotation, you need login credentials for PRTG.


#### Public Map Rotation

You can also set up a [public](#) map rotation that you can use without login credentials. For this purpose, you need to create a custom URL that includes the map IDs and the maps' secret keys:

1. In the Public Access [settings](#) of all maps that you want to include in the map rotation, select Allow public access. The Secret Key setting appears.
2. Note the secret keys of all maps that you want to include in the map rotation.
3. Find the map IDs and note them as well. To find the ID of a map, open the map with your browser. The map ID is included in the URL of the map as the value of the parameter `id`. In the URL <https://<yourprtgserver>/map.htm?id=2124>, for example, the number 2124 is the needed ID.


4. Create the public map rotation URL. The complete URL has the following format:

[https://yourprtgserver/public/mapshow.htm?  
ids=mapid1:secretkey1,mapid2:secretkey2,mapid3:secretkey3](https://yourprtgserver/public/mapshow.htm?ids=mapid1:secretkey1,mapid2:secretkey2,mapid3:secretkey3).

-  Make sure that you connect each map ID and the respective secret key with a colon, and that you separate each `mapid:secretkey` token from the next `mapid:secretkey` token with a comma.

This is an example URL for the public rotation of two maps with the map IDs 9507 and 9358:

[https://prtg.example.com/public/mapshow.htm?ids=9507:4049BEA1-B89C-4B5D-ACC4-  
3C8E00566EB8,9358:718D3CE1-DF00-4B92-AE8A-E0253B912C37](https://prtg.example.com/public/mapshow.htm?ids=9507:4049BEA1-B89C-4B5D-ACC4-3C8E00566EB8,9358:718D3CE1-DF00-4B92-AE8A-E0253B912C37)

5. Open the URL in your browser to start the public map rotation.
6. You can change the interval until a new map appears. Hover over  in the lower-right corner and choose from 10s, 30s, 60s (seconds), 10m (minutes), and Refresh (now).

## 8.12 Setup






In the setup settings of the PRTG web interface, you can define almost all system settings for PRTG. However, you need to define some of the machine-oriented settings via two Windows administration tools (see section [Others](#) <sup>[2800]</sup> below).

Click Setup in the [main menu bar](#) <sup>[249]</sup> to show the available options.

 Some setup options are only available for PRTG Network Monitor (marked with ) , so you cannot use these with PRTG Hosted Monitor.

 Some setup options are only available for PRTG Hosted Monitor (marked with ) , so you cannot use these with PRTG Network Monitor.



In this section:

- [Account Settings](#) <sup>[2801]</sup>
  - [My Account](#) <sup>[2801]</sup>
  - [Notification Templates](#) <sup>[2808]</sup>
  - [Notification Contacts](#) <sup>[2842]</sup>
  - [Schedules](#) <sup>[2846]</sup>
  - [API Keys](#) <sup>[2851]</sup>
- [System Administration](#) <sup>[2855]</sup>
  - [Manage Subscription](#) 
  - [User Interface](#) <sup>[2855]</sup>
  - [Monitoring](#) <sup>[2869]</sup>
  - [Notification Delivery](#) <sup>[2877]</sup>
  - [Core & Probes](#) <sup>[2887]</sup>
  - [User Accounts](#) <sup>[2901]</sup>
  - [User Groups](#) <sup>[2912]</sup>
  - [Administrative Tools](#) <sup>[2918]</sup>
  - [Cluster](#) <sup>[2923]</sup> 
  - [Single Sign-On](#) <sup>[2925]</sup>
  - [Maintainer Mode](#) <sup>[2931]</sup>
- [PRTG Status](#) <sup>[2935]</sup>
  - [System Status](#) <sup>[2935]</sup>
  - [Cluster Status](#) <sup>[2960]</sup> 
- [License Information](#) <sup>[2962]</sup> 
- [Auto-Update](#) <sup>[2969]</sup> 

- [Optional Downloads](#)  2974
- [Help and Support Center](#)  2976
- [Contact Support](#)  2977

## Others

There are some settings that you need to make in the [PRTG Administration Tool](#)  3040.






- For more information, see sections [PRTG Administration Tool on PRTG Core Server Systems](#)  3041 and [PRTG Administration Tool on Remote Probe Systems](#)  3067.

## 8.12.1 Account Settings

To open the account settings of the user, select Setup | Account Settings from the [main menu bar](#) . Select the various tabs to change the different settings.





In this section:

- [My Account](#) 
- [Notification Templates](#) 
- [Notification Contacts](#) 
- [Schedules](#) 
- [API Keys](#) 








### 8.12.1.1 My Account

On the My Account tab, you can define and edit settings for the user account. All settings are specific to the user account.

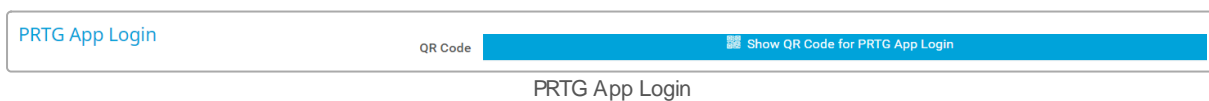
 This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

 If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.

In this section:

- [PRTG App Login](#) 
- [User Account Settings](#) 
- [API Access](#) 
- [Account Settings](#) 
- [Group Membership](#) 
- [PRTG Web Interface](#) 
- [Ticket System](#) 

### PRTG App Login



Setting	Description
QR Code	Click Show QR Code for PRTG App Login to display the QR code and to copy your account settings to a <a href="#">PRTG app</a> .

## User Account Settings

User Account Settings

Login Name

Display Name

Primary Email Address






Password  Do not change the password  
 Specify a new password

Passhash

User Account Settings

Setting	Description
Login Name	<p>Enter a login name for the user account.</p> <p><b>i</b> The login name must not contain the following invalid characters: " / \ [ ] : ;   = , + * ? &lt; &gt;</p> <p><b>i</b> This option is not available in PRTG Hosted Monitor.</p>
Display Name	<p>Enter a display name that you recognize. PRTG uses it for display purposes only, for example on the Welcome page.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Primary Email Address	<p>Enter the primary email address. This is the email address that PRTG uses by default for the ticket system, including important system messages, and password recovery.</p> <p><b>i</b> Make sure that your email client can show HTML emails, otherwise you cannot read emails from PRTG.</p>
Password	<p>Define whether to change the password for the user account:</p> <ul style="list-style-type: none"> <li>▪ Do not change the password</li> <li>▪ Specify a new password</li> </ul> <p><b>i</b> For security reasons, PRTG does not display the password.</p>





Setting	Description
	<p>If you specify a new password, enter the old password, then enter the new password twice.</p> <ul style="list-style-type: none"> <li> The new password must be at least 8 characters long. It must contain a number and a capital letter.</li> <li> Do not use leading or trailing whitespaces in the new password.</li> <li> This option is not available in PRTG Hosted Monitor.</li> </ul>
Passhash	<p>Click Show passhash to display the passhash for the user account. This is necessary for authentication for the <a href="#">PRTG API</a>.</p> <ul style="list-style-type: none"> <li> This setting is for your information only. You cannot change it.</li> <li> This option is not available in PRTG Hosted Monitor.</li> </ul>


## API Access

 These settings are only available in PRTG Hosted Monitor.



**API Access**

API User Name  johnqpublic@example.com

API Passhash  Show passhash

Generate API Passhash  Generate new passhash

API Access

Setting	Description
API User Name	<p>Shows the API user name of the user account. This is necessary for authentication for the PRTG API.</p> <ul style="list-style-type: none"> <li> This setting is for your information only. You cannot change it.</li> </ul>
API Passhash	<p>Click Show passhash to display the API passhash of the user account. This is recommended for authentication for the PRTG API.</p> <ul style="list-style-type: none"> <li> This setting is for your information only. You cannot change it.</li> </ul>
Generate API Passhash	<p>Click Generate new passhash to reset the passhash of the user.</p>

## Account Settings

### Account Settings

Primary Group  ⓘ

PRTG Administrators

Status  ⓘ

Active

Last Login  ⓘ

06/09/2023 15:09:34

Account Settings

Setting	Description
Primary Group	<p>Select the primary group for the user account from the dropdown list.</p> <ul style="list-style-type: none"> <li><span style="font-size: 0.8em;"> ⓘ</span> Every user account must be a member of a primary group to make sure there is no user account without group membership. Membership in other user groups is optional.</li> <li><span style="font-size: 0.8em;"> ⓘ</span> You cannot change the primary group of <a href="#">Active Directory users</a>. Users that you add via <a href="#">Active Directory integration</a> can only have the respective Active Directory group as their primary group.</li> </ul>
Status	<ul style="list-style-type: none"> <li><span style="font-size: 0.8em;"> ⓘ</span> This setting is for your information only. You cannot change it.</li> </ul>
Last Login	<p>Shows the time stamp of the last login of the user account.</p> <ul style="list-style-type: none"> <li><span style="font-size: 0.8em;"> ⓘ</span> This setting is for your information only. You cannot change it.</li> </ul>

## Group Membership

### Group Membership

Member of  ⓘ

▼
User Group Name

PRTG Administrators

PRTG Users Group

User Group1

Group Membership

Setting	Description
Member of	<p>Shows the user groups that the user account is a member of. You can define access rights to device tree objects, libraries, maps, reports and the ticket system at group level.</p> <p><b>i</b> This setting is for your information only. You cannot change it.</p>

## PRTG Web Interface

**PRTG Web Interface**

**Automatic Refresh** i  Automatically refresh pages (default)  
 Do not automatically refresh pages

**Refresh Interval (Sec.)** i 30

---

**Audible Alarms** i  Do not play audible alarms (default)  
 Play audible alarms on dashboard pages only  
 Play audible alarms on all pages

**Home Page URL** i /welcome.htm






**Time Zone** i (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

**Date Format** i Use System Settings

**Color Mode** i  Light (default)  
 Dark

PRTG Web Interface

Setting	Description
Automatic Refresh	<p>Define if you want PRTG to automatically reload web pages in the PRTG web interface for the user:</p> <ul style="list-style-type: none"> <li>Automatically refresh pages (default): PRTG automatically refreshes single page elements on web pages in the PRTG web interface.</li> <li>Do not automatically refresh pages: PRTG does not automatically refresh single page elements on web pages in the PRTG web interface.</li> </ul>
Refresh Interval (Sec.)	<p><b>This setting is only visible if you select</b> Automatically refresh pages (default) <b>above.</b></p> <p>Enter the number of seconds that PRTG waits between two refreshes. We recommend that you use 30 seconds or more. The minimum value is 20 seconds. The maximum value is 600 seconds.</p>

Setting	Description
	<p> Shorter refresh intervals create more CPU load on the probe system. If you experience load issues while using the PRTG web interface (or <a href="#">maps</a><sup>[2776]</sup>), set a longer refresh interval.</p>
Audible Alarms	<p>Define whether PRTG plays an audible alarm on web pages in the PRTG web interface when there is a new <a href="#">alarm</a><sup>[2801]</sup>:</p> <ul style="list-style-type: none"> <li>▪ Do not play audible alarms (default): PRTG does not play sound files on any web pages.</li> <li>▪ Play audible alarms on dashboard pages only: When there is a new alarm, PRTG plays a predefined sound on <a href="#">dashboard</a><sup>[237]</sup> pages only. The sound is played with every refresh of the dashboard page if there is at least one new alarm.</li> <li>▪ Play audible alarms on all pages: When there is a new alarm, PRTG plays a predefined sound on all web pages. PRTG plays the sound with every page refresh if there is at least one new alarm.</li> </ul> <p> PRTG only plays audible alarms if the New Alarms value in the <a href="#">global header area</a><sup>[168]</sup> of the PRTG web interface is greater than 0 after a page refresh. PRTG does not consider the number of old alarms.</p> <p> For more information, see the Knowledge Base: <a href="#">Which audible notifications are available in the PRTG web interface and in the PRTG app for desktop?</a> and <a href="#">Why are audible alerts in public maps not working in Chrome?</a></p>
Home Page URL	<p>Define the user's default home page in the PRTG web interface. This is the page that the user sees after logging in or when selecting <a href="#">Home</a><sup>[237]</sup> from the main menu. Enter a PRTG-internal web page.</p>
Time Zone	<p>Define the time zone for the user account. Depending on the time zone that you select, PRTG shows the local time zone of the user account in all data tables and graph legends.</p> <p> PRTG receives the Coordinated Universal Time (UTC) from the system time of the PRTG core server for this purpose.</p> <p> If you get a warning message about differing time zones, see the Knowledge Base: <a href="#">Why do I get a warning message when time zones differ?</a></p>
Date Format	<p>Select the date format for the user:</p> <ul style="list-style-type: none"> <li>▪ Use default settings: Use the date format of the PRTG core server system.</li> <li>▪ DD.MM.YYYY HH:MM:SS (24h)</li> <li>▪ DD.MM.YYYY HH:MM:SS (A.M./P.M.)</li> <li>▪ MM/DD/YYYY HH:MM:SS (24h)</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ MM/DD/YYYY HH:MM:SS (A.M./P.M.)</li> <li>▪ YYYY-MM-DD HH:MM:SS (24h)</li> <li>▪ YYYY-MM-DD HH:MM:SS (A.M./P.M.)</li> </ul> <p><b>i</b> This setting takes effect after the next login.</p>
Color Mode	<p>Select a color mode for the PRTG web interface:</p> <ul style="list-style-type: none"> <li>▪ Light (default)</li> <li>▪ Dark</li> </ul>

## Ticket System

**Ticket System**

Email Notifications **i**

Receive an email when a ticket changes (default)  
 Do not receive any emails from the ticket system

Ticket System

Setting	Description
Email Notifications	<p>Define if the user receives emails from the ticket system:</p> <ul style="list-style-type: none"> <li>▪ Receive an email when a ticket changes (default): The user receives an email each time a ticket is assigned to the user or to the user group they are a member of, or if a ticket is changed.             <ul style="list-style-type: none"> <li><b>i</b> If the user edits tickets that are assigned to them or the user group they are a member of, or if they assign a ticket to themselves or their user group, they do not get an email.</li> </ul> </li> <li>▪ Do not receive any emails from the ticket system: The user does not receive any emails from the ticket system.</li> </ul>

**i** Save your settings. If you leave the page, all changes to the settings are lost.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Which audible notifications are available in the PRTG web interface and in the PRTG app for desktop?

- <https://kb.paessler.com/en/topic/26303>

Why are audible alerts in public maps not working in Chrome?

- <https://kb.paessler.com/en/topic/83142>

Why do I get a warning message when time zones differ?

- <https://kb.paessler.com/en/topic/81306>

## Others

There are some settings that you must define in the [PRTG Administration Tool](#)<sup>30401</sup>. For more information, see sections:

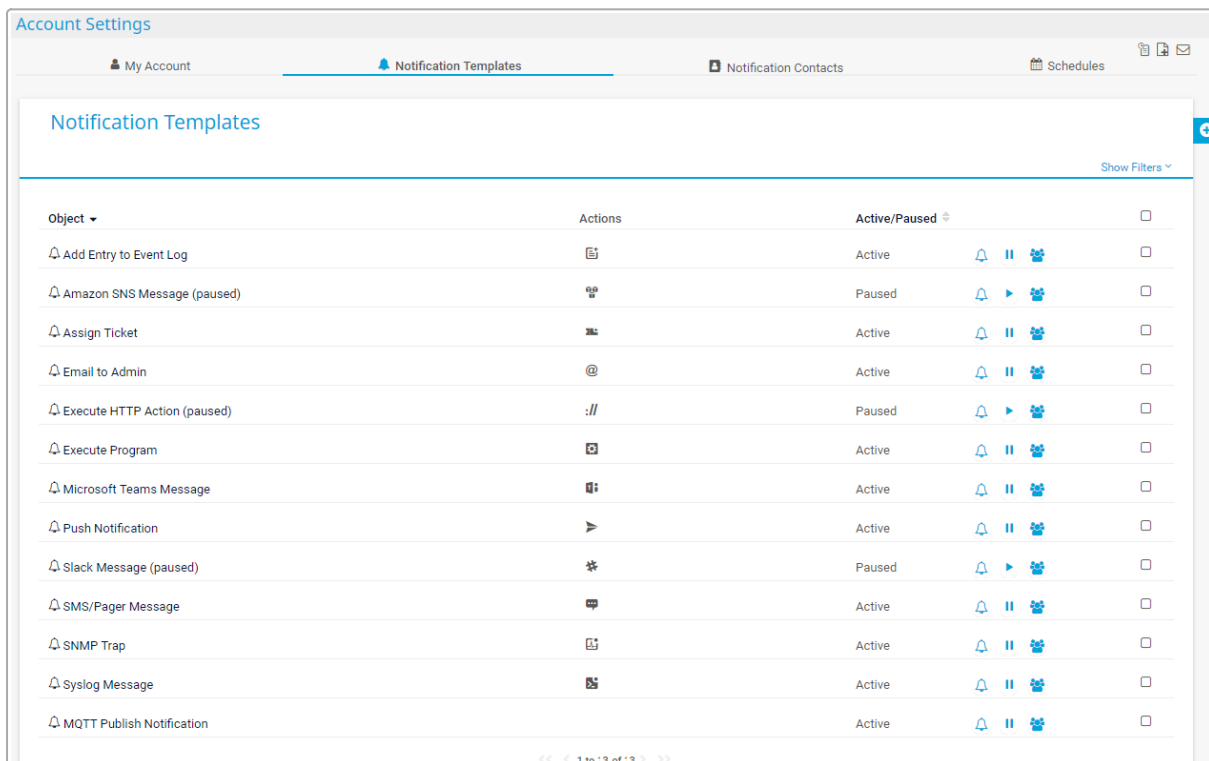
- [PRTG Administration Tool on PRTG Core Server Systems](#)<sup>30411</sup>
- [PRTG Administration Tool on Remote Probe Systems](#)<sup>30671</sup>

### 8.12.1.2 Notification Templates

On the Notification Templates tab, you can define and edit user account-specific notifications. You can use notification templates to trigger notifications for specific [sensor states](#)<sup>1811</sup> and values.








**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

**☁** If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.








Notification Templates Tab


In this section:

- [Note](#) 
- [Overview](#) 
- [Notification Template Settings](#) 
- [Basic Settings](#) 
- [Notification Summarization](#) 
- [Access Rights](#) 
- [Notification Methods](#) 

## Note

You must take the following four steps to set up and use notifications:

1. Check and set up the [notification delivery](#)  settings if you use PRTG Network Monitor. These settings define how PRTG sends messages.
2. Check and set up [notification contacts](#)  for the user accounts. These contacts define the recipients to which PRTG sends notifications.
3. Check and set up several [notification templates](#) . These templates define the notification methods and their content.
  - ❶ You can also check or edit notification templates via the Notification Triggers tab. For more information, see section [Notification Triggers Settings](#) .
4. Check and set up [notification triggers settings](#)  for objects. These triggers define when PRTG sends notifications.








❶ Usually, there are three successive attempts to deliver a notification. If all of these attempts fail, the notification is lost. To never miss a notification, we recommend that you always set up at least two notifications with different notification methods for a notification trigger, for example, one email notification and one SMS notification. If delivery via email fails, PRTG can still notify you via smartphone as a fallback. For example, use the latency setting of a [state trigger](#)  to choose a notification with a different notification method than in the first trigger condition, or set up a second trigger with a different notification method for the corresponding object.





■ For a detailed step-by-step guide, see the Paessler website: [How to set up notifications via the PRTG web interface](#).

■ Custom notification scripts are also available in the [PRTG Sensor Hub](#).

## Overview


Click the Notification Templates tab to show a list of all notification templates, what actions they perform, and their status (active or paused). To edit a notification template, enable the check box next to the notification template and choose from the following options.

Option	Description
Send test notification (  )	Triggers the notification immediately for testing purposes.  <b>i</b> When you test notifications, PRTG does not resolve the placeholders, but rather sends the original variables instead.
Used by (  )	Show all objects that trigger the notification.
Pause (  )	Pauses the notification.  <b>i</b> If you manually <a href="#">pause</a> <sup>[227]</sup> a notification, PRTG does not send messages when this notification is triggered.
Resume (  )	Resumes the notification.
Clone (  )	Creates a clone of the notification.
Delete (  )	Deletes the notification.  <b>i</b> You cannot delete predefined notifications.
Settings (  )	Opens the <a href="#">settings</a> <sup>[2810]</sup> of a notification template.

**i** You can also use the quick action buttons Send test notification (  ), Used by (  ), Pause (  ) or Resume (  ) next to the status of a notification template.

 See also sections [Working with Table Lists](#)<sup>[218]</sup> and [Multi-Edit](#)<sup>[2718]</sup>.

## Notification Template Settings

Hover over  and select Add Notification Template from the menu to add a new notification template. You can also click the name of a notification template to edit it.

**i** When a user with administrative rights creates a new object, only other users with administrative rights can view or edit the new object by default. When a read/write user creates a new object, all members of the read/write user's primary group can view and edit the new object as well. This behavior applies to [libraries](#)<sup>[2738]</sup>, [maps](#)<sup>[2778]</sup>, [reports](#)<sup>[2754]</sup>, [notification templates](#)<sup>[2808]</sup>, and [schedules](#)<sup>[2846]</sup>. For more information, see section [Access Rights Management](#)<sup>[145]</sup>.



## Basic Settings

**Basic Settings**

Template Name ⓘ Notification Template

---

Tags ⓘ +

---

Status ⓘ  Started (default)  
 Paused

---

Schedule ⓘ None

---

Notification Handling during Scheduled Pause ⓘ  Collect notifications and send them when reactivated  
 Discard notifications during paused status

Basic Settings

Setting	Description
Template Name	<p>Enter a name to identify the notification template.</p> <p> ⓘ If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Tags	<p>Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically <a href="#">inherited</a><sup>138</sup>.</p> <p> ⓘ For performance reasons, it can take some minutes until you can filter for new tags that you added.</p>
Status	<p>Select the status of the notification template:</p> <ul style="list-style-type: none"> <li>▪ Started (default): PRTG executes the notifications that are defined in the notification template whenever it is triggered.</li> <li>▪ Paused: PRTG does not execute any notifications that are defined in the notification template.</li> </ul>
Schedule	<p>Define if you want to use a schedule to activate a notification template only during specific time spans:</p> <ul style="list-style-type: none"> <li>▪ None</li> <li>▪ Saturdays</li> <li>▪ Sundays</li> <li>▪ Weekdays</li> <li>▪ Weekdays Eight-To-Eight (08:00 - 20:00)</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Weekdays Nights (17:00 - 09:00)</li> <li>▪ Weekdays Nights (20:00 - 08:00)</li> <li>▪ Weekdays Nine-To-Five (09:00 - 17:00)</li> <li>▪ Weekends</li> </ul> <p><b>i</b> Use this setting to pause notifications, for example, during regular maintenance periods or system restarts.</p> <p><b>i</b> The overall status of the notification template must be Started (default) to apply any schedule settings.</p> <p><b>■</b> For more information, see section <a href="#">Schedules</a> <small>2846</small>.</p>
Notification Handling during Scheduled Pause	<p>Define how PRTG handles notifications that are triggered during a <a href="#">scheduled</a> pause:</p> <ul style="list-style-type: none"> <li>▪ Collect notifications and send them when reactivated: PRTG collects all notifications that are triggered during a scheduled pause and sends them all out once the paused status ends.</li> <li>▪ Discard notifications during paused status: PRTG discards all notifications that are triggered during a scheduled pause.</li> </ul> <p><b>i</b> If you manually pause a notification, PRTG never collects notifications that are triggered while the notification is paused.</p>

## Notification Summarization

**Notification Summarization**

**Method** i

Always notify immediately, never summarize  
 Send first down message immediately, then summarize  
 Send first down and up message immediately, then summarize  
 Send all down messages immediately, summarize the others  
 Send all down and up messages immediately, summarize the others  
 Always summarize messages, regardless of type

**Subject for Summarized Email or SNS Messages** i [%sitename] %summarycount Summarized Notifications

**Time Span for Summarizing Messages (in Minutes)** i 1

Notification Summarization

Setting	Description
Method	<p>Define if and how PRTG collects and summarizes several notifications into one or more messages with a maximum of 1,000 characters:</p> <ul style="list-style-type: none"> <li>▪ Always notify immediately, never summarize: PRTG always sends out one notification for each notification trigger that it receives as soon as possible, for example, immediately.</li> <li>▪ Send first down message immediately, then summarize: When PRTG receives several down triggers, it sends the first notification immediately, then it continues to summarize notification triggers into one message, regardless of the sensor status.</li> <li>▪ Send first down and up message immediately, then summarize: When PRTG receives several down or up triggers, it sends each first notification immediately, then it continues to summarize notification triggers into one message, regardless of the sensor status.</li> <li>▪ Send all down messages immediately, summarize the others: When PRTG receives several down triggers, it sends out one notification for each trigger that it receives, but it summarizes notifications for all non-down triggers into one message.</li> <li>▪ Send all down and up messages immediately, summarize the others: When PRTG receives several down or <b>up</b> triggers, it sends out one notification for each trigger that it receives, but it summarizes the notifications for all non-down and non-up triggers into one message.</li> <li>▪ Always summarize notifications, regardless of type: When PRTG receives several notification triggers, it summarizes the notifications, regardless of the kind of notification trigger that it receives. <ul style="list-style-type: none"> <li>ⓘ The maximum number of notifications (see below) still applies.</li> <li>ⓘ Regardless of the option that you choose, PRTG never summarizes notifications of the types Send Slack Message, Send Microsoft Teams Message, Execute HTTP Action, Execute Program, and Assign Ticket because it always sends them immediately. PRTG can summarize the messages of all other notification types.</li> <li>ⓘ 'first down' and 'first up' messages refer to the notification trigger condition and the clear condition respectively. You can also define warning or unusual states as notification trigger conditions or even thresholds or other triggers notification summarizations. The <b>condition clear</b> triggers, if applicable, are defined in the respective notification trigger conditions as well. The notification triggers all qualify as 'first down' or 'first up' messages.</li> <li>ⓘ PRTG collects up to 25 single notifications for one summarization and sends out the message as soon as this number is reached (or when the gathering time passes). If PRTG receives more than 25 notifications within the defined time span, you receive more than one message with up to 25 entries each. For example, if PRTG collects 74 notifications, this results in 3 summarized messages with 25, 25, and 24 collected notifications.</li> </ul> </li> </ul>

Setting	Description
Subject for Summarized Email or SNS Messages	<p>Define a subject that PRTG includes when it sends summarized notifications. The default subject is [%sitename%] %summarycount Summarized Notifications.</p> <p><b>i</b> PRTG only uses the subject for the notification methods Send Email and Send Amazon Simple Notification Service Message.</p> <p><b>■</b> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a> <sup>3325</sup>.</p>
Time Span for Summarizing Messages (in Minutes)	<p>Define a time span in minutes to define how long PRTG collects notifications for summarization. Enter an integer.</p> <p><b>i</b> If you enter a long time span, for example, 60 minutes, PRTG collects notifications for one hour before it sends them out summarized unless other features (see above) require an earlier message dispatch.</p>

## Access Rights


Access Rights	
User Group Access <sup>1</sup>	Rights
<div style="text-align: right;">User Group</div>	
RO User Group	No access
PRTG Users Group	No access

Access Rights





























Setting	Description
User Group Access	<p>Define the user groups that have access to the notification template. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights:</p> <ul style="list-style-type: none"> <li>▪ No access: Users in this user group cannot see or edit the notification template. The object does not show up in lists.</li> <li>▪ Read access: Users in this user group can see the notification template and view its settings.</li> <li>▪ Write access: Users in this user group can see the notification template and view and edit its settings. However, they cannot edit its access rights settings.</li> <li>▪ Full access: Users in this user group can see the notification template, view and edit its settings, and edit its access rights settings.</li> </ul> <p><b>i</b> You can create new user groups in the <a href="#">User Groups</a> <sup>2912</sup> settings.</p>

## Notification Methods



With the following settings, you can add one or more methods for how PRTG sends out a notification message. You can choose one method or combine several methods. Whenever the notification is triggered, PRTG sends out messages or performs actions for all configured methods at once.

To select a notification method, click  in front of it. You can then see and set the options as described in this section. The following notification methods are available:

 Some notification types are only available for PRTG Network Monitor (marked with ). You cannot use these with PRTG Hosted Monitor.

- [Send Email](#)  
- [Add Entry to Event Log](#)  
- [Send SMS/Pager Message](#)  
- [Execute HTTP Action](#)  
- [Execute Program](#)  
- [Send Syslog Message](#)  
- [Send SNMP Trap](#)  
- [Send Amazon Simple Notification Service Message](#)  
- [Assign Ticket](#)  
- [Send Push Notification](#)  
- [Send Microsoft Teams Message](#)  
- [Send Slack Message](#)  
- [Send MQTT Publish Notification](#)  
- [Send OPC UA Notification](#)  

## Send Email @

 This notification method uses notification contacts to deliver the email notifications. Set up notification contacts in advance in the [notification contacts](#)  settings.

Send Email

Sender <sup>?</sup>  Default  
 Custom

Send to User, Send to User Group, and Send to Email Address all work simultaneously. Every user, user group, or email address that you define here all receive the email notifications.

Send to User <sup>?</sup> PRTG System Administrator

---

Send to User Group <sup>?</sup> None

---

Send to Email Address <sup>?</sup>

---

Subject <sup>?</sup> [%sitename] %device %name %status %down (%message)

---

Format <sup>?</sup>  HTML  
 Text  
 Custom text

---

Priority <sup>?</sup> Highest





---

HTTP Version <sup>?</sup>  HTTP 1.1 (default)  
 HTTP 1.0

Send Email

Setting	Description
Sender	<p>Define which sender email address and sender name appear in the <b>FROM</b> part of the email notifications:</p> <ul style="list-style-type: none"> <li>▪ Default: Use the default sender email address and sender name from the <a href="#">notification delivery</a> <sup>2878</sup> settings.</li> <li>▪ Custom: Enter a custom sender email address and sender name.</li> </ul>
Sender Email Address	<p><b>This setting is only visible if you select Custom above.</b></p> <p>Enter an email address to use as the sender of the email notifications.</p> <p><sup>i</sup> If you enter a custom sender email address, it overrides the email address in the <a href="#">notification delivery</a> <sup>2879</sup> settings.</p> <p><sup>i</sup> The outgoing Simple Mail Transfer Protocol (SMTP) server in the notification delivery settings must allow the email address so that it can deliver email notifications.</p>
Sender Name	<p><b>This setting is only visible if you select Custom above.</b></p> <p>Enter a sender name to use as the sender of the email notifications.</p> <p><sup>i</sup> If you enter a custom sender name, it overrides the sender name in the <a href="#">notification delivery</a> <sup>2879</sup> settings.</p>

Setting	Description
Send to User	<p>Select a user account to send the email notifications to. PRTG sends the email notifications to every active email <a href="#">notification contact</a><sup>[2844]</sup> for this user account. Leave None to not use this option.</p> <ul style="list-style-type: none"> <li><span data-bbox="395 495 427 528">i</span> Read/write users can send notifications to any user that is a member of the same user group as the read/write user.</li> <li><span data-bbox="395 577 427 611">i</span> Send to User, Send to User Group, and Send to Email Address all work simultaneously. Because of this, you can define more than one user as a recipient of this notification. PRTG sends the email notifications to the active email <a href="#">notification contacts</a><sup>[2844]</sup> of the user that you select, to the active email notification contacts of all members of the user group that you select, and to all email addresses that you enter under Send to Email Address.</li> </ul>
Send to User Group	<p>Select a user group to send the email notifications to all members of this user group. PRTG sends the email notifications to every active email <a href="#">notification contact</a><sup>[2844]</sup> of every user in the user group. Leave None to not use this option.</p> <ul style="list-style-type: none"> <li><span data-bbox="395 934 427 967">i</span> If you select a user group and a specific member of this user group as recipients, the user only receives <b>one</b> single email. This also applies if you enter an individual email address under Send to Email Address that is already defined as an email notification contact of the selected user.</li> <li><span data-bbox="395 1081 427 1115">i</span> If you define individual email addresses under Send to Email Address, define a specific user account under Send to User, and define a user group here, PRTG sends the message to the individual email addresses, to the individual user, as well as to the members of the selected user group. In all cases, PRTG sends <b>one</b> message with all recipients in the <b>To</b> part of the email.</li> <li><span data-bbox="395 1261 427 1294">i</span> Read/write users can send email notifications to all user groups that they are members of.</li> <li><span data-bbox="395 1344 427 1377">i</span> Send to User, Send to User Group, and Send to Email Address all work simultaneously. Because of this, you can define more than one user as a recipient of this notification. PRTG sends the email notifications to the active email <a href="#">notification contacts</a><sup>[2844]</sup> of the user that you select, to the active email notification contacts of all members of the user group that you select, and to all email addresses that you enter under Send to Email Address.</li> </ul>
Send to Email Address	<p>Enter one or more email addresses to which PRTG sends the email notifications. If you enter more than one email address, separate them with commas. Leave this field empty to only send email notifications to the email notification contacts of the user or to the members of the user group you choose above.</p> <ul style="list-style-type: none"> <li><span data-bbox="395 1731 427 1765">i</span> We recommend that you use Send to User and/or Send to User Group instead because you can then manage the notification contacts of users.</li> <li><span data-bbox="395 1814 427 1848">i</span> Send to User, Send to User Group, and Send to Email Address all work simultaneously. Because of this, you can define more than one user as a recipient of this notification. PRTG sends the email notifications to the active email <a href="#">notification contacts</a><sup>[2844]</sup> of the user that you select, to the active email notification contacts of all members of the user group that you select, and to all email addresses that you enter under Send to Email Address.</li> </ul>


Setting	Description
Subject	<p>Enter the subject of the email notifications. The default subject is [%sitename] %device %name %status %down (%message).</p> <p> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a> <sup>3325</sup>.</p>
Format	<p>Define the kind of email that PRTG sends when the notification is triggered:</p> <ul style="list-style-type: none"> <li>▪ HTML: PRTG uses the default HTML email template for the message part of the email.</li> </ul> <p> Make sure that your email client can show HTML emails, otherwise you cannot read emails from PRTG.</p> <ul style="list-style-type: none"> <li>▪ Text: PRTG uses the default plain text email template for the message part of the email.</li> <li>▪ Custom text: PRTG uses custom plain text for the message part of the email. Define a custom text below.</li> </ul>
Custom Text	<p><a href="#">This setting is only visible if you select Custom text above.</a></p> <p>Enter the desired message for this email notification in plain text format. You can use placeholders here.</p> <p> For more information, see section <a href="#">Placeholders for Notifications</a> <sup>3325</sup>.</p>
Priority	<p>Define the priority that PRTG sets for the email:</p> <ul style="list-style-type: none"> <li>▪ Very High</li> <li>▪ High</li> <li>▪ Medium</li> <li>▪ Low</li> <li>▪ Very Low</li> </ul> <p> Most email clients can show this priority flag.</p>
HTTP Version	<p>Define the HTTP version that PRTG uses to send the email:</p> <ul style="list-style-type: none"> <li>▪ HTTP 1.1 (default): Use HTTP version 1.1.</li> <li>▪ HTTP 1.0: Use HTTP version 1.0.</li> </ul>


Add Entry to Event Log 


 This option is not available in PRTG Hosted Monitor.






Add Entry to Event Log

Log File   Application  
 PRTG Network Monitor

Event Type  Error


Message  [%sitename] %device %name %status %down (%message)

Add Entry to Event Log

Setting	Description
Log File	<p>Define the log file to which PRTG adds an event:</p> <ul style="list-style-type: none"> <li>Application: PRTG adds an entry to the <a href="#">Application</a> log file under <a href="#">Windows Logs</a> in the event log</li> <li>PRTG Network Monitor: PRTG adds an entry to the <a href="#">PRTG Network Monitor</a> log file under <a href="#">Applications and Services Logs</a> in the event log.</li> </ul>
Event Source	<p><a href="#">This setting is only visible if you select Application above.</a></p> <p>Enter the source for the event. This is usually the name of the application.</p>
Event Type	<p>Select the type of the event:</p> <ul style="list-style-type: none"> <li>Error: An event that indicates a significant problem such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error event is logged.</li> <li>Warning: An event that is not necessarily significant, but might indicate a possible future problem. For example, when disk space is low, a Warning event is logged.</li> <li>Information: An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, it might be appropriate to log an Information event.</li> </ul>
Message	<p>Define the message that PRTG writes in the event log. The default message is <a href="#">[%sitename] %device %name %status %down (%message)</a>.</p> <p> To reset this field to the default value, enter only an asterisk (*).</p> <p> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a> .</p>

## Send SMS/Pager Message

 You must first set up this notification method in the [Notification Delivery](#)  settings.

 This notification method uses notification contacts to deliver the SMS/pager messages. Set up notification contacts in advance in the [notification contacts](#)  settings.

This notification method uses the central proxy settings that you define for the PRTG core server. For more information, see section [Core & Probes](#) (section Proxy Configuration).

**Send SMS/Pager Message**

Send to User, Send to User Group, and Send to Number all work simultaneously. Every user, user group, or number that you define here all receive the notifications.

Send to User

Send to User Group


Send to Phone Number

Message




HTTP Version  HTTP 1.1 (default)  
 HTTP 1.0

Send SMS/Pager Message

Setting	Description
Send to User	Select a user account from the dropdown list. PRTG sends the SMS/pager message to every <a href="#">SMS notification contact</a> for the user account. Leave None to not use this option.
Send to User Group	Select a user group from the dropdown list. PRTG sends the SMS/pager message to every SMS notification contact for every member of the <a href="#">user group</a> .  <p><b>i</b> If you select a user group and a specific member of this user group as recipients at the same time, this user receives the SMS/pager message only once. This also applies if you enter an individual phone number below that is already defined as an SMS notification contact for the selected user.</p>
Send to Phone Number	Enter a phone number to send the SMS/pager message to. If you enter more than one phone number, use commas as separators.  <p><b>i</b> The format depends on the SMS provider. Usually, you use a plus sign (+), followed by the country code and the number. For example, <a href="#">+1555012345</a>.</p> <p><b>i</b> Make sure that the number format meets the requirements of the SMS provider or the hardware that you use in combination with an application programming interface (API) call. Sometimes, a plus sign is not required. The wrong format might result in undelivered messages.</p> <p><b>i</b> We recommend that you use Send to User and/or Send to User Group instead because you can then manage the notification contacts of users.</p>
Message	Define the SMS/pager message. The default message is <a href="#">[%sitename] %device %name %status %down (%message)</a> .  <p><b>i</b> To reset this field to the default value, enter only an asterisk (*).</p>

Setting	Description
	<p> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a> <sup>[3325]</sup>.</p>
HTTP Version	<p>Define the HTTP version that PRTG uses to send the SMS/pager message:</p> <ul style="list-style-type: none"> <li>▪ HTTP 1.1 (default): Use HTTP version 1.1.</li> <li>▪ HTTP 1.0: Use HTTP version 1.0.</li> </ul>

## Execute HTTP Action: //

-  Regardless of the Notification Summarization method that you use, PRTG always sends notifications of the type Execute HTTP Action immediately. PRTG never summarizes them.
-  This notification method uses the central proxy settings that you define for the PRTG core server. For more information, see section [Core & Probes](#) <sup>[2888]</sup> (section Proxy Configuration).
-  For more information, see section [Custom Notifications](#) <sup>[3151]</sup>. You can find ready-to-use custom notifications in the [PRTG Sensor Hub](#), see [below](#) <sup>[2841]</sup>.


Execute HTTP Action

URL  www.example.com

SNI Handling 

Do not send SNI (default)

Send SNI

HTTP Method 



GET (default)






POST

PUT



PATCH

Execute HTTP Action

Setting	Description
URL	<p>Enter the URL that PRTG sends the request to.</p> <p> HTTP notifications work with or without Secure Sockets Layer (SSL).</p> <p> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a> <sup>[3325]</sup>.</p>


Setting	Description
SNI Handling	<p>Define if PRTG sends the Server Name Indication (SNI) extension to the Transport Layer Security (TLS) protocol along with the HTTP request:</p> <ul style="list-style-type: none"> <li>▪ Do not send SNI (default): PRTG does not send the SNI when it executes the HTTP action.</li> <li>▪ Send SNI: PRTG sends the SNI when it calls the target URL. Specify the SNI below.</li> </ul>
SNI Name	<p><a href="#">This setting is only visible if you select Send SNI above.</a></p> <p>Enter the SNI name that the endpoint configuration requires. Usually, this is the fully qualified domain name (FQDN) of the virtual host.</p>
HTTP Method	<p>Select the HTTP method that the notification uses:</p> <ul style="list-style-type: none"> <li>▪ GET (default): Use the GET method.</li> <li>▪ POST: Use the POST method.</li> <li>▪ PUT: Use the PUT method.</li> <li>▪ PATCH: Use the PATCH method.</li> </ul>
Payload	<p><a href="#">This setting is only visible if you select POST, PUT, or PATCH above.</a></p> <p>Enter a payload. The payload is the data that PRTG transmits to the URL.</p> <ul style="list-style-type: none"> <li> You cannot use Extensible Markup Language (XML) or JavaScript Object Notation (JSON).</li> <li> Only the content type <a href="#">application/x-www-form-urlencoded</a> is supported.</li> <li> You can use line breaks.</li> <li> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a> <sup>[3325]</sup>.</li> </ul>
HTTP Version	<p><a href="#">This setting is only visible if you select POST above.</a></p> <p>Select the HTTP version that PRTG uses to execute the HTTP action:</p> <ul style="list-style-type: none"> <li>▪ HTTP 1.1 (default): Use HTTP version 1.1.</li> <li>▪ HTTP 1.0: Use HTTP version 1.0.</li> </ul> <p> Make sure that the target supports the HTTP version that you select.</p>


## Execute Program


-  Regardless of the Notification Summarization method that you use, PRTG always sends notifications of the type Execute Program immediately. PRTG never summarizes them.
-  To remotely run PowerShell scripts, make sure that you set the according Execution Policy. For more information, see the Knowledge Base: [PowerShell 32 bit and 64 bit and Execution Policy](#)


 For more information, see section [Custom Notifications](#)<sup>[315]</sup>. You can find ready-to-use custom notifications in the [PRTG Sensor Hub](#), see [below](#)<sup>[284]</sup>.


 This option is not available in PRTG Hosted Monitor.


 **Execute Program**


Executable File 

Parameters 




Domain or Computer Name 


User Name 

Password 

Timeout (Sec.) 


Execute Program


Setting	Description
Executable File	<p>Select an executable file from the list. PRTG runs it every time the notification is triggered.</p> <ul style="list-style-type: none"> <li> You see the files that are in the corresponding \Notifications\EXE subfolder of the <a href="#">PRTG program directory</a><sup>[321]</sup>. For files to appear in this list, store them as .bat, .cmd, .exe, .com, .ps1, or .vbs.</li> <li> In a cluster, copy the files to every cluster node. This makes sure that PRTG can execute the notification even when the master node fails. If your custom notification executes an external program, install it on all cluster nodes as well.</li> </ul>
Parameters	<p>Enter the parameters that the notification passes to the executable. For example, if you use a batch file that contains a %1 variable, you can provide a value for this variable. The default parameters are <a href="#">[%sitename] %device %name %status %down (%message)</a>.</p> <ul style="list-style-type: none"> <li> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a><sup>[332]</sup>.</li> </ul>


Setting	Description
	<p> You need to escape special characters and whitespaces in your parameters and surround them with double quotation marks ("). See section <a href="#">Escape Special Characters and Whitespaces in Parameters</a> <sup>3312</sup> for details.</p>
Domain or Computer Name	Enter a Windows authority if you want to use a different security context for the program than the security context of the PRTG core server.
User Name	Enter the user name for Windows access.
Password	Enter the password for Windows access.
Timeout (Sec.)	Enter a timeout in seconds. After this time passes, PRTG stops the process if it is still running. Enter an integer.


## Send Syslog Message


 This option is not available in PRTG Hosted Monitor.


 **Send Syslog Message**

Host/IP Address  192.0.2.0



Syslog Port  514




Facility  User-level messages

Encoding   ANSI  
 UTF-8 (default)

Message  [%sitename] %device %name %status %down (%message)

Send Syslog Message

Setting	Description
Host/IP Address	<p>Define the IP address or the Domain Name System (DNS) name of the system that runs the syslog server.</p> <p> You can receive and analyze syslog messages with the <a href="#">Syslog Receiver</a> sensor.</p>
Syslog Port	<p>Enter the port that PRTG sends the syslog messages to. The default port is 514.</p> <p> You can only use the User Datagram Protocol (UDP).</p>


Setting	Description
Facility	<p>Define the facility of the syslog messages:</p> <ul style="list-style-type: none"> <li>User-level messages</li> <li>Local use <a href="#">0-7</a></li> </ul>
Encoding	<p>Define the encoding of the syslog messages that PRTG sends to the syslog receiver:</p> <ul style="list-style-type: none"> <li>ANSI</li> <li>UTF-8</li> </ul> <p> Make sure that the syslog receiver supports the encoding that you select.</p>
Message	<p>Define the syslog message. The default message is <code>[%sitename] %device %name %status %down (%message)</code>.</p> <p> To reset this field to the default value, enter only an asterisk (*).</p> <p> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a> <sup>3325</sup>.</p>

### Syslog Message Severity Status

 Depending on the status of the sensor that triggers the syslog notification, PRTG automatically sets the Severity level of the syslog messages.

Status	Severity level
 Up	Notice (5)
 Warning	Warning (4)
 Down	Error (3)

### Send SNMP Trap

 For more information about the object identifiers (OID) that PRTG uses in the content of the Simple Network Management Protocol (SNMP) traps, see the Knowledge Base: [Is it possible to send SNMP traps using PRTG?](#)

 This option is not available in PRTG Hosted Monitor.

Send SNMP Trap

Host/IP Address ⓘ

SNMP Port ⓘ

Community String ⓘ

Custom Trap Code ⓘ

Message ID ⓘ

Message ⓘ

Agent IP ⓘ

Include Sensor ID ⓘ

Do not include sensor ID (default)
  Include sensor ID


Send SNMP Trap

Setting	Description
Host/IP Address	Define the IP address or DNS name of the system that runs the trap receiver. ⓘ You can receive and analyze SNMP trap messages with the <a href="#">SNMP Trap Receiver</a> sensor.
SNMP Port	Enter the port on which PRTG sends trap messages. The default port is <a href="#">162</a> .
Community String	Enter the community string of the device. The default community string is <a href="#">public</a> . Enter a string or leave the field empty.
Custom Trap Code	Enter a code to identify the purpose of the trap. The default trap code is <a href="#">0</a> . Enter an integer.
Message ID	Enter an ID to identify the origin of the trap. Enter an integer. PRTG sends it on the OID <a href="#">1.3.6.1.4.1.32446.1.1.1</a> .
Message	Define the trap message. ⓘ To reset this field to the default value, enter only an asterisk (*). ■ You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a> <sup>[3325]</sup> .
Agent IP	Define the IP address of the agent. Leave this field empty to use the IP address of the PRTG web server.



Setting	Description
Include Sensor ID	<p>Define if PRTG should include the sensor ID of the sensor that triggers the notification:</p> <ul style="list-style-type: none"> <li>Do not include sensor ID (default): Do not include the sensor ID with the notification message.</li> <li>Include sensor ID: Include the sensor ID with the notification message. PRTG sends it on the OID <a href="#">1.3.6.1.4.1.32446.1.1.5</a>.</li> </ul>

### Send Amazon Simple Notification Service Message

 **Send Amazon Simple Notification Service Message**

AWS Access Key ID ?

AWS Secret Access Key ?

Location ?

Amazon Resource Name ?

This field is required.





Subject ?

Message ?


Send Amazon Simple Notification Service Message

Setting	Description
AWS Access Key ID	Enter your access key ID from <a href="https://aws.amazon.com">aws.amazon.com</a> . Enter a string.
AWS Secret Access Key	Enter your secret access key from <a href="https://aws.amazon.com">aws.amazon.com</a> . Enter a string.
Location	<p>Define the location of your Amazon service:</p> <ul style="list-style-type: none"> <li>Africa (Cape Town)</li> <li>Asia Pacific (Hong Kong)</li> <li>Asia Pacific (Mumbai)</li> <li>Asia Pacific (Osaka)</li> <li>Asia Pacific (Seoul)</li> <li>Asia Pacific (Singapore)</li> <li>Asia Pacific (Sydney)</li> </ul>

2827

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Asia Pacific (Tokyo)</li> <li>▪ Canada (Central)</li> <li>▪ China (Beijing)</li> <li>▪ China (Ningxia)</li> <li>▪ Europe (Frankfurt)</li> <li>▪ Europe (Stockholm)</li> <li>▪ Europe (Milan)</li> <li>▪ Europe (Ireland)</li> <li>▪ Europe (London)</li> <li>▪ Europe (Paris)</li> <li>▪ Middle East (Bahrain)</li> <li>▪ South America (São Paulo)</li> <li>▪ US East (Northern Virginia)</li> <li>▪ US East (Ohio)</li> <li>▪ US West (Northern California)</li> <li>▪ US West (Oregon)</li> </ul>
Amazon Resource Name	Enter the Amazon resource name. Enter a string.
Subject	<p>Enter the subject of the Amazon Simple Notification Service (SNS) message. Enter a string.</p> <p> The maximum length for the subject is <b>202</b> characters. PRTG ignores characters that exceed this length.</p>
Message	<p>Define the SNS message. The default SNS message is <code>[%sitename] %device %name %status %down (%message)</code>.</p> <p> To reset this field to the default value, enter only an asterisk (*).</p> <p> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a> <sup>[3325]</sup>.</p> <p> PRTG only sends the message if you use email-based notifications delivered by Amazon SNS. For SMS delivery, PRTG only sends the subject and ignores the message because of SMS size restrictions.</p>

## Assign Ticket

 Regardless of the Notification Summarization method that you use, PRTG always sends notifications of the type Assign Ticket immediately. PRTG never summarizes them.

For more information about the ticket system, see section [Tickets](#)<sup>[213]</sup>.

Assign Ticket

Assign to User Group or User <sup>i</sup>

To user group  
 To user

User Group <sup>i</sup> PRTG Administrators

Subject <sup>i</sup> %device %name %status %down (%message)

Content <sup>i</sup> Sensor: %name  
Status: %status %down

Date/Time: %datetime (%timezone)

When Condition Clears <sup>i</sup>

Close the notification ticket (recommended)  
 Do not close the notification ticket

Assign Ticket

Setting	Description
Assign to User Group or User	Specify whether to assign the <a href="#">notification ticket</a> <sup>[213]</sup> to a user group or to a single user: <ul style="list-style-type: none"> <li>To user group: Assign the notification ticket to a user group.</li> <li>To user: Assign the notification ticket to a single user.</li> </ul>
User Group	Select the user group to which PRTG assigns the notification ticket. <p><sup>i</sup> Read/write users can assign tickets to all user groups that they are a member of as well as to administrators and individual users that are members of the same user group as the read/write user.</p>
User	Select the user to which PRTG assigns the notification ticket. <p><sup>i</sup> Read/write users can assign tickets to all user groups that they are a member of as well as to administrators and individual users that are members of the same user group as the read/write user.</p>
Subject	Enter the subject of the notification ticket. The default subject is <code>%device %name %status %down (%message)</code> . <p> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a><sup>[325]</sup>.</p>
Content	Enter the message of the notification ticket. The default message is <p>Sensor: %name Status: %status %down</p>

Setting	Description
	<p>Date/Time: %datetime (%timezone)                      Last Result: %lastvalue                      Last Message: %message</p> <p>Probe: %probe                      Group: %group                      Device: %device (%host)</p> <p>Last Scan: %lastcheck                      Last Up: %lastup                      Last Down: %lastdown                      Uptime: %uptime                      Downtime: %downtime                      Cumulated since: %cumsince                      Location: %location</p> <p><b>i</b> To reset this field to the default value, enter only an asterisk (*).</p> <p><b>■</b> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a> <sup>[3325]</sup>.</p>
When Condition Clears	<p>Define how PRTG handles the notification ticket when the defined trigger condition clears:</p> <ul style="list-style-type: none"> <li>▪ Close the notification ticket (recommended): Automatically close the notification ticket if the trigger condition is not met anymore.</li> <li>▪ Do not close the notification ticket: Do not close the notification ticket after the condition clears.</li> </ul>


## Send Push Notification

**■** Push notifications only work with the apps [PRTG for Android](#) <sup>[2969]</sup> and [PRTG for iOS](#) <sup>[2988]</sup>. You must activate push notifications in the settings of the app first. For more information about the setup, see the Knowledge Base: [How can I use push notifications with PRTG?](#)

**i** This notification method uses notification contacts to deliver push notifications. Set up notification contacts in advance in the [notification contacts](#) <sup>[2844]</sup> settings.


**i** The PRTG core server needs to communicate with the PRTG Cloud on port 443 to send push notifications. It uses <https://api.prtgcloud.com:443>, which is the same as for the [Cloud HTTP v2](#) sensor, the [Cloud Ping v2](#) sensor, and [support tickets](#) <sup>[2977]</sup>.


**i** Send to User and Send to User Group both work simultaneously. Because of this, you can define more than one user as a recipient of push notifications. PRTG sends push notifications to the active [push notification contacts](#) <sup>[2844]</sup> of the user that you select, and to the active push notification contacts of all members of the user group that you select.


 **Send Push Notification**


Send to User and Send to User Group both work simultaneously. This means that every push device of the user or user group receives the push notifications.

Note: The PRTG core server must be able to reach the PRTG Cloud on TCP port 443 to send push notifications.






Send to User  PRTG System Administrator

Send to User Group  None


Message  [%sitename] %device %name %status %down (%message)

HTTP Version   HTTP 1.1 (default)  
 HTTP 1.0

Send Push Notification

Setting	Description
Send to User	<p>Select the user that PRTG sends push notifications to. PRTG sends the push notifications to each active push notification contact of the user. Leave None to not use this option.</p> <p> You can edit push notification contacts of a user in the <a href="#">Notification Contacts</a> <sup>2844</sup> settings and also activate push notifications in the Android or iOS app with the user.</p>
Send to User Group	<p>Select the user group that PRTG sends push notifications to. PRTG sends the push notifications to each active push notification contact of every member of the group. Leave None to not use this option.</p> <p> If you select a user group and a specific member of the group as recipients at the same time, the user receives the text message only one time.</p> <p> You can edit user groups in the <a href="#">User Groups</a> <sup>2912</sup> settings and push notification contacts in the <a href="#">Notification Contacts</a> <sup>2844</sup> settings.</p>
Message	<p>Define the message of the push notification. The default message is [%sitename] %device %name %status %down (%message).</p> <p> To reset this field to the default value, enter only an asterisk (*).</p> <p> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a> <sup>3325</sup>.</p>
HTTP Version	<p>Define the HTTP version that PRTG uses to send the push notification:</p> <ul style="list-style-type: none"> <li>HTTP 1.1 (default): Use HTTP version 1.1.</li> <li>HTTP 1.0: Use HTTP version 1.0.</li> </ul>

## Send Microsoft Teams Message

 Regardless of the Notification Summarization method you use, PRTG always sends notifications of the type Send Microsoft Teams Message immediately. PRTG never summarizes them.

**Send Microsoft Teams Message**

Teams Webhook URL ?

---

This field is required.

Title ?

%device: %name

---

Subtitle ?

%message

---

Content ?

Use default content

Define custom content

Send Microsoft Teams Message

Setting	Description
Teams Webhook URL	<p>Enter the URL of the incoming webhook that you set up in your Microsoft Teams channel.</p> <p><span style="color: #0070C0;">■</span> For more information, see the Knowledge Base: <a href="#">How do I create a webhook for the PRTG Notifications to Slack and Microsoft Teams?</a></p>
Title	<p>Enter the title of the Microsoft Teams notification. The default title is <a href="#">Enter value</a>.</p> <p><span style="color: #0070C0;">■</span> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a> <sup>[3325]</sup>.</p>
Subtitle	<p>Enter the subtitle of the Microsoft Teams notification. The default subtitle is <code>%message</code>.</p> <p><span style="color: #0070C0;">■</span> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a> <sup>[3325]</sup>.</p>
Content	<p>Define the content of the Microsoft Teams notification:</p> <ul style="list-style-type: none"> <li>▪ Use default content: Use the default notification message content. This includes information about the <a href="#">Status</a>, <a href="#">Last Scan</a>, <a href="#">Last Value</a>, <a href="#">Last Up</a>, <a href="#">Coverage</a>, <a href="#">Downtime</a>, <a href="#">Priority</a>, <a href="#">Probe</a>, and <a href="#">Group</a>.</li> <li>▪ Define custom content: Define custom notification message content. Choose Custom Content below.</li> </ul>
Custom Content	<p><a href="#">This setting is only visible if you select Define custom content above.</a></p> <p>Enable the check boxes in front of content that you want PRTG to include in the Microsoft Teams notifications. Disable the check boxes in front of the content that you do not want to include.</p> <p>The following types of monitoring information are available:</p> <ul style="list-style-type: none"> <li>▪ Name</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Host</li> <li>▪ Status</li> <li>▪ Last scan</li> <li>▪ Last value</li> <li>▪ Message</li> <li>▪ Last down</li> <li>▪ Last up</li> <li>▪ Coverage</li> <li>▪ Downtime</li> <li>▪ Uptime</li> <li>▪ Priority</li> <li>▪ Probe</li> <li>▪ Group</li> <li>▪ Device</li> <li>▪ Date and time</li> <li>▪ Time zone</li> <li>▪ Comments (probe)</li> <li>▪ Comments (group)</li> <li>▪ Comments (device)</li> <li>▪ Comments (sensor)</li> <li>▪ History</li> </ul> <p>■ For more information, see section <a href="#">Placeholders for Notifications</a> <sup>3325</sup>.</p>

## Send Slack Message #

ⓘ Regardless of the Notification Summarization method you use, PRTG always sends notifications of the type Send Slack Message immediately. PRTG never summarizes them.

Send Slack Message

Slack Webhook URL ❗

This field is required.

Sender Name ❗

%sitename

Title ❗

%device: %name

Subtitle ❗

%message

Content ❗



Use default content

Define custom content

Send Slack Message

Setting	Description
Slack Webhook URL	<p>Enter the URL of the incoming webhook that you set up in your Slack workspace.</p> <p><span style="color: #0070C0;">■</span> For more information, see the Knowledge Base: <a href="#">How do I create a webhook for the PRTG Notifications to Slack and Microsoft Teams?</a></p>
Sender Name	<p>Enter a sender name to use as the sender of Slack notifications.</p> <p><span style="font-size: 1.2em;">❗</span> This field overrides the sender that you might have defined in your Slack workspace.</p>
Title	<p>Enter the title of the Slack notifications. The default title is <a href="#">Enter value</a>.</p> <p><span style="color: #0070C0;">■</span> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a><sup>[3325]</sup>.</p>
Subtitle	<p>Enter the subtitle of the Slack notifications. The default subtitle is <a href="#">% message</a>.</p> <p><span style="color: #0070C0;">■</span> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a><sup>[3325]</sup>.</p>
Content	<p>Define the content of the Slack notifications:</p> <ul style="list-style-type: none"> <li>▪ Use default content: Use the default notification message content. This includes information about the <a href="#">Status</a>, <a href="#">Last Scan</a>, <a href="#">Last Value</a>, <a href="#">Last Up</a>, <a href="#">Coverage</a>, <a href="#">Downtime</a>, <a href="#">Priority</a>, <a href="#">Probe</a>, and <a href="#">Group</a>.</li> <li>▪ Define custom content: Define custom notification message content. Choose Custom Content below.</li> </ul>



Setting	Description
Custom Content	<p><b>This setting is only visible if you select</b> Define custom content <a href="#">above</a>.</p> <p>Enable the check boxes in front of the content that you want PRTG to include in the Slack notifications. Disable the check boxes in front of the content that you do not want to include.</p> <p>The following types of monitoring information are available:</p> <ul style="list-style-type: none"> <li>▪ Name</li> <li>▪ Host</li> <li>▪ Status</li> <li>▪ Last scan</li> <li>▪ Last value</li> <li>▪ Message</li> <li>▪ Last down</li> <li>▪ Last up</li> <li>▪ Coverage</li> <li>▪ Downtime</li> <li>▪ Uptime</li> <li>▪ Priority</li> <li>▪ Probe</li> <li>▪ Group</li> <li>▪ Device</li> <li>▪ Date and time</li> <li>▪ Time zone</li> <li>▪ Comments (probe)</li> <li>▪ Comments (group)</li> <li>▪ Comments (device)</li> <li>▪ Comments (sensor)</li> <li>▪ History</li> </ul> <p> For more information, see section <a href="#">Placeholders for Notifications</a> .</p>

### Send MQTT Publish Notification

**i** Regardless of the Notification Summarization method you use, PRTG might not send notifications of the type Send MQTT Publish Notification immediately.

**Send MQTT Publish Notification**

MQTT Broker ?   
This field is required.

Port ?

Timeout (Sec.) ?

User Authentication ?

None

User name and password

Transport-Level Security ?

Do not use transport-level security

Use transport-level security

MQTT Topic ?





ClientID ?



Message ?

Send MQTT Publish Notification

Setting	Description
MQTT Broker	Enter the address for the connection to the MQTT broker (server).
Port	Enter the port for the connection to the MQTT broker. The default port for secure connections is <b>8883</b> and the default port for unsecure connections is <b>1883</b> .
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is <b>300</b> seconds (5 minutes).
User Authentication	Select if you want to connect without credentials or define credentials for access to the MQTT broker: <ul style="list-style-type: none"> <li>▪ None (default): Connect without credentials.</li> <li>▪ User name and password: Define credentials for the connection.</li> </ul>
User Name	Enter the user name for access to the Message Queue Telemetry Transport (MQTT) broker.
Password	Enter the password for access to the MQTT broker.
Transport-Level Security	Select if you want to use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection: <ul style="list-style-type: none"> <li>▪ Do not use transport-level security (default): Establish the connection without connection security.</li> </ul>

2836

Setting	Description
	<ul style="list-style-type: none"> <li>Use transport-level security: Establish the connection with the strongest SSL/TLS method that the target device provides.</li> </ul>
Server Authentication	<p>This setting is only visible if you select Use transport-level security above.</p> <p>Select if you want to use a certificate for server authentication:</p> <ul style="list-style-type: none"> <li>Disable (default): Do not use a certificate for server authentication.</li> <li>Enable: Use a certificate for server authentication.</li> </ul>
CA Certificate	<p>Paste the certificate authority (CA) certificate for the verification of the MQTT broker.</p> <p> The certificate must be in Privacy-Enhanced Mail (PEM) format.</p>
Client Authentication	<p>This setting is only visible if you select Use transport-level security above.</p> <p>Select if you want to use a certificate for client authentication:</p> <ul style="list-style-type: none"> <li>Disable (default): Do not use a certificate for client authentication.</li> <li>Enable: Use a certificate for client authentication.</li> </ul>
Client Certificate	<p>Paste the certificate that you created for authenticating the sensor against the MQTT broker.</p> <p> The certificate must be in PEM format.</p>
Client Key	<p>Enter the client key for access to the MQTT broker.</p> <p> The client key must be in PEM format and it must be encrypted using the Client Key Password.</p>
Client Key Password	<p>Enter the password for the client key certificate.</p>
MQTT Topic	<p>Enter the topic for the MQTT publish notifications. The default topic is <a href="#">PRTG/%sitename/notifications</a>.</p> <p> MQTT clients that are subscribed to this topic receive the MQTT publish notifications.</p>
ClientID	<p>Enter the ClientID for the connection to the MQTT broker (server). The default ClientID is <a href="#">PRTG - %sitename</a>.</p>
Message	<p>Define the message of the MQTT publish notifications. The default message is <a href="#">PRTG - [%sitename] %device %name %status %down (%message)</a>.</p>

Setting	Description
	<p> To reset this field to the default value, enter only an asterisk (*).</p> <p> You can use placeholders. For more information, see section <a href="#">Placeholders for Notifications</a> <sup>[3325]</sup>.</p>

## Send OPC UA Notification

Send OPC UA Notification

Note: This notification method is neither intended to control any processes or machines nor is it intended for real-time alerting. We recommend that you use OPC UA notifications for notification purposes only.

OPC UA Server <sup>ⓘ</sup>

Port <sup>ⓘ</sup>

Server Path <sup>ⓘ</sup>

Node ID <sup>ⓘ</sup>

Timeout (Sec.) <sup>ⓘ</sup>

Security Mode <sup>ⓘ</sup>  None (default)  
 Sign  
 Sign & Encrypt



Authentication Method <sup>ⓘ</sup>  Anonymous (default)  
 User name and password

Data Type <sup>ⓘ</sup>  Boolean  
 Int64  
 Double

Boolean <sup>ⓘ</sup>  True (default)  
 False

Send OPC UA Notification

Setting	Description
OPC UA Server	Enter the address for the connection to the OPC Unified Architecture (OPC UA) server.
Port	Enter the port for the connection to the OPC UA server. The default port for secure connections is 4843. The default port for unsecure connections is 4840.
Server Path	Enter the path of the OPC UA server endpoint if you run more than one server under the same IP address or DNS name.
NodeID	Enter the NodeID for the OPC UA notification. PRTG writes the data that you define below to the specified NodeID.
Timeout (Sec.)	Enter a timeout in seconds for the request.

Setting	Description
Security Mode	<p>Select if you want to use encryption:</p> <ul style="list-style-type: none"> <li>▪ None (default): Do not use encryption.</li> <li>▪ Sign: Sign messages between the sensor and the OPC UA server.</li> <li>▪ Sign &amp; Encrypt: Sign and encrypt messages between the sensor and the OPC UA server.</li> </ul>
Security Policy	<p><a href="#">This setting is only visible if you select Sign or Sign &amp; Encrypt above.</a></p> <p>Select if you want to use a security policy and define which policy you want to use:</p> <ul style="list-style-type: none"> <li>▪ None (default): Do not use a security policy.</li> <li>▪ Basic256Sha256: Use the Basic256Sha256 security policy.</li> <li>▪ Basic256: Use the Basic256 security policy.</li> </ul>
Client Certificate	<p><a href="#">This setting is only visible if you select Sign or Sign &amp; Encrypt above.</a></p> <p>Enter the certificate that you created for authenticating the sensor against the OPC UA server.</p> <p> The certificate must meet the following requirements:</p> <ul style="list-style-type: none"> <li>▪ The key size must be 2048-bit or 4096-bit.</li> <li>▪ The secure hash algorithm must be <a href="#">SHA256</a>.</li> <li>▪ DataEncipherment must be part of the KeyUsage certificate extension.</li> <li>▪ A uniform resource indicator (URI) must be set in subjectAltName.</li> <li>▪ The certificate must be in Privacy-Enhanced Mail (PEM) format.</li> </ul>
Client Key	<p><a href="#">This setting is only visible if you select Sign or Sign &amp; Encrypt above.</a></p> <p>Enter the client key for access to the OPC UA server.</p> <p> The client key must be in PEM format and it must be encrypted using the Client Key Password.</p>
Client Key Password	<p><a href="#">This setting is only visible if you select Sign or Sign &amp; Encrypt above.</a></p> <p>Enter the password for the client key.</p>
Authentication Method	<p>Select if you want to connect without credentials or define credentials for access to the OPC UA server:</p> <ul style="list-style-type: none"> <li>▪ Anonymous (default): Connect without credentials.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ User name and password: Define credentials for the connection.</li> <li>ⓘ Most OPC UA servers do not support User name and password authentication without a client certificate. To use User name and password authentication, select Sign or Sign &amp; Encrypt under Security Mode and Basic256Sha256 or Basic256 under Security Policy and enter the Client Certificate, Client Key, and Client Key Password that you want to use.</li> <li>ⓘ If you select None (default) under Security Mode and use User name and password authentication, PRTG sends the unencrypted password to the OPC UA server.</li> <li>ⓘ Most OPC UA servers do not support User name and password authentication without a client certificate. To use User name and password authentication, select Sign or Sign &amp; Encrypt under Security Mode and Basic256Sha256 or Basic256 under Security Policy and enter the Client Certificate, Client Key, and Client Key Password that you want to use.</li> </ul>
User Name	<p>This setting is only visible if you select User name and password <a href="#">above</a>.</p> <p>Enter the user name for access to the OPC UA server.</p>
Password	<p>This setting is only visible if you select User name and password <a href="#">above</a>.</p> <p>Enter the password for access to the OPC UA server.</p>
Data Type	<p>Select the type of the data that PRTG sends:</p> <ul style="list-style-type: none"> <li>▪ Boolean: PRTG sends a Boolean.</li> <li>▪ Int64: PRTG sends a 64-bit integer.</li> <li>▪ Double: PRTG sends a double value.</li> </ul>
Boolean	<p>This setting is only visible if you select Boolean <a href="#">above</a>.</p> <p>Select the Boolean value that PRTG sends:</p> <ul style="list-style-type: none"> <li>▪ True (default)</li> <li>▪ False</li> </ul> <p>ⓘ If you select Boolean as Data Type, the data type on the OPC UA server must be Boolean.</p>
Int64	<p>This setting is only visible if you select Int64 <a href="#">above</a>.</p> <p>Enter the 64-bit integer that PRTG sends.</p>

Setting	Description
	<p><b>i</b> If you select Int64 as Data Type, the data type on the OPC UA server must be Int64.</p>
Double	<p>This setting is only visible if you select Double above.</p> <p>Enter the double value that PRTG sends.</p> <p><b>i</b> If you select Double as Data Type, the data type on the OPC UA server must be Double.</p>

- i** Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

## PRTG Sensor Hub Notifications

In addition to the standard notifications, you can also create custom notifications. To do so, write a script or a program and use it with an Execute Program notification or an Execute HTTP Action notification. There are also many free scripts, plugins, and add-ons for PRTG in the [PRTG Sensor Hub](#).

## Others

- For information about the Comments and History tabs, see section [Object Settings](#)<sup>201</sup>.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

PowerShell 32 bit and 64 bit and Execution Policy

- <https://kb.paessler.com/en/topic/20443>

Is it possible to send SNMP traps using PRTG?

- <https://kb.paessler.com/en/topic/1133>

How can I use push notifications with PRTG?

- <https://kb.paessler.com/en/topic/60892>

How do I create a webhook for the PRTG Notifications to Slack and Microsoft Teams?

- <https://kb.paessler.com/en/topic/80010>

Which audible notifications are available in the PRTG web interface and in the PRTG app for desktop?

- <https://kb.paessler.com/en/topic/26303>

How do I troubleshoot erratic behavior of push notifications in the PRTG app for desktop or PRTG apps?

- <https://kb.paessler.com/en/topic/86064>

## PAESSLER WEBSITE

You can find custom notification scripts in the PRTG Sensor Hub

- <https://www.paessler.com/sensor-hub>

### 8.12.1.3 Notification Contacts

On the Notification Contacts tab, you can define and change the notification contacts of the user account.

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

**☁** If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.

Description	Recipient	Type	Status
Primary Email Address	johnpublic@example.com	Email	Active
Email Admin	admin@example.com	Email	Active
SMS Admin Mobile	+491234567890	SMS	Active

Notification Contacts Tab

Notification contacts are unique for each user account. This means that every user can individually define how they want to receive [notifications](#) from PRTG. Recipients of notifications are email addresses, phone numbers, push devices (with [PRTG for Android](#) or [PRTG for iOS](#)), and users of certain instant messaging services.

The [notification methods](#) Send Email, Send SMS/Pager Message, and Send Push Notification let you define a user who receives notifications for every **active** notification contact. If you select a user group, PRTG sends the notifications to **all active** notification contacts of **all** users that are in the user group. To exclude notification contacts from the notification delivery, use the Pause button to deactivate them.

In this section:

- [Note](#)
- [Notification Contacts Overview](#)
- [Notification Contacts Settings](#)
- [Add Email Contact](#)
- [Add SMS Contact](#)



## Note

You must take the following four steps to set up and use notifications:

1. Check and set up the [notification delivery](#) [2877] settings if you use PRTG Network Monitor. These settings define how PRTG sends messages.
2. Check and set up [notification contacts](#) [2842] for the user accounts. These contacts define the recipients to which PRTG sends notifications.
3. Check and set up several [notification templates](#) [2808]. These templates define the notification methods and their content.
  - ❗ You can also check or edit notification templates via the Notification Triggers tab. For more information, see section [Notification Triggers Settings](#) [2693].
4. Check and set up [notification triggers settings](#) [2693] for objects. These triggers define when PRTG sends notifications.

❗ Usually, there are three successive attempts to deliver a notification. If all of these attempts fail, the notification is lost. To never miss a notification, we recommend that you always set up at least two notifications with different notification methods for a notification trigger, for example, one email notification and one SMS notification. If delivery via email fails, PRTG can still notify you via smartphone as a fallback. For example, use the latency setting of a [state trigger](#) [2694] to choose a notification with a different notification method than in the first trigger condition, or set up a second trigger with a different notification method for the corresponding object.

■ For a detailed step-by-step guide, see the Paessler website: [How to set up notifications via the PRTG web interface](#).

■ Custom notification scripts are also available in the [PRTG Sensor Hub](#).

## Notification Contacts Overview

Click the Notification Contacts tab to show a list of all notification contacts for the user account. You have the following options:

Option	Description
Pause (⏸)	Pauses the notification contact. If a notification contact is <a href="#">paused</a> [227], PRTG does not send any messages to the contact when a notification for this user is triggered.
Resume (▶)	Resumes the notification contact. When a notification for this user is triggered, PRTG sends a message to this user.
Edit (✎)	Open the <a href="#">settings of the notification contact</a> [2844] and change its description and recipient. <ul style="list-style-type: none"> <li>❗ This is not possible for predefined notification contacts, for example, for <a href="#">Primary Email Address</a>. You can change the primary email address under <a href="#">My Account</a> [2801].</li> </ul>

Option	Description
Delete (🗑️)	Delete the notification contact.  ⓘ This is not possible for predefined notification contacts, for example, for <a href="#">Primary Email Address</a> .

## Notification Contacts Settings

Hover over  and select Add Email Contact or Add SMS Contact from the menu to add a new notification contact. You can also click the  next to a notification contact to edit it.

ⓘ PRTG automatically adds push contacts for the corresponding user when you install a PRTG app for iOS or Android on your smartphone or tablet, connect to PRTG, and activate push notifications. You cannot manually add push contacts. If your mobile device actively rejects push notifications for a push contact, for example, because you deactivate push on the target device or reset it, PRTG automatically pauses the push contact. The affected user account receives a [ToDo ticket](#) <sup>[213]</sup> in this case.

**Add New Notification Contact** ✕

---

[Add New Notification Contact](#)

Description ⓘ  
Email Admin

---

Recipient ⓘ  
admin@example.com

---

Contact Type  
*Email*

---

[Cancel](#) OK

Add New Notification Contact

## Add Email Contact

Setting	Description
Description	Enter a description to identify the email contact.  ⓘ If the name contains angle brackets (<>), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a>

Setting	Description
Recipient	<p>Enter a valid email address for the email contact.</p> <p>■ For the contact type <b>Push</b>, this field shows a unique token that you cannot change. PRTG uses this token to send push notifications through the cloud. For more information, see the Knowledge Base: <a href="#">How can I use push notifications with PRTG?</a></p>
Type	<p>Shows the type of the notification contact.</p> <p>ⓘ This setting is for your information only. You cannot change it.</p> <p>ⓘ If you want to use a different contact type, create a new contact with Add Email Contact or Add SMS Contact, or activate push notifications in your PRTG for iOS or Android app.</p>

Click OK to save your settings, or click Cancel to close the dialog box without changes to the notification contact.

### Add SMS Contact

Setting	Description
Description	<p>Enter a description to identify the SMS contact.</p> <p>ⓘ If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Recipient	<p>Enter a valid phone number for the SMS contact. The format of the phone number depends on the SMS provider. You can use a plus sign (+) or 00, followed by the country code and the number. For example, <b>+1555012345</b> or <b>001555012345</b>.</p> <p>ⓘ Make sure that the number format meets the requirements of your SMS provider or the hardware that you use in combination with an application programming interface (API) call. Sometimes a preceding plus sign is not required. The wrong format might result in undelivered messages.</p> <p>■ For the contact type <b>Push</b>, this field shows a unique token that you cannot change. PRTG uses this token to send push notifications through the cloud. For more information, see the Knowledge Base: <a href="#">How can I use push notifications with PRTG?</a></p>
Contact Type	<p>Shows the type of the notification contact.</p> <p>ⓘ This setting is for your information only. You cannot change it.</p>

Setting	Description
	<p><b>i</b> If you want to use a different contact type, create a new contact with Add Email Contact or Add SMS Contact, or activate push notifications in your PRTG for iOS or Android app.</p>

Click OK to save your settings, or click Cancel to close the dialog box without changes to the notification contact.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How can I use push notifications with PRTG?

- <https://kb.paessler.com/en/topic/60892>

### ■ PAESSLER WEBSITE

You can find custom notification scripts in the PRTG Sensor Hub

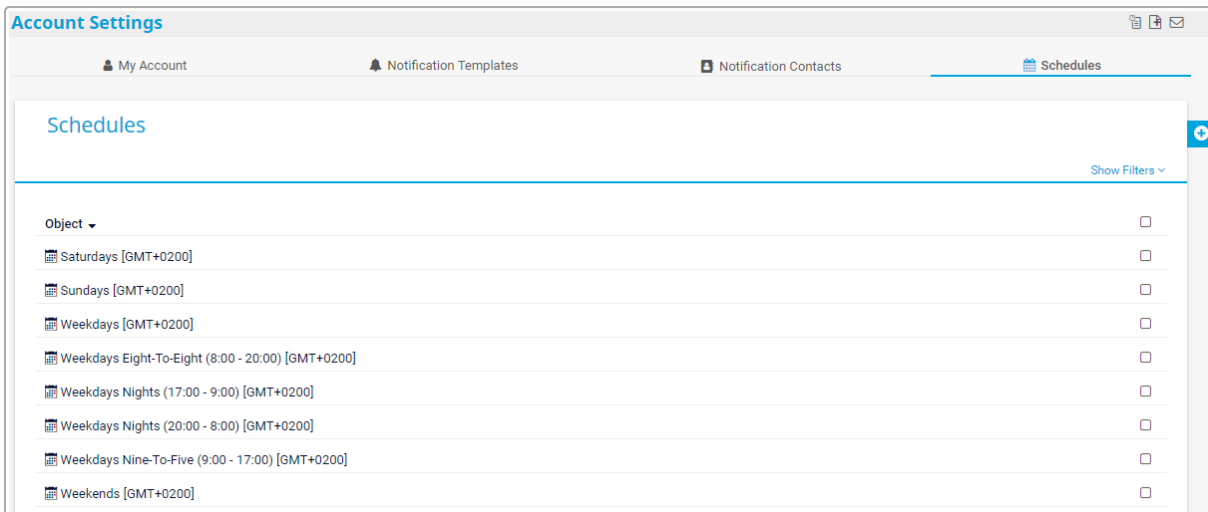
- <https://www.paessler.com/sensor-hub>

#### 8.12.1.4 Schedules

On the Schedules tab, you can define or change schedules for the user account. You can use schedules to [pause](#)<sup>[227]</sup> monitoring and notifications for certain time periods with the period lists option. Also, you can activate monitoring and notifications at certain times with the time table option. You can also use schedules to define the time periods that PRTG covers when you create [reports](#)<sup>[2754]</sup>.

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

**☁** If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.



Schedules Settings




In this section:

- [Schedules Settings](#) <sup>2847</sup>
- [Basic Settings](#) <sup>2848</sup>
- [Access Rights](#) <sup>2850</sup>
- [Schedules and Time Zones](#) <sup>2850</sup>
- [Period Definition Syntax](#) <sup>2851</sup>
- [Others](#) <sup>2851</sup>

## Schedules Settings

**i** When a user with administrative rights creates a new object, only other users with administrative rights can view or edit the new object by default. When a read/write user creates a new object, all members of the read/write user's primary group can view and edit the new object as well. This behavior applies to [libraries](#) <sup>2738</sup>, [maps](#) <sup>2776</sup>, [reports](#) <sup>2754</sup>, [notification templates](#) <sup>2808</sup>, and [schedules](#) <sup>2846</sup>. For more information, see section [Access Rights Management](#) <sup>145</sup>.

Click the Schedules tab to show a list of all schedules. To edit a schedule, enable the check box next to a schedule and choose from the following options:

Option	Description
Used by 	Shows a list of objects that use this schedule.
Delete 	Deletes the schedule. <b>i</b> This is not possible for predefined schedules.
Settings 	Opens the settings of the schedule.

See also sections [Working with Table Lists](#)<sup>[218]</sup> and [Multi-Edit](#)<sup>[2718]</sup>.

Hover over  and select Add Schedule from the menu. You can also click the name of a schedule to edit it.

## Basic Settings

*Schedule Saturdays [GMT +0100]*

---

Settings
Comments
History

### Basic Settings

Schedule Name

Tags








Selection Method  Use weekday/hour time table (default)  
 Use list of period definitions



Time Table (active time slots)

All off	Mo	Tu	We	Th	Fr	Sa	Su
0:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>


Edit Schedule Time Table

Setting	Description
Schedule Name	Enter a name to identify the schedule.  ⓘ If the name contains angle brackets (<>), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a>

Setting	Description
Tags	<p>Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically <a href="#">inherited</a><sup>[138]</sup>.</p> <p> For performance reasons, it can take some minutes until you can filter for new tags that you added.</p> <p> For more information, see section <a href="#">Tags</a><sup>[138]</sup>.</p>
Selection Method	<p>Select the method that you want to use to define a schedule:</p> <ul style="list-style-type: none"> <li>▪ Use weekday/hour time table (default): Select specific days of the week or specific hours in which the schedule is <b>active</b>. This means that monitoring objects, notifications, and reports are not <b>paused</b>.</li> <li>▪ Use list of period definitions: Enter a list of period definitions in which the schedule is <b>inactive</b>. This means that monitoring objects, notifications, and reports are <b>paused</b>.</li> </ul>
Time Table (active time slots)	<p><b>This setting is only visible if you select Use weekday/hour time table (default) above.</b></p> <p>Enable or disable check boxes or use buttons to define the schedule:</p> <ul style="list-style-type: none"> <li>▪ Weekday buttons (  ): Use the weekday buttons Mo, Tu, We, Th, Fr, Sa, and Su to define the days of the week in which the schedule is active. For example, click the Mo button to set the schedule to active for <b>all hours every Monday</b>. This enables all check boxes under the Mo column.</li> <li>▪ Hour buttons (  ): Use the hour buttons 0:00 - 23:00 to define the hours of the day in which the schedule is active. For example, if the 0:00 button is blue, click it to set the schedule to active for the hour <b>0:00 of all days</b> of the week. If the 0:00 button is white, click it to set the schedule to inactive for the hour <b>0:00 of all days</b> of the week.</li> <li>▪ All off button (  ): Use the All off button to disable all check boxes, and to deselect all weekday buttons and hour buttons.</li> <li>▪ All on button (  ): Use the All on button to enable all check boxes, and to select all weekday buttons and hour buttons.</li> </ul> <p> For more information, see <a href="#">Schedules and Time Zones</a><sup>[2850]</sup> below.</p>
Period List (inactive time slots)	<p><b>This setting is only visible if you select Use list of period definitions above.</b></p> <p>Enter the date and time periods in which the schedule is <b>inactive</b>. The periods must have the following format:</p>


Setting	Description
	<p><a href="#">ww:hh:mm-ww:hh:mm</a></p> <p> Make sure that you enter each period exactly in this format. Otherwise you receive an error message. Go back to the schedule and correct the period in this case. For details and examples, see <a href="#">Period Definition Syntax</a> <sup>2851</sup> below.</p> <p> For more information, see <a href="#">Schedules and Time Zones</a> <sup>2850</sup> below.</p>

## Access Rights

Setting	Description
User Group Access	<p>Define the user groups that have access to the object. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights:</p> <ul style="list-style-type: none"> <li>▪ No access: Users in this user group cannot see or edit the object. The object does not show up in lists.</li> <li>▪ Read access: Users in this user group can see the object and view its settings.</li> <li>▪ Write access: Users in this user group can see the object and view and edit its settings. However, they cannot edit the object's access rights settings.</li> <li>▪ Full access: Users in this user group can see the object, view and edit its settings, and edit its access rights settings.</li> </ul> <p> You can create new user groups in the <a href="#">User Groups</a> <sup>2912</sup> settings.</p>

 Click OK to save your settings. If you close the dialog without saving, all changes to the settings are lost.

## Schedules and Time Zones

-  Schedules use the time zone of the PRTG core server system. This might be different from other time displays in PRTG that are saved in UTC.
- If you select Use weekday/hour time table (default), PRTG converts the time in which the schedule is active to the time zone of [the user account](#) <sup>2909</sup>. This means that the schedule applies according to the time that the user account shows.
  - If you select Use list of period definitions, PRTG does **not** adjust the time in which the schedule is inactive to the time zone of the user account. The schedule applies according to the time on the PRTG core server system in this case. Because of this, you encounter time shifts for schedules if there are changes to the time zone on the server or because of daylight saving and standard time changes.



## Period Definition Syntax

Define one or more periods of time during which the object that uses this schedule is **inactive**. In each line, enter one range in the format `ww:hh:mm-ww:hh:mm`. The following values are possible:

- **ww**: mo, tu, we, th, fr, sa, su.
- **hh**: Enter the hour in the 24-hour format. For example, a number between 00 and 23.  
❗ You must use the 24-hour format. You cannot use A.M./P.M.
- **mm**: Enter the minute. For example, a number between 00 and 59.

### Example

This example shows a schedule that pauses an object during the weekend as well as on Wednesday evenings.

```
fr:19:30-mo:06:05
we:18:45-we:23:00
```

Any object that uses this schedule is inactive (paused) from Friday, 7:30 P.M. to Monday, 6:05 A.M. as well as on Wednesday from 6:45 P.M. to 11 P.M. It is active during the other times.

## Others

- For information about the comments and history tabs, see section [Object Settings](#)<sup>[201]</sup>.

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

## Others

There are some settings that you must define in the [PRTG Administration Tool](#)<sup>[3040]</sup>. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#)<sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#)<sup>[3067]</sup>

### 8.12.1.5 API Keys


On the API Keys tab, you can add, edit, and delete API keys that are specific to the user account.

❗ This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

☁ If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.

## API Keys Overview

Click the API Keys tab to show a list of all API keys for the user account. You have the following options:

Option	Description
Edit (✎)	Open the <a href="#">settings of the API key</a> <sup>[2854]</sup> and change its name, description, and access level.
Delete (🗑)	Delete the API key.   You can select and delete multiple API keys at once using <a href="#">multi-edit</a> <sup>[2718]</sup> .

## Add API Key

Hover over  and select Add API Key from the menu to add a new API key.

Add New API Key



Add New API Key

Here you can add, modify, and delete API keys. With API keys, you can authenticate with the PRTG API without a user name and password.

We recommend the following best practices:

- Give API keys the least possible access level that you can work with
- Use separate API keys for different integrations and applications
- Store your API keys in a safe place to prevent unauthorized access
- Rotate your API keys regularly to prevent abuse in case they are leaked or exposed
- Delete unused API keys immediately

For more information, see the [PRTG Manual: API Keys](#)

Name ⓘ

Example API key

Description ⓘ

Full access API key

Access Level ⓘ

Full access

API Key ⓘ

EXAMPLEAPIKEYWITHFULLACCESS=====

**Important:** Copy and store this API key. After you click OK, the API key will not be visible again.

Cancel

**OK**

Add new API key

Setting	Description
Name	Enter a name to identify the API key. ⓘ If the name contains angle brackets (<>), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a>
Description	Enter a description for the API key.
Access Level	Select the access level for the API key: <ul style="list-style-type: none"> <li>▪ Read access</li> <li>▪ Acknowledge access</li> <li>▪ Write access</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Full access</li> </ul> <p><b>i</b> For more information about access rights in PRTG, see section <a href="#">Access Rights Management</a> [145].</p>
API Key	<p>Shows the token.</p> <p><b>i</b> Copy and store this token. After you click OK, the token will not be visible again.</p> <p><b>i</b> This setting is for your information only. You cannot change it. If you lose it, you should remove the API key and create a new one.</p>

Click OK to save your settings, or click Cancel to close the dialog box without creating an API key.

### Edit API Key

**Edit API Key**
✕

---

Edit API Key

**Name** ⓘ

Example API key

---

**Description** ⓘ

Full access API key

---

**Access Level** ⓘ

Full access ▼

---

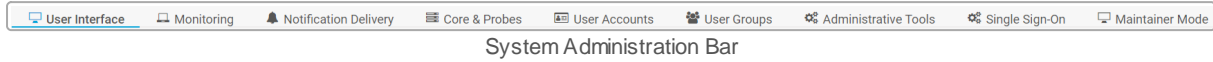
Cancel
OK

Edit API Key

After creation, you can edit the name, the Name, the Description, and the Access Level of your API keys.

## 8.12.2 System Administration

To open the system administration, select Setup | System Administration from the [main menu bar](#) <sup>[249]</sup>. Select the various tabs to change the different settings.



In this section:

- [User Interface](#) <sup>[2855]</sup>
- [Monitoring](#) <sup>[2869]</sup>
- [Notification Delivery](#) <sup>[2877]</sup>
- [Core & Probes](#) <sup>[2887]</sup>
- [User Accounts](#) <sup>[2901]</sup>
- [User Groups](#) <sup>[2912]</sup>
- [Administrative Tools](#) <sup>[2918]</sup>
- [Cluster](#) <sup>[2923]</sup>
- [Single Sign-On](#) <sup>[2925]</sup>
- [Maintainer Mode](#) <sup>[2931]</sup>

### 8.12.2.1 User Interface

On the User Interface tab, you can define global settings regarding the PRTG web interface, PRTG web server settings and performance, Geo Maps, and graph settings.

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

**☁** If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.

In this section:

- [PRTG Web Interface](#) <sup>[2856]</sup>
- [Geo Maps](#) <sup>[2859]</sup>
- [PRTG Web Server](#) <sup>[2860]</sup>
- [Graph Settings](#) <sup>[2866]</sup>

## PRTG Web Interface

**PRTG Web Interface**

Site Name ⓘ PRTG Network Monitor

---

DNS Name ⓘ

---

Language ⓘ English

---

Graph Type ⓘ  Display area graphs (default)  
 Display line graphs

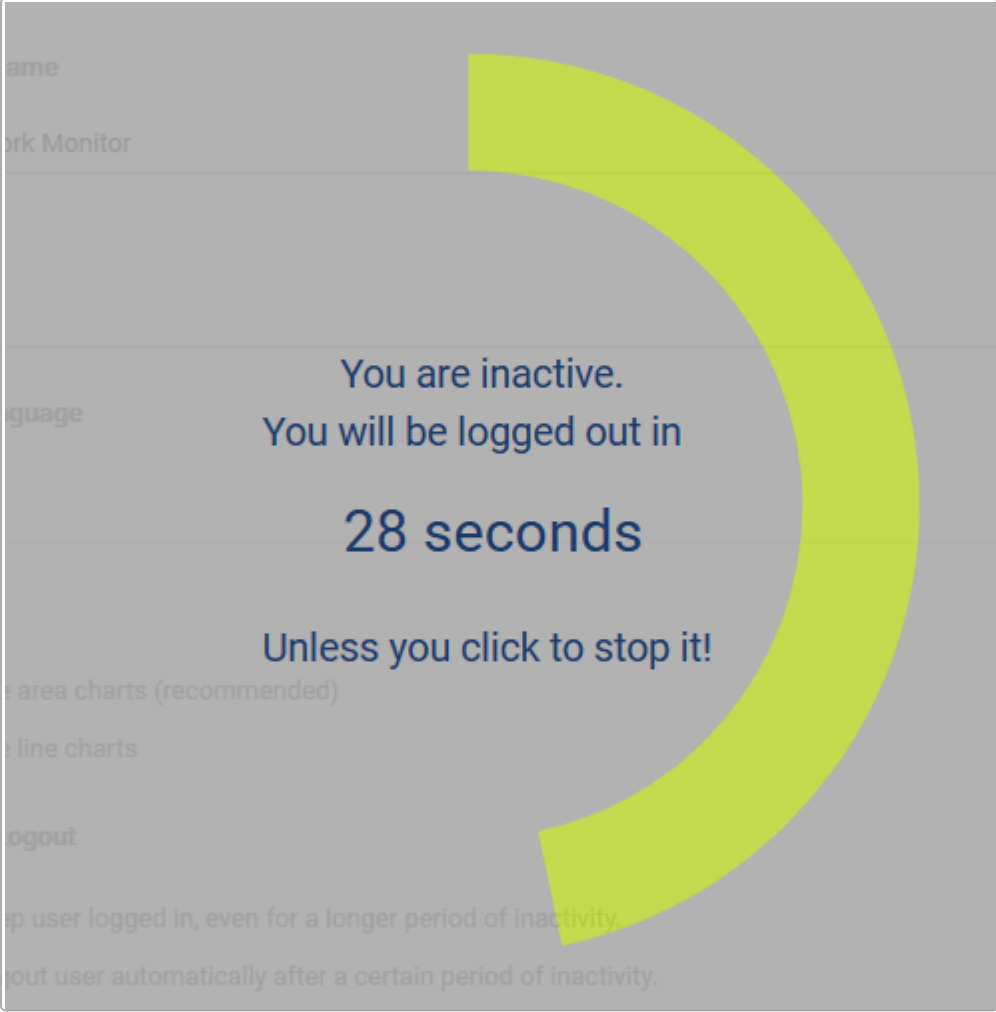
Automatic Logout ⓘ  Do not log out users after a period of inactivity  
 Log out users after a period of inactivity

Google Analytics Tracking ID ⓘ

PRTG Web Interface

Setting	Description
Site Name	<p>In the PRTG web interface, you can see the site name on the <a href="#">Login</a><sup>[153]</sup> screen and in the title bar of the browser window. PRTG also uses the site name in notification emails by default. Enter a string.</p> <p> ⓘ If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({}), for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
DNS Name	<p>Enter a Domain Name System (DNS) name if the PRTG web interface is also reachable via the DNS name. PRTG also uses the DNS name in notification emails to generate links by default. Enter a string.</p> <p> ⓘ Do not use the special characters " and \ in the DNS name.</p> <p> ⓘ In a cluster, only the master node uses the DNS name that you enter. You cannot enter a DNS name for a failover node.</p> <p> ☁ This option is not available in PRTG Hosted Monitor.</p>
Language	<p>Select the language. The default language is English.</p> <p> ⓘ This setting defines the language of the PRTG web interface and the <a href="#">PRTG Administration Tool</a><sup>[8040]</sup>.</p> <p>List of available languages:</p> <ul style="list-style-type: none"> <li>▪ Deutsch (German)</li> <li>▪ English</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Español (Spanish)</li> <li>▪ Français (French)</li> <li>▪ Nederlands (Dutch)</li> <li>▪ Português (Portuguese)</li> <li>▪ Русский (Russian)</li> <li>▪ 日本語 (Japanese)</li> <li>▪ 简体中文 (Simplified Chinese)</li> </ul> <p><b>i</b> If you change this setting, PRTG needs to restart the PRTG core server to apply your changes. After you click Save, a dialog box appears that asks you to confirm the restart. Click OK to trigger the restart. During the restart, all users of the PRTG web interface, the <a href="#">PRTG app for desktop</a><sup>[2984]</sup>, or the <a href="#">PRTG Apps for Mobile Network Monitoring</a><sup>[2988]</sup> are disconnected and reconnected.</p>
Graph Type	<p>Select how PRTG displays graphs in the PRTG web interface and in <a href="#">reports</a><sup>[2754]</sup>:</p> <ul style="list-style-type: none"> <li>▪ Display area graphs (recommended): Display series of data points connected by straight lines. Areas between axis and lines are shaded.</li> <li>▪ Display line graphs: Display series of data points connected by straight lines.</li> </ul> <p><b>i</b> We recommend that you use area charts for better visibility.</p> <p><b>i</b> PRTG automatically displays graphs that contain data from more than one cluster node as line graphs.</p>
Automatic Logout	<p>Define if PRTG automatically logs inactive users out of the PRTG web interface:</p> <ul style="list-style-type: none"> <li>▪ Do not log out users after a period of inactivity: Do not log out users even if they are inactive for a longer period of time.</li> <li>▪ Log out users after a period of inactivity: Log out users if they are inactive for a certain period of time for security reasons.</li> </ul>
Period of Inactivity	<p><b>This setting is only visible if you select Log out users after a period of inactivity above.</b></p> <p>Specify the period of inactivity in minutes after which PRTG automatically logs out users. Enter an integer.</p> <p><b>i</b> PRTG redirects users to the <a href="#">Login</a><sup>[153]</sup> screen after this period of inactivity.</p> <p><b>i</b> If the value you enter is greater than <b>1 minute</b>, a logout countdown appears 1 minute before PRTG logs out users. If the value is 1 minute, users see the logout countdown <b>30 seconds</b> before PRTG logs them out. Click in the browser window to stop the countdown and to stay logged in to the PRTG web interface.</p>

Setting	Description
	 <p style="text-align: center;">Logout Countdown</p>
<p>Google Analytics Tracking ID</p>	<p>Enter your <a href="#">Google Analytics Tracking ID</a> to track the usage of pages in the PRTG web interface with Google Analytics. Enter a string or leave the field empty. The string looks like this <code>UA-xxxxxx-xx</code>, for example.</p> <p><b>i</b> You need a Google Analytics account for this feature. Create a tracking ID within the Google Analytics portal and enter it here. PRTG then dynamically integrates it into the PRTG web interface.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">How can I integrate Google Analytics into PRTG?</a></p> <p><b>☁</b> This option is not available in PRTG Hosted Monitor.</p>



## Geo Maps

**Geo Maps**

**Service Provider** ?

Disable Geo Maps integration

Default

HERE Maps

Google Maps

**Map Type** ?

Standard (default)

Satellite

Geo Maps

Setting	Description
Service Provider	<p>Select if and how you want to enable the Geo Maps feature. If you enable the feature, PRTG uses the first line of the <a href="#">location setting</a><sup>422</sup> of an object to show it on a geographical map. Choose a map provider:</p> <ul style="list-style-type: none"> <li>▪ <b>Disable Geo Maps integration:</b> Disable the Geo Maps feature and do not show geographical maps in the PRTG web interface.</li> <li>▪ <b>Default:</b> Use the default option HERE Maps to show geographical maps.</li> <li>▪ <b>HERE Maps:</b> Use HERE Maps to show geographical maps.</li> <li>▪ <b>Google Maps:</b> Use Google Maps to show geographical maps. Sign up for a Google Maps API key to use this service.</li> </ul> <p><span style="color: #0070C0;">■</span> For more information about the different map providers, see the Knowledge Base: <a href="#">Which provider should I use for the Geo Maps feature of PRTG?</a></p>
Map Type	<p>The options that are available depend on the map provider that you select above. Default, HERE Maps, and Google Maps all have the following options:</p> <ul style="list-style-type: none"> <li>▪ <b>Standard (default):</b> Show geographical maps in a standard map view.</li> <li>▪ <b>Satellite:</b> Show geographical maps in a satellite view.</li> </ul> <p>In addition to these options, Google Maps also has the following options:</p> <ul style="list-style-type: none"> <li>▪ <b>Terrain:</b> Show geographical maps in a terrain view.</li> <li>▪ <b>Hybrid (satellite and standard map):</b> Show geographical maps in a hybrid view.</li> </ul>
Google Maps Static API Key	<p><span style="color: #0070C0;">This setting is only visible if you select Google Maps above.</span></p> <p>Enter your Google Maps Static API key.</p>

Setting	Description
	<p>■ For more information on how to get a Google API key, see the Knowledge Base: <a href="#">How do I get a Google Maps API key for use in PRTG?</a></p>

## PRTG Web Server

### PRTG Web Server

**Performance Handling** ⓘ  Do not limit features or delay display (default)  
 Limit features and delay display

**IP Address for PRTG Web Server** ⓘ  Localhost, 127.0.0.1 (PRTG is not accessible from other computers)  
 All IP addresses available on the PRTG core server system (default)  
 Specify IP addresses

**TCP Port for PRTG Web Server** ⓘ  Secure HTTPS server (default port 443, recommended, mandatory for internet access)  
 Unsecure HTTP server (default port 80)  
 Custom configuration


**Connection Security** ⓘ  High security (TLS 1.3, TLS 1.2)  
 Default security (TLS 1.3, TLS 1.2) (recommended)  
 Weakened security (TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0)

**Import Your Own Certificate** *Tip: You can install your own trusted SSL certificate for PRTG to avoid web browser warnings when you connect to the PRTG web interface. To ease the certificate import, we recommend that you use the PRTG Certificate Importer. For more information about this freeware tool, refer to [our webpage](#) where you can also directly download the PRTG Certificate Importer.*

**Active IP Address/Port Combination(s)** ⓘ

IP Address:Port
10.49.196.180:443
10.49.196.180:80
127.0.0.1:443
127.0.0.1:80
127.0.0.1:8085

PRTG Web Server

Setting	Description
Performance Handling	<p>Select if you want to enable performance improvements for the PRTG web interface:</p> <ul style="list-style-type: none"> <li>▪ Do not limit features or delay display (recommended): Provide full functionality and show all menu items and live data. <ul style="list-style-type: none"> <li>ⓘ We recommend that you use this option.</li> </ul> </li> <li>▪ Limit features and delay display: Improve the reaction time and speed of the PRTG web interface by delaying the display of monitoring data and hiding some features.</li> </ul> <p> For more information on how to speed up the PRTG web interface, see the Knowledge Base: <a href="#">How can I speed up PRTG—especially for large installations?</a></p>
IP Address for PRTG Web Server	<p>The PRTG web server provides access via the PRTG web interface and the <a href="#">PRTG app for desktop</a><sup>2984</sup>. Once you specify an IP address, you use it to log in to the PRTG web interface in your browser. Specify on which IP address the PRTG web server runs:</p> <ul style="list-style-type: none"> <li>▪ Localhost, 127.0.0.1 (PRTG is not accessible from other computers): Use <a href="#">127.0.0.1</a> only. The PRTG web interface and the PRTG app for desktop are only accessible from the PRTG core server system. <ul style="list-style-type: none"> <li>ⓘ Either the selected port or at least one port in the range from <a href="#">8080</a> to <a href="#">8089</a> must be available on <a href="#">127.0.0.1</a>.</li> <li>ⓘ If you run PRTG on localhost, do not use the DNS name <a href="#">http://localhost</a> to log in to the PRTG web server. This might considerably slow down the PRTG web interface. Use your local IP address or <a href="#">http://127.0.0.1</a> instead.</li> </ul> </li> <li>▪ All IP addresses available on the PRTG core server system (recommended): Use all IP addresses that are available on the PRTG core server system and enable access to the PRTG web server for all of these IP addresses. <ul style="list-style-type: none"> <li>ⓘ The selected Transmission Control Protocol (TCP) port for the PRTG web server must be available on all selected IP addresses.</li> </ul> </li> <li>▪ Specify IP addresses: Select specific IP addresses on which the PRTG web server runs. The list is specific to your setup. Enable check boxes in front of every IP address that you want the PRTG web server to be available at. You can also select all IP addresses by clicking the Select all IP addresses button or deselect all addresses by clicking the Deselect all IP addresses button. <ul style="list-style-type: none"> <li>ⓘ Either the selected port or at least one port in the range from <a href="#">8080</a> to <a href="#">8089</a> must be available on the specified IP address.</li> <li>ⓘ Regardless of the setting that you select, one port in the range from <a href="#">8080</a> to <a href="#">8180</a> must be available on the specified IP address so that PRTG can create reports. The report engine tries to connect to the PRTG core server on one of these ports.</li> </ul> </li> </ul>

Setting	Description
	<p><b>i</b> If PRTG does not find a network card on startup, it switches this setting to Localhost, 127.0.0.1 (PRTG is not accessible from other computers). This setting remains even if a network card is available later on. If you disable or remove the network card on the PRTG core server system, check this setting.</p> <p><b>i</b> If you change this setting, PRTG needs to restart the PRTG core server to apply your changes. After you click Save, a dialog box appears that asks you to confirm the restart. Click OK to trigger the restart. During the restart, all users of the PRTG web interface, the <a href="#">PRTG app for desktop</a><sup>[2984]</sup>, or the <a href="#">PRTG Apps for Mobile Network Monitoring</a><sup>[2985]</sup> are disconnected and reconnected.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
<p>TCP Port for PRTG Web Server</p>	<p>Specify how the PRTG web server accepts incoming web page requests:</p> <ul style="list-style-type: none"> <li>▪ Secure HTTPS server (port 443, recommended, mandatory for internet access): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured HTTPS connection on port 443. <ul style="list-style-type: none"> <li><b>i</b> This setting is required if you want to access the PRTG web interface via the internet.</li> <li><b>i</b> Although the connection is secure, you see an SSL certificate warning in your browser when you log in to the PRTG web interface because the default certificate is unknown to your browser. For more information, see the Knowledge Base: <a href="#">Why does my browser show an SSL certificate warning when I open the PRTG web interface?</a>. You can install a different SSL certificate for PRTG. For more information, see the Paessler website: <a href="#">How to use your own SSL certificate with the PRTG web server</a>.</li> <li><b>i</b> If port 80 is available, PRTG reserves it as well. If port 80 is not available, PRTG tries port 8080 as fallback. If this port is also not available, PRTG searches from port 8081 upwards for a free port. PRTG sends a <a href="#">ticket</a><sup>[213]</sup> that shows you the currently used port number and switches back to port 80 as soon as it is available again. When users try to connect on port 80 via HTTP, they are redirected to port 443 via HTTPS. You can change this behavior via a registry setting. If port 443 is not available, PRTG tries port 8443 as fallback. If this port is also not available, PRTG searches from port 8444 upwards for a free port. PRTG sends a ticket that shows you the currently used port number and switches back to port 443 as soon as it is available again.</li> </ul> </li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Unsecure HTTP server (default port 80, not recommended): Use the PRTG web server without SSL/TLS on port 80.               <ul style="list-style-type: none"> <li>ⓘ This setting is not recommended for WAN connections.</li> <li>ⓘ If you use the PRTG web server via the internet without connection security, attackers could potentially spy on credentials that you enter in PRTG. We strongly recommend that you use this option only in a LAN.</li> </ul> </li> <li>▪ Custom configuration: Specify a custom port for the PRTG web server and the security of the connection. This option is intended for systems that already have a web server on the standard port.               <ul style="list-style-type: none"> <li>ⓘ If PRTG always uses a fallback port after a server restart, check for other programs that use the same port as PRTG. For example, the Microsoft Microsoft Internet Information Services (IIS) web server also uses port 80 (port 443 for secure connections) by default and blocks it. We recommend that you disable such programs and services on startup.</li> <li>ⓘ If you change this setting, PRTG needs to restart the PRTG core server to apply your changes. After you click Save, a dialog box appears that asks you to confirm the restart. Click OK to trigger the restart. During the restart, all users of the PRTG web interface, the <a href="#">PRTG app for desktop</a><sup>[2984]</sup>, or the <a href="#">PRTG Apps for Mobile Network Monitoring</a><sup>[2988]</sup> are disconnected and reconnected.</li> </ul> </li> </ul> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
PRTG Web Server Port	<p>This setting is only visible if you select Custom configuration above.</p> <p>Enter the TCP port number (between 1 and 65535) that you want the PRTG web server to run on. Enter an integer.</p> <ul style="list-style-type: none"> <li>ⓘ If you use a secure connection and port 80 is free, PRTG also reserves it. When users try to connect on port 80 via HTTP, they are redirected to the custom port via HTTPS. You can change this behavior via a registry setting.</li> <li>ⓘ If the port that you define for secure connections is not available, PRTG tries port 8443 as fallback. If this port is also not available, PRTG searches from port 8444 upwards for a free port. PRTG sends a <a href="#">ticket</a><sup>[213]</sup> that shows you the currently used port and switches back to the original port as soon as it is available again.</li> <li>ⓘ If you change this setting, PRTG needs to restart the PRTG core server to apply your changes. After you click Save, a dialog box appears that asks you to confirm the restart. Click OK to trigger the restart. During the restart, all users of the PRTG web interface, the <a href="#">PRTG app for desktop</a><sup>[2984]</sup>, or the <a href="#">PRTG Apps for Mobile Network Monitoring</a><sup>[2988]</sup> are disconnected and reconnected.</li> </ul>

Setting	Description
	<p>☁ This option is not available in PRTG Hosted Monitor.</p>
<p>PRTG Web Server Security</p>	<p><a href="#">This setting is only visible if you select Custom configuration above.</a></p> <p>Specify if you want to use connection security:</p> <ul style="list-style-type: none"> <li>▪ Use HTTPS (secured with SSL/TLS): Use an SSL/TLS secured HTTPS connection on the port that you define as PRTG Web Server Port. <ul style="list-style-type: none"> <li>ⓘ Although the connection is secure, you see an SSL certificate warning in your browser when you log in to the PRTG web interface, because the default certificate is unknown to your browser. You can install a different SSL certificate for PRTG later. For more information, see the Paessler website: <a href="#">How to use your own SSL certificate with the PRTG web server.</a></li> </ul> </li> <li>▪ Do not use connection security: Use the PRTG web server without SSL/TLS on the port that you define as PRTG Web Server Port. <ul style="list-style-type: none"> <li>ⓘ We recommend that you do not use this setting for WAN connections.</li> <li>ⓘ If you use the PRTG web server without connection security on the internet, attackers could potentially spy on credentials that you enter in PRTG. We strongly recommend that you use this setting in a LAN only.</li> <li>ⓘ If you change this setting, PRTG needs to restart the PRTG core server to apply your changes. After you click Save, a dialog box appears that asks you to confirm the restart. Click OK to trigger the restart. During the restart, all users of the PRTG web interface, the <a href="#">PRTG app for desktop</a><sup>[2984]</sup>, or the <a href="#">PRTG Apps for Mobile Network Monitoring</a><sup>[2985]</sup> are disconnected and reconnected.</li> </ul> </li> </ul> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
<p>Connection Security</p>	<p>Specify the security level to use for connections to and from the PRTG web server:</p> <ul style="list-style-type: none"> <li>▪ High security (TLS 1.3, TLS 1.2): Only accept high security connections from clients like web browsers, apps, the PRTG app for desktop, or API clients. <ul style="list-style-type: none"> <li>ⓘ These clients must support modern forward secrecy cipher suites.</li> </ul> </li> <li>▪ Default security (TLS 1.3, TLS 1.2) (recommended): Only accept high security connections from clients like web browsers, apps, the PRTG app for desktop, or API clients. <ul style="list-style-type: none"> <li>ⓘ These clients must support modern forward secrecy cipher suites.</li> </ul> </li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Weakened security (TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0): If you have clients that do not support High security (TLS 1.3, TLS 1.2) or Default security (TLS 1.3, TLS 1.2) (recommended), temporarily use this setting so that they can connect. This setting accepts TLS 1.3, TLS 1.2, TLS 1.1 and TLS 1.0 connections.               <ul style="list-style-type: none"> <li>ⓘ This might be necessary, for example, for older browsers, browsers that run on old network components, or some default browsers on Android systems.</li> <li>ⓘ We strongly recommend that you update your clients and then use Default security (TLS 1.3, TLS 1.2) (recommended) or High security (TLS 1.3, TLS 1.2).</li> <li>ⓘ If you set a registry key in previous PRTG versions to override the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) version and cipher suites of PRTG web server connections or probe connections, High security (TLS 1.3, TLS 1.2) overrides the registry setting and only TLS 1.3 and TLS 1.2 are allowed. If you select Default security (TLS 1.3, TLS 1.2) (recommended), the <a href="#">registry value overrides this setting</a> and the connection security that you defined in the registry applies.</li> <li>ⓘ PRTG displays the SSL/TLS versions and cipher suites that are used for connections to and from the PRTG web server under <a href="#">Setup   PRTG Status</a><sup>[2935]</sup>.</li> <li>ⓘ If you change this setting, PRTG needs to restart the PRTG core server to apply your changes. After you click Save, a dialog box appears that asks you to confirm the restart. Click OK to trigger the restart. During the restart, all users of the PRTG web interface, the <a href="#">PRTG app for desktop</a><sup>[2984]</sup>, or the <a href="#">PRTG Apps for Mobile Network Monitoring</a><sup>[2988]</sup> are disconnected and reconnected.</li> </ul> </li> </ul> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
<p>Active IP Address/Port Combinations</p>	<p>Shows all active combinations of the IP addresses and ports on which the PRTG web server listens for web requests.</p> <ul style="list-style-type: none"> <li>ⓘ This setting is for your information only. You cannot change it.</li> <li>ⓘ PRTG internally uses port 8085 for report generation.</li> </ul> <p>☁ This option is not available in PRTG Hosted Monitor.</p>

## Graph Settings

PRTG shows several graphs on the Overview tabs and x Days tabs of objects in the PRTG web interface. PRTG keeps these in RAM for fast graph display. The longer the time frames and the shorter the intervals are, the more memory PRTG uses for this. You can adapt the details for all four graphs. This setting also changes the caption of the graphs and tabs in the PRTG web interface and the PRTG app for desktop.

**i** If you change this setting, PRTG needs to restart the PRTG core server to apply your changes. After you click Save, a dialog box appears that asks you to confirm the restart. Click OK to trigger the restart. During the restart, all users of the PRTG web interface, the [PRTG app for desktop](#)<sup>[2984]</sup>, or the [PRTG Apps for Mobile Network Monitoring](#)<sup>[2988]</sup> are disconnected and reconnected.

**Graph Settings**

*The RAM usage of PRTG depends on the memory that it requires to store the data for group, device, and sensor graphs. This is necessary for fast graph display. You can reduce the memory requirement by using shorter time frames with longer intervals. Select the period and the average interval to use for the graphs and tables.*

*Note: If you change this setting, PRTG needs to restart the PRTG core server to apply your changes. Afterwards, PRTG recalculates the data cache. During recalculation, the graphs might show incomplete data.*

Live Graph <b>i</b>	120 values (= 2 hours with a scanning interval of 1 minute)	▼
Graph 1 <b>i</b>	2 days with averages of 5 minutes	▼
Graph 2 <b>i</b>	60 days with averages of 6 hours	▼
Graph 3 <b>i</b>	365 days with averages of 1 day	▼

Graph Settings

Setting	Description
Live Graph	<p><b>i</b> The live graph is only available for sensors.</p> <p>The live graph does not have a fixed time span but you can define how many values to display. The actual time span that the live graph covers depends on the scanning interval of the sensor that you view. PRTG automatically calculates the time span. The default is <b>120 Values</b>. This results in a graph that covers a time span of two hours if a sensor has a 1-minute scanning interval. Other scanning intervals result in graphs that cover different time spans.</p> <p>Define how many values the graph displays:</p> <ul style="list-style-type: none"> <li>▪ 60 values: Cover a time span of one hour if a sensor has a scanning interval of one minute.</li> </ul> <p><b>i</b> This setting uses the least amount of RAM. We recommend this setting for installations with 10,000 sensors or more.</p> <ul style="list-style-type: none"> <li>▪ 120 values: Cover a time span of two hours if a sensor has a scanning interval of one minute.</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ 240 values: Cover a time span of four hours if a sensor has a scanning interval of one minute.</li> <li>▪ 480 values: Cover a time span of eight hours if a sensor has a scanning interval of one minute.</li> <li>▪ 960 values: Cover a time span of 16 hours if sensor has a scanning interval of one minute.</li> </ul> <p><b>i</b> This setting uses the most amount of RAM.</p>
Graph 1	<p>By default, this is the 2 days graph in the PRTG web interface. You can change it to have more or less detail. PRTG averages the monitoring results of the actual scanning intervals of the sensors.</p> <p>Define how many values the graph displays:</p> <ul style="list-style-type: none"> <li>▪ 1 day with averages of 1 minute: Cover a time span of one day with averages of one minute. This results in 1440 values.</li> <li>▪ 1 day with averages of 5 minutes: Cover a time span of one day with averages of five minutes. This results in 288 values.</li> <li>▪ 1 day with averages of 15 minutes: Cover a time span of one day with averages of 15 minutes. This results in 96 values.</li> </ul> <p><b>i</b> This setting uses the least amount of RAM. We recommend this setting for installations with 10,000 sensors or more.</p> <ul style="list-style-type: none"> <li>▪ 2 days with averages of 1 minute : Cover a time span of two days with averages of one minute. This results in 2880 values.</li> </ul> <p><b>i</b> This setting uses the most amount of RAM.</p> <ul style="list-style-type: none"> <li>▪ 2 days with averages of 5 minutes: Cover a time span of two days with averages of five minutes. This results in 576 values.</li> <li>▪ 2 days with averages of 15 minutes: Cover a time span of two days with averages of 15 minutes. This results in 192 values.</li> <li>▪ 4 days with averages of 1 hour: Cover a time span of two days with averages of one hour. This results in 96 values.</li> </ul> <p><b>i</b> This setting uses the least amount of RAM. We recommend this setting for installations with 10,000 sensors or more.</p>
Graph 2	<p>By default, this is the 30 days graph in the PRTG web interface. You can change it to have more or less detail.</p> <p>Define how many values the graph displays:</p> <ul style="list-style-type: none"> <li>▪ 10 days with averages of 1 hour: Cover a time span of 10 days with averages of one hour. This results in 240 values.</li> <li>▪ 20 days with averages of 1 hour: Cover a time span of 20 days with averages of one hour. This results in 480 values.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ 30 days with averages of 1 hour: Cover a time span of 30 days with averages of one hour. This results in 720 values.</li> <li>▪ 30 days with averages of 6 hours: Cover a time span of 30 days with averages of six hours. This results in 120 values.</li> <li>ⓘ This setting uses the least amount of RAM. We recommend this setting for installations with 10,000 sensors or more.</li> <li>▪ 40 days with averages of 1 hour: Cover a time span of 40 days with averages of one hour. This results in 960 values.</li> <li>▪ 40 days with averages of 6 hours: Cover a time span of 40 days with averages of six hours. This results in 160 values.</li> <li>▪ 60 days with averages of 1 hour: Cover a time span of 60 days with averages of one hour. This results in 1440 values.</li> <li>ⓘ This setting uses the most amount of RAM.</li> <li>▪ 60 days with 6 hour averages of 6 hours: Cover a time span of 60 days with averages of six hours. This results in 240 values.</li> </ul>
Graph 3	<p>By default, this is the 365 days graph in the PRTG web interface. You can change it to more or less detail by choosing a time span covered and a monitoring interval average associated with it.</p> <p>Define how many values the graph displays:</p> <ul style="list-style-type: none"> <li>▪ 100 days with averages of 1 day: Cover a time span of 100 days with averages of one day. This results in 100 values.</li> <li>ⓘ This setting uses the least amount of RAM. We recommend this setting for installations with 10,000 sensors or more.</li> <li>▪ 200 days with averages of 1 day: Cover a time span of 200 days with averages of one day. This results in 200 values.</li> <li>▪ 365 days with averages of 1 day: Cover a time span of 365 days with averages of one day. This results in 365 values.</li> <li>▪ 400 days with averages of 1 day: Cover a time span of 400 days with averages of one day. This results in 400 values.</li> <li>▪ 750 days with averages of 1 day: Cover a time span of 750 days with averages of one day. This results in 750 values.</li> <li>ⓘ This setting uses the most amount of RAM.</li> </ul>

ⓘ Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

More

■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How can I integrate Google Analytics into PRTG?

- <https://kb.paessler.com/en/topic/61406>

Which provider should I use for the Geo Maps feature of PRTG?

- <https://kb.paessler.com/en/topic/34603>

How do I get a Google Maps API key for use in PRTG?

- <https://kb.paessler.com/en/topic/32363>

How can I speed up PRTG—especially for large installations?

- <https://kb.paessler.com/en/topic/2733>

Which domains and ports does the Geo Maps feature use?

- <https://kb.paessler.com/en/topic/35823>

Which limitations apply when using the Google Maps API in PRTG?

- <https://kb.paessler.com/en/topic/7913>

Why does my browser show an SSL certificate warning when I open the PRTG web interface?

- <https://kb.paessler.com/en/topic/89984>

## ■ PAESSLER WEBSITE

How to use your own SSL certificate with the PRTG web server

- <https://www.paessler.com/support/how-to/ssl-certificate>


## Others


There are some settings that you must define in the [PRTG Administration Tool](#)<sup>[3040]</sup>. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#)<sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#)<sup>[3067]</sup>

### 8.12.2.2 Monitoring

On the Monitoring tab, you can define global settings for scanning intervals, unusual and similar sensors detection, auto-discovery, and uptime threshold.

 This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

 If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.

In this section:

- [Scanning Intervals](#)<sup>[2870]</sup>
- [Unusual Detection](#)<sup>[2871]</sup>
- [Similar Sensors Detection](#)<sup>[2873]</sup>
- [Recommended Sensors Detection](#)<sup>[2874]</sup>
- [Auto-Discovery](#)<sup>[2875]</sup>
- [Experimental Features](#)<sup>[2876]</sup>
- [Uptime Threshold](#)<sup>[2876]</sup>

## Scanning Intervals

☁ This option is not available in PRTG Hosted Monitor.

### Scanning Intervals

**Available Intervals** ⓘ

30s






1m

5m

10m

Scanning Intervals



Setting	Description
Available Intervals	<p>Define the scanning intervals available in the dropdown list of <a href="#">every object's settings</a><sup>[201]</sup>. In the text field, enter one value in each line. Use <b>s</b>, <b>m</b>, <b>h</b>, and <b>d</b> to define seconds, minutes, hours, and days. By default, the following scanning intervals are available:</p> <ul style="list-style-type: none"> <li>▪ 30s: 30 seconds</li> <li>▪ 1m: 60 seconds</li> <li>▪ 5m: 5 minutes</li> <li>▪ 10m: 10 minutes</li> <li>▪ 15m: 15 minutes</li> <li>▪ 30m: 30 minutes</li> <li>▪ 1h: 1 hour</li> <li>▪ 4h: 4 hours</li> <li>▪ 6h: 6 hours</li> <li>▪ 12h: 12 hours</li> <li>▪ 1d: 24 hours</li> </ul>

Setting	Description
	<p> We recommend that you do not use scanning intervals that are below <b>10</b> seconds to prevent system overload. Scanning intervals that are below 10 seconds are not officially supported. The maximum supported scanning interval is <b>10</b> days.</p> <p> PRTG might convert values that you enter to a more readable equivalent of the values. For example, if you enter <b>24h</b> (24 hours), PRTG displays this as <b>1d</b> (one day) in the dropdown list in the object settings.</p> <p> Valid values are positive integers followed by <b>s</b>, <b>m</b>, <b>h</b>, and <b>d</b>. You can also define specific points in time to indicate when PRTG executes scanning actions. Enter up to 50 concrete Coordinated Universal Time (UTC) points in time according to the formula <b>@ UTC hh:mm , hh:mm</b>. You do not need to use a space before and/or after the comma. However, PRTG always saves the entries with a space both before and after the comma.</p> <p> Your local time might be different from the UTC time.</p> <p> For more information on how to set specific points in time as a scanning time for sensors, see the Knowledge Base: <a href="#">Can I set a sensor to run at a specific time?</a></p>


## Unusual Detection

The Unusual Detection feature sets sensors to the Unusual [status](#)<sup>[181]</sup> when there are values that are not typical for the time span in which they are measured. PRTG compares the current average values to the historic monitoring results for this purpose. If the current values show a big difference to the values that are normally retrieved by a sensor, this sensor indicates this with the Unusual status.


You can define the granularity of the unusual detection, that is, how big the difference must be to cause the Unusual status. If you disable the unusual detection by setting both settings to Never, sensors never show the Unusual status.

-  You can enable and disable unusual detection for specific devices, groups, and probes in the respective [object settings](#)<sup>[455]</sup>.
-  Unusual detection requires sensor data from at least four weeks (28 to 34 days) to have enough data available for comparison. If less data is available, PRTG cannot calculate the Unusual status.


**Unusual Detection**

Show Unusual Status When  24h average is <20% or >500% of weekday average (default)

---

Show Unusual Status When  Hourly average is <20% or >500% of hour-of-day average (default)

---

Log Unusual Events   Do not log unusual events

Log and display unusual events on a sensor's Log tab

Unusual Detection

Setting	Description
Show Unusual When	<p>Define when a sensor shows the Unusual status by comparing the day of the week:</p> <ul style="list-style-type: none"> <li>▪ Never: Disable unusual detection for weekday average.</li> <li>▪ 24h average is &lt;80% or &gt;120% of weekday average: Show the Unusual status when the average of the values measured on the day before is either lower than 80% or higher than 120% than usual on the same weekday.</li> <li>▪ 24h average is &lt;50% or &gt;200% of weekday average: Show the Unusual status when the average of the values measured on the day before is either lower than 50% or higher than 200% than usual on the same weekday.</li> <li>▪ 24h average is &lt;20% or &gt;500% of weekday average (recommended): Show the Unusual status when the average of the values measured on the day before is either lower than 20% or higher than 500% than usual on the same weekday.</li> <li>▪ 24h average is &lt;10% or &gt;1,000% of weekday average: Show the Unusual status when the average of the values measured on the day before is either lower than 10% or higher than 1,000% than usual on the same weekday.</li> <li>▪ 24h average is &lt;1% or &gt;10,000% of weekday average: Show the Unusual status when the average of the values measured on the day before is either lower than 1% or higher than 10,000% than usual on the same weekday.</li> </ul> <p><b>i</b> If you enable this unusual detection, the average of the values that were measured on the day before is compared to the average of the same day of the week in previous weeks.</p> <p>For example, consider a traffic sensor that usually measures 100 MB of average traffic on a weekday. If you choose the first option, the sensor shows the Unusual status if the average from the day before is lower than 80 MB or higher than 120 MB.</p>
Show Unusual When	<p>Define when a sensor shows the Unusual status by comparing the hour of the day:</p> <ul style="list-style-type: none"> <li>▪ Never: Disable unusual detection for hour-of-day average.</li> <li>▪ Hourly average is &lt;80% or &gt;120% of hour-of-day average: Show the Unusual status when the average of the values measured in the hour before is either lower than 80% or higher than 120% than usual in this hour of this weekday.</li> <li>▪ Hourly average is &lt;50% or &gt;200% of hour-of-day average: Show the Unusual status when the average of the values measured in the hour before is either lower than 50% or higher than 200% than usual in this hour of this weekday.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Hourly average is &lt;20% or &gt;500% of hour-of-day average (recommended): Show the Unusual status when the average of the values measured in the hour before is either lower than 20% or higher than 500% than usual in this hour of this weekday.</li> <li>▪ Hourly average is &lt;10% or &gt;1,000% of hour-of-day average: Show the Unusual status when the average of the values measured in the hour before is either lower than 10% or higher than 1,000% than usual in this hour of this weekday.</li> <li>▪ Hourly average is &lt;1% or &gt;10,000% of hour-of-day average: Show the Unusual status when the average of the values measured in the hour before is either lower than 1% or higher than 10,000% than usual in this hour of this weekday.</li> </ul> <p><b>i</b> If you enable this unusual detection, the average of the values that were measured in the hour before is compared to the average of the same hour on the same day of the week in previous weeks.</p> <p>Consider a traffic sensor that usually measures 10 MB average traffic within an hour. If you choose the first option, the sensor would show the Unusual status if the average from the hour before is below 8 MB or above 12 MB.</p>
Log Unusual Events	<p>Define if you also want to record unusual events and display them on the Log tab of a sensor that shows the Unusual status:</p> <ul style="list-style-type: none"> <li>▪ Do not log unusual events</li> <li>▪ Log and display unusual events on a sensor's Log tab</li> </ul>

## Similar Sensors Detection

The Similar Sensors Detection feature enables PRTG to analyze sensor data for similarities. The detection runs in the background with low priority. The recommended setting for the analysis depth is to let PRTG automatically decide how many channels it analyzes. However, you can also override this setting.

**i** Similar sensors analysis requires sensor data from at least seven days to have enough data for comparison. If not enough data is available, PRTG does not display data in the Similar Sensors Overview or in the Similar Sensors section on a sensor's Overview tab. For more information, see section [Similar Sensors](#)<sup>[195]</sup>.

**i** When similar sensors analysis is turned off or if your PRTG installation exceeds 1,000 sensors and you select Manage automatically based on sensor count (default), PRTG does not show the Similar Sensors Overview in the [main menu bar](#)<sup>[241]</sup>.

**Similar Sensors Detection**

Analysis Depth ⓘ

- Manage automatically based on sensor count (default)
- Analyze only primary channels
- Analyze all channels (higher CPU load)
- Disable detection of similar sensors

Similar Sensors Detection

Setting	Description
Analysis Depth	<p>Define the number of channels that PRTG analyzes to detect similarities between sensors, or disable the analysis. The analysis depth depends on the total number of sensors you have:</p> <ul style="list-style-type: none"> <li>▪ <b>Manage automatically based on sensor count (default):</b> Analyze all channels for up to 500 sensors and only the primary channels for up to 1,000 sensors. For more than 1,000 sensors, PRTG disables the analysis. <ul style="list-style-type: none"> <li>☑ This is the default setting in PRTG Network Monitor.</li> </ul> </li> <li>▪ <b>Analyze only primary channels:</b> Only analyze the primary channels. <ul style="list-style-type: none"> <li>ⓘ Be aware of potentially high CPU load on the PRTG core server system if your PRTG installation has more than 1,000 sensors.</li> </ul> </li> <li>▪ <b>Analyze all channels (higher CPU load):</b> Analyze all channels. <ul style="list-style-type: none"> <li>ⓘ Be aware of potentially high CPU load on the PRTG core server system if your PRTG installation has more than 500 sensors.</li> </ul> </li> <li>▪ <b>Disable detection of similar sensors:</b> Do not detect similarities. Select this option if you are not interested in the analysis results or if you want to keep the CPU load on the PRTG core server system to a minimum. <ul style="list-style-type: none"> <li>☁ This is the default setting in PRTG Hosted Monitor.</li> </ul> </li> </ul>

## Recommended Sensors Detection

The Recommended Sensors Detection feature enables PRTG to analyze devices in your network and to suggest sensors that are missing for a complete monitoring setup. The analysis runs with low priority in the background when you add a new device, when the last analysis was executed more than 30 days ago, or when you [manually start](#)<sup>[198]</sup> it.

■ See section [Recommended Sensors](#)<sup>[197]</sup> for more information, for example, on [SNMP settings](#)<sup>[198]</sup>, on the [results](#)<sup>[198]</sup> you get and on how to [add the suggested sensors](#)<sup>[199]</sup>.

☁ This option is not available in PRTG Hosted Monitor.

**Recommended Sensors Detection**

Detection Handling ⓘ

- Manage automatically based on sensor count (default)
- Always show recommended sensors
- Disable sensor recommendation

Recommended Sensors Detection



Setting	Description
Detection Handling	<p>Define if you want PRTG to analyze your devices and to recommend useful sensors:</p> <ul style="list-style-type: none"> <li>Manage automatically based on sensor count (default): Run the detection engine for installations with up to 5,000 sensors. If you exceed this threshold, PRTG disables the detection engine for performance reasons. <ul style="list-style-type: none"> <li><b>i</b> We recommend that you select this option so that you do not miss any important monitoring data about your network, without risking running into performance issues.</li> </ul> </li> <li>Always show recommended sensors: Always analyze your devices even if your installation exceeds 5,000 sensors and if you never want to miss any suggestion to complete your monitoring. <ul style="list-style-type: none"> <li><b>i</b> If you select this option, keep it in mind in case you encounter performance issues.</li> </ul> </li> <li>Disable sensor recommendations: Never recommend sensors. Select this option if you have performance issues with PRTG or if you do not want to see this information on devices' Overview tabs. Moreover, you do not see the option Recommend Now in <a href="#">device context menus</a><sup>[229]</sup> or on Overview tabs anymore.</li> </ul> <p><b>■</b> For more information about the Overview tab, see the Knowledge Base: <a href="#">What options do I have to review my monitoring data in detail?</a></p>

## Auto-Discovery

Auto-Discovery

Run Auto-Discovery At 04:00

Auto-Discovery

Setting	Description
Run Auto-Discovery At	<p>Define the time when PRTG automatically runs an <a href="#">auto-discovery</a><sup>[254]</sup> in your network if you configured a daily or weekly schedule in the <a href="#">auto-discovery group settings</a><sup>[267]</sup>. Select a full hour.</p> <ul style="list-style-type: none"> <li>00:00 - 23:00</li> </ul> <p><b>i</b> We recommend that you choose a time when there is little user activity in your network because auto-discoveries can produce a certain amount of load.</p>

## Experimental Features

**Experimental Features**

You can enable or disable experimental features here. Do not expect that all functions work properly, or that experimental features work as expected at all. Be aware that experimental features can be removed from PRTG at any time.

Beta Sensors ⓘ

Disable (default)

Enable

PowerShell Security Enhancement ⓘ

Enable (default)

Disable

Experimental Features

**i** The operating methods of the experimental features might change at any time. Do not expect that all functions work properly, or that the experimental features work as expected at all. Be aware that Paessler might remove these features at any time.

Setting	Description
Beta Sensors	<p>Select if you want to enable or disable sensors in beta status:</p> <ul style="list-style-type: none"> <li>▪ <b>Disable (default):</b> Disable sensors in beta status.</li> <li>▪ <b>Enable:</b> Enable sensors in beta status. <ul style="list-style-type: none"> <li><b>i</b> Beta sensors then become available in the <a href="#">Add Sensor</a> dialog.</li> <li><b>i</b> If you disable beta sensors, existing beta sensors change to the Unknown status.</li> </ul> </li> </ul>
PowerShell Security Enhancement	<p>Select if you want to improve PowerShell security by hiding command-line parameters in the process explorer and the event log:</p> <ul style="list-style-type: none"> <li>▪ <b>Enable (default):</b> Enable PowerShell security enhancement. <ul style="list-style-type: none"> <li><b>i</b> If you enable PowerShell Security Enhancement, PowerShell scripts that use the <a href="#">write-host</a> cmdlet to provide their output to PRTG do not work anymore. Custom scripts only work if you use the <a href="#">write-output</a> cmdlet.</li> <li><b>i</b> Enabling this feature can also improve the performance of PowerShell sensors.</li> </ul> </li> <li>▪ <b>Disable:</b> Disable PowerShell security enhancement.</li> </ul>

## Uptime Threshold

**Uptime Threshold**

Minimum Uptime ⓘ 99.99 %

Uptime Threshold

Setting	Description
Minimum Uptime	<p>Define which uptime in percent PRTG regards as 100 percent. This setting affects the colors that you see next to sensor icons in reports.</p> <ul style="list-style-type: none"> <li>▪ 90 % - 99.999 %</li> </ul>

**i** Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

## More

### ■ KNOWLEDGE BASE

How can I speed up PRTG—especially for large installations?

- <https://kb.paessler.com/en/topic/2733>

Can I set a sensor to run at a specific time?

- <https://kb.paessler.com/en/topic/3723>

## Others


There are some settings that you must define in the [PRTG Administration Tool](#)<sup>[3040]</sup>. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#)<sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#)<sup>[3067]</sup>

### 8.12.2.3 Notification Delivery

On the Notification Delivery tab, you can define and test global settings for notification delivery. If you do not want to use a specific notification method, leave the respective fields empty.

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

 If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.

In this section:

- [Note](#)<sup>[2878]</sup>
- [SMTP Delivery](#)<sup>[2878]</sup>
- [SMS Delivery](#)<sup>[2883]</sup>

## Note

You must take the following four steps to set up and use notifications:

1. Check and set up the [notification delivery](#) settings if you use PRTG Network Monitor. These settings define how PRTG sends messages.
2. Check and set up [notification contacts](#) for the user accounts. These contacts define the recipients to which PRTG sends notifications.
3. Check and set up several [notification templates](#). These templates define the notification methods and their content.
  - ⓘ You can also check or edit notification templates via the Notification Triggers tab. For more information, see section [Notification Triggers Settings](#).
4. Check and set up [notification triggers settings](#) for objects. These triggers define when PRTG sends notifications.

ⓘ Usually, there are three successive attempts to deliver a notification. If all of these attempts fail, the notification is lost. To never miss a notification, we recommend that you always set up at least two notifications with different notification methods for a notification trigger, for example, one email notification and one SMS notification. If delivery via email fails, PRTG can still notify you via smartphone as a fallback. For example, use the latency setting of a [state trigger](#) to choose a notification with a different notification method than in the first trigger condition, or set up a second trigger with a different notification method for the corresponding object.

■ For a detailed step-by-step guide, see the Paessler website: [How to set up notifications via the PRTG web interface](#).

■ Custom notification scripts are also available in the [PRTG Sensor Hub](#).

## SMTP Delivery

**SMTP Delivery**

Delivery Mechanism ⓘ

Use direct delivery with the built-in email server (default)

Use one SMTP relay server (recommended in LANs/NATs)

Use two SMTP relay servers (primary and fallback server)

Sender Email Address ⓘ johnqpublic@example.com

Sender Name ⓘ PRTG Network Monitor

HELO Ident ⓘ Example

Test SMTP Settings Test SMTP Settings

SMTP Delivery

Setting	Description
Delivery Mechanism	Define how PRTG sends emails via the Simple Mail Transfer Protocol (SMTP):

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Use direct delivery with the built-in email server (default): Use the built-in SMTP relay server. This server manages its own email queue. For each email, it looks up the target SMTP server via the MX record of the target domain, and sends the email.</li> <li>▪ Use one SMTP relay server (recommended in LANs/NATs): Set up your own SMTP relay server to send emails. Enter data below.</li> <li>▪ Use two SMTP relay servers (primary and fallback server): Set up two SMTP relay servers with one as the primary relay server and one as the fallback relay server. Enter data below.</li> </ul> <p><b>i</b> If you monitor the IT infrastructure in your network address translation (NAT) or LAN, use your own LAN-based relay server to ensure faster delivery of notification emails.</p> <p><b>☁</b> This option is not available in PRTG Hosted Monitor. PRTG Hosted Monitor uses sendgrid for email notifications. For more information, see the Paessler website: <a href="#">FAQ – PRTG Hosted Monitor</a>.</p>
Sender Email Address	<p>Enter an email address to use as the sender of all email notifications. This setting is global and applies to all email notifications by default.</p> <p><b>i</b> You can override the sender email in the settings of individual <a href="#">notification templates</a> <small>28151</small>.</p>
Sender Name	<p>Enter a name to use as the sender of all email notifications. This setting is global and applies to all email notifications by default.</p> <p><b>i</b> You can override the sender name in the settings of individual notification templates.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
HELO Ident	<p>Enter a server name for the HELO part of the mail protocol.</p> <p><b>i</b> For some mail servers, the HELO identifier must be the valid principal host domain name for the client host. For more information, see <a href="#">SMTP RFC 2821</a>.</p> <p><b>i</b> The HELO identifier must be a unique name.</p> <p><b>i</b> Only ASCII characters are allowed.</p> <p><b>i</b> We recommend that you use the Domain Name System (DNS) name of the PRTG core server system.</p> <p><b>☁</b> This option is not available in PRTG Hosted Monitor.</p>

Setting	Description
SMTP Relay Server	<p><b>This setting is only visible if you select</b> Use one SMTP relay server (recommended in LANs/NATs) <b>or</b> Use two SMTP relay servers (primary and fallback server) <a href="#">above</a>.</p> <p>Enter the IP address or DNS name of the SMTP relay server.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
SMTP Relay Port	<p><b>This setting is only visible if you select</b> Use one SMTP relay server (recommended in LANs/NATs) <b>or</b> Use two SMTP relay servers (primary and fallback server) <a href="#">above</a>.</p> <p>Enter the port for the connection to the SMTP server. The default port is <a href="#">25</a>.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
SMTP Relay Authentication	<p><b>This setting is only visible if you select</b> Use one SMTP relay server (recommended in LANs/NATs) <b>or</b> Use two SMTP relay servers (primary and fallback server) <a href="#">above</a>.</p> <p>Select the kind of authentication that the SMTP server requires:</p> <ul style="list-style-type: none"> <li>▪ Use no authentication (default): Use SMTP without authentication.</li> <li>▪ Use standard SMTP authentication: Use standard authentication.</li> <li>▪ Use SASL authentication: Use secure authentication via Simple Authentication and Security Layer (SASL).</li> </ul> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
SMTP Relay User Name	<p><b>This setting is only visible if you select</b> Use standard SMTP authentication <b>or</b> Use SASL authentication <a href="#">above</a>.</p> <p>Enter a valid user name.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
SMTP Relay Password	<p><b>This setting is only visible if you select</b> Use standard SMTP authentication <b>or</b> Use SASL authentication <a href="#">above</a>.</p> <p>Enter a valid password.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>

Setting	Description
<p>Connection Security</p>	<p><b>This setting is only visible if you select</b> Use one SMTP relay server (recommended in LANs/NATs) <b>or</b> Use two SMTP relay servers (primary and fallback server) <b>above</b>.</p> <p>Define the connection security for SMTP connections:</p> <ul style="list-style-type: none"> <li>▪ Use SSL/TLS if the server supports it (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ Do not use connection security: Use an unsecure connection with plain text transfer.</li> </ul> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
<p>SSL/TLS Method</p>	<p><b>This setting is only visible if you select</b> Use one SMTP relay server (recommended in LANs/NATs) <b>and</b> Use SSL/TLS if the server supports it (default) <b>above</b>.</p> <p>Select the SSL or TLS version that the SMTP server supports:</p> <ul style="list-style-type: none"> <li>▪ Auto-Negotiate (TLS 1.0 or higher)</li> <li>▪ SSLv3</li> <li>▪ TLS 1.0</li> <li>▪ TLS 1.1</li> <li>▪ TLS 1.2</li> <li>▪ TLS 1.3</li> </ul> <p>ⓘ If you select Auto-Negotiate (TLS 1.0 or higher), PRTG uses the highest available TLS level supported by the SMTP endpoint.</p> <p>ⓘ This is only relevant for secure connections. If you do not get a connection, try a different setting.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
<p>SMTP Relay Server (Fallback)</p>	<p><b>This setting is only visible if you select</b> Use two SMTP relay servers (primary and fallback server) <b>above</b>.</p> <p>Enter the IP address or DNS name of the fallback SMTP relay server.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
<p>SMTP Relay Port (Fallback)</p>	<p><b>This setting is only visible if you select</b> Use two SMTP relay servers (primary and fallback server) <b>above</b>.</p>

Setting	Description
	<p>Enter the port for the connection to the fallback SMTP server. The default port is <a href="#">25</a>.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
<p>SMTP Relay Authentication (Fallback)</p>	<p><a href="#">This setting is only visible if you select Use two SMTP relay servers (primary and fallback server) above.</a></p> <p>Select the kind of authentication that the fallback SMTP server requires:</p> <ul style="list-style-type: none"> <li>▪ Use no authentication (default): Use SMTP without authentication.</li> <li>▪ Use standard SMTP authentication: Use standard authentication.</li> <li>▪ Use SASL authentication: Use secure authentication via Simple Authentication and Security Layer (SASL).</li> </ul> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
<p>SMTP Relay User Name (Fallback)</p>	<p><a href="#">This setting is only visible if you select Use two SMTP relay servers (primary and fallback server) and Use standard SMTP authentication or Use SASL authentication above.</a></p> <p>Enter a valid user name.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
<p>SMTP Relay Password (Fallback)</p>	<p><a href="#">This setting is only visible if you select Use two SMTP relay servers (primary and fallback server) and Use standard SMTP authentication or Use SASL authentication above.</a></p> <p>Enter a valid password.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
<p>Connection Security (Fallback)</p>	<p><a href="#">This setting is only visible if you select Use two SMTP relay servers (primary and fallback server) above.</a></p> <p>Define the connection security for SMTP connections:</p> <ul style="list-style-type: none"> <li>▪ Use SSL/TLS if the server supports it (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection.</li> <li>▪ Do not use connection security: Use an unsecure connection with plain text transfer.</li> </ul>



Setting	Description
	☁ This option is not available in PRTG Hosted Monitor.
SSL/TLS Method (Fallback)	<p>This setting is only visible if you select Use two SMTP relay servers (primary and fallback server) and Use SSL/TLS if the server supports it (default) above.</p> <p>Select the SSL or TLS version that the SMTP server supports:</p> <ul style="list-style-type: none"> <li>▪ Auto-Negotiate (TLS 1.0 or higher)</li> <li>▪ SSLv3</li> <li>▪ TLS 1.0</li> <li>▪ TLS 1.1</li> <li>▪ TLS 1.2</li> <li>▪ TLS 1.3</li> </ul> <p>ⓘ If you select Auto-Negotiate (TLS 1.0 or higher), PRTG uses the highest available TLS level supported by the SMTP endpoint.</p> <p>ⓘ This is only relevant for secure connections. If you do not get a connection, try a different setting.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
Test SMTP Settings	<p>Click Test SMTP Settings to test your SMTP notification delivery configuration.</p> <ul style="list-style-type: none"> <li>▪ Email Address: Enter an email address to send the test email notification to.</li> <li>▪ Subject: Enter a subject for the test email notification.</li> </ul>

## SMS Delivery

- ⓘ Your PRTG Network Monitor license or PRTG Hosted Monitor subscription does not include the cost for SMS delivery. Refer to the pricing information of the service provider that you plan to use to find out more about their pricing.
- ⓘ Although PRTG has built-in support for the application programming interface (API) of some SMS providers, we cannot officially provide support for them. If you have technical questions about SMS delivery beyond PRTG, contact your SMS provider directly.
- ⓘ Instead of using a preconfigured provider, you can use a custom URL that enables you to use extended parameters. This is also an alternative to using providers for which we offer preconfigured options.

**i** You need an internet connection to send text messages via the HTTP API.

**■** For information about sending SMS via separate hardware using third-party software, see the Knowledge Base: [How can I send SMS text message notifications via a modem or a mobile phone with PRTG?](#)

**SMS Delivery**

Configuration Mode **i**

Disable SMS delivery (default)  
 Select an SMS provider from a list of providers  
 Enter a custom URL for a provider not listed

SMS Delivery

Setting	Description
Configuration Mode	Define a mode for the SMS delivery configuration: <ul style="list-style-type: none"> <li>▪ Disable SMS delivery (default): Do not use SMS delivery.</li> <li>▪ Select an SMS provider from a list of providers: Select a provider from a list below.</li> <li>▪ Enter a custom URL for a provider not listed: Use a different provider and manually enter the custom URL below.</li> </ul>
Service Provider	<p><b>This setting is only visible if you select</b> Select an SMS provider from a list of providers <b>above</b>.</p> <p>Select a service provider from the list:</p> <ul style="list-style-type: none"> <li>▪ BulkSMS All regions (except South Africa): Enter a User Name and Password below.               <ul style="list-style-type: none"> <li>▫ URL: <code>https://www.bulksms.co.uk:443/eapi/submission/send_sms/2/2.0</code></li> <li>▫ Port: 443</li> </ul> </li> <li>▪ BulkSMS South Africa: Enter a User Name and Password below.               <ul style="list-style-type: none"> <li>▫ URL: <code>https://bulksms.2way.co.za:443/eapi/submission/send_sms/2/2.0</code></li> <li>▫ Port: 443</li> </ul> </li> <li>▪ Agile Telecom: Enter a User Name and Password below.               <ul style="list-style-type: none"> <li>▫ URL: <code>http://agiletelecom.com/sms hurricane3.0.asp</code></li> <li>▫ Port: 80</li> </ul> </li> <li>▪ Esendex: Enter a User Name, Password, and Account below.               <ul style="list-style-type: none"> <li>▫ URL: <code>https://www.esendex.com/secure/messenger/formpost/SendSMS.aspx</code></li> </ul> </li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▫ Port: 443</li> </ul> <p><b>i</b> Some providers might require a port configuration in your firewall. Use the respective port from the list above.</p>
User Name	<p><b>This setting is only visible if you select</b> Select an SMS provider from a list of providers <a href="#">above</a>.</p> <p>Enter a user name for the service provider account.</p>
Password	<p><b>This setting is only visible if you select</b> Select an SMS provider from a list of providers <a href="#">above</a>.</p> <p>Enter a password for the service provider account.</p>
Account	<p><b>This setting is only visible if you select</b> Select an SMS provider from a list of providers <a href="#">and Esendex above</a>.</p> <p>Enter the account number or the API ID to connect your account if your provider asks you to register, for example <a href="#">EX0000000</a>. Enter a string or leave the field empty.</p>
Custom URL	<p><b>This setting is only visible if you select</b> Enter a custom URL for a provider not listed <a href="#">above</a>.</p> <p>From the documentation of your SMS provider, enter the service URL that it uses to send SMS messages.</p> <p>Use the following placeholders for the recipient phone number and the text message:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">%SMSNUMBER</a></li> <li>▪ <a href="#">%SMSTEXT</a></li> </ul> <p><b>i</b> Use the <a href="#">GET</a> method to request the custom URL. <a href="#">POST</a> requests are not supported.</p>
HTTP Authentication	<p><b>This setting is only visible if you select</b> Enter a custom URL for a provider not listed <a href="#">above</a>.</p> <p>Select if PRTG uses HTTP basic authentication when it calls the custom URL of the SMS provider:</p> <ul style="list-style-type: none"> <li>▪ Do not use HTTP basic authentication (default)</li> <li>▪ Use HTTP basic authentication</li> </ul> <p><b>i</b> HTTP basic authentication is necessary if the custom URL looks like this <a href="#">https://[username]:[password]@my.custom.sms.provider/</a>.</p>

Setting	Description
Custom SNI	<p><b>This setting is only visible if you select</b> Enter a custom URL for a provider not listed <a href="#">above</a>.</p> <p>Define if PRTG sends the Server Name Indication (SNI) extension to the Transport Layer Security (TLS) protocol along with the HTTP request:</p> <ul style="list-style-type: none"> <li>▪ Do not send SNI (default): PRTG does not send the SNI when it executes the HTTP action.</li> <li>▪ Send SNI: PRTG sends the SNI when it calls the target URL. Specify the SNI below.</li> </ul>
Encoding for SMS	<p><b>This setting is only visible if you select</b> Enter a custom URL for a provider not listed <a href="#">above</a>.</p> <p>Define the encoding of the URL string that PRTG sends to the SMS provider:</p> <ul style="list-style-type: none"> <li>▪ ANSI local system code page (default)</li> <li>▪ UTF-8</li> <li>▪ UTF-16</li> </ul>
Virtual Host (SNI)	Enter the SNI name that the endpoint configuration requires. Usually, this is the fully qualified domain name (FQDN) of the virtual host.
Maximum Length of Text	<p>Some SMS providers do not allow SMS messages that exceed a certain amount of characters. PRTG restricts the number of characters according to the length specified in this field. A value of 0 means that PRTG sends the entire SMS.</p> <p><b>i</b> The use of some special characters, especially ones that are not in the GSM-7 alphabet, might cause the message to be cut off after 70 characters and the special characters might not display properly. The exact results depend on which SMS provider you use.</p>
Test SMS Settings	<p>Click Test SMS Settings to test your SMS notification delivery configuration.</p> <ul style="list-style-type: none"> <li>▪ Number: Enter a phone number to send the test SMS notification to.</li> <li>▪ Message: Enter a message for the test SMS notification.</li> </ul>

**i** The notification methods Send SMS/Pager Message and Execute HTTP Action use the central proxy settings of the PRTG core server. For more information, see section [Core & Probes](#) <sup>2888</sup> (section Proxy Configuration).

**i** Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How can I send SMS text message notifications via a modem or a mobile phone with PRTG?

- <https://kb.paessler.com/en/topic/393>

Which URLs does PRTG use for its preconfigured SMS providers?

- <https://kb.paessler.com/en/topic/13123>

Why do I get a connection timeout message when sending SMS via bulksms?

- <https://kb.paessler.com/en/topic/12253>

Can Gmail / Google Apps / G-Suite be used for SMTP relay?

- <https://kb.paessler.com/en/topic/2823>

How can I enable notification delivery logging?

- <https://kb.paessler.com/en/topic/55363>

Can I use Microsoft Office 365 as SMTP relay server for PRTG email delivery?

- <https://kb.paessler.com/en/topic/75534>

### ■ PAESSLER WEBSITE

FAQ – PRTG Hosted Monitor


- <https://www.paessler.com/prtg/prtg-hosted-monitor/faq>


You can find custom notification scripts in the PRTG Sensor Hub

- <https://www.paessler.com/sensor-hub>

## 8.12.2.4 Core & Probes

On the Core & Probes tab, you can define settings for the PRTG core server as well as for probe connections if you use remote probes or mini probes.

 If you cannot save changes to Core & Probes settings because you get an **Error (Bad Request)** with the message **Active Directory Domain not accessible**, make sure that you provide the correct access type for your domain in section **Active Directory Integration**<sup>28971</sup>. For example, change Use the PRTG core server service account (usually Local System) (default) to Use explicit credentials and provide correct credentials for the domain. PRTG automatically sets the access type to Use the PRTG core server service account (usually Local System) (default) by default, so you might need to change this.

 If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

In this section:

- [Proxy Configuration](#) <sup>2888</sup>
- [Probe Connection Settings](#) <sup>2890</sup>
- [Multi-Platform Probe Connection Settings](#) <sup>2895</sup>
- [Active Directory Integration](#) <sup>2897</sup>
- [Historic Data Purging](#) <sup>2899</sup>

## Proxy Configuration

 This option is not available in PRTG Hosted Monitor.

### Proxy Configuration

Proxy Server Handling **i**

Do not use a proxy server (default)

Use a proxy server

Proxy Configuration

Setting	Description
Proxy Server Handling	<p>Define if you want to use PRTG with a direct internet connection or if a proxy is necessary:</p> <ul style="list-style-type: none"> <li>▪ Do not use a proxy server (default): Do not use a proxy. Use this setting if a direct internet connection to the PRTG core server system is available.</li> <li>▪ Use a proxy server: Define proxy settings below. Use this setting if a proxy is mandatory in your network.</li> </ul> <p><b>i</b> We recommend that you use PRTG with a direct internet connection.</p> <p><b>i</b> The proxy settings are valid for <a href="#">auto-update</a> <sup>2969</sup>, <a href="#">activating the product</a> <sup>104</sup>, obtaining <a href="#">Geo Maps</a> <sup>2731</sup> tiles, and for sending HTTP, push, and SMS text message <a href="#">notifications</a> <sup>2815</sup>.</p>
Server	<p><b>This setting is only visible if you select Use a proxy server above</b></p> <p>Enter the address of the proxy server that you use for outbound connections. Enter a valid address.</p>
Port	<p><b>This setting is only visible if you select Use a proxy server above</b></p> <p>Enter the port number of the proxy server that you use for outbound connections. Enter an integer.</p>

Setting	Description
Proxy Authentication	<p><a href="#">This setting is only visible if you select Use a proxy server above</a></p> <p>Determine whether the proxy server needs credentials or not:</p> <ul style="list-style-type: none"><li>▪ Do not use authentication: Do not use credentials for proxy connections.</li><li>▪ User name and password: Define credentials (user name and password) below. Use this setting if the proxy server requires credentials.</li></ul>
User Name	<p><a href="#">This setting is only visible if you select User name and password above.</a></p> <p>Enter a user name for proxy authentication. Enter a string.</p>
Password	<p><a href="#">This setting is only visible if you select User name and password above.</a></p> <p>Enter a password for proxy authentication. Enter a string.</p>

## Probe Connection Settings

**Probe Connection Settings**

**Probe Connection IP Addresses** ⓘ

Local probe only, 127.0.0.1

All IP addresses available on this computer

Specify IP addresses

**Access Keys** ⓘ

**Allow IP Addresses** ⓘ

**Deny IP Addresses** ⓘ

**Deny GIDs** ⓘ

**Connection Security** ⓘ

High security (TLS 1.3, TLS 1.2)

Default security (TLS 1.3, TLS 1.2) (recommended)

Weakened security (TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0)

**Mini Probes** ⓘ

Do not allow mini probes (default)

Allow mini probes to connect to the PRTG web server


Allow mini probes to connect to an extra port

**PRTG MultiBoard File Transfer** ⓘ

Disable (default)

Enable

Probe Connection Settings






Setting	Description
Probe Connection IP Addresses	<p>Define how the PRTG core server handles incoming connections from probes:</p> <ul style="list-style-type: none"> <li>Local probe only, 127.0.0.1: Only accept local probe connections. The PRTG core server does not allow the use of <a href="#">remote probes</a> [3196].</li> </ul> <p> This is the default setting in PRTG Network Monitor.</p>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ All IP addresses available on this computer: Accept incoming connections from remote probes, no matter on which IP address of the PRTG core server they come in.               <ul style="list-style-type: none"> <li>☁ This is the default setting in PRTG Hosted Monitor.                   <ul style="list-style-type: none"> <li>▪ Specify IP addresses: Accept incoming connections from remote probes only on the selected IP address(es) of the PRTG core server. In the list, select the IP addresses by enabling a check box in front of the desired IP addresses.</li> </ul> </li> </ul> </li> <li>ⓘ You can also change this setting in the <a href="#">PRTG Administration Tool on PRTG Core Server Systems</a><sup>[6046]</sup>.</li> <li>ⓘ If you change this setting, PRTG needs to restart the PRTG core server to apply your changes. After you click Save, a dialog box appears that asks you to confirm the restart. Click OK to trigger the restart. During the restart, all users of the PRTG web interface, the <a href="#">PRTG app for desktop</a><sup>[2984]</sup>, or the <a href="#">PRTG Apps for Mobile Network Monitoring</a><sup>[2988]</sup> are disconnected and reconnected.</li> <li>☁ This option is not available in PRTG Hosted Monitor.</li> </ul>
Access Keys	<p>Enter a list of access keys for remote probe connections. Enter one access key per line.</p> <ul style="list-style-type: none"> <li>ⓘ Every remote probe and multi-platform probe that wants to connect to this PRTG installation has to use one of these keys.</li> <li>■ For more information on how to set an access key for a remote probe, see section <a href="#">PRTG Administration Tool</a><sup>[3067]</sup>.</li> </ul>
Allow IP Addresses	<p>Enter a list of remote probe IP addresses or Domain Name System (DNS) names that you want to allow to connect to the PRTG core server. Enter one IP address or DNS name per line. The following options are also possible:</p> <ul style="list-style-type: none"> <li>▪ [Empty]: An empty field does not allow any remote probes (only the local probe). Enter IP addresses or DNS names to allow remote probe connections.           <ul style="list-style-type: none"> <li>ⓘ We recommend that you use IP addresses instead of DNS names because DNS name resolution might be cached.</li> </ul> </li> <li>▪ any: Enter the word any to automatically allow all remote probe connections.           <ul style="list-style-type: none"> <li>☁ This is the default setting in PRTG Hosted Monitor.               <ul style="list-style-type: none"> <li>ⓘ We recommend that you only use this option in intranets in PRTG Network Monitor, not in PRTG Hosted Monitor.</li> </ul> </li> </ul> </li> <li>ⓘ PRTG always automatically allows the local probe (127.0.0.1). PRTG checks the list of allowed IP addresses before it checks the list of denied IP addresses.</li> </ul>

Setting	Description
	<p><b>i</b> If the IP address of a remote probe regularly changes (for example, because of an internet provider that dynamically assigns IP addresses), enter the potential IP address range for the remote probe or use any.</p> <p><b>■</b> You can use the PRTG syntax for IP address ranges. For more information, see section <a href="#">Define IP Address Ranges</a><sup>[180]</sup>.</p>
Deny IP Addresses	<p>Enter a list of remote probe IP addresses or DNS names that you do <b>not</b> want to allow to connect to the PRTG core server. Enter one IP address or DNS name per line.</p> <p><b>i</b> You can use Deny IP Addresses to explicitly deny connections from remote probes that you do not want to include in your setup either at all or for a certain time. You can also use it to allow access to an IP address range under Allow IP Addresses, but to deny access to a single IP address from the IP address range.</p> <p><b>■</b> You can use the PRTG syntax for IP address ranges. For more information, see section <a href="#">Define IP Address Ranges</a><sup>[180]</sup>.</p> <p><b>i</b> If you deny the IP address or DNS name of a remote probe, you must restart the PRTG core server to apply your changes.</p> <p><b>i</b> We recommend that you use IP addresses rather than DNS names because DNS name resolution might be cached.</p>
Deny GIDs	<p>Enter a list of global IDs (GID) Enter one GID per line. PRTG denies access to matching GIDs.</p> <p><b>i</b> If you remove a remote probe from the device tree or if you deny a remote probe after installation, PRTG automatically adds its GID to this list. The remote probe is no longer able to connect. Denying GIDs is more precise than denying IP addresses, where other remote probes at the same location could also be excluded.</p> <p><b>i</b> A GID is the ID that PRTG attributes to every probe that you include in your monitoring.</p>
Connection Security	<p>Specify the security level that the PRTG web server accepts for connections to and from the PRTG core server:</p> <ul style="list-style-type: none"> <li>▪ High security (TLS 1.3, TLS 1.2): Only accept high security connections from probes.</li> <li>▪ Default security (TLS 1.3, TLS 1.2) (recommended): Only accept high security connections from probes.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Weakened security (TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0): Additionally accept TLS 1.1-secured and TLS 1.0-secured connections from probes.               <ul style="list-style-type: none"> <li>❗ If you have probes that do not support TLS 1.3-secured or TLS 1.2-secured connections because you updated from an older PRTG version, you can use this setting to connect to and to <a href="#">update</a> older probes. After the update, we recommend that you change this setting to High security (TLS 1.3, TLS 1.2) or Default security (TLS 1.3, TLS 1.2) (recommended).</li> </ul> </li> <li>❗ If you set a registry key in previous PRTG versions to override the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) version and cipher suites of PRTG web server connections or probe connections, High security (TLS 1.3, TLS 1.2) overrides the registry setting and only TLS 1.3 and TLS 1.2 are allowed. If you select Default security (TLS 1.3, TLS 1.2) (recommended), the <a href="#">registry value overrides this setting</a> and the connection security that you defined in the registry applies.</li> <li>❗ If you change this setting, PRTG needs to restart the PRTG core server to apply your changes. After you click Save, a dialog box appears that asks you to confirm the restart. Click OK to trigger the restart. During the restart, all users of the PRTG web interface, the <a href="#">PRTG app for desktop</a>, or the <a href="#">PRTG Apps for Mobile Network Monitoring</a> are disconnected and reconnected.</li> </ul> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
Mini Probes	<p>Define if you want to allow mini probe connections to the PRTG core server:</p> <ul style="list-style-type: none"> <li>▪ Do not allow mini probes: Mini probes cannot connect to the PRTG web server. You are not able to monitor with mini probes if you choose this option.</li> <li>▪ Allow mini probes to connect to the PRTG web server: Mini probes can connect to the PRTG web server and use the <a href="#">defined TCP port for the web server</a> for this purpose. The default port for secure connections is 443.</li> <li>▪ Allow mini probes to connect to an extra port: Mini probes can connect to the PRTG web server via a specific port. Use this if you do not want the whole PRTG web server to be reachable from other networks all the time only because of mini probes.               <ul style="list-style-type: none"> <li>❗ SSL/TLS must be enabled on the mini probe port.</li> </ul> </li> <li>❗ If you want to use mini probes, you need to configure the PRTG web server to accept connections from mini probes and select Secure HTTPS server (port 443, recommended, mandatory for internet access) in the <a href="#">PRTG web server settings</a>.</li> </ul> <p>■ For more information, see section <a href="#">Mini Probe API</a>. See also the Knowledge Base: <a href="#">Where can I find PRTG mini probes which are ready to use?</a></p>

Setting	Description
	<p> If you change this setting, PRTG needs to restart the PRTG core server to apply your changes. After you click Save, a dialog box appears that asks you to confirm the restart. Click OK to trigger the restart. During the restart, all users of the PRTG web interface, the <a href="#">PRTG app for desktop</a><sup>[2984]</sup>, or the <a href="#">PRTG Apps for Mobile Network Monitoring</a><sup>[2988]</sup> are disconnected and reconnected.</p> <p> This option is not available in PRTG Hosted Monitor.</p>
Mini Probe Port	<p><b>This setting is only visible if you select</b> Allow mini probes to connect to an extra port <a href="#">above</a>.</p> <p>Enter the number of the port for mini probe connections. Make sure that SSL is available on this port.</p> <p> If you change this setting, PRTG needs to restart the PRTG core server to apply your changes. After you click Save, a dialog box appears that asks you to confirm the restart. Click OK to trigger the restart. During the restart, all users of the PRTG web interface, the <a href="#">PRTG app for desktop</a><sup>[2984]</sup>, or the <a href="#">PRTG Apps for Mobile Network Monitoring</a><sup>[2988]</sup> are disconnected and reconnected.</p> <p> This option is not available in PRTG Hosted Monitor.</p>
PRTG MultiBoard File Transfer	<p>Select if you want to allow PRTG MultiBoard to access the PRTG data directories and PRTG program directories of the PRTG core servers connected to PRTG MultiBoard:</p> <ul style="list-style-type: none"> <li>▪ <b>Disable (default):</b> Do not allow PRTG MultiBoard to access, configure, and transfer PRTG files. You will not be able to use the Probe Transfer, Configuration Viewer, and Template Transfer features.</li> <li>▪ <b>Enable:</b> Allow PRTG MultiBoard to access, configure, and transfer PRTG files.</li> </ul> <p> PRTG MultiBoard requires access to the <a href="#">PRTG Configuration.dat</a> file for the Probe Transfer and Configuration Viewer features.</p>

## Multi-Platform Probe Connection Settings

### Multi-Platform Probe Connection Settings

**Multi-Platform Probe Connections** ⓘ

Do not allow multi-platform probe connections (default)

Allow multi-platform probe connections

**NATS Connection Security** ⓘ

TLS (default)

Unsecure (not recommended)

**NATS Server Host** ⓘ

localhost:23561

**NATS User Name** ⓘ

**NATS Password** ⓘ

**NATS Server Certificate Authority Handling** ⓘ

Use system certificate store (default)

Specify a certificate authority certificate file

**Connection Log Level** ⓘ

Info (default)

Multi-Platform Probe Connection Settings

Setting	Description
Multi-Platform Probe Connections	<p>Define if you want to allow multi-platform probe connections to the PRTG core server:</p> <ul style="list-style-type: none"> <li>▪ Do not allow multi-platform probe connections (default): Multi-platform probes cannot connect to the PRTG core server. You are not able to monitor with multi-platform probes if you select this option.</li> <li>▪ Allow multi-platform probe connections: Allow multi-platform probes to connect to the PRTG core server. PRTG automatically creates a <a href="#">Multi-Platform Probe Connection Health (Autonomous) sensor</a> on your PRTG core server.</li> </ul> <p> ⓘ Multi-platform probes connect to the PRTG core server via a NATS server.</p> <p> ■ For more information, see the <a href="#">Multi-Platform Probe for PRTG</a> manual.</p> <p> ⓘ If you change this setting, PRTG needs to restart the PRTG core server to apply your changes. After you click Save, a dialog box appears that asks you to confirm the restart. Click OK to trigger the restart. During the restart, all users of the PRTG web interface, the <a href="#">PRTG app for desktop</a><sup>[2984]</sup>, or the <a href="#">PRTG Apps for Mobile Network Monitoring</a><sup>[2988]</sup> are disconnected and reconnected.</p>
NATS Connection Security	<p>This setting is only visible if you select Allow multi-platform probe connections above.</p>

Setting	Description
	<p>Define the connection security level between the PRTG core server and the NATS server.</p> <ul style="list-style-type: none"> <li>▪ TLS (default): Select Transport Layer Security (TLS) for an encrypted communication channel to the NATS server. This configures the NATS connection to use the <a href="#">tls://</a> schema.</li> <li>▪ Unsecure (not recommended): All data sent between the PRTG core server and the NATS server, including passwords and other sensitive information, will be transmitted in plain text. The NATS connection will use the unencrypted <a href="#">nats://</a> schema.</li> </ul>
<p>NATS Server Host</p>	<p><a href="#">This setting is only visible if you select</a> Allow multi-platform probe connections <a href="#">above</a>.</p> <p>Enter the host name and the port of the NATS server. An encrypted NATS server connection follows the format <a href="#">host name:port</a>. The default host is <a href="#">localhost:23561</a>.</p> <ul style="list-style-type: none"> <li>❗ Enter the host name as a fully qualified domain address name (FQDN) of the system that runs the NATS server.</li> <li>❗ The default port for this connection is <a href="#">23561</a>. The NATS server supports port numbers <a href="#">1 - 65535</a>.</li> </ul>
<p>NATS User Name</p>	<p><a href="#">This setting is only visible if you select</a> Allow multi-platform probe connections <a href="#">above</a>.</p> <p>Enter the user name for authentication against the NATS server. Enter a string.</p>
<p>NATS Password</p>	<p><a href="#">This setting is only visible if you select</a> Allow multi-platform probe connections <a href="#">above</a>.</p> <p>Enter the password for authentication against the NATS server. Enter a string.</p>
<p>NATS Server Certificate Authority Handling</p>	<p><a href="#">This setting is only visible if you select</a> TLS (default) <a href="#">above</a>.</p> <p>Define the CA certificate the NATS server uses:</p> <ul style="list-style-type: none"> <li>▪ Use system certificate store (default): Use the CA certificate from your system's certificate store.</li> <li>▪ Specify a certificate authority certificate file: Define a CA certificate file below. Use this setting if you created your own TLS certificate.</li> </ul> <p>■ For more information, see the Knowledge Base: <a href="#">How can I create a TLS certificate?</a></p>

Setting	Description
Certificate File Name	<p>This setting is only visible if you select Specify a certificate authority certificate file above.</p> <p>Select the CA certificate to use for TLS validation. This file must match the CA certificate used to install the NATS server.</p>
Connection Log Level	<p>Define the log severity level of the multi-platform probe connection that will appear in the log file:</p> <ul style="list-style-type: none"> <li>▪ Error: Log critical events.</li> <li>▪ Warning: Log unexpected events that might result in future errors.</li> <li>▪ Info (default): Log events that are significant to the normal operation of the the probe adapter.</li> <li>▪ Debug: Log detailed events that occur during the operation of the probe adapter. Useful for identifying issues.</li> <li>▪ Trace: Log all events of the probe adapter.</li> </ul> <p><b>i</b> The log level decreases in severity, with Error being the highest severity and Trace being the lowest. The log file will record all logs pertaining to the selected log severity level and all higher severity levels. For example, if you select Info (default), the log file will contain logs identified as Info, Warning, and Error. If you select Debug, the log file will contain logs identified as Error, Warning, Info, and Debug.</p> <p><b>i</b> You can find the log files in the <a href="#">PRTG data directory</a> <sup>3214</sup>: C:\ProgramData\Paessler\PRTG Network Monitor\Logs\probeadapter.</p> <p><b>i</b> We recommend that you only set your level to Debug or Trace when you are troubleshooting your setup due to the large amount of logs the probe adapter generates. Treat log files created at these log levels as confidential as some logs may contain sensitive information.</p>

## Active Directory Integration

 This option is not available in PRTG Hosted Monitor.

**Active Directory Integration**

Domain Name <sup>3</sup>


---

Domain Access <sup>3</sup>  Use domain name (default)  
 Specify domain controllers

LDAP Connection Security <sup>3</sup>  Use LDAP without connection security (default)  
 Use LDAP over SSL

Access Type <sup>3</sup>  Use the PRTG core server service account (usually Local System) (default)  
 Use explicit credentials

Active Directory Integration

Setting	Description
Domain Name	<p>To use the Microsoft Entra ID integration, enter the name of your local domain. Enter a string or leave the field empty.</p> <p> PRTG does not support trusted domains or AD subdomains. For more important notes about AD integration, see section <a href="#">Active Directory Integration</a><sup>[5082]</sup>, section Notes and Restrictions.</p>
Domain Access	<p>Define how PRTG performs <a href="#">Active Directory (AD)</a> queries:</p> <ul style="list-style-type: none"> <li>▪ Use domain name (default): Use the entry in the Domain Name field above.</li> <li>▪ Specify domain controllers: Use specific domain controllers. Specify the domain controllers below.</li> </ul>
Primary Domain Controller	<p><a href="#">This setting is only visible if you select Specify domain controllers above.</a></p> <p>Enter the DNS name of the primary domain controller.</p>
Backup Domain Controller (optional)	<p><a href="#">This setting is only visible if you select Specify domain controllers above.</a></p> <p>Optionally enter the DNS name of the backup domain controller or leave the field empty.</p>
LDAP Connection Security	<p>Define if you want to use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection to the LDAP server:</p> <ul style="list-style-type: none"> <li>▪ Use LDAP without connection security (default): Do not use an SSL/TLS-secured connection.</li> <li>▪ Use LDAP over SSL: Use an SSL/TLS-secured connection.</li> </ul>
Access Type	<p>Define which user account PRTG uses to configure AD access:</p> <ul style="list-style-type: none"> <li>▪ Use the PRTG core server service account (usually Local System) (default): Use the same Windows user account configured for the PRTG core server service. In a default installation, this is the "local system" Windows user account. If this account does not have the right to query all groups of your Active Directory, do not use this option.</li> <li>▪ Use explicit credentials: Define a user account that PRTG uses to authenticate against the Active Directory. This should be a user account with full access to all of your AD groups.</li> </ul> <p>PRTG uses this account to query the AD for available groups.</p>
User Name	<p><a href="#">This setting is only visible if you select Use explicit credentials above.</a></p> <p>Enter the Windows user account name that PRTG uses to authenticate for AD configuration.</p>



Setting	Description
Password	<p>This setting is only visible if you select Use explicit credentials above.</p> <p>Enter the password for the Windows user account that PRTG uses to authenticate for AD configuration.</p>

## Historic Data Purging












Data purging enables you to automatically delete unnecessary data to free up disk space and to improve system performance. You can define different time spans for several kinds of data.




■ For more information on storage locations, see section [Data Storage](#) <sup>[3213]</sup>.


☁ PRTG Hosted Monitor purges historic data using the default purging limits of PRTG Network Monitor except the configuration backups that are purged after 30 days. You cannot modify historic data purging limits in PRTG Hosted Monitor.

Historic Data Purging	
Log File Records ⓘ	30
PRTG Web Server Log Records ⓘ	30
Historic Sensor Data ⓘ	365
Toplist Records ⓘ	30
Closed Tickets ⓘ	365
Reports ⓘ	365
Configuration Auto-Backups ⓘ	365
Screenshots of HTTP Full Web Page Sensor ⓘ	10

Historic Data Purging

Setting	Description
Log File Records	<p>Define how long PRTG keeps records in the system log file <a href="#">Log Database.db</a>. Enter a value in days. PRTG automatically deletes all entries that are older than this value. This also affects the content of the <a href="#">Logs</a> tab of monitoring objects like sensors.</p> <ul style="list-style-type: none"> <li> Keep this value as low as possible to enhance system performance.</li> <li> The default value is 30 days.</li> </ul>
PRTG Web Server Log Records	<p>PRTG creates one PRTG web server log file every day. Define how many PRTG web server log files to keep. Enter a value in days. PRTG automatically deletes all PRTG web server log files that older than this value.</p> <ul style="list-style-type: none"> <li> The default value is 30 days.</li> </ul>
Historic Sensor Data	<p>Define for how long PRTG keeps historic sensor data for all sensors. Enter a value in days.</p> <ul style="list-style-type: none"> <li> Historic sensor data is the basis for reports on monitoring data. If you decrease this value, less historic monitoring data is available.</li> <li> Depending on the scanning intervals and the number of sensors in your setup, the file that contains this data can become large. For smaller installations up to 500 sensors, 365 is usually appropriate.</li> <li> The default value is 365 days.</li> <li> The maximum value is 9999 days.</li> </ul>
Toplist Records	<p>Define for how long PRTG keeps toplist records for <a href="#">Flow (NetFlow, jFlow, sFlow, IPFIX)</a> and <a href="#">Packet Sniffer</a> sensors. Enter a value in days. We recommend that you use 30 days here.</p> <ul style="list-style-type: none"> <li> Old toplist data is deleted automatically as soon as a limit of 2 GB is reached. The oldest data is deleted from the database first.</li> <li> The default value is 30 days.</li> </ul>
Closed Tickets	<p>Define for how long PRTG keeps tickets that are in the <a href="#">Closed</a> status. Enter a value in days.</p> <ul style="list-style-type: none"> <li> The default value is 365 days.</li> </ul>
Reports	<p>Define the maximum age for PDF reports. Enter a value in days. PRTG automatically deletes all reports that are older than this value.</p> <ul style="list-style-type: none"> <li> The default value is 365 days.</li> </ul>

Setting	Description
Configuration Auto-Backups	<p>Define the maximum age for daily configuration backups. Enter a value in days. PRTG automatically deletes all configuration backup files that are older than this value.</p> <p> The default value is <b>365</b> days.</p> <p> PRTG Hosted Monitor purges the configuration backups after <b>30</b> days.</p>
Screenshots of HTTP Full Web Page Sensor	<p>Define for how long PRTG keeps the screenshots of the <a href="#">HTTP Full Web Page</a> sensor (PhantomJS browser engine). Enter a value in days. PRTG automatically deletes screenshots that are older than this value with every sensor scan.</p> <p> The default value is <b>10</b> days.</p>

 Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

## More

### ■ KNOWLEDGE BASE

Where can I find PRTG mini probes which are ready to use?

- <https://kb.paessler.com/en/topic/61215>

What is the multi-platform probe and how can I use it?

- <https://kb.paessler.com/en/topic/90140>

How can I create a TLS certificate?

- <https://kb.paessler.com/en/topic/91877>

## Others

There are some settings that you must define in the [PRTG Administration Tool](#)<sup>[3040]</sup>. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#)<sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#)<sup>[3067]</sup>















### 8.12.2.5 User Accounts

On the User Accounts tab, administrators can add new user accounts, edit user accounts, and define which user groups that users are members of.

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.



**☁** If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.

In this section:

- [User Accounts Overview](#) 
- [Add User Accounts](#) 
- [User Account Settings Tabs](#) 
- [Settings Tab](#) 
  - [User Account Settings](#) 
  - [API Access](#) 
  - [Account Settings](#) 
  - [Group Membership](#) 
  - [PRTG Web Interface](#) 
  - [Ticket System](#) 
- [Notification Contacts Tab](#) 
- [Comments Tab](#) 
- [History Tab](#) 
- [API Keys Tab](#) 

## User Accounts Overview

The User Accounts tab shows a list of all user accounts in this PRTG installation and various types of information about each user.







Column Header	Description
Object	Shows the name of the user account. Click the user account to open its <a href="#">settings</a>  .
Type	Shows the user type, for example, <a href="#">read-only user</a> .
Email	Shows the primary email address of the user account.
Primary Group	Shows the primary group of the user account. Click the user group name to open its <a href="#">settings</a>  .

Column Header	Description
Group Memberships	Shows all user groups that the user account belongs to.
Active/Paused	Shows the status of the user account. This can be <a href="#">active</a> or <a href="#">paused</a> .

For more information, see section [Working with Table Lists](#) <sup>[218]</sup>.

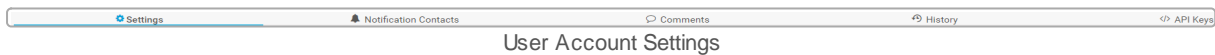
## Add User Accounts

You have several options to add user accounts:

-  To add a new user to PRTG Network Monitor, hover over  and select Add User from the menu. The options are almost the same as for editing users.
  -  To add a new user to PRTG Hosted Monitor, click Invite User. The options are almost the same as for editing users but PRTG Hosted Monitor automatically generates the initial account password. The new user can change it later. Click Send Invite to save your settings and to send the invitation per email to the defined primary email address.
  - To batch-add several users at once, hover over  and select Add Multiple Users from the menu. In the dialog box that appears, select a [user group](#) <sup>[2912]</sup> from the dropdown list and enter or paste a list of email addresses. Separate them by a space, comma, semicolon, or a new line. Click OK to confirm. For each email address, PRTG creates a new, local user account in the user group, using the email address as the value for Login Name, Display Name, and Primary Email Address. PRTG automatically generates a new password and sends it to the email address.
-  Access rights to device tree objects, libraries, maps, reports, or the ticket system are defined in user groups. Make sure that the user is a member of the correct user group with the required group access rights.
-  You cannot delete [predefined](#) objects such as the [PRTG System Administrator](#) user account, the [PRTG Users Group](#), or the [PRTG Administrators](#) group.

## User Account Settings Tabs

Click on a user account and select the various tabs to change the different settings.



## Settings Tab

### User Account Settings

**User Account Settings**

Login Name ⓘ prtgadmin

Display Name ⓘ PRTG System Administrator

Primary Email Address ⓘ johnqpublic@example.com

Password ⓘ  Do not change the password  
 Specify a new password

Passhash ⓘ Show passhash

User Account Settings

Setting	Description
Login Name	<p>Enter a login name for the user account.</p> <p><b>i</b> The login name must not contain the following invalid characters: " / \ [ ] : ;   = , + * ? &lt; &gt;</p> <p><b>☁</b> This option is not available in PRTG Hosted Monitor.</p>
Display Name	<p>Enter a display name that the user recognizes. PRTG uses it for display purposes only, for example on the Welcome page.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
Primary Email Address	<p>Enter the primary email address. This is the email address that PRTG uses by default for the ticket system, including important system messages, and password recovery.</p> <p><b>i</b> Make sure that your email client can show HTML emails, otherwise you cannot read emails from PRTG.</p>
Login Type	<p><b>☁</b> This setting is only visible for PRTG Hosted Monitor instances if a <a href="#">Microsoft Entra ID connection (formerly Azure Active Directory) has been successfully configured.</a></p> <ul style="list-style-type: none"> <li>▪ Auth0 (default): Send the user a random password to log in to the PRTG Hosted Monitor instance.</li> <li>▪ Federated Directory: Add a user from your Microsoft Entra tenant. <ul style="list-style-type: none"> <li><b>i</b> Use this option when you have configured a Microsoft Entra ID connection for your PRTG Hosted Monitor instance and want to add a user from your Microsoft Entra tenant.</li> </ul> </li> </ul>

Setting	Description
	<p>■ For more information, see the Knowledge Base: <a href="#">How to integrate Microsoft Entra ID into PRTG Hosted Monitor?</a>.</p>
Password	<p>Define whether to change the password for the user account:</p> <ul style="list-style-type: none"> <li>▪ Do not change the password</li> <li>▪ Specify a new password</li> </ul> <p>ⓘ For security reasons, PRTG does not display the password.</p> <p>If you specify a new password, enter the old password, then enter the new password twice.</p> <p>ⓘ The new password must be at least 8 characters long. It must contain a number and a capital letter.</p> <p>ⓘ Do not use leading or trailing whitespaces in the new password.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
Passhash	<p>Click Show passhash to display the passhash for the user account. This is necessary for authentication for the <a href="#">PRTG API</a>.</p> <p>ⓘ This setting is for your information only. You cannot change it.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>

## API Access

☁ These settings are only available in PRTG Hosted Monitor.

**API Access**

API User Name ⓘ *johnpublic@example.com*

API Passhash ⓘ Show passhash

Generate API Passhash ⓘ Generate new passhash

API Access

Setting	Description
API User Name	<p>Shows the API user name of the user account. This is necessary for authentication for the PRTG API.</p> <p>ⓘ This setting is for your information only. You cannot change it.</p>

Setting	Description
API Passthrough	Click Show passthrough to display the API passthrough of the user account. This is recommended for authentication for the PRTG API.  <b>i</b> This setting is for your information only. You cannot change it.
Generate API Passthrough	Click Generate new passthrough to reset the passthrough of the user.

## Account Settings

**Account Settings**

**User Type** **i**  Read/write user  
 Read-only user

**Acknowledge Alarms** **i**  Allow user to acknowledge alarms  
 Do not allow user to acknowledge alarms (default)

**Password Change** **i**  Allow user to change the account password  
 Do not allow user to change the account password (default)

**Primary Group** **i** PRTG Users Group

---

**Status** **i**  Active  
 Paused

**Last Login** **i** (has not logged in yet)

Account Settings

Setting	Description
User Type	<p>Define the user type:</p> <ul style="list-style-type: none"> <li>▪ Read/write user: Can only view monitoring results, libraries, maps, reports, and also edit the according settings. In addition, they can add and delete objects, libraries, maps, and reports. The user can acknowledge alarms, edit notification templates, notification contacts, and schedules.</li> <li>▪ Read-only user: Can only view monitoring results, libraries, maps, reports, and the according settings. The user can acknowledge alarms and change their own password if allowed. This is a good choice for public or semi-public logins.</li> </ul> <p><b>i</b> Read-only users cannot be members of groups with administrative rights.</p> <p><b>i</b> This setting is not available for the <a href="#">PRTG System Administrator</a> user account.</p>



Setting	Description
Acknowledge Alarms	<p><b>This setting is only visible if you select Read-only user above.</b></p> <p>Acknowledging an alarm is an action that requires write access. However, you can explicitly allow a read-only user to <a href="#">acknowledge alarms</a><sup>[203]</sup>:</p> <ul style="list-style-type: none"> <li>▪ Allow user to acknowledge alarms: Allow the read-only user to acknowledge alarms.</li> <li>▪ Do not allow user to acknowledge alarms (default): Do not allow the read-only user to acknowledge alarms.</li> </ul>
Password Change	<p><b>This setting is only visible if you select Read-only user above.</b></p> <p>Define if the user can change their account password:</p> <ul style="list-style-type: none"> <li>▪ Allow user to change the account password: Allow the read-only user to change their password. The option to change their password is available in the <a href="#">My Account</a><sup>[280]</sup> settings of the user.</li> <li>▪ Do not allow user to change the account password (default): Do not allow the read-only user to change their password.</li> </ul>
Primary Group	<p>Select the primary group for the user account from the dropdown list.</p> <p><b>i</b> Every user account must be a member of a primary group to make sure there is no user account without group membership. Membership in other user groups is optional.</p> <p><b>i</b> You cannot change the primary group of <a href="#">Active Directory users</a>. Users that you add via <a href="#">Active Directory integration</a><sup>[308]</sup> can only have the respective Active Directory group as their primary group.</p> <p>Select Create new user group for this user to create a user group for the new user. This option is only visible when you add a new user account. The default name of the new user group is the Display Name of the new user.</p>
Status	<p>Define the status of the user:</p> <ul style="list-style-type: none"> <li>▪ Active: Can log in to the PRTG web interface.</li> <li>▪ Paused: Cannot log in to the PRTG web interface. Use this option to temporarily deny access for this user.</li> </ul> <p><b>i</b> This setting is not available for the <a href="#">PRTG System Administrator</a> user account.</p>
Last Login	<p>Shows the time stamp of the last login of the user account.</p> <p><b>i</b> This setting is for your information only. You cannot change it.</p>

## Group Membership

Group Membership

Member of ?

▼ User Group Name

PRTG Administrators

PRTG Users Group

User Group1

Group Membership

Setting	Description
Member of	<p>Shows the user groups that the user account is a member of. You can define access rights to device tree objects, libraries, maps, reports and the ticket system at group level.</p> <p><span style="font-size: 0.8em;">?</span> This setting is for your information only. You cannot change it.</p>

## PRTG Web Interface

PRTG Web Interface

Automatic Refresh ?

Automatically refresh pages (default)

Do not automatically refresh pages

Refresh Interval (Sec.) ? 30

Audible Alarms ?

Do not play audible alarms (default)

Play audible alarms on dashboard pages only

Play audible alarms on all pages

Home Page URL ? /welcome.htm

Time Zone ? (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

Date Format ? Use System Settings

Color Mode ?

Light (default)

Dark

PRTG Web Interface

Setting	Description
Automatic Refresh	<p>Define if you want PRTG to automatically reload web pages in the PRTG web interface for the user:</p> <ul style="list-style-type: none"> <li>▪ Automatically refresh pages (default): PRTG automatically refreshes single page elements on web pages in the PRTG web interface.</li> <li>▪ Do not automatically refresh pages: PRTG does not automatically refresh single page elements on web pages in the PRTG web interface.</li> </ul>
Refresh Interval (Sec.)	<p><b>This setting is only visible if you select</b> <a href="#">Automatically refresh pages (default)</a> <b>above.</b></p> <p>Enter the number of seconds that PRTG waits between two refreshes. We recommend that you use <b>30</b> seconds or more. The minimum value is <b>20</b> seconds. The maximum value is <b>600</b> seconds.</p> <p><b>i</b> Shorter refresh intervals create more CPU load on the probe system. If you experience load issues while using the PRTG web interface (or <a href="#">maps</a><sup>[2776]</sup>), set a longer refresh interval.</p>
Audible Alarms	<p>Define whether PRTG plays an audible alarm on web pages in the PRTG web interface when there is a new <a href="#">alarm</a><sup>[2901]</sup>:</p> <ul style="list-style-type: none"> <li>▪ Do not play audible alarms (default): PRTG does not play sound files on any web pages.</li> <li>▪ Play audible alarms on dashboard pages only: When there is a new alarm, PRTG plays a predefined sound on <a href="#">dashboard</a><sup>[237]</sup> pages only. The sound is played with every refresh of the dashboard page if there is at least one new alarm.</li> <li>▪ Play audible alarms on all pages: When there is a new alarm, PRTG plays a predefined sound on all web pages. PRTG plays the sound with every page refresh if there is at least one new alarm.</li> </ul> <p><b>i</b> PRTG only plays audible alarms if the New Alarms value in the <a href="#">global header area</a><sup>[168]</sup> of the PRTG web interface is greater than 0 after a page refresh. PRTG does not consider the number of old alarms.</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which audible notifications are available in the PRTG web interface and in the PRTG app for desktop?</a> and <a href="#">Why are audible alerts in public maps not working in Chrome?</a></p>
Home Page URL	<p>Define the user's default home page in the PRTG web interface. This is the page that the user sees after logging in or when selecting <a href="#">Home</a><sup>[237]</sup> from the main menu. Enter a PRTG-internal web page.</p>
Time Zone	<p>Define the time zone for the user account. Depending on the time zone that you select, PRTG shows the local time zone of the user account in all data tables and graph legends.</p>

Setting	Description
	<p><b>i</b> PRTG receives the Coordinated Universal Time (UTC) from the system time of the PRTG core server for this purpose.</p> <p><b>■</b> If you get a warning message about differing time zones, see the Knowledge Base: <a href="#">Why do I get a warning message when time zones differ?</a></p>
Date Format	<p>Select the date format for the user:</p> <ul style="list-style-type: none"> <li>▪ Use default settings: Use the date format of the PRTG core server system.</li> <li>▪ DD.MM.YYYY HH:MM:SS (24h)</li> <li>▪ DD.MM.YYYY HH:MM:SS (A.M./P.M.)</li> <li>▪ MM/DD/YYYY HH:MM:SS (24h)</li> <li>▪ MM/DD/YYYY HH:MM:SS (A.M./P.M.)</li> <li>▪ YYYY-MM-DD HH:MM:SS (24h)</li> <li>▪ YYYY-MM-DD HH:MM:SS (A.M./P.M.)</li> </ul> <p><b>i</b> This setting takes effect after the next login.</p>
Color Mode	<p>Select a color mode for the PRTG web interface:</p> <ul style="list-style-type: none"> <li>▪ Light (default)</li> <li>▪ Dark</li> </ul>

## Ticket System

**Ticket System**

Email Notifications **i**
 Receive an email when a ticket changes (default)
  Do not receive any emails from the ticket system

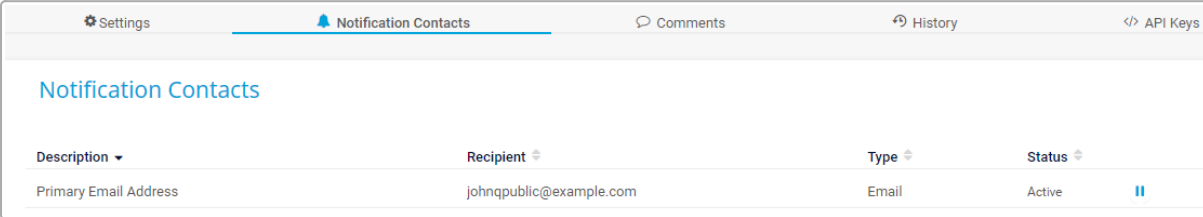
Ticket System

Setting	Description
Email Notifications	<p>Define if the user receives emails from the ticket system:</p> <ul style="list-style-type: none"> <li>▪ Receive an email when a ticket changes (default): The user receives an email each time a ticket is assigned to the user or to the user group they are a member of, or if a ticket is changed.</li> </ul> <p><b>i</b> If the user edits tickets that are assigned to them or the user group they are a member of, or if they assign a ticket to themselves or their user group, they do not get an email.</p>

Setting	Description
	<ul style="list-style-type: none"> <li>Do not receive any emails from the ticket system: The user does not receive any emails from the ticket system.</li> </ul>

 Save your settings. If you leave the page, all changes to the settings are lost.

## Notification Contacts Tab



Description	Recipient	Type	Status
Primary Email Address	johnqpublic@example.com	Email	Active

Notification Contacts

The Notification Contacts tab shows a list of all notification contacts of the selected user account.

Setting	Description
Description	Shows the description for the email contact.
Recipient	Shows the email address for the email contact.
Type	Shows the type of the notification contact.

 You can add new notification contacts under Setup | Account Settings | [Notification Contacts](#)<sup>2842</sup>.

## Comments Tab

On the Comments tab, you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

## History Tab

On the History tab, all changes in the settings of an object are logged with a time stamp, the name of the user who made the change, and a message. The history log retains the last 100 entries.

## API Keys Tab

On the API Keys tab, you can add, edit, and delete API keys that are specific to the user account. For more information, see section [API Keys](#)<sup>2851</sup>.

## More

### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Which audible notifications are available in the PRTG web interface and in the PRTG app for desktop?

- <https://kb.paessler.com/en/topic/26303>

Why are audible alerts in public maps not working in Chrome?

- <https://kb.paessler.com/en/topic/83142>

Why do I get a warning message when time zones differ?

- <https://kb.paessler.com/en/topic/81306>

## Others

There are some settings that you must define in the [PRTG Administration Tool](#)<sup>[3040]</sup>. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#)<sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#)<sup>[3067]</sup>

### 8.12.2.6 User Groups

On the User Groups tab, you can define access rights for monitoring objects, libraries, maps, and reports at user group level. This means that group membership determines what a user can do and which monitoring objects, libraries, maps, or reports they can see. This does not apply to read-only users, who always have only read access, no matter what access rights the user group they belong to has. You can define group access rights for each object in the object's settings.

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

**☁** If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.


## User Groups Overview

The User Groups tab shows a list of all user groups in this PRTG installation and various types of information about each user group.

Column Header	Description
Object	Shows the name of the user group. Click the user group to open its

Column Header	Description
	<a href="#">settings</a> <sup>[2914]</sup>
Type	Shows the user group type, for example, a <a href="#">PRTG user group</a> , an <a href="#">Active Directory group</a> , or a <a href="#">single sign-on (SSO) group</a> .
Members	Shows all users that are a member of this user group.
Primary Group	Shows all users that have this user group as their primary group. Click the user group name to open its <a href="#">settings</a> <sup>[2914]</sup> .
Active Directory Group	Shows the Active Directory group that the user group is connected to.
SSO Claim	Shows the access claim for the SSO group that the user group is connected to.

## Add User Groups

- To add a new user group to PRTG Network Monitor or to PRTG Hosted Monitor, hover over  and select Add User Group from the menu. The options are almost the same as for editing user groups.
- For each user group you create, PRTG automatically adds a new [group in the device tree](#)<sup>[133]</sup> with the name [\[group\\_name\] home](#).
- For each user group you create, PRTG automatically adds a new [email notification](#)<sup>[2815]</sup> to the [notification templates](#)<sup>[2808]</sup>. It has the name [Email to all members of group \[group\\_name\]](#). The new user group automatically has [read access](#)<sup>[145]</sup> to the new notification template.
- By default, there are no [access rights](#)<sup>[145]</sup> defined on objects for a newly created user group. Initially, users in this user group do not see any objects in the device tree except the automatically created [\[group\\_name\] home](#) group for which they have write access. This does not apply if the new user group is an administrator group. Edit the [settings](#)<sup>[201]</sup> of objects in your device tree, libraries, maps, or reports, and set access rights for the new user group in the Access Rights section.
  - ① The easiest way to set access rights is in the [root group settings](#)<sup>[420]</sup> and to use the [inheritance of settings](#)<sup>[136]</sup>.
  - ① The multi-edit option is not available for the [predefined](#) user groups [PRTG Administrators](#) and [PRTG Users Group](#).
  - ① You cannot delete [predefined](#) objects such as the [PRTG System Administrator](#) user account, the [PRTG Users Group](#), or the [PRTG Administrators](#) group.
  - ① If you want to delete an Active Directory group from PRTG, you must delete all users that are in the user group first. This is because the Active Directory users have this user group as their primary group, and user accounts must have a primary group.

## User Group Settings

**User Group Settings**

User Group Name ⓘ

---

Administrative Rights ⓘ  Give user group members administrative rights  
 Do not give user group members administrative rights (default)

Home Page URL ⓘ

---

Active Directory Integration ⓘ  Do not use Active Directory integration (default)  
 Use Active Directory integration







Sensor Creation Rights ⓘ  Allow user group members to create all sensors (default)  
 Allow user group members to create certain sensors only




Ticket System Access ⓘ  Allow user group members to use the ticket system (default)  
 Do not allow user group members to use the ticket system

User Group Settings

Setting	Description
User Group Name	Enter a name for the user group.  ⓘ If the name contains angle brackets (<>), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a>
Administrative Rights	Define if the user group members have administrative rights: <ul style="list-style-type: none"> <li>▪ Give user group members administrative rights: Give administrative rights to all user group members.  ⓘ If you select this option, all user group members have full access to all device tree objects, libraries, maps, reports, and the ticket system. In addition, they can manage user accounts and user groups, and they can change the monitoring configuration of PRTG.</li> <li>▪ Do not give user group members administrative rights (default): Do not give the user group member administrative rights. Access to device tree objects, libraries, maps, and reports for user group members are defined in an object's settings.</li> </ul>
Home Page URL	Define the default home page for the user group members. This is the page that the user sees after logging in or when selecting <a href="#">Home</a> <sup>[237]</sup> from the main menu. Enter a PRTG-internal web page.  ⓘ This applies to new users that were either added via <a href="#">Active Directory Integration</a> <sup>[308]</sup> or using the <a href="#">Add Multiple Users option</a> <sup>[2903]</sup> .
Active Directory or Single Sign-On Integration	Define whether to connect this user group to external users:



Setting	Description
	<ul style="list-style-type: none"> <li>▪ Do not use Active Directory integration (default): Do not connect this user group to a user group in your Active Directory or to a single sign-on integration. Use local user accounts instead.</li> <li>▪ Use Active Directory integration: Connect this user group to a user group in your Active Directory. <ul style="list-style-type: none"> <li>■ For more information, see section <a href="#">Active Directory Integration</a><sup>[3081]</sup>.</li> </ul> </li> <li>▪ Use single sign-on integration: Connect this user group to a single sign-on integration. <ul style="list-style-type: none"> <li>■ For more information, see the Knowledge Base: <a href="#">How to integrate Microsoft Entra ID into PRTG?</a></li> <li>■ For more information, see the Knowledge Base: <a href="#">How to integrate Okta SSO into PRTG?</a></li> </ul> </li> </ul> <p> You cannot change credentials for users that are members of an Active Directory group.</p> <p> This option is not available in PRTG Hosted Monitor.</p>
Active Directory Group	<p><a href="#">This setting is only visible if you select Use Active Directory integration above.</a></p> <p>Select the user group whose members can log in to PRTG using their Active Directory domain credentials. The according user accounts have the <a href="#">access rights</a><sup>[145]</sup> of the user group you just created.</p> <p> You need to configure a valid Active Directory domain in the <a href="#">Core &amp; Probes</a><sup>[2887]</sup> settings for user groups to appear in the dropdown list.</p> <p>■ For more information, see section <a href="#">Active Directory Integration</a><sup>[3081]</sup>.</p> <p> If your Active Directory contains more than 1,000 entries in total, PRTG displays an input field instead of a dropdown list. This is for performance reasons. In the input field, you can only enter the name of the user group in your Active Directory. PRTG then automatically adds the domain name prefix.</p> <p> PRTG caches the list of the user groups in your Active Directory for one hour. You can update this list earlier by manually clearing the cache via the <a href="#">Administrative Tools</a><sup>[2918]</sup> by clicking Go! in the Clear Caches section.</p> <p> This option is not available in PRTG Hosted Monitor.</p>
SSO Group Claim	<p><a href="#">This setting is only visible if you select Use single sign-on integration above.</a></p> <p>Enter the access claim for the SSO group, for example a scope name or an Azure group object ID.</p>

Setting	Description
	<p> This option is not available in PRTG Hosted Monitor.</p>
<p>User Type</p>	<p><a href="#">This setting is only visible if you select Use Active Directory integration above.</a></p> <p>Define the default user access rights for all new users in this user group:</p> <ul style="list-style-type: none"> <li>▪ Read/write user: Can only view monitoring results, libraries, maps, reports, and also edit the according settings. In addition, they can add and delete objects, libraries, maps, and reports. The user can acknowledge alarms, edit notification templates, notification contacts, and schedules.</li> <li>▪ Read-only user: Can only view monitoring results, libraries, maps, reports, and the according settings. The user can acknowledge alarms and change their own password if allowed. This is a good choice for public or semi-public logins.</li> </ul> <p> Read-only users cannot be members of groups with administrative rights.</p> <p> If a user logs in to PRTG for the first time using Active Directory credentials, PRTG automatically creates a new, local user account for this user with the user type that you define.</p>
<p>Acknowledge Alarms</p>	<p><a href="#">This setting is only visible if you select Read-only user above.</a></p> <p>Acknowledging an alarm is an action that requires write access. However, you can explicitly allow a read-only user to <a href="#">acknowledge alarms</a><sup>[203]</sup>:</p> <ul style="list-style-type: none"> <li>▪ Allow user group members to acknowledge alarms: Allow read-only user group members to acknowledge alarms.</li> <li>▪ Do not allow user group members to acknowledge alarms (default): Do not allow read-only user group members to acknowledge alarms.</li> </ul>
<p>Sensor Creation Rights</p>	<p>Define if user group members can create all sensors or only specific sensors:</p> <ul style="list-style-type: none"> <li>▪ Allow user group members to create all sensors (default): No restrictions for group members apply.</li> <li>▪ Allow user group members to create certain sensors only: Select the allowed sensors from the list of available sensors.</li> </ul>
<p>Allowed Sensors</p>	<p><a href="#">This setting is only visible if you select Allow user group members to create certain sensors only above.</a></p>

Setting	Description
	<p>A list of all available sensors is shown. Select the sensors that user group members can create by enabling check boxes in front of the respective sensor names.</p> <ul style="list-style-type: none"> <li><b>i</b> You can also select all items or cancel the selection by using the check box in the table header.</li> <li><b>i</b> PRTG displays sensors that are in use in bold print.</li> <li><b>i</b> This setting does not apply when a user group member runs an <a href="#">auto-discovery</a><sup>[254]</sup>. The auto-discovery adds all sensors that are defined in the used device templates. This setting does also not apply when a user group member adds <a href="#">recommended sensors</a><sup>[197]</sup>.</li> </ul>
Ticket System Access	<p>Define if user group members can use the <a href="#">ticket system</a><sup>[213]</sup>:</p> <ul style="list-style-type: none"> <li>▪ Allow user group members to use the ticket system (default): Users in this user group can read, create, assign, and modify tickets. <ul style="list-style-type: none"> <li><b>i</b> Group members that are read-only users never have access to the ticket system.</li> </ul> </li> <li>▪ Do not allow user group members to use the ticket system: The <a href="#">Tickets</a><sup>[247]</sup> menu item in the main menu bar is not visible to users in this user group.</li> </ul>

## Group Members

Group Members

Members **i**

	User Name	
<input checked="" type="checkbox"/>	John Q. Public	
<input type="checkbox"/>	PRTG System Administrator	

Group Members

Setting	Description
Members	<p><b>This setting is only visible if you select &lt;% C_Do_not_use_Active_Directory_or_single_sign-on_integration%&gt; above.</b></p> <p>Define which local user accounts are members of this user group. To add a user account from the list, enable the check box in front of the user name. The available user accounts depend on your setup.</p>

## Primary Group Users

Primary Group Users

[User List](#) ⓘ John Q. Public

Primary Group Users

Setting	Description
User List	Shows a list of all user accounts that have this user group as their primary group. This is only shown for your information. You can change the primary group of a user account in the <a href="#">user account's settings</a> ⓘ.

ⓘ Save your settings. If you leave the page, all changes to the settings are lost.

### More

#### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

How to integrate Microsoft Entra ID into PRTG?

- <https://kb.paessler.com/en/topic/88527>

How to integrate Okta SSO into PRTG?

- <https://kb.paessler.com/en/topic/90482>

### Others

There are some settings that you must define in the [PRTG Administration Tool](#) ⓘ. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#) ⓘ
- [PRTG Administration Tool on Remote Probe Systems](#) ⓘ

#### 8.12.2.7 Administrative Tools

On the Administrative Tools tab, you can start system-specific processes for debugging purposes.

ⓘ This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

☁ If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.

## Administrative Tools For The PRTG Core Server

### Administrative Tools For The PRTG Core Server

**Create Configuration Snapshot**

Saves the current configuration as a .zip file in the \Configuration Auto-Backups subfolder of the PRTG data directory of your PRTG installation.

[Go!](#)

**Write Core Status File**

Creates a debug file on the PRTG core server system.

[Go!](#)

**Clear Caches**

Clears the internal caches of the PRTG web server for Geo Maps, the Active Directory integration, and the Active Directory group list.

[Go!](#)

**Load Lookups and File Lists**

Reloads the lookup files from the \lookups\custom subfolder of the PRTG program directory, and other file lists that are displayed in the PRTG web interface, for example, SNMP libraries, device icons, and report templates.

[Go!](#)

**Recalculate PRTG Graph Data Cache**

Deletes the data cache file and automatically recalculates it. If you apply recalculation, PRTG needs to restart the PRTG core server.

[Go!](#)

**Restart PRTG Core Server Service**

Restarts the PRTG core server service.

[Go!](#)

**Reload Logging Configuration**



Apply changes to the logging configuration to all PRTG modules.

[Go!](#)

Administrative Tools For The PRTG Core Server

Setting	Description
Create Configuration Snapshot	<p>Create a snapshot of the PRTG configuration. This action might take up to 100 seconds. Once it finishes, you can find a .zip file that contains a *.dat file in the \Configuration Auto-Backups subfolder of the <a href="#">PRTG data directory</a> <sup>[3214]</sup>.</p> <ul style="list-style-type: none"> <li><span style="color: #0070C0;">i</span> The name of the .zip file has the format <b>PRTG Configuration (Snapshot YYYY-MM-DD HH-MM-SS).zip</b>.</li> <li><span style="color: #0070C0;">i</span> If you run PRTG in a cluster, this action is executed on the cluster node you are logged in to.</li> </ul> <p><span style="color: #0070C0;">☁</span> This option is not available in PRTG Hosted Monitor.</p>
Write Core Status File	<p>Create status files of the PRTG core server. You can find the two text files in the \Logs\debug subfolder of the PRTG data directory. PRTG creates new files every time you click Go!.</p> <ul style="list-style-type: none"> <li><span style="color: #0070C0;">i</span> The files have the names <b>Core State (Global Debug Data).txt</b> and <b>Core State (Memory Debug Data).txt</b>.</li> <li><span style="color: #0070C0;">i</span> If you run PRTG in a cluster, this action is executed on the cluster node you are logged in to.</li> </ul> <p><span style="color: #0070C0;">☁</span> This option is not available in PRTG Hosted Monitor.</p>

Setting	Description
Clear Caches	<p>PRTG caches tiles for <a href="#">Geo Maps</a>, user data for <a href="#">Active Directory Integration</a>, and the <a href="#">Active Directory Group</a> list. Click Go! to delete the cache if you encounter broken Geo Maps tiles, if you changed a user's password in the Active Directory, or if you added groups in the Active Directory.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
Load Lookups and File Lists	<p>(Re)load the <a href="#">lookup files</a> from the \lookups\custom subfolder of the <a href="#">PRTG program directory</a>. In this subfolder, your customized lookup files are stored. If you have created a new lookup file or changed something in a lookup file, it might be necessary to load or to reload these files.</p> <p>With this option, you can also manually reload file lists in the PRTG web interface. If you have added new <a href="#">device icons</a>, <a href="#">device templates</a>, <a href="#">report templates</a>, .oidlib files for the <a href="#">SNMP Library</a> sensor, or language files to the PRTG program directory on the PRTG core server system while the server was running, reloading the file lists might be necessary to display new files in the PRTG web interface.</p> <p><b>i</b> Usually you do not need to reload file lists manually. A list is automatically reloaded when opening the according settings page with a latency of 10 seconds. If you save new device templates via the PRTG web interface, the template list is refreshed immediately.</p> <p>☁ This option is not available in PRTG Hosted Monitor.</p>
Recalculate PRTG Graph Data Cache	<p>PRTG constantly writes monitoring data to disk and keeps the graphs for your graph tabs in memory. If PRTG unexpectedly ends, the graph cache might become corrupted. In this case, graphs might be empty or show wrong data.</p> <p>If you experience graph display problems, a graph recalculation fixes the problem. Click Go! to delete the data cache file and to automatically recalculate it.</p> <p><b>i</b> If you apply the recalculation, PRTG needs to restart the PRTG core server. Because of this, all users of the PRTG web interface, the <a href="#">PRTG app for desktop</a>, or the <a href="#">PRTG apps for iOS or Android</a> are disconnected. After you click Go!, a dialog window appears that asks you to confirm the required restart. Click OK to trigger the restart.</p> <p><b>i</b> Directly after this action, your graphs are empty. PRTG successively refills them while the recalculation in the background progresses. Until the recalculation is finished, the performance of the PRTG web interface might be affected because of the high disk input/output (I/O) activity.</p>

Setting	Description
Restart PRTG Core Server Service	<p>Restart the PRTG core server service manually. Click Go! to restart it.</p> <p><b>i</b> If you restart the PRTG core server service, all users of the PRTG web interface, the PRTG app for desktop, or the PRTG apps for iOS or Android are disconnected. Clicking Go! immediately restarts the PRTG core server service.</p> <p><b>i</b> If you want to schedule an automatic restart of Windows services for both the PRTG core server service and the PRTG probe service, you can do this in the corresponding <a href="#">probe settings</a> .</p> <p> This option is not available in PRTG Hosted Monitor.</p>
Reload Logging Configuration	<p>For debugging reasons, it might be necessary to change the log levels of the PRTG core server. The Paessler support team takes you through the necessary steps that are required to change your logging configuration. The log level changes vary according to the PRTG installation, its setup, and the solution of an issue.</p> <p>To apply the changes, click Go!.</p>

## Administrative Tools For Probes

**Administrative Tools For Probes**

**Write Probe Status Files**

Creates a set of debug files on all probe systems.

**Restart All Probes**

Restarts all PRTG probe services. For disconnected probes, please use the PRTG Administration Tool on the respective probe system to start the PRTG probe service.

---

Probe #1 "Local Probe"

Connected From: 127.0.0.1:63007  
 Last Data: 06/10/2023 18:06:08 (0 sec ago) (W. Europe Standard Time)  
 .NET Framework Support: Installed: 4.7.2 or later

Administrative Tools For Probes

Setting	Description
Write Probe Status Files	<p>Create status files of all probes. PRTG writes status files for the local probe on the PRTG core server (in a cluster, on the cluster node you are logged in to) as well as for all classic remote probes. PRTG creates new files each time you click Go!.</p>

Setting	Description
	<p>On the respective systems, you find six text files in the \Logs\debug subfolder of the PRTG data directory. The files have the names <a href="#">Probe State (Global Debug Data).txt</a>, <a href="#">Probe State (Memory Debug Data).txt</a>, <a href="#">Probe State (Scheduler Debug Data).txt</a>, <a href="#">Probe State (Syslog).txt</a>, <a href="#">Probe State (Trap).txt</a>, and <a href="#">Probe State (xFlow Debug Data).txt</a>.</p> <p><b>i</b> This setting does not apply to any <a href="#">multi-platform probes</a> <sup>[3316]</sup>. For more information, see the <a href="#">Multi-Platform Probe for PRTG</a> manual.</p>
Restart All Probes	<p>Restart all probes as well as the local probe Windows service. If you have <a href="#">classic remote probes</a> <sup>[3190]</sup>, this restarts the probe Windows services on the remote probe systems as well. To restart single probes only, see below.</p> <p><b>i</b> You cannot restart disconnected probes here. Use the <a href="#">PRTG Administration Tool</a> <sup>[3040]</sup> on the probe system to start a disconnected probe on a Windows system. Restart disconnected probes on non-Windows systems directly from the probe system.</p> <p><b>i</b> If you run PRTG in a cluster, this action is executed on the cluster node you are logged in to. In this case, remote probes are only restarted if you are logged in to the primary master node. The cluster probe Windows service of failover nodes is not restarted if you execute this action on the primary master node. If you want to restart the cluster probe Windows service of a failover node, log in to the PRTG web interface of this failover node and click Go! there.</p> <p><b>i</b> This setting does not apply to any <a href="#">multi-platform probes</a> <sup>[3316]</sup>. For more information, see the <a href="#">Multi-Platform Probe for PRTG</a> manual.</p>
Probe [#Number] "[Name]"	<p>This section shows information about the connection status. If the probe is connected, the field shows the source IP address and port number that the probe uses. For the <a href="#">local probe</a>, the IP address is always 127.0.0.1. You also see information about the date when the last data packet was received from the probe.</p> <p>If you want to restart a single probe, click the corresponding Restart Probe button. Entries for every single probe follow.</p> <p><b>i</b> You cannot restart disconnected probes here. Use the <a href="#">PRTG Administration Tool</a> <sup>[3040]</sup> on the probe system to start a disconnected probe on a Windows system. Restart disconnected probes on non-Windows systems directly from the probe system.</p> <p><b>☁</b> This option is not available on the hosted probe of a PRTG Hosted Monitor instance.</p>


## Others


There are some settings that you must define in the [PRTG Administration Tool](#) <sup>[3040]</sup>. For more information, see sections:




- [PRTG Administration Tool on PRTG Core Server Systems](#) 
- [PRTG Administration Tool on Remote Probe Systems](#) 

### 8.12.2.8 Cluster

On the Cluster tab, you can change cluster-related settings. See the [cluster status](#)  to see if all cluster nodes are properly connected.

 This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.



 If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.





 This feature is not available in PRTG Hosted Monitor.


### Cluster Node Setup


Cluster Node Setup				
	Node Name	Node ID	Node Status	IP Addresses/DNS Names for Node-Node Connections
1	PRTG Network Monitor (	A1B2C3D4E5F6G7H8J9	Active	#2 ⇒ #1 192.0.2.0
2	Failover Node	11111111-2222-3333-4444-555555555555	<input checked="" type="radio"/> Active <input type="radio"/> Inactive	#1 ⇒ #2 192.0.2.1

Cluster Node Setup

Setting	Description
Node Name	<p>Enter the name of the cluster node. PRTG uses it for display purposes only.</p> <p> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({}), for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>
NodeID	<p>The ID is unique for every cluster node.</p> <p> We recommend that you use the default value.</p>
Node Status	<p>Set the state for each failover node:</p> <ul style="list-style-type: none"> <li>▪ Active: Set the failover node to active.</li> <li>▪ Inactive: Set the failover node to inactive. PRTG disables it in the cluster configuration. The failover node is no longer an active part of the cluster and it does not appear in the cluster status anymore.</li> </ul>

Setting	Description
	<p> This setting is not available for the master node of a cluster. The master node is always Active.</p>
<p>IP Addresses/DNS Names Used for Node-Node Connections</p>	<p>Define the IP addresses or Domain Name System (DNS) names that PRTG uses for the node-node connections. You can enter different values for every connection.</p> <p>For example, in the field #2 =&gt; #1, enter the address under which the master node is reachable from the second cluster node. Usually, this is the IP address or DNS name of the master node. Do this for all available cluster node connections, for example, if you have three cluster nodes, enter the address under which the second cluster node is reachable from the third cluster node in the field #3 =&gt; #2.</p> <p> For more information, see the Paessler website: <a href="#">How to set up a failover cluster in PRTG in 6 steps.</a></p> <p> If you use <a href="#">remote probes</a> outside your local network or outside your network address translation (NAT), make sure that the IP addresses or DNS names that you enter are valid for both the cluster nodes to reach each other and for remote probes to reach all cluster nodes individually. These addresses must not be private and must be reachable from the outside, otherwise the remote probes cannot connect.</p> <p> Multi-platform probes do not support clusters.</p>

 Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

 For more information on how to set a cluster node into Maintenance Mode, see section [Cluster Status](#).

 The entire setup process for a cluster requires several different steps. For more information and step-by-step guidance, see the Paessler website: [How to set up a failover cluster in PRTG in 6 steps.](#)

## More

### KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

### PAESSLER WEBSITE

How to set up a failover cluster in PRTG in 6 steps

- <https://www.paessler.com/support/how-to/failover-cluster>

## Others


There are some settings that you must define in the [PRTG Administration Tool](#)<sup>[3040]</sup>. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#)<sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#)<sup>[3067]</sup>

### 8.12.2.9 Single Sign-On

On the Single Sign-On tab, you can select a single sign-on (SSO) provider and configure other related settings.

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

 If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.

## Requirements and Restrictions

SSO has the following requirements and restrictions.

 For more information, see also section [Notes](#)<sup>[2930]</sup>.

Requirement/Restriction	Description
SSO configuration	<p>You must first configure Microsoft Entra ID or Okta accordingly before you can integrate it into PRTG or PRTG Hosted Monitor for SSO. For example, you must register PRTG as an application.</p> <ul style="list-style-type: none"> <li>▪ For more information, see the Knowledge Base: <a href="#">How to integrate Microsoft Entra ID into PRTG?</a></li> <li>▪ For more information, see the Knowledge Base: <a href="#">How to integrate Microsoft Entra ID into PRTG Hosted Monitor?</a></li> <li>▪ For more information, see the Knowledge Base: <a href="#">How to integrate Okta SSO into PRTG?</a></li> </ul>
Freeware edition	<ul style="list-style-type: none"> <li>▪ SSO is not available for the <a href="#">freeware edition</a><sup>[20]</sup>.</li> </ul>
SSO users	<ul style="list-style-type: none"> <li>▪ Do not have access to the <a href="#">PRTG API</a><sup>[3084]</sup>.</li> <li>▪ Cannot log on to a failover node in a cluster.</li> <li>▪ Cannot change the Login Name in PRTG.</li> </ul>

## Single Sign-On Settings

**Single Sign-On Settings**

SSO Login <sup>?</sup>  Disable (default)   
  Enable

Provider <sup>?</sup> Microsoft Entra ID ▼

Configuration Endpoint <sup>?</sup>    
 Load Configuration

Authorization Endpoint <sup>?</sup>

Token Endpoint <sup>?</sup>

JSON Web Key Set (JWKS) URI <sup>?</sup>

Issuer <sup>?</sup>

Scope <sup>?</sup>

Application (Client) ID <sup>?</sup>

Client Secret <sup>?</sup>

Group Claim Retrieval <sup>?</sup>  Access token (default)   
  GraphQL

Endpoint Handling <sup>?</sup>  Select from a list of endpoints (default)   
  Manually enter a URL

Available Callback URLs <sup>?</sup>  Callback URLs

Test Single Sign-On Authorization Endpoint <sup>?</sup> Test Single Sign-On Authorization Endpoint

Single Sign-On Settings

Setting	Description
SSO Login	Define if you want to enable login via SSO: <ul style="list-style-type: none"> <li>▪ Disable (default)</li> <li>▪ Enable</li> </ul>
Provider	<b>This setting is only visible if you select Enable above.</b> Select an SSO provider from the dropdown list: <ul style="list-style-type: none"> <li>▪ Microsoft Entra ID: Use Microsoft Entra ID as the SSO provider.</li> <li>▪ Okta: Use Okta as the SSO provider.</li> </ul>
Configuration Endpoint	<b>This setting is only visible if you select Enable above.</b>

Setting	Description
	<p>Enter the configuration endpoint URL.</p> <p><b>i</b> Click Load Configuration to automatically fill in the values for Authorization Endpoint, Token Endpoint, JSON Web Key Set (JWKS) URI, and Issuer. If this does not work, then manually enter the values.</p> <p>Microsoft Entra ID URL format example:</p> <pre>https://login.microsoftonline.com/&lt;tenant-ID&gt;/v2.0/.well-known/openid-configuration</pre> <p><b>i</b> Make sure to replace &lt;tenant-ID&gt; with the <a href="#">directory (tenant) ID</a> from Microsoft Entra ID.</p> <p>Okta URL format example:</p> <pre>https://&lt;your-Okta-domain&gt;/oauth2/&lt;authorization-server-ID&gt;/well-known/oauth-authorization-server</pre> <p><b>i</b> You can find the URL in the field <a href="#">Metadata URI</a> under Security   API in the Okta administrator console.</p>
<p>Authorization Endpoint</p>	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Enter the entire endpoint URL for authorization purposes, not only the server part.</p> <p>Microsoft Entra ID example:</p> <pre>https://login.microsoftonline.com/&lt;tenant-ID&gt;/oauth2/v2.0/authorize</pre> <p><b>i</b> Make sure to replace &lt;tenant-ID&gt; with the <a href="#">directory (tenant) ID</a> from Microsoft Entra ID.</p> <p>Okta example:</p> <pre>https://&lt;your-Okta-domain&gt;/oauth2/default/v1/authorize</pre> <p><b>i</b> Make sure to replace &lt;your-Okta-domain&gt; with the <a href="#">Okta domain</a> of your application from the Okta administrator console.</p>
<p>Token Endpoint</p>	<p><a href="#">This setting is only visible if you select Enable above.</a></p> <p>Enter the entire token endpoint URL, not only the server part.</p> <p>Microsoft Entra ID example:</p> <pre>https://login.microsoftonline.com/&lt;tenant-ID&gt;/oauth2/v2.0/token</pre> <p><b>i</b> Make sure to replace &lt;tenant-ID&gt; with the <a href="#">directory (tenant) ID</a> from Microsoft Entra ID.</p> <p>Okta example:</p>

Setting	Description
	<pre>https://&lt;your-Okta-domain&gt;/oauth2/default/v1/token</pre> <p><b>i</b> Make sure to replace &lt;your-Okta-domain&gt; with the <b>Okta domain</b> of your application from the Okta administrator console.</p>
<p>JSON Web Key Set (JWKS) URI</p>	<p><b>This setting is only visible if you select Enable above.</b></p> <p>Enter the URI of the JWKS, not only the server part.</p> <p>Microsoft Entra ID example:</p> <pre>https://login.microsoftonline.com/&lt;tenant-ID&gt;/discovery/v2.0/keys</pre> <p><b>i</b> Make sure to replace &lt;tenant-ID&gt; with the <b>directory (tenant) ID</b> from Microsoft Entra ID.</p> <p>Okta example:</p> <pre>https://&lt;your-Okta-domain&gt;/oauth2/default/v1/keys</pre> <p><b>i</b> Make sure to replace &lt;your-Okta-domain&gt; with the <b>Okta domain</b> of your application from the Okta administrator console.</p>
<p>Issuer</p>	<p><b>This setting is only visible if you select Enable above.</b></p> <p>Enter the SSO issuer.</p> <p>Microsoft Entra ID example:</p> <pre>https://login.microsoftonline.com/&lt;tenant-ID&gt;/v2.0</pre> <p><b>i</b> Make sure to replace &lt;tenant-ID&gt; with the <b>directory (tenant) ID</b> from Microsoft Entra ID.</p> <p>Okta example:</p> <pre>https://&lt;your-Okta-domain&gt;/oauth2/default</pre> <p><b>i</b> Make sure to replace &lt;your-Okta-domain&gt; with the <b>Okta domain</b> of your application from the Okta administrator console.</p>
<p>Scope</p>	<p><b>This setting is only visible if you select Enable above.</b></p> <p>Enter the scope for SSO.</p> <p>Microsoft Entra ID example:</p> <pre>openid profile offline_access email api://&lt;client-ID&gt;/&lt;scope-name&gt;</pre> <p><b>i</b> Make sure to replace &lt;client-ID&gt; with the <b>application (client) ID</b> from Microsoft Entra ID and the &lt;scope-name&gt; with a scope name.</p> <p>Okta example:</p> <pre>openid offline_access email profile</pre>

Setting	Description
Application (Client) ID	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Enter the <a href="#">application (client) ID</a> from Microsoft Entra ID or the <a href="#">Client ID</a> of your application from the Okta administrator console.</p>
Client Secret	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Enter the client secret to verify the integrity of the SSO token.</p>
Group Claim Retrieval	<p>This setting is only visible if you select <a href="#">Microsoft Entra ID above</a>.</p> <p>Select if you want to use an access token or GraphQL to retrieve the group claims from <a href="#">Microsoft Graph</a>:</p> <ul style="list-style-type: none"> <li>▪ Access token (default)</li> <li>▪ GraphQL</li> </ul> <p><b>i</b> If you select GraphQL to retrieve the group claims, PRTG automatically adds <a href="#">user.read</a> to the scope.</p> <p><b>i</b> If you select GraphQL and log in for the first time, a window opens and asks for the needed permissions. Click <a href="#">Accept</a> to grant the permissions.</p>
Endpoint Handling	<p>This setting is only visible if you select <a href="#">Enable above</a>.</p> <p>Define whether to select the callback from a list of callbacks or to manually enter a callback:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Select from a list of endpoints (default)</a>: Select an endpoint from a list of available endpoints.</li> <li>▪ <a href="#">Manually enter a URL</a>: Manually enter an endpoint URL below. <ul style="list-style-type: none"> <li><b>i</b> You need to enter a manual callback if you access PRTG via a different DNS name. For example, if you access PRTG via <a href="#">myPRTG.example.com</a> but the actual DNS name of the PRTG core server is <a href="#">myPRTG.internal.example.com</a>, you need to enter a manual callback.</li> </ul> </li> </ul>
Available Callback URLs	<p>This setting is only visible if you select <a href="#">Enable and select Select from a list of endpoints (default) above</a>.</p> <p>This list shows the available callbacks of this PRTG instance. Select the callbacks that your users use to connect to PRTG.</p> <p><b>i</b> If you define an HTTPS endpoint in this field, you need to configure the HTTPS endpoint as a valid redirection URI in your SSO provider's settings.</p>

Setting	Description
External Callback URL	<p>This setting is only visible if you select <b>Enable</b> and select <b>Manually enter a URL</b> above.</p> <p>If you access PRTG via a different DNS name, define the HTTPS endpoint.</p> <p>This is necessary if the DNS name that you configured under <b>Setup   System Administration   User Interface</b> does not appear in the <b>Available Callback URLs</b> list. For example, if you access PRTG via <a href="#">myPRTG.example.com</a> but the actual DNS name of the PRTG core server is <a href="#">myPRTG.internal.example.com</a>, then enter <a href="#">myPRTG.example.com</a>. Also make sure to add the port used by PRTG for HTTPS and the endpoint in the URL, for example: <a href="#">myPRTG.example.com:PORT/cb</a>.</p> <p><b>i</b> If you define an HTTPS endpoint in this field, you need to configure the HTTPS endpoint as a valid redirection URI in your SSO provider's settings.</p>
Available Callback URLs (for reference)	<p>This setting is only visible if you select <b>Enable</b> and select <b>Manually enter a URL</b> above.</p> <p>This list shows the available callbacks URLs of this PRTG instance for reference purposes.</p>
Test Single Sign-On Authorization Endpoint	<p>Click <b>Test Single Sign-On Authorization Endpoint</b> to call the <a href="#">authorization</a> endpoint to check if starting the single sign-on process will succeed.</p> <p><b>i</b> In case of errors, check the answer from the endpoint.</p>

**i** Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

## Notes

- If you want to further improve the security for sign-in events, we recommend that you enable multi-factor authentication for Microsoft Entra ID or Okta.
  - For more information, see the Knowledge Base: [How can I enable Microsoft Entra ID multifactor authentication?](#)
  - For more information, see the Knowledge Base: [How can I enable Okta multi-factor authentication?](#)
- When an SSO user [logs in to the PRTG web interface](#)<sup>153</sup>, PRTG automatically creates a corresponding local account on the PRTG core server.



- By default, no access rights for monitoring objects, libraries, maps, or reports are set for the new user group in PRTG. This is why, initially, users in this user group do not see monitoring objects, libraries, maps, or reports. This does not apply if the new user group has administrative rights. Edit the monitoring [object's settings](#)<sup>[201]</sup> and the settings of libraries, maps, and reports, and set access rights for the newly created user group in the respective Access Rights section.
  - ❗ We recommend that you set these access rights in the [root group settings](#)<sup>[453]</sup> and use the [inheritance of settings](#)<sup>[136]</sup>.
- A local user account for an SSO user is only created if this SSO user has successfully logged in to PRTG. If you want to send [email notifications](#)<sup>[2815]</sup> to an SSO group in PRTG, using the option Send to User Group in the notification settings, a member of this SSO group must log in to PRTG at least once to receive email notifications. To avoid this, enter the email address of the SSO group in the Send to Email Address field in the notification settings and select None for the Send to User Group option.
- If you want to delete an SSO group from PRTG, you must delete all users that are in this user group first. This is because SSO users always have this user group set as their primary group, and user accounts cannot be without a primary group.
- If a license is not valid, is temporarily unavailable, or is being updated, SSO does not work during this time.

## More

### KNOWLEDGE BASE

How to integrate Microsoft Entra ID into PRTG?

- <https://kb.paessler.com/en/topic/88527>

How to integrate Microsoft Entra ID into PRTG Hosted Monitor?

- <https://kb.paessler.com/en/topic/91634>

How to integrate Okta SSO into PRTG?

- <https://kb.paessler.com/en/topic/90482>

How can I enable Microsoft Entra ID multifactor authentication?

- <https://kb.paessler.com/en/topic/89808>

How can I enable Okta multi-factor authentication?

- <https://kb.paessler.com/en/topic/91187>

## Others

There are some settings that you must define in the [PRTG Administration Tool](#)<sup>[3040]</sup>. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#)<sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#)<sup>[3067]</sup>

### 8.12.2.10 Maintainer Mode

Use the Maintainer Mode to pause and resume devices or check the status of devices without an active user session or user account.

## Maintainer Mode Settings

Maintainer Mode Settings

Maintainer Mode ?

Disable (default)

Enable

Maintainer Mode Settings

Setting	Description
Maintainer Mode	Define if you want to enable Maintainer Mode: <ul style="list-style-type: none"> <li>▪ Disable (default)</li> <li>▪ Enable</li> </ul>
Access Key	<p style="color: #0070C0;">This setting is only visible if you select Enable above.</p> <p>Shows the access key that you need for the API for authentication purposes.</p> <p><span style="font-size: 0.8em;">?</span> The access keys are URL friendly.</p>
Generate new access key	<p style="color: #0070C0;">This setting is only visible if you select Enable above.</p> <p>Enable the check box next to Generate new access key, click Save, and reload the page to generate a new access key.</p>

## Maintainer Mode API Endpoints and Parameters

You can execute the following actions by using the following endpoints:

### 1. Query Device Status

Endpoint	Parameter	Description
\api\public\maintainer_querydevicestatus.htm	NodeID	Use this parameter to define the object ID of the device of which you want to query the status. Enter an integer. <p><span style="font-size: 0.8em;">?</span> You can find the object ID in the info box on the Overview tab of the device.</p>
	accesskey	Use this parameter to define the access key that you need for the API for authentication purposes. Enter a string.

Example

```
https://yourserver/api/public/maintainer_querydevicestatus.htm?
nodeid=deviceID&accesskey=myaccesskey
```

2. Pause Device


Endpoint	Parameter	Description
\api\public\maintainer_pausedevice.htm	NodeID	Use this parameter to define the object ID of the device of which you want to query the status. Enter an integer.  <b>i</b> You can find the object ID in the info box on the Overview tab of the device.
	accesskey	Use this parameter to define the access key that you need for the API for authentication purposes. Enter a string.
	name	Use this parameter to define a name for the user that pauses the device. Enter a string.  <b>i</b> The name appears in the status on the Overview tab of the device.
	comment	Use this parameter to define a comment for the paused device. Enter a string.  <b>i</b> The comment appears in the status on the Overview tab of the device.

Example

```
https://yourserver/api/public/maintainer_pausedevice.htm?
nodeid=deviceID&accesskey=myaccesskey&name=myname&comment=mycomment
```

3. Resume Device

Endpoint	Parameter	Description
\api\public\maintainer_resumedevice.htm	NodeID	Use this parameter to define the object ID of the device of which you want to query the status. Enter an integer.  <b>i</b> You can find the object ID in the info box on the Overview tab of the device.

Endpoint	Parameter	Description
	accesskey	Use this parameter to define the access key that you need for the API for authentication purposes. Enter a string.
	name	Use this parameter to define a name for the user that resumes the device. Enter a string.   The name appears in the log on the Log tab of the device.

### Example

```
https://yourserver/api/public/maintainer_resumedevice.htm?
nodeid=deviceID&accesskey=myaccesskey&name=myname
```

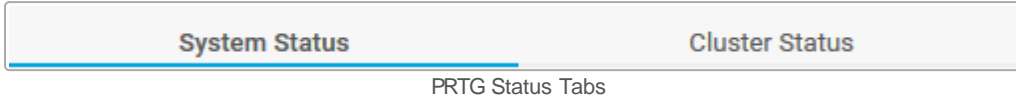
### Others

There are some settings that you must define in the [PRTG Administration Tool](#)<sup>[3040]</sup>. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#)<sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#)<sup>[3067]</sup>

## 8.12.3 PRTG Status

To view the status of your PRTG installation, select Setup | PRTG Status from the [main menu bar](#)<sup>[249]</sup>. Select the various tabs to change the different settings.



In this section:

- [System Status](#)<sup>[2935]</sup>
- [Cluster Status](#)<sup>[2960]</sup>

### 8.12.3.1 System Status

On the System Status tab, you can view relevant system information. Furthermore, this page shows interesting usage statistics. Use the quick links for fast access to status information.

**i** You might need this data for debugging or when you contact the Paessler support team. They ask you in some cases to provide system status information to analyze any issues with PRTG.

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.











**☁** If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.



Quick Links

In this section:

- [Software Version and Server Information](#)<sup>[2936]</sup>
- [License Information](#)<sup>[2937]</sup>
- [System Startup Log](#)<sup>[2939]</sup>
- [System Warnings](#)<sup>[2940]</sup>
- [Cluster Status](#)<sup>[2940]</sup>
- [Local Status](#)<sup>[2941]</sup>
- [Cluster Connections](#)<sup>[2942]</sup>
- [PRTG Core Server System Memory](#)<sup>[2943]</sup>
- [Thread Information](#)<sup>[2946]</sup>

- [Activity History](#) 
- [Auto-Discovery Tasks](#) 
- [Background Tasks](#) 
- [Database Objects](#) 
- [Sensors Sorted by Impact on System Performance](#) 
- [Sensors Sorted by Interval](#) 
- [Probes](#) 
- [System Settings](#) 
- [Web Server Activity](#) 
- [Synchronization](#) 






## Software Version and Server Information

This section shows information about the software version and the PRTG core server system.

Software Version And Server Information	
<b>PRTG Version</b>	PRTG Network Monitor 23.3.88.1421 x64
<b>Auto-Update Status</b>	Version 23.3.88.1421 successfully installed
<b>Operating System</b>	Microsoft Windows 10 Enterprise (10.0 Build 19045), 2 CPUs (Double x64 Model 106 Step 6), code page "Windows-1252", on VMware
<b>Server Time</b>	06/10/2023 18:28:49 (W. Europe Standard Time)
<b>Server CPU Load</b>	1%
<b>User Name</b>	PRTG System Administrator
<b>Active User Sessions</b>	PRTG System Administrator
<b>Browser</b>	Mozilla Firefox (Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/115.0)

Software Version and Server Information

Category	Description
PRTG Version	Shows the exact build version of the PRTG installation.
Auto-Update Status	Shows the latest auto-update message available from the <a href="#">auto-update</a>  . For example, the message indicates that an update was successfully installed.  ☁ This information is not displayed in PRTG Hosted Monitor.

Category	Description
Operating System	<p>Shows the exact Windows version, build, and service packs, the number and kind of CPUs, and the computer name of the PRTG core server system.</p> <ul style="list-style-type: none"> <li> If you run PRTG in a cluster, this shows information for the system of the cluster node you are logged in to.</li> <li> If you run PRTG on virtual systems, some of the information might not be available.</li> <li> This information is not displayed in PRTG Hosted Monitor.</li> </ul>
Server Time	<p>Shows the date and time of the PRTG core server system.</p> <ul style="list-style-type: none"> <li> If you run PRTG in a cluster, this shows information for the system of the cluster node you are logged in to.</li> </ul>
Server CPU Load	<p>Shows the CPU load of the PRTG core server system.</p> <ul style="list-style-type: none"> <li> If you run PRTG in a cluster, this shows information for the system of the cluster node you are logged in to.</li> </ul>
User Name	<p>Shows the <a href="#">user name</a>  of the user account that you are logged in to PRTG with.</p>
Active User Sessions	<p>Shows the user names of all user accounts that are logged in to PRTG.</p> <ul style="list-style-type: none"> <li> When a user account logs out, it takes up to 1 minute until the user name disappears.</li> </ul>
Browser	<p>Shows the name and user agent string of the browser that you are viewing this page with.</p>







## License Information

This section shows information about your license.



## License Information

License Status	Activation was successful
License Name	Example Organization
License Key	P10000-FFSEJ3-ZHGRD5-UR1CS9-U73FG2-G645F1-YVF1D0-H83234
System ID	SYSTEMID-AAAA1111-BBBB2222-3333CCCC-4444DDDD-5555EEEE
Customer ID	012345678
Licensed Edition	PRTG Network Monitor (next validation on 15/3/2024 at the latest)
Last Update	13/06/2024 11:06:54
Subscription until	07/05/2027 (1059 days left)
Number of Sensors	Unlimited

License Information


Setting	Description
License Status	<p>Shows the activation status of this PRTG installation. Usually, PRTG automatically completes the activation during installation or when you change your license information.</p> <p> If PRTG cannot directly connect to the internet, a manual activation is necessary.</p> <p> For more information, see section <a href="#">Activate the Product</a><sup>[104]</sup>.</p>
License Name	<p>Shows the owner of the <a href="#">license</a><sup>[102]</sup> that you use for this PRTG installation, for example <a href="#">ExampleOrganization</a>.</p> <p> The License Name, license key, and system ID make up your license information.</p> <p> You can find the label License Owner in some documents from the Paessler Portal. License Owner is the same as License Name. PRTG might ask you for this information during installation or when you <a href="#">change your license key</a><sup>[102]</sup>.</p>
License Key	<p>Shows the <a href="#">license</a><sup>[102]</sup> key that you use for this PRTG installation.</p> <p> The License Name, license key, and system ID make up your license information.</p>
System ID	<p>The system ID is a fixed value that is automatically assigned to a PRTG installation.</p> <p> The License Name, license key, and system ID make up your license information.</p>



Setting	Description
Customer ID	<p>This setting is only visible if you have a subscription license.</p> <p>Shows the customer ID of the license that you use for this PRTG installation.</p>
Customer ID	<p>This setting is only visible if you have a subscription license.</p> <p>Shows the customer ID of the license that you use for this PRTG installation.</p>
Licensed Edition	<p>Shows the license that you use for this PRTG installation. This determines how many sensors you can use in PRTG.</p> <p> PRTG regularly validates subscription licenses. You can see the next validation date here.</p>
Last Update	<p>Shows the date of the last update for this PRTG installation. We recommend that you use the <a href="#">auto-update</a><sup>2969</sup>.</p>
Subscription until / Maintenance until	<p>Shows the expiration date and the number of days that remain for your active maintenance or subscription. Manage your license at the <a href="#">Paessler Portal</a> for continued access to any available updates and to our premium email support.</p>
Number of Sensors	<p>Shows the number of sensors that you can use in PRTG. If you reach the limit, PRTG automatically sets each new sensor that you add to the Paused <a href="#">status</a><sup>181</sup>.</p> <p>Editions that allow an <b>unlimited</b> number of sensors do not restrict the number of possible sensors by license, so you can create sensors until you reach the <a href="#">performance limit</a><sup>27</sup>. This means that you can use about 10,000 sensors per PRTG core server. However, this number depends on the performance of the PRTG core server system, and sensors and scanning intervals.</p> <p> For more information, see section <a href="#">System Requirements</a><sup>22</sup>.</p>

## System Startup Log

This section shows the log information that was created during the last startup of the PRTG core server.

 If you run PRTG in a cluster, this shows information for the system of the cluster node you are logged in to.

## System Startup Log

```
07:42:52 Initializing License
07:42:52 Initialize License: OK
07:42:56 - 0% - Starting PRTG Core Server (07/07/2021)
07:42:56 - 1% - Read Basic OSK Definitions: OK
07:42:56 - 2% - Read Template Defaults: OK
07:43:03 - 3% - Initialize Sensor Types: OK
07:43:03 - 4% - Initializing Help System
07:43:35 - 5% - Load Configuration: Reading File
07:43:36 - 10% - Load Configuration: Parsing Data
07:43:38 - 25% - Load Configuration: OK
07:43:39 - 29% - Load Lookups: OK
07:43:39 - 30% - Initialize System Options: OK
07:43:39 - 36% - Start Notification Manager: OK
07:43:40 - 37% - Load MIBs: OK
07:43:40 - 40% - Check Database Integrity: OK
07:43:40 - 41% - Initialize RawData Store: OK
07:43:40 - 43% - Initialize Probes: OK
07:43:40 - 45% - Initialize DataSync: OK
07:43:40 - 47% - Initialize Schedules: OK
07:43:40 - 50% - Preload Graph Cache
07:43:40 - 60% - Preload Graph Cache 269/269
07:43:40 - 75% - Scan For Last Data: 119/119
07:43:41 - 80% - Initialize Background Tasks: OK
07:43:43 - 82% - Initialize Cluster: OK
07:43:43 - 85% - Initialize Notification Engine: OK
07:43:43 - 90% - Initialize Sensor States: OK
07:43:43 - 98% - Starting PRTG Core Engine
07:43:43 - 100% - PRTG Core Server is Running
```

System Startup Log

## System Warnings

This section shows if there are any warnings. Usually, you see [None](#).

### System Warnings

None

System Warnings

## Cluster Status

This setting is only visible if you have a [failover cluster](#)<sup>[128]</sup>. This section shows all of your cluster nodes.

## Cluster Status

**Node 1: PRTG Network Monitor Primary Node (Current Master)**  
⇒ Failover Node (192.0.2.1, Connected)

**Node 2: Failover Node Secondary Node (Failover Node)**  
⇒ PRTG Network Monitor (192.0.2.0, Connected)

Cluster Status

Category	Description
Node x	Shows the name and type of the cluster node (primary node or secondary node) and its status (current master node or failover node). It also shows all connections from this cluster node to the other cluster nodes.  ■ For more information, see section <a href="#">Cluster Status</a> <sup>2960</sup> .

## Local Status

This setting is only visible if you have a [failover cluster](#) <sup>128</sup>. This section shows information about the cluster node that you are logged in to.

## Local Status

Server State: PRTG Network Monitor: Current Master  
Cluster Messages:  
Number: 1943, NumberFast: 2, Received: 0, Init: 0, Tree: 0, Update: 0, Data: 0, File: 0, State: 0, Processed: 0, Broadcast: 1945, Broadcast Sent: 0

Local Status

Category	Description
Server State	Shows the name of the cluster node and its status (current master node or failover node).
Cluster Messages	Shows internal summary information about the cluster node and the communication between the cluster nodes. You might be asked about this by the Paessler support team.

## Cluster Connections

This setting is only visible if you have a [failover cluster](#)<sup>[128]</sup>. This section shows information about the connections between the cluster nodes.

### Cluster Connections

State of Local Node: Treeversion: 154926376807  
 Server Volume: 0 KB  
 State of cluster members:  
 Node: **PRTG Network Monitor**  
 State CRC: 1497873791  
 KeepAlive: 04.05.2023 13:25:48  
 Buffer: 0  
 Remote IP: 192.0.2.0  
 Node: **Failover Node**  
 State CRC: 0  
 KeepAlive: 04.05.2023 13:25:49  
 Buffer: 0  
 Remote IP: 192.0.2.1

Message state of cluster members:  
**Failover Node {11111111-2222-3333-4444-5555555555}**  
 Connected  
 Connects: 1  
 Disconnects: 0  
 Sent: 11  
 Received: 0  
 Volume: 0  
 Buffer: 0

Cluster Connections

Category	Description
State of Local Node	Shows the treeversion and size of the server volume, both types of internal system information.
State of Cluster Members	Shows the name and IP address, a state cyclic redundancy check (CRC) code, the time stamp of the last "keep alive" signal, the size of the buffer, and the remote IP address of each cluster node.
Message State of Cluster Members	Shows the name and unique identifier, the connection state, and statistics about the cluster message system of each cluster node.

## PRTG Core Server System Memory

This section shows machine-oriented information regarding the memory usage of the PRTG core server system.

- ① If you run PRTG in a cluster, this shows information for the system of the cluster node you are logged in to.

## PRTG Core Server System Memory

Committed	1280 KB
Allocated	85 KB
Unused	1107 KB
Free Physical	8070072 KB
Total Physical	16476968 KB
Free Pagefile	7957900 KB
Total Pagefile	18967336 KB
Free Virtual	137430213588 KB
Total Virtual	137438953344 KB
Free Effective	7957900 KB
Object Count	515
BaseInstance	275 KByte
BaseAccess	33 KByte
BaseHistory	103 KByte
BaseCurrent	17738 KByte
BaseData	7663 KByte
BaseChannel	18614 KByte
BaseTrigger	75 KByte
BaseIDs	0 KByte
BaseLookup	9 KByte
BaseCheck	27 KByte
BaseDeplist	11 KByte
Datasets	27719 KByte
State	1219 KByte
Interface	1480 KByte
IndexCache	31 KByte
TreeTotal	75005 KByte
DatasetCache	0 KByte (0)
StorageSystem	2888 KByte
Sessions	0 KB (1)
StateObjects	1 #
Cluster Messages	0 KByte (0)
Cluster Change	0 KByte (0)
Cluster Stateupdate	0 KByte (0)

Category	Description
Committed	The amount of memory that your system commits to the PRTG core server system.
Allocated	The amount of memory that the PRTG core server system is currently using.
Unused	The amount of allocated memory that the PRTG core server system is currently not using.
Free Physical	The amount of free memory that is currently available in the physical memory of the PRTG core server system.
Total Physical	The total amount of memory that is provided by the physical memory of the PRTG core server system.
Free Pagefile	The amount of free memory that is currently available in your system's pagefile(s).
Total Pagefile	The total amount of memory of your system's pagefile(s).
Free Virtual	The amount of free memory that is available in the virtual memory of the PRTG core server system.
Total Virtual	The total amount of memory of the virtual memory of the PRTG core server system.
Free Effective	The effective amount of free memory on your PRTG core server system. This corresponds to Free Pagefile.
Object Count	The number of PRTG-internal data structures, also known as tree nodes, for example, the number of sensors, users, and reports.
BaseInstance	The amount of memory that is used for the tree node <a href="#">Instance</a> .
BaseAccess	The amount of memory that is used for the tree node <a href="#">Access Rights</a> .
BaseHistory	The amount of memory that is used for the tree node <a href="#">History of Configuration Changes</a> .
BaseCurrent	The amount of memory that is used for the tree node <a href="#">Current Configuration Information</a> .
BaseData	The amount of memory that is used for the tree node <a href="#">Configuration Data</a> .

Category	Description
BaseChannel	The amount of memory that is used for the tree node <a href="#">Channel Settings</a> .
BaseTrigger	The amount of memory that is used for the tree node <a href="#">Trigger</a> .
BaseIDs	The amount of memory that is used for the tree node <a href="#">IDs</a> .
BaseLookup	The amount of memory that is used for the tree node <a href="#">Sensor Lookups</a> .
BaseCheck	The amount of memory that is used for the tree node <a href="#">Check Requests</a> .
BaseDeplist	The amount of memory that is used for the tree node <a href="#">Dependency List</a> .
Datasets	The amount of memory that is currently used for datasets, like for graphs.
State	The amount of memory that is currently used for user-specific datasets.
Interface	The amount of memory that is currently used for tree node-specific table objects.
IndexCache	The amount of memory that is currently used for the index dataset cache that is particularly important in a cluster.
TreeTotal	The total amount of memory that is used by the PRTG tree.
DatasetCache	The amount of memory that is currently used for the dataset cache, in particular regarding historic data. In parentheses, you see the number of datasets that are saved in the cache.
StorageSystem	The amount of memory space that is currently used for the storage system.
Sessions	The amount of memory that is currently used for sessions. A user can activate more than one session. In parentheses, you see the number of currently activated sessions.
StateObjects	The number of user-specific state objects that are found in the memory of the PRTG core server system.

## Thread Information

The section shows machine-oriented information regarding threads that are running on the PRTG core server system.



**i** If you run PRTG in a cluster, this shows information for the system of the cluster node you are logged in to.

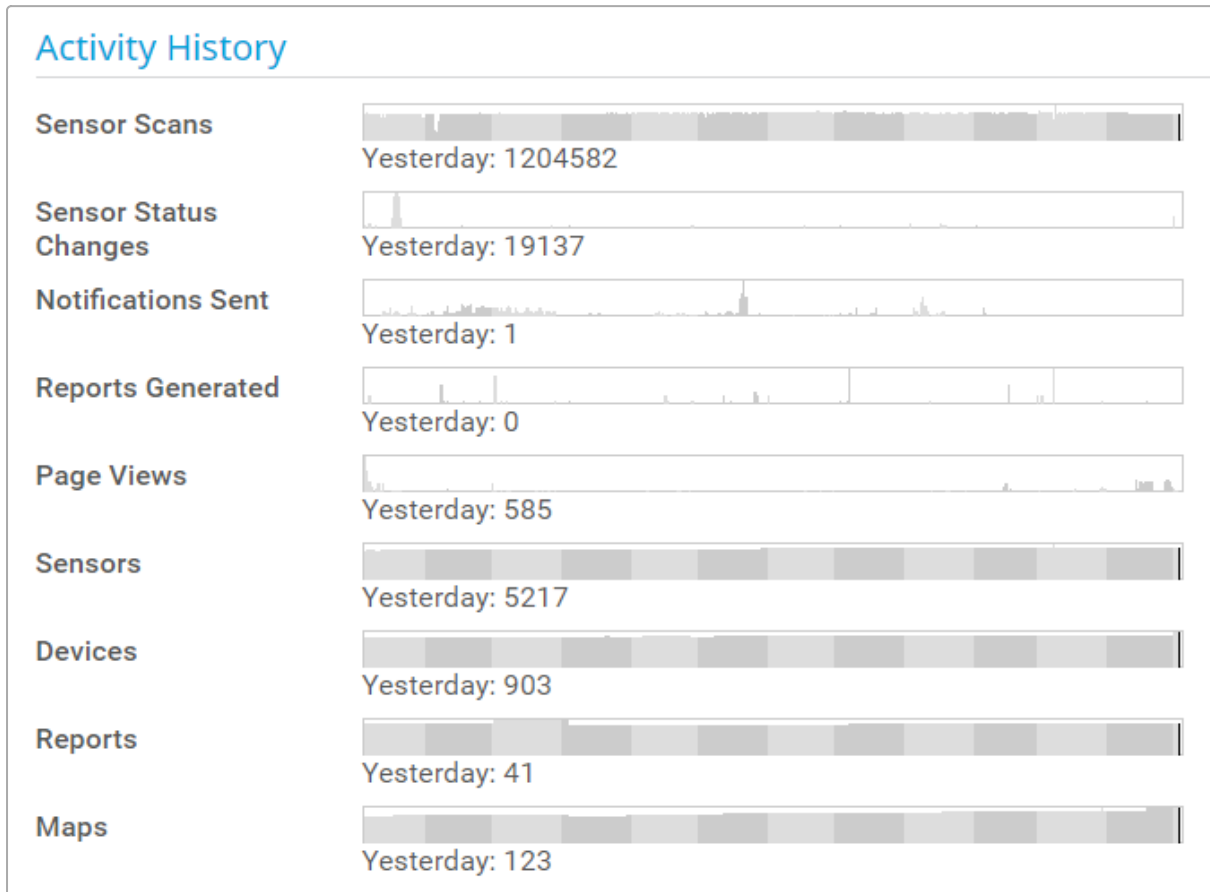
### Thread Information

StateObjectUpdate(1) 0	#8132 0,14 sec Running
StateObjectUpdate(1) 1	#8136 0,11 sec Running
StateObjectUpdate(1) 2	#8140 0,02 sec Running
StateObjectUpdate(2) 0	#8144 0,09 sec Running
StateObjectUpdate(2) 1	#8148 0,19 sec Running
StateObjectUpdate(2) 2	#8152 0,13 sec Running
EventStorage	#8568 0,00 sec Running
SystemMain	#8008 1,41 sec Running
NotificationManager	#17340 1,53 sec Running
FactoryManager	#17368 0,00 sec Running
RawDataManager	#17500 3,13 sec Running
ProbeManager	#17360 0,19 sec Running
DataCalc (1)	#17388 0,00 sec Running
ScheduleManager	#17376 4,17 sec Running
DataCalc (0)	#17384 0,00 sec Running
DataSynchronizer	#17372 0,33 sec Running
DependencyManager	#17380 0,31 sec Running
BackgroundManager	#17472 0,16 sec Running
DataCalc (2)	#17392 0,00 sec Running
ClusterManager	#17488 0,91 sec Running
CorrelationAnalyzer	#17512 170,44 sec Running
ClientConnectionManager	#17712 0,00 sec exit=0
ClusterConnectionManager	#17716 0,00 sec exit=0
ClientConnectionManager	#15724 0,02 sec Running
ClusterConnectionManager	#15908 0,03 sec Running

Thread Information

## Activity History

This section shows how busy PRTG was for you in the past. The graphs indicate the number of activities in the last 365 days. Below the graphs, you see statistics about the past day.



Activity History

Category	Description
Sensor Scans	Shows how often all <a href="#">sensors</a> <sup>[134]</sup> refreshed their data in the past.
Sensor Status Changes	Shows how often the <a href="#">sensor states</a> <sup>[187]</sup> changed in the past.
Notifications Sent	Shows how many <a href="#">notifications</a> <sup>[2735]</sup> PRTG sent out in the past.
Reports Generated	Shows how many <a href="#">reports</a> <sup>[2754]</sup> PRTG created in the past.
Page Views	Shows how often pages in the PRTG web interface were opened in the past.
Sensors	Shows how many sensors existed in the past.

Category	Description
Devices	Shows how many <a href="#">devices</a> <sup>1341</sup> existed in the past.
Reports	Shows how many reports existed in the past.
Maps	Shows how many <a href="#">maps</a> <sup>2776</sup> existed in the past.

## Auto-Discovery Tasks

This section shows information on the [auto-discovery](#) <sup>254</sup>.

Auto-Discovery Tasks	
<b>Running Gateway/DHCP</b>	<b>1</b>

Auto-Discovery Tasks


Category	Description
Running	Shows the number of auto-discovery tasks that are running.  <b>i</b> A high number of auto-discovery tasks can negatively influence system performance.

## Background Tasks

This section shows information on background tasks.

Background Tasks	
<b>Historic Data</b>	done
<b>Toplist Buffer</b>	0
<b>Similar Sensors Detection</b>	status: currently suspended, setting: Manage automatically based on sensor count (recommended)
<b>Recommended Sensors Detection</b>	engine enabled, nothing to do

Background Tasks

Category	Description
Historic Data	Shows if PRTG is recalculating the historic data cache in the background. If so, you see the tasks to do until done. Usually, PRTG does this calculation after every PRTG core server restart.
Toplist Buffer	Shows the size of the Toplist buffer. When you use <a href="#">Flow (NetFlow, jFlow, sFlow, IPFIX)</a> <sup>[6011]</sup> or <a href="#">Packet Sniffer</a> <sup>[6009]</sup> sensors, PRTG stores Toplist data. The data stream received is buffered and written to the data directory of the PRTG core server system.   Depending on the number and size of the data stream as well as the hard disk and system performance of the PRTG core server system, the buffer size can rise. When the buffer size reaches <b>500</b> , PRTG drops Toplist data, which can lead to incorrect Toplist values for the sensors.
Similar Sensors Detection	Shows the status and the selected setting for the depth of the <a href="#">similar sensors</a> <sup>[192]</sup> analysis.
Recommended Sensors Detection	Shows the status of the detection engine and the tasks of the <a href="#">recommended sensors detection</a> <sup>[2874]</sup> .

## Database Objects

This section shows statistic information about your monitoring configuration. This information might be necessary when contacting the Paessler support team.

## Database Objects

Probes	4
Groups	584
Devices	903
Sensors	5217
Channels	24075
User Groups	10
Users	142
Notifications	32
Schedules	11
Maps	123
Libraries	21
Reports	41
Bitfield/Boolean/Integer/Range Lookups	1/241/3021/88
Requests/Second	16

Database Objects

Category	Description
Probes	Shows the total number of <a href="#">probes</a> <sup>[458]</sup> in the PRTG installation.
Groups	Shows the total number of <a href="#">groups</a> <sup>[526]</sup> in the PRTG installation.
Devices	Shows the total number of devices in the PRTG installation.
Sensors	Shows the total number of sensors in the PRTG installation.
Channels	Shows the total number of <a href="#">channels</a> <sup>[134]</sup> in the PRTG installation.
User Groups	Shows the total number of <a href="#">user groups</a> <sup>[2912]</sup> in the PRTG installation.
Users	Shows the total number of <a href="#">users</a> <sup>[2907]</sup> in the PRTG installation.
Notifications	Shows the total number of <a href="#">notifications</a> <sup>[2808]</sup> in the PRTG installation.

Category	Description
Schedules	Shows the total number of <a href="#">schedules</a> <sup>2846</sup> in the PRTG installation.
Maps	Shows the total number of created maps in the PRTG installation.
Libraries	Shows the total number of created <a href="#">libraries</a> <sup>2738</sup> in the PRTG installation.
Reports	Shows the total number of reports in the PRTG installation.
BitField/Boolean/Integer/Range Lookups	Shows the total number of used lookups by <a href="#">lookup type</a> <sup>6189</sup> .
Requests/Second	Shows a value that is calculated from the total number of sensors and the average scanning interval configured. This number indicates how many monitoring requests per second are sent from the probes to the devices in your network.  <i>i</i> There are no general guidelines on what a good value is here. This depends on the sensors that you use as well as on the performance of the probe system.

## Sensors Sorted by Impact on System Performance

This section shows all sensors that you use in your configuration in order of performance impact (from very low to very high). If the CPU load of the probe system is very high, you can see which sensors might be causing this issue. Consider the recommended number of sensors in the respective [sections](#) for sensors with a high or very high performance impact.

*i* In the list, internal short names are used for sensors instead of the official designations. You can find a list of all sensors and their internal IDs, among others, via [/sensorlist.htm](https://yourserver/sensorlist.htm), for example <https://yourserver/sensorlist.htm>.

*i* You can also see the performance impact of a sensor on the sensor's Overview tab or in the [Add Sensor](#) <sup>414</sup> dialog.

■ For an overview list of all sensors, including their performance impact, see section [Available Sensor Types](#) <sup>3232</sup>.

### Sensors Sorted By Impact On System Performance

<b>Very low</b>	1x clusterstate, 2x commonsaas, 2x corestate, 1x corestateautonomous, 6x dns, 100x ping, 2x probestate, 24x snmptraffic, 3x snmpuptime, 7x ssl, 7x sslcertificate, 2x systemstate
<b>Low</b>	16x http, 61x remotedesktop, 1x smtp, 3x snmpcpu, 3x snmpdiskfree, 6x snmpmemory
<b>Medium</b>	
<b>High</b>	3x wmiantivirus, 3x wmidiskhealth, 4x wmidiskspace, 12x wmiologicaldiskv2, 3x wmiimemory, 4x wminetwork, 3x wmilogfile, 6x wmiphysicaldiskv2, 3x wmiprocessor, 3x wmiuptime
<b>Very high</b>	3x lastwindowsupdate

Sensors Sorted by Impact on System Performance

### Sensors Sorted by Interval

Shows all sensors used in your configuration in order of scanning interval. Choose reasonable scanning intervals for sensors that can affect the system performance. See the respective [sections](#) for sensors for more information.

**i** In the list, internal short names are used for sensors instead of the official designations. You can find a list of all sensors and their internal IDs, among others, via </sensorlist.htm>, for example <https://yourserver/sensorlist.htm>.

### Sensors Sorted By Interval

<b>30 s</b>	100x ping
<b>60 s</b>	2x corestate, 2x probestate, 2x systemstate, 1x wmidiskspace, 4x wminetwork, 16x http, 7x sslcertificate, 7x ssl, 6x dns, 61x remotedesktop, 1x smtp, 24x snmptraffic, 3x snmpcpu, 3x snmpdiskfree, 3x snmpuptime, 6x snmpmemory, 3x wmiprocessor, 6x wmiphysicaldiskv2, 3x wmidiskhealth, 12x wmiologicaldiskv2, 3x wmiantivirus, 1x clusterstate, 1x corestateautonomous
<b>10 m</b>	3x wmidiskspace, 3x wmiimemory, 3x wmilogfile, 3x wmiuptime
<b>15 m</b>	2x commonsaas
<b>1 h</b>	3x lastwindowsupdate

Sensors Sorted by Interval

### Probes

This section lists all probes in your monitoring setup. If there are no remote probes, only the local probe or the hosted probe appears in the list, which always runs on the PRTG core server.

**i** If you run PRTG in a cluster, this shows information for the system of the cluster node you are logged in to. Remote probes (if any) are only shown when you are logged in to the primary master node. When you are logged in to a failover node, the cluster probe on this cluster node appears as **local probe**.

## Probes


### Probe #1 "Local Probe"

connected from: 192.0.2.0:55909

Last Data: 06/10/2023 18:06:08 (0 sec ago) (W. Europe Standard Time)

.NET Framework Support: Installed: 4.7.2 or later

Probes

Category	Description
Probe #x "[Name]"	<p>Shows information about the connection status. If the probe is connected, the field shows the source IP address and port number used by the probe. For the <a href="#">local probe</a>, the IP address is always 127.0.0.1. You also see information about the date when the last data packet was received from the probe.</p> <p>If you want to restart a single probe, open the <a href="#">Administrative Tools</a>  settings.</p>

## System Settings

This sections shows information about system settings.



## System Settings

Web Server URL	https://10.242.8.177
Web Server IP Addresses	0.0.0.0
Web Server Ports	80,443
Web Server Port Usage	SSL
SSL/TLS Versions for Web Server	TLS 1.2
Web Server Ciphers	ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256!ADH!aN ULL!eNULL!LOW!3DES!MD5!EXP!PSK!SRP!DSS!RC4
SSL/TLS Versions for Probe Port	TLS 1.1, TLS 1.2
Probe Ciphers	ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+A ES128:DH+AES:ECDH+3DES:DH+3DES:RSA+AES:RSA+3DES:!ADH! AECDH:!MD5:!DSS
DH Parameters Size	1024
Incoming Probe Connection Binding	127.0.0.1:23560
Incoming Probe Connection IP Addresses	127.0.0.1
Incoming Probe Connection Port	23560
Probe Allow IP Addresses	
Probe Deny IP Addresses	
Data Path	C:\ProgramData\Paessler\PRTG Network Monitor\

System Settings

Category	Description
Web Server URL	Shows the URL to access the <a href="#">PRTG web interface</a> <sup>152</sup> .  <b>i</b> If you run PRTG in a cluster, this shows information for the system of the cluster node you are logged in to.
Web Server IP Addresses	Shows all IP addresses that the PRTG web server runs on.

Category	Description
	<p><b>i</b> If you run PRTG in a cluster, this shows information for the system of the cluster node you are logged in to.</p>
Web Server Ports	<p>Shows the ports that the PRTG web server runs on.</p> <p><b>i</b> If you run PRTG in a cluster, this shows information for the system of the cluster node you are logged in to.</p>
Web Server Port Usage	Shows the type of port used by the PRTG web server.
SSL/TLS Versions for Web Server	<p>Shows the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) versions used for connections to and from the PRTG web server.</p> <p><b>i</b> This is only shown if you use an SSL/TLS-secured connection.</p>
Web Server Ciphers	<p>Shows the ciphers used by the PRTG web server.</p> <p><b>i</b> This is only shown if you use an SSL/TLS-secured connection.</p>
SSL/TLS Versions for Probe Port	Shows the SSL/TLS versions used for the probe port.
Probe Ciphers	Shows the ciphers used for the remote probe connection.
DH Parameters Size	<p>Shows the length of the Diffie-Hellman (DH) parameters.</p> <p><b>i</b> This is only shown if you use an SSL/TLS-secured connection.</p>
Incoming Probe Connection Binding	Shows a combination of the incoming probe connection IP address and the incoming probe connection port.
Incoming Probe Connection IP Addresses	<p>Shows a list of all IP addresses on which PRTG listens for incoming remote probe connections.</p> <p><b>i</b> This is the same information as in the <a href="#">Core &amp; Probes</a> settings. <b>0.0.0.0</b> means that the PRTG core server listens on all local network adapter IP addresses.</p>
Incoming Probe Connection Port	Shows the port number on which the PRTG listens for incoming remote probe connections. The default port is <b>23560</b> .
Probe Allow IP Addresses	Shows all source IP addresses that PRTG accepts for incoming remote probe connections.

Category	Description
	<p><b>i</b> This is the same information as in the <a href="#">Core &amp; Probes</a><sup>2891</sup> settings. <b>any</b> means that all remote probe connections are accepted, regardless of the IP address of the remote probe system.</p>
Probe Deny IP Addresses	<p>Shows all source IP addresses that PRTG denies for incoming remote probe connections.</p> <p><b>i</b> This is the same information as in the <a href="#">Core &amp; Probes</a><sup>2892</sup> settings. Denied IP addresses are superior to allowed IP addresses. If this field is empty, there are no denied IP addresses.</p> <p><b>i</b> PRTG automatically adds the IP address of a remote probe system to this list when you delete a remote probe from the <a href="#">device tree</a><sup>132</sup>.</p>
Data Path	<p>Shows the path where PRTG stores its configuration, monitoring database, etc.</p> <p><b>i</b> To change this setting, open the <a href="#">PRTG Administration Tool</a><sup>3047</sup> on the PRTG core server system (or of the respective cluster node, if applicable).</p> <p><b>i</b> If you run PRTG in a cluster, this shows information for the system of the cluster node you are logged in to.</p>

## Web Server Activity

This section shows statistics about the PRTG web server since the last startup. All values are reset when the PRTG core server is restarted.

- i** If you run PRTG in a cluster, this shows information for the system of the cluster node you are logged in to.

## Web Server Activity

<b>Time Since Startup</b>	1 h 25 m
<b>Page Views</b>	8 (136/24h)
<b>Geo Maps(mapquest.roadmap)</b>	21 (356/24h)
<b>HTTP Requests</b>	203 (3439/24h)
<b>HTTP Requests &gt; 500 ms</b>	0 (0%)
<b>HTTP Requests &gt; 1000 ms</b>	1 (0%)
<b>HTTP Requests &gt; 5000 ms</b>	0 (0%)
<b>Slow Request Ratio</b>	0%

Web Server Activity

Category	Description
Time Since Startup	Shows the time that has passed since the PRTG web server was started.
Page Views	Shows the total number of page views on this PRTG core server.
Geo Maps	Shows the total number of geographical maps shown on this PRTG core server.
HTTP Requests	Shows the total number of HTTP requests to this PRTG core server.
HTTP Requests > 500 ms	Shows for how many (percent) of the HTTP requests above the page delivery took longer than 500 milliseconds (ms).
HTTP Requests > 1000 ms	Shows for how many (percent) of the HTTP requests above the page delivery took longer than 1,000 ms.
HTTP Requests > 5000 ms	Shows for how many (percent) of the HTTP requests above the page delivery took longer than 5,000 ms.
Slow Request Ratio	Shows a calculated number of the HTTP request values above. ⓘ The lower this number is, the faster the PRTG web interface is.
Failed Logins (Recent/Total)	Shows the number of recent failed logins and failed logins in total. ⓘ PRTG only shows this statistic when the number of failed logins is larger than 50.

## Synchronization

The PRTG core server holds the configuration of the entire monitoring setup and deploys it to the probes. This section shows statistics about the synchronization of the PRTG core server with the local probe and all connected remote probes (if any), since the last startup of the PRTG core server. All values are reset when the PRTG core server is restarted.

**i** If you run PRTG in a cluster, this shows information for the system of the cluster node you are logged in to. You must log in to the primary master node to see synchronization data for remote probe connections.

Synchronization	
<b>Last Synchronization with a Probe</b>	05.05.2021 09:54:41 (Nothing to do, Timing:187/171/46/2841/2887/12656)
<b>Probe/Core Message Count</b>	29745
<b>Raw Buffer Count</b>	0 (OK)
<b>Configuration Requests Sent</b>	258 of 258
<b>Configuration Requests Deleted</b>	0
<b>Configuration Requests with Response</b>	0

Synchronization

Category	Description
Last Synchronization with a Probe	Shows the time stamp of the last probe synchronization, and if there is still something to do.
Probe/Core Message Count	Shows the total number of messages sent between the PRTG core server and probes, as well as a calculated message speed value.
Raw Buffer Count	Shows the number of raw buffers and a corresponding status indicator.
Configuration Requests Sent	Shows the total number of configuration requests and the requests that still need to be sent.
Configuration Requests Deleted	Internal debug information. Usually, this value is 0.

Category	Description
Configuration Requests With Response	Internal debug information. Usually, this value is 0.

## More

### ■ KNOWLEDGE BASE

How can I speed up PRTG—especially for large installations?

- <https://kb.paessler.com/en/topic/2733>

## Others

There are some settings that you must define in the [PRTG Administration Tool](#)<sup>[3040]</sup>. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#)<sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#)<sup>[3067]</sup>

### 8.12.3.2 Cluster Status

On the Cluster Status tab, you can view all cluster nodes.

**i** This tab is only available if you run PRTG in a [failover cluster](#)<sup>[128]</sup>.

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

**☁** If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.

**☁** This feature is not available in PRTG Hosted Monitor.

The following information is available:

- Cluster Status: Shows all connected cluster nodes
- Cluster Log: Shows all log entries for cluster connections

**Cluster Status**

Node 1: PRTG Network Monitor (10.0.10.34)  
Primary Node (Current Master)      Start Maintenance Mode

Connection To	IP	State
⇒ Node 10.0.10.35	10.0.10.35	Connected

Node 2: Node 10.0.10.35  
Secondary Node (Failover Node, Version: 104386)      Start Maintenance Mode

Connection To	IP	State
⇒ PRTG Network Monitor (10.0.10.34)	10.0.10.34	Connected

**Cluster Log**      Items: 50      Show Filters

Date Time	Object	Status	Message	Cluster Node
04/10/2023 09:04:03	Cluster Probe	Connection connected	Cluster: Connected to node	Node 10.0.10.35
04/10/2023 09:02:03	Cluster Probe	Cluster	Node 2 Connection 1 (10.0.10.35): TCP connected from	Node 10.0.10.35
04/10/2023 09:01:03	Cluster Probe	Connection connected	Cluster: Connected to node	PRTG Network Monitor (10.0.10.34)
04/10/2023 04:05:35	Cluster Probe	Cluster	Node 1 Connection 1 (10.0.10.34): TCP connected from	PRTG Network Monitor (10.0.10.34)

Cluster Status

Click the Start Maintenance Mode link to put a cluster node in maintenance mode. A cluster node in this mode is still connected to the cluster, but PRTG discards its monitoring results until you click the Stop Maintenance Mode link. You can use this to explicitly exclude a cluster node from monitoring if you know that the monitoring values are not accurate, for example, because you are reconfiguring the server. During maintenance, PRTG displays a cluster node with a transparent color in the overview graphic.

**i** On the Cluster Status tab, you do not see if your [remote probes are connected to failover nodes](#) <sup>[3210]</sup>. Connect to your failover nodes and explicitly check if remote probes are connected, for example, in the device tree of the PRTG web interface on a cluster node.

**■** For more information about cluster settings, see section [Cluster](#) <sup>[2923]</sup>.

## Others

There are some settings that you must define in the [PRTG Administration Tool](#) <sup>[3040]</sup>. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#) <sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#) <sup>[3067]</sup>

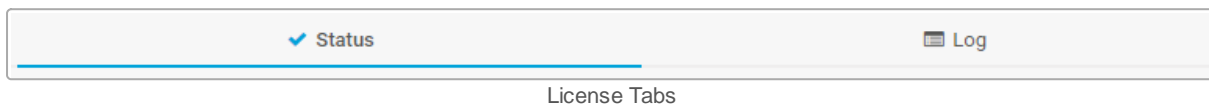
## 8.12.4 License Information

On the License Information tab, you can view information about your license and enter your license key.

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

**☁** If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.

**☁** This option is not available in PRTG Hosted Monitor.



In this section:

- [Status](#)<sup>[2962]</sup>
- [License Information](#)<sup>[2963]</sup>
- [Log](#)<sup>[2964]</sup>
- [Change and Update License Information](#)<sup>[2964]</sup>
- [Update Your License Information](#)<sup>[2965]</sup>
- [Proxy Configuration](#)<sup>[2966]</sup>

### Status

Click the Status tab to view information about your license.



## License Information




### License Information

<b>License Status</b>	<b>Activation was successful</b>
<b>License Name</b>	Example Organization
<b>License Key</b>	P10000-FFSEJ3-ZHGRD5-UR1CS9-U73FG2-G645F1-YVF1D0-H83234
<b>System ID</b>	SYSTEMID-AAAA1111-BBBB2222-3333CCCC-4444DDDD-5555EEEE
<b>Customer ID</b>	012345678
<b>Licensed Edition</b>	PRTG Network Monitor (next validation on 15/3/2024 at the latest)
<b>Last Update</b>	02/02/2024 13:21:54
<b>Subscription until</b>	07/05/2027 (1059 days left)
<b>Number of Sensors</b>	Unlimited

Manage License
Change License Key
Refresh Information
Deactivate this License

License Information

Setting	Description
License Status	<p>Shows the activation status of this PRTG installation. Usually, PRTG automatically completes the activation during installation or when you change your license information.</p> <p> If PRTG cannot directly connect to the internet, a manual activation is necessary.</p> <p> For more information, see section <a href="#">Activate the Product</a><sup>[104]</sup>.</p>
License Name	<p>Shows the owner of the <a href="#">license</a><sup>[102]</sup> that you use for this PRTG installation, for example <a href="#">ExampleOrganization</a>.</p> <p> The License Name, license key, and system ID make up your license information.</p> <p> You can find the label License Owner in some documents from the Paessler Portal. License Owner is the same as License Name. PRTG might ask you for this information during installation or when you <a href="#">change your license key</a><sup>[102]</sup>.</p>
License Key	<p>Shows the <a href="#">license</a><sup>[102]</sup> key that you use for this PRTG installation.</p> <p> The License Name, license key, and system ID make up your license information.</p>


Setting	Description
System ID	<p>The system ID is a fixed value that is automatically assigned to a PRTG installation.</p> <p> The License Name, license key, and system ID make up your license information.</p>
Customer ID	<p><b>This setting is only visible if you have a subscription license.</b></p> <p>Shows the customer ID of the license that you use for this PRTG installation.</p>
Licensed Edition	<p>Shows the license that you use for this PRTG installation. This determines how many sensors you can use in PRTG.</p> <p> PRTG regularly validates subscription licenses. You can see the next validation date here.</p>
Last Update	<p>Shows the date of the last update for this PRTG installation. We recommend that you use the <a href="#">auto-update</a><sup>[2969]</sup>.</p>
Subscription until / Maintenance until	<p>Shows the expiration date and the number of days that remain for your active maintenance or subscription. Manage your license at the <a href="#">Paessler Portal</a> for continued access to any available updates and to our premium email support.</p>
Number of Sensors	<p>Shows the number of sensors that you can use in PRTG. If you reach the limit, PRTG automatically sets each new sensor that you add to the Paused <a href="#">status</a><sup>[181]</sup>.</p> <p>Editions that allow an <b>unlimited</b> number of sensors do not restrict the number of possible sensors by license, so you can create sensors until you reach the <a href="#">performance limit</a><sup>[27]</sup>. This means that you can use about 10,000 sensors per PRTG core server. However, this number depends on the performance of the PRTG core server system, and sensors and scanning intervals.</p> <p> For more information, see section <a href="#">System Requirements</a><sup>[22]</sup>.</p> <p>To upgrade your license right now, click Need more sensors? Click here to upgrade! to visit the Paessler Portal.</p>

## Log

Click the Log tab to show a [table list](#)<sup>[218]</sup> of all system log entries with all messages and status changes regarding your license.

## Change and Update License Information

Use the following buttons to edit your license or refresh your maintenance information.

Button	Description
Manage License	Click to open the Paessler Portal and manage your PRTG Network Monitor license. This button is <b>only</b> visible to users of a commercial license.
Deactivate this License	<p>If you want to use the license of a PRTG installation on a different computer, click this button to deactivate the license. This is necessary, for example, when you move PRTG to a different computer, because a PRTG license can be active on only one computer at the same time. Once you have deactivated the license, the PRTG installation on this computer reverts to the <a href="#">freeware edition</a><sup>20</sup> after a grace period of 30 days.</p> <p> See also section <a href="#">Activate the Product</a><sup>104</sup>.</p>

## Update Your License Information

Click Change License Key or Refresh Information on the Status tab to update your license. Provide the necessary information and click Update License to complete the activation of your license.

**i** If you have any issues with license activation or updates, click Contact Support in the page footer to contact us directly via the [Paessler Help Desk](#). This requires internet access.

### Step 1: Choose Activation Type

Setting	Description
Activation Type	<p>Define how you want to validate and activate your license:</p> <ul style="list-style-type: none"> <li>▪ Automatic (online activation with optional HTTP proxy): Activate the license online. PRTG connects to the activation server and validates your license. The license is activated automatically. For automatic activation, the PRTG core server system must have internet access.</li> <li>▪ Manual (offline activation): Activate the license manually. Use this if the PRTG core server system has no access to the internet and cannot connect to activation.paessler.com. <ul style="list-style-type: none"> <li><b>i</b> This is the default selection if the PRTG core server system is offline.</li> </ul> </li> </ul>

### Step 2: Verify Your PRTG License

Setting	Description
License Key	Enter the license key that you received from Paessler GmbH. To avoid typing errors, copy and paste the License Key. It must exactly match your license key.
License Name	<p>If prompted, enter the License Name that you have received from Paessler GmbH. It must exactly match. To avoid typing errors, copy and paste the License Name.</p> <p><b>i</b> You can find the label License Owner in some documents from the Paessler Portal. License Owner is the same as License Name. PRTG might ask you for this information during installation or when you <a href="#">change your license key</a><sup>[102]</sup>.</p>
System ID	<p>This field shows the system ID, a fixed value assigned to your PRTG installation.</p> <p><b>i</b> This setting is for your information only. You cannot change it.</p>

For offline activation, click Save to File to write your license information into a text file.

### Step 3a: Activate Your PRTG

If you select the automatic activation type, you can now update your license. Define if you need an HTTP proxy for the HTTPS connection to the activation server and click Update License.

## Proxy Configuration

 This option is not available in PRTG Hosted Monitor.

Setting	Description
Proxy Server Handling	<p>Define if you want to use PRTG with a direct internet connection or if a proxy is necessary:</p> <ul style="list-style-type: none"> <li>▪ Do not use a proxy server (default): Do not use a proxy. Use this setting if a direct internet connection to the PRTG core server system is available.</li> <li>▪ Use a proxy server: Define proxy settings below. Use this setting if a proxy is mandatory in your network.</li> </ul> <p><b>i</b> We recommend that you use PRTG with a direct internet connection.</p> <p><b>i</b> The proxy settings are valid for <a href="#">auto-update</a><sup>[2963]</sup>, <a href="#">activating the product</a><sup>[104]</sup>, obtaining <a href="#">Geo Maps</a><sup>[2731]</sup> tiles, and for sending HTTP, push, and SMS text message <a href="#">notifications</a><sup>[2815]</sup>.</p>

Setting	Description
Server	<p>This setting is only visible if you select Use a proxy server <a href="#">above</a></p> <p>Enter the address of the proxy server that you use for outbound connections. Enter a valid address.</p>
Port	<p>This setting is only visible if you select Use a proxy server <a href="#">above</a></p> <p>Enter the port number of the proxy server that you use for outbound connections. Enter an integer.</p>
Proxy Authentication	<p>This setting is only visible if you select Use a proxy server <a href="#">above</a></p> <p>Determine whether the proxy server needs credentials or not:</p> <ul style="list-style-type: none"> <li>▪ Do not use authentication: Do not use credentials for proxy connections.</li> <li>▪ User name and password: Define credentials (user name and password) below. Use this setting if the proxy server requires credentials.</li> </ul>
User Name	<p>This setting is only visible if you select User name and password <a href="#">above</a>.</p> <p>Enter a user name for proxy authentication. Enter a string.</p>
Password	<p>This setting is only visible if you select User name and password <a href="#">above</a>.</p> <p>Enter a password for proxy authentication. Enter a string.</p>

### Step 3b: Request Activation Data

**i** The following step only applies to PRTG Network Monitor. If you use PRTG Enterprise Monitor, see the Paessler website: [How to use PRTG Enterprise Monitor in an offline environment in 5 steps](#).

If you select Manual (offline activation), you must request your activation data at <https://shop.paessler.com/service/licenseactivation/> using your license information. Open the activation page from a computer with internet access and provide your license information.

Generate the key file for your license and provide this data below.

### Step 4: Provide Activation Data

**i** This step is only necessary if you activate your license offline.

- Copy the content of the key file that you have generated on <https://shop.paessler.com/service/licenseactivation/>.

- Paste it into the Activation Data field. Alternatively, click Load from File if you have saved the key file with your activation data.
- Click Update License to complete the activation of your license.

## More

### ■ KNOWLEDGE BASE

How do I upgrade to a later edition of PRTG?

- <https://kb.paessler.com/en/topic/4193>

The automatic license activation of my PRTG Enterprise Monitor license does not work. What can I do?

- <https://kb.paessler.com/en/topic/89281>

### ■ PAESSLER WEBSITE

How to use PRTG Enterprise Monitor in an offline environment in 5 steps

- <https://www.paessler.com/support/how-to/prtg-enterprise-monitor-offline>

## Others

There are some settings that you must define in the [PRTG Administration Tool](#)<sup>[3040]</sup>. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#)<sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#)<sup>[3067]</sup>

## 8.12.5 Auto-Update

In the Auto-Update settings, you can check the status of the auto-update, view logs, and edit settings. When a new version of PRTG is available on the Paessler website, PRTG automatically downloads the setup file if a direct internet connection is available. The [PRTG System Administrator](#) user then receives a [ToDo ticket](#)<sup>[213]</sup> with instructions to initiate the update installation.

**i** If you use the [freeware edition or trial edition](#)<sup>[20]</sup>, automatic software updates are available at any time. If you use a [commercial edition](#)<sup>[20]</sup>, you need to have an active subscription or active maintenance to receive updates.

**i** This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

**☁** If 15 minutes (900) seconds have passed since your last credential-based login and you open a setup page from a different setup page, PRTG asks you to enter your credentials again for security reasons. A dialog box appears. Enter your Login Name and Password and click OK to continue.

**☁** This option is not available in PRTG Hosted Monitor.

The screenshot shows the 'Auto-Update' settings page. At the top, there are three tabs: 'Status', 'Log', and 'Settings'. The 'Status' tab is selected. Below the tabs, there is a message box that says: 'Here you can automatically update your PRTG installation. If you are using the freeware or trial edition you can always update to the latest version for free. If you are using a commercial edition your license key must be covered by a valid maintenance contract in order to download updates. You can always prolong your maintenance at <https://shop.paessler.com>. You can deactivate automatic downloading in the [Settings tab](#).' Below this is a section titled 'Update Status For PRTG Network Monitor' with a table:

Remaining Maintenance Days	4655 (04/07/2036)
Latest Message from Auto-Update	
Currently Installed Version	23.3.88.1421+
Currently Selected Release Channel	Preview <a href="#">Select Other Release Channel</a>
Latest Version Available from Paessler	23.4.89.1500 <b>NEW!</b> <a href="#">Check For Latest Update and Download</a>
Latest Downloaded Version	

Auto-Update

Auto-update has the following tabs:

- **Status:** Click the Status tab to download and install updates.
- **Log:** Click the Log tab to show log information about the update status of PRTG, newest first. In the [table list](#)<sup>[218]</sup>, you can filter the items by using the [respective options](#)<sup>[218]</sup>.  
**■** For more information, see section [Logs](#)<sup>[210]</sup>.
- **Settings:** Click the Settings tab to configure the auto-update and release channel. See [Software Auto-Update](#)<sup>[2970]</sup> below.

## Using Auto-Update

If there is a new version available, you see detailed information about the available version. Read these notes carefully. You find a summary of current and past release notes below the update section. For more information about the release notes, see the Paessler website: [PRTG Release Notes and Version History](#).

To install the latest available version, click Install Update [version number]. PRTG asks you to confirm installation and license.

**i** Downloaded software versions are automatically saved in the \download subfolder of the [PRTG program directory](#). The [prtg.zip](#) that contains all necessary files is also cached in this subfolder.

## Manually Install an Interim Update

Not all available updates from Paessler are pushed to all customers but they are still available on the website. Sometimes the Paessler support team might ask you to update to the latest version.

In this case, click Check For Latest Update and Download. PRTG connects to the Paessler servers and downloads the setup file, regardless of the status of the update check. Then click Install Update [version number].

**i** To manually install an interim update, a direct internet connection is necessary on the PRTG core server system.

## Software Auto-Update

Software Auto-Update

When a New Version is Available **i**

Automatically download and install  
 Automatically download and alert the admin  
 Alert the admin only

Release Channel **i**

Stable: Updated about once per month (most conservative option, recommended)  
 Preview: Updated about once per month (thoroughly tested in our labs, do not use on production systems!)  
 Canary: Updated daily (for testing only, do not use on production systems!)

Software Auto-Update

Setting	Description
When a New Version is Available	Define what PRTG does when software updates are available: <ul style="list-style-type: none"> <li>Automatically download and install: Download and install any new version as soon as PRTG detects that a newer version is available. PRTG checks for a newer version once per day.</li> <li><b>i</b> The installation of a new version restarts the PRTG core server service and PRTG probe service and might also include a system restart.</li> </ul>



Setting	Description
	<ul style="list-style-type: none"> <li>▪ Automatically download and alert the admin: Download any new version as soon as PRTG detects that a newer version is available. PRTG checks for a newer version once per day. After successful download, PRTG creates a <a href="#">ToDo ticket</a><sup>[213]</sup> for the <a href="#">PRTG System Administrator</a> user.</li> <li>▪ Alert the admin only: Do not download updates. Only create a ToDo ticket. You can still manually download updates via the <a href="#">auto-update</a><sup>[2970]</sup>.</li> </ul>
Installation Time	<p><b>This setting is only visible if you select</b> Automatically download and install above.</p> <p>Select the desired time for the installation of updates from the dropdown list. You can select As soon as the update is available to install updates at any time of the day.</p>
Release Channel	<p>Define the release channel that PRTG delivers updates in:</p> <ul style="list-style-type: none"> <li>▪ Stable: Updated about once every 8 weeks (most conservative option, default): Deliver updates in the Stable release channel. These are our best tested versions. <ul style="list-style-type: none"> <li>ⓘ Use these software versions for live environments that you depend on.</li> </ul> </li> <li>▪ Preview: Updated twice between stable releases (thoroughly tested in our labs, do not use on production systems): Deliver updates in the Preview release channel. Versions in this channel were thoroughly tested in our labs but might still contain limitations in certain monitoring configurations. <ul style="list-style-type: none"> <li>ⓘ Use this release channel if you are willing to take a little risk for the benefit of getting new features and bug fixes a little earlier.</li> <li>ⓘ We strongly recommend that you <b>not</b> use these software versions in live environments that you depend on.</li> </ul> </li> <li>▪ Canary: Updated daily (testing only, should not be used on production systems): Deliver updates in the Canary release channel. These versions are updated every night. <ul style="list-style-type: none"> <li>ⓘ Use with caution. Software versions in this channel have not been tested, might contain severe bugs, and are provided for testing purposes only.</li> <li>We strongly recommend that you <b>not</b> use these software versions in live environments that you depend on.</li> </ul> </li> </ul>

ⓘ Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

## Notes

There are a few things that we ask you to consider regarding automatic software updates:

- For automatic software updates to work, the PRTG core server system must have direct internet access. If a proxy connection is necessary, configure it in the [Core & Probes](#) settings.
  - For more information about the update servers, see the Knowledge Base: [Which servers does PRTG connect to for software auto-update, activation, etc.?](#)
- During installation, the PRTG core server system might restart without notice.
- PRTG automatically updates classic remote probes, which might cause short downtimes in the monitoring of remote locations. In rare cases, a manual update of classic remote probes is required after you update the PRTG core server. In these cases, you are notified in the device tree, and the monitoring of remote locations is interrupted until you perform the [manual update](#) on the remote probe system. If a probe system uses several network connections with different IP addresses, make sure that these IP addresses are included in the [list of allowed IP addresses](#). Otherwise, the remote probe on this system might be disconnected after an update.
- PRTG does not automatically update multi-platform probes. If you installed a multi-platform probe via the Paessler Linux package repository, your package manager notifies you when there is an update. Otherwise, manually update your multi-platform probes with the updated package. For more information, see the [Multi-Platform Probe for PRTG](#) manual.
- In a cluster, you only need to install the update on one cluster node. PRTG automatically deploys the new version to all other cluster nodes. This might cause a short amount of downtime for the monitoring on the cluster nodes, one after the other.
- If you run several individual PRTG core servers that are not in a cluster, you must initiate and confirm an update for each single PRTG core server.
- You can disable automatic downloading on the auto-update [Settings](#) tab. PRTG then only downloads updates when you click Check For Latest Update and Download.
- PRTG does not start auto-update downloads if less than 500 MB disk space is available on the PRTG core server system. If this is the case, you can check this on the [Log](#) tab.
- Virus scanners might potentially cause issues when downloading or installing software updates. To avoid such issues, we recommend that you make the appropriate exclusions for the PRTG program directory.

## More

### ■ KNOWLEDGE BASE

Which servers does PRTG connect to for software auto-update, activation, etc.?

- <https://kb.paessler.com/en/topic/32513>

Which information does PRTG send back to Paessler?

- <https://kb.paessler.com/en/topic/28103>

### ■ PAESSLER WEBSITE

Release notes for the "stable" release channel

- <https://www.paessler.com/prtg/history/stable>

## Others

There are some settings that you must define in the [PRTG Administration Tool](#)<sup>[3040]</sup>. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#)<sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#)<sup>[3067]</sup>

## 8.12.6 Optional Downloads

To see optional downloads, select Setup | Optional Downloads from the [main menu bar](#)<sup>[249]</sup>. Click a tab to switch between different options.



In this section:

- [PRTG Apps](#)<sup>[2974]</sup>
- [PRTG MultiBoard](#)<sup>[2974]</sup>
- [Remote Probes](#)<sup>[2974]</sup>

### PRTG Apps

To monitor your network while on the go, use our free PRTG apps for smartphones and tablets. They run on iOS and Android.

■ For more information, see section [PRTG Apps for Mobile Network Monitoring](#)<sup>[2988]</sup>.

■ For more information about PRTG for iOS and PRTG for Android, see the Paessler website: [PRTG apps for iOS or Android](#).

### PRTG MultiBoard

Download PRTG MultiBoard to your system. You can run it on Windows, macOS, or Linux to manage one or several independent [PRTG core servers](#)<sup>[125]</sup> or PRTG Hosted Monitor instances with a native, cross-platform application.

■ For more information, see section [PRTG MultiBoard](#)<sup>[2984]</sup>.

### Remote Probes

With remote probes, you can extend your monitoring to distributed networks that are not directly reachable from your PRTG core server system. The version of the classic remote probe installer must match your version of PRTG, so it is a good idea to download it from here.

■ For more information, see section [Install a Remote Probe](#)<sup>[106]</sup>.

■ For more information about the Multi-platform probe, see : [Multi-Platform Probe for PRTG \(PDF\)](#).

### More

■ PAESSLER WEBSITE

PRTG MultiBoard

- <https://www.paessler.com/prtg/extensions/prtg-multiboard>

PRTG app for desktop

- <https://www.paessler.com/prtg/apps/desktop>

PRTG apps for iOS or Android

- <https://www.paessler.com/prtg/apps/mobile>

## Others

There are some settings that you must define in the [PRTG Administration Tool](#)<sup>[3040]</sup>. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#)<sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#)<sup>[3067]</sup>

## 8.12.7 Help and Support Center

In the Help and Support Center, you can access help and support information for PRTG.

**Help and Support Center**

<p><b>PRTG MANUAL</b></p> <p>The PRTG Manual provides in-depth coverage of all topics you need for network monitoring with PRTG, including:</p> <ul style="list-style-type: none"> <li>• Basic Concepts of PRTG</li> <li>• Basic Procedures in the PRTG Web Interface</li> <li>• Advanced Procedures in the PRTG Web Interface</li> <li>• Device and Sensor Setup</li> <li>• Sensor Technologies</li> </ul> <p><a href="#">READ MANUAL »</a></p>	<p><b>KNOWLEDGE BASE</b></p> <p>The Knowledge Base contains thousands of articles about PRTG, including:</p> <ul style="list-style-type: none"> <li>• Tutorials and How-Tos</li> <li>• Tips and Tricks</li> <li>• Custom Code</li> <li>• Workarounds</li> <li>• Contribute: Make your own questions, answers, and custom content available for all PRTG users worldwide!</li> </ul> <p><a href="#">GET ANSWERS »</a></p>	<p><b>VIDEO TUTORIALS</b></p> <p>Find comprehensive videos created by our network monitoring professionals, including:</p> <ul style="list-style-type: none"> <li>• PRTG Basics</li> <li>• All About Monitoring</li> <li>• PRTG Advanced</li> <li>• PRTG Webcasts</li> <li>• PRTG Apps</li> </ul> <p><a href="#">HAVE A LOOK »</a></p>
<p><b>ADVANCED TOPICS</b></p> <p>This section covers various topics and special use cases for advanced users, including:</p> <ul style="list-style-type: none"> <li>• Active Directory Integration</li> <li>• Application Programming Interface (API)</li> <li>• Lookups</li> <li>• Setting up Remote Probes and Failover Clusters</li> <li>• And many more!</li> </ul> <p><a href="#">LEARN MORE »</a></p>	<p><b>TECHNICAL SUPPORT</b></p> <p><i>This feature is only available if you have an active maintenance plan.</i></p> <p>If the existing help resources don't provide the assistance you need, you can open a support ticket. Our usual response time to tickets is within 24 hours on business days. Use the Contact Support form to describe your issue with as much detail as possible.</p> <p>We are happy to help!</p> <p><a href="#">CONTACT SUPPORT »</a></p>	<p><b>CUSTOMER SERVICE</b></p> <p>Let us help you with your license purchase, upgrade, or maintenance extension. Our Customer Service Team is happy to assist you with quotes (and valuable license/maintenance information), guide you through the purchasing process, and facilitate the contact to our system engineers and/or our partners in your region.</p> <p><a href="#">CONTACT US »</a></p>

Help and Support Center

The following help and support topics are available:

- [PRTG Manual](#)<sup>[14]</sup>
- [Knowledge Base](#)
- [Video Tutorials](#)
- [Advanced Topics](#)<sup>[3080]</sup>
- [Technical Support](#)<sup>[2977]</sup>
- [Customer Service](#)<sup>[161]</sup>

### Others

There are some settings that you must define in the [PRTG Administration Tool](#)<sup>[3040]</sup>. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#)<sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#)<sup>[3067]</sup>

## 8.12.8 Contact Support

### IMPORTANT INFORMATION

The Contact Support feature is only available for users with an active subscription of PRTG Network Monitor, PRTG Enterprise Monitor, or PRTG Hosted Monitor or if you have valid maintenance. This feature is not available for freeware edition licenses.

For technical issues, use the Contact Paessler Support / Send Your Feedback to Paessler form in PRTG. To open the form, select Setup | Contact Support from the [main menu bar](#)<sup>[249]</sup>. You can also open the form via Contact Support in the footer on every page in the PRTG web interface.

Alarms Maps Reports Logs Tickets Setup

TRUSTPILOT  
★★★★★

# System Administrator!

Do You  
PRTG?

**20**  
Current Alarms

!!	12	Down
!	0	Down (Ackn
W	8	Warning
U	0	Unusual

[View All Al](#)

## License Status

**4656**  
Maintenance Days Left  
[Get Maintenance](#)

**9855**  
Sensors Available  
[Recommended Setup](#)

[Contact Support](#) [? Help](#)

How to Open the Contact Support Form

When you click Contact Support, the following form appears:



Contact Paessler Support / Send Your Feedback to Paessler ✕

---

Ask a Question or Give Feedback

Your Ticket ID PAE<id>  
(If You Have One) ⓘ

---

Your Email Address

johnqpublic@example.com

---

Scope of Your Question

PRTG configuration and usage

PRTG Desktop and PRTG apps for iOS or Android

Technical issues (performance, web server, sensors, probes, cluster)

Critical issue (large parts of my monitoring do not work)

Other (including feedback and feature requests)

Helpful resources:

- Help with installation, licensing, and setup
- Information about data storage/backup/migration and updating PRTG
- Working with user accounts and user rights
- Installing an SSL certificate for the PRTG web server
- Configuring a failover cluster

Emotional State

OK ▼

---

Enter a Subject for Your Question/Feedback ⓘ

---

**This field is required.**

Contact Paessler Support / Send Your Feedback to Paessler

On the one hand, you can use this form to ask for support regarding technical issues. To make the support contact more comfortable, PRTG can automatically attach a screenshot in combination with a Support Bundle that contains several selected PRTG log files and status files. This information really helps the Paessler support team to analyze any issue you might have with PRTG. Also consider the suggested links to articles regarding the scope of your issue.

On the other hand, you can use this form to give us [feedback](#). Help improve PRTG by providing criticism, praise, bug reports, and feature requests. Any comments are welcome. Your feedback is handled directly by the Paessler support team.

PRTG securely transmits your feedback or support question including the support bundle to Paessler via the PRTG Cloud. Read more in our Knowledge Base on [how we handle your feedback](#).

- ⓘ Make sure that your PRTG core server system has access to the internet and can reach the URL <https://api.prtgcloud.com:443>

## Form Details

Ask a Question or Give Feedback

Provide the following information in this section of the contact form.

Field	Description
Your Ticket ID PAE<id>	<p>If you already have an open ticket (directly via the <a href="#">Paessler Help Desk</a>), enter the ticket ID. You can find it in your confirmation email regarding the request we received. You can provide the ID with PAE in front or only the number.</p> <p>ⓘ If you leave this field empty, you create a new ticket when you submit this form.</p>
Your Email Address	<p>Enter your email address. You can provide any of your addresses. However, by default, PRTG uses the email address of your user account to be able to associate you with your license.</p>
Scope of Your Question	<p>Select a topic regarding your issue and consider the suggested links.</p>
Emotional State	<p>If you want to, you can express your feelings about PRTG.</p>
Enter a Subject for Your Question/Feedback	<p>Provide short information with a maximum of 60 characters to indicate the topic of your issue.</p>
Enter a Detailed Description	<p>Leave any comments. They can be feedback or support questions. If you have a support question, describe your issue with as much detail as possible.</p>

## Attach a Screenshot and/or Support Bundle

To provide the most helpful information possible, you can attach a screenshot of the selected page and a support bundle with useful analytical data about your PRTG installation.

Setting	Description
Do not attach screenshot	<p>Send the ticket without a screenshot.</p> <p>ⓘ If you ask for technical help, we recommend that you attach a screenshot. This helps us a lot to analyze your issue and to provide a solution.</p>

Setting	Description
Create and attach screenshot (recommended)	<p>PRTG creates a screenshot of the selected page and sends it with your ticket. You can see a preview below the screenshot section.</p> <p><b>i</b> We recommend that you open the contact support form directly on the page where you encountered an issue. Taking screenshots is not possible on some generic error pages that are not meaningful enough for the Paessler support team.</p>

In section Support Bundle, you can choose from several packages that differ in coverage of information.

Setting	Description
Support Bundle	<p>Select the information you want to send to the Paessler support team:</p> <ul style="list-style-type: none"> <li>▪ Attach Base Pack with log files (recommended): Contains the following data about PRTG: <ul style="list-style-type: none"> <li>▫ System status</li> <li>▫ Lists of sensors in the Down status or the Unknown status</li> <li>▫ Core and probe health data</li> <li>▫ Current log entries</li> </ul> </li> <li>▪ Attach Base Pack with log files and PRTG configuration file: Contains the Base Pack and the PRTG configuration file. <ul style="list-style-type: none"> <li><b>i</b> Send this package only if the Paessler support team asks you to. User names, encrypted passwords in the <a href="#">config.dat</a> file, and passwords that your browser masks while you enter them on settings pages are removed before PRTG sends this package to the Paessler support team.</li> </ul> </li> <li>▪ Do not attach a Support Bundle: The ticket does not contain files. Choose this option only when sending feedback.</li> </ul>

Click Submit to send your request directly to the Paessler support team, or click Cancel to return to the page where you opened the contact form.

## Helpdesk

Write us in English or German and communicate via the [Helpdesk](#). The Paessler support team works closely with our development department to guarantee the fastest and most constructive assistance possible. As they need to analyze a lot of data over the course of a support case, like log files and screenshots, they use the Helpdesk as their primary support mechanism. Their office is staffed Monday to Friday from 07:00 to 22:00 (UTC+1), so you receive an answer within 24 hours on business days. Depending on the complexity of the case, they might need to ask for remote access to your system, or to schedule a remote desktop session.

## Other Resources

### Knowledge Base

Find answers to common questions in our [Knowledge Base](#).

### Supported Versions

Note that we only support PRTG versions that were released in the last 12 months. For more information on released versions, see the Paessler website: [Release notes for the "stable" release channel](#).

### License and Upgrades

If you have questions or feedback regarding your license purchase or want to upgrade your license, [contact our customer service](#)<sup>[161]</sup>.

### Network Planning

If you need help with your network setup or detailed installation planning, our partners are always happy to help. Please [contact a partner near you](#).

### Security Reports

If you are a user of PRTG or any of our other services and would like to file a security report, send an email to [security@paessler.com](mailto:security@paessler.com). Always include a detailed technical summary in your email. If you wish to send us an encrypted email, use the public key available at the [Paessler Help Desk](#).

## More

### ■ KNOWLEDGE BASE

How can I propose new features or sensors for PRTG?

- <https://kb.paessler.com/en/topic/79245>

### ■ PAESSLER WEBSITE

Release notes for the "stable" release channel

- <https://www.paessler.com/prtg/history/stable>

## Others

There are some settings that you must define in the [PRTG Administration Tool](#)<sup>[3040]</sup>. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#)<sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#)<sup>[3067]</sup>

# Part 9


# PRTG MultiBoard

## 9 PRTG MultiBoard

PRTG MultiBoard is a PRTG extension that functions as an alternative interface for PRTG. It is available on Windows, macOS, and Linux and you can use it to connect to one or several independent [PRTG core servers](#) <sup>[125]</sup> or PRTG Hosted Monitor instances to configure your setup, view monitoring results, and keep an eye on your network. It is a cross-platform application for fast access to data and monitoring management.

PRTG MultiBoard natively includes most PRTG features. For a few options, the application opens an external browser window using your default browser, for example, for system setup or probe installation.

**i** PRTG MultiBoard is mainly designed to review and manage PRTG installations that you already set up. If you have just started with monitoring, we recommend that you first run through the [smart setup](#) <sup>[41]</sup> in the [PRTG web interface](#) <sup>[152]</sup> and add your network devices there. Once finished, you can seamlessly switch to PRTG MultiBoard.

 PRTG Hosted Monitor supports connections from PRTG MultiBoard. For more information, see section [Using PRTG Hosted Monitor](#).

 Download the PRTG MultiBoard from the Paessler website: [PRTG MultiBoard](#).

### Requirements

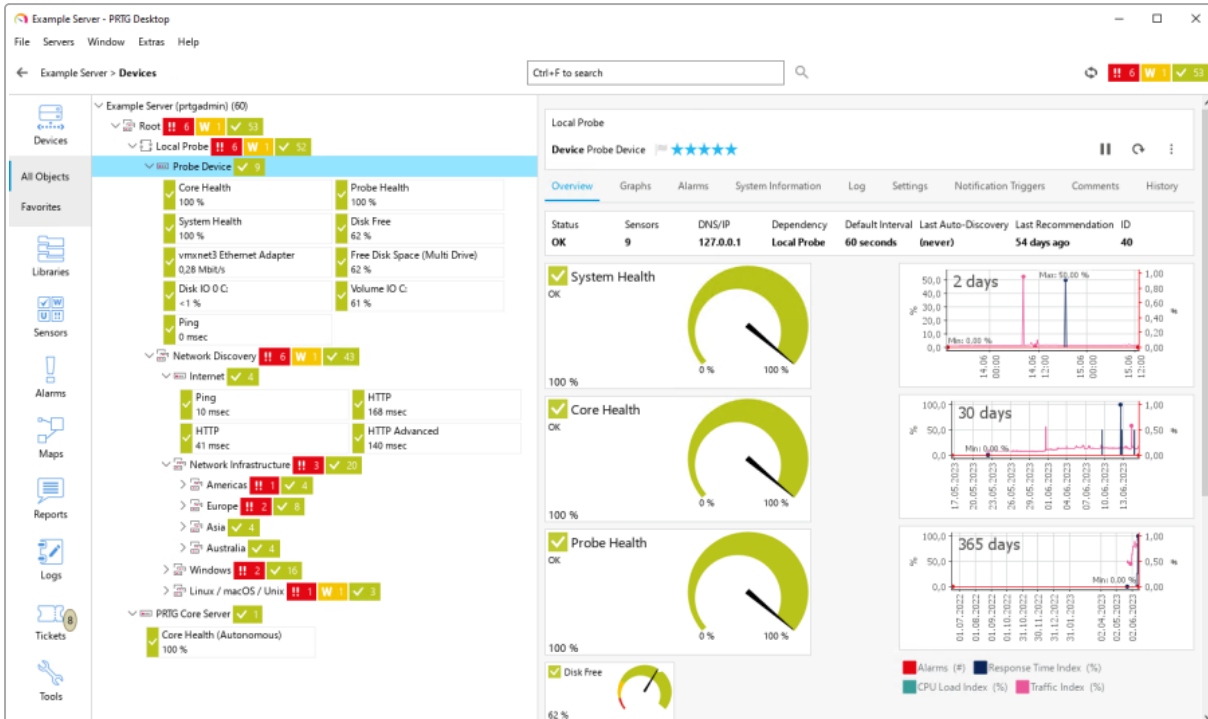
 For more information, see the [PRTG MultiBoard and PRTG app for desktop manual \(PDF\)](#).

Category	Requirement
PRTG version	Your PRTG core server or PRTG Hosted Monitor instance must run as of PRTG 17.4.35.
PRTG license type	You must be a Paessler PRTG Enterprise Monitor user.  <b>i</b> PRTG Network Monitor users can use the general features of PRTG MultiBoard with the <a href="#">Paessler PRTG app for desktop</a> .

### General Features

General features include Multi-Edit, Desktop Alerts, and Compare Sensors.

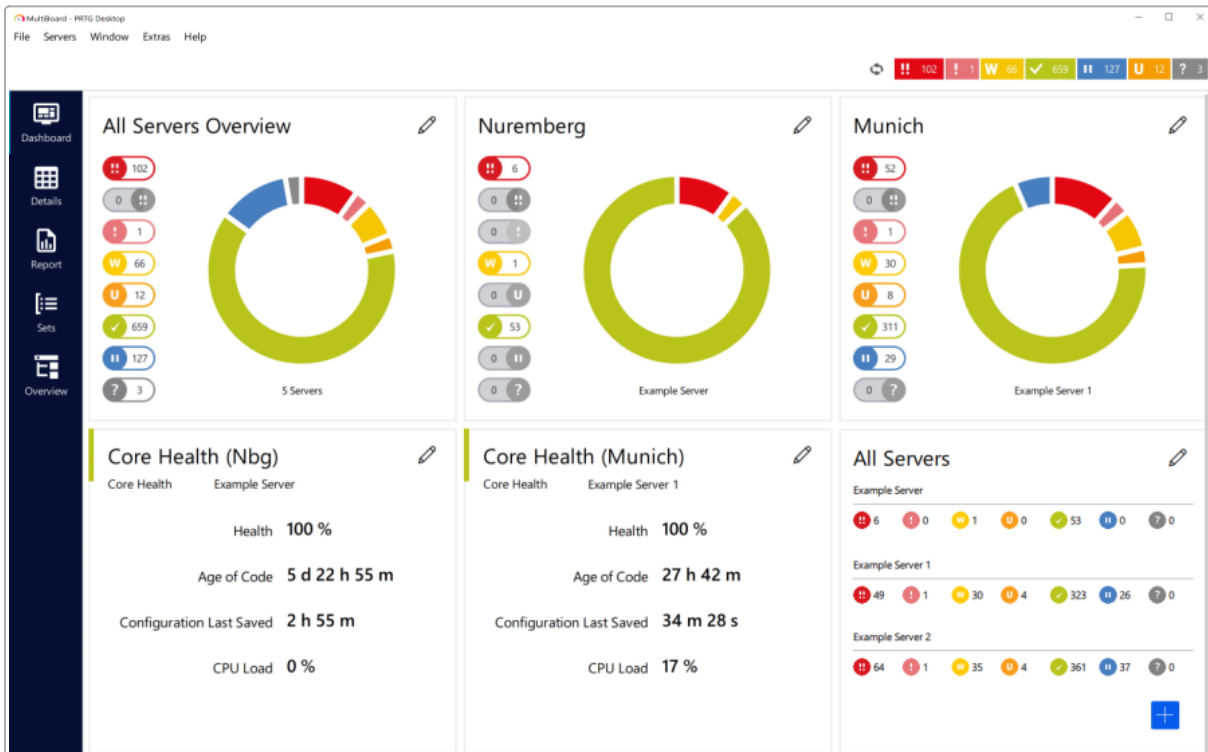
**i** These features are available for PRTG Network Monitor users.



PRTG app for desktop window

## MultiBoard Features

MultiBoard features include the MultiBoard, Probe Transfer, Configuration Viewer, and Template Transfer features.



MultiBoard window

With MultiBoard, you can connect to several independent servers to view their data and manage your monitoring centrally. Within the MultiBoard pages, you can find the following:

- **Dashboard:** Use different widget types to show overviews of your configured servers at a glance.
- **Details:** Display all sensors of all configured servers as a sensor list or in a more detailed table view.
- **Report:** Display an overview of the number of sensors on each connected server and in total, and the number of sensors that show a specific status.
- **Sets:** Group sensors into customized sensor sets across all your PRTG core servers and PRTG Hosted Monitor instances.
- **Overview:** View and edit all device tree objects in all of your PRTG core servers and PRTG Hosted Monitor instances.

## More

### ■ KNOWLEDGE BASE

Which audible notifications are available in the PRTG web interface and in the PRTG app for desktop?

- <https://kb.paessler.com/en/topic/26303>

How do I troubleshoot erratic behavior of push notifications in the PRTG app for desktop or PRTG apps?

- <https://kb.paessler.com/en/topic/86064>

### ■ PAESSLER WEBSITE

How to set up notifications for the PRTG app for desktop

- <https://www.paessler.com/support/how-to/notifications-desktop>

Paessler PRTG MultiBoard

- <http://www.paessler.com/prtg/extensions/prtg-multiboard>



## Part 10

# PRTG Apps for Mobile Network Monitoring

## 10 PRTG Apps for Mobile Network Monitoring

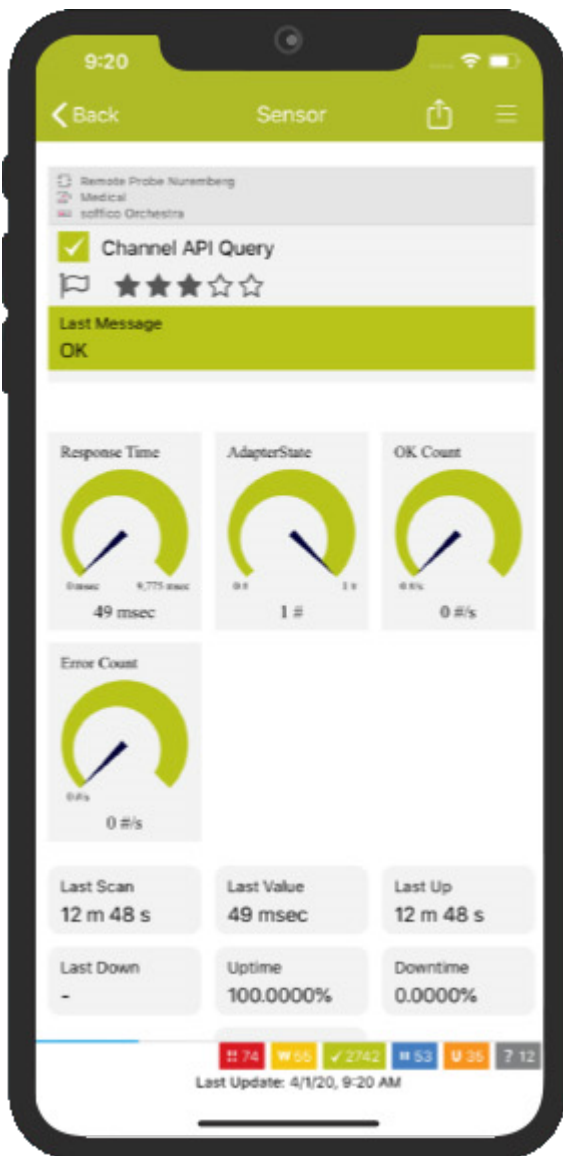
You can access your PRTG installation on your mobile devices with PRTG apps for iOS or Android. You can download and use these apps for free. [PRTG for iOS](#)<sup>2988</sup> and [PRTG for Android](#)<sup>2989</sup> let you monitor your network while on the go.

The basic requirements to use these free PRTG apps are a running PRTG core server that is accessible from the network your device is connected to (either directly or via a VPN connection) and a recent operating system version on your mobile device. For details about requirements, see below.

### PRTG for iOS

PRTG for iOS is the iOS app that you can use as of PRTG 13. You can use the newest PRTG app version on iPhone, iPad, and iPod touch as of iOS version 9. You can also use free [push notifications](#)<sup>2830</sup> with this PRTG app (required: at least PRTG for iOS 14.3.6; PRTG 15.4.20).

■ For more information and to download this PRTG app, see the Paessler website: [PRTG for iOS](#). For troubleshooting solutions, see the Knowledge Base: [I have an issue with PRTG for iOS. What can I do?](#)

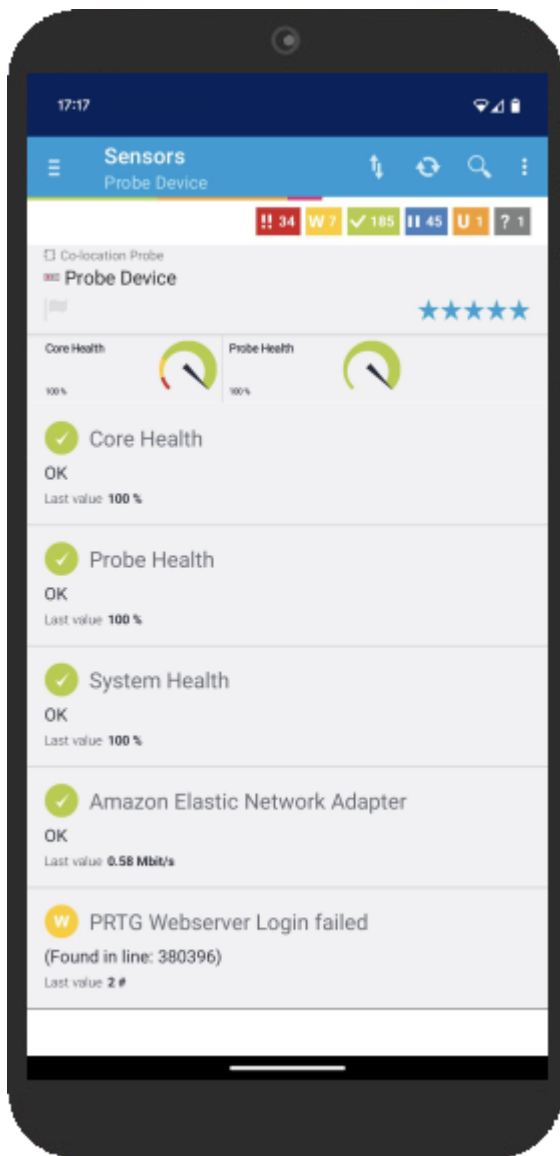


Sensor and channels on PRTG for iOS

## PRTG for Android

PRTG for Android is the Android app that you can use as of PRTG 14. Use it on your smartphone or tablet as of Android version 4.0, or on a Kindle Fire. For full functionality, we recommend that you use at least Android 4.1. You can also use free [push notifications](#) <sup>2830</sup> with the PRTG app (required: at least PRTG for Android 14.3.2; PRTG 15.4.20).

- For more information and to download this PRTG app, see the Paessler website: [PRTG for Android](#). For troubleshooting solutions, see the Knowledge Base: [I have an issue with PRTG for Android. What can I do?](#)



Sensor List on PRTG for Android

## More

### KNOWLEDGE BASE

I have an issue with PRTG for iOS. What can I do?

- <https://kb.paessler.com/en/topic/88395>

I have an issue with PRTG for Android. What can I do?

- <https://kb.paessler.com/en/topic/88151>

Which features do the PRTG apps for iOS or Android support?

- <https://kb.paessler.com/en/topic/60042>

How can I use push notifications with PRTG?

- <https://kb.paessler.com/en/topic/60892>

How do I troubleshoot erratic behavior of push notifications in the PRTG app for desktop or PRTG apps?

- <https://kb.paessler.com/en/topic/86064>

■ PAESSLER WEBSITE

PRTG apps for iOS or Android

- <https://www.paessler.com/prtg/apps/mobile>

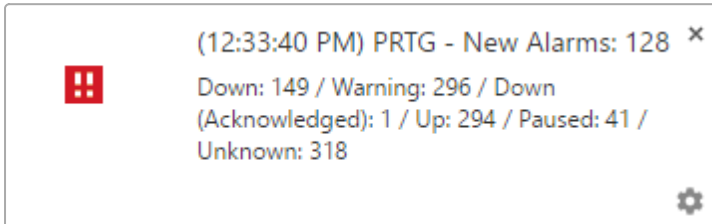
# Part 11

# Desktop Notifications

# 11 Desktop Notifications

While you are logged in to the PRTG web interface with Google Chrome or Mozilla Firefox, PRTG can show notifications on your desktop whenever there are new alarms in your monitoring.

PRTG shows desktop notifications (by default, in the lower-right corner of your desktop) whenever there are new alarms after a page refresh in the PRTG web interface. The notification displays the number of new alarms and the current number of each [sensor status](#)<sup>[181]</sup>.



Example of a Desktop Notification in Google Chrome

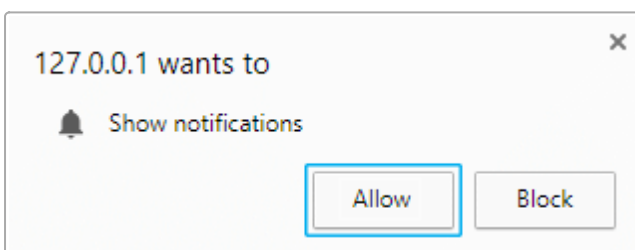
**i** Desktop notifications are not available for Internet Explorer.

## Desktop Notifications Settings

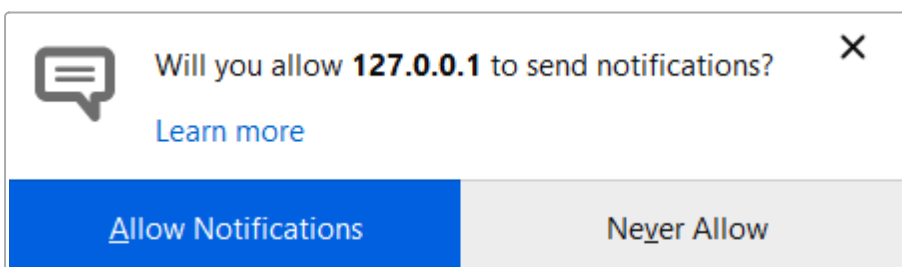
When you log in to the PRTG web interface, a message appears, asking you to allow desktop notifications. You must initially allow the notifications for each installation or profile of Firefox or Google Chrome.

**i** Desktop notifications in Google Chrome are not available for HTTP connections. See section [User Interface](#)<sup>[2856]</sup> for more information.

- In Google Chrome, click Allow to add the URL of the PRTG web interface to the allowed sites.
- In Firefox, click Allow Notifications to add the URL of the PRTG web interface to the allowed sites.



Click 'Allow' to enable Desktop Notifications in Google Chrome



Click 'Allow Notifications' to enable Desktop Notifications in Mozilla Firefox

## Disabling or Re-Enabling Desktop Notifications

To disable or re-enable desktop notifications for the PRTG web interface, edit your browser options:

- In Google Chrome: Click the View site information icon in the address bar of the browser. You can block or re-enable notifications for the PRTG web interface in section Notifications.
- In Mozilla Firefox: Click the Notification permission icon in the address bar of the browser. You can block or re-enable notifications for the PRTG web interface in section Permissions.

## Others

There are some settings that you must define in the [PRTG Administration Tool](#)<sup>[3040]</sup>. For more information, see sections:

- [PRTG Administration Tool on PRTG Core Server Systems](#)<sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#)<sup>[3067]</sup>














# Part 12

# Sensor Technologies

## 12 Sensor Technologies

This section introduces different technologies that PRTG uses for monitoring to give you more background information.

In this section:

- [Monitoring via SNMP](#)  2997
- [Monitoring via WMI](#)  3004
- [Monitoring via SSH](#)  3007
- [Monitoring Bandwidth via Packet Sniffing](#)  3009
- [Monitoring Bandwidth via Flows](#)  3011
- [Bandwidth Monitoring Comparison](#)  3014
- [Monitoring Quality of Service](#)  3016
- [Monitoring Backups](#)  3021
- [Monitoring Virtual Environments](#)  3022
- [Monitoring Databases](#)  3028
- [Monitoring via HTTP](#)  3032

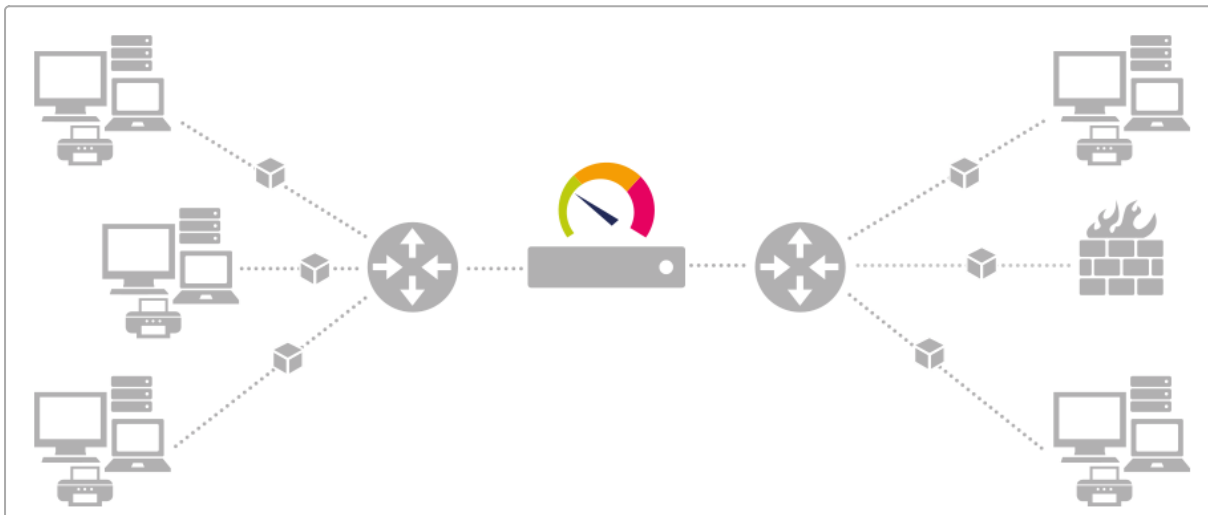
## 12.1 Monitoring via SNMP

Monitoring via the Simple Network Management Protocol (SNMP) is the most basic method of gathering bandwidth and network usage data.

### How SNMP Monitoring Works

SNMP is a set of standards for communication with devices in a Transmission Control Protocol (TCP)/IP network. SNMP monitoring is useful if you are responsible for servers and network devices such as hosts, routers, hubs, and switches. It enables you to keep an eye on network and bandwidth usage, and to monitor important metrics such as uptime and traffic levels.

You can use SNMP to monitor the bandwidth usage of routers and switches on a port-by-port basis, as well as device readings such as memory and CPU load. The target devices must support SNMP. Most devices with enabled SNMP require the same configuration (identical SNMP version and community string). To learn how to set up SNMP on a specific device, search the internet for its name and SNMP configuration.



Network Monitoring via SNMP

When you use a sensor with this technology, PRTG sends small data packets to a device, which in turn trigger reply packets. Compared to other bandwidth monitoring technologies via World Wide Name (WWN), packet sniffing, or Windows Management Instrumentation (WMI), the SNMP option creates the least CPU and network load.

### Reasons to Choose SNMP Monitoring

SNMP is the most commonly used method because it requires minimal bandwidth and CPU cycles. If your network devices support SNMP and/or if you want to monitor large networks with several hundred or thousands of sensors, we recommend that you start with SNMP.

Besides network usage monitoring, another well-known feature of SNMP is the ability to also monitor other network parameters such as CPU load, disk usage, temperature, as well as many other readings, depending on the queried device.

## SNMP Network Issues

To use SNMP for monitoring purposes, it is necessary that User Datagram Protocol (UDP) packets can be bidirectionally sent from the PRTG core server to the target device. This is usually the case in LANs and intranets. For connections across the internet, to a perimeter network (also known as DMZ, demilitarized zone, and screened subnet), or for WAN connections, some changes to the traversed firewalls might be necessary.

Keep in mind that SNMP v1 and v2c are no secure protocols, so you should not use them on the internet or with data connections that are not secure. Only SNMP v3 supports encryption.

## Understanding SNMP Sensors

To better understand and set up SNMP sensors, you might want to learn more about the principles of object identifiers (OID) and Management Information Base (MIB) files.

■ For more information, see the Knowledge Base: [How do SNMP, MIBs and OIDs work?](#)


■ For more information about all SNMP sensors, see section [Available Sensor Types](#) .

## SNMP Versions

PRTG supports three versions of the SNMP protocol: version 1, 2c, and 3.

### SNMP v1

This is the oldest and most basic version of SNMP.

- Pro: Supported by most SNMP-compatible devices.
- Con: Limited security because it only uses a simple password ([community string](#) ) and sends data in clear text (unencrypted). Because of this, you should only use it inside LANs behind firewalls, but not in WANs. SNMP v1 only supports 32-bit counters, which are not enough for high-load (gigabits/second) bandwidth monitoring.


### SNMP v2c

This version adds 64-bit counters.

- Advantage: Supports 64-bit counters to monitor bandwidth usage in networks with gigabits/second loads.
- Disadvantage: Limited security (see SNMP v1).

### SNMP v3

This version adds authentication and encryption to SNMP.

- Advantage: Offers user accounts and authentication for multiple users and optional data packet encryption to increase available security. Has all advantages of SNMP v2c.
- Disadvantage: Difficult to configure and higher overhead for the probe, which reduces the number of devices that you can monitor (see [SNMP Overload and Limitations of the SNMP System](#)  for more information).

## SNMP Traps

Various devices can send SNMP trap messages to notify you of system events.

- PRTG supports SNMP v1 and SNMP v2c traps.
- The destination for SNMP traps is the IP address of the trap receiver, which is the IP address of the probe system to which you add the [SNMP Trap Receiver](#) sensor.

## Which SNMP Version Should I Choose?

This depends on your environment. Here are some guidelines:

- If your network is publicly accessible, you might want to use SNMP v3, which has encryption and secure access. However, this also adds overhead, which results in less performance.
- If your network is isolated or well-protected behind firewalls, the lower security level of SNMP v1 or SNMP v2c might be sufficient.
- If you have a lot of devices to monitor, SNMP v2c is preferable since it has a shorter scanning interval and supports 64-bit counters.

Make sure to set the same SNMP version in the PRTG settings (for example, in the [root group settings](#) <sup>420</sup>) as in the target device. If you select an SNMP version that is not supported by the server or target device, you receive an error message. These error messages often do not explicitly say that you are using the wrong SNMP version and only provide minimum information, such as [cannot connect](#). Similar errors occur when community strings, user names, or passwords do not match.

■ For more information about basic requirements for SNMP monitoring, see the Knowledge Base: [My SNMP sensors don't work. What can I do?](#)

## SNMP Overload and Limitations of the SNMP System

SNMP v1 and v2 scale directly with the performance of the hardware and the speed of the network. In our labs, we can monitor 30,000 SNMP v1 sensors in a 60-second scanning interval with one PRTG core server (and local probe) plus two remote probes with 10,000 sensors each.

SNMP v3 has performance limitations because of the use of encryption. Furthermore, keep in mind that SNMP v3, unlike SNMP v1 and v2c, does not scale with more CPU power. Because of this limitation, PRTG can only handle a limited number of requests per second so that you can use only a limited number of sensors using SNMP v3.

Furthermore, the PRTG core server and probes should run on different computers. If you experience increased values in the [Interval Delay SNMP](#) or [Open Requests](#) channels of the [Probe Health](#) sensor (values above 0 % indicate that the SNMP requests cannot be performed at the desired interval), you need to distribute the load among probes. SNMP v1 and v2 do not have this limitation.

If you run into SNMP overload problems, you have the following options:

- Increase the scanning interval of the SNMP v3 sensors.
- Distribute the SNMP v3 sensors among two or more probes.
- Evenly distribute the SNMP v3 sensors on your devices (about 10 to 100 sensors per device).

- Check if your target devices answer fast enough. Performance issues might also result from slow SNMP v3 devices.
- Switch to SNMP v1 or v2 if you can go without encryption.

## What is the SNMP Community String?

The SNMP community string is similar to a user ID or password that allows access to the statistics of a device. PRTG sends the community string along with all SNMP requests. If the correct community string is provided, the device responds with the requested information. If the community string is incorrect, the device discards the request and does not respond.

- ❗ SNMP community strings are only used by devices that support SNMP v1 and SNMP v2c. SNMP v3 uses safer user name/password authentication, along with an encryption key.

By convention, most SNMP v1/v2c equipment ships with a read-only community string set to the value public. It is standard practice for network managers to change all the community strings to customized values during device setup.

## Check SNMP Capability

Make sure that each target device supports SNMP, and that SNMP is enabled. You can find out whether a device supports SNMP by either going to the vendor's website or checking that it is enabled in the configuration of the device.

- ✂ If you are uncertain whether SNMP is enabled on the target device and works, we recommend that you try [SNMP Tester](#). You can scan for uptime to perform a basic check for SNMP availability of the target device.

### Setup Checklist

1. Enable SNMP on the device.
  2. In the security settings of the device, allow SNMP access for the PRTG core server system.
  3. Allow User Datagram Protocol (UDP) packages to be sent bidirectionally from the PRTG core server to the device.
  4. SNMP requires the use of UDP ports >1023 to the PRTG client side. This is important for your firewall settings.
  5. Make sure that the firmware of the device is up to date.
  6. Select the appropriate SNMP protocol.
- ❗ It is important to know which SNMP version you need to select, because if it is not supported by the server or device you want to monitor, you receive an error message.

■ For more information, see the Knowledge Base: [My SNMP sensors don't work. What can I do?](#)



SNMP Monitoring Overview

## Vendor-specific SNMP Sensors

PRTG offers many vendor-specific SNMP sensors for some common vendors. These sensors are programmed to match the respective end devices. There are also workarounds for known vendor implementation issues, for example, if SNMP has not been fully implemented on an end device according to the RFCs. Here, our vendor-specific sensors still automatically receive the most important values.

### Supported Vendors

- APC
- Buffalo
- Cisco
- Dell
- Fujitsu
- HP

- HPE
- IBM
- Jakarta
- Juniper
- LenovoEMC
- NetApp
- Nutanix
- Poseidon
- QNAP
- Rittal
- SonicWall
- Synology

## Generic SNMP Sensors

PRTG offers several generic sensors that work with almost every device that supports SNMP, the corresponding Management Information Base (MIB) file and OIDs, and it correctly implements the respective RFCs. The standard SNMP libraries of PRTG include predefined, common values for the generic SNMP sensors. You can monitor the following parameters with the generic sensors.

## Operating System-based SNMP Sensors

PRTG also offers several operating system-based SNMP sensors that extend your SNMP monitoring. You can monitor the following parameters with these sensors.

## Custom SNMP Sensors

PRTG also offers custom SNMP sensors. The monitoring capabilities of these sensors extend the scope of the generic sensors. With custom sensors, you can show certain values that are not included in the standard libraries of PRTG. With these sensors, you can monitor most devices that support SNMP and for which PRTG does not have native sensors. Basically, you only need to find out the required OIDs for the desired device readings, for example, in the vendor's documentation for your hardware device.

- For more information, see the Knowledge Base: [How do I find out which OID I need for an SNMP Custom sensor?](#)

## More

### ■ KNOWLEDGE BASE

How do SNMP, MIBs and OIDs work?

- <https://kb.paessler.com/en/topic/653>

My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>



The interface numbers on my switch keep changing. What can I do?

- <https://kb.paessler.com/en/topic/62217>

What can I check if SNMP and SSH sensors throw timeout and auth errors?

- <https://kb.paessler.com/en/topic/63794>

What can I monitor with the SNMP Custom Table sensor?

- <https://kb.paessler.com/en/topic/68539>

How can I import my MIB files into PRTG?

- <https://kb.paessler.com/en/topic/733>

How do I find out which OID I need for an SNMP Custom sensor?

- <https://kb.paessler.com/en/topic/903>

Can't find a sensor for my device in PRTG but I believe it supports SNMP. How to proceed?

- <https://kb.paessler.com/en/topic/65638>

## PAESSLER TOOLS

MIB Importer and SNMP Tester

- <https://www.paessler.com/tools>

## PAESSLER WEBSITE

IT Explained - What is SNMP?

- <https://www.paessler.com/it-explained/snmp>

Resource Center - SNMP Monitoring

- <https://www.paessler.com/support/it-knowledge/resources>

## VIDEO TUTORIAL

SNMP basics

- <https://www.paessler.com/support/videos-and-webinars/videos/snmp-basics>

SNMP debugging

- <https://www.paessler.com/support/videos-and-webinars/videos/snmp-debugging>

## 12.2 Monitoring via WMI

You can monitor Windows systems via Windows Management Instrumentation (WMI) and [Windows performance counters](#)<sup>[3004]</sup>. WMI is the Microsoft base technology for monitoring and managing Windows-based systems. PRTG uses it to access data of various Windows configuration parameters and status values. Note that sensors that use the WMI protocol generally have a high impact on system performance. In addition to strict WMI sensors, there are sensors that can use performance counters to monitor Windows systems.

To monitor via WMI and performance counters, it is usually sufficient to provide [credentials for Windows systems](#)<sup>[422]</sup> in PRTG. However, monitoring via WMI is not always trivial and can cause issues.

■ If you run into issues with WMI, see the Knowledge Base: [My WMI sensors don't work. What can I do?](#)

It is also possible to use Simple Network Management Protocol (SNMP) for Windows devices. The same information is often available using any of these protocols. Regarding performance, the preference is SNMP, then WMI or performance counters.

### How WMI Works

WMI allows access to the data of many Windows configuration parameters, as well as system status values. Access can be local or remote via a network connection. WMI is based on [COM](#) and [DCOM](#) and is integrated in Windows versions as of Windows Server 2000. PRTG officially supports WMI as of Windows 7.

ⓘ WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the PRTG probe service only runs with 32-bit support. Without it, WMI sensors do not work.

To monitor remote machines, WMI sensors need Active Directory account credentials to have access to the WMI interface. You can enter these credentials in the settings of the parent device or group, or in the [root group](#)<sup>[420]</sup>. The sensor then inherits these settings.

ⓘ Sensors using the WMI protocol generally have a high impact on the system performance. Try to stay below 200 WMI sensors per [probe](#)<sup>[124]</sup>. Above this number, consider using [remote probes](#)<sup>[8198]</sup> for load balancing.

■ For more information about all WMI sensors, see section [Available Sensor Types](#)<sup>[3282]</sup>.

### Monitoring Windows Systems: Performance Counters

Besides sensors that can monitor Windows systems only via WMI, PRTG provides sensors that can use a [hybrid](#) approach. If you choose the hybrid approach, these sensors first try to query data via Windows performance counters using the [Remote Registry](#) service. These Windows sensors use WMI as a fallback if performance counters are not available or cannot be read out. When running in fallback mode, PRTG tries to connect to performance counters again after 24 hours. You can change the Preferred Data Source in the Windows Compatibility Options in the [device settings](#)<sup>[597]</sup>.

ⓘ You can identify these hybrid sensors by looking at their categories, for example, in the [Add Sensor](#)<sup>[414]</sup> dialog. Search directly for "windows" and select "Performance Counters" as Technology Used. Among them are various sensors with "Windows" in the name, as well as some Hyper-V sensors.

## Limitations of WMI on Windows Server 2008 (R1)

You should be aware that the performance of WMI-based monitoring is drastically limited when the monitoring station or the monitored client runs on Windows Server 2008 (R1). When it comes to network monitoring via WMI, Windows Server 2008 R2 is many times faster than Windows Server 2008 (R1).

- i** These are not limitations of PRTG. They arise from the WMI functionality built into the Windows operating systems mentioned.
- i** These limitations also apply to Windows Vista, which is no longer officially supported. You can still monitor machines that run Windows Vista, but the PRTG core server and probes are no longer supported on this operating system.

The results of our tests are:

- As of Windows Server 2008 R2 or Windows 7, you can run most WMI sensors if you provide optimal conditions, such as running the PRTG core server system and the target systems exclusively under Windows Server 2008 R2 and being located within the same LAN segment. Actual performance can be significantly lower depending on the network topology and the WMI health of the target systems. We have seen configurations that could not go beyond 500 sensors (and even less).
- On Windows 2008 (R1), you can run about 300 WMI sensors with a 1-minute scanning interval.
- The more Windows 2008/Windows 7 client systems you have in your network, the more the WMI monitoring performance is affected.
- System performance (CPU, memory, etc.) of virtualization does not strongly affect WMI monitoring performance.

If you want to use WMI for network monitoring of more than 20 or 30 systems, consider the following rules:

- Do not use Windows 2008 (R1) as monitoring stations for WMI-based network monitoring.
- Use at least Windows Server 2008 R2 for WMI-based network monitoring instead.
- Consider setting up remote probes for the WMI monitoring. You still get far better WMI monitoring performance with a remote probe on a virtual machine (VM) running Windows Server 2008 R2 than on any physical system running Windows 2008.
- Consider switching to SNMP-based monitoring for large networks. Using SNMP, you can monitor 10 times as many objects than with WMI on the same hardware.

## More

### KNOWLEDGE BASE

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Which WQL queries are used by the PRTG WMI sensors?

- <https://kb.paessler.com/en/topic/8783>

Why do I receive the sensor error message 'Connection could not be established (code: PE015)'?

- <https://kb.paessler.com/en/topic/81843>

 VIDEO TUTORIAL

Bandwidth monitoring with SNMP and WMI

- <https://www.paessler.com/support/videos-and-webinars/videos/bandwidth-monitoring-basic>

 PAESSLER TOOLS

WMI Tester

- <https://www.paessler.com/tools/wmitester>

## 12.3 Monitoring via SSH

Monitoring via Secure Shell (SSH) enables you to gather performance and system data from many Linux and Unix distributions, as well as from certain macOS X systems. If your system is supported, this monitoring technology works without any additional software on the target systems.

### How Monitoring via SSH Works

To monitor remote machines via SSH, PRTG needs the credentials (preferably root access) of the devices. If you use SSH sensors, you can enter the necessary credentials in the [settings](#)<sup>[201]</sup> of the parent device or group, or in the root group, in the Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems section. The sensors then inherit these settings by default.

With each scanning interval, PRTG logs in to your devices and queries data by executing specific commands.

■ For more information about all SSH sensors, see section [Available Sensor Types](#)<sup>[3232]</sup>.

■ For a list of encryption algorithms that the SSH sensors support, see the Knowledge Base: [Which encryption algorithms do PRTG SSH sensors support?](#)

### Limitations When Using SSH Monitoring

Because of the plurality of Linux/Unix derivatives, SSH sensors cannot support all distributions on the market. Also, only certain macOS systems are supported.

■ For a list of successfully tested distributions, see the Knowledge Base: [Which Linux or macOS distributions are supported by the Linux/Unix sensors \(SSH, SNMP\)?](#)

### Authentication via SSH Private Key

PRTG supports authentication via password or via private key.

When you use a private key, make sure to note the following:

- Provide the key in [OpenSSH RSA](#) format.
- The key cannot be encrypted. PRTG does not support password-protected keys.
- The key must be provided as an [RSA](#) key; you cannot use [DSA](#) keys.

When you provide an unencrypted RSA private key in OpenSSH RSA format, copy the entire key, including the

```
-----BEGIN RSA PRIVATE KEY-----
```

and

```
-----END RSA PRIVATE KEY-----
```

lines, into the designated text field in PRTG and Save your settings. Once you have pasted in and saved the private key, PRTG shows it as

```
*****
```

Make sure that a corresponding public key exists on the target device.

- For more information about how to convert and use an SSH key, see the Knowledge Base: [How can I use private keys for my SSH sensors with PRTG?](#)

## More

### ■ KNOWLEDGE BASE

Which encryption algorithms do PRTG SSH sensors support?

- <https://kb.paessler.com/en/topic/90689>

Which Linux or macOS distributions are supported by the Linux/Unix sensors (SSH, SNMP)?

- <https://kb.paessler.com/en/topic/6733>

How can I use private keys for my SSH sensors with PRTG?

- <https://kb.paessler.com/en/topic/32883>

How do I enable SSH on my macOS system?

- <https://kb.paessler.com/en/topic/33113>

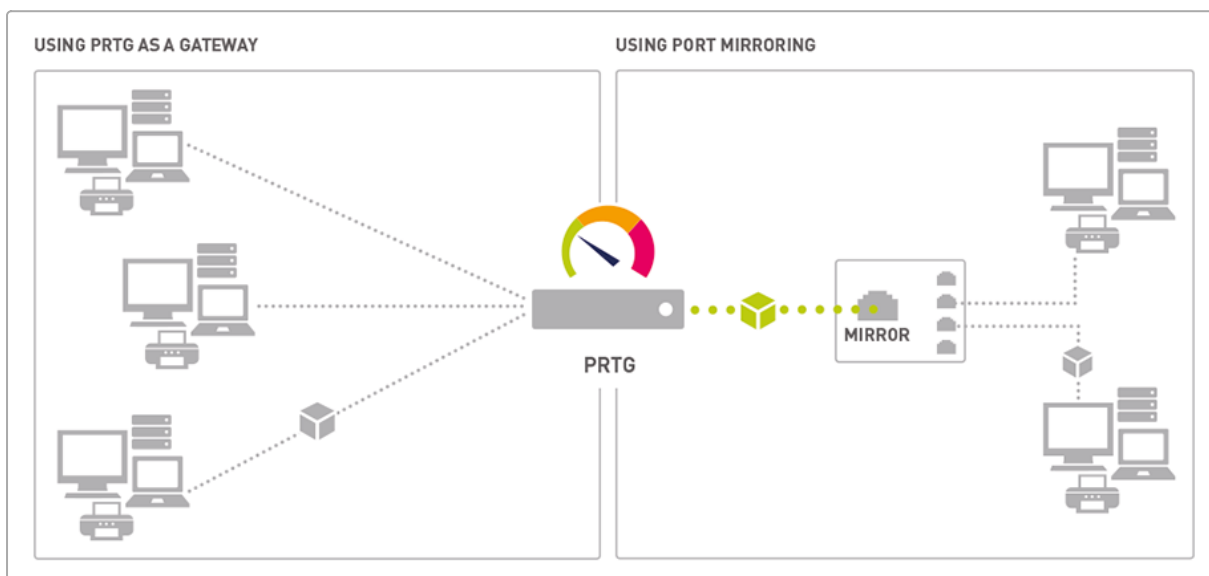
## 12.4 Monitoring Bandwidth via Packet Sniffing

Packet sniffing comes into consideration if your network devices do not support the Simple Network Management Protocol (SNMP) or Flow (NetFlow, jFlow, sFlow, IPFIX) to measure bandwidth usage and if you need to differentiate the bandwidth usage by network protocol and/or IP addresses.

❶ Packet Sniffer sensors support [Toplists](#)<sup>[2707]</sup> (for example, Top Talkers or Top Connections).

### How Packet Sniffing Works

If you need to know what applications or IP addresses cause the traffic in your network, you can use a packet sniffer. A packet sniffer looks at every single data package that travels through your network for accounting purposes.



Monitoring with PRTG via Packet Sniffer Sensors

PRTG can analyze the packets that pass the network card of a PC or you can connect it to the monitoring port of a switch. To calculate bandwidth usage, PRTG inspects all network data packets either passing the PC's network card (shown on the left side in the schema above) or the data packages that a monitoring port of a switch (right side) sends with its built-in packet sniffer. Using remote probes, you can set up packet sniffers anywhere in your network.

❶ Packet Sniffer sensors use the [npcap library](#) to monitor traffic.

■ For more information, see section [Add Remote Probe](#)<sup>[3196]</sup>.

[Comparing](#)<sup>[3014]</sup> the four bandwidth monitoring technologies that PRTG provides (SNMP, Windows Management Instrumentation (WMI), flows, and packet sniffing), packet sniffing creates the most CPU and network load, so you should only use it in small to medium-sized networks, on dedicated computers for larger networks, or for individual computers.

## Reasons to Choose Packet Sniffing

It is important to understand that the packet sniffer can only access and inspect data packages that actually flow through the network interfaces of the probe system. This is fine if you only want to monitor the traffic of this machine (for example, your web server). In switched networks, only the traffic for a specific machine is sent to each machine's network card, so PRTG usually cannot discern the traffic of the other machines in the network.

If you also want to monitor the traffic of other devices in your network, you must use a switch that offers a monitoring port or port mirroring configuration (Cisco calls it Switched Port Analyzer (SPAN)). In this case, the switch sends a copy to the monitoring port of all data packages traveling through the switch. As soon as you connect one of the probe system's network cards to the switch's monitoring port, PRTG can analyze the entire traffic that passes through the switch.

An alternative is to set up the PRTG core server system as the gateway for all other computers in the network.


## Packet Sniffer Sensors

PRTG offers the following packet sniffer sensors:

- [Packet Sniffer](#)
- [Packet Sniffer \(Custom\)](#)

## Header-Based Packet Sniffing

For packet sniffing, PRTG looks at the IP addresses and ports of source and destination to assess the protocol. This is a very fast method and saves system resources.

 Sometimes, this method is not fully accurate. For example, it is not possible to identify HTTP traffic on ports other than [80](#), [8080](#), and [443](#) as HTTP. HTTP traffic on non-standard ports would not be accounted as such.

## More

### KNOWLEDGE BASE

How can I change the default groups and channels for flow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>



## 12.5 Monitoring Bandwidth via Flows

Using Flow (NetFlow, jFlow, sFlow, IPFIX) protocols, you can monitor the bandwidth usage of all packets going through a device. In PRTG, you can view [Toplists](#) for all xFlow sensors.

xFlows are monitoring data pushed from network devices to PRTG. You can use them to monitor where and how much data is traveling to and from. This way, they determine which machine, protocol, or user is consuming bandwidth. PRTG supports the following xFlow types:

- NetFlow v5/v9 and IPFIX: Originally introduced by Cisco and supported by several vendors.
- jFlow: Traffic sampling technology introduced by Juniper networks.
- sFlow: Short for [sampled flow](#), introduced by HP. sFlow uses statistical sampling of the traffic at defined intervals to achieve scalability for high volume interfaces.

You can also use [packet sniffing](#) for bandwidth monitoring if your hardware does not support any of these xFlow versions.

### How Flow Monitoring works

You can measure bandwidth usage by IP address or by application in a network, using one of the flow protocols. They are the best choice especially for networks with high traffic (connections with hundreds of megabits or gigabits).


For flow monitoring, the router gathers bandwidth usage data (flows), aggregates it, and sends information about it to PRTG using User Datagram Protocol (UDP) packets. When you use sampling (mandatory for sFlow), only information about every n-th packet is sent to PRTG, which reduces CPU load a lot. Because the switch already performs an aggregation of traffic data beforehand, the flow of data to PRTG is much smaller than the monitored traffic. This makes flow the ideal option for high traffic networks that need to differentiate the bandwidth usage by network protocol and/or IP addresses.

### NetFlow and IPFIX Monitoring

The NetFlow (and IPFIX) protocol is mainly used by Cisco devices. Once configured, the router sends a NetFlow or IPFIX packet for each data flow to the monitoring system running on a probe. You can filter and evaluate the data in PRTG. Different NetFlow and IPFIX sensors are available: The basic sensors offer predefined channel definitions, the custom variants enable you to define your own channels.

The advantage of using NetFlow or IPFIX:

- Generates little CPU load on the router itself (according to Cisco, 10,000 active flows create about 7% additional CPU load; 45,000 active flows account for about 20% additional CPU load).
- Generates less CPU load on the PRTG core server system compared to Packet Sniffer sensors.

 You must enable NetFlow or IPFIX export on the target device. The device must send a flow data stream to the IP address of the probe system on which you set up the NetFlow or IPFIX sensor.

 You can monitor Juniper [jFlow](#) with the corresponding sensors as well. Basically they are adjusted NetFlow v5 sensors.

ⓘ NetFlow Lite monitoring is possible using the Sampling Mode of the [NetFlow v9](#) sensor or of the [NetFlow v9 \(Custom\)](#) sensor. You can turn on the sampling mode and define a suitable Sampling Rate in the sensor settings. Note that NetFlow Lite monitoring might not work in every case even with active sampling mode.

## sFlow Monitoring

sFlow works similar to NetFlow monitoring. The router sends data flow packets to the monitoring system running on a probe. The most obvious difference between the two flow protocols: With sFlow, not all of the traffic is analyzed, but only every n-th packet.

The advantage is clear: There is less data to analyze, there is less CPU load needed, and less monitoring traffic is generated. Nevertheless, you can get a good insight into your network bandwidth usage.

ⓘ PRTG supports sFlow v5.

## Set Up Flow Sensors

Find details on how to set up the different flow sensors in the following sections:

- [NetFlow v5](#)
- [NetFlow v5 \(Custom\)](#)
- [NetFlow v9](#)
- [NetFlow v9 \(Custom\)](#)
- [IPFIX](#)
- [IPFIX \(Custom\)](#)
- [sFlow](#)
- [sFlow \(Custom\)](#)
- [jFlow v5](#)
- [jFlow v5 \(Custom\)](#)

## Limitations

For example, with a dual core, 2.5 Ghz hardware system, you can process about 100,000 flows per second for one flow stream. Using sampling, the number of actual flows can be much higher. When using complex filters, the value can be much lower. For example, with a router sending about 2,000 flows/second (which corresponds to mixed traffic at gigabit/second level without sampling) you can expect to configure up to 50 flow sensors operating properly.

PRTG internally monitors its own flow processing. You can see decreased values in the Health channels of the [Core Health](#) and [Probe Health](#) sensors as soon as flow packets are not processed because of an overload (you find these sensors on the local probe device).

If you experience an overload, consider using sampling or setting up multiple probes and distributing the flow streams to them. We recommend that you do not add more than 50 flow sensors per probe.

- ① IPv6 flows are supported by NetFlow v9 sensors and IPFIX sensors, other flow sensors only support IPv4.

## More

### ■ KNOWLEDGE BASE

Can I add custom channels to standard Packet Sniffer and NetFlow sensors?

- <https://kb.paessler.com/en/topic/2143>

What filter rules can be used for custom Packet Sniffing, Flow, or IPFIX sensors?

- <https://kb.paessler.com/en/topic/483>

How do the channel definitions for custom Packet Sniffing, Flow, and IPFIX sensors work?

- <https://kb.paessler.com/en/topic/473>

Does my Cisco device (router/switch) support NetFlow export?

- <https://kb.paessler.com/en/topic/5333>

Do you have any configuration tips for Cisco routers and PRTG?

- <https://kb.paessler.com/en/topic/563>

How do I monitor Cisco ASA firewalls using NetFlow 9 and PRTG?

- <https://kb.paessler.com/en/topic/1423>

How can I change the default groups and channels for flow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

What is the Active Flow Timeout in flow sensors?

- <https://kb.paessler.com/en/topic/66485>

### ✂ PAESSLER TOOLS

NetFlow Generator and NetFlow Tester

- <https://www.paessler.com/tools>

## 12.6 Bandwidth Monitoring Comparison

The following table shows the differences between the four bandwidth monitoring methods available in PRTG:

Category	<a href="#">WMI</a> <sup>[3004]</sup>	<a href="#">SNMP</a> <sup>[2997]</sup>	<a href="#">Packet Sniffer</a> <sup>[3009]</sup>	<a href="#">Flow (IPFIX, NetFlow, sFlow, jFlow)</a> <sup>[3011]</sup>
Setup	Medium	Low Low to high (depending on filter rules used)	Can be high (for example, the switch must be configured)	
Traffic filtering	No	No	Yes	Yes
Differentiate bandwidth usage by protocol or IP addresses	No	No	Yes	Yes
PRTG can show Toplists (Top Talkers, Top Connections, Top Protocols, custom)	No	No	Yes	Yes
Filter bandwidth usage by IP address	No	No	Yes	Yes
Filter bandwidth usage by MAC address	No	No	Yes	No
Filter bandwidth usage by physical network port	Yes	Yes	No	No
Monitor network parameters other than bandwidth usage	Yes	Yes	No	No
CPU load on the PRTG core server system	Medium	Low	Higher, depends on the amount of traffic	Higher, depends on the amount of traffic
Excess bandwidth usage of monitoring	Small	Small	None (except when monitoring switch ports are used)	Depends on the traffic

## More

### ■ KNOWLEDGE BASE

Should I use SNMP, Flow (IPFIX/NetFlow/sFlow) or Packet Sniffing for my monitoring?

- <https://kb.paessler.com/en/topic/923>

How do I differentiate between excessive bandwidth usage with PRTG?

- <https://kb.paessler.com/en/topic/2923>

## 12.7 Monitoring Quality of Service

PRTG can monitor the Quality of Service (QoS) in a network with dedicated QoS sensors, as well as Cisco IP service level agreement (SLA) and Cisco Class Based Quality of Service (CBQoS). Slight variations in network parameters like jitter, packet loss, or packet delay variation (PDV) usually have only little effect on Transmission Control Protocol (TCP) based services (for example, HTTP and Simple Mail Transfer Protocol (SMTP)). But for User Datagram Protocol (UDP) based services like Voice over IP (VoIP) and video streaming, a steady stream of data packets is crucial. The sound quality of a VoIP call drops noticeably when UDP packets are not received in time, or if packets are lost or in the wrong order.

As a rule of thumb for good quality of service (from a VoIP perspective), it is important to have low measurements for jitter (less than 20 to 50 ms) and PDV (less than 100 ms), and preferably **zero** measurements for packet loss, duplicated packets, or packets in wrong order.

For QoS measurements, four sensors are available:

- [QoS \(Quality of Service\) One Way](#)
- [QoS \(Quality of Service\) Round Trip](#)
- [Cisco IP SLA](#)
- [SNMP Cisco CBQoS](#)

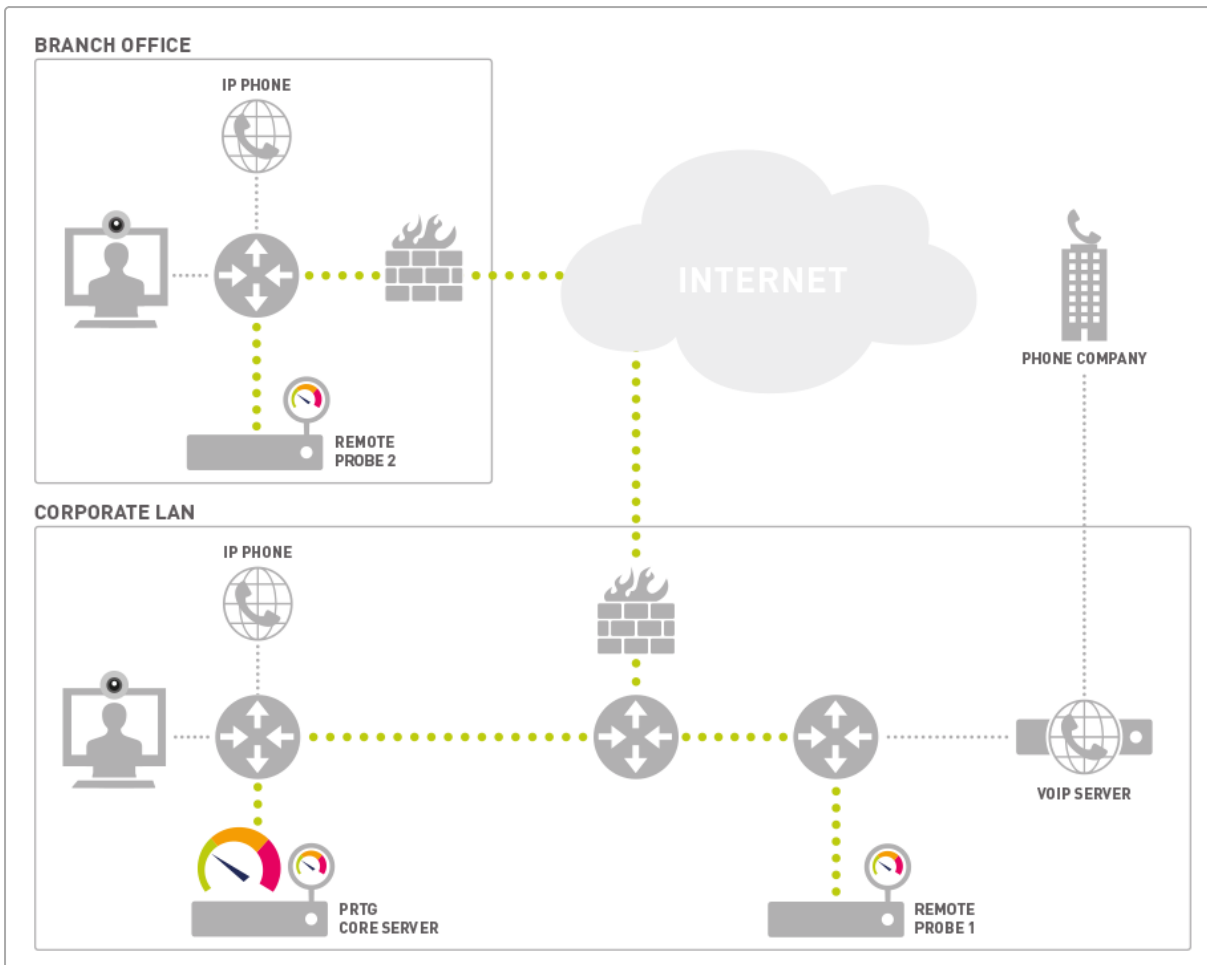
### QoS (Quality of Service) Sensors

The QoS sensors monitor the quality of a network connection by measuring the following parameters:

- Jitter in ms according to RFC 3550
- PDV in ms according to RFC 3393
- Lost packets in %
- Out-of-order packets in %
- Duplicated packets in %

The QoS sensors measure the quality of service by sending UDP packets between two probes. This means that you can test any network connection in your network by placing a [remote probe](#) on (or near) each end of the connection and measuring the connection quality between them. This way, you can find network issues that can affect VoIP sound quality or cause video streaming issues.

■ You can also use the QoS (Quality of Service) Round Trip sensor without installing a remote probe at the connection endpoint. For more information about the PRTG QoS Reflector, see the Knowledge Base: [How can I monitor QoS round trips without using remote probes?](#)



Monitoring Quality of Service with PRTG

The measurements for QoS monitoring are taken between two probes. So the first step is to place two PCs running a remote probe on (or near) both ends of the connection that you want to monitor. As an alternative, the local probe on the PRTG core server system can also be used as one end, or you can use the PRTG QoS Reflector (see the [Knowledge Base](#)) to bounce the packets when monitoring QoS roundtrips. If any firewalls, packet filters, or network address translation (NAT) systems are used, you must configure them as necessary so that the UDP packets can reach the target probe.

Create a new QoS sensor on a probe device, or, if you use the QoS (Quality of Service) Round Trip sensor, on any device. With the settings for the number and for the size of the packets, you can configure the test data stream. 1,000 packets of 172 bytes each is a good start, but if your applications use larger packets, you might want to enter other values here. Try to configure the test streams with parameters similar to that of the UDP services you are using across this connection.

- Find details about settings in the sections [QoS \(Quality of Service\) One Way](#) sensor and [QoS \(Quality of Service\) Round Trip](#) sensor.

## Cisco IP SLA Sensor

Wikipedia describes IP SLA as [a feature included in the Cisco IOS Software that can allow administrators the ability to Analyze IP Service Levels for IP applications and services. IP SLA uses active traffic-monitoring technology to monitor continuous traffic on the network. This is a reliable method in measuring over head network performance.](#) IP SLA is mostly used to monitor the sound quality of VoIP traffic.

If you have not done so already, add a device that represents the Cisco target device. Then create a new Cisco IP SLA sensor on this device.

■ Find details about settings in section [Cisco IP SLA](#) sensor.

This feature is only available in the more expensive Cisco devices. If you do not have IP SLA-capable routers and switches, you can still get similar information with QoS sensors (see [above](#)) that do not require any special hardware.

PRTG monitors the following parameters: Impairment Calculated Planning Impairment Factor (ICPIF), Mean Opinion Score (MOS), Average Jitter, Packets Lost, Packets Out of Sequence, Packets Late, Average Round Trip Time (RTT), Domain Name System (DNS) RTT, TCP RTT, Transaction RTT.

Two of these parameters are especially interesting for VoIP: MOS and ICPIF.

## SNMP Cisco CBQoS Sensor

Cisco CBQoS provides information about QoS of Cisco network devices that support the [Modular QoS Command-Line Interface \(MQC\)](#). With Class Based QoS, you can obtain monitoring data that includes summary counts and rates by traffic class before and after the enforcement of QoS policies, according to Cisco's CBQoS Management Information Base (MIB) definition.

PRTG determines CBQoS data via SNMP. The corresponding sensor is available as of PRTG 13.x.5. CBQoS is available in Cisco IOS by default as of version 12.4(4)T.

To monitor CBQoS, add a device to PRTG for the Cisco target device. Then create a new SNMP Cisco CBQoS sensor on this device.

■ See section [SNMP Cisco CBQoS](#) sensor for more details.

This sensor supports the following CBQoS classes:

- Class Map: statistical data about class maps, such as pre-policy and post-policy packets and sizes, drop packets and size, as well as no-buffer drop packets
- Match Statement: statistical data about match statement specific information, such as pre-policy packets and size
- Queueing: statistical data about queueing actions, such as current and maximum queue depth, drop packets, and drop size

You can select the desired CBQoS entries that you want to monitor while creating the sensor. The available entries are specified with their particular connections, their descriptions, and class types.



## Voice over IP

For MOS measurements, Cisco conducted a panel test where a wide range of listeners judged the quality of voice samples sent using particular codecs, on a scale of 1 (poor quality) to 5 (excellent quality). The Cisco device calculates the corresponding value for the network connection based on network parameter measurements like jitter and packet loss.

■ The Cisco IP SLA sensor reads out the MOS directly from the Cisco device. For the QoS (Quality of Service) One Way sensor and the QoS (Quality of Service) Round Trip sensor, PRTG calculates the MOS by itself. For more information, see the Knowledge Base: [How does PRTG calculate the MOS score for QoS sensors?](#)

The values and their meanings are:

MOS	Quality	Expected Quality Impairment
5	Excellent	Imperceptible
4	Good	Perceptible, but not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying

The second interesting parameter ICPIF is the sum of measured impairment factors minus a user-defined access Advantage Factor that is intended to represent the user's expectations, based on how the call was placed (for example, a mobile call versus a land-line call) (quoted from the Cisco website).

Upper Limit for ICPIF	VoIP Call Communication Quality
5	Very good
10	Good
20	Adequate
30	Limiting case
45	Exceptional limiting case
55	Customers likely to react strongly (complaints, change of network operator)

## More

### ■ KNOWLEDGE BASE

How can I monitor QoS round trips without using remote probes?

- <https://kb.paessler.com/en/topic/61176>

How does PRTG calculate the MOS score for QoS sensors?

- <https://kb.paessler.com/en/topic/59491>

### ■ PAESSLER WEBSITE

How to connect PRTG through a firewall in 4 steps

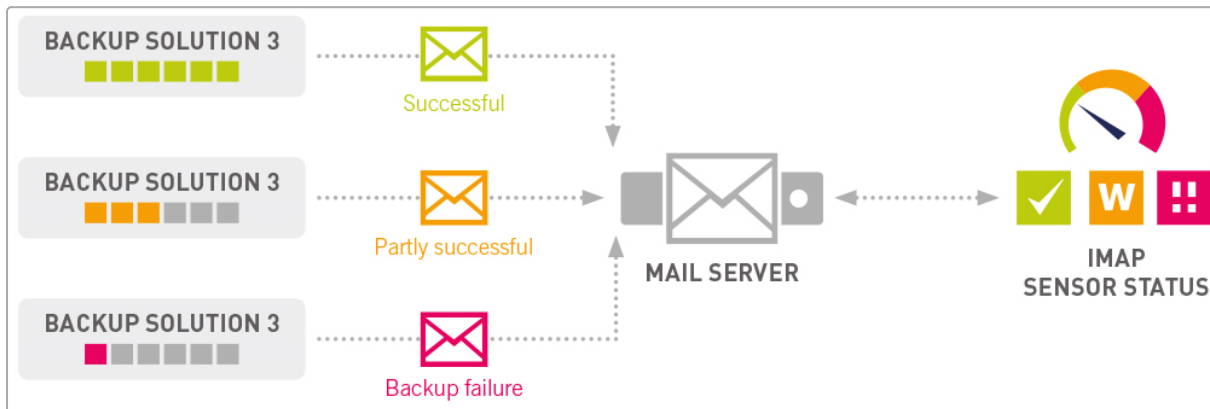
- <https://www.paessler.com/support/how-to/firewall>

## 12.8 Monitoring Backups

Monitoring your backup software enables you to be sure that your recent backups succeeded. With PRTG, you can check the email notifications of various backup jobs. You only need to do two things for backup monitoring:

1. Configure your backup software to send emails to a dedicated email account.
2. Configure the [IMAP](#) sensor for backup monitoring.

PRTG analyzes the backup emails for you and sets the status of the IMAP sensor accordingly. This way you see the states of all your backup jobs.



Backup Monitoring via Email

### Setting up Backup Monitoring

Refer to our Knowledge Base for a step-by-step tutorial on how to monitor your backup jobs: [How can I monitor my backup software to be sure backup succeeded last night?](#)

### More

#### KNOWLEDGE BASE

How can I monitor my backup software to be sure backup succeeded last night?

- <https://kb.paessler.com/en/topic/47023>

Can I analyze multipart emails using the IMAP sensor?

- <https://kb.paessler.com/en/topic/63532>

## 12.9 Monitoring Virtual Environments

Monitoring your complete IT infrastructure in a comprehensive way usually means monitoring not only your physical infrastructure, but also your virtual environments. With the layer of virtualization added to the layers that represent your physical hardware, it also becomes necessary to plan beforehand how you want to logically set up your monitoring infrastructure.

### Monitoring All Layers of Your IT Infrastructure

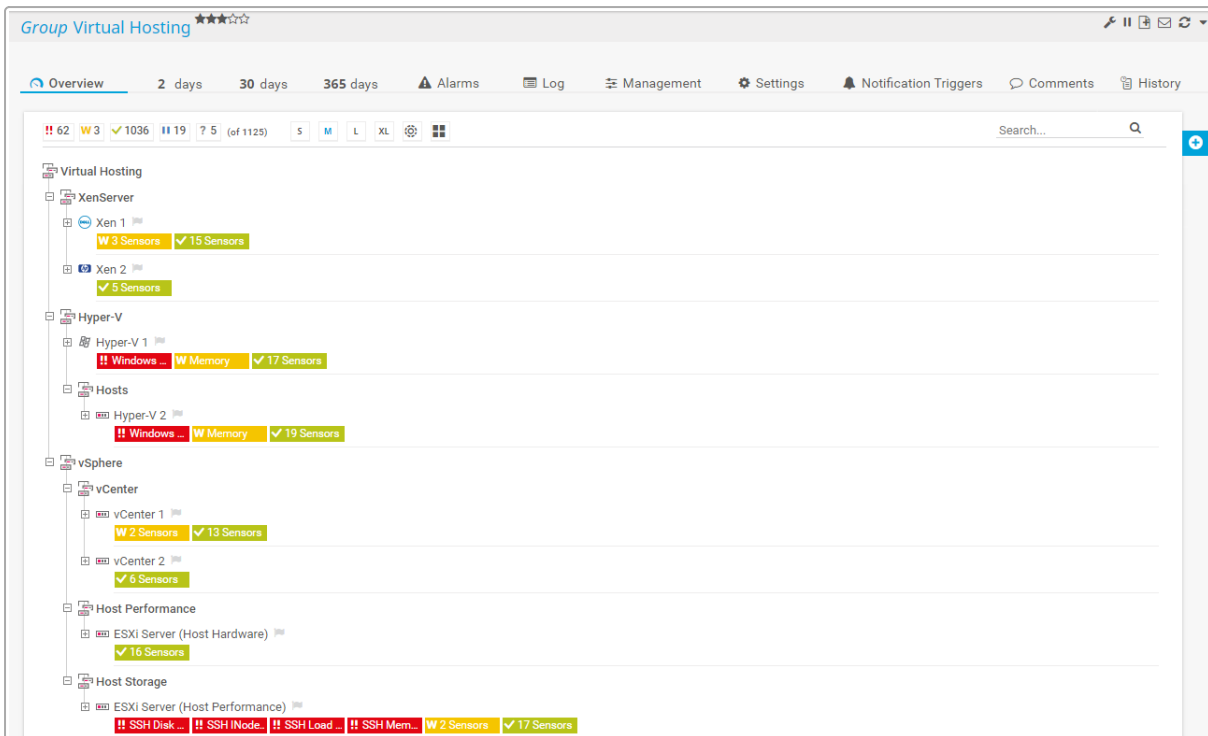
In general, you can assume that with the layer of virtualization, you need to monitor a total of four layers in your IT infrastructure.

Layer	Description
Hardware (Server Racks)	<p>Usually, you monitor most of the hardware components in your network with <a href="#">SNMP sensors</a><sup>[3263]</sup>. With <a href="#">this monitoring technology</a><sup>[2997]</sup>, you can gather monitoring data such as CPU load, memory, and disk space. You can also get information about the network traffic and bandwidth usage of your routers and switches.</p> <p>Alerts can tell you if there is an issue with a hardware component or if hardware resources are running out. In addition, you can identify potential bottlenecks that might affect your virtualized infrastructure.</p>
Host Server Hardware	<p>We recommend that you explicitly monitor the host hardware of your virtualization solution. If you have issues with your virtual machines (VM), the origin might be a host hardware failure. You should closely monitor your VM host servers to be alerted if the hardware status changes in any significant way.</p> <p>Besides the standard hardware sensors, PRTG provides specific sensors for various virtualization host servers. The following monitoring data of your host servers can prevent issues in virtualized environments:</p> <ul style="list-style-type: none"> <li>▪ VMware: current reading and health status (via Web-based Enterprise Management (WBEM)), a general status as shown in vSphere (via Simple Object Access Protocol (SOAP)), and disk space of a VMware data store (via SOAP)</li> <li>▪ Hyper-V: host health-critical values; deposited pages; network traffic; CPU usage of guests, hypervisor, and in total</li> <li>▪ Citrix XenServer: CPU, memory, and network usage; the number of running VMs on the host server; and load average</li> </ul>
Resource Usage of VMs	<p>VMs run on their particular host servers. PRTG can show you the status of single VMs and several of their performance counters. You might want to know which resources a single VM uses and needs, but we do not recommend that you monitor single VMs in every case because it has a noticeable influence on overall performance. Often, it is sufficient to only monitor VMs that are critical for your network. If a VM reaches its capacity limits, PRTG can alert you so that you can take the respective steps to solve the issue.</p>

Layer	Description
	<p>Indicators for a healthy VM that you can monitor with PRTG:</p> <ul style="list-style-type: none"> <li>▪ VMware: CPU and memory usage, disk read and write speed, read and write latency, and network usage</li> <li>▪ Hyper-V: CPU usage, disk read and write speed</li> <li>▪ Citrix XenServer: CPU usage and free memory</li> </ul>
<p>Operating Systems of VMs</p>	<p>You can monitor, for example, the Windows operating system of a single VM with the standard <a href="#">WMI sensors</a><sup>[3282]</sup>. <a href="#">With this technology</a><sup>[3004]</sup>, you can access data of various Windows parameters. Other operating systems like Linux/macOS can make data available via <a href="#">SSH</a><sup>[3007]</sup> and SNMP.</p> <p>The status of the operating systems on your VMs can indicate potential issues. You can monitor these but be careful with regard to performance considerations. This is because sensors using the WMI protocol have a high impact on system performance, so you should only monitor operating systems that are critical for your infrastructure. Furthermore, you do not need to monitor every item multiple times. For example, it might be sufficient to monitor free disk space only as a needed resource of the actual VM, not for the VM's operating system itself.</p>

## Monitoring the Virtual Infrastructure

To monitor your IT infrastructure, best practice is to first set up the monitoring of your data center's hardware layer in PRTG. This way, you can detect potential bottlenecks that might have an impact on your virtual servers. Then, you can prepare to start monitoring your virtual environment. If you use several solutions for virtual hosting, it is also a good idea to group related host servers, their VMs, and the operating systems. The screenshot below shows a possible structure of monitoring a virtual environment with PRTG.



Grouped Virtual Components

At the top level, you can see the [Virtual Hosting](#) group. This group contains several subgroups for the virtualization solutions Citrix [XenServer](#), Microsoft [Hyper-V](#), and VMware [vSphere](#). The [vSphere](#) group, for example, has three subgroups: we monitor the vCenter VMs and the vCenter Windows operating system ([vCenter](#) group), the performance of the host server ([Host Performance](#) group), and the storage system of the host ([Host Storage](#) group).

## Devices for Physical Hosts

In PRTG, set up devices that represent the physical hosts of your VMs. For example, for your VMware hosts, add devices that represent the ESXi servers. For Hyper-V, add devices that represent your Hyper-V host servers. For Citrix, add devices that represent your XenServers.

Then you can add suitable sensors to the host server devices. If you run the [auto-discovery](#)<sup>[254]</sup>, many sensors are automatically created. Several preconfigured host hardware sensors are available:

- [VMware Host Hardware \(WBEM\)](#)
- [VMware Host Hardware Status \(SOAP\)](#)
- [VMware Host Performance \(SOAP\)](#)
- [Hyper-V Host Server](#)
- [Citrix XenServer Host](#)

These sensors monitor hardware-specific counters to make sure that no hardware issues affect your actual VMs. Additional sensors can monitor the host hardware via the Simple Network Management Protocol (SNMP) (for example, traffic and custom requests), and the data storage on ESXi servers via SOAP. There are also sensors for network adapters and storage devices that are connected to a Hyper-V host server.

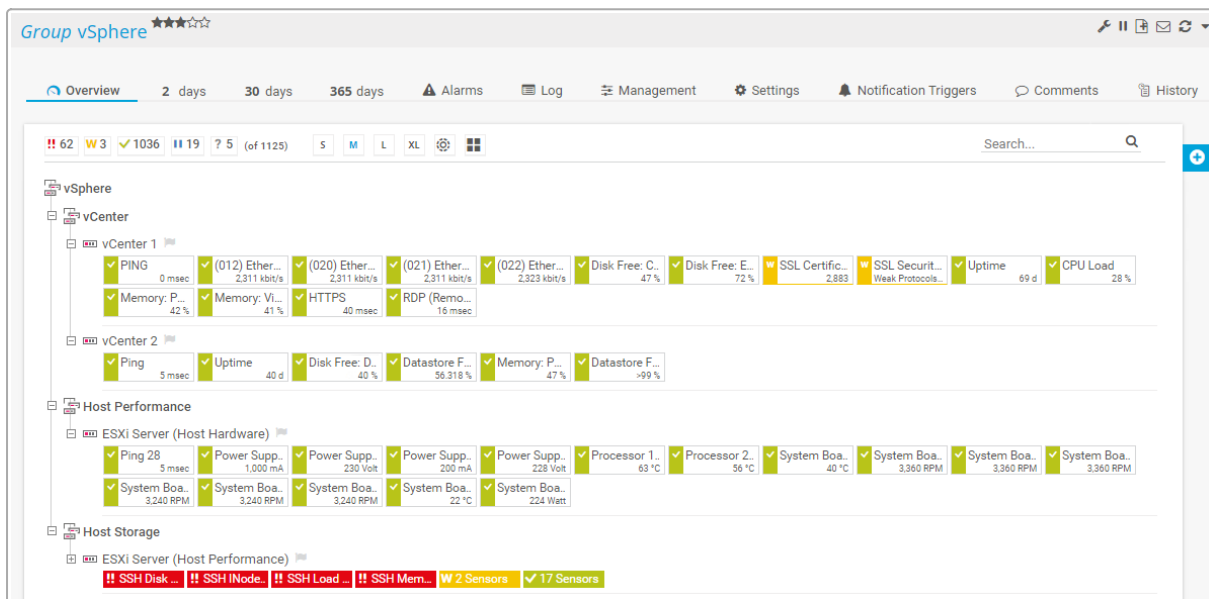
## Devices for Virtual Machines

To monitor your actual VMs, add them to your host servers in PRTG. For a better overview, you might want to add a device to PRTG that represents your host server and add sensors for your VM there. The respective sensors for VMs show you the performance of single VMs as well as their resource usage. This identifies VMs with low performance so that you can react before there is an issue with one or more of your VMs. As mentioned before, you can additionally monitor the operating systems of your VMs, if necessary. See the following sections for details about particular virtualization solutions.

### VMware Virtual Machine

The [VMware Virtual Machine \(SOAP\)](#) sensor monitors VMs on a VMware host server via SOAP. The general idea is to add a [vCenter](#) server as a device to your [vCenter](#) group and use it as a parent device to which you add the sensors for your VMs. This way, in the case of [vMotion](#), when your VMs change their host server, PRTG can follow these movements and does not lose the monitored VMs.

For this sensor, .NET 4.7.2 or later must be installed on the probe system. If you use many VMware sensors, we also recommend that you adjust the settings on your VMware host server to accept more incoming connections.

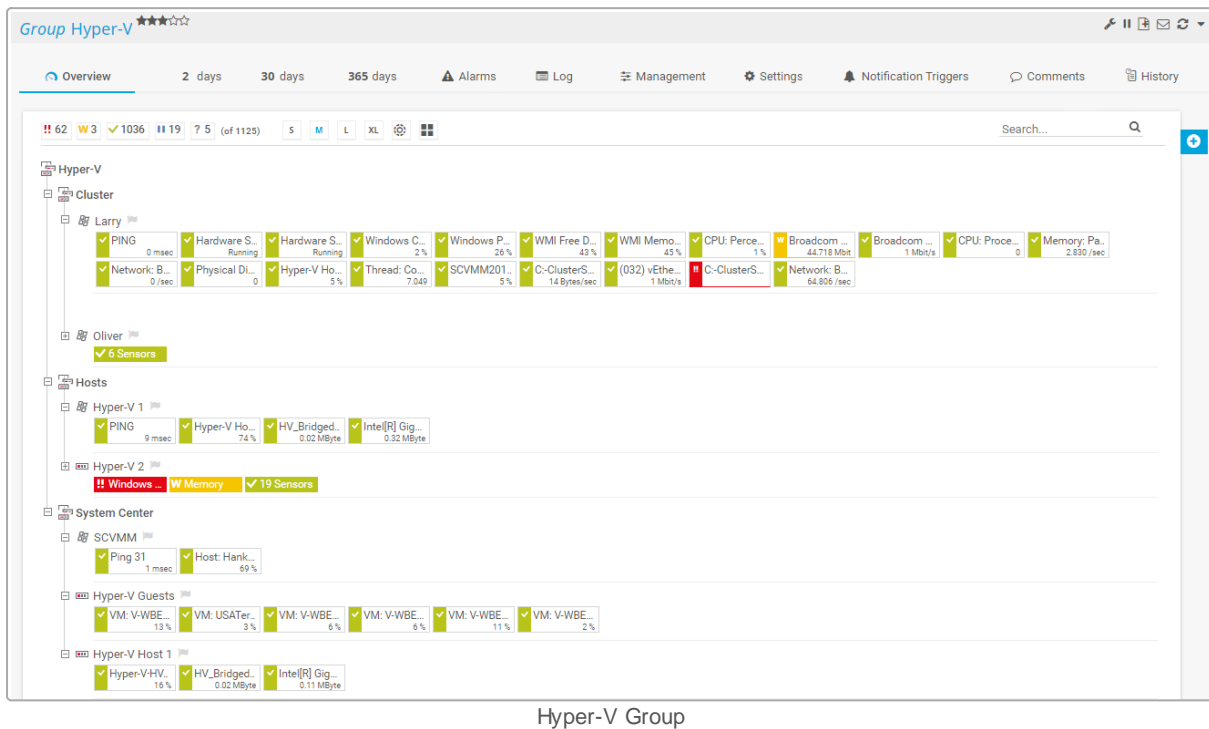


vSphere Group

This screenshot shows an example of a [vSphere](#) group. As recommended, the sensors for the VMware virtual machines are added to the [vCenter 1](#) device. There is also a dedicated [vCenter 2](#) device for the vCenter Windows operating system with common WMI sensors for CPU, memory, disk, and network usage. The ESXi host servers are organized in their own groups regarding performance and storage. In this example, PRTG monitors the hosts with the standard SNMP hardware sensors as well as with the specific VMware ESXi host sensors.

### Microsoft Hyper-V Virtual Machine

The [Hyper-V Virtual Machine](#) sensor monitors VMs via Windows Management Instrumentation (WMI) or Windows performance counters, as configured in the [Windows Compatibility Options](#) [648] of the parent device. With this hybrid approach, the sensor first tries to query data via performance counters and uses WMI as a fallback if no performance counters are available. Performance counters generally need less system resources than WMI. The parent device of this sensor must be a Windows server running Hyper-V. You should also disable the User Account Control (UAC) in the Windows operating system of the VM. Otherwise, the sensor might change to the Down status with the error message [The virtual machine is not running or is powered off](#). Also, this sensor does not support [Live Migration](#).



Hyper-V Group

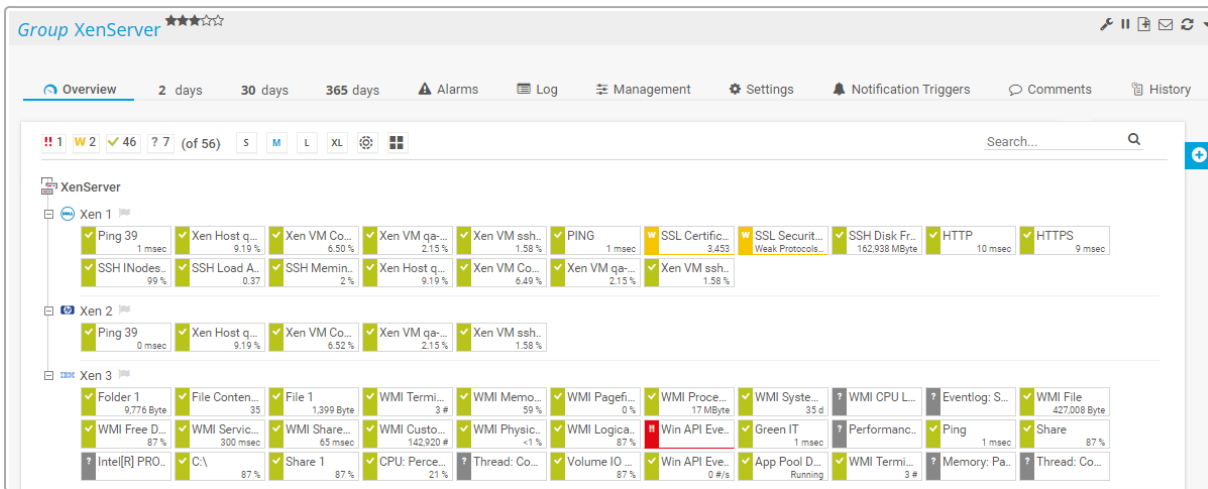
This screenshot shows an example of a [Hyper-V](#) group. There is a dedicated group for failover clusters where two cluster nodes are monitored with several SNMP and WMI sensors, as well as Hyper-V Host Server sensors and sensors for the Hyper-V virtual machines. This makes sure that Hyper-V and failover clusters work without any issues. The Hyper-V hosts are monitored the same way, organized in a dedicated group for hosts.

### Citrix XenServer Virtual Machine

The [Citrix XenServer Virtual Machine](#) sensor monitors VMs via HTTP. For this sensor, you must add a device that represents a Citrix XenServer running at least version 5.0. Another requirement is the Microsoft .NET Framework. You must install .NET 4.7.2 or later on the probe system.

In a XenServer pool, each host knows each running VM. Because of this, there is no central instance that provides all available data, so it does not matter on which host you query your VMs. All queries on any host are automatically forwarded to the pool master that manages the XenServer pool. Therefore, it is sufficient to create the desired sensors for your XenServer VMs on a device that represents one host server of your pool. The XenServer sensors find out which host is running and retrieve the respective data.





XenServer Group

This screenshot shows an example of a **XenServer** group. There are two devices for XenServer hosts, **Xen 1** and **Xen 2**, that each have a Citrix XenServer Host sensor and several Citrix XenServer Virtual Machine for the particular VMs on this host. Furthermore, the Windows operating system is represented as a dedicated **virtualcontrol** device that PRTG monitors with several WMI sensors regarding CPU, disk, memory, and network usage.

## Performance Considerations

For best performance when monitoring virtual environments, we strongly recommend that you use a computer with at least Windows Server 2016 installed on the probe system. For example, you can run up to 300 VMware sensors with a 60-second scanning interval as of Windows Server 2016, while you can only use 30 VMware sensors with the same scanning interval on Windows Server 2008 R2.

## 12.10 Monitoring Databases

Monitoring your databases lets you make sure that database queries are processed in time, and that the database itself performs within the defined parameters. Furthermore, database monitoring with PRTG can alert you via a corresponding sensor status if database queries return unexpected result values.

PRTG comes with built-in native sensors for the most common databases:

- Microsoft SQL servers
- MySQL servers
- PostgreSQL servers
- Oracle SQL servers

It is also possible to monitor many other database servers. For this case, PRTG uses the ActiveX Data Objects (ADO) interface.

There are two types of database sensors:

- [Sensors that monitor databases directly](#)<sup>[3028]</sup>: Monitor databases from the user perspective. These sensors send a request to the database server and receive corresponding values. You can optionally process data tables and show values in individual channels or monitor transactions.
- [Sensors that monitor database performance](#)<sup>[3031]</sup>: Monitor databases with a more abstract view on the servers. Usually, these sensors monitor performance counters via Windows Management Instrumentation (WMI).

### Sensors Monitoring Databases Directly


PRTG provides several sensors that can monitor the content of databases. Sensors of this type connect to the database server, execute a defined query, and show the execution time of the whole request and the query. You can use these sensors to process the data table and show requested values in individual channels.

The following sensors are available for this kind of monitoring:

- [Microsoft SQL v2](#)
- [MySQL v2](#)
- [Oracle SQL v2](#)
- [PostgreSQL](#)

For these sensors, you can define valid Structured Query Language (SQL) statements that the sensors send to the database server. Define the queries in an SQL script file and store it in the respective \Custom Sensors\sql subfolder of the [PRTG program directory](#)<sup>[3213]</sup>.

You can select this SQL script when you add the sensor. With every [scanning interval](#)<sup>[450]</sup>, the sensor executes this script with the defined query against the database and the database returns corresponding values in individual channels (see the [example](#)<sup>[3029]</sup> below for sample channel value selections). Use the [channel settings](#)<sup>[2682]</sup> to define limits for specific values.

 These sensors need .NET 4.7.2 or later installed on the probe system.

Alternatively, you can monitor almost all available database servers with the [ADO SQL v2](#) sensor via an ADO connection.

### Example: SQL Channel Value Selection

The SQL (v2) sensors determine their channel values by using column numbers, column names, row numbers, or key value pairs. This section shows which option you can choose to get the desired value from an SQL data table.

Consider the following data table that an SQL query might return from a database:

article_id	articles_av ailable	first_listing	orders
00	12	2001	4
01	345	2005	56
02	678	2008	290
03	90	2012	32

This data table has four columns with the following numbering:

- Column 0 has the name "article\_id"
- Column 1 has the name "articles\_available"
- Column 2 has the name "first\_listing"
- Column 3 has the name "orders"

The numbering of columns starts with 0, as well as the numbering for rows starts with 0. The table has four rows, each row contains the properties of one "article". The "articles" have the IDs 00, 01, 02, 03. This also illustrates the proper row numbering (0, 1, 2, 3).

With the options for channel value selection in SQL sensors, you can read out the following values:

- All values that are in row 0 (here: 00, 12, 2001, 4)
- All values that are in column 0 (here: 00, 01, 02, 03)
- All values that are in column 1 (here: 12, 345, 678, 90)

It is not possible to get values from any other cell in a data table. If you need this, you must reconstruct your data table.

The following samples show possible results for channel value selections regarding this data table:

Sample Channel Value Selection	Description
Channel Value Selection by Column Number	<p>This channel shows the value in row 0 of the column you specify. Consider you define "1" as column number. Then the channel value is "12" because it is the cell in column 1 and row 0.</p> <p>Possible return values for this option:</p> <ul style="list-style-type: none"> <li>▪ Column number "0" returns "00"</li> <li>▪ Column number "1" returns "12"</li> <li>▪ Column number "2" returns "2001"</li> <li>▪ Column number "3" returns "4"</li> </ul>
Channel Value Selection by Column Name	<p>This channel shows the value in row 0 of the column you specify. Consider you define "orders" as column name. Then the channel value is "4" because it is the cell in column "orders" and row 0.</p> <p>Possible return values for this option:</p> <ul style="list-style-type: none"> <li>▪ Column name "article_id" returns "00"</li> <li>▪ Column name "articles_available" returns "12"</li> <li>▪ Column name "first_listing" returns "2001"</li> <li>▪ Column name "orders" returns "4"</li> </ul>
Channel Value Selection by Row Number	<p>This channel shows the value in column 0 of the row you specify. Consider you define "1" as row number. Then the channel value is "01" because it is the cell in row 1 and column 0.</p> <p>Possible return values for this option:</p> <ul style="list-style-type: none"> <li>▪ Row number "0" returns "00"</li> <li>▪ Row number "1" returns "01"</li> <li>▪ Row number "2" returns "02"</li> <li>▪ Row number "3" returns "03"</li> </ul>
Channel Value Selection by Key Value Pair	<p>This channel shows the value in column 1 of the same row where the key in column 0 was found. Consider you define "02" as key. Then the channel value is "678" because it is the cell in the same row in column 1 as the key in column 0.</p> <p>Possible return values for this option:</p> <ul style="list-style-type: none"> <li>▪ Key "00" returns "12"</li> <li>▪ Key "01" returns "345"</li> <li>▪ Key "02" returns "678"</li> <li>▪ Key "03" returns "90"</li> </ul>

This sample channel value selection illustrates how to choose the correct option to get needed values from an SQL data table and shows which cells the SQL sensors can address.

#### UDF: Counting Returned Rows

If you execute a User-defined Function (UDF) on the SQL server and want to know how many rows this UDF returns, follow these steps:

- A command to execute your UDF on the SQL server might look like this, for example:

```
exec myUDF
```

- To get the information how many rows this UDF returns, extend the query in your SQL script:

```
exec myUDF;  
select @@rowcount as row_count
```

- Create a new SQL v2 sensor and select Data Processing during sensor creation.
- In the settings of your SQL sensor, select Column name under Select Channel Value by.
- Enter row\_count into the Channel #x Column Name field of the channel to show the value from this column in the channel.
- To count table rows returned by a **SELECT** statement, choose the option Count table rows in the sensor settings section Data Processing.

## Sensors Monitoring Database Performance

Performance sensors for database servers have a more abstract view on databases and observe performance externally. They do not read out any values of the database, neither do they send SQL queries to databases. This sensor is only available for Microsoft SQL.

The Microsoft SQL server sensors monitor performance via WMI. You can manually set up different performance counters for your server instances, for example, general statistics, access methods, buffer and memory manager, locks, and SQL statistics.

Microsoft SQL Server performance sensors are available for Microsoft SQL Server 2008, 2012, 2014, 2016, 2017, and 2019:

- [WMI Microsoft SQL Server 2008](#)
- [WMI Microsoft SQL Server 2012](#)
- [WMI Microsoft SQL Server 2014](#)
- [WMI Microsoft SQL Server 2016](#)
- [WMI Microsoft SQL Server 2017](#)
- [WMI Microsoft SQL Server 2019](#)

## 12.11 Monitoring via HTTP

HTTP is a standard application layer protocol and the basis for data communication on the internet. It is a request-response method for client-server architectures, where the client sends a request and the server processes and responds to the request.

Monitoring via HTTP is useful if you want to monitor websites or web servers. It enables you to keep an eye on the availability and download times of a website or the performance statistics of a web server. There are also a lot of other possible use cases for HTTP sensors. For example, you can request any application programming interface (API) that is reachable via HTTP and monitor returned values. This approach lets you include almost any type of device or application into your monitoring.

PRTG comes with sensors for HTTP monitoring:

- [AWS Alarm v2](#)
- [AWS EBS v2](#)
- [AWS EC2 v2](#)
- [AWS ELB v2](#)
- [AWS RDS v2](#)
- [Cisco Meraki License](#)
- [Cisco Meraki Network Health](#)
- [Cloud HTTP v2](#)
- [Common SaaS](#)
- [Dell EMC Unity Enclosure Health v2](#)
- [Dell EMC Unity File System v2](#)
- [Dell EMC Unity Storage Capacity v2](#)
- [Dell EMC Unity Storage LUN v2](#)
- [Dell EMC Unity Storage Pool v2](#)
- [Dell EMC Unity VMware Datastore v2](#)
- [FortiGate System Statistics](#)
- [FortiGate VPN Overview](#)
- [HPE 3PAR Common Provisioning Group](#)
- [HPE 3PAR Virtual Volume](#)
- [HTTP](#)
- [HTTP Advanced](#)
- [HTTP Apache ModStatus PerfStats](#)
- [HTTP Apache ModStatus Totals](#)
- [HTTP Content](#)
- [HTTP Data Advanced](#)
- [HTTP Full Web Page](#)

- [HTTP IoT Push Data Advanced](#)
- [HTTP Push Count](#)
- [HTTP Push Data](#)
- [HTTP Push Data Advanced](#)
- [HTTP Transaction](#)
- [HTTP v2](#)
- [HTTP XML/REST Value](#)
- [Microsoft Azure SQL Database](#)
- [Microsoft Azure Storage Account](#)
- [Microsoft Azure Subscription Cost](#)
- [Microsoft Azure Virtual Machine](#)
- [NetApp Aggregate v2](#)
- [NetApp I/O v2](#)
- [NetApp LIF v2](#)
- [NetApp LUN v2](#)
- [NetApp NIC v2](#)
- [NetApp Physical Disk v2](#)
- [NetApp SnapMirror v2](#)
- [NetApp System Health v2](#)
- [NetApp Volume v2](#)
- [Redfish Power Supply](#)
- [Redfish System Health](#)
- [Redfish Virtual Disk](#)
- [REST Custom](#)
- [REST Custom v2](#)
- [SSL Certificate](#)
- [SSL Security Check](#)
- [Veeam Backup Job Status](#)
- [Veeam Backup Job Status Advanced](#)

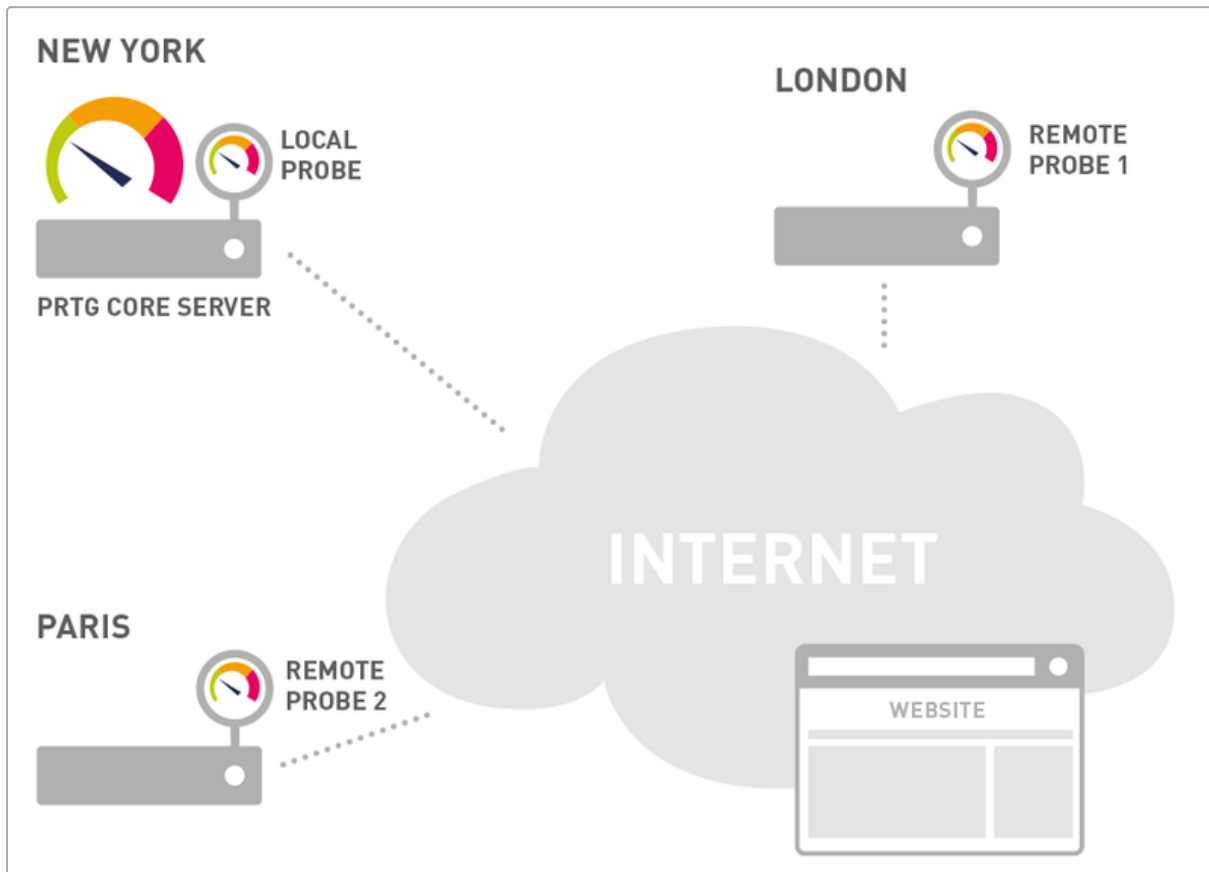
## Use Cases

- Monitor the availability and loading times of a website
- Monitor the source code and specific content of a website
- Test the login, purchasing, and shipping processes of a web shop
- Monitor performance statistics and activity of Apache web servers

## Types of HTTP Monitoring

### Availability Monitoring

This type monitors the availability of a website or a specific website element. For example, the HTTP sensor shows how long the HTML code of a website takes to load. If the sensor shows a loading time that is much longer than expected, the website might not be responding or might be unavailable.



Cloud Monitoring with HTTP Provides Better Performance Statistics

The HTTP sensor uses different HTTP requests to request the specified URL:

- GET (default): requests the website directly
- POST: sends post form data to the URL
- HEAD: requests the HTTP header only, without the actual web page body, saving bandwidth

The HTTP Advanced sensor also monitors the availability of a website, along with other parameters such as bytes received, download bandwidth (speed), and time to first byte, which shows you how fast your web server responds. This sensor lets you use a (custom) user agent when connecting to the target URL and lets you send custom HTTP headers to the target URL.

The Cloud HTTP v2 sensor monitors a web server from various locations across the globe. For example, the URL of a website to measure the loading time of a page's source code or the URL of a page asset to measure its availability and loading time. The sensor also shows the global average response time.



The Common SaaS monitors the availability of your cloud services and is an important pillar for unified monitoring.

## Content Monitoring

This type monitors internal values of a web server based application or changes to specific content on a website. The HTTP Full Web Page sensor measures the time it takes to download a web page including all embedded page elements, for example Flash content or images.

 This monitoring option can create a lot of bandwidth traffic, depending on the page size and the scanning interval.

Additionally, the HTTP Content sensor monitors a numeric value returned by an HTTP request. It can also optionally trigger a 'change' notification to notify you of changes to the content.

## Example: Content Monitoring


 For example, consider a URL <http://www.example.com/status.html> that returns a PHP script with the current system status in a simple HTML page.

```
<html>
  <body>
    Description: Script gives back current status of disk free (%) and CPU usage (%).
    [85.5][12.0]
  </body>
</html>
```

You would configure the HTTP Content sensor using

- the script URL from above,
- value type Float,
- and number of channels 2.

The sensor calls the URL with every scanning interval and only regards the two values in brackets [ ], handling each of them in one channel. The additional description text and HTML tags are not necessary. In this example, they are added in case a human calls the URL.

 If you define the number of channels as 1, the sensor only reads the first value. The second value is ignored. Using 3 as number of channels results in a sensor error message.

To be notified when the website content changes, you first need to configure a Trigger 'change' notification in the sensor's settings and then the notification itself.

 For more information, see section [Notification Triggers Settings](#)  <sup>2702</sup>.

## Performance Monitoring

The HTTP Transaction sensor checks if a web shop is working as expected: with a series of requests, for example, you can simulate the login, purchasing, and shipping processes. Only if all actions can be completed successfully in a row, the check returns an "OK" message. If anything goes wrong, you are immediately alerted and can react instantly to avoid loss of earnings for your company because the web shop is unavailable or very slow.

### Apache Web Server Monitoring

The HTTP Apache ModStatus PerfStats and HTTP Apache ModStatus Totals sensors monitor performance statistics and the activity of an Apache web server using mod\_status over HTTP. Among other HTTP sensors, these sensors let you enter credentials for web pages that need authentication and let you choose the necessary authentication method.

### Security Monitoring

PRTG also provides the option to monitor the security of your website by checking the status of Secure Sockets Layer (SSL) certificates and the security of a connection:

- [SSL Certificate](#) sensor: monitors the certificate of an SSL/TLS-secured connection. For example, it displays whether a certificate has been revoked, or is trusted as root authority, or is self-signed.
- [SSL Security Check](#) sensor: monitors the SSL connectivity to the port of a device. It tries to connect to the specified TCP/IP port number of a device with different SSL/TLS versions and shows if a specific protocol is supported.

### Push Monitoring

PRTG provides the option to monitor passively received data. For this purpose, you can set up a device in a way that it automatically sends the data to PRTG. Specific sensors can receive this data and alert you based on your individual settings. For example, all Linux/Unix and most network devices support remote devices generating data, which has to be configured on each device, and sending the messages to a probe system. Usually, only the destination IP and port are required.

■ For more information, see the Paessler website: [How to use push monitoring via HTTP](#).

### Other Data

You can also monitor other types of data from your website, for example the number of website visitors via the HTTP XML/REST Value sensor. The sensor lets you monitor values within the returned Extensible Markup Language (XML) code, provided your web analytics tool has an XML export option. The HTTP Data Advanced sensor accesses a web server and retrieves XML or JavaScript Object Notation (JSON) encoded data.

The REST Custom sensor queries a Representational State Transfer (REST) application programming interface (API) endpoint and maps the JSON or XML result to sensor values. The mapping rule has to be available as a REST configuration file in JSON template (\*.template) format according to the PRTG API definition.

■ For more information about the return value format, see section [Custom Sensors](#) .

## HTTP Status Codes

The HTTP sensors show their status depending on the HTTP status codes that they receive. By default, the sensor states are the following:

HTTP Status Code	HTTP Sensor Status
2xx Success	Up
3xx Redirection	Warning, Down for too many redirects)
4xx Client Error	Down
5xx Server Error	Down

**i** You need to configure your HTTP sensors manually only if you want to change these default reactions. In this case, you can change the sensor status based on limits and/or keyword checks.

## Other HTTP Sensor Settings

- **Server Name Indication:** You can configure SNI, which has to be a fully qualified domain name (FQDN) and must match the configuration of the target server. For more information, see the Knowledge Base: [My HTTP sensors fail to monitor websites which use SNI. What can I do?](#)
- **HTTP Version:** You can choose the HTTP version that the sensor uses when connecting to the target URL.
- **Authentication Method:** You can define if the configured URL needs authentication, enter credentials, and choose an authentication method.
- **Custom User Agent:** You can enter a string to be used as user agent when connecting to the target URL.
- **Custom HTTP Headers:** You can send custom HTTP headers to the target URL.

## HTTP Sensor Troubleshooting

For troubleshooting and other tips for monitoring with HTTP sensors, see [More](#) below.

### More

#### ■ KNOWLEDGE BASE

My HTTP sensors fail to monitor websites which use SNI. What can I do?

- <https://kb.paessler.com/en/topic/67398>

Which user agent should I use in the HTTP Advanced sensor's settings?

- <https://kb.paessler.com/en/topic/30593>

HTTP Full Web Page sensor is unable to navigate. What can I do?

- <https://kb.paessler.com/en/topic/59999>

What to do when I see a CreateUniqueTempDir() error message for my HTTP Full Web Page sensor?

- <https://kb.paessler.com/en/topic/40783>

Where can I find more information about the HTTP XML/REST Value sensor?

- <https://kb.paessler.com/en/topic/62463>

Why does my HTTP XML/REST Value sensor return a 404 error?

- <https://kb.paessler.com/en/topic/46503>

# Part 13

# PRTG Administration Tool

## 13 PRTG Administration Tool

The PRTG Administration Tool is part of every PRTG installation. You can use it to edit the administrative settings of local probe and remote probe installations.

You can start the PRTG Administration Tool from the Windows Start menu on the PRTG core server system or on the remote probe system. If you start the PRTG Administration Tool on the PRTG core server system, you can change settings that affect the entire installation and the local probe. If you run the PRTG Administration Tool on a remote probe system, you can only change settings that are related to the remote probe.

Any settings that you change require a restart of the affected PRTG core server service and PRTG probe service to apply any changes to the configuration.

- ① You can also change many administrative settings via the [Setup](#) <sup>[2799]</sup> in the PRTG web interface. For probes, administrative settings are also available on the Settings [tab](#) <sup>[521]</sup> in the PRTG web interface.
- ① You can review the history of all changes to the settings of the PRTG Administration Tool in the \Logs\serveradmin subfolder of the [PRTG program directory](#) <sup>[3213]</sup>. The name of the corresponding log file is ServerAdmin.log.

In this section:


- [PRTG Administration Tool on PRTG Core Server Systems](#) <sup>[3041]</sup>
- [PRTG Administration Tool on Remote Probe Systems](#) <sup>[3067]</sup>


## 13.1 PRTG Administration Tool on PRTG Core Server Systems

With the PRTG Administration Tool, you can define various system settings regarding the PRTG core server installation, restart services, and view log information. You can also change many of these settings via the [system administration](#) [2855] in the PRTG web interface.

In this section:

- [Start the PRTG Administration Tool](#) [3041]
- [PRTG Web Server](#) [3041]
- [PRTG Core Server](#) [3046]
- [Cluster](#) [3047]
- [Administrator](#) [3054]
- [Probe Settings for Core Connection](#) [3055]
- [Probe Settings for Monitoring](#) [3058]
- [Service Start/Stop](#) [3059]
- [Logs and Info](#) [3062]
- [Send Logs to Paessler](#) [3063]
- [Activate Changed Settings](#) [3065]

 This section describes the settings that are available in the PRTG Administration Tool when you open it on the PRTG core server system. This means that you can edit settings for the PRTG core server or PRTG web server and the local probe.

 Settings that you define are only valid for the PRTG core server system on which you start the PRTG Administration Tool. Make sure that you log in to the system that you want to make changes to and open the PRTG Administration Tool there.


 This feature is not available in PRTG Hosted Monitor.

### Start the PRTG Administration Tool

- From the Windows Start menu, select the PRTG Network Monitor folder and click PRTG Administration Tool to open the application.
- Confirm the question of the Windows [User Account Control](#) with Yes to allow the PRTG Administration Tool to start.

### PRTG Web Server

Edit IP addresses, ports, access methods, and language for the PRTG web interface.

 You can also change these settings under Setup | System Administration | User Interface in the PRTG web interface. For more information, see section [User Interface](#) [2860].

PRTG Network Monitor - PRTG Administration Tool
✕

**PAESSLER**
PRTG Network Monitor

Probe Settings for Core Connection	Probe Settings for Monitoring	Service Start/Stop	Logs and Info
PRTG Web Server	PRTG Core Server	Cluster	Administrator

**TCP Port for PRTG Web Server**

Secure HTTPS server (default port 443, recommended, mandatory for internet access)  
 Unsecure HTTP server (default port 80)  
 Custom configuration

Use HTTPS (secured with SSL/TLS)
 Web server port:

Do not use connection security
 443

**IP Address for PRTG Web Server**

Localhost, 127.0.0.1 (PRTG is not accessible from other computers)  
 All IP addresses available on this computer (recommended)  
 Specify IP addresses:

192.0.2.0  
 127.0.0.1

Note: The selected TCP port must be available on all selected IP addresses.

**Select System Language**

English

PRTG Web Server Tab

Setting	Description
TCP Port for PRTG Web Server	Specify how the PRTG web server accepts incoming web page requests:



Setting	Description
	<ul style="list-style-type: none"> <li>▪ Secure HTTPS server (default port 443, recommended, mandatory for internet access): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured HTTPS connection on port 443.               <ul style="list-style-type: none"> <li>❗ This setting is required if you want to access the PRTG web interface via the internet.</li> <li>❗ Although the connection is secure, you see an SSL certificate warning in your browser when you log in to the PRTG web interface because the default certificate is unknown to your browser. For more information, see the Knowledge Base: <a href="#">Why does my browser show an SSL certificate warning when I open the PRTG web interface?</a>. You can install a different SSL certificate for PRTG. For more information, see section <a href="#">How to use your own SSL certificate with the PRTG web server</a>.</li> <li>❗ If port 80 is available, PRTG reserves it as well. If port 80 is not available, PRTG tries port 8080 as fallback. If this port is also not available, PRTG searches from port 8081 upwards for a free port. PRTG sends a <a href="#">ticket</a><sup>[213]</sup> that shows you the currently used port number and switches back to port 80 as soon as it is available again. When users try to connect on port 80 via HTTP, they are redirected to port 443 via HTTPS. You can change this behavior via a registry setting. If port 443 is not available, PRTG tries port 8443 as fallback. If this port is also not available, PRTG searches from port 8444 upwards for a free port. PRTG sends a ticket that shows you the currently used port number and switches back to port 443 as soon as it is available again.</li> </ul> </li> <li>▪ Unsecure HTTP server (default port 80): Use the PRTG web server without SSL/TLS on port 80.               <ul style="list-style-type: none"> <li>❗ This setting is not recommended for WAN connections.</li> <li>❗ If you use the PRTG web server via the internet without connection security, attackers could potentially spy on credentials that you enter in PRTG. We strongly recommend that you use this option only in a LAN.</li> </ul> </li> <li>▪ Custom configuration: Specify a custom port for the PRTG web server and the security of the connection. This option is intended for systems that already have a web server on the standard port.               <ul style="list-style-type: none"> <li>❗ If PRTG always uses a fallback port after a server restart, check for other programs that use the same port as PRTG. For example, the Microsoft Microsoft Internet Information Services (IIS) web server also uses port 80 (port 443 for secure connections) by default and blocks it. We recommend that you disable such programs and services on startup.</li> </ul> </li> </ul>
<p>Custom configuration: <a href="#">Connection security</a></p>	<p><a href="#">This setting is only visible if you select Custom configuration above.</a></p> <p>Specify if you want to use connection security:</p>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Use HTTPS (secured with SSL/TLS): Use an SSL/TLS secured HTTPS connection on the port that you define as PRTG Web Server Port.               <ul style="list-style-type: none"> <li>❗ Although the connection is secure, you see an SSL certificate warning in your browser when you log in to the PRTG web interface, because the default certificate is unknown to your browser. You can install a different SSL certificate for PRTG later. For more information, see the Paessler website: <a href="#">How to use your own SSL certificate with the PRTG web server.</a></li> </ul> </li> <li>▪ Do not use connection security: Use the PRTG web server without SSL/TLS on the port that you define as PRTG Web Server Port.               <ul style="list-style-type: none"> <li>❗ We recommend that you do not use this setting for WAN connections.</li> <li>❗ If you use the PRTG web server without connection security on the internet, attackers could potentially spy on credentials that you enter in PRTG. We strongly recommend that you use this setting in a LAN only.</li> </ul> </li> </ul>
<p>Custom configuration: <a href="#">Web server port</a></p>	<p><a href="#">This setting is only visible if you select Custom configuration above.</a></p> <p>Enter the TCP port number (between 1 and 65535) that you want the PRTG web server to run on.</p> <p>Enter the TCP port number (between 1 and 65535) that you want the PRTG web server to run on. Enter an integer.</p> <ul style="list-style-type: none"> <li>❗ If you use a secure connection and port 80 is free, PRTG also reserves it. When users try to connect on port 80 via HTTP, they are redirected to the custom port via HTTPS. You can change this behavior via a registry setting.</li> <li>❗ If the port that you define for secure connections is not available, PRTG tries port 8443 as fallback. If this port is also not available, PRTG searches from port 8444 upwards for a free port. PRTG sends a <a href="#">ticket</a><sup>[213]</sup> that shows you the currently used port and switches back to the original port as soon as it is available again.</li> </ul>
<p>IP Address for PRTG Web Server</p>	<p>The PRTG web server provides access via the PRTG web interface and the <a href="#">PRTG app for desktop</a><sup>[2984]</sup>. Once you specify an IP address, you use it to log in to the PRTG web interface in your browser. Specify on which IP address the PRTG web server runs:</p>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Localhost, 127.0.0.1 (PRTG is not accessible from other computers): Use <a href="#">127.0.0.1</a> only. The PRTG web interface and the PRTG app for desktop are only accessible from the PRTG core server system. <ul style="list-style-type: none"> <li>❗ Either the selected port or at least one port in the range from <a href="#">8080</a> to <a href="#">8089</a> must be available on <a href="#">127.0.0.1</a>.</li> <li>❗ If you run PRTG on localhost, do not use the DNS name <a href="#">http://localhost</a> to log in to the PRTG web server. This might considerably slow down the PRTG web interface. Use your local IP address or <a href="#">http://127.0.0.1</a> instead.</li> </ul> </li> <li>▪ All IP addresses available on this computer (recommended): Use all IP addresses that are available on the PRTG core server system and enable access to the PRTG web server for all of these IP addresses. <ul style="list-style-type: none"> <li>❗ The selected Transmission Control Protocol (TCP) port for the PRTG web server must be available on all selected IP addresses.</li> </ul> </li> <li>▪ Specify IP addresses: Select specific IP addresses on which the PRTG web server runs. The list is specific to your setup. Enable check boxes in front of every IP address that you want the PRTG web server to be available at. You can also select all IP addresses by clicking the Select all IP addresses button or deselect all addresses by clicking the Deselect all IP addresses button. <ul style="list-style-type: none"> <li>❗ Either the selected port or at least one port in the range from <a href="#">8080</a> to <a href="#">8089</a> must be available on the specified IP address.</li> <li>❗ Regardless of the setting that you select, one port in the range from <a href="#">8080</a> to <a href="#">8180</a> must be available on the specified IP address so that PRTG can create reports. The report engine tries to connect to the PRTG core server on one of these ports.</li> <li>❗ If PRTG does not find a network card on startup, it switches this setting to Localhost, 127.0.0.1 (PRTG is not accessible from other computers). This setting remains even if a network card is available later on. If you disable or remove the network card on the PRTG core server system, check this setting.</li> </ul> </li> </ul>
<p>Select System Language</p>	<p>Select the language. The default language is English.</p> <p>❗ This setting defines the language of the PRTG web interface and the <a href="#">PRTG Administration Tool</a><sup>[3046]</sup>.</p> <p>List of available languages:</p> <ul style="list-style-type: none"> <li>▪ Deutsch (German)</li> <li>▪ English</li> <li>▪ Español (Spanish)</li> <li>▪ Français (French)</li> <li>▪ Nederlands (Dutch)</li> </ul>





Setting	Description
	<ul style="list-style-type: none"> <li>▪ Português (Portuguese)</li> <li>▪ Русский (Russian)</li> <li>▪ 日本語 (Japanese)</li> <li>▪ 简体中文 (Simplified Chinese)</li> </ul>

## PRTG Core Server

Define settings for the PRTG core server.

The screenshot shows the 'PRTG Network Monitor - PRTG Administration Tool' window. The 'PRTG Core Server' tab is selected. The interface includes a header with the Paessler logo and 'PRTG Network Monitor'. Below the header are four tabs: 'Probe Settings for Core Connection', 'Probe Settings for Monitoring', 'Service Start/Stop', and 'Logs and Info'. Under 'Probe Settings for Core Connection', there are sub-tabs for 'PRTG Web Server', 'PRTG Core Server', 'Cluster', and 'Administrator'. The 'PRTG Core Server' sub-tab is active, showing the 'Probe Connection Management' section with three radio button options: 'Accept connections from the local probe only (default, does not allow remote probes)', 'Accept connections from remote probes on all IP addresses' (which is selected), and 'Accept connections from remote probes on selected IP addresses only:'. Below these options is a list of IP addresses with checkboxes: '192.0.2.0' (unchecked) and '127.0.0.1' (checked). The 'Local Storage of Data Files and Monitoring Database' section contains a 'Folder:' label, a text box with the path 'C:\ProgramData\Paessler\PRTG Network Monitor\' and a browse button (...), and a 'Revert to default folder' button. A note below reads: 'Note: Please copy your data files to the desired location BEFORE you change the path here.' At the bottom right, there are 'Save & Close' and 'Cancel' buttons.

PRTG Core Server Tab





Setting	Description
Probe Connection Management	<p>Define how PRTG handles incoming connections from probes:</p> <ul style="list-style-type: none"> <li>▪ Accept connections from the local probe only (default, does not allow remote probes): Only accept connections from the local probe. If you select this option, you cannot use <a href="#">remote probes</a>.</li> <li>▪ Accept connections from remote probes on all IP addresses: Accept incoming connections from remote probes, no matter on which IP address of the PRTG core server they come in.</li> <li>▪ Accept connections from remote probes on selected IP addresses only: Accept incoming connections from remote probes on the selected IP address(es) of the PRTG core server. In the list, select the IP addresses by enabling a check box in front of the desired IP addresses.</li> </ul> <p> You can also change this setting under Setup   System Administration   <a href="#">Core &amp; Probes</a> in the PRTG web interface.</p>
Local Storage of Data Files and Monitoring Database	<p>Select the directory where PRTG stores configuration and monitoring data. Click  to choose a different folder on the system.</p> <p> Before you change the path, make sure you stop both the PRTG core server service and the PRTG probe service and copy all data to the new location.</p> <p> The directory name must include only ANSI characters. PRTG does not support data paths with non-ANSI characters.</p> <p>Click Revert to default folder to reset this setting to the default.</p>

## Cluster

On the Cluster tab, you can change how the PRTG core server behaves in a cluster. Before you change settings here, see section [Failover Cluster Configuration](#).

Cluster Tab

Setting	Description
Cluster Settings	<p>Depending on the cluster settings, different options are available.</p> <ul style="list-style-type: none"> <li>Cluster Mode: Shows the cluster mode of the PRTG core server. Possible values are Standalone (no cluster mode), Cluster Mode: Master Node, or Cluster Mode: Failover Node.</li> </ul> <p><b>i</b> This setting is for your information only. You cannot change it.</p> <ul style="list-style-type: none"> <li>Cluster Port: This setting is only visible if PRTG runs in cluster mode.</li> <li>Cluster Access Key: This setting is only visible if PRTG runs in cluster mode.</li> <li>Cluster NodeID: This setting is only visible if PRTG runs in cluster mode.</li> </ul>

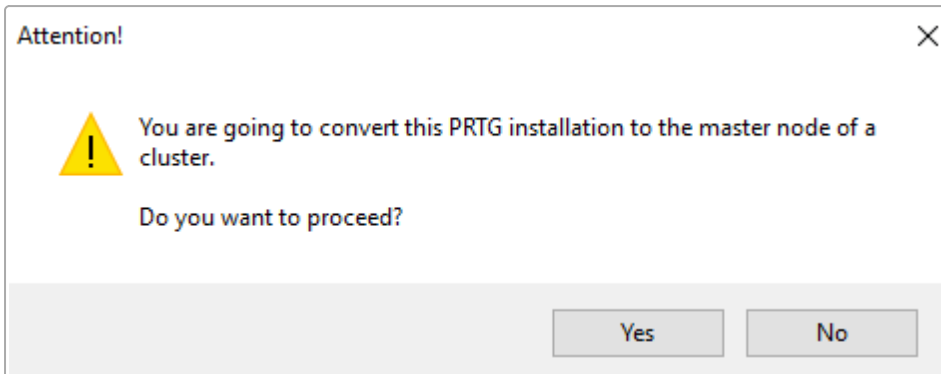
Setting	Description
	<p> This setting is for your information only. You cannot change it.</p>
Cluster Mode Actions	<p>Depending on the cluster settings, you see different active buttons.</p> <ul style="list-style-type: none"> <li>▪ Create a Cluster</li> <li>▪ Join a Cluster</li> <li>▪ Change Cluster Settings</li> <li>▪ Revert to Standalone</li> </ul> <p> For details, see section <a href="#">Cluster Mode Actions</a> <small>3049</small> below.</p>
Master Heartbeat	<p>This section is only visible if PRTG runs in cluster mode. The current master node can execute an external executable file on a regular basis. We call this a <b>heartbeat</b>.</p> <p>You can use this, for example, to report the IP address of the current master node to a dynamic Domain Name System (DNS) provider, so that a DNS name is always redirected to the current master node in case the primary master node fails and a failover node (with a different IP address) becomes the current master node.</p> <ul style="list-style-type: none"> <li>▪ No heartbeat: Do not execute a file on a regular basis.</li> <li>▪ Run an external executable file every 5 minutes: Click  to browse for the file that you want to execute. This can be, for example, a command-line tool or a batch file. PRTG executes it on the current master node only, in a fixed interval of five minutes. You cannot change the interval.</li> </ul> <p> Make sure that the selected file is available under the same (local) path on all failover nodes. In case one of your failover nodes becomes the current master node, PRTG can only execute the heartbeat reliably if the executable file exists on all of your failover nodes.</p>

### Cluster Mode Actions

Follow these instructions to create or to join a cluster, to change a cluster's settings, or to revert a cluster node to standalone mode:

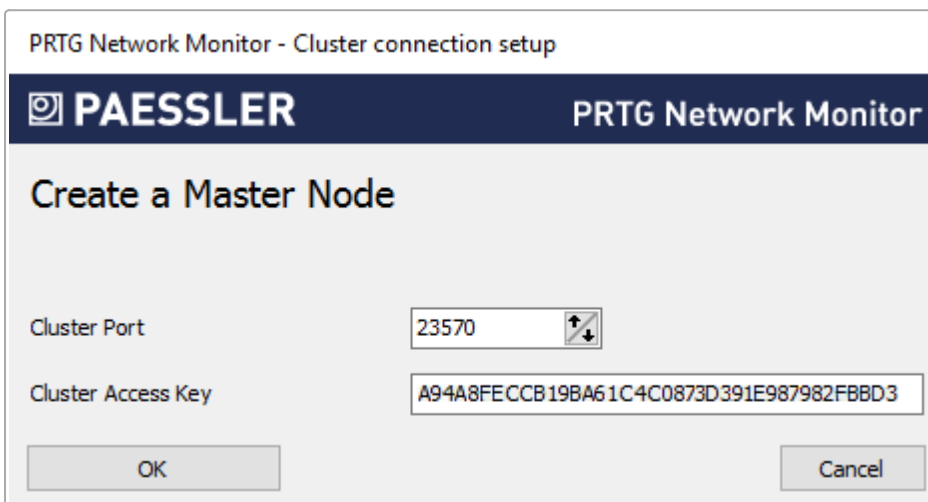
#### Create a Cluster

- Click Create a Cluster to create a cluster. The current PRTG core server is then the **master node** of the cluster.
- Click Yes to convert this installation to a master node.



Converting an Installation to a Master Node

- A dialog box appears.



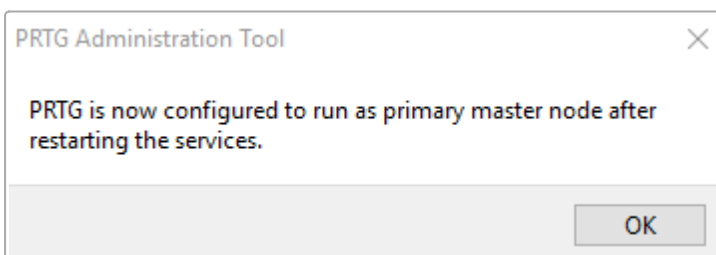
Creating a Master Node

- Enter a Cluster Port. This is the port on which PRTG sends the internal communication between the cluster nodes. Make sure that connections between the cluster nodes are possible on the port that you select.
- Enter or paste a Cluster Access Key. This is a unique access key. All cluster nodes must use the same cluster access key to join the cluster. Connection attempts with a different access key are not possible.

**i** We recommend that you use the default value.

- Save the Cluster Access Key so that you have it at hand when you configure the failover nodes.

- After confirming your settings, you are asked to restart Windows services. Click OK to restart the Windows services so that your changes take effect.

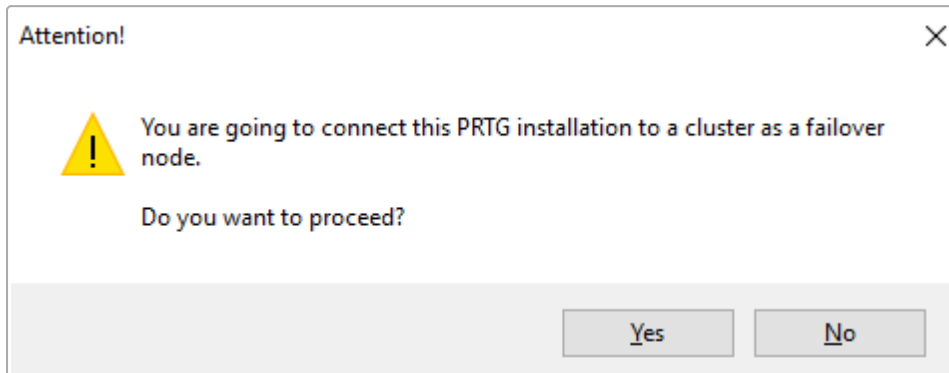


Restart Services to Apply Changes



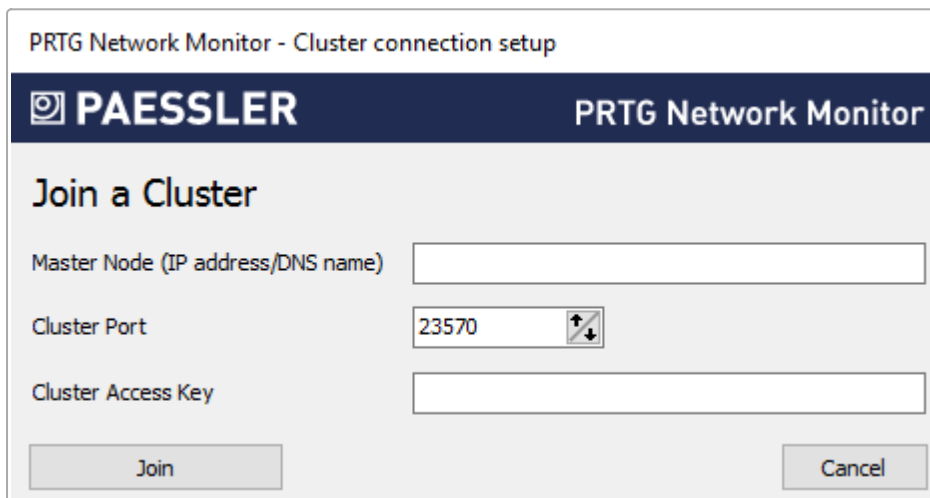
### Join a Cluster

- Click Join a Cluster to add this installation to a cluster that already has a [master node](#). The current PRTG core server is then a [failover node](#).
- This button is also available if the PRTG core server is in Cluster Mode: Master Node. This option then changes the master node to a failover node.
- Click Yes to convert this installation into a failover node.



Converting an Installation to a Failover Node

- A dialog box appears.

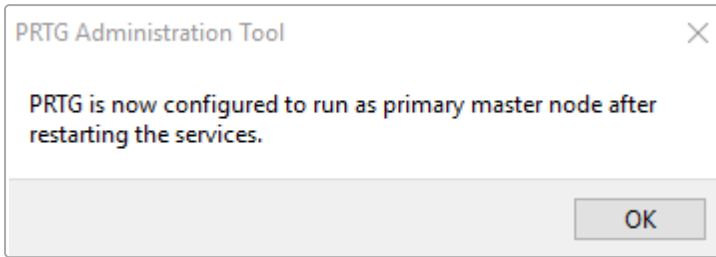


Cluster Connection Setup

- Enter a Master Node (IP address/DNS name) for the cluster. It must be reachable from the machine that runs the failover node.
- Enter the other settings as defined in the settings of the [master node](#). Make sure that you use the same settings on all cluster nodes.
- Enter a Cluster Port. This is the port on which PRTG sends the internal communication between the cluster nodes. Make sure that connections between the cluster nodes are possible on the port that you select.
- Enter or paste a Cluster Access Key. This is a unique access key. All cluster nodes must use the same cluster access key to join the cluster. Connection attempts with a different access key are not possible.

**i** We recommend that you use the default value.

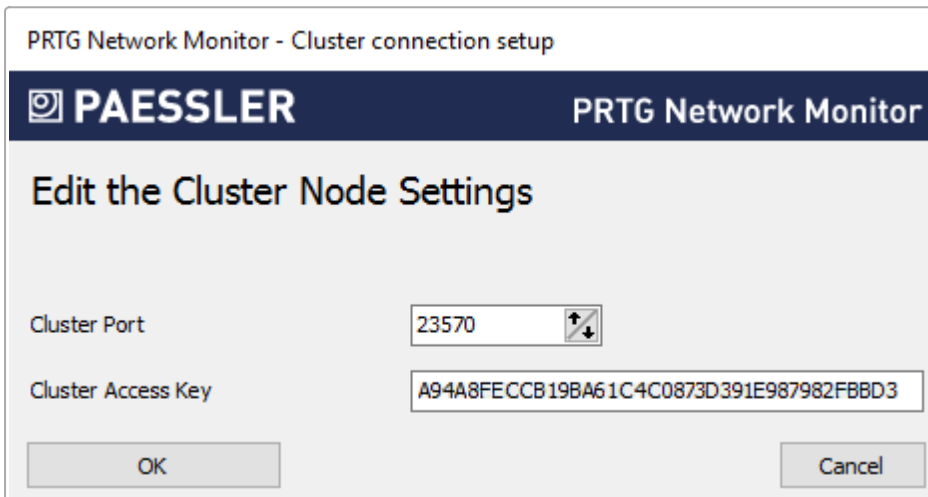
- After confirming your settings, you are asked to restart Windows services. Click OK to restart the Windows services so that your changes take effect.



Restart Services to Apply Changes

### Change Cluster Settings

- If you run PRTG in cluster mode, you can change the settings. Click Change Cluster Settings to do so.
- A dialog box appears.

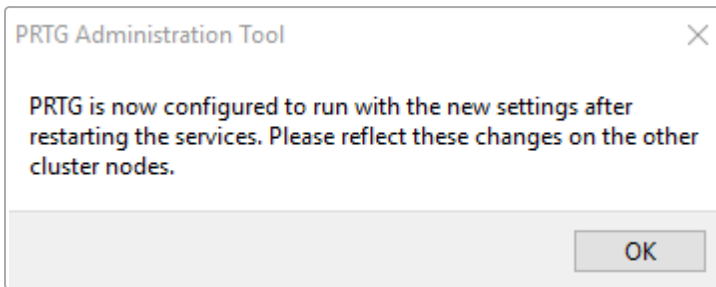


Edit Cluster Node Settings

- Enter a Cluster Port. This is the port on which PRTG sends the internal communication between the cluster nodes. Make sure that connections between the cluster nodes are possible on the port that you select.
- Enter or paste a Cluster Access Key. This is a unique access key. All cluster nodes must use the same cluster access key to join the cluster. Connection attempts with a different access key are not possible.

**i** We recommend that you use the default value.

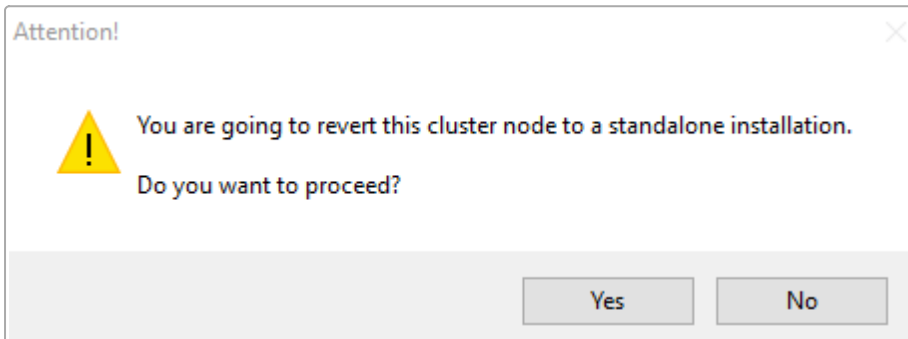
- Make sure that you use the same settings on all cluster nodes.
- After confirming your settings, you are asked to restart Windows services. Click OK to restart the Windows services so that your changes take effect.



Restart Services to Apply Changes

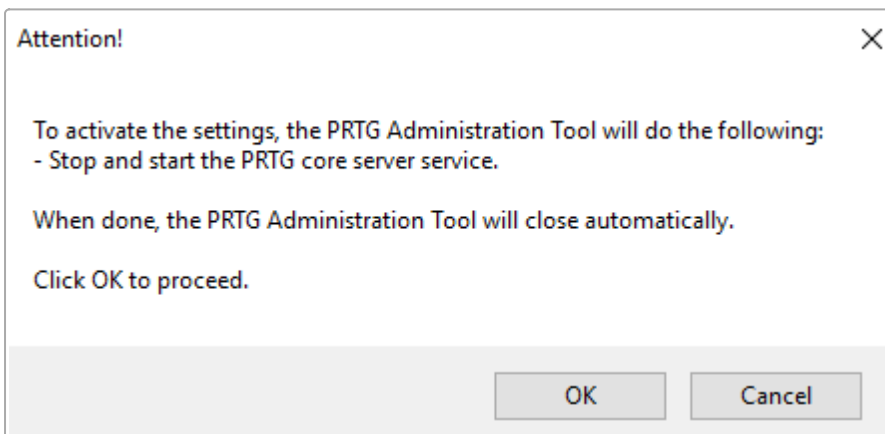
#### Revert to Standalone

- Click Revert to Standalone to revert this cluster node to a standalone installation.
- A dialog box appears.



Revert Cluster to Standalone Installation

- Click Yes to convert this cluster node to a standalone installation.
- A dialog box appears where PRTG asks you to agree to restart the PRTG core server service. Click OK to proceed.



Restart Services

- ① When you revert a cluster node to Standalone mode, the cluster probe remains in the device tree to keep your device and sensor setup. If you want to completely remove the cluster probe from the device tree, you need to delete it manually.

## Administrator



On the Administrator tab, you can change settings for the [PRTG System Administrator](#) user.

- ① You can also change the password for the [PRTG System Administrator](#) user account under Setup | Account Settings | [My Account](#) in the PRTG web interface.

The screenshot shows the 'Administrator' tab in the PRTG Administration Tool. The main heading is 'Login Credentials for the PRTG System Administrator User Account'. There are three input fields: 'Email Address' with the value 'johnqpublic@example.com', 'Login Name' with the value 'prtgadmin', and 'Password' with a masked value '\*\*\*\*\*'. A 'Generate new password' button is located to the right of the password field. At the bottom right, there are 'Save & Close' and 'Cancel' buttons.

Administrator Tab

Setting	Description
Email Address	Enter a valid email address for the <a href="#">PRTG System Administrator</a> user account. By default, PRTG sends notifications and important messages

Setting	Description
	to this address.
Login Name	Enter a login name for the <a href="#">PRTG System Administrator</a> user account. You use it when you log in to the PRTG web interface or the PRTG app for desktop.   The default login name is <a href="#">prtgadmin</a> .
Password	Click Generate new password and confirm to generate a new password for the <a href="#">PRTG System Administrator</a> user account. Click Save & Close to set the new password. You use it when you log in to the PRTG web interface or the PRTG app for desktop.   The default password is <a href="#">prtgadmin</a> .

## Probe Settings for Core Connection

Define general settings regarding the local probe and connections.

Probe Settings for Core Connection Tab

Probe Settings

Setting	Description
Probe Name	Enter a meaningful name to identify the local probe. By default, PRTG shows this name in the <a href="#">device tree</a> <sup>[164]</sup> , as well as in <a href="#">alarms</a> <sup>[202]</sup> , <a href="#">logs</a> <sup>[210]</sup> , <a href="#">notifications</a> <sup>[2735]</sup> , <a href="#">reports</a> <sup>[2754]</sup> , <a href="#">maps</a> <sup>[2776]</sup> , <a href="#">libraries</a> <sup>[2738]</sup> , and <a href="#">tickets</a> <sup>[213]</sup> . Enter a string.  ⓘ If the name contains angle brackets (<>), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a>
Reconnect Time	Define the time that PRTG waits for the local probe to reconnect to the PRTG core server if the connection fails. Enter an integer.

### Connection to PRTG Core Server

These settings affect the way that the local probe connects to the PRTG core server.

Setting	Description
Server (IPv4 Address or DNS Name)	The local probe connects to the PRTG core server via <a href="#">127.0.0.1</a> . You cannot change this.
GID	<p>The <a href="#">probe GID</a> is a unique identifier for the local probe. You cannot change the GID on the PRTG core server system.</p> <ul style="list-style-type: none"> <li>ⓘ Edit GID and Generate new GID are only available on the remote probe system. For more information, see section <a href="#">PRTG Administration Tool on Remote Probe Systems</a><sup>[3067]</sup>.</li> <li>ⓘ You can deny GIDs under Setup   System Administration   <a href="#">Core &amp; Probes</a><sup>[2890]</sup> in the PRTG web interface.</li> </ul>
Access Key	<p>Access Key is only available on the remote probe system.</p> <ul style="list-style-type: none"> <li>ⓘ For more information, see section <a href="#">PRTG Administration Tool on Remote Probe Systems</a><sup>[3067]</sup>.</li> </ul>
Confirm Access Key	<p>Confirm Access Key is only available on the remote probe system.</p> <ul style="list-style-type: none"> <li>ⓘ For more information, see section <a href="#">PRTG Administration Tool on Remote Probe Systems</a><sup>[3067]</sup>.</li> </ul>

### Path for the PRTG Data Directory on the Probe System

Setting	Description
Path	This setting is not available on the PRTG core server system. Please use Local Storage of Data Files and Monitoring Database on the <a href="#">PRTG Core Server</a> <sup>[3046]</sup> tab instead.

## Probe Settings for Monitoring

PRTG Network Monitor - PRTG Administration Tool

**PAESSLER** PRTG Network Monitor

PRTG Web Server PRTG Core Server Cluster Administrator

Probe Settings for Core Connection **Probe Settings for Monitoring** Service Start/Stop Logs and Info

**IPv4: Outgoing IP Address for Monitoring Requests**

IPv4 Address	Adapter Name	Adapter Type
<input checked="" type="radio"/> auto		
<input type="radio"/> 192.0.2.1	Ethernet0	Ethernet

**IPv6: Outgoing IP Address for Monitoring Requests**

IPv6 Address	Adapter Name	Adapter Type
<input checked="" type="radio"/> auto		
<input type="radio"/> 2001:db8::1234:5678	Ethernet0	Ethernet

Save & Close Cancel

Probe Settings for Monitoring Tab

Define the IP address to use for outgoing monitoring requests.

- If more than one IP is available on the system, you can specify the IP address that PRTG uses for the outgoing monitoring requests of certain sensors.
  - This setting is for sensors that use the following connection types: HTTP, Domain Name System (DNS), File Transfer Protocol (FTP), Internet Message Access Protocol (IMAP), Post Office Protocol version 3 (POP3), port, remote desktop, Simple Mail Transfer Protocol (SMTP), and Simple Network Management Protocol (SNMP).
  - The setting is valid for all monitoring requests that this probe sends.
  - This setting is useful for devices that expect a certain IP address when they are queried.
  - The default setting is auto. PRTG automatically selects an IP address.
- i** This feature does not support all sensors for technical reasons.
- i** If you change this setting, some sensors might stop working. For example, sensors might show the Down status if the selected IP address is blocked on the way to or directly on the target device.

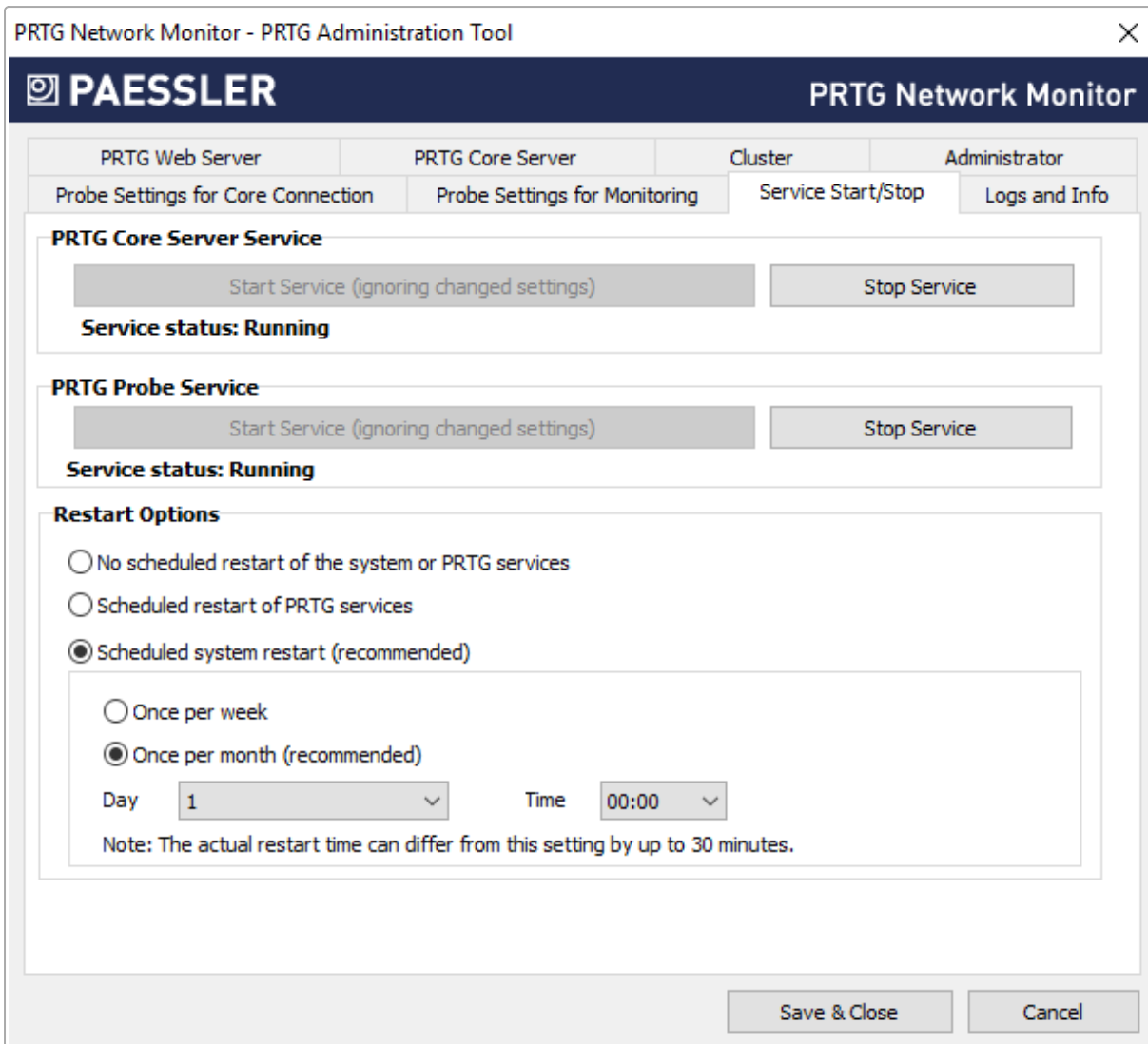


Setting	Description
IPv4: Outgoing IP for Monitoring Requests	Define the IP address for outgoing requests that use the IPv4 protocol. The list shows all available IP addresses on the system. Choose a specific IP address or select auto.
IPv6: Outgoing IP for Monitoring Requests	Define the IP address for outgoing requests that use the IPv6 protocol. The list shows all available IP addresses on the system. Choose a specific IP address or select auto.  ■ For more information, see section <a href="#">IPv6 Support</a> <sup>[150]</sup> .

## Service Start/Stop

You can manually start and stop the PRTG core server service and PRTG probe service. Click the respective buttons to start or stop the respective service. Both actions usually take from a few seconds up to several minutes. You can also restart the PRTG core server service and PRTG probe service under Setup | System Administration | [Administrative Tools](#)<sup>[2919]</sup> in the PRTG web interface.

**i** We recommend that you schedule automatic system restarts.



Service Start/Stop Tab

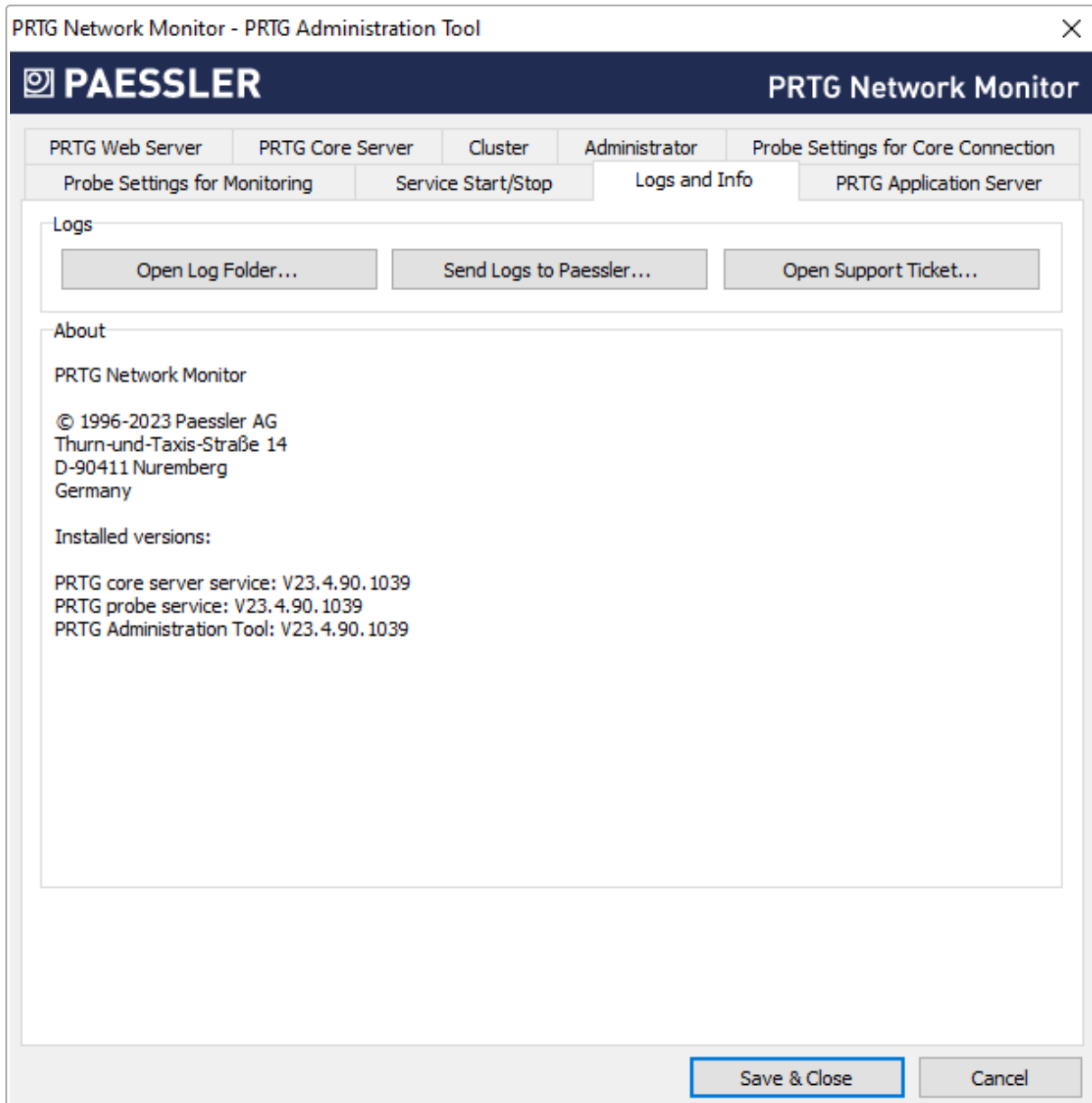
### Restart Options

Setting	Description
Restart Options	<p>Define if you want to schedule an automatic restart:</p> <ul style="list-style-type: none"> <li>▪ <b>No scheduled restart of the system or PRTG services:</b> Do not automatically perform a scheduled restart of services. We recommend that you manually restart the PRTG core server system every few weeks. You can also restart the PRTG core server service and PRTG probe service under <a href="#">Administrative Tools</a> (2918) in the PRTG web interface.</li> <li>▪ <b>Scheduled restart of PRTG services:</b> Restart the PRTG core server service on the PRTG core server system. If you select this option, the PRTG probe service restarts as well. Define a schedule under Restart Schedule.</li> </ul>

Setting	Description
	<p>☁ This setting is not available on the hosted probe of a PRTG Hosted Monitor instance.</p> <ul style="list-style-type: none"> <li>▪ Scheduled system restart (recommended): Define a schedule under Restart Schedule. We recommend that you restart every PRTG core server system once a month for best performance.</li> </ul>
Restart Schedule	<p><b>This setting is only visible if you select</b> Scheduled restart of PRTG services <b>or</b> Scheduled system restart (recommended) <a href="#">above</a>.</p> <p>Choose how often you want to restart the PRTG core server service, PRTG probe service, or the PRTG core server system:</p> <ul style="list-style-type: none"> <li>▪ Once per week: Select a day and a time below.</li> <li>▪ Once per month (recommended): Select a day of the month and a time below.</li> </ul>
Day	<p><b>This setting is only visible if you select</b> Scheduled restart of PRTG services <b>or</b> Scheduled system restart (recommended) <a href="#">above</a>.</p> <p>Select a day of the week (<a href="#">Monday</a> to <a href="#">Sunday</a>) or month (<a href="#">1st</a> to <a href="#">30th</a> or <a href="#">Last</a>). If you select Last, PRTG restarts the PRTG core server system on the last day of the month, regardless of how many days the month has.</p> <p><b>i</b> If you select a date that does not exist in every month (for example, the 30th day in February), PRTG automatically restarts the PRTG core server system on the last day of this month.</p>
Time	<p><b>This setting is only visible if you select</b> Scheduled restart of PRTG services <b>or</b> Scheduled system restart (recommended) <a href="#">above</a>.</p> <p>Select the time of the day when PRTG restarts the PRTG core server system.</p> <p><b>i</b> You get a Windows warning message 10 minutes before the restart to inform you about the restart if you are logged in to PRTG. The actual restart time can differ by up to 30 minutes from the time you enter here.</p>

**i** You can also define a restart schedule on the Settings [tab](#)<sup>523</sup> of a remote probe in the PRTG web interface.

## Logs and Info



Logs and Info Tab

## Logs

Button	Description
Open Log Folder	Open the <a href="#">PRTG data directory</a> <sup>[3214]</sup> to access all logs that PRTG creates.
Send Logs to Paessler	Open an assistant to send logs to the Paessler support team. See <a href="#">Send Logs to Paessler</a> <sup>[3063]</sup> for details.

Button	Description
	<ul style="list-style-type: none"> <li>ⓘ This feature is only available with the <a href="#">commercial edition</a> of PRTG.</li> <li>ⓘ You can also send logs with the support bundle via <a href="#">Contact Support</a> in the PRTG web interface.</li> </ul>
Open Support Ticket	<p>Open the Help Desk portal on the Paessler website in a browser window.</p> <ul style="list-style-type: none"> <li>ⓘ If you need help, we recommend that you use the Contact Support option in the PRTG web interface instead.</li> </ul>

### About

The About section shows information about the version of installed PRTG programs and copyright information.

### Send Logs to Paessler

- ⓘ You can also send logs with the support bundle via Contact Support in the PRTG web interface.

Send Logs to Paessler

**PAESSLER**
PRTG Network Monitor

### Send Logs to Paessler

Name

Email

Ticket#

Please supply your ticket number (PAEXXXX) if you already have an open support ticket.

Configuration  Include configuration file (contains passwords)

Note: All passwords used in PRTG are encrypted in the configuration file, but SNMP community names and hostnames might be written in plain text.

If you click the "Send" button, this program will upload the relevant log files and, if selected, the configuration file of your PRTG installation to the Paessler FTP server and support ticket system.

Please ensure that outgoing FTP and HTTP connections are enabled on this machine.

Note: Support communication can only be provided in English or German!

Send Logs to Paessler

If you open a support ticket, the Paessler support team might ask you to send logs for further analysis.

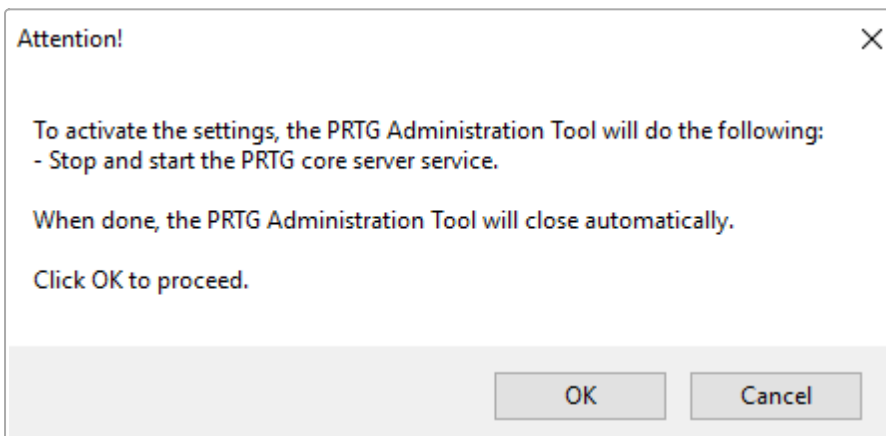
Field	Description
Name	Enter your name.
Email	Enter a valid email address. You can provide any email address but we recommend that you use the email address of your user account, which PRTG enters by default.
Ticket #	This field is optional. If you have already opened a ticket with the Paessler support team, provide the ticket number you received. Your files are then automatically associated with your ticket.

Field	Description
	Enter the ticket number starting with <b>PAE</b> followed by four or more digits, for example, <b>PAE12345</b> . If you do not have a ticket number, leave this field empty.
Configuration	<p>Define if you want to include the configuration file. PRTG removes all passwords from the configuration file before sending it to the Paessler support team.</p> <p><b>i</b> If a configuration file is too large, some 32-bit systems might not be able to send the file with hidden passwords. In these cases, PRTG confirms that you still want to send the configuration file to the Paessler support team. The passwords are still encrypted.</p>

Click Send to start the data upload. PRTG then automatically collects, compresses, and sends your logs to our FTP over SSL (FTPS) server. Make sure that FTPS and HTTP connections are allowed on the remote probe system.

### Activate Changed Settings

After you change settings, click Save & Close. A new dialog box appears where PRTG asks you to agree to restart the PRTG core server service. Click OK to proceed.



Restart Services

### More

#### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Why does my browser show an SSL certificate warning when I open the PRTG web interface?

- <https://kb.paessler.com/en/topic/89984>

Which ports does PRTG use on my system?

- <https://kb.paessler.com/en/topic/61462>



## 13.2 PRTG Administration Tool on Remote Probe Systems

If you start the PRTG Administration Tool on a remote probe system, you can define various probe-related settings, restart services, and view log information. You can also change many of these settings via the [system administration](#)<sup>[2853]</sup> and the [probe settings](#)<sup>[521]</sup> in the PRTG web interface.

**i** The PRTG Administration Tool is only available on Windows systems and does not affect multi-platform probes. For more information on how to configure and restart multi-platform probes, see the [Multi-Platform Probe for PRTG](#) manual.

In this section:

- [Start the PRTG Administration Tool](#)<sup>[3067]</sup>
- [Probe Settings for Core Connection](#)<sup>[3067]</sup>
- [Probe Settings for Monitoring](#)<sup>[3071]</sup>
- [Service Start/Stop](#)<sup>[3072]</sup>
- [Scheduled Restart Settings](#)<sup>[3073]</sup>
- [Logs and Info](#)<sup>[3075]</sup>
- [Send Logs to Paessler](#)<sup>[3076]</sup>
- [Activate Changed Settings](#)<sup>[3078]</sup>

**i** This section describes the available settings in the PRTG Administration Tool when you open it on a remote probe system. This is not the complete set of available settings. If you need access to all settings regarding the entire PRTG installation, open the PRTG Administration Tool on the PRTG core server system.

**i** Settings you make here are only valid for the remote probe system on which you open the PRTG Administration Tool. Make sure that you log in to the system that you want to make changes to and open the PRTG Administration Tool there.

### Start the PRTG Administration Tool

- From the Windows Start menu, select the PRTG Network Monitor folder and click PRTG Administration Tool to open the application.
- Confirm the question of the Windows [User Account Control](#) with Yes to allow the PRTG Administration Tool to start.

### Probe Settings for Core Connection

Define general settings regarding the remote probe and connections.

Probe Settings for Core Connection Tab

Probe Settings

Setting	Description
Probe Name	<p>Enter a name to identify the remote probe. PRTG shows this name, for example, in the device tree, and in all alarms by default. Enter a string.</p> <p><b>i</b> If the name contains angle brackets (&lt;&gt;), PRTG replaces them with braces ({} for security reasons. For more information, see the Knowledge Base: <a href="#">What security features does PRTG include?</a></p>




Setting	Description
Reconnect Time	Define the time that PRTG waits for the remote probe to reconnect to the PRTG core server if the connection fails. Enter an integer.

#### Connection to PRTG Core Server

These settings affect the way the remote probe connects to the PRTG core server.

Setting	Description
Server (IPv4 Address or DNS Name)	Enter the IP address or Domain Name System (DNS) name of the PRTG core server.
GID	<p>The <b>probe GID</b> (global ID (GID)) is a unique identifier for the remote probe. We recommend that you do not change it.</p> <p><b>Exceptions:</b> If you substitute a remote probe from a different computer, you must copy the GID from the old probe to the new probe. To do so, click Edit GID and confirm the warning with Yes. You can then change the GID. PRTG checks if the GID is valid. You can also generate a new GID if necessary. To do so, click Generate new GID and confirm the warning with Yes.</p> <p><b>i</b> You can deny GIDs under Setup   System Administration   <a href="#">Core &amp; Probes</a><sup>[2890]</sup> in the PRTG web interface. If you remove a remote probe from the device tree or if you <a href="#">deny a remote probe after installation</a><sup>[106]</sup>, PRTG automatically enters its GID in the Deny GIDs list.</p>
Access Key	<p>The probe access key must match one of the access keys in the PRTG core server installation. If it does not match, the remote probe is not able to connect to the PRTG core server.</p> <p><b>■</b> For more information, see section <a href="#">Core &amp; Probes</a><sup>[2890]</sup>.</p> <p><b>i</b> Also check the allowed and denied IP addresses in the <a href="#">Core &amp; Probes</a><sup>[2890]</sup> settings to make sure that the PRTG core server accepts the IP address of the remote probe.</p>
Confirm Access Key	If you enter an access key for a remote probe, enter it in this field again to confirm it.

#### Path for the PRTG Data Directory on the Probe System

Setting	Description
Path	<p>Select the directory where PRTG stores configuration and monitoring data. Click  to choose a different folder on the system.</p> <p> Before you change the path, make sure you stop both the PRTG core server service and the PRTG probe service and copy all data to the new location.</p> <p> The directory name must include only ANSI characters. PRTG does not support data paths with non-ANSI characters.</p>

Language for the PRTG Administration Tool for Remote Probes

Setting	Description
[your language]	<p>Choose the language for the PRTG Administration Tool on the remote probe. The default is English.</p> <p>List of available languages:</p> <ul style="list-style-type: none"> <li>▪ Deutsch (German)</li> <li>▪ English</li> <li>▪ Español (Spanish)</li> <li>▪ Français (French)</li> <li>▪ Nederlands (Dutch)</li> <li>▪ Português (Portuguese)</li> <li>▪ Русский (Russian)</li> <li>▪ 日本語 (Japanese)</li> <li>▪ 简体中文 (Simplified Chinese)</li> </ul>

## Probe Settings for Monitoring

**IPv4: Outgoing IP for Monitoring Requests**

IPv4 Address	Adapter Name	Adapter Type
<input checked="" type="radio"/> auto		
<input type="radio"/> 192.0.2.0	Ethernet 2	Ethernet
<input type="radio"/> 192.0.2.1	Wi-Fi	IEEE80211

**IPv6: Outgoing IP for Monitoring Requests**

IPv6 Address	Adapter Name	Adapter Type
<input checked="" type="radio"/> auto		
<input type="radio"/> 2001:db8::1234:5678	Ethernet 2	Ethernet
<input type="radio"/> 2001:db8::1234:1234	Ethernet 2	Ethernet
<input type="radio"/> 2001:db8::3333:4444	Wi-Fi	IEEE80211
<input type="radio"/> 2001:db8::4444:5555	Wi-Fi	IEEE80211
<input type="radio"/> 2001:db8::5555:6666	Wi-Fi	IEEE80211
<input type="radio"/> 2001:db8::6666:7777	iphttpsinterface	Tunnel
<input type="radio"/> 2001:db8::7777:8888	inhttpsinterface	Tunnel

Buttons: Save & Close, Cancel

Probe Settings for Monitoring Tab

Define the IP address to use for outgoing monitoring requests.

- If more than one IP is available on the system, you can specify the IP address that PRTG uses for the outgoing monitoring requests of certain sensors.
- This setting is for sensors that use the following connection types: HTTP, Domain Name System (DNS), File Transfer Protocol (FTP), Internet Message Access Protocol (IMAP), Post Office Protocol version 3 (POP3), port, remote desktop, Simple Mail Transfer Protocol (SMTP), and Simple Network Management Protocol (SNMP).
- The setting is valid for all monitoring requests that this probe sends.
- This setting is useful for devices that expect a certain IP address when they are queried.
- The default setting is auto. PRTG automatically selects an IP address.

**i** This feature does not support all sensors for technical reasons.

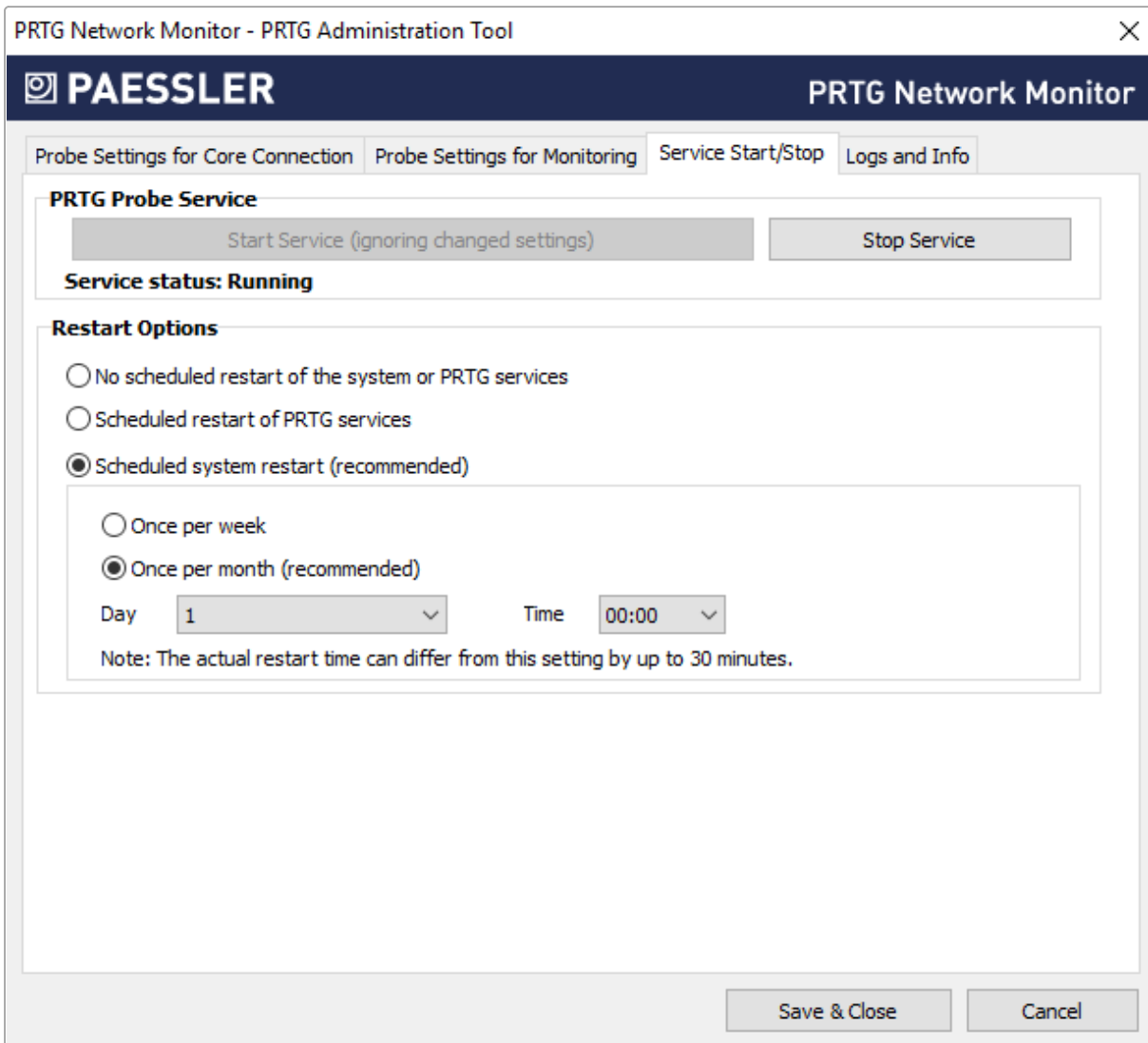
**i** If you change this setting, some sensors might stop working. For example, sensors might show the Down status if the selected IP address is blocked on the way to or directly on the target device.

Setting	Description
IPv4: Outgoing IP for Monitoring Requests	Define the IP address for outgoing requests that use the IPv4 protocol. The list shows all available IP addresses on the system. Choose a specific IP address or select auto.
IPv6: Outgoing IP for Monitoring Requests	Define the IP address for outgoing requests that use the IPv6 protocol. The list shows all available IP addresses on the system. Choose a specific IP address or select auto.  ■ For more information, see section <a href="#">IPv6 Support</a> <sup>[150]</sup> .

## Service Start/Stop

You can manually start and stop the PRTG probe service. Click Start Service to start the service or Stop Service to stop it. Both actions usually take from a few seconds up to several minutes. You can also restart the PRTG probe service under Setup | System Administration | [Administrative Tools](#)<sup>[2919]</sup> in the PRTG web interface.

**i** We recommend that you schedule automatic service restarts.



Service Start/Stop Tab

## Scheduled Restart Settings

☁ This setting is not available on the hosted probe of a PRTG Hosted Monitor instance.

Setting	Description
Restart Options	<p>Define if you want to schedule an automatic restart:</p> <ul style="list-style-type: none"> <li>No scheduled system or service restart: Do not automatically perform a scheduled restart of services. We recommend that you manually restart the PRTG core server system every few weeks. You can initiate a restart of the PRTG probe service in the <a href="#">Administrative Tools</a> [2918] in the PRTG web interface.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>▪ Scheduled restart of PRTG services: Restart the PRTG probe service on the probe system. If you select this option on the local probe, the PRTG core server service restarts as well. Define a schedule under Restart Schedule.</li> <li>▪ Scheduled system restart (recommended): Define a schedule under Restart Schedule. We recommend that you restart probe systems once a month for best performance.</li> </ul>
Restart Schedule	<p><b>This setting is only visible if you select</b> Scheduled restart of PRTG services <b>or</b> Scheduled system restart (recommended) <b>above</b>.</p> <p>Choose how often you want to restart the PRTG probe service or the probe system:</p> <ul style="list-style-type: none"> <li>▪ Once per week: Select a day and a time below.</li> <li>▪ Once per month (recommended): Select a day of the month and a time below.</li> </ul>
Day	<p><b>This setting is only visible if you select</b> Scheduled restart of PRTG services <b>or</b> Scheduled system restart (recommended) <b>above</b>.</p> <p>Select a day of the week (<b>Monday</b> to <b>Sunday</b>) or month (<b>1st</b> to <b>30th</b> or <b>Last</b>). If you select Last, PRTG restarts the PRTG core server system on the last day of the month, regardless of how many days the month has.</p> <p><b>i</b> If you select a date that does not exist in every month (for example, the 30th day of February), PRTG automatically initiates the restart on the last day of this month.</p>
Time	<p><b>This setting is only visible if you select</b> Scheduled restart of PRTG services <b>or</b> Scheduled system restart (recommended) <b>above</b>.</p> <p>Select the time of day when PRTG performs the restart.</p> <p><b>i</b> You get a Windows warning message 10 minutes before the restart to inform you about the restart if you are logged in to PRTG. The actual restart time can differ by up to 30 minutes from the time you enter here.</p>

**i** You can also define a restart schedule on the Settings [tab](#) of a remote probe in the PRTG web interface.



## Logs and Info

Send Logs to Paessler

**PAESSLER**
PRTG Network Monitor

### Send Logs to Paessler

Name

Email

Ticket#

Please supply your ticket number (PAEXXXX) if you already have an open support ticket.

If you click the "Send" button, this program will upload the relevant logfiles to Paessler's FTP server and support ticket system.

Please ensure that outgoing FTP and HTTP connections are enabled on this machine.



Note: Support communication can only be provided in English or German!

Send
Cancel

Logs and Info Tab

## Logs

Button	Description
Open Log Folder	Open the <a href="#">PRTG data directory</a> <sup>[3214]</sup> to access all logs that PRTG creates.
Send Logs to Paessler	<p>Open an assistant to send logs to the Paessler support team. See <a href="#">Send Logs to Paessler</a><sup>[3076]</sup> for details.</p> <p> This feature is only available with the <a href="#">commercial edition</a><sup>[20]</sup> of PRTG.</p>

Button	Description
	<p> You can also send logs with the support bundle via <a href="#">Contact Support</a> in the PRTG web interface.</p>
Open Support Ticket	<p>Open the Help Desk portal on the Paessler website in a browser window.</p> <p> If you need help, we recommend that you use the Contact Support option in the PRTG web interface instead.</p>

## About

The About section shows information about the version of installed PRTG programs and copyright information.

## Send Logs to Paessler

 You can also send logs with the support bundle via Contact Support in the PRTG web interface.

Send Logs to Paessler

**PAESSLER**
PRTG Network Monitor

### Send Logs to Paessler

Name

Email

Ticket#

Please supply your ticket number (PAEXXXX) if you already have an open support ticket.

If you click the "Send" button, this program will upload the relevant logfiles to Paessler's FTP server and support ticket system.

Please ensure that outgoing FTP and HTTP connections are enabled on this machine.

Note: Support communication can only be provided in English or German!

Send Logs to Paessler

If you open a support ticket, the Paessler support team might ask you to send logs for further analysis.

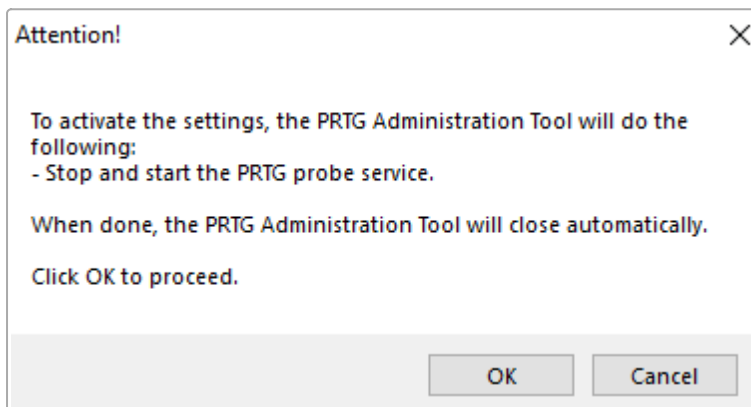
Field	Description
Name	Enter your name.
Email	Enter a valid email address. You can provide any email address but we recommend that you use the email address of your user account, which PRTG enters by default.
Ticket #	This field is optional. If you have already opened a ticket with the Paessler support team, provide the ticket number you received. Your files are then automatically associated with your ticket.

Field	Description
	Enter the ticket number starting with <b>PAE</b> followed by four or more digits, for example, <b>PAE12345</b> . If you do not have a ticket number, leave this field empty.

Click Send to start the data upload. PRTG then automatically collects, compresses, and sends your logs to our FTP over SSL (FTPS) server. Make sure that FTPS and HTTP connections are allowed on the remote probe system.

### Activate Changed Settings

After you change settings, click Save & Close. A new window opens where PRTG asks you to agree to restart the PRTG probe service. Click OK to proceed.



Restart Services

### More

#### ■ KNOWLEDGE BASE

What security features does PRTG include?

- <https://kb.paessler.com/en/topic/61108>

Which ports does PRTG use on my system?

- <https://kb.paessler.com/en/topic/61462>






















# Part 14

## Advanced Topics

# 14 Advanced Topics


In this section, we cover more advanced topics. If you already have some experience with PRTG, you might want to learn more about the following topics.

In this section:

- [Active Directory Integration](#) 
- [Application Programming Interface \(API\) Definition](#) 
  - [HTTP API](#) 
  - [Live Data](#) 
  - [Live Graphs](#) 
  - [Historic Data](#) 
  - [Object Manipulation](#) 
  - [Custom Sensors](#) 
  - [Custom Notifications](#) 
  - [Mini Probe API](#) 
- [Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors](#) 
- [Channel Definitions for Flow, IPFIX, and Packet Sniffer Sensors](#) 
- [Define IP Address Ranges](#) 
- [Define Lookups](#) 
- [Regular Expressions](#) 
- [Calculating Percentiles](#) 
- [Add Remote Probe](#) 
  - [Remote Probes and Multiple Probes](#) 
  - [Classic Remote Probe Setup via Device Tools](#) 
- [Failover Cluster Configuration](#) 
- [Data Storage](#) 

## 14.1 Active Directory Integration

You can add PRTG user groups to PRTG, or you can add user groups from an Active Directory (AD). When you integrate the AD into PRTG, you map a user group from the AD to a user group in PRTG. All members of the AD group can then log in to PRTG with their AD domain credentials.

 You cannot add single AD users to PRTG. You can only allow access for entire AD groups. PRTG automatically creates a user account for each AD user that successfully logs in to PRTG.

 This feature is not available in PRTG Hosted Monitor.



### Step 1: Prepare the AD

- In the AD, make sure that the users that you want to give access to PRTG are members of the same user group in the AD.
- You can also organize users into different user groups, for example, one user group whose members have administrative rights in PRTG, and one user group whose members only have read access in PRTG.


### Step 2: Prepare the PRTG Core Server

- Make sure that the PRTG core server system is a member of the domain that you want to integrate it into. To check this setting, open the Windows Control Panel and click the Change settings link under System, section Computer name, domain, and workgroup settings.

### Step 3: Add AD Domain and Credentials (optional) to System Settings

- In the [PRTG web interface](#) <sup>124</sup>, select Setup | System Administration | Core & Probes from the main menu.
- In section Active Directory Integration, enter the name of the local AD domain in the Domain Name field.
  -  You can only integrate one AD domain into PRTG.
- The following process is optional. PRTG uses the same Windows user account from which a user runs the PRTG core server service. By default, this is the [local system](#) Windows user account. If this user does not have sufficient rights to query a list of all user groups from the AD, provide the credentials of a user account that has full AD access by using the Use explicit credentials option as Access Type.
  -  If you cannot save changes to the Core & Probes settings because you get an [Error \(Bad Request\)](#) with the message [Active Directory Domain not accessible](#), select Use explicit credentials as Access Type and provide the correct credentials for your AD domain.
- Save your settings.

### Step 4: Add a New User Group

- Go to the User Groups [tab](#) <sup>2912</sup>.
- Hover over  and click Add User Group to add a new user group.
- Enter a User Group Name to identify the group and select Use Active Directory integration under Active Directory or Single Sign-On Integration.

- From the Active Directory Group dropdown list, select the group in the AD whose members have access to PRTG. If you have a very large AD with more than 1,000 entries, you see an input field instead of a dropdown list. In this case, you can only enter the name of the user group in the AD. PRTG automatically adds the domain name prefix.
- For User Type, define the [access rights](#)<sup>[145]</sup> that a user from the selected AD group has when they log in to PRTG for the first time. You can choose between Read/write user and Read-only user. Read-only access is useful to only show data to a large group of users.
- Click Create.

All users in this newly created AD group can now log in to PRTG with their AD domain credentials. Their user accounts have the [group access rights](#)<sup>[145]</sup> of the user group that you just created.

## Notes and Restrictions

- AD users can [log in](#)<sup>[153]</sup> to the PRTG web interface with their Windows user name and password. Do not enter any domain information in the Login Name field. When an AD user logs in, PRTG automatically creates a corresponding local account on the PRTG core server. PRTG synchronizes credentials every hour.
- Do not change the Login Name in PRTG for AD users unless the name changes in the AD. If you change the Login Name in PRTG, it has no effect on the name in the AD.
- AD queries are in read-only mode and are compatible with Read-only Domain Controllers (RODC).
- For performance reasons, PRTG caches all requests to AD servers for one hour. If a password changes, if you add a new user group in the AD, or if you change the group membership of an AD user, you must either wait one hour or manually clear the cache by selecting Setup | System Administration | Administrative Tools from the main menu and clicking Go! in the Clear Caches section.
- By default, no access rights for monitoring objects, libraries, maps, or reports are set for the new user group in PRTG. This is why, initially, users in this user group do not see monitoring objects, libraries, maps, or reports. This does not apply if the new user group has administrative rights. Edit the monitoring [object's settings](#)<sup>[201]</sup> and the settings of libraries, maps, and reports, and set access rights for the newly created user group in the respective Access Rights section.
  - ⓘ We recommend that you set these access rights in the [root group settings](#)<sup>[453]</sup> and use the [inheritance of settings](#)<sup>[136]</sup>.
- PRTG only supports **explicit** user group rights. If the AD uses groups that are members of other user groups, PRTG does **not** regard the inherited implicit rights of the parent group and therefore refuses the login for members of these user groups.
- PRTG ignores AD information about organization units (OU). PRTG cannot read these values. However, if you use the AD in an [auto-discovery group](#)<sup>[262]</sup>, you can restrict the auto-discovery to machines that are part of an OU.
- You can integrate only one AD domain into PRTG.
- PRTG does not support trusted domains or AD subdomains.
- If you have a very large AD with more than 1,000 entries, you see an input field instead of a dropdown list. In this case, you can only enter the name of the user group in the AD. PRTG automatically adds the domain name prefix.
- A local user account for an AD user is only created if this AD user has successfully logged in to PRTG. If you want to send [email notifications](#)<sup>[2815]</sup> to an AD group in PRTG using the option Send to User Group in the notification settings, a member of this AD group has to log in to PRTG at least once to receive email notifications. To avoid this, enter the email address of the AD group in the Send to Email Address field in the notification settings and select None for the Send to User Group option.



- If you want to delete an AD group from PRTG because of some changes to the AD, for example, you must delete all users that are in this user group first. This is because AD users always have this user group set as their primary group, and user accounts must have a primary group.
- If you change the group membership of an AD user, this change is only reflected in the respective user groups in PRTG if this AD user has logged in to PRTG again.
- If you delete an AD user from all user groups in the AD that are related to PRTG access, this user cannot log in to PRTG anymore. However, you still see the user in the user account list in PRTG.

## More

### KNOWLEDGE BASE

How to integrate Microsoft Entra ID into PRTG?

- <https://kb.paessler.com/en/topic/88527>

## 14.2 Application Programming Interface (API) Definition

The PRTG API enables you to access monitoring data and manipulate objects using HTTP requests, run your own written sensors and notifications, and implement mini probes.

In this section:

- [HTTP API](#)<sup>[3085]</sup>
- [Live Data](#)<sup>[3088]</sup>
  - [Single Object Property](#)<sup>[3089]</sup>
  - [Single Object Status](#)<sup>[3092]</sup>
  - [Multiple Object Property or Status](#)<sup>[3099]</sup>
  - [System Information](#)<sup>[3120]</sup>
- [Live Graphs](#)<sup>[3124]</sup>
- [Historic Data](#)<sup>[3127]</sup>
- [Object Manipulation](#)<sup>[3130]</sup>
- [Custom Sensors](#)<sup>[3137]</sup>
- [Custom Notifications](#)<sup>[3151]</sup>
- [Mini Probe API](#)<sup>[3153]</sup>

### More

#### KNOWLEDGE BASE

How can I share my self-written PRTG script/program with other PRTG users?

- <https://kb.paessler.com/en/topic/63737>

Where can I find PRTG mini probes which are ready to use?

- <https://kb.paessler.com/en/topic/61215>

## 14.2.1 HTTP API

All calls to the PRTG API are performed by HTTP GET requests. The URLs consist of a path to the API function and some parameters.

- If you are accessing the PRTG API inside your secure LAN, you can use HTTP. In environments that are not secure (for example, when accessing your PRTG core server via the internet), you should use HTTPS requests to make sure that your parameters and passwords are encrypted. This way, all communication between the PRTG core server and your client is Secure Sockets Layer (SSL) encrypted.
- For every API call, the default limit of items is **500**. If you want to receive more items per call, add a `count=xxx` parameter with enough room for all sensors.
- You must include authentication with API key or user name and `passhash` (or user name and password) in each request.  
■ See section [Authentication](#) for more information.
- All data in the GET parameters must be **UTF-8**-encoded and **URL** encoded.

### Output Formats

Most data that you can request from the PRTG API is available in data tables in the Extensible Markup Language (XML), the JavaScript Object Notation (JSON) format, and the comma-separated values (CSV) format (using the XML format is recommended). Here are some sample calls with different output formats.

 **Examples**

**XML**

```
https://yourserver/api/table.xml?content=sensors&columns=sensor
```

**JSON**

```
https://yourserver/api/table.json?content=sensors&columns=sensor
```

**CSV**

```
https://yourserver/api/table.xml?content=sensors&columns=sensor&output=csvtable
```

The example URLs consist of the following elements.

Element	Description
yourserver	The name of your PRTG server.
/api/table.xml or /api/table.json	Addresses an API function. Here, the function renders a table in the XML format or in the JSON format.
content=sensors	Parameter for additional control. In this case, it includes all sensors in the table.

Element	Description
columns=sensor	Parameter for additional control. In this case, only the names of all sensors are shown in the table.
output=csvtable (optional)	Renders a table in the CSV format.

## Authentication

All requests to the PRTG API are stateless, which means that there is no multi-step login process of any kind. You must include the authentication with an API key or with a user name and a passhash (or a user name and a password) in each request by using the apitoken parameter or the user name and passhash (or user name and password) parameters:

apitoken parameter

- apitoken=myapitoken

**i** You can add, edit, and delete your API keys in the account settings on the [API Keys](#)  tab.

user name and passhash (or user name and password) parameters

- username=myuser&passhash=hash (or password=mypassword)

**i** You can request the passhash for an account with the following API call:

<https://yourserver/api/getpasshash.htm?username=myuser&password=mypassword>

**i** Make sure that the user name and password are URL-encoded.

### Examples

```
https://yourserver/api/table.xml?content=sensors&columns=sensor&apitoken=myapitoken
```

or:

```
https://yourserver/api/table.xml?content=sensors&columns=sensor&username=myuser&password=mypassword
```

or:

```
https://yourserver/api/table.xml?content=sensors&columns=sensor&username=myuser&passhash=hash
```

## Versioning

Most XML replies from the PRTG API contain a `<version>` field that contains the [program version](#) and [buildnumber](#) of the server's PRTG installation. Your client must look at this version number and compare it to the version number that was used to develop the client. Do not accept version numbers older (smaller) than this one. You should display a warning to the user (or stop processing) if the version number differs by **0.1** or more (for example, version **18.1** vs. **18.2**, or version **17.x** vs. **18.x**). PRTG API conventions or parameters might have changed between versions.

**i** Newer versions of the same major version of PRTG reply to API calls just like previous versions did.

## Error Handling

Depending on whether an API call was successfully processed or not, the PRTG core server replies with the following HTTP status codes:

HTTP Status Code	Meaning	Comments
200	OK	The API call was successfully completed , the XML response contains the result data.
302	Found	The API call was successfully completed and a new object was created (the redirection URL contains the new object ID).
400	Bad Request	The API call could not be successfully completed. The XML response contains the error message.
401	Unauthorized	The user name/password credentials cannot be accepted.

For 400 error codes, the error .xml document includes the error message as follows:

```
<?xml version="1.0" encoding="UTF-8" ?>
<prtg>
  <version>23.4.90.1235+</version>
  <error>Sorry, there is no object with the specified id.</error>
</prtg>
```

## More

### ■ KNOWLEDGE BASE

How can I use the PRTG Application Programming Interface (API)?

- <https://kb.paessler.com/en/topic/593>

## 14.2.2 Live Data


You can access live data and live status data of objects using the PRTG API.

In this section:

- [Single Object Property](#) [3089]
- [Single Object Status](#) [3092]
- [Multiple Object Property or Status](#) [3099]
- [System Information](#) [3120]

### Getting PRTG System Status

You can also get the PRTG system status such as the number of alarms or messages using the following API calls.

 **Examples**

Live system status in the Extensible Markup Language (XML) format:

```
/api/getstatus.xml?id=0
```

Live system status in the JavaScript Object Notation (JSON) format:

```
/api/getstatus.htm?id=0
```

All sensors in use in the JSON format:


```
/api/sensortypesinuse.json
```

Number of all sensor states:

```
/api/gettreenodestats.xml
```

### Getting PRTG Health Status

You can also get the overall PRTG system health status such as probe connection status and if login is possible using the following API calls:

 **Examples**

Live overall system status of PRTG in the JSON format:

```
/api/healthstatus.json
```

Live overall system status of PRTG Hosted Monitor in the JSON format:

```
/api/healthstatus.json&mode=hosted
```

## Getting PRTG Health Data

You can also get the PRTG health data such as system CPU used (%), system memory used (%), disk space used (%), disk space used (GB), health (%), total number of probes, disconnected probes, total sensors, and sensor in the Unknown status using the following API calls:

### Example

Live health data of PRTG in the JSON format using `maxage`:

```
/api/health.json&maxage=age
```

**i** `maxage` is the age in seconds for data to be considered "old". For example, if data is older than 4 minutes and `maxage=120`, the data will be refreshed and then sent to the client.

Live health data of PRTG in the JSON format using `refreshnow`:

```
/api/health.json&refreshnow=1/anything_else
```

**i** If `refreshnow=1`, the data will be refreshed before the API call is returned. Also, if `refreshnow=1` is present in the API call, `maxage` will not be considered.

## More

### KNOWLEDGE BASE

How can I use the PRTG Application Programming Interface (API)?

- <https://kb.paessler.com/en/topic/593>

### 14.2.2.1 Single Object Property

You can access live data and live status data of single objects using the PRTG API.

**i** Authentication with API key or user name and `passhash`<sup>[2803]</sup> (or user name and password) must always be included in each PRTG API request. See section [HTTP API](#)<sup>[8086]</sup> for more information.

In this section:

- [Property/Setting of an Object](#)<sup>[3089]</sup>
- [Supported Object Types](#)<sup>[3090]</sup>
- [Available Channel Parameters](#)<sup>[3091]</sup>
- [Property of a Channel](#)<sup>[3091]</sup>

### Property/Setting of an Object


You can get the properties or settings of an object (name, hostname, url) using the following API calls.

**i** Because properties might contain HTML content, we recommend that you include `&show=nohtmlencode` in all `getobjectproperty` API calls.

 Examples

Get an object property/setting:

```
/api/getobjectproperty.htm?id=objectid&name=propertyname&show=nohtmlencode
```

 For **propertyname**, look at the name of the INPUT fields while editing an object. You can discern the **propertyname** parameter by opening the Settings tab of an object and looking at the HTML source of the INPUT fields. For example, the INPUT field for the tags of an object has the name **tags\_**. Leave away the underscore **\_** and use **tags** as a value for the **propertyname** parameter.

Get a list of all tags for object ID 1003

```
/api/getobjectproperty.htm?id=1003&name=tags&show=nohtmlencode
```

The Extensible Markup Language (XML) result looks like this:

```
<?xml version="1.0" encoding="UTF-8" ?>
<prtg>
  <version>23.4.90.1235+</version>
  <result>probehealthsensor</result>
</prtg>
```

## Supported Object Types

[getobjectproperty.htm](#) supports the following object types:

- probe
- group
- device
- sensor
- channel
- library
- map
- notification
- report
- schedule
- user account

[getobjectproperty.htm](#) does not support the object types **ticket** and **user group**.



## Available Channel Parameters

Name of Input Field	Setting Name (as displayed in the PRTG web interface)
name	Name
limitmode	Limit disabled or enabled (0 or 1)
limitmaxerror	Upper Error Limit
limitmaxwarning	Upper Warning Limit
limitminwarning	Lower Warning Limit
limitminerror	Lower Error Limit
limiterroormsg	Error Limit Message
limitwarningmsg	Warning Limit Message

## Property of a Channel

With this API call, you can get a sensor's [channels settings](#)<sup>2681</sup>, for example channel limits. In general, this works like getting properties of any other object. To get channel properties via the PRTG API, you need to provide

- the ID of a sensor (parameter `id`),
- a `subtype` (`channel` for channels), and
- a `subid` (ID of the channel that you want to edit)

**i** Because properties might contain HTML content, we recommend that you include `&show=nohtmlencode` in all `getobjectproperty` API calls.

### Examples

#### Get a channel limit

```
/api/getobjectproperty.htm?  
id=sensorid&subtype=channel&subid=channelid&name=limitname&show=nohtmlencode
```

For example, the following API call gets the upper warning limit of a channel with the ID `0` of a sensor with the ID `1003`

```
/api/getobjectproperty.htm?  
id=1003&subtype=channel&subid=0&name=limitmaxwarning&show=nohtmlencode
```

The XML result looks like this:

```
<?xml version="1.0" encoding="UTF-8" ?>
<prtg>
  <version>23.4.90.1235+</version>
  <result>25</result>
</prtg>
```

## More

### ■ KNOWLEDGE BASE

How can I use the PRTG Application Programming Interface (API)?

- <https://kb.paessler.com/en/topic/593>

### 14.2.2.2 Single Object Status

You can access live data and live status data of single objects using the PRTG API.

- ❗ Authentication with API key or user name and [passhash](#) (or user name and password) must always be included in each PRTG API request. See section [HTTP API](#) for more information.

In this section:

- [Status of an Object](#)
- [Supported Object Types](#)
- [Supported getobjectstatus Output Columns \("Name=" Parameter\)](#)
- [Sensor Details](#)
- [Ticket Status and Message](#)

## Status of an Object

You can get the status information (lastvalue, downtime) of an object using the following API calls:

### 🗨 Examples

Get object status:

```
/api/getobjectstatus.htm?id=objectid&name=columnname
```

The Extensible Markup Language (XML) result looks like this:

```
<?xml version="1.0" encoding="UTF-8" ?>
<prtg>
  <<version>23.4.90.1235</version>
  <result>True</result>
</prtg>
```

**i** In some cases, the result can contain HTML formatting elements.

## Supported Object Types

[getobjectstatus.htm](#) supports the following object types:

- probe
- group
- device
- sensor


## Supported getobjectstatus Output Columns ("Name=" Parameter)





With [getobjectstatus.htm](#), you can use the following column names for the `name` parameter.

**i** Only one column name is allowed in the API call.

**i** If you want to use combinations of column names or more than one object in a single API call, use a [table](#) API call instead. For more information, see section [Multiple Object Property or Status](#) <sup>3093</sup>.

Column Name	What It Displays	Can Be Used for
objid	ID of the object	probes, groups, devices, sensors
type	Object type or sensor type	probes, groups, devices, sensors
name	Name of the object	probes, groups, devices, sensors
tags	List of all tags. This includes tags from the object itself plus tags that are inherited from parent objects.	probes, groups, devices, sensors
active	True/false depending on whether an object is set to paused by a user	probes, groups, devices, sensors
downtime	Cumulated downtime of the sensor (displayed as percentage of uptime+downtime)	sensors

Column Name	What It Displays	Can Be Used for
downtime	Cumulated downtime of the sensor (in minutes/hours)	sensors
downtimesince	Elapsed time since the last Up status of the sensor	sensors
uptime	Cumulated uptime of the sensor (displayed as percentage of uptime+downtime)	sensors
uptime	Cumulated uptime of the sensor (in minutes/hours)	sensors
uptimesince	Elapsed time since the last Down status of a sensor	sensors
knowntime	Sum of cumulated uptime and downtime of the sensor   The output contains HTML.	sensors
cumsince	Time stamp when accumulation of uptimes/downtimes began	sensors
sensor	Name of the sensor	sensors
interval	Effective interval setting for the sensor	sensors
lastcheck	Time stamp of the last sensor result   The output contains HTML.	sensors
lastup	Time stamp of the most recent Up status of the sensor   The output contains HTML.	sensors
lastdown	Time stamp of the most recent Down status of the sensor   The output contains HTML.	sensors
device	For sensors: ID of the associated device	devices, sensors

Column Name	What It Displays	Can Be Used for
	For devices: name of the associated device	
group	For sensors: ID of the associated group For devices: name of the associated group	groups, devices, sensors
probe	Name of the associated probe	probes, groups, devices, sensors
grpdev	Name of the associated device and associated group, separated by slash	sensors
notifiesx	Returns a string containing the number of each trigger type defined for this object. If trigger inheritance is active, it displays <a href="#">Inherited</a> .	probes, groups, devices, sensors
intervalx	Either <a href="#">Inherited</a> or the current interval setting of the object	probes, groups, devices, sensors
dependency	Name of an associated dependency or <a href="#">Parent</a>   The output contains HTML.	probes, groups, devices, sensors
probegroupdevice	Partial object hierarchy with names of associated device, group, and probe separated by angle brackets (>).   The output contains HTML.   <a href="#">probegroupdevice</a> is not available in the CSV format.   For the complete object hierarchy, use probe, group, device instead.	probes, groups, devices, sensors
status	Integer of the status of the object (0=None, 1=Unknown, 2=Scanning, 3=Up, 4=Warning, 5=Down, 6=No Probe, 7=Paused by User, 8=Paused by Dependency, 9=Paused by Schedule, 10=Unusual, 11=Not Licensed, 12=Paused Until, 13=Down Acknowledged, 14=Down Partial)	probes, groups, devices, sensors


Column Name	What It Displays	Can Be Used for
message	Detailed message of the object ⓘ The output contains HTML.	probes, groups, devices, sensors
priority	Priority setting of the object ⓘ The output contains HTML.	probes, groups, devices, sensors
lastvalue	Last sensor result value	sensors
upsens	Number of sensors in the Up status ⓘ PRTG only counts the sensor itself or sensors below the object in the hierarchy. ⓘ If the count is <1 PRTG returns "".	probes, groups, devices, sensors
downsens	Number of sensors in the Down status ⓘ PRTG only counts the sensor itself or sensors below the object in the hierarchy. ⓘ If the count is <1 PRTG returns "".	probes, groups, devices, sensors
downacksens	Number of sensors in the Down (Acknowledged) status ⓘ PRTG only counts the sensor itself or sensors below the object in the hierarchy. ⓘ If the count is <1 PRTG returns "".	probes, groups, devices, sensors
partialdownsens	Number of sensors in the Down (Partial) status ⓘ PRTG only counts the sensor itself or sensors below the object in the hierarchy. ⓘ If the count is <1 PRTG returns "".	probes, groups, devices, sensors
warnsens	Number of sensors in the Warning status	probes, groups, devices, sensors

Column Name	What It Displays	Can Be Used for
	<p>ⓘ PRTG only counts the sensor itself or sensors below the object in the hierarchy.</p> <p>ⓘ If the count is &lt;1 PRTG returns "".</p>	
pausedsens	<p>Number of sensors in the Paused status</p> <p>ⓘ PRTG only counts the sensor itself or sensors below the object in the hierarchy.</p> <p>ⓘ If the count is &lt;1 PRTG returns "".</p>	probes, groups, devices, sensors
unusualsens	<p>Number of sensors in the Unusual status</p> <p>ⓘ PRTG only counts the sensor itself or sensors below the object in the hierarchy.</p> <p>ⓘ If the count is &lt;1 PRTG returns "".</p>	probes, groups, devices, sensors
undefinedsens	<p>Number of sensors in an undefined status, like None, Unknown, No Probe</p> <p>ⓘ PRTG only counts the sensor itself or sensors below the object in the hierarchy.</p> <p>ⓘ If the count is &lt;1 PRTG returns "".</p>	probes, groups, devices, sensors
totalsens	<p>Number of all sensors</p> <p>ⓘ PRTG only counts the sensor itself or sensors below the object in the hierarchy.</p> <p>ⓘ If the count is &lt;1 PRTG returns "".</p>	probes, groups, devices, sensors
favorite	<p>An exclamation mark (!) if the object is marked as favorite</p> <p>ⓘ The output contains HTML.</p>	groups, devices, sensors
schedule	<p>Name of the associated schedule</p>	probes, groups, devices, sensors

Column Name	What It Displays	Can Be Used for
minigraph	Numeric data for the minigraphs. Numbers are 5-minute averages for the last 24 hours (must be scaled to the maximum of the series). There are two datasets: " " separates measured value series and error series.   The output contains HTML.	sensors
comments	Object comments	probes, groups, devices, sensors
host	Hostname or IP address	devices
condition	For probes: If the probe is connected or disconnected (0=Disconnected, 1=Unauthorized, 2=Connected, 3=Banned, 4=Init)  For groups: The auto-discovery status	probes, groups
basetype	Object type (string)	probes, groups, devices, sensors
baselink	URL of the object	probes, groups, devices, sensors
icon	URL of the device icon	devices
parentid	ID of the parent object	probes, groups, devices, sensors
location	Location property (used in Geo Maps)   The output contains HTML.	devices
groupnum devicenum	Number of groups or devices in the probe or group	probes, groups

## Sensor Details

You can get details about a sensor (sensortype, interval, uptime) using the following API calls:

-  You need the sensor ID to get details about a sensor. You can find the ID on the sensor's Overview tab or by hovering over a sensor in the device tree, for example. For more information about the Overview tab, see the Knowledge Base: [What options do I have to review my monitoring data in detail?](#)



 Examples

Get details about a sensor in the XML format:

```
/api/getsensordetails.xml?id=sensorid
```

Get details about a sensor in the JavaScript Object Notation (JSON) format:

```
/api/getsensordetails.json?id=sensorid
```

## Ticket Status and Message

The following API calls return status and message of a ticket.

 Examples

The status of a ticket:

```
/api/getticketstatus.htm?id=ticketid
```

The subject and assignee of a ticket:

```
/api/getticketmessage.htm?id=ticketid
```

## More

### KNOWLEDGE BASE

How can I use the PRTG Application Programming Interface (API)?


- <https://kb.paessler.com/en/topic/593>

What options do I have to review my monitoring data in detail?

- <https://kb.paessler.com/en/topic/90007>

### 14.2.2.3 Multiple Object Property or Status

You can access live data and live status data of multiple objects using the PRTG API.

 Authentication with API key or user name and [passhash](#)<sup>[2803]</sup> (or user name and password) must always be included in each PRTG API request. See section [HTTP API](#)<sup>[8086]</sup> for more information.

In this section:

- [Property or Status of Multiple Objects](#)<sup>[3100]</sup>
- [Table Query Builder](#)<sup>[3100]</sup>
- [Output Data Format](#)<sup>[3100]</sup>
- [RAW Date/Time Format](#)<sup>[3101]</sup>
- [Common Data Table Parameters](#)<sup>[3101]</sup>
- [Filtering by Object ID](#)<sup>[3102]</sup>

- [Sorting and Advanced Filtering](#) <sup>[3103]</sup>
- [Supported Output Columns \("columns=" Parameter\)](#) <sup>[3111]</sup>

## Property or Status of Multiple Objects

Most data that you can request from the PRTG API is available in data tables in the Extensible Markup Language (XML) format, the JavaScript Object Notation (JSON) format, and the comma-separated values (CSV) format (using the XML format is recommended). The API function [/api/table.xml](#) is used to access data in tables. Here are some sample calls (URLs are shown without authentication parameters to enhance readability).

- i** The example URLs only show the XML URLs. Use the API function [/api/table.csv](#) or the `output=constable` parameter to select the CSV format, or [/api/table.json](#) to return the JSON format.

**Examples**

A hierarchical list of all groups, devices, and sensors with their status information:

```
/api/table.xml?content=sensortree
```



**i** `sensortree` does not support JSON output.

All sensors (with status information):

```
/api/table.xml?
content=sensors&columns=objid,group,device,sensor,status,message,lastvalue,priority
,favorite
```

All recent log entries:

```
/api/table.xml?
content=messages&columns=objid,datetime,parent,type,name,status,message
```

You have the easiest start if you use the [table query builder](#) <sup>[3100]</sup> or click , which most data tables have in the PRTG web interface. Navigate to the information that you want to use, click , and you are taken to a URL that renders the content of the table in XML format. You can now use the URL as it is or change various parameters to suit your needs.

- For more information on possible raw message status values returned by table-based API calls, see the Knowledge Base: [Is there a list of log status values for the PRTG API?](#)

## Table Query Builder

You can use the query builder tool to experiment with the PRTG API and to fine-tune your queries. You can find it in the PRTG web interface under Setup | PRTG API, section Live Data.

## Output Data Format

XML data from the PRTG API contains the fields that you requested in the `columns` parameter. In most cases, numeric values are included twice: One field contains the value in human-readable format and an additional `_RAW` field contains the value as a number, which is better suited for further processing and calculations.

**Example**

```
<status>Up</status>
<status_RAW>3</status_RAW>
<lastvalue>98 %</lastvalue>
<lastvalue_RAW>97.7583</lastvalue_RAW>
<message>Created.<br/>18.3.43.1360</message>
<message_RAW>Created. 18.3.43.1360</message_RAW>
```

- The **status** field shows the value Up (the according RAW value is 3).
- The **lastvalue** field shows the value 98% (the according RAW value is 97.7583).
- The **message** field shows the text Created.<br/>18.3.43.1360 (the according RAW value is Created. 18.3.43.1360).

**i** Strings returned from **\_RAW** columns are surrounded by double quotation marks (") in JSON output.

### RAW Date/Time Format

For columns with date/time value, the RAW value is defined as follows: The integral part of a value is the number of days that have passed since Dec 30th, 1899. The fractional part of a value is a fraction of a 24-hour day that has elapsed. To find the fractional number of days between two dates, subtract the two values. Similarly, to increment a date and time value by a certain fractional number of days, add the fractional number to the date and time value.

Here are some examples of date/time RAW values and their corresponding dates and times:

RAW Date/Time Value	Description
0	12/30/1899 00h00m (12:00 midnight)
2.75	1/1/1900 18h00m (6:00 pm)
35065	1/1/1996 00h00m (12:00 midnight)

### Common Data Table Parameters

The following parameters are common to all data table API calls:


Parameter	Description	Possible Values
content	Select the objects that you want to have in your table.	sensortree (JSON output not supported)

Parameter	Description	Possible Values
		devices sensors tickets ticketdata messages values channels reports storedreports toplists sysinfo (only JSON output supported)
columns	Comma-separated list of columns per record	see <a href="#">Supported Output Columns ("columns=" Parameter)</a>
output	Control the output format	xml: default format (recommended) xmltable: an HTML table in the XML format csvtable: CSV format html: HTML table json: JSON format jsontable: a table in the JSON format
count	Maximum number of items (The default count is 500)	1-50000
start	Start with this entry number (can be used with "count" to request the data page by page)	any

### Filtering by Object ID

Add an ID parameter (for example, `id=1`) to the API URL to select a subset of items for the data table, for example, to reduce the amount of data transferred for each data table API call. The data table only contains information for this object ID and its child objects.

**i** Some table types require an ID. If you omit the ID parameter or if it has the value zero (0), all available objects are used.


Table Type (content=)	ID Required or Optional	Description	Object Types Allowed for the ID
sensortree	optional	You only get a part of the tree (the object with the specified ID and all child objects below it).   JSON output is not supported.	Probe Group
sensors devices	optional	You only get the object with the specified ID and all child objects below it.	Probe Group Device
tickets messages	optional	You only get tickets or log file entries that are related to the object with the specified ID or any child objects below it.	Any object
values channels	required	You get the data values (or channels) of the sensor with the specified ID.	Sensor
reports	not used	This data table always includes all reports.	n/a
storedreports	required	You get a list of stored .pdf files of the report selected by the ID.	Report
ticketdata	required	You get the history of the ticket selected by the ID.	Ticket
sysinfo	required	You get system information of the object with the specified ID.	Device

## Sorting and Advanced Filtering

There are various options to further filter and to sort the data for each data table API call:

Parameter	Description	Possible Values
filter_drel	<p>Only include records younger than this setting</p> <p><b>i</b> For <a href="#">content=messages</a> and <a href="#">content=tickets</a> only.</p>	<p>today</p> <p>yesterday</p> <p>7days</p> <p>30days</p> <p>12months</p> <p>6months</p>
filter_status	<p>Only include sensors with a specific status. Using multiple filter_status fields performs a logical OR.</p> <p><b>i</b> For <a href="#">content=sensors</a> and <a href="#">content=devices</a> only.</p>	<p>Unknown=1</p> <p>Collecting=2</p> <p>Up=3</p> <p>Warning=4</p> <p>Down=5</p> <p>NoProbe=6</p> <p>Paused by User=7</p>


Parameter	Description	Possible Values
		Paused by Dependency = 8 Paused by Schedule = 9 Unusual = 10 Paused by License = 11 Paused Until = 12 Down Acknowledged = 13 Down Partial = 14
filter_tags	Only include sensors with a specific tag. Using multiple filter_tag fields performs a logical OR. ⓘ For <a href="#">content=sensors</a> only.	@tag(tagname)

Parameter	Description	Possible Values
filter_xyz	<p>Filter the data. (Samples: filter_type=ping, filter_favorite=1). Using multiple filter_xyz fields performs a logical AND.</p> <p>Filtering using columns is only possible for tree objects. You cannot use columns to filter objects like messages or tickets, for example. For <a href="#">content=tickets</a>, you can use the special filter terms filter_status, filter_user, and filter_type (this corresponds to column tickettype).</p> <p>Like for messages, you can also use filter_drel, filter_dstart, and filter_dend.</p> <p> Multiple filters are not available for tickets.</p>	filter_xyz where xyz is any column name used in the columns parameter



Parameter	Description	Possible Values
		Numerical values not equal to/above/below: use filter _xy z= @n eq(value), filter _xy z= @above(value), filter _xy z= @below(value)

Parameter	Description	Possible Values
		<p>Partial match substrings: use filter _xy z= @sub(s ubstring 1,substring2)</p> <p>Exact match substrings: use filter _xy z= @xt(s ubstring) or filter _xy z= @nt(xt(s ubstring))</p>

Parameter	Description	Possible Values
		<p> @txt and @nxt require that you enter the entire substring to filter properly. The filters are case sensitive. Use @nxt if you want to define a substring to exclude from the results.</p>

Parameter	Description	Possible Values
sortby	Sort the data. If this parameter is omitted, the table is sorted based on the first column. Add a leading "-" to reverse sort order. (Samples: sortby=name, sortby=lastvalue, sortby=-lastvalue, sortby=uptime)	Any column name used in the columns parameter.   Log tables with content=messages are always sorted by descending date.

 Examples

Here are some samples for filtered API calls:

All sensors that are not in the Up [status](#)<sup>1811</sup> (with their status and downtime information):

```
/api/table.xml?
content=sensors&columns=objid,downtimesince,device,sensor,lastvalue,status,message,
priority
&filter_status=5&filter_status=4&filter_status=10&filter_status=13&filter_status=14
&sortby=priority
```

**Fastest Ping sensors:**

```
/api/table.xml?
content=sensors&columns=objid,sensor,lastvalue,status,message&sortby=lastvalue
&filter_type=ping
```

**Log entries of the last 7 days for object id 2003:**

```
/api/table.xml?content=messages&id=2003&start=0&filter_drel=7days&columns=
objid,datetime,type,name,status,message
```

**Supported Output Columns ("columns=" Parameter)**

You can use the following column names for the `columns` parameter (separated by comma, for example, `columns=objid,name,type`).

Column Name	What It Displays	Can Be Used for
objid	ID of the object	all object tables
type	Object type (group, device, report, etc.), or the sensor type (ping, http, etc.), or event type for tickets (relevant for ToDo tickets)	all object tables
name	Name of the object or channel.  For log messages/tickets: the name of the related object.  For stored reports: the name of the report file.	all object tables  channels  messages  storedreports  toplists  tickets
tags	List of all tags (for tickets: tags for the related object). This includes tags from the object itself plus tags that are inherited from parent objects.	all object tables (except for user)

Column Name	What It Displays	Can Be Used for
active	True/false depending on whether an object is set to paused by a user (for tickets: related object). For notifications that are paused by schedule, it also displays the end of the schedule.	all object tables
downtime	Cumulated downtime of the sensor (displayed as percentage of uptime+downtime)	sensors
downtimetype	Cumulated downtime of the sensor (in minutes/hours)	sensors
downtimesince	Elapsed time since last Up status of the sensor	sensors
uptime	Cumulated uptime of the sensor (displayed as percentage of uptime+downtime)	sensors
uptimetype	Cumulated uptime of the sensor (in minutes/hours)	sensors
uptimesince	Elapsed time since the last Down status of the sensor	sensors
knowntime	Sum of cumulated uptime and downtime of the sensor	sensors
cumsince	Time stamp when accumulation of uptimes/downtimes began	sensors
sensor	Name of the sensor	sensors toplists
interval	Effective interval setting for the sensor	sensors
lastcheck	Time stamp of the last sensor result	sensors
lastup	Time stamp of the most recent Up status of the sensor	sensors

Column Name	What It Displays	Can Be Used for
lastdown	Time stamp of the most recent Down status of the sensor	sensors
device	Name of the associated device	sensors devices
group	Name of the associated group	sensors devices groups
probe	Name of the associated probe	sensors devices groups probes
grpdev	Name of the associated device and the associated group separated by a forward slash (/)	sensors devices
notifiesx	Number of each trigger type defined for the object	probes groups devices sensors
intervalx	Either <a href="#">Inherited</a> or the current interval setting of the object	probes groups devices sensors
accessrights	Access rights of the current user for the sensor tree object	all objects (except for user), for example: probes groups devices sensors
dependency	Name of an associated dependency or <a href="#">Parent</a>	probes

Column Name	What It Displays	Can Be Used for
		groups devices sensors
probegroupdevice	<p>Partial object hierarchy with names of associated device, group, and probe separated by a forward slash (/).</p> <ul style="list-style-type: none"> <li><b>i</b> The output contains HTML.</li> <li><b>i</b> <code>probegroupdevice</code> is not available in the CSV format.</li> <li><b>i</b> For the complete object hierarchy, use <code>probe</code>, <code>group</code>, <code>device</code> instead.</li> </ul>	sensor device group probe
status	<p>For sensor tree objects: status of the object (0=None, 1=Unknown, 2=Scanning, 3=Up, 4=Warning, 5=Down, 6=No Probe, 7=Paused by User, 8=Paused by Dependency, 9=Paused by Schedule, 10=Unusual, 11=Not Licensed, 12=Paused Until, 13=Down Acknowledged, 14=Down Partial)</p> <p>For messages: category of the log message</p> <p>For tickets: status of ticket (open, resolved, closed)</p>	sensors devices groups probes messages tickets
message	Detailed message of the sensor tree object (for example, last error of the sensor) or the history entry, log entry, ticket subject	sensors devices groups probes messages tickets ticketdata history



Column Name	What It Displays	Can Be Used for
priority	Priority setting of the sensor tree object or the priority of the log entry/ticket	sensors devices groups probes messages tickets (not supported: schedule, notification, user)
lastvalue	Last sensor result value or channel values  When used with channels, you must use <code>lastvalue_</code> to automatically display volumes and speed.	sensors channels
upsens	Number of sensors in the Up status   PRTG only counts the sensor itself or sensors below the object in the hierarchy.	all sensors devices groups probes
downsens	Number of sensors in the Down status   PRTG only counts the sensor itself or sensors below the object in the hierarchy.	all sensors devices groups probes
downacksens	Number of sensors in the Down (Acknowledged) status   PRTG only counts the sensor itself or sensors below the object in the hierarchy.	all sensors devices groups probes
partialdownsens	Number of sensors in the Down (Partial) status   PRTG only counts the sensor itself or sensors below the object in the hierarchy.	all sensors devices groups probes

Column Name	What It Displays	Can Be Used for
warnsens	<p>Number of sensors in the Warning status</p> <p><b>i</b> PRTG only counts the sensor itself or sensors below the object in the hierarchy.</p>	<p>all sensors</p> <p>devices</p> <p>groups</p> <p>probes</p>
pausedsens	<p>Number of sensors in the Paused status. This includes all Paused states ('paused by user', 'paused by dependency', 'paused by schedule', etc.).</p>	<p>all sensors</p> <p>devices</p> <p>groups</p> <p>probes</p>
unusualsens	<p>Number of sensors in the Unusual status</p> <p><b>i</b> PRTG only counts the sensor itself or sensors below the object in the hierarchy.</p>	<p>all sensors</p> <p>devices</p> <p>groups</p> <p>probes</p>
undefinedsens	<p>Number of sensors in an undefined status, like None, Unknown, No Probe</p> <p><b>i</b> PRTG only counts the sensor itself or sensors below the object in the hierarchy.</p>	<p>all sensors</p> <p>devices</p> <p>groups</p> <p>probes</p>
totalsens	<p>Number of all sensors</p> <p><b>i</b> PRTG only counts the sensor itself or sensors below the object in the hierarchy.</p>	<p>all sensors</p> <p>devices</p> <p>groups</p> <p>probes</p>
size	<p>Performance impact of the sensor (1=Very Low, 2=Low, 3=Medium, 4=High, 5=Very High)</p>	<p>sensors</p>
value	<p>The channel value or the Toplist value</p>	<p>values</p> <p>topdata</p>

Column Name	What It Displays	Can Be Used for
	Should only be used as <code>value_</code> , because then it is expanded for all visible channels/toplist columns	
coverage	Sensor coverage of the time span in a value table.	values
favorite	An exclamation mark (!) if the sensor tree object is marked as favorite	sensors devices groups probes
user	User responsible for a history entry or the user (or user group) a ticket is assigned to.	history tickets ticketdata
parent	Name of the parent object of the associated object of a log message	messages
datetime	Time stamp or time span of the object (for tickets: last modification)	messages tickets ticketdata values history storedreports topidx
dateonly	Like <code>datetime</code> but only the date part	messages tickets history values
timeonly	Like <code>datetime</code> but only the time part	messages tickets history

Column Name	What It Displays	Can Be Used for
		values
schedule	For sensor tree objects: Name of the associated schedule  For reports: Report generation schedule	probes groups devices sensors reports
period	Period of the report (day, week, etc.)	reports
email	Email address of the report	reports
template	Template used by the report	reports
lastrun	Time stamp of the last generation of a report	reports
nextrun	Time stamp of the next generation of a report	reports
size	Size of a stored report	size of a stored report
minigraph	Numeric data for the minigraphs. Numbers are 5-minute averages for the last 24 hours (must be scaled to the maximum of the series). There are two datasets: " " separates measured value series and error series.	sensors
deviceicon	Device icon	devices
comments	Object comments  For tickets: related object	all objects
host	Hostname or IP address	devices
devices	For probes: probe status (0=Disconnected, 1=Unauthorized, 2=Connected, 3=Banned, 4=Init)	probes groups

Column Name	What It Displays	Can Be Used for
	For groups: auto-discovery status	
basetype	Object type (string)	all tree objects
baselink	URL of the object	all tree objects
icon	URL of the device icon	devices
parentid	ID of the parent object or ID of a ticket	all tree objects tickets
location	Location property (used in Geo Maps)	devices
fold	Subobjects are folded up (true) or down (false)  For tickets: user (or user group) to which a ticket is assigned read it since last change	probes groups tickets
groupnum devicenum	Number of groups or devices in the probe or group	probes groups
tickettype	Type of ticket: user, notification, todo	tickets
modifiedby	User who edited the ticket most recently	tickets ticketdata
actions	Types of all ticket edits	ticketdata
content	Text of the ticket that was added with the last edit	ticketdata
channel	Number of channels with an ID greater than or equal to 0	sensors
_key, _value	Key value pair from the system table	sysinfo (category: system)

Column Name	What It Displays	Can Be Used for
_displayname, _class, _caption	Display name, class, and caption from the system table	sysinfo (category: hardware)
_user, _domain	User and domain pair from the system table	sysinfo (category: loggedonusers)
_displayname, _creationdate, _processid	Display name, creation date, and process id from the system table	sysinfo (category: processes)
_displayname, _state, _startmode	Display name, state, and start mode from the system table	sysinfo (category: services)
_displayname, _version	Display name and version pair from the system table	sysinfo (category: software)

## More

### ■ KNOWLEDGE BASE

Is there a list of log status values for the PRTG API?

- <https://kb.paessler.com/en/topic/76501>

How can I use the PRTG Application Programming Interface (API)?

- <https://kb.paessler.com/en/topic/593>

### 14.2.2.4 System Information

You can access live data and live status data for system information using the PRTG API.

- ❗ Authentication with API key or user name and [passhash](#)<sup>[2803]</sup> (or user name and password) must always be included in each PRTG API request. See section [HTTP API](#)<sup>[8086]</sup> for more information.

To retrieve system information using API calls, we recommend that you use the following order:

1. Refresh the system information so that it is up to date, if necessary.  
For details, see [Scan Now](#)<sup>[3121]</sup>.
2. Retrieve generic system information to make sure that the last scan (step 1) was successful and that there are no errors.  
For details, see [Generic Data](#)<sup>[3121]</sup>.
3. Retrieve system information in the form of data tables.  
For details, see [Data Tables](#)<sup>[3122]</sup>.

- ❗ System information API calls only support the JavaScript Object Notation (JSON) output.

## Scan Now

The following API calls to retrieve new information for a [system information](#) <sup>[205]</sup> category. To refresh system information via the API, you need to provide

- the ID of a device (parameter `id`), and
- a `kind` ([system information category](#) <sup>[3127]</sup>).

**i** We recommend that you only refresh system information if absolutely necessary because the refresh triggers a rescan of all system information tables.

**Examples**

Refresh process information

```
/api/sysinfochecknow.json?id=deviceid&kind=processes
```

Refresh hardware information

```
/api/sysinfochecknow.json?id=deviceid&kind=hardware
```

**i** `sysinfochecknow` only supports JSON output.


## Supported Output Columns ("kind=" Parameter)

Column Name	Category (as displayed in the PRTG web interface)
system	System
hardware	Hardware
processes	Processes
services	Services
software	Software
loggedonusers	Users

## Generic Data

The following API calls retrieve generic data about the system information category since the last scan, for example time stamps and if the last scan was successful. To retrieve this information via the PRTG API, you need to provide

- the ID of a device (parameter `id`), and
- a `kind` (system information category).


 Examples

**Users**

```
/api/sysinfo.json?id=deviceid&kind=loggedonusers
```

**Services**


```
/api/sysinfo.json?id=deviceid&kind=services
```

 **sysinfo** only supports JSON output.

## Data Tables

The following API calls retrieve all information from a system information category table. To retrieve this information via the PRTG API, you need to provide

- the content type (always **sysinfo**),
- the category (as displayed in the PRTG web interface),
- columns (see [Supported Output Columns \("columns=" Parameter\)](#)<sup>B122</sup>), and
- the ID of a device (parameter id).

 Examples

**System**

```
/api/table.json?
id=deviceid&content=sysinfo&category=system&usecaption=true&headers=key,value&columns=_key,_value
```

**Software**

```
/api/table.json?
id=deviceid&content=sysinfo&category=software&usecaption=true&headers=key,value&columns=_displayname,_version
```

 Data tables for system information only support JSON output.

## Supported Output Columns ("columns=" Parameter)

You can use the following sysinfo-specific column names for the **columns** parameter (separated by comma, for example, **columns=\_key,\_value**).

- For a list of all supported column names, see section [Multiple Object Property or Status](#)<sup>B111</sup>.



Column Name	Description	Can Be Used for
_key, _value	Key value pair from the system table	sysinfo (category: system)
_displayname, _class, _caption	Display name, class, and caption from the system table	sysinfo (category: hardware)
_user, _domain	User and domain pair from the system table	sysinfo (category: loggedonusers)
_displayname, _creationdate, _processid	Display name, creation date, and process id from the system table	sysinfo (category: processes)
_displayname, _state, _startmode	Display name, state, and start mode from the system table	sysinfo (category: services)
_displayname, _version	Display name and version pair from the system table	sysinfo (category: software)

## More

### ■ KNOWLEDGE BASE

How can I use the PRTG Application Programming Interface (API)?

- <https://kb.paessler.com/en/topic/593>

### 14.2.3 Live Graphs

You can use live sensor graphs from PRTG in other web pages using the PRTG API. PRTG renders graphs as .png or .svg files. You can include them in other web pages.

**i** Authentication with API key or user name and [passhash](#) (or user name and password) must always be included in each PRTG API request. See section [HTTP API](#) for more information.

**Examples**

Live graph as a .png file:

```
/chart.png?type=graph&width=300&height=160&graphid=2&id=0
```

Live graph as an .svg file:

```
/chart.svg?type=graph&width=300&height=160&graphid=2&id=0
```

**i** To switch between PNG and SVG images, change the file extension of `/chart` to `.png` or `.svg`.

**i** The URL does not start with `/api`. When placing these URLs on web pages, keep in mind that the URLs contain the account user name and password/passhash. This can imply security issues. We recommend that you set up a dedicated [read-only](#) user account in PRTG that is member of a dedicated user group, for example, that only has read access to the root group and all underlying entries or, even better, only for the object IDs that are used for graph URLs.

#### Parameters for Live Graph URLs (chart.png or chart.svg)

Parameter	Description
type	Must be <a href="#">graph</a>
graphid	Select time span of the graph: <ul style="list-style-type: none"> <li>▪ 0=live</li> <li>▪ 1=last 48 hours</li> <li>▪ 2=30 days</li> <li>▪ 3=365 days</li> </ul>
width	Width of the image in pixels
height	Height of the image in pixels
id	The object ID of the desired graph object. This is usually the ID of a sensor.
clgid	The NodeID of the cluster node of the desired graph object

Parameter	Description
	<p><b>i</b> Use the format <code>clgid=%7BXXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX%7D</code>. You can also use <code>clgid=%7B00000000-0000-0000-0000-000000000000%7D</code> to return a graph that has data from all cluster nodes.</p>
graphstyling	<p>Allow control of some graph styles:</p> <ul style="list-style-type: none"> <li>▪ Display legend: <code>graphstyling=showLegend%3D%271%27</code></li> <li>▪ Hide legend: <code>graphstyling=showLegend%3D%270%27</code></li> <li>▪ Control font size: <code>graphstyling=baseFontSize%3D%27XX%27</code> (XX is the font size)</li> <li>▪ Control legend and font size at the same time: <code>graphstyling=showLegend%3D%271%27+baseFontSize%3D%275%27</code></li> </ul>
bgcolor	<p>Background color of the PNG image, for example, #ffff. This affects the area that surrounds the graph.</p> <p><b>i</b> The value must be URL encoded, for example, %23ffff.</p>
plotcolor	<p>Color of the graph's plot area, for example, #ffff. This affects the whole area within the graph box.</p> <p><b>i</b> The value must be URL encoded, for example, %23ffff.</p>
plotcolor1	<p>Alternating color of the graph's plot area, for example, #ffff. This affects the tiles within the graph box alternating with <code>plotcolor2</code>. The result is a striped graph box.</p> <p><b>i</b> The value must be URL encoded, for example, %23ffff.</p> <p><b>i</b> This parameter is overwritten when using the parameter <code>plotcolor</code>.</p>
plotcolor2	<p>Alternating color of the graph's plot area, for example, #ffff. This affects the tiles within the graph box alternating with <code>plotcolor1</code>. The result is a striped graph box.</p> <p><b>i</b> The value must be URL encoded, for example, %23ffff.</p> <p><b>i</b> This parameter is overwritten when using the parameter <code>plotcolor</code>.</p>
gridcolor	<p>Color of grid lines in the graph's plot area, for example, #ffff. This affects the horizontal and vertical lines within the graph box.</p> <p><b>i</b> The value must be URL encoded, for example, %23ffff.</p>

Parameter	Description
hide	Do not show defined channels in the graph. Use the ID of a channel to hide it. For example, use <code>hide=-4</code> to not show the Downtime channel in the graph. To hide more than one channel, use commas to separate the IDs.

## Retrieving Chart Legends (JSON)

You can show the legend of a sensor graph (channel IDs, colors, units, channel names) in the JavaScript Object Notation (JSON) format.

 Example

Chart legend in the JSON format:

```
/api/chartlegend.json?id=sensorid
```

## More

### KNOWLEDGE BASE

How can I use the PRTG Application Programming Interface (API)?

- <https://kb.paessler.com/en/topic/593>

## 14.2.4 Historic Data

You can download the historic monitoring data for one sensor in the Extensible Markup Language (XML) format or the comma-separated values (CSV) format using the following API calls. You can either request the results of each single monitoring request (called raw data) or you can let PRTG calculate averages of the data (for example, hourly or daily averages).

To avoid potential server overload, the number of requestable values per API call is limited by means of automatic averaging as follows:

Minimum Level of Detail (Average Interval)	Maximum Timeframe per API Call
Raw data (all single monitoring requests)	For up to 40 days per API request
60 minutes/1 hour averages	40 to 500 days per API request ⓘ If you try to use a larger time span than 500 days, PRTG automatically reduces it to 365 days.

ⓘ API calls for historic data are limited to 5 requests per minute.

### API Calls for Historic Data

ⓘ Authentication with API key or user name and [passhash](#) (or user name and password) must always be included in each PRTG API request. See section [HTTP API](#) for more information.

The API calls for historic data tables look like this:

**Examples**

**XML:**

```
/api/historicdata.xml?id=objectid&avg=0&sdate=2023-01-20-00-00-00&edate=2023-01-21-00-00-00
```

**CSV:**

```
/api/historicdata.csv?id=objectid&avg=0&sdate=2023-01-20-00-00-00&edate=2023-01-21-00-00-00
```

**JavaScript Object Notation (JSON):**

```
/api/historicdata.json?id=objectid&avg=0&sdate=2023-01-20-00-00-00&edate=2023-01-21-00-00-00&usecaption=1
```

ⓘ You must supply the object ID of a sensor as well as a start date/time [sdate](#) and end date/time [edate](#).

**i** If you use the JSON call, additionally provide the parameter `usecaption=1` to get more information than just the raw data table.

## API Call for Historic Graphs

Historic graphs are also available (in the PNG format):

**Example**

**PNG:**

```
/chart.png?id=objectid&avg=15&sdate=2023-01-20-00-00-00&edate=2023-01-21-00-00-00&width=850&height=270&graphstyling=baseFontSize='12'%20showLegend='1'&graphid=-1
```

## Common Parameters for Historic Data API Calls

You can use the following parameters for the graphs and the data tables:

Parameter	Description	Possible Values
id	ID of the specific sensor	integer
sdate	Start of the time span (date and time)	yyyy-mm-dd-hh-mm-ss
edate	End of the time span (date and time)	yyyy-mm-dd-hh-mm-ss
avg	Average interval in seconds; use 0 to download raw data (= results of all single monitoring requests)	integer
width/height	Width and height of the graph in pixels	integer
graphstyling	baseFontSize='x' sets the size of the font showLegend='x' enables (1) or disables (0) the graph legend	baseFontSize='x'%20showLegend='x'

## Historic Data Query Builder

You can also use the [historic data reports](#) <sup>185</sup> to manually generate and analyze historic sensor data via the PRTG web interface.

## More

**KNOWLEDGE BASE**

How can I export historic data from the PRTG API?

- <https://kb.paessler.com/en/topic/76768>

How can I export raw sensor data automatically from PRTG?

- <https://kb.paessler.com/en/topic/343>

## 14.2.5 Object Manipulation

You can use the following functions to manipulate objects (URLs are shown without user name or passhash to enhance readability).

In this section:

- [Changing Object Settings](#) <sup>[3130]</sup>
- [Supported Object Types for rename.htm](#) <sup>[3131]</sup>
- [Switch Inheritance Off/On](#) <sup>[3131]</sup>
- [Changing Properties of Channels](#) <sup>[3131]</sup>
- [Pausing/Resuming](#) <sup>[3132]</sup>
- [Supported Object Types for pause.htm](#) <sup>[3132]</sup>
- [Error Handling](#) <sup>[3133]</sup>
- [Rescanning, Triggering Auto-Discovery](#) <sup>[3133]</sup>
- [Reordering Objects in the Sensor Tree](#) <sup>[3133]</sup>
- [Report-related](#) <sup>[3133]</sup>
- [Notification-related](#) <sup>[3134]</sup>
- [Adding/Deleting Objects](#) <sup>[3134]</sup>
- [Supported Object Types for duplicateobject.htm](#) <sup>[3134]</sup>
- [Duplicating Sensors and Changing Clone Settings](#) <sup>[3135]</sup>
- [Setting Geo Location](#) <sup>[3136]</sup>

### Changing Object Settings

**i** Authentication with API key or user name and [passhash](#) <sup>[2803]</sup> (or user name and password) must always be included in each PRTG API request. See section [HTTP API](#) <sup>[3086]</sup> for more information.

#### Examples

Rename an object:

```
/api/rename.htm?id=objectid&value=newname
```

Set priority of an object (valid values for x are 1 to 5):

```
/api/setpriority.htm?id=objectid&prio=x
```

Change properties of objects:

```
/api/setobjectproperty.htm?id=id_of_object&name=property_name&value=new_value
```

**i** This function can change most string and number properties of objects (names, numeric values, object identifiers (OID), etc.). Use it with caution. You can discern the [property\\_name](#) parameter by opening the Settings page of an object and looking at the HTML source of the INPUT fields. For example, the INPUT field for the tags of an object has the name `tags_`. Leave away the underscore `_` and use `tags` as a value for the [property\\_name](#) parameter.



## Supported Object Types for rename.htm

[rename.htm](#) supports the following object types:

- group
- device
- sensor
- map
- report
- library
- notification template
- schedule
- user
- user group

[rename.htm](#) does not support other object types.


## Switch Inheritance Off/On

This API call sets the [inherit](#) setting of objects (location, credentials, compatibility options, proxy settings, scanning interval, access rights, channel unit). In general, this works like changing properties for any other object.

### Example

Replace the parameter [inheritType](#) with the name of the inheritance type:

```
/api/setobjectproperty.htm?id=id_of_object&name=inheritType_&value=0_or_1
```

 This internal name must be followed by an underscore (`_`), in contrast to changing properties above. Use the value `0` for switching off inheritance, and `1` for switching on inheritance. For example, the inheritance type for the scanning interval setting has the name `intervalgroup_`. Thus, this specific part in the URL is `&name=intervalgroup_&value=0` (switches off inheritance for scanning interval).

 This call does not work with the Schedules, Dependencies, and Maintenance Window settings.

## Changing Properties of Channels

With this API call, you can change a sensor's [channel settings](#)<sup>2681</sup>. In general, this works like changing properties of any other object. To set channel properties via the PRTG API, you need to provide

- the ID of a sensor (parameter `id`),
- a `subtype` (channel for channels), and
- a `subid` (ID of the channel that you want to edit).

**Example: Enabling and Setting Limits for Channels**

Set limits for channels:

```
/api/setobjectproperty.htm?
id=sensorid&subtype=channel&subid=0&name=limitmaxerror&value=limitvalue
```

**i** You must set the limits for a channel before you can enable limits.

Enable limits for channels:

```
/api/setobjectproperty.htm?
id=sensorid&subtype=channel&subid=0&name=limitmode&value=1
```

For example, the following API call sets the upper error limit of a channel with the ID 0 of a sensor with the ID 2970 to the value 25.

```
/api/setobjectproperty.htm?
id=2970&subtype=channel&subid=0&name=limitmaxerror&value=25
```

**i** For Toplists, you can use the subtype **toplist** to change the properties. When using this subtype, **subid** is the ID of a Toplist.

■ For a list of available channel parameters, see section [Single Object Property](#)<sup>3091</sup>.

## Pausing/Resuming

**Examples**

Pause a sensor or object indefinitely:

```
/api/pause.htm?id=objectid&pausemsg=yourmessage&action=0
```

Pause a sensor or object for x minutes:

```
/api/pauseobjectfor.htm?id=objectid&pausemsg=yourmessage&duration=x
```

**i** The pause message is optional. You can leave out the parameter **&pausemsg=yourmessage** if you do not want to display a message.

Simulate an error for a sensor:

```
/api/simulate.htm?id=objectid&action=1
```

**i** **simulate.htm** only works for sensors in the Up, Warning, Unusual, or Unknown [status](#)<sup>181</sup>.

Resume monitoring of a sensor or object:

```
/api/pause.htm?id=objectid&action=1
```

## Supported Object Types for pause.htm

**pause.htm** supports the following object types:

- probe
- group

- device
- sensor
- notification
- user account

[pause.htm](#) does not support other object types.

## Error Handling (Acknowledge Alarm)

### Example

Acknowledge the Down status:

```
/api/acknowledgealarm.htm?id=objectId&ackmsg=yourmessage
```

## Rescanning, Triggering Auto-Discovery

### Examples

Scan a sensor now:

```
/api/scannow.htm?id=objectId
```

Run an auto-discovery for a group or device:

```
/api/discovernow.htm?id=objectId&template=filename
```

**i** Providing a [device template](#) 27251 for auto-discovery is optional. You can leave out the parameter `&template=filename` to run the auto-discovery with the options defined in the object's settings. If you use a template, provide the whole file name including file extension surrounded by double quotation marks (") and encode whitespaces, if necessary. Example: `&template="Linux%20SNMP.odt"`

**i** [discovernow.htm](#) overrides the Auto-Discovery setting of the target group or device. If it is set to No auto-discovery, it automatically changes to Standard auto-discovery (default).

## Reordering Objects in the Sensor Tree

### Example

Move an object in the sensor tree (x can be [up](#), [down](#), [top](#), [bottom](#)):

```
/api/setposition.htm?id=objectId&newpos=x
```

## Report-related

### Example

Add a group, device, or sensor to a report:

```
/api/reportaddsensor.htm?id=reportid&addid=objectid
```


## Notification-related

 Example

Trigger a notification immediately for testing purposes:

```
/api/notificationtest.htm?id=objectid
```

```
/api/notificationtest.json?id=objectid
```


 **objectid** is the ID of the notification template.

## Adding/Deleting Objects

Adding and deleting objects in your configuration is the most complex and potentially most critical process when using the PRTG API. Keep in mind that adding or deleting objects is much better guided in the normal PRTG web interface with more warnings and alerts.

 We recommend that you use the PRTG web interface for adding and deleting objects, if possible.

### Deleting Objects

 API calls to the delete function immediately delete the referenced object including all subobjects, if there are any. For example, deleting a group deletes all its devices and sensors. There is no way to undo a deletion, so use this function with care.

 Example

Delete an object:

```
/api/deleteobject.htm?id=objectid&approve=1
```

### Adding Objects

Adding completely new objects from scratch is not supported via the PRTG API because of the complexity of object creation and its parameters. To add new objects to PRTG, create a "master" object that is cloned into new objects.

## Supported Object Types for `duplicateobject.htm`

`duplicateobject.htm` supports the following object types:

- group
- device
- sensor

- report
- library
- map
- notification template

[duplicateobject.htm](#) does not support other object types.

 Examples

Duplicate a group:

```
/api/duplicateobject.htm?
id=id_of_group_to_clone&name=new_name&targetid=id_of_target_group
```

Duplicate a device:

```
/api/duplicateobject.htm?
id=id_of_device_to_clone&name=new_name&host=new_hostname_or_ip&targetid=id_of_target_group
```

Duplicate a sensor:




```
/api/duplicateobject.htm?
id=id_of_sensor_to_clone&name=new_name&targetid=id_of_target_device
```

Duplicate a library:

```
/api/duplicateobject.htm?id=id_of_library_to_clone&name=new_name
```

Duplicate a notification template:

```
/api/duplicateobject.htm?id=id_of_notification_template_to_clone&name=new_name
```

-  If [duplicateobject](#) succeeds, the PRTG core server replies with a redirect to the URL of the new object (for example, [/sensor.htm?id=1234](#)), so your application should parse the new object ID from this URL.
-  When a group, device, or sensor is cloned, it is initially set to Paused so you have the chance to edit parameters as desired. You must resume it with an API call afterward.
-  The API calls for duplicating reports, maps, libraries, and notification templates do not require a [targetid](#).

## Duplicating Sensors and Changing Clone Settings

The following process duplicates a sensor, changes some settings, and then starts monitoring:

 Example

Duplicate the sensor (the server replies with a redirect to the new object's web page, for example [/sensor.htm?id=10214](#), parse id [10214](#) from the URL):

```
/api/duplicateobject.htm?id=2002&name=mynewsensor&targetid=2001
```

Rename the new sensor:

```
/api/setobjectproperty.htm?id=10214&name=name&value=newname
```

Change the OID (in this example for an [SNMP Custom](#) sensor):

```
/api/setobjectproperty.htm?id=10214&name=oid&value=1.2.3.4.5.6.7
```

Resume monitoring for the new sensor:

```
/api/pause.htm?id=10214&action=1
```

## Setting Geo Location

You can set the location of any object via an API call. Provide the object ID together with parameters for location and/or longitude and latitude.

If only the location parameter is specified, the PRTG core server executes the geo location lookup (this can take up to three minutes). Provide the name of the location, for example, [New York](#). It is shown in the Location settings, no matter the longitude or latitude.

If the longitude and latitude parameter is specified, the marker in the map is set to this position, no matter of the location parameter. Provide longitude and latitude separated by a comma, for example - [73.998672,40.714728](#).

### Example

Set the geo location of an object:

```
/api/setlonlat.htm?  
id=objectid&location=name_of_object_location&lonlat=longitude,latitude
```

## More

### KNOWLEDGE BASE

How can I use the PRTG Application Programming Interface (API)?

- <https://kb.paessler.com/en/topic/593>

## 14.2.6 Custom Sensors

Custom sensors can perform a number of monitoring tasks that extend the standard sensor set. Apart from parameterized versions of Simple Network Management Protocol (SNMP), Packet Sniffer, and NetFlow sensors, you can create your own sensors using Windows Management Instrumentation Query Language (WQL) or Python, by compiling an .exe file, using any Windows software development tool, and you can request any Representational State Transfer (REST) application programming interface (API) that returns JavaScript Object Notation (JSON) or Extensible Markup Language (XML) and map the results to channels.

**i** The multi-platform probe currently does not support all custom sensor types. For more information, see the Knowledge Base: [What is the multi-platform probe and how can I use it?](#)

The following documentation describes the custom [EXE/Script](#)<sup>[3137]</sup>, [Python Script](#), and [SSH Script](#) sensors. The defined XML and JSON formats for the advanced sensors are also used for advanced HTTP data sensors and the [REST Custom](#) sensor.

**■** For more information about custom sensors based on SNMP, Windows Management Instrumentation (WMI), Packet Sniffing, and Flow (NetFlow, jFlow, sFlow, IPFIX), see the respective [custom sensors](#)<sup>[2676]</sup>.

**i** For each sensor interval, PRTG can run an external process. The process can be a Windows .exe file, or a .bat, .cmd, .vbs, or PowerShell file, as well as a Python or Secure Shell (SSH) script.

In this section:

- [Standard and Advanced EXE/Script Sensor](#)<sup>[3137]</sup>
- [Standard and Advanced SSH Script Sensor](#)<sup>[3138]</sup>
- [Interface Definition for EXE/BAT/CMD/VBS/PowerShell/SSH Sensors](#)<sup>[3138]</sup>
- [Return Values for EXE/BAT/CMD/VBS/PowerShell/SSH Sensors](#)<sup>[3139]</sup>
- [Standard EXE/Script Sensor](#)<sup>[3139]</sup>
- [SSH Script Sensor](#)<sup>[3140]</sup>
- [Advanced Script, HTTP Data, and REST Custom Sensors](#)<sup>[3140]</sup>
- [Advanced Script, HTTP Data, and REST Custom Sensors: Elements](#)<sup>[3142]</sup>
- [Command-line Parameters](#)<sup>[3148]</sup>
- [Environment Values](#)<sup>[3150]</sup>

### Standard and Advanced EXE/Script Sensor

**i** You must create the sensor as a file and store it in a specific subfolder on the probe system. In a cluster, you must store it on each cluster node.

Place executables (.exe), batch files (.cmd, .bat), VBS scripts (.vbs), or PowerShell scripts (.ps1) into a subfolder of the [PRTG program directory](#)<sup>[3213]</sup>. For the standard [EXE/Script](#) sensor, this is the following subfolder of the PRTG program directory:

```
Custom Sensors\EXE
```

If your executable or script returns XML or JSON, you use it with the [EXE/Script Advanced](#) sensor. In this case, store your file in the following subfolder of the PRTG program directory:

```
Custom Sensors\EXEXML
```

You find a sample set of demo sensors in these subfolders, too. As soon as a file is placed into the subfolders mentioned above, you can create your own custom EXE sensor and select the new file from the list of files.

The probe then executes the file on the probe system using the account configured for the PRTG probe service (the default is [system](#)). The local probe runs the file on the local PRTG core server system. For remote probes, the file actually runs on the remote probe system.

**i** If you use a PowerShell script (.ps1) and if the PowerShell Security Enhancement [experimental feature](#)<sup>[2876]</sup> is enabled, scripts that use the [write-host](#) cmdlet to provide their output to PRTG do not work. Use the [write-output](#) cmdlet instead.

**i** We recommend that you not edit the demo files. Create your own new files and make sure to give them unique names that do not start with [Demo](#), for example.

**i** If your custom sensor code relies on other files (for example, .NET framework, Windows PowerShell) you must manually copy or install these files on the probe system.

**i** EXE sensors fail if they attempt to open any graphical user interface windows using the Win32 APIs. This is not allowed for processes that are started by a system service.

## Standard and Advanced SSH Script Sensor

**i** You must create the sensor as an SSH script and place it in a specific directory on the target system running your Linux/Unix installation where the script is executed.

Place your SSH script files for the standard [SSH Script](#) sensor in the following directory of the target system:

```
/var/prtg/scripts
```

If your SSH script returns XML or JSON, you use it with the [SSH Script Advanced](#) sensor. In this case, store your file in the following directory of the target system:

```
/var/prtg/scriptsxml
```

As soon as a file is placed into the respective directory, you can create your own SSH script sensor and select the new script file from the list of scripts.

**i** With each scanning interval, PRTG executes the script on the target system and receives the result as a sensor result.

## Interface Definition for EXE/BAT/CMD/VBS/PowerShell/SSH Sensors

Every time the sensor is run, the selected file is executed. The string entered in the Parameters field of the sensor's settings is used as command line (you can use placeholders, see [Command-line Parameters](#)<sup>[3148]</sup>). The executable file must send the results to the Standard OUT. For the format of returned data, see below.



**i** If the executable file does not return control to the PRTG process, it is killed as soon as the timeout value set for this sensor is reached.

You can test the .exe file that you want to use for the sensor via the command line (cmd.exe). To do so, start the .exe file and pipe the results into a file.

**Example**

```
sensorexex parameter > result.txt
```

The results are written into the file [result.txt](#) and you can check the results with notepad or any other text editor.

#### Remarks

- For PowerShell scripts, make sure that they are executed by either signing the files or changing the security policy for Powershell.exe accordingly.
- In SSH scripts, you can use alphanumeric characters and the special characters ".", "\_", "-", "=", and "/" outside of quoted strings in the Parameters field of the sensor's settings.
- The API interface for custom EXE sensors is compatible with the custom EXE sensors provided by PRTG.

#### Return Values for EXE/BAT/CMD/VBS/PowerShell/SSH Sensors

The expected return values are different, depending on the type of EXE/Script sensor used. The standard sensor needs a simple [value:message](#) pair. The EXE/Script Advanced sensor processes an XML or JSON return value. When using the standard SSH Script sensor, it expects [returncode:value:message](#) as result. See details below.

#### Standard EXE/Script Sensor

The returned data for standard EXE/Script sensors must be in the following format:

```
value:message
```

**i** Value has to be a 64-bit integer or float. It is used as the resulting value for this sensor (for example, bytes, milliseconds) and stored in the database. The message can be any string (maximum length: [2000](#) characters).

The exit code of the executable file has to be one of the following values:

Value	Description
0	OK
1	WARNING

Value	Description
2	System Error (for example, a network/socket error)
3	Protocol Error (for example, web server returns a 404)
4	Content Error (for example, a web page does not contain a required word)

## SSH Script Sensor

The returned data for standard SSH Script sensors must be in the following format:

```
returncode:value:message
```

**i** Value has to be a 64-bit integer or float. It is used as the resulting value for this sensor (for example, bytes, milliseconds) and stored in the database. The message can be any string (maximum length: 2000 characters).

The SSH script `returncode` has to be one of the following values:

Value	Description
0	OK
1	WARNING
2	System Error (for example, a network/socket error)
3	Protocol Error (for example, web server returns a 404)
4	Content Error (for example, a web page does not contain a required word)

## Advanced Script, HTTP Data, and REST Custom Sensors

The returned data for the [EXE/Script Advanced](#), [Python Script Advanced](#), [SSH Script Advanced](#), [HTTP Push Data Advanced](#), [HTTP Data Advanced](#), and [HTTP IoT Push Data Advanced](#) sensors must be in XML or JSON format, the REST configuration file for the [REST Custom](#) sensor must be available as JSON template.

Most parameters have a default value and are not required. The following minimum examples leave most parameters to their default values and return two static channel values.

 Examples

**XML Return Format: Minimum Example:**

```
<prtg>
  <result>
    <channel>First channel</channel>
    <value>10</value>
  </result>
  <result>
    <channel>Second channel</channel>
    <value>20</value>
  </result>
</prtg>
```

**To return an error, the XML format is:**

```
<prtg>
  <error>1</error>
  <text>Your error message</text>
</prtg>
```

**JSON Return Format: Minimum Example**

```
{
  "prtg": {
    "result": [
      {
        "channel": "First channel",
        "value": 10
      },
      {
        "channel": "Second channel",
        "value": 20
      }
    ]
  }
}
```

**To return an error, the JSON format is:**

```
{
  "prtg": {
    "error": 1,
    "text": "Your error message"
  }
}
```

**i** You can find a more detailed demo script for the EXE/Script Advanced sensor in the \Custom Sensors\EXEXML subfolder of the [PRTG program directory](#) [3213]. You find demo files for other sensors in the \Custom Sensors folder as well.

## Advanced Script, HTTP Data, and REST Custom Sensors: Elements

You can optionally define the encoding of your .xml file at the beginning of the document. For example, to define UTF-8, you would use:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

You can use the following elements in the section between `<result>` and `</result>`. In each section, you can return one channel. You can define a maximum of 50 channels.

**i** If you exceed this limit, PRTG tries to display all channels. However, be aware that this is an unsupported procedure and you experience limited usability and performance.

**i** For XML output, the tag names are not case-sensitive. For example, you can use both "VALUE" and "value". For JSON output, the tag names are case-sensitive but you can also use lowercase. For example, you can use both "CustomUnit" and "customunit".

Tag	Mandatory	Description	Possible Content
<code>&lt;Channel&gt;</code>	Yes	Name of the channel as displayed in user interfaces. <b>i</b> This parameter is required and must be unique for the sensor.	Any string
<code>&lt;Value&gt;</code>	Yes	The value as integer or float. <b>i</b> Make sure the <code>&lt;Float&gt;</code> setting matches the kind of value provided. Otherwise PRTG shows 0 values.	Integer or float value
<code>&lt;Unit&gt;</code>	No	The unit of the value. The default is <a href="#">Custom</a> . This is useful for PRTG to convert volumes and times.	BytesBandwidth BytesDisk Temperature Percent TimeResponse TimeSeconds Custom Count

Tag	Mandatory	Description	Possible Content
			<p>CPU: This is a % unit that is accounted to the CPU load in index graphs.</p> <p>BytesFile</p> <p>SpeedDisk</p> <p>SpeedNet</p> <p>TimeHours</p>
<CustomUnit>	No	If Custom is used as unit, this is the text displayed behind the value.	Any string (keep it short)
<SpeedSize> <VolumeSize>	No	<p>Size used for the display value. For example, if you have a value of 50000 and use Kilo as size, the display is 50 kilo #.</p> <p>The default is <b>One</b> (value used as returned). For the Bytes and Speed units, this is overridden by the setting in the user interface.</p>	<p>One</p> <p>Kilo</p> <p>Mega</p> <p>Giga</p> <p>Tera</p> <p>Byte</p> <p>KiloByte</p> <p>MegaByte</p> <p>GigaByte</p> <p>TeraByte</p> <p>Bit</p> <p>KiloBit</p> <p>MegaBit</p> <p>GigaBit</p> <p>TeraBit</p>
<SpeedTime>	No	See above, used when displaying the speed. The default is <b>Second</b> .	<p>Second</p> <p>Minute</p> <p>Hour</p> <p>Day</p>
<Mode>	No	Select if the value is an absolute value or counter. The default is <b>Absolute</b> .	Absolute

Tag	Mandatory	Description	Possible Content
			Difference
<Float>	No	<p>Define if the value is a float. The default is 0 (no). If set to 1 (yes), use a dot as decimal separator in values.</p> <p><b>i</b> Define decimal places with the &lt;DecimalMode&gt; element.</p>	<p>0 (= no, integer)</p> <p>1 (= yes, float)</p>
<DecimalMode>	No	<p>Init value for the Decimal Places option. If 0 is used in the &lt;Float&gt; element (use integer), the default is <b>Auto</b>. Otherwise (for float) the default is <b>All</b>.</p> <p><b>i</b> You can change this initial setting later in the sensor's <a href="#">channel settings</a> <sup>[268]</sup>.</p>	<p>Auto</p> <p>All</p>
<Warning>	No	<p>If enabled for at least one channel, the entire sensor is set to the Warning status. The default is 0 (no).</p>	<p>0 (= no)</p> <p>1 (= yes)</p>
<ShowChart>	No	<p>Init value for the Show in graphs option. The default is 1 (yes).</p> <p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and can be omitted). You can change this initial setting later in the sensor's channel settings.</p>	<p>0 (= no)</p> <p>1 (= yes)</p>
<ShowTable>	No	<p>Init value for the Show in tables option. The default is 1 (yes).</p> <p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and can be omitted). You can change this initial setting later in the sensor's channel settings.</p>	<p>0 (= no)</p> <p>1 (= yes)</p>

Tag	Mandatory	Description	Possible Content
<LimitMaxError>	No	<p>Define an upper error limit for the channel. If enabled, the sensor is set to the Down status if this value is exceeded and the LimitMode is activated.</p> <p><b>i</b> Provide the value for the limit in the unit of the base data type as it is used in the &lt;Value&gt; element of this section. When a sensor shows the Down status triggered by a limit, it still receives data in its channels.</p> <p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and can be omitted). You can change this initial setting later in the sensor's channel settings.</p>	String with numbers
<LimitMaxWarning>	No	<p>Define an upper warning limit for the channel. If enabled, the sensor is set to the Warning status if this value is exceeded and the LimitMode is activated.</p> <p><b>i</b> Provide the value for the limit in the unit of the base data type as it is used in the &lt;Value&gt; element of this section. When a sensor shows the Down status triggered by a limit, it still receives data in its channels.</p> <p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and can be omitted). You can change this initial setting later in the sensor's channel settings.</p>	String with numbers
<LimitMinWarning>	No	<p>Define a lower warning limit for the channel. If enabled, the sensor is set to the Warning status if this value falls below the defined limit and the LimitMode is activated.</p>	String with numbers

Tag	Mandatory	Description	Possible Content
		<p><b>i</b> Provide the value for the limit in the unit of the base data type as it is used in the &lt;Value&gt; element of this section. When a sensor shows the Down status triggered by a limit, it still receives data in its channels.</p> <p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and can be omitted). You can change this initial setting later in the sensor's channel settings.</p>	
<LimitMinError>	No	<p>Define a lower error limit for the channel. If enabled, the sensor is set to the Down status if this value falls below the defined limit and the LimitMode is activated.</p> <p><b>i</b> Provide the value for the limit in the unit of the base data type as it is used in the &lt;Value&gt; element of this section. When a sensor shows the Down status triggered by a limit, it still receives data in its channels.</p> <p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and can be omitted). You can change this initial setting later in the sensor's channel settings.</p>	String with numbers
<LimitErrorMsg>	No	<p>Define an additional message. It is added to the sensor's message when entering the Down status that is triggered by a limit.</p> <p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and can be omitted). You can change this initial setting later in the sensor's channel settings.</p>	Any string



Tag	Mandatory	Description	Possible Content
<LimitWarningMessage>	No	<p>Define an additional message. It is added to the sensor's message when entering the Warning status that is triggered by a limit.</p> <p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and can be omitted). You can change this initial setting later in the sensor's channel settings.</p>	Any string
<LimitMode>	No	<p>Define if the limit settings defined above are active. The default is 0 (no; limits inactive). If 0 is used, the limits are written to the channel settings as predefined values, but limits are disabled.</p> <p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and can be omitted). You can change this initial setting later in the sensor's channel settings.</p>	0 (= no) 1 (= yes)
<ValueLookup>	No	<p>Define if you want to use a lookup file (for example, to view integers as status texts). Enter the ID of the lookup file that you want to use, or omit this element to not use lookups.</p> <p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and can be omitted). You can change this initial setting later in the sensor's channel settings.</p>	Any string
<NotifyChanged>	No	<p>If a returned channel contains this tag, it triggers a change notification that you can use with the <a href="#">change trigger</a> to send a notification.</p>	No content required

You can use the following elements in the section between `<prtg>` and `</prtg>`, outside the `<result>` section.

**i** For XML output, the tag names are not case-sensitive. For example, you can use both "TEXT" and "text". For JSON output, the tag names are case-sensitive but you can also use lowercase. For example, you can use both "Text" and "text".

Tag	Mandatory	Description	Possible Content
<code>&lt;Text&gt;</code>	No	Text the sensor returns in the Message field with every scanning interval. There can be one message per sensor, regardless of the number of channels. The default message is <b>OK</b> .  <b>i</b> This element has to be provided outside of the <code>&lt;result&gt;</code> element.	Any string  Maximum length: 2000 characters  <b>i</b> PRTG does not support the number sign (#) in sensor messages. If a message contains a number sign, PRTG clips the message at this point.
<code>&lt;Error&gt;</code>	No	If enabled, the sensor returns the Down status. This element can be combined with the <code>&lt;Text&gt;</code> element to show an error message. The default is <b>0</b> .  <b>i</b> This element has to be provided outside of the <code>&lt;result&gt;</code> element. A sensor in this error status cannot return any data in its channels. If used, all channel values in the <code>&lt;result&gt;</code> section are ignored.	0 (= no)  1 (= yes, set sensor to error; ignore <code>&lt;result&gt;</code> section)

**i** Each run (sensor scan) might return either any number of channels (`<result>...</result>`) or one error response. It is not possible to mix result and error entries.

**i** You can either write the XML output to standard OUT line by line, or give back the entire expression in one line without breaks.

## Command-line Parameters

In the `parameter` field, you can use the following placeholders:

Placeholder	Description
%sensorid	The ID of the EXE/Script sensor.
%deviceid	The ID of the device the sensor is created on.
%groupid	The ID of the group the sensor is created in.
%probeid	The ID of the probe the sensor is created on.
%host	The IP address/DNS name of the device the sensor is created on.
%device	The name of the device the sensor is created on.
%group	The name of the group the sensor is created in.
%probe	The name of the probe the sensor is created on.
%name	The name of the EXE/Script sensor.
%windowsdomain	The domain for Windows access (can be inherited from parent).
%windowsuser	The user name for Windows access (can be inherited from parent).
%windowspassword	The password for Windows access (can be inherited from parent).
%linuxuser	The user name for Linux access (can be inherited from parent).
%linuxpassword	The password for Linux access (can be inherited from parent).
%snmpcommunity	The community string for SNMP v1 or v2 (can be inherited from parent).

**i** You need to escape placeholders that you use in the [parameter](#) field with quotation marks so that they can be correctly resolved from the command line.

**i** You need to escape special characters and whitespaces in your parameters and surround them with double quotation marks ("). See section [Escape Special Characters and Whitespaces in Parameters](#)<sup>[3312]</sup> for details.

**■** See section [Inheritance of Settings](#)<sup>[136]</sup> for more information on inherited settings.

## Environment Values

If the Set placeholders as environment values option is enabled in the sensor's settings, the values of all placeholders available for [command-line parameters](#) <sup>3148</sup> are additionally provided as "Environment Variables" during run time, so you can use them in your executable or script file. The variables' names are the same as for placeholders mentioned above, with the prefix `prtg_` and without the `%` character. For example, refer to the sensor's own name by using the variable `prtg_name`.

Additionally, the following variables are available:

Variable	Description
<code>prtg_version</code>	The version number of your PRTG installation.
<code>prtg_url</code>	The IP address/DNS name of your PRTG installation.
<code>prtg_primarychannel</code>	The ID of the sensor's primary channel (1 if not set).

## More

You can find sample projects for these custom sensors and more information about custom scripts here:

- \Custom Sensors\EXE subfolder of the [PRTG program directory](#) <sup>3213</sup>.

### ■ KNOWLEDGE BASE

Custom sensors

- <https://kb.paessler.com/en/tags/custom-script-exe>

Guide for PowerShell-based custom sensors

- <https://kb.paessler.com/en/topic/71356>

What is the multi-platform probe and how can I use it?

- <https://kb.paessler.com/en/topic/90140>

### ■ PAESSLER WEBSITE

You can find scripts for custom sensors that were written by dedicated PRTG customers in the PRTG Sensor Hub.

- <https://www.paessler.com/sensor-hub>

## 14.2.7 Custom Notifications

In addition to the various standard methods for notifications, you can define your own notifications that can trigger desired actions. The following documentation describes these custom notifications. You can also combine different notification methods in one notification.

■ For more general information about notifications based on email, messaging, and others, see section [Notifications](#) <sup>[2735]</sup>.

### Execute HTTP Action

This notification method executes a GET request or sends any POST, PUT, or PATCH data to a custom URL. You can execute specific actions on a web server or control any web service that accepts commands via one-time HTTP requests. Whenever a notification of this kind is triggered, the HTTP action is sent.

With this method, you can also call any application programming interface (API) function of the PRTG web interface. For example, you can automatically pause a sensor or acknowledge an alarm.

ⓘ Authentication with API key or user name and [passhash](#) <sup>[2803]</sup> (or user name and password) must always be included in each PRTG API request. See section [HTTP API](#) <sup>[8086]</sup> for more information.

#### Examples

To automatically pause the sensor that triggers the notification, enter the following HTTP action:

```
http://yourserver/api/pause.htm?id=%  
sensorid&action=0&username=myuser&password=mypassword
```

To use the notification to automatically acknowledge the alarm that triggered it, enter this HTTP action:

```
http://yourserver/api/acknowledgealarm.htm?id=%sensorid&ackmsg=Auto-  
Acknowledged&username=myuser&password=mypassword
```

■ For more information about authentication within the URL and for other possible actions you can configure, see sections [HTTP API](#) <sup>[3083]</sup> and [Object Manipulation](#) <sup>[3130]</sup>.

### Execute Program

With this notification method, you can execute a script or a program as an external process. It can be a Windows executable file or a .bat, .cmd, or PowerShell file. You can use .exe, .com, .bat, .cmd, .vbs, or .ps1 files.

ⓘ You must create the notification as a file and place it in a specific subfolder on the PRTG core server system (in a cluster, copy the files to every cluster node).

Place executables (.exe, .com), batch files (.cmd, .bat), VBS scripts (.vbs), or PowerShell scripts (.ps1) into the folder:

```
\Notifications\EXE
```

As soon as a file is placed into the subfolder, you can create or edit your own custom execute program notification and select the new file from the list of files. You can also enter start parameters and use PRTG placeholders for this.

#### Notes

- PRTG executes the file on the local PRTG core server system using the account configured for the PRTG core server service (the default is [system](#)).
- If your custom notification's code relies on other files (for example, .dll, .NET framework, or Windows PowerShell), you must copy/install these files on the PRTG core server system manually.
- Make sure the return code of the executable is 0 (zero). Otherwise PRTG assumes something went wrong with the notification and tries to send it up to 3 times.
- If you run PRTG in a cluster, copy the respective files to every cluster node to make sure the notification also works when the primary master node is not reachable.
- EXE notifications fail if they attempt to open any graphical user interface windows using the Win32 APIs (this is not allowed for processes that are started by a system service).
- To remotely run PowerShell scripts, make sure that you set the according Execution Policy. For more information, see the Knowledge Base: [PowerShell 32 bit and 64 bit and Execution Policy](#).

#### Placeholders

- For more information about the placeholders you can use, see section [Placeholders for Notifications](#) 3325.

#### PRTG Sensor Hub

You can find scripts for custom sensors that were written by dedicated PRTG customers in the [PRTG Sensor Hub](#).

#### More

##### ■ KNOWLEDGE BASE

##### Custom notifications

- <https://kb.paessler.com/en/tags/custom-notification>

##### PowerShell 32 bit and 64 bit and Execution Policy

- <https://kb.paessler.com/en/topic/20443>


## 14.2.8 Mini Probe API


### Important Notice

We do not further develop the Mini Probe API because we plan major changes to the underlying PRTG Application Programming Interface (PRTG API). You can still use the Mini Probe API "as is" but note that it may be deprecated at any time.

 Knowledge Base: [Where can I find PRTG mini probes which are ready to use?](#)

Mini probes allow users to create small probes on any device to meet specific needs. In general, probes are the part of PRTG that run monitoring processes and deliver monitoring results back to the PRTG core server. Mini probes gather monitoring data from platforms where it is not possible or is inapplicable to use the common local and remote probes of PRTG. Mini probes have a less complex implementation than standard probes so that you can create them on any platform. The only requirement is HTTPS connectivity to send monitoring data to your PRTG core server.










 With the current version of PRTG, you can use the mini probe interface with your custom code to implement solutions to special scenarios that you might have in your network. Note that there are major changes planned to the underlying PRTG API. Therefore, any code you write now likely needs to be changed later, so it can be used for future versions of PRTG. For example, if the available HTTP Push sensors are not sufficient for your needs, you can still use the Mini Probe API.

 Because the mini probe requires a Secure Sockets Layer (SSL) secured connection to the PRTG core server, it is not possible by default to connect if SSL is deactivated for PRTG. This is necessary because probably unencrypted passwords are transferred between the probe and the PRTG core server. So it is important to encrypt the connection even on internal routes. If your network setup ensures security in a different way (for example, a VPN), you can use a registry key option for disabling SSL to get a connection to your mini probe.

 For more information, see the Knowledge Base: [How can I disable SSL for Mini Probes?](#)

 The Mini Probe API is not available in PRTG Hosted Monitor

In this section:

- [Differences Between Probe Types](#)  <sup>3154</sup>
- [The PRTG Mobile Probe Protocol](#)  <sup>3153</sup>
  - [Communication and Security](#)  <sup>3153</sup>
  - [Authentication](#)  <sup>3153</sup>
  - [HTTP Requests](#)  <sup>3153</sup>
- [JSON Definition](#)  <sup>3157</sup>
  - [Sensor Definition](#)  <sup>3157</sup>
  - [Tasks Definition](#)  <sup>3162</sup>
  - [Data Definition](#)  <sup>3164</sup>

## Differences Between Probe Types

The following table shows technical specifications of the two probe types in PRTG.

Functionality	Local and Remote Probes	Mini Probe
Connection Protocol from Probe to PRTG Core Server	Protocol from PRTG	HTTPS
Security	Data is secured with SSL and an access key. New probe connections must be approved by an administrator. IP address and globally unique identifier (GUID) filtering is possible.	The same security level as for local and remote probes.
Estimated Limit for Sensors per Probe	Several thousand sensors	Fewer than 100 sensors
Estimated Limit for Probes per Installation	Hundreds of probes	Fewer than 100 probes
Estimated Minimum Scanning Interval	Some seconds	At least 60 seconds
Estimated Number of Sensors	More than 200	A few
Updates to New PRTG Versions by the PRTG Core Server	Yes	No
Complexity	High	Very low
Documented API	No	Yes
Supported Platforms	At least Windows (32-bit/64-bit)	Any platform
Scheduling of Sensor Requests Performed by	Probe	Probe
Code Managed by	Paessler GmbH	Writer of the probe
Probe Scans for Available Measurements Beforehand	Yes	No
Sensors Support <a href="#">Inheritance of Settings</a> <small>[136]</small>	Yes	No



Functionality	Local and Remote Probes	Mini Probe
Limitations by Administrator for Allowed Sensors that a User Can Create	Yes	No

## The PRTG Mobile Probe Protocol

The PRTG Mini Probe Protocol (PMPP) is a simple, lightweight protocol that extends PRTG with custom remote probes. It can be implemented in a variety of programming languages and runs on any kind of platform. These include, for example, Linux, Android, macOS, and iOS.

**i** Mini probes are not intended for high performance monitoring and support only the sensors that you implement.

## Communication and Security

The PMPP uses GET and POST requests via HTTPS to communicate with the PRTG core server. All requests are sent to the defined Transmission Control Protocol (TCP) port for the common PRTG web server (the default port is 443 for SSL), or you specify an extra port explicitly for mini probe connections in the [Core & Probes](#) settings. Mini probes use the GET method to receive tasks, and the POST method to send information about the probe and the monitoring results to the PRTG core server.

**i** The data format of some HTTP fields has to be JavaScript Object Notation (JSON) encoded. See [JSON Definition](#) for data definitions that require JSON. All exchanged data is secured with SSL.

## Authentication

The PMPP uses the same authentication methods as the common remote probes in PRTG. The authentication includes the following steps:

- Allow and deny IP addresses filter
- Deny global ID (GID) filter
- Access key
- Unique GID that must be approved in the PRTG web interface
- In addition, mini probes must be allowed to connect in the probe connection settings in PRTG. Additionally, you must provide the mini probe's IP address in the Allow IP Addresses field (or enter any).

There are no sessions on the server: Every request must contain the required authentication information.

**■** For more details, see section [Core & Probes](#).

## HTTP Requests

The PMPP includes three different HTTP requests that are sent to the PRTG web server:

- announce: An announce request is sent once when the probe starts. Afterward, the task and data commands are run in a scheduled manner.
- tasks: With a tasks request, the probe requests a list of tasks to perform.
- data: The data request sends the monitoring results to the core.

All requests of the mini probe to the PRTG core server must contain the following HTTP fields:

- gid: The unique GUID of the probe. We recommend a GUID that is generated by the operating system. This identifier must stay the same for as long as the probe installation exists. You can use any string. If you clone a probe, you must update this field to a new value.
- key: An access key as defined in the probe settings of the PRTG core server. The key has to be encoded in SHA1 hash (for example, `key=a94a8fe5ccb19ba61c4c0873d391e987982fbbd3`).
- protocol: The version of the protocol you use. Currently, this value is "1"

All requests return common HTTP response codes.

■ For more information, see section [HTTP API](#)<sup>[3085]</sup>.

### Announce Request

The announce request uses the POST method and provides all required information about the capabilities of the mini probe for the PRTG core server. The target URL is <https://<yourPRTGserver>/probe/announce>.

**i** This HTTP request must be sent at least once to be able to add sensors. We recommend you send this request every time the probe starts. You should NOT send it with every scanning interval.

The announce request must contain the following HTTP fields:

- name: The name of the mini probe. PRTG uses this name to create a corresponding node in the device tree.
- version: The version number of the mini probe you have implemented. This is a single integer, for example, 1.
- baseinterval: The number of seconds between two calls of the task/data requests. We recommend 60 or 300 seconds. Depending on the usage, higher or lower values are possible.
- sensors: The definition of supported sensors in JSON format.  
■ See [Sensor Definition](#)<sup>[3157]</sup> for more information.
- icon (optional): You can optionally send the file name of a device icon to show it for the mini probe device in the PRTG web interface.

**i** If you change the definition of a sensor that has already been announced, these changes are only active after the next start of PRTG. A definition never changes while PRTG is running. However, there is one exception: Setting the "deprecated" flag works without any restart. Because of this, you can replace a sensor with a new one that uses a different definition.

### Tasks Request

The tasks request uses the GET method and is sent from your mini probe in the defined scheduler interval to the PRTG core server (for example, every 5 minutes). The target URL is

```
https://<PRTGserver>/probe/tasks
```

This HTTP request returns a list of tasks in JSON format that need to be run by the mini probe.

■ See [Tasks Definition](#) <sup>3162</sup> for more information.

### Data Request

The data request uses the POST method and contains the HTTP field data. This HTTP field contains any number of sensor results in JSON format. The target URL is

```
https://<PRTGserver>/probe/data
```

You can split the results of one tasks list into several result requests (for example, if some sensors are faster than others). The mini probe should combine as many results as possible into one request but keep the time between measurement and reporting of the value at a low level.

■ See [Data Definition](#) <sup>3164</sup> for more information.

### JSON Definition

All data definitions of sensors, tasks, and result data of mini probes are JSON encoded. JSON is a language-independent data format that is used to transmit data objects consisting of attribute-value pairs between a server and an application. Refer to the JSON documentation for a general overview of this data format.

### Sensor Definition

This section shows how you can define the available sensors for your mini probe. Sensor definitions are specified in the HTTP field "sensors" of the announce request. The sensor types definition is a JSON array where each sensor type is defined in one array element as a JSON object. A JSON object denoting a sensor definition consists of the following JSON name/value pairs:

Name	Mandatory	Description	Possible Value
kind	X	Unique identifier for the sensor type in the mini probe. Used in the tasks definition to identify the sensor type.  ⓘ Underscore "_" is not allowed here.	Any string
name	X	The display name of the sensor.	Any string
deprecated	—	You can flag the sensor to status deprecated. A flagged sensor can still run but this kind of sensor is not shown when you add new sensors to the probe.	1 (= deprecated) 0 (= not deprecated)

Name	Mandatory	Description	Possible Value
description	—	A short description of the sensor that is shown in the <a href="#">Add Sensor</a> <sup>[414]</sup> dialog in the PRTG web interface.	Any string
help	—	A help text that is shown in a popup in the Add Sensor dialog in the PRTG web interface.	Any string
tag	—	A default tag for the sensor that is automatically added to the sensor.	Any string
default	—	A sensor of this type is automatically created with the probe if set to "default".	(= set to default) 0 (= not default)
groups	—	In the "groups" array, available settings for this sensor type are defined.	An array of grouped settings JSON objects.  ⓘ See <a href="#">Definition of Setting Groups Objects</a> <sup>[3158]</sup> for more information.

### Definition of Setting Groups Objects

One settings group definition (one element of the "groups" array) consists of three elements:


Name	Mandatory	Description	Possible Value
name	X	The internal name of the settings group.	Any unique string
caption	X	The label of the settings group as shown in the PRTG web interface.	Any string
fields	X	The available settings of the settings group.	An array of field definition objects.  ⓘ See <a href="#">Parameters for Setting Fields</a> <sup>[3158]</sup> for more information.

### Parameters for Setting Fields

The following table shows available JSON name/value pairs for setting fields:

Name	Mandatory	Description	Available in Type	Possible Value
type	X	Type of the field. This defines the possible content.	All	Edit Password Integer Radio  See <a href="#">Definition of Setting Fields: Field Types</a> <sup>[3160]</sup> for more information.
name	X	The internal name of the field. The name has to be unique per sensor. It is sent with the settings of the probe in the task request.	All	Any unique string
caption	X	The label of the field. It is displayed left of the field.	All	Any string
required	—	If a field is defined as required, this field has to be set when adding or editing the sensor settings. The default is not required.	All	0 (= not required) 1 (= required)
default	—	The default value of the field.	All	Any string or integer (depending on the field type)
help	—	A help text that is displayed right of the field.  You can use limited BBCode: "[b]" and "[/b]" for bold, "[i]" and "[/i]" for italics, and "[br]" for line break.	All	Any string

Name	Mandatory	Description	Available in Type	Possible Value
maximum	—	The maximum value that is allowed for this field.	Integer	Integer
minimum	—	The minimum value that is allowed for this field.	Integer	Integer
options	—	A JSON array that provides several radio buttons to choose a desired option.	Radio	"name": "value" pairs. See <a href="#">Example</a> <sup>[3160]</sup> below.

 Example

"name": "value" pairs that define radio button options:

```


{
    "1": "This is option 1",
    "2": "This is option 2",
    "XYZ": "Another option"
}

```

### Definition of Setting Fields: Field Types

A sensor type can have any number of setting fields that are organized in groups of settings. One field is one element in the "fields" array of a settings group. Currently, mini probes support four different field types for settings:

- edit: One line edit field.
- password: An edit field with masked characters.
- integer: A number field with optional minimum/maximum selection.
- radio: A selection of multiple options with radio buttons.

 Example

The following is a detailed example that shows the JSON object definition of a sensor type that is used in the HTTP field sensors of the announce request.

This sensor type is called [Sample Sensor](#) and is from the type [Sample](#). It has a description, a help text, and a default tag. There are two setting groups, [Group](#) and [group2](#), with several setting fields (six in the first group, one in the second group). The example also shows how you can use the available JSON name/value pairs in the [fields](#) array object.

```
[
  {
    "kind": "Sample",
    "name": "Sample Sensor",
    "description": "This is a sample demo sensor",
    "help": "This is the help text of the demo sensors",
    "tag": "demosensor",
    "groups": [
      {
        "name": "Group",
        "caption": "Group",
        "fields": [
          {
            "type": "edit",
            "name": "simpleedit",
            "caption": "Edit Field",
          },
          {
            "type": "edit",
            "name": "extendededit",
            "caption": "Edit Field 2",
            "required": "yes",
            "default": "Default Value",
            "help": "Help text displayed to the right of the field"
          },
          {
            "type": "integer",
            "name": "simplenumber",
            "caption": "Number",
          },
          {
            "type": "integer",
            "name": "number2",
            "caption": "Number 2",
            "required": "1",
            "minimum": 23,
            "maximum": 99,
            "help": "Number field with limit 23-99"
          },
          {
            "type": "password",
            "name": "password",
          }
        ]
      }
    ]
  }
]
```

```

        "caption": "Password",
        "help": "This is a password field"
    },
    {
        "type": "radio",
        "name": "radiotest",
        "caption": "Radio test",
        "help": "This is a radio selection field",
        "options": {
            "1": "This is option 1",
            "2": "This is option 2",
            "3": "This is option 3"
        },
        "default": "2"
    },
    ]
},
{
    "name": "group2",
    "caption": "Group 2",
    "fields": [
        {
            "name": "testfield2",
            "caption": "Test2",
            "type": "edit"
        }
    ]
}
]
}
]

```

### Tasks Definition

A tasks definition is a JSON array where each task is one object. Tasks contain all name/value pairs as defined in the sensor settings definition, which are filled with the values you have provided. Additionally, the following information is included:

Name	Mandatory	Description	Possible Value
kind	X	The type of the sensor.	String



Name	Mandatory	Description	Possible Value
sensorid	X	The ID of the sensor.	Integer
host	X	The IP address/DNS name of the parent device as specified for this device. For the probe device, the default is <a href="#">127.0.0.1</a> .	IP address/DNS name
all defined fields	X	All fields that are defined in the sensor setting group objects are included in the tasks definition as name/value pairs.	name/value pairs

**i** This data comes from PRTG, so the mandatory JSON objects are included automatically.

**Example**

Definition of two tasks, the first one is the simplest possible one without any values, and the second one uses the sensor settings objects as defined above:

```
[
  {
    "sensorid": "2009",
    "kind": "ping",
    "host": "www.google.com"
  },
  {
    "sensorid": "2010",
    "kind": "sample",
    "host": "www.paessler.com",
    "simpleedit": "Test2",
    "extendededit": "Extended Test",
    "simplenumber": "3",
    "number2": "42",
    "password": "masked text",
    "radiotest": "1",
    "testfield2": "This is test 3"
  }
]
```

## Data Definition

A data definition is a JSON array where each result of a task is one object. Every array element contains the following name/value pairs:

Name	Mandatory	Description	Possible Value
sensorid	X	The ID of a specific sensor.	Integer
time	—	<p>The time of measurement in Coordinated Universal Time (UTC)/GMT time zone as a JSON number in the Unix time format (in milliseconds since Unix epoch, which is 00:00:00 UTC on January 1, 1970). Time values must be strictly chronological, so the Unix time of each measurement must be greater than the one before. The time values should be close to the current time (which is now) to prevent sensors in the Unknown <a href="#">status</a><sup>[181]</sup>.</p> <p><b>i</b> If no time value is provided, the current time (now) is used.</p>	JSON number defining Unix time
message	—	An optional text message.	Any string
channel	X	The channel result values.	<p>An array of name/value pairs.</p> <p><b>i</b> See <a href="#">Parameters for Data Definitions: Channel Result Values</a><sup>[3165]</sup> for more information.</p>

### Examples

Data definition object with sensor status **OK**:

```
[
  {
    "sensorid":"2003",
    "message":"Optional Message",
    "channel":[
      {
        "name":"Time",
        "mode":"integer",
        "unit":"TimeResponse",
        "value":6
        "showchart":1
        "showtable":1
      }
      {
        "name":"Pages",
        "mode":"counter",
        "unit":"Custom",
        "customunit":"Pages",
        "value":99
      }
    ]
  }
]
```

Data definition object with sensor status error:

```
[
  {
    "sensorid":"2003",
    "error":"Response",
    "code":10,
    "message":"Error Message"
  }
]
```

#### Parameters for Data Definitions: Channel Result Values

The following table shows name/value pairs that can be used in the "channel" array objects of data definition objects:

Name	Mandatory	Description	Possible Value
Name	X	The name of the channel as displayed in user interfaces.	Any string
Value	X	Any number without quotation marks.	An integer, float, or counter value
Mode	—	The type of the value. <b>i</b> Make sure that it matches the provided value, otherwise PRTG shows 0 values.	Integer, float, or counter
Unit	—	The unit of the value. <b>i</b> If you set the correct unit type instead of using custom units, PRTG can display received values better.	BytesBandwidth BytesMemory BytesDisk BytesFile TimeResponse TimeSeconds TimeHours Temperature Percent Count CPU: This is a % unit that is accounted to the CPU load in index graphs. Custom (define the name of the unit using the additional field customunit)
ShowChart	—	Init value for the Show in graphs option. <b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings.	0 (= do not show graph) 1 (= show graph)

Name	Mandatory	Description	Possible Value
ShowTable	—	<p>Init value for the Show in graphs option.</p> <p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings.</p>	<p>0 (= do not show table)</p> <p>1 (= show table)</p>
SpeedSize VolumeSize	—	<p>Size used for the display value. For example, if you have a value of 50000 and use Kilo as size, the display is 50 kilo #. The default is <b>One</b> (value used as returned).</p> <p><b>i</b> For the Bytes and Speed units, this is overridden by the setting in the user interface.</p>	<p>One</p> <p>Kilo</p> <p>Mega</p> <p>Giga</p> <p>Tera</p> <p>Byte</p> <p>KiloByte</p> <p>MegaByte</p> <p>GigaByte</p> <p>TeraByte</p> <p>Bit</p> <p>KiloBit</p> <p>MegaBit</p> <p>GigaBit</p> <p>TeraBit</p>
SpeedTime	—	<p>See above, used when displaying the speed. The default is <b>Second</b>.</p>	<p>Second</p> <p>Minute</p> <p>Hour</p> <p>Day</p>

Name	Mandatory	Description	Possible Value
decimalMode	—	<p>Init value for the Decimal Places option. If 0 is used in the float mode (use integer), the default is <a href="#">Automatic</a>. Otherwise (for float), the default is <a href="#">All</a>.</p> <p><b>i</b> You can change this initial setting later in the sensor's <a href="#">channel settings</a> <sup>[268]</sup>.</p>	<p>Automatic</p> <p>All</p> <p>Custom</p>
decimalDigits	—	<p>If you define Custom as decimalMode, specify the number of digits after the delimiter.</p>	Integer
ValueLookup	—	<p>Define if you want to use a lookup file (for example, to view integers as status texts). Enter the ID of the lookup file that you want to use, or omit this element to not use lookups.</p> <p><b>■</b> See section <a href="#">Define Lookups</a> <sup>[318]</sup> for more information.</p> <p><b>i</b> This setting is only considered on the first sensor scan, when the channel is newly created. It is ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings.</p>	Any string
LimitMaxError	—	<p>Define an upper error limit for the channel. If enabled, the sensor is set to the Down status if this value is exceeded and the LimitMode is activated.</p> <p><b>i</b> Provide the value for the limit in the unit of the base data type as it is used in the &lt;Value&gt; element of this section. When a sensor shows the Down status triggered by a limit, it still receives data in its channels.</p>	Integer

Name	Mandatory	Description	Possible Value
		<p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings.</p>	
LimitMaxWarning	—	<p>Define an upper warning limit for the channel. If enabled, the sensor is set to the Warning status if this value is exceeded and the LimitMode is activated.</p> <p><b>i</b> Provide the value for the limit in the unit of the base data type as it is used in the &lt;Value&gt; element of this section.</p> <p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings.</p>	Integer
LimitMinWarning	—	<p>Define a lower warning limit for the channel. If enabled, the sensor is set to the Warning status if this value falls below the defined limit and the LimitMode is activated.</p> <p><b>i</b> Provide the value for the limit in the unit of the base data type as it is used in the &lt;Value&gt; element of this section.</p>	Integer

Name	Mandatory	Description	Possible Value
		<p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings.</p>	
LimitMinError	—	<p>Define a lower error limit for the channel. If enabled, the sensor is set to the Down status if this value falls below the defined limit and the LimitMode is activated.</p> <p><b>i</b> Provide the value for the limit in the unit of the base data type as it is used in the &lt;Value&gt; element of this section.</p> <p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings.</p>	Integer
LimitErrorMsg	—	<p>Define an additional message. It is added to the sensor's message when entering the Down status that is triggered by a limit.</p> <p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings.</p>	Any string



Name	Mandatory	Description	Possible Value
LimitWarningMessage	—	<p>Define an additional message. It is added to the sensor's message when entering the Warning status that is triggered by a limit.</p> <p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings.</p>	Any string
LimitMode	—	<p>Define if the limit settings defined above are active. The default is 0 (no; limits inactive). If 0 is used, the limits are written to the channel settings as predefined values, but limits are disabled.</p> <p><b>i</b> The values defined with this element are only considered during the first sensor scan when the channel is newly created. They are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings.</p>	0 (= no) 1 (= yes)
Warning	—	<p>If enabled for at least one channel, the entire sensor is set to the Warning status. The default is 0 (no).</p>	0 (= no) 1 (= yes)
Message	—	<p>Text the sensor returns in the Message field with every scanning interval. There can be one message per sensor, regardless of the number of channels. The default message is <b>OK</b>.</p>	Any string

Name	Mandatory	Description	Possible Value
Error	—	<p>The type of error.</p> <p><b>i</b> The type is not necessarily shown in PRTG.</p>	<p>Data: The monitored device returned a value but the sensor could not process it.</p> <p>Response: The monitored device reported an error. This includes timeouts, HTTP response codes, etc.</p> <p>Exception: Error in sensor handling.</p> <p>Socket: Socket error.</p>
Code	—	The error code that is stored in the database.	Integer

## More

### ■ Knowledge Base

How can I disable SSL for Mini Probes?

- <https://kb.paessler.com/en/topic/60356>

Where can I find PRTG mini probes which are ready to use?

- <https://kb.paessler.com/en/topic/61215>

## 14.3 Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors


You can use filter rules for the Include Filter, Exclude Filter, and Channel Definition fields of [packet sniffer](#)<sup>[3009]</sup>, [flow, and IPFIX](#)<sup>[3011]</sup> sensors. The filter rules are based on the following format:

```
field[filter]
```


In this section:

- [Valid Fields for All Sensors](#)<sup>[3173]</sup>
- [Additional Fields for Packet Sniffer Sensors Only](#)<sup>[3174]</sup>
- [Additional Fields for NetFlow v5 and jFlow v5 Sensors Only](#)<sup>[3174]</sup>
- [Additional Fields for NetFlow v9 and IPFIX Sensors Only](#)<sup>[3175]</sup>
- [Additional Fields for sFlow Sensors Only](#)<sup>[3176]</sup>
- [Valid Data Formats](#)<sup>[3176]</sup>
- [Examples](#)<sup>[3176]</sup>


### Valid Fields for All Sensors

Field	Possible Filter Values
IP	IP address or Domain Name System (DNS) name  For more information, see section <a href="#">Valid Data Formats</a> <sup>[3176]</sup> .
Port	Any number
SourceIP	IP address or DNS name
SourcePort	Any number
DestinationIP	IP address or DNS name
DestinationPort	Any number
Protocol	<a href="#">Transmission Control Protocol (TCP)</a> , <a href="#">User Datagram Protocol (UDP)</a> , <a href="#">Internet Control Message Protocol (ICMP)</a> , <a href="#">Open Shortest Path First (OSPF)</a> , any number
ToS	<a href="#">Type of Service (ToS)</a> : any number
DSCP	<a href="#">Differentiated Services Code Point (DSCP)</a> : any number

### Additional Fields for Packet Sniffer Sensors Only

Field	Possible Filter Values
MAC	Physical address  For more information, see section <a href="#">Examples</a> <sup>3176</sup> .
SourceMAC	Physical address
DestinationMAC	Physical address
EtherType	<a href="#">IPV4</a> , <a href="#">ARP</a> , <a href="#">RARP</a> , <a href="#">APPLE</a> , <a href="#">AARP</a> , <a href="#">IPV6</a> , <a href="#">IPXold</a> , <a href="#">IPX</a> , any number
VlanPCP	IEEE 802.1Q VLAN Priority Code Point
VlanID	IEEE 802.1Q VLAN Identifier
TrafficClass	IPv6 Traffic Class: corresponds to <a href="#">TOS</a> used with <a href="#">IPv4</a>
FlowLabel	IPv6 Flow Label

### Additional Fields for NetFlow v5 and jFlow v5 Sensors Only

Field	Possible Filter Values
Interface	Any number
ASI	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP address of the sending device. Use this if you have several devices that send flow data on the same port, and you want to divide the traffic of each device into a different channel.  Possible values: IP address or DNS name  For more information, see section <a href="#">Valid Data Formats</a> <sup>3176</sup> .
SourceASI	Any number


Field	Possible Filter Values
DestinationASI	Any number

### Additional Fields for NetFlow v9 and IPFIX Sensors Only


Field	Possible Filter Values
Interface	Any number
ASI	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	<p>IP address of the sending device. Use this if you have several devices that send flow data on the same port, and you want to divide the traffic of each device into a different channel.</p> <p>Possible values: IP address or DNS name</p> <p> For more information, see section <a href="#">Valid Data Formats</a> <sup>3176</sup>.</p>
SourceASI	Any number
DestinationASI	Any number
MAC	Physical address
SourceMAC	Physical address
DestinationMAC	Physical address
Mask	Mask values represent subnet masks in the form of a single number (number of contiguous bits).
DestinationMask	Mask values represent subnet masks in the form of a single number (number of contiguous bits).
NextHop	IP address or DNS name
VLAN	VLAN values represent a VLAN identifier (any number).

Field	Possible Filter Values
SourceVLAN	VLAN values represent a VLAN identifier (any number).
DestinationVLAN	VLAN values represent a VLAN identifier (any number).

### Additional Fields for sFlow Sensors Only

Field	Possible Filter Values
Interface	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	<p>IP address of the sending device. Use this if you have several devices that send flow data on the same port, and you want to divide the traffic of each device into a different channel.</p> <p>Possible values: IP address or DNS name</p> <p> For more information, see section <a href="#">Valid Data Formats</a> <sup>B176</sup>.</p>
MAC	Physical address
SourceMAC	Physical address
DestinationMAC	Physical address

### Valid Data Formats

- IP fields support wildcards (\*), range (10-20) and hostmask ( /10, /255.255.0.0) syntax, as well as DNS names.
  -  IP fields do not support IPv6 wildcards, IPv6 ranges, and IPv6 hostmasks.
- Number fields support range (80-88) syntax.
- Protocol and EtherType fields support numbers and a list of predefined constants.

 For more information on IP address ranges, see section [Define IP Address Ranges](#) <sup>B180</sup>.

### Examples

All of the following filter rules are valid examples:

```
SourceIP[10.0.0.1]
SourceIP[10.*.*.*]
SourceIP[10.0.0.0/10]
DestinationIP[10.0.0.120-130]
DestinationPort[80-88]
Protocol[UDP]
MAC[00-60-50-X0-00-01]
DSCP[46]
```

You can create more complex expressions by using parentheses ( ) and the words **and**, **or**, or **and not**. For example, these are valid filter rules:

```
Protocol[TCP] and DestinationIP[10.0.0.1]
```

This rule filters for all TCP traffic with the destination IP address 10.0.0.1.

```
Protocol[TCP] or DestinationIP[10.0.0.1]
```

This rule filters for all TCP traffic and all traffic with the destination IP address 10.0.0.1.

```
Protocol[TCP] and (DestinationIP[10.0.0.1] or SourceIP[10.0.0.120-130])
```

This rule filters for all TCP traffic with either the destination IP address 10.0.0.1 or the source IP address range 10.0.0.120-130.

```
Protocol[TCP] and not (DestinationIP[10.0.0.1] or SourceIP[10.0.0.120-130])
```

This rule filters for all TCP traffic that does not have the destination IP address 10.0.0.1 and the source IP address range 10.0.0.120-130.

## More

### KNOWLEDGE BASE

How can I change the default groups and channels for flow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

## 14.4 Channel Definitions for Flow, IPFIX, and Packet Sniffer Sensors

With [custom Flow sensors](#), [custom IPFIX](#)<sup>[3011]</sup>, or [custom Packet Sniffer sensors](#)<sup>[3009]</sup>, you have the option to provide a Channel Definition with the following syntax, one entry per channel:

```
#<id> : <Name>
<Rule>
```

### Syntax

- The `<id>` must be 1 or a higher number, and it must be unique for the sensor. This means that each channel definition must have a unique ID.
  - ❗ The maximum channel ID that you can use is **2147483648** ( $2^{31}$ ). PRTG does not support higher IDs. We recommend that you use channel IDs like 1, 2, or 3.
- The `<id>` is linked to the historic data.
  - ❗ As soon as you change the ID, you lose the history for the channel that the ID was linked to.
- One rule can span multiple lines.
- The next rule starts with a `#` as the first character in a line.
- The `<name>` is the display name of the channel.
- PRTG processes the rules from top to bottom (the number does not matter) and accounts the data to the first match.
- PRTG automatically adds one channel named Other. This channel counts all traffic for which you do not define a specific channel.
- After the name, you can use an optional `[<unit>]` to override the automatic unit, which is based on the source sensor.

The `<Rule>` syntax is identical to the one described in section [Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors](#)<sup>[3173]</sup>. Because PRTG accounts data to the first match, make sure that you start with the most specific rule at the top and get less specific towards the bottom.

❗ We recommend that you write the rules list in an external editor first and then paste it into the Channel Definition field of the sensor. If the rules contain an error, PRTG removes the entries after you add them.

❗ You cannot delete channels even if you remove a channel from the channel definition. You also cannot change the display name of channels using the channel definition of custom flow sensors. You can only rename channels in the [channel settings](#)<sup>[2681]</sup>.

### Example

General example:

```
#5:HTTP
Protocol[TCP] and
(SourcePort[80] or DestinationPort[80] or SourcePort[8080] or
DestinationPort[8080])
```

Channel definition example for differentiating by protocol:



```
#1:TCP
Protocol[TCP]

#2:UDP
Protocol[UDP]

#3:ICMP
Protocol[ICMP]
```

## More

### ■ KNOWLEDGE BASE

How can I change the default groups and channels for flow and Packet Sniffer sensors?


- <https://kb.paessler.com/en/topic/60203>

## 14.5 Define IP Address Ranges

In some setting fields, you can either enter a host name or a single IP address, or you can define IP address ranges. These are available, for example, for [Flow and Packet Sniffer sensors](#)<sup>[2832]</sup> and for [probe connection settings](#)<sup>[2890]</sup>. PRTG follows a common syntax for IP address ranges.

■ For the supported syntax of the automatic network discovery feature in PRTG, see section [Add an Auto-Discovery Group](#)<sup>[267]</sup>.

### Available Options

Option	Description	Syntax	Examples
Simple	Enter a fixed IP address.	a.b.c.d	10.0.10.9
Hostname	Enter a hostname. PRTG resolves it to an IP address in your network.	hostname	device-xyz
Hostmask	Enter a hostmask. A hostmask defines the relevant bits of the IP address.   Valid hostmasks are /0 - /32 for IPv4 and /0 - /128 for IPv6.	a.b.c.d/h or a.b.c.d/e.f.g.h	10.0.0.0/24
Range	Enter an IP address range. Replace each letter of a, b, c, d with either <ul style="list-style-type: none"> <li>▪ * (asterisk) for any value; corresponds to 0-255 or</li> <li>▪ x-y for any range between 0 and 255.</li> </ul>	a.b.c.d	10.0.0.1-20 or 10.*.0.* or 10.0.0-50.*


## 14.6 Define Lookups

PRTG uses lookups for some sensors and for other sensors that have custom channels. In general, lookups map status values as returned by a device (usually integers) to more informative expressions in words. Additionally, lookups can define a [sensor status](#)<sup>[181]</sup> based on the status value returned by a device, just like [channel limits](#)<sup>[2682]</sup> can define a sensor status. For a printer that returns the status value 1, for example, PRTG can show a sensor in the Warning status with the text message **Toner Low** instead of only displaying the status value 1.

You can customize lookups by defining your own text messages that a channel shows and by mapping them to a certain sensor status. See section [Customizing Lookups](#)<sup>[3187]</sup>.

If a channel uses lookups, you can individually define how to control the status of the sensor, either by using the lookup definition or by using limits for numeric values returned by the device. For more information, see section [Channel Settings](#)<sup>[2682]</sup>. It is not possible to use both definitions at the same time.

- i Lookups do not change data in the PRTG database, they merely change the way a sensor shows a channel. Any change to lookup definition files applies to historic data as well as to live data.
- i Some exceptions apply to the [SNMP Custom String Lookup](#) sensor that basically does an inverse lookup. It does not map an integer to a text message but only looks for matching strings in the lookup definition and shows a status based on this text value.

 To upload customized lookups to PRTG Hosted Monitor, see section [Manage a PRTG Hosted Monitor Subscription](#).

In this section:

- [Requirement: Channel Unit "Custom"](#)<sup>[3181]</sup>
- [Visualization of Lookup Channels](#)<sup>[3182]</sup>
- [Lookups Directory and Format](#)<sup>[3184]</sup>
- [The XML Schema](#)<sup>[3185]</sup>
- [Customizing Lookups](#)<sup>[3187]</sup>
- [desiredValue Attribute](#)<sup>[3189]</sup>
- [Lookup Types: SingleInt, Boolean, BitField, Range](#)<sup>[3189]</sup>
- [Define Lookup Files in Channel Settings](#)<sup>[3190]</sup>
- [Loading Lookups](#)<sup>[3190]</sup>
- [Debugging](#)<sup>[3191]</sup>

### Requirement: Channel Unit "Custom"

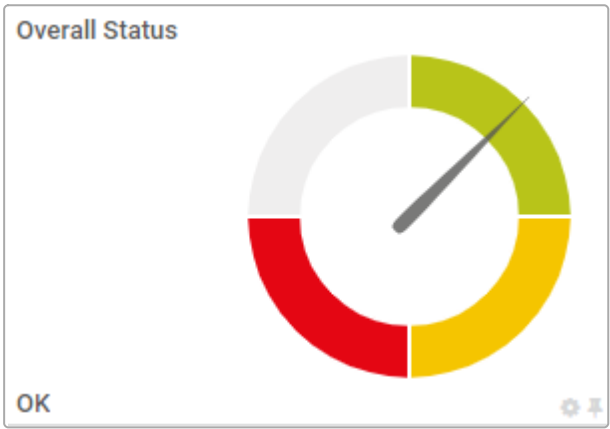

All channels with an enabled Lookup need to use the Channel Unit **"Custom"**. For more information, see section [Channel Settings](#)<sup>[2682]</sup>.

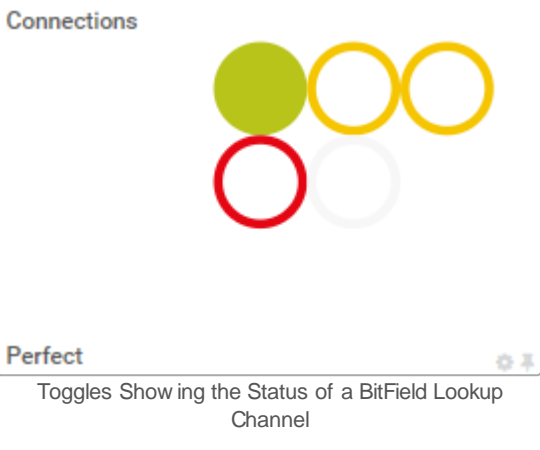
- i There are sensors that provide the Channel Unit **"Lookup"** in their settings. Do **not** use the Channel Unit **"Custom"** for channels of these sensors if you want to use lookups. This results in malfunctioning lookup definitions. For the following sensors, select the Channel Unit **"Lookup"** in the settings and select the lookup file directly under Channel Lookup during sensor creation:

- [Microsoft SQL v2](#)
- [MySQL v2](#)
- [Oracle SQL v2](#)
- [PostgreSQL](#)
- [SNMP Custom Advanced](#)
- [SNMP Custom Table](#)

### Visualization of Lookup Channels

PRTG can display channels that use lookups as follows.

Lookup Type	Visualization	Example
SingleInt, Range	Gauge	 <p>A Gauge Showing the Status of a Lookup Channel</p>
Boolean	Switch	 <p>A Switch Showing the Status of a Boolean Lookup Channel</p>

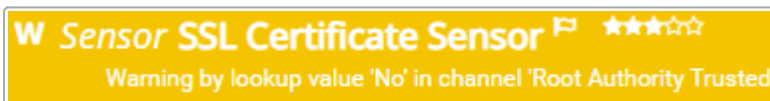
Lookup Type	Visualization	Example
BitField	Toggles	

You can view the text messages for the different lookup values by hovering over the respective section.



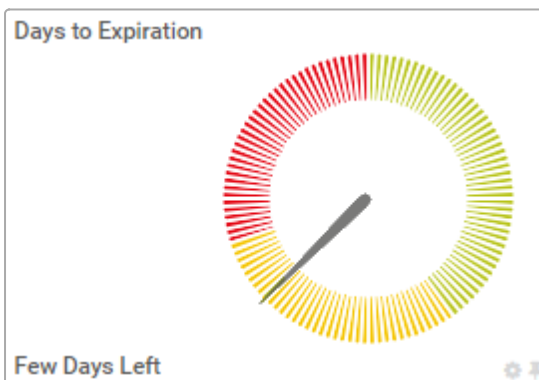
Gauge Showing the Respective Lookup Message when Hovering over a Color Section

To see which lookup value in which channel shows the Warning or Down status, check the sensor message on a sensor's Overview tab:



Sensor Message on the Overview Tab

**i** We recommend that you stay below 120 lookup values to display visually informative gauges for primary channels. Non-primary channels have an upper limit of around 40 lookup values for gauges.



Gauge Showing 120 Lookup Values

- i** The various sensor states that are displayed in gauges always follow the clockwise order Up < Warning < Down < Unknown. This order stays the same, no matter which numeric value you map to which sensor status in the lookup definition. See the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="example.lookups" desiredValue="1" undefinedState="olsWarning"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="PaeValueLookup.xsd">
<Lookups>
  <SingleInt state="OK" value="1">
    Works
  </SingleInt>
  <SingleInt state="OK" value="2">
    Works a bit
  </SingleInt>
  <SingleInt state="Warning" value="4">
    Is slow
  </SingleInt>
  <SingleInt state="Error" value="8">
    Does not work
  </SingleInt>
  <SingleInt state="OK" value="16">
    Works sometimes
  </SingleInt>
</Lookups>
</ValueLookup>
```

Even though the value 8 comes before the value 16, PRTG displays the state **OK** (shown as the Up status) before the state **Error** (shown as the Down status).

- See [Lookups Directory and Format](#)<sup>[3184]</sup> and [The XML Schema](#)<sup>[3185]</sup> for more information about the lookup code and format.

## Lookups Directory and Format

Lookups are defined in Extensible Markup Language (XML) format in files that end with **.ov**. PRTG standard lookup files are located in the `\lookups` subfolder of the [PRTG program directory](#)<sup>[3213]</sup>. PRTG maintains these files. In each of the files, lookups for one or more sensors are defined. Furthermore, the `\lookups` subfolder contains the `\custom` subfolder to store your customized lookups.

- For a list of all standard lookup files, see section [Standard Lookup Files](#)<sup>[3335]</sup>.

The files follow a basic principle. For each numeric value, you can define the following:

- A message that the sensor looks up and shows instead of the numeric value.
- The status that the sensor shows.

❗ Use the [SNMP Custom String Lookup](#) sensor to map a string to a corresponding status. For this purpose, use the [lookup type](#)<sup>3189</sup> SingleInt.

☁ You cannot access this directory on PRTG Hosted Monitor instances.

## The XML Schema

An exemplary schema of the .xml files that contain the lookup definitions can look like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="..." desiredValue="..." undefinedState="..." xmlns="..." xsi="...">
  <Lookups>
    <SingleInt state="..." value="...">status text</SingleInt>
    <SingleInt state="..." value="...">status text</SingleInt>
    <SingleInt state="..." value="...">status text</SingleInt>
  </Lookups>
</ValueLookup>
```

Element	Description	Attributes, Value Assignment, and Content
<?xml> <a href="#">content</a>	This is the XML declaration that every .xml file begins with.	<ul style="list-style-type: none"> <li>version and encoding are <a href="#">1.0</a> and <a href="#">UTF-8</a> respectively</li> <li>content: &lt;ValueLookup&gt;<a href="#">contentValueLookup</a>&lt;/ValueLookup&gt;</li> </ul>
<ValueLookup> <a href="#">contentValueLookup</a> </ValueLookup>	Defines the ID of the channel, which <a href="#">desiredValue</a> is used, the status for undefined values ( <a href="#">undefinedState</a> ), and links to the predefined schema definitions in PRTG that allow you to edit lookup files with supported editors.	<ul style="list-style-type: none"> <li>id: Specifies how the name of the lookup file is shown in the <a href="#">channel settings</a><sup>2681</sup>. ❗ PRTG parses the <a href="#">id</a> as a lowercase string.</li> <li><a href="#">desiredValue</a><sup>3189</sup>: Contains the value that PRTG uses for the calculation of the <a href="#">Coverage</a>.</li> <li>undefinedState: Optionally define a status for values that are not defined in the lookup file. If the target device returns a value that is not included in the lookup definition, the sensor shows this status (<a href="#">OK</a>, <a href="#">Warning</a>, <a href="#">Error</a>, or <a href="#">None</a>) with an according message. Without a definition of <a href="#">undefinedState</a>, the sensor only shows the returned value.</li> </ul>

Element	Description	Attributes, Value Assignment, and Content
		<ul style="list-style-type: none"> <li>▪ xmlns:xsi/xsi: Refers to predefined XML schema definitions in PRTG that allow you to edit lookup files with supported editors.</li> <li>▪ <code>contentValueLookup</code>: Lookup definitions  <code>&lt;Lookups&gt;contentLookups&lt;/Lookups&gt;</code></li> </ul>
<code>&lt;Lookups&gt; contentLookups &lt;/Lookups&gt;</code>	Defines the particular lookups for the sensor data.	<ul style="list-style-type: none"> <li>• <code>contentLookups</code>: One or more lookup entries, see below.</li> </ul>
<code>&lt;SingleInt&gt; status text &lt;/SingleInt&gt;</code>  <code>&lt;Boolean&gt; status text &lt;/Boolean&gt;</code>  <code>&lt;BitField&gt; status text &lt;/BitField&gt;</code>  <code>&lt;Range&gt; status text &lt;/Range&gt;</code>	<p>Each element defines one lookup entry. There can be one or more lookup entries from the same <a href="#">lookup type</a> <sup>B189</sup>.</p> <p><b>i</b> You can use only <b>one</b> kind of lookup type in <b>one</b> lookup file. This means only <b>SingleInt</b>, only <b>Boolean</b>, only <b>BitField</b>, or only <b>Range</b>. Different lookup types in one file are not allowed.</p> <p>The notation for the different lookup types can vary:</p> <ul style="list-style-type: none"> <li>▪ <code>&lt;SingleInt state="..." value="..."&gt;status text&lt;/SingleInt&gt;</code></li> <li>▪ <code>&lt;Boolean state="..." value="..."&gt;status text&lt;/Boolean&gt;</code></li> <li>▪ <code>&lt;BitField state="..." value="..."&gt;status text&lt;/BitField&gt;</code></li> <li>▪ <code>&lt;Range state="..." from="..." to="..."&gt;status text&lt;/Range&gt;</code></li> </ul>	<ul style="list-style-type: none"> <li>▪ <code>state</code>: Defines the status that the sensor shows. Allowed values are <b>OK</b>, <b>Warning</b>, <b>Error</b>, and <b>None</b>. <b>None</b> does not trigger a status change.</li> <li>▪ <b>i</b> <code>State</code> values must be capitalized for the sensor to work properly.</li> <li>▪ <code>value</code>: Defines the value that triggers the lookup. Enter an integer.</li> <li>▪ <b>i</b> Range always needs both values "from" and "to".</li> <li>▪ <code>status text</code>: Defines a <code>status text</code> that PRTG uses as substitution text and shows instead of the integer, for example, a status message.</li> <li>▪ <b>i</b> The SNMP Custom String Lookup sensor maps the status text to one of the specified states. For this sensor, use <b>SingleInt</b>.</li> </ul>

Because all .xml files that contain lookup definitions are delivered in a previously specified schema as indicated above, you can [customize lookups](#) <sup>B187</sup> accordingly.



## Example

The following code illustrates the lookup definition for the toner status of the [SNMP HP LaserJet Hardware](#) sensor:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="oid.paessler.hplaserjet.tonerstatus" desiredValue="1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="PaeValueLookup.xsd">
  <Lookups>
    <SingleInt state="OK" value="0">Toner Okay</SingleInt>
    <SingleInt state="Warning" value="1">Toner Low</SingleInt>
    <SingleInt state="Error" value="2">No Toner Cartridge Loaded</SingleInt>
  </Lookups>
</ValueLookup>
```



In our example, the lookup file has the following effect:

Value as Reported from HP Printer	Text Shown in PRTG (Channel)	Sensor Status Shown in PRTG	
0	Toner Okay		Up
1	Toner Low		Warning
2	No Toner Cartridge Loaded		Down

## Customizing Lookups

 To upload customized lookups to PRTG Hosted Monitor, see section [Manage a PRTG Hosted Monitor Subscription](#).

If you want to change the status definitions of a channel, follow these steps:

1. Find out the (file) name of the default lookup file in the settings of the channel that you want to change the status definitions for.
  2. From the \lookups subfolder of the [PRTG program directory](#) , copy this file into the \lookups\custom subfolder. Make sure that you do not change the file name.  
OR  
create a new .xml file there.
-  If you use the same ID in the [ValueLookup](#) tag, the files in the \lookups\custom subfolder have a higher priority than the original files in the \lookups folder. This way, PRTG prefers your customizations to the original lookup settings. If you want to use custom lookup definitions [in addition](#) to the standard lookups, define a new ID in the lookup file that is not used by any other lookup file. PRTG identifies lookup definitions via this ID, it does [not](#) use the file name.

3. Open the file with an XML or text editor and customize the lookups as you like. You can define your own text messages or customize sensor states for specific return values. For example, if you do not want a sensor to show the Down status for the return value 2 but only the Warning status, replace the state **Error** with **Warning**.

**i** All possible states are specified in the LookupState.xsd file in the custom directory. Follow the schema of the .xml files that are delivered with PRTG to make sure that you safely edit lookups.

**i** If you [import an .oidlib file](#) that contains lookups (you can see this in section [Lookup in MIB Importer](#)), you can define your own sensor states for the returned values. If you add an [SNMP Library](#) sensor and use this .oidlib file, PRTG creates a lookup definition file that uses the [lookupname](#) of the chosen library as **id** parameter. Override this lookup definition with your own custom lookup as described in this section. This is important because lookups that you add via an .oidlib file do not contain any status definitions and result in the Warning status of the sensor by default because of the entry `undefinedState="Warning"`.

**i** If you use an SNMP Custom String Lookup sensor, you can create a new custom lookup definition in the \lookups\custom subfolder with the expected return values. In this case, use the [lookupname](#) of the chosen library as **id** parameter to override the lookups from the .oidlib file.

**i** When you save an edited lookup, make sure that you save it as an .ov file. Otherwise, the lookup might accidentally be saved as a .txt file and might not be loaded.

#### Example for Lookups Customization

For example (for illustration purposes only), imagine you want

- the sensor to show the Warning status for all undefined values that the target device might return,
- to change the shown status for the return value 2 from the Down to the Warning status, and
- to add the state **None** (shown as the Unknown status) to the [example<sup>B1871</sup>](#) above.

Then take the following steps:

1. Copy the file `oid.paessler.hplaserjet.tonerstatus` to the \lookups\custom subfolder of the PRTG program directory.
2. Open this file with a text editor.
3. Leave the **id** value unchanged to prioritize the customized lookup file.
4. Insert the status definition for undefined values into the [ValueLookup](#) element:  
`undefinedState="Warning"`
5. Replace the state **Error** with **Warning** for value 2.
6. Add a [SingleInt](#) element with the state **None** for the (hypothetical) return value 3.
7. Save the file and [reload<sup>B1901</sup>](#) the custom lookup folder in PRTG.

The customized lookup file looks like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="oid.paessler.hp.laserjet.tonerstatus" desiredValue="1"
undefinedState="Warning" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="PaeValueLookup.xsd">
  <Lookups>
    <SingleInt state="OK" value="0">Toner Okay</SingleInt>
    <SingleInt state="Warning" value="1">Toner Low</SingleInt>
    <SingleInt state="Warning" value="2">No Toner Cartridge
Loaded</SingleInt>
    <SingleInt state="None" value="3">Unknown Status of Toner</SingleInt>
  </Lookups>
</ValueLookup>
```

■ See also the [SNMP Custom String Lookup](#) sensor for a lookup definition that maps a string value to a sensor status.

### desiredValue Attribute

It is necessary to define a [desiredValue](#) in the lookup files. The desiredValue corresponds to a [status value](#) that triggers a lookup. PRTG calculates the percentage of time this specific status was monitored. PRTG displays the result for all data tables and graphs that show averaged values.

Considering the example above where the desiredValue is **1**, PRTG calculates the percentage of time that the toner status showed the Warning status. If, during a time span of five minutes, four of five sensor scans returned [Warning](#), PRTG shows an average of 80% for this time span because 80% of the time, the sensor showed the Warning status.

**i** The desiredValue attribute always has to be an [integer](#). For the lookup type [Range](#), use an integer that you defined for one of your "from" or "to" parameters in the lookup file.

■ For more information, see the Knowledge Base: [Can I graph text values?](#)

### Lookup Types: SingleInt, Boolean, BitField, Range

Besides the lookup type [SingleInt](#) as seen above, there are three other lookup types: [Boolean](#), [BitField](#), and [Range](#). Using these types, you can define lookup values beyond simple integers.

Lookup Type	Description	Syntax
SingleInt	Use an <a href="#">integer</a> to define a lookup for one status value.	value="int" <b>i</b> PRTG supports the full 32-bit integer range.
Boolean	Use <b>0</b> or <b>1</b> to define a lookup for two different status values.	value="0" value="1"

Lookup Type	Description	Syntax
BitField	Use a <a href="#">bitfield</a> for multiple status values.	<p>Only use this lookup type if you have some basic knowledge of bitmasks. See section <a href="#">More</a><sup>[19]</sup> for a general introduction.</p> <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> Every value has to be zero (0) or has to equal a power of two (for example, 1, 2, 4, 8, 16, 32, 64, etc.).</li> <li><span style="color: red;">❗</span> The SNMP Custom String Lookup sensor does not support BitFields.</li> </ul>
Range	Use an inter range <a href="#">from-to</a> to define a lookup for several status values.	<p>from="int" to="int"</p> <ul style="list-style-type: none"> <li><span style="color: red;">❗</span> Using ranges, the parameters "from" and "to" must always be defined. If you want to query only one single value in a range file, this value must be set as a parameter for "from" <b>and</b> "to" (for example, from="2" to="2").</li> <li><span style="color: red;">❗</span> The SNMP Custom String Lookup sensor does not support ranges.</li> <li><span style="color: red;">❗</span> The full 32-bit integer range is supported.</li> </ul> <p><span style="color: blue;">■</span> For more information, see the Knowledge Base: <a href="#">Custom lookup range</a>.</p>

❗ You can use only **one** kind of lookup type in **one** lookup file. This means, only [SingleInt](#), only [Boolean](#), only [BitField](#), or only [Range](#). Different lookup types in one file are not allowed.

## Define Lookup Files in Channel Settings


For each sensor with a custom channel, you can define a lookup file to use with the option Lookup in the channel settings. This option is visible for many SNMP sensors, some application sensors, and always for the following sensors:

- [EXE/Script](#)
- [EXE/Script Advanced](#) (if you define a Custom unit)
- [SNMP Custom](#)

■ For more information, see section [Channel Settings](#)<sup>[268]</sup>.

## Loading Lookups

You can (re)load the lookups in the custom folder by going to Setup | System Administration | [Administrative Tools](#)<sup>[291]</sup> in the PRTG web interface and clicking Go! under Load Lookups and File Lists.

 A sensor whose lookup file you have modified and reloaded does not re-evaluate this lookup before the next sensor scan. For sensors with long scanning intervals, use the Scan Now option from the [context menu](#)<sup>[229]</sup> to immediately apply the new lookup definition and to avoid an incorrect sensor status.

## Debugging

What happens if...

- a return value is defined in the lookups that is never returned by a device because the value is not assigned? The value is never triggered, so PRTG ignores this entry.
- PRTG receives a return value that is not defined for lookups? No substitution message can be found. PRTG only shows the return value. You can optionally define a status for unknown values with a definition of [undefinedState](#) in the [ValueLookup](#) element (see section [The XML Schema](#)<sup>[185]</sup>).
- different lookup types are in one lookup file? This is not allowed and PRTG discards this lookup definition. If you use miscellaneous lookup types in one file, for example, ranges and SingleInts together, PRTG creates a ticket when loading lookups or restarting the PRTG core server with the following error message: [Lookup file "\[...\]" could not be loaded \(" " is not a valid integer\)](#).
- XML code is incorrect? PRTG creates a new ticket when it loads lookups or restarts the PRTG core server with a corresponding error message and discards this lookup definition.
- a lookup file has a file extension other than [.ovm](#)? The file is not loaded.
- alerting is disabled or based on limits? [Error](#) and [Warning](#) states that are defined in the lookup do not apply. Make sure that you select the option Enable alerting based on lookups in the channel settings if you want to use lookup definitions to control the sensor status.
- you define a scaling factor in channel settings? This does not modify the values that are defined by lookups. Any applied lookup always uses the raw value as retrieved from the target device. If you use a scaling factor for such a channel, you notice the scaling in data graphs but the channel value appears unmodified in data tables.

## More

### KNOWLEDGE BASE

Custom lookup range

- <https://kb.paessler.com/en/topic/55493>

Can I graph text values?

- <https://kb.paessler.com/en/topic/73062>

### VIDEO TUTORIAL

How to configure lookups in PRTG

- <https://www.paessler.com/support/videos-and-webinars/videos/prtg-lookups>

### PAESSLER TOOLS

MIB Importer

- <https://www.paessler.com/tools/mibimporter>

## 14.7 Regular Expressions

For some sensors, you can use regular expressions (regex) to match a search pattern. PRTG supports Perl Compatible Regular Expression (PCRE).

The following sensors support regex:

- [DHCP](#)
- [File Content](#)
- [HTTP Advanced](#)
- [IMAP](#)
- [Port](#)
- [SNMP Custom String](#)
- [WMI Custom String](#)

**i** You can only use regex for the respective sensors if you explicitly enable regex in the sensors' settings.

**i** PRTG supports regex options in the form [\(?ismxUJ\)](#) and their negations, for example, [\(?-i\)](#). PRTG does not support regex flags like [/g](#) (global), [/s](#) (single line), or [/gs](#), and does not correctly search for the target string if you try to set flags.

### Common Search Patterns

Find matches that contain the word [error](#) or [alarm](#):

```
\b(error|alarm)\b
```

Find matches that contain the word [ERROR](#), not [error](#), using case sensitivity:

```
(?-i)\bERROR\b
```

Find matches that contain the words [error](#) and [alarm](#), in any order:

```
(?=.*\berror\b)(?=.*\balarm\b).*
```

Find matches that contain all of the words [tree](#), [flower](#), [leaf](#), and [bug](#), in any order:

```
(?=.*\btree\b)(?=.*\bflower\b)(?=.*\bleaf\b)(?=.*\bbug\b).*
```

**i** It is not possible to match an empty string with the regex search with sensors.

### Example

The search pattern

```
(?i)(?=.*\berror\b)(?=.*\balarm\b).*
```

matches the following expressions:

- Alarm error
- Error alarm

- I am an error and I trigger an alarm.
- I am an alarm and I indicate an error.
- An alarm combined with an error indeed!
- An error combined with an alarm, too!



## 14.8 Calculating Percentiles

PRTG not only monitors your network and informs you in the case of issues that are worth a closer look, it also stores a lot of historic data that it gathers from your sensors. This means that you have a base for the statistical analysis and evaluation of what is and was happening in your network. When you create a [report](#)<sup>[2754]</sup> or a [historic data report](#)<sup>[188]</sup>, you get raw data, sums, averages, and percentages of your monitoring data.

Additionally, PRTG also offers percentile calculation. This statistical method arranges your data, for example, from the lowest value to the highest value, and calculates the percentile that you want, optimally informing you about the distribution of your network-relevant data.

**i** For example, if you request the 95th percentile, you know that 95 percent of the measured data is below a certain value and PRTG can tell you what this certain value is.

If applied to bandwidth, for example, you know which values you have when talking about the 5 percent of unusually high bandwidth consumption, and which value your users do not exceed 95 percent of the time. Service providers often use percentiles to offer billing that excludes infrequent usage peaks.

**■** If you want to know more about the formula that PRTG uses for percentile calculation, see the Knowledge Base: [What are percentiles and what differences do they make in PRTG reports?](#)

### More

#### **■** KNOWLEDGE BASE

What are percentiles and what differences do they make in PRTG reports?

- <https://kb.paessler.com/en/topic/9563>

## 14.9 Add Remote Probe

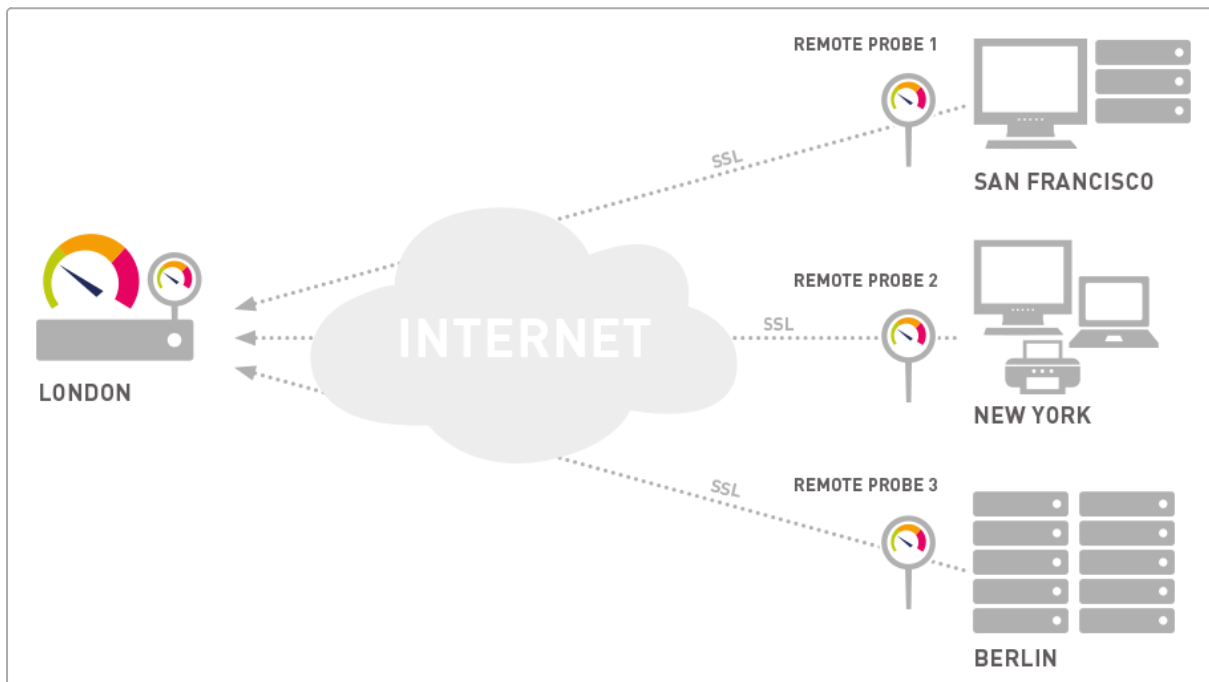
Remote probes can extend your monitoring with PRTG:

- Monitor different subnetworks that are separated from your PRTG core server by a firewall, and keep an eye on remote locations. You can install [one or more remote probes](#)<sup>[3198]</sup>.
- Distribute monitoring load by taking it from the PRTG core server system and putting it on one or more remote probe systems.

☁ You need a classic remote probe if you want to monitor your local network with a PRTG Hosted Monitor instance.

There are three types of remote probes:

1. [Classic remote probe](#)<sup>[3313]</sup>
2. [Multi-platform probe](#)<sup>[3316]</sup>
3. [Mini probe](#)<sup>[3316]</sup>



Monitoring Remote Locations via Remote Probes

### Classic Remote Probe

For more information on how to add a classic remote probe, see the following sections:

- Background information: [Remote Probes and Multiple Probes](#)<sup>[3198]</sup>
- Step-by-step installation: [Install a Remote Probe](#)<sup>[106]</sup>
- Partially automatic installation: [Classic Remote Probe Setup via Device Tools](#)<sup>[3202]</sup>
- Quick installation guide on the Paessler website: [How to install a PRTG remote probe in 4 steps](#)

## Multi-Platform Probe

For more information on how to add a multi-platform probe, see the [Multi-Platform Probe for PRTG](#) manual.

## More

### PAESSLER WEBSITE

How to install a PRTG remote probe in 4 steps

- <https://www.paessler.com/support/how-to/remote-probe-installation>

How to connect PRTG through a firewall in 4 steps

- <https://www.paessler.com/support/how-to/firewall>

### VIDEO TUTORIAL

Distributed monitoring with PRTG

- [https://www.paessler.com/support/videos-and-webinars/videos/distributed\\_monitoring](https://www.paessler.com/support/videos-and-webinars/videos/distributed_monitoring)

## 14.9.1 Remote Probes and Multiple Probes

Upon installation, PRTG automatically creates the first probe, namely the local probe in PRTG Network Monitor, and the hosted probe in PRTG Hosted Monitor. They run on the PRTG core server system and monitor all reachable devices, servers, and services from the system, using the sensors you configure.

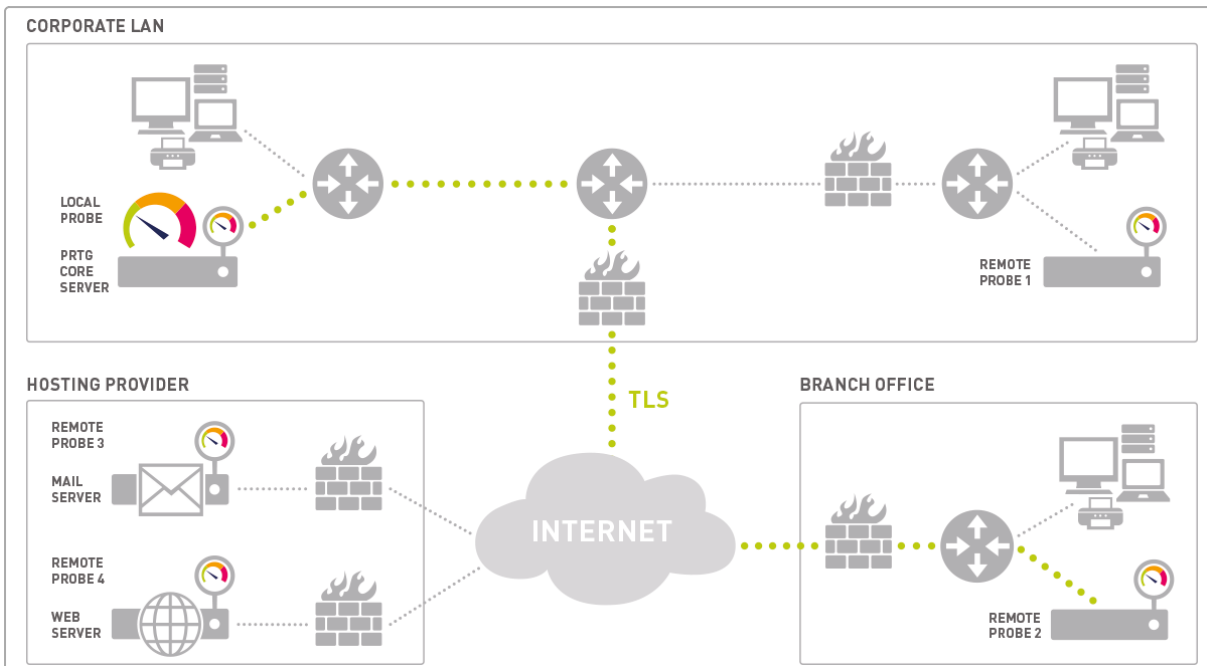
Working only with a local probe should suffice for LAN monitoring with PRTG Network Monitor and if you want to monitor one location only. For LAN monitoring with PRTG Hosted Monitor, at least one classic remote probe is required because the hosted probe can only reach targets that are publicly available via the internet.

### Scenarios That Require Remote Probes

There are several situations that make it necessary to work with remote probes in the same LAN or in remote locations:

- You use PRTG Hosted Monitor and want to monitor your local network.
- You have more than one location and you need to make sure that services are available from all locations.
- Your network is divided into several LANs that are separated by firewalls, and the local probe cannot monitor specific services across these firewalls.
- You want to monitor systems in a secure network and you need a secure connection between the PRTG core server and that network.
- You want to sniff packets on a different computer.
- You want to monitor NetFlow data on a different computer.
- You experience performance issues with CPU-intensive sensors like Packet Sniffer or NetFlow sensors and need to distribute the load among more than one computer.
- You want to monitor a non-Windows system. This is only possible with a [multi-platform probe](#)<sup>B316</sup>.

The following chart shows an example for a remote probe scenario.



Monitoring a Distributed Network with PRTG

The PRTG core server inside the [corporate LAN](#) (top left) can monitor:

- Services that are inside the [corporate LAN](#) using the [local probe](#).
- Services that are behind a firewall in the [corporate LAN](#) using [remote probe 1](#).
- Secured services that are inside the [branch office](#) (bottom right) using [remote probe 2](#).
- Secured services on [mail server](#) and [web server](#) using [remote probe 3](#) and [remote probe 4](#) installed directly on these servers.
- Public services on the internet using any of the probes.

## How Probes Work

As soon as a probe starts, it automatically connects to the [PRTG core server](#)<sup>[125]</sup>, downloads the sensor configuration, and begins its monitoring tasks. The PRTG core server sends new configuration data to a probe as soon as the user changes the monitoring configuration. Probes monitor autonomously and send the monitoring results back to the PRTG core server for each check that they perform.

If the connections between the PRTG core server and a probe fail for any reason (for example, restarting the PRTG core server system), the probe continues to monitor and stores the results. During a connection loss, a buffer stores a maximum of **500,000** sensor results in the RAM of the remote probe system (up to 50 - 200 MB). This means that for 100 sensors with a 1-minute scanning interval, the probe can buffer the monitoring results of up to 3 days (or 52 minutes for 10,000 sensors with a 1-minute scanning interval). The probe automatically reconnects to the PRTG core server as soon as it is available again and transmits all monitoring results that it gathered during the connection loss.

The connection between a probe and the PRTG core server is initiated by the probe and is secured with Secure Sockets Layer (SSL)/Transport Layer Security (TLS). This means that the data that is sent back and forth between the PRTG core server and the probe is not visible to someone that is capturing data packets. The PRTG core server provides an open TCP/IP port and waits for connection attempts from probes. If a new probe connects for the first time, you receive a ToDo [ticket](#)<sup>[213]</sup> and then you see the new probe in the device tree.

As a security precaution, you must manually approve the probe in the device tree before you can create any sensors. You can also deny a probe. PRTG then disconnects it. PRTG accepts no further connection attempts and it adds the probe IP address to the Deny IP Addresses list in the probe's [system settings](#)<sup>[2887]</sup>. This makes sure that unauthorized probes cannot connect to a PRTG core server.

Because the remote probe initiates the connection, you must make sure that a connection to your PRTG core server from the outside can be established. The process is the same as if you wanted to allow access to the PRTG web server provided by the PRTG core server via port 80 or 443. In most cases, this means that you will require an [allow](#) or [allow-nat](#) network address translation (NAT) rule that enables a remote probe to reach the PRTG core server via the Transmission Control Protocol (TCP) port [23560](#). Then, the remote probe uses a dynamic port from the high port range ([49152 - 65535](#)) for outgoing connections.

☁ For remote probe connections to PRTG Hosted Monitor instances, the above also applies with the main difference that you only have to configure the remote probe side so that the outgoing connection to your PRTG Hosted Monitor (DNS name or underlying IP address) is possible and is reachable under this specific port.

If you run PRTG in a cluster, remote probes also connect to all cluster nodes and send monitoring data. This works as described above for a single PRTG core server. If the master node fails, you can still see monitoring data on the failover nodes. You can define the Cluster Connectivity of each probe in the probe's [settings](#)<sup>[521]</sup>, section Administrative Probe Settings.

## Automatic Probe Update

Whenever you install a new version of PRTG on the PRTG core server, all classic remote probes automatically download and install the updated version as soon as they reconnect to the updated PRTG core server.

❗ PRTG does not automatically update multi-platform probes. If you installed a multi-platform probe via the Paessler Linux package repository, your package manager notifies you when there is an update. Otherwise, manually update your multi-platform probes with the updated package. For more information, see the [Multi-Platform Probe for PRTG](#) manual.

PRTG updates the local probe when you update the PRTG core server. All classic remote probes automatically download the new binaries via the SSL/TLS-secured probe connection or PRTG core server connection. Downloading the 4 MB file takes anywhere from a few seconds (in LANs) up to a few minutes (via internet connections), depending on the available bandwidth. As soon as the update is downloaded, the remote probe disconnects, installs the update, and reconnects to the PRTG core server. This takes between 20 and 100 seconds. Note that during the update phase, monitoring by the local probe can be affected because of the bandwidth that is required for the downloads.

❗ If a classic remote probe keeps disconnecting after an update, check if the server with the remote probe has two network connections with different IP addresses. Make sure that these addresses are in the list of allowed IP addresses in the [Core & Probes](#)<sup>[2890]</sup> settings.

## Delete Remote Probe

If you delete a connected remote probe via the device tree, it stops the [PRTG probe service](#) on the remote probe system and sets the startup type to manual. We recommend that you additionally uninstall the remote probe on the remote probe system.

If you delete a disconnected remote probe, it does not stop the [PRTG probe service](#) on the remote probe system and does not affect the startup type. The remote probe will continue to try to reconnect to the PRTG core server until you manually stop the PRTG probe service or uninstall the remote probe on the remote probe system.

## More

### PAESSLER WEBSITE

How to connect PRTG through a firewall in 4 steps

- <https://www.paessler.com/support/how-to/firewall>

### KNOWLEDGE BASE

What is the multi-platform probe and how can I use it?

- <https://kb.paessler.com/en/topic/90140>

### VIDEO TUTORIAL

Distributed monitoring with PRTG

- [https://www.paessler.com/support/videos-and-webinars/videos/distributed\\_monitoring](https://www.paessler.com/support/videos-and-webinars/videos/distributed_monitoring)

## 14.9.2 Classic Remote Probe Setup via Device Tools

You can directly install a classic remote probe via the [context menu](#)<sup>[229]</sup> of a device in the device tree. This partially automatic installation mechanism is an alternative to the [Classic Remote Probe Installer](#)<sup>[106]</sup>. For a quick installation guide, see the Paessler website: [How to install a PRTG remote probe in 4 steps](#).

**i** This is an experimental feature. It might not work in all situations. In this case, see section [Debugging](#)<sup>[3206]</sup>.

**☁** This feature is not available in PRTG Hosted Monitor.

**i** You cannot install a remote probe on the local probe device or hosted probe device. The Classic Remote Probe Setup via Device Tools is also not available for devices on remote probes. In this case, use the Classic Remote Probe Installer.

**i** If you run PRTG in a cluster, see [Cluster and Remote Probes Outside the LAN](#)<sup>[8204]</sup>.

### Steps to Take

To install a remote probe directly from the device tree in the PRTG web interface, follow these steps:

- [Step 1: Meet the Requirements](#)<sup>[3202]</sup>
- [Step 2: Prepare the PRTG Core Server](#)<sup>[3203]</sup>
- [Step 3: Configure the Failover Node](#)<sup>[3204]</sup>
- [Step 4: Confirm the Failover Node](#)<sup>[3205]</sup>
- [Step 5: Approve the New Remote Probe](#)<sup>[3206]</sup>

### Step 1: Meet the Requirements

To install a classic remote probe on a target system, make sure that you meet the following requirements:

- The target system runs on at least Windows 7.
- The target system is accessible via remote procedure call (RPC). This is usually the case when your PRTG core server and the target system are located in the same LAN segment. Otherwise, open Windows [services.msc](#) on the target system and start the RPC service.
- Programs are allowed to communicate through your Windows Firewall. Open the settings of your firewall and select Allow an app through firewall. Mark the check box for Remote Service Management, and the check box Public in the corresponding line.
- Because the remote probe initiates the connection, you must make sure that a connection to your PRTG core server from the outside can be established. The process is the same as if you wanted to allow access to the PRTG web server provided by the PRTG core server via port 80 or 443. In most cases, this means that you will require an [allow](#) or [allow-nat](#) network address translation (NAT) rule that enables a remote probe to reach the PRTG core server via the Transmission Control Protocol (TCP) port [23560](#). Then, the remote probe uses a dynamic port from the high port range ([49152 - 65535](#)) for outgoing connections.

**■** If you need to set a different port, which we do not recommend, see the Knowledge Base: [How can I customize ports for core-probe connections used by PRTG?](#)



**i** You cannot install a remote probe on a system that already has a probe installed.

**■** For more information on the requirements for remote probes, see section [System Requirements](#) <sup>23</sup>.

## Step 2: Prepare the PRTG Core Server

**i** Because remote probes need to connect to your PRTG core server, PRTG needs to accept incoming remote probe connections. So, with PRTG Network Monitor, first prepare your PRTG core server before you install a remote probe.

Edit the relevant settings in section [Core & Probes](#) <sup>2887</sup>. From the main menu in the [PRTG web interface](#) <sup>1241</sup>, select Setup | System Administration | Core & Probes to access the probe settings and go to the Probe Connection Settings.

### Probe Connection Settings

**Probe Connection IP Addresses** <sup>1</sup>

Local probe only, 127.0.0.1

All IP addresses available on this computer

Specify IP addresses

**Access Keys** <sup>1</sup>

**Allow IP Addresses** <sup>1</sup>

**Deny IP Addresses** <sup>1</sup>

**Deny GIDs** <sup>1</sup>

**Connection Security** <sup>1</sup>

High security (TLS 1.3, TLS 1.2)

Default security (TLS 1.3, TLS 1.2) (recommended)

Weakened security (TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0)

**Mini Probes** <sup>1</sup>

Do not allow mini probes (default)

Allow mini probes to connect to the PRTG web server

Allow mini probes to connect to an extra port

**PRTG MultiBoard File Transfer** <sup>1</sup>

Disable (default)

Enable

Probe Connection Settings in System Administration

### Step 2.1: Probe Connection IP Addresses

By default, a PRTG core server accepts connections from the local probe only (IP address [127.0.0.1](#)). This setting is the most secure setting, but it does not allow any remote probes to connect to your PRTG core server.

To accept remote probes, select one of the following settings:

- All IP addresses available on this computer: Any IP address on your PRTG core server system accepts incoming probe connections.
- Specify IP addresses: Specify IP addresses that accept incoming connections.


### Step 2.2: Allow IP Addresses


In the Allow IP Addresses field, you can enter the IP address of the target system on which you want to install a remote probe. You can also enter the word [any](#). This sets the PRTG core server to accept remote probe connections from any IP address.

 If you use [any](#), make sure that you only write the word in lower case. Other variations are not valid.


Other settings are not required. For more information about the fields for Access Keys, Deny IP Addresses, and Deny GIDs, see section [Core & Probes](#)<sup>[2890]</sup>.

When you are done, click Save to save your settings.

 If you change this setting, PRTG needs to restart the PRTG core server to apply your changes. After you click Save, a dialog box appears that asks you to confirm the restart. Click OK to trigger the restart. During the restart, all users of the PRTG web interface, the [PRTG app for desktop](#)<sup>[2984]</sup>, or the [PRTG Apps for Mobile Network Monitoring](#)<sup>[2988]</sup> are disconnected and reconnected.

 To edit the core-probe connection settings, you can also use the [PRTG Administration Tool](#)<sup>[3041]</sup> on your PRTG core server.

### Cluster and Remote Probes Outside the LAN

 If you run PRTG as a cluster and you want to run remote probes outside your local network, you must make sure that your cluster nodes and the addresses that they use are reachable from the outside. Check your cluster node settings under [Cluster](#)<sup>[2923]</sup> before you install a remote probe outside your local network. Enter valid Domain Name System (DNS) names or IP addresses for both cluster nodes to reach each other and for remote probes to individually reach all cluster nodes. Remote probes outside your LAN cannot connect to your cluster nodes if they use local addresses.



If you already have a remote probe installed outside your LAN and the remote probe is disconnected because of this, follow these steps:


1. Uninstall the remote probe.
2. Update the [cluster node settings](#)<sup>[2923]</sup> with addresses that are reachable from outside your LAN.
3. Restart the PRTG core servers.
4. Install the remote probe again. It then obtains the IP address or DNS name entries that it can reach.

 See also section [Failover Cluster Configuration](#)<sup>[3210]</sup>, section Remote Probes in a Cluster.



### Step 3: Configure the Failover Node

If you have not yet done so, [add a device](#)<sup>[364]</sup> that represents the target system on which you want to install the remote probe. Set the correct Windows credentials for this device.

1. Open the [device settings](#) .
2. In the Credentials for Windows Systems section, provide Domain or Computer Name, User Name, and Password for the target system. You can also [inherit](#)  the credentials from the settings of a parent object in the device tree.

 Make sure that this user account has administration rights on the target system.

## Step 4: Confirm the Failover Node

1. In the device tree, open the [context menu](#) .
2. Select Device Tools | Install Remote Probe to open the install dialog in a new window.
  -  This option is only available for devices on the local probe of PRTG Network Monitor.






**Install Remote Probe on Device Workstation**

Please note: This is an experimental feature, it might not work in all situations. Please send your feedback to [support@paessler.com](mailto:support@paessler.com).

You are about to install a remote probe on the computer "Workstation". This will allow PRTG to monitor this computer locally instead of using remote monitoring features. This can sometimes be a good workaround for performance or authentication problems (for example, for WMI sensors). Additionally, this will allow you to use some probe-only sensors like Packet Sniffer, NetFlow, and others.

---

**Details**

Device Name	 Workstation
Status	OK
Priority	★★★★☆
Parent Probe	 Probe (Local Probe) 
Parent Group	 Servers
Sensors by State	 2 (Total: 2)

---

**Prerequisites**

Please make sure you fulfill the following conditions.

- The target device must be a computer with a supported Windows version.
- The target computer must be accessible through RPC (this is usually the case when your PRTG server and the target computer are located in the same LAN segment).
- Open or forward port 23560 in your firewall to allow connections between the probe and your PRTG core server.
- Windows credentials must be set in the [device settings](#) or its parents' settings (current user name: paesslergmbh\Testadmin) and the user account must have administration rights on the target machine.
- You have to allow remote probe connections to your PRTG core server. Open the **Core & Probes** tab in the System Administration of your PRTG web interface. In section **Probe Connection Settings**, select the option **All IPs available on this computer** or specify IPs for the setting **Probe Connection IPs**. Do not use the "Local Probe only" (127.0.0.1) setting! (Current setting: 10.0.0.1)

---

**Start Probe Installation**

The installation will take between 10 and 100 seconds.

[Install Remote Probe on "Workstation"](#)

Remote Probe Installation Dialog

The install dialog includes four sections:

- Experimental feature notice and short introduction
- Details: Overview of the device like Device Name, Status, Priority, Parent Probe, Parent Group, and Sensors by Status.
- Prerequisites: Make sure that you meet the requirements listed here. If not, PRTG cannot start the installation process. Open requirements are highlighted in red.

#### Prerequisites

Please make sure you fulfill the following conditions.

- The target device must be a computer with a supported Windows version.
- The target computer must be accessible through RPC (this is usually the case when your PRTG server and the target computer are located in the same LAN segment).
- Open or forward port 23560 in your firewall to allow connections between the probe and your PRTG core server.
- You cannot install a remote probe on a probe device.
- Windows credentials must be set in the device settings or its parents' settings (current user name: test\test) and the user account must have administration rights on the target machine.
- **Please correct before proceeding:** You have to allow remote probe connections to your PRTG core server. Open the Core & Probes tab in the System Administration of your PRTG web interface. In section Probe Connection Settings, select the option All IPs available on this computer or specify IPs for the setting Probe Connection IPs. Do not use the "Local Probe only" (127.0.0.1) setting! (Current setting: 127.0.0.1)

Installation Unable to Start Because Prerequisites Are Not Met

- Start Probe Installation: Time estimation for the installation and installation start button

If all prerequisites are met, you can install the remote probe on the target system by clicking Install Remote Probe on "[device name]". Wait until the process has ended. If the installation is successful, the following message appears in the Start Probe Installation section: **Done. Result is: OK.**

- ① Every time you start an installation, PRTG automatically adds a new key to the field Access Keys in the [Core & Probes](#) settings, no matter if the installation is successful or not.

## Step 5: Approve the New Remote Probe

If the installation is successful, you receive further instructions after the result message. You also receive a new [ToDo ticket](#).

Click Approve and auto-discover to acknowledge the new remote probe and to instantly start an [auto-discovery](#) in this network. Click Approve new probe to acknowledge the new remote probe without running an auto-discovery. You can also discard the remote probe by clicking Deny.

- ① When you deny or remove a remote probe, this device's global ID (GID) is listed in the Deny GIDs field in the [Core & Probes](#) settings. Future probe connections from this device are automatically denied.

- ① When you deny the remote probe in the device tree, this does **not** uninstall the remote probe but only denies access to the PRTG core server. The remote probe continues to run on the target system until you uninstall it manually.

Wait while the remote probe connects. Once the remote probe has connected, you can create groups, devices, and sensors to customize your monitoring via the new remote probe.

## Debugging

- Note that installing a remote probe directly from the device tree in the PRTG web interface is an experimental feature. This approach might not be possible in all situations.
- Make sure you meet all the requirements as described in [step 1](#) such as the Windows Firewall settings.
- If the quick installation procedure as described in this section does not work with your setup, manually install the remote probe via the Classic Remote Probe Installer as described in section [Install a Remote Probe](#).

## More

**KNOWLEDGE BASE**

How can I customize ports for core-probe connections used by PRTG?

- <https://kb.paessler.com/en/topic/65084>

## ■ PAESSLER WEBSITE

How to connect PRTG through a firewall in 4 steps

- <https://www.paessler.com/support/how-to/firewall>

How to install a PRTG remote probe in 4 steps

- <https://www.paessler.com/support/how-to/remote-probe-installation>

## 14.10 Failover Cluster Configuration

A failover cluster consists of two or more PRTG core servers that work together to form a high availability monitoring system. PRTG offers the single failover cluster (one master node and one failover node) in all licenses, including the freeware edition.

☁ This feature is not available in PRTG Hosted Monitor.



Illustration of a Single Failover Cluster

■ For more information about clusters in general, see section [Failover Cluster](#)<sup>[128]</sup>.

### Before You Start

Consider the following notes about clusters:

- You need two target systems that run any Windows version (as of Windows 7). The target systems can be physical machines or virtual machines (VM). For more information, see section [System Requirements](#)<sup>[22]</sup>.
- The machines must be up and running.
- The machines must be similar in regard to the system performance and speed (like CPU, RAM, etc.).
- In a cluster, each of the cluster nodes individually monitors the devices that you add to the cluster probe. This means that the monitoring load increases with every cluster node. Make sure that your devices and your network can handle these additional requests. Often, a longer scanning interval for your entire monitoring setup is a good idea. For example, set a scanning interval of five minutes in the root group's [settings](#)<sup>[420]</sup>.
- We recommend that you install PRTG on dedicated, physical machines for best performance.
- Keep in mind that a machine that runs a cluster node might automatically restart without prior notice, for example, because of special software updates.
- Both machines must be visible for each other through the network.
- Communication between the two machines must be possible in **both directions**. Make sure that no software or hardware firewall blocks communication. All communication between cluster nodes is directed through one specific Transmission Control Protocol (TCP) port. You define the port during the cluster setup. By default, it is TCP port [23570](#).

- In a cluster, a Domain Name System (DNS) name that you enter under Setup | System Administration | User Interface in the PRTG web interface is only used in links that point to the master node. You cannot enter a DNS name for a failover node. This means that any HTTP or HTTPS links that point to a failover node (for example, in notifications or in maps) always point to the failover node's IP address in your local network and might therefore not be reachable from external networks or from the internet, particularly if you use network address translation (NAT) rules.
- Email notifications for failover: The failover master node sends notifications if the primary master node is not connected to the cluster. To make sure that PRTG can deliver emails in this case, configure the [notification delivery](#) settings so that PRTG can use them to deliver emails from your failover node as well. For example, use the option to set up a secondary Simple Mail Transfer Protocol (SMTP) email server. This fallback server must be available for the failover master node so that it can send emails over it independently from the first email server.
- Make your machines secure. Every cluster node has full access to all stored credentials, other configuration data, and the monitoring results of the cluster. Also, PRTG software updates can be deployed from every cluster node. So, make sure you take security precautions to avoid security attacks like hackers and Trojans. Secure every cluster node as carefully as the master node.
- Run cluster nodes either on 32-bit or 64-bit Windows versions only. Avoid using both 32-bit and 64-bit versions in the same cluster. This configuration is not supported and might result in an unstable system. Also, ZIP compression for the cluster communication is disabled and you might encounter higher network traffic between your cluster nodes.
- If you run cluster nodes on Windows systems with different time zone settings and you use [schedules](#) to pause monitoring of sensors, the schedules apply **at the local time of each cluster node**. Because of this, the overall status of a particular sensor is shown as Paused every time the schedule matches a cluster node's local system time. Use the same time zone setting on each Windows system with a cluster node to avoid this behavior.
- The password for the **PRTG System Administrator** user account is not automatically synchronized on cluster nodes. The default credentials (**prtgadmin**) for the **PRTG System Administrator** user account do not work on the failover node. For more information, see the Knowledge Base: [I cannot log in to my failover node anymore. What can I do?](#)
- Stay below 2,500 sensors per cluster for best performance in a single failover. Clusters with more than 5,000 sensors are not officially supported. For each additional failover node, divide the number of sensors by two.

In cluster mode, you cannot use sensors that wait for data to be received. Because of this, you can use the following sensors only on a [local probe or remote probe](#):

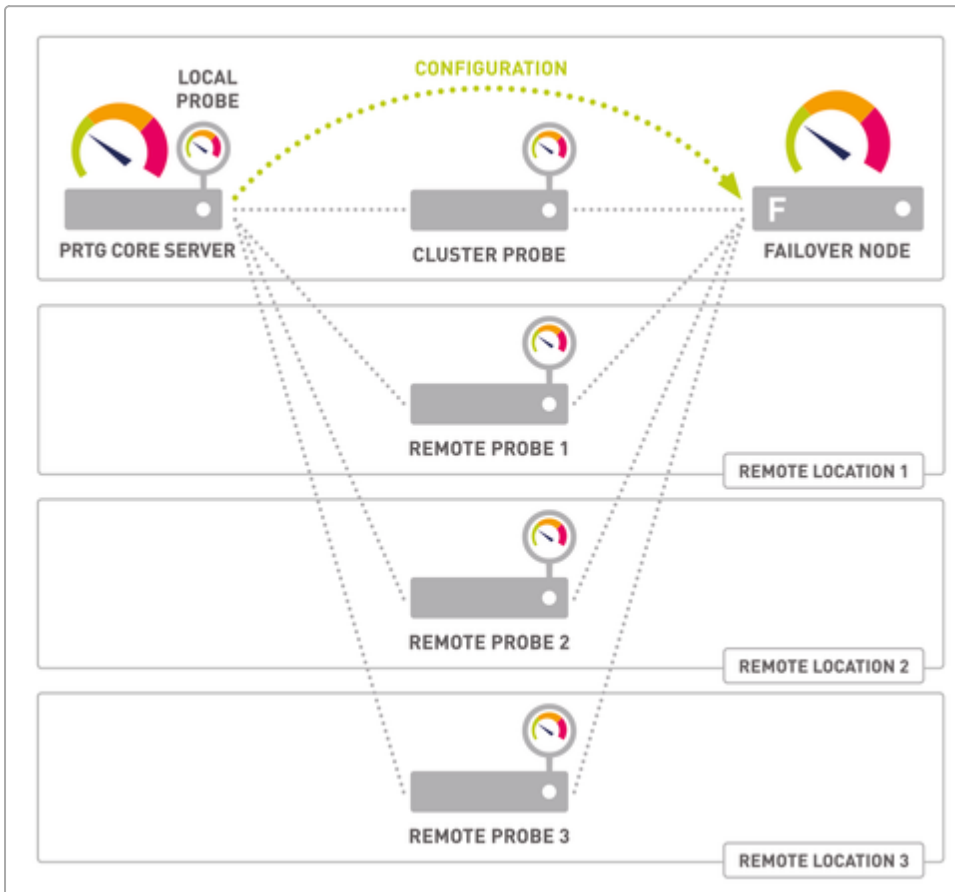
- [DHCP](#)
- [HTTP Push Count](#)
- [HTTP Push Data](#)
- [HTTP Push Data Advanced](#)
- [IPFIX](#) and [IPFIX \(Custom\)](#)
- [jFlow v5](#) and [jFlow v5 \(Custom\)](#)
- [NetFlow v5](#) and [NetFlow v5 \(Custom\)](#)
- [NetFlow v9](#) and [NetFlow v9 \(Custom\)](#)
- [Packet Sniffer](#) and [Packet Sniffer \(Custom\)](#)
- [sFlow](#) and [sFlow \(Custom\)](#)
- [SNMP Trap Receiver](#)

- [Syslog Receiver](#)

## Remote Probes in a Cluster

PRTG provides cluster support for classic remote probes. This means that all of your classic remote probes can connect to all of your cluster nodes. Because of this, you can still see the monitoring data of classic remote probes and sensor warnings and errors even when your master node fails.

- ❗ You cannot add multi-platform probes to a cluster. For more information about the multi-platform probe, see the [Multi-Platform Probe for PRTG](#) manual.



Remote Probes with Cluster Connectivity

Consider the following notes about clusters with classic remote probes:

- You must allow remote probe connections to your failover nodes. To do so, log in to each system in your cluster and open the [PRTG Administration Tool](#)<sup>[3046]</sup>. On the PRTG Core Server tab, accept connections from remote probes on each cluster node.
- If you use remote probes [outside your local network](#): You must use IP addresses or Domain Name System (DNS) names for your cluster nodes that are valid for both the cluster nodes to reach each other and for remote probes to reach all cluster nodes individually. Open the [Cluster](#)<sup>[2923]</sup> settings and adjust the entries for cluster nodes accordingly so that these addresses are reachable from the outside. New remote probes try to connect to these addresses but cannot reach cluster nodes that use private addresses.



- If you use network address translation (NAT) with remote probes [outside the NAT](#): You must use IP addresses or DNS names for your cluster nodes that are reachable from the outside. If your cluster nodes are inside the NAT and the cluster configuration only contains internal addresses, your remote probes from outside the NAT are not able to connect. The PRTG core server must be reachable under the same address for both other cluster nodes and remote probes.
  - A remote probe only connects to the PRTG core server with the defined IP address when it starts.
    - ❗ This PRTG core server must be the primary master node.
  - Initially, remote probes are not visible on failover nodes. You need to set their Cluster Connectivity first in the [Administrative Probe Settings](#)<sup>[521]</sup> for them to be visible and to work with all cluster nodes. Select Remote probe sends data to all cluster nodes for each remote probe that you want to connect to all cluster nodes.
  - Newly connected remote probes are visible and work with all cluster nodes immediately after you acknowledge the probe connection. The connectivity setting Remote probe sends data to all cluster nodes is default for new remote probes.
  - As soon as you activate a remote probe for all cluster nodes, it automatically connects to the correct IP addresses and ports of all cluster nodes.
  - Once a remote probe has connection data from the primary master node, it can connect to all other cluster nodes also when the primary master node fails.
  - Changes that you make in the connection settings of cluster nodes are automatically sent to the remote probes.
  - If a PRTG core server (cluster node) in your cluster is not running, the remote probes [deliver monitoring data](#)<sup>[519]</sup> after the PRTG core server restarts. This happens individually for each PRTG core server in your cluster.
  - If you enable cluster connectivity for a remote probe, it does not deliver monitoring data from the past when cluster connectivity was disabled. For sensors that use difference values, the difference between the current value and the last value is shown with the first new measurement (if the respective sensor previously sent values to the PRTG core server).
  - Except for this special case, all PRTG core servers show the same values for sensors on devices that you add to the cluster probe.
  - The PRTG core server that is responsible for the configuration and management of a remote probe is always the current master node. This means that only the current master node performs all tasks of the PRTG core server. If you use a split cluster with several master nodes, only the master node that appears first in the cluster configuration is responsible.
- ❗ You can use remote probes in a cluster as described above, which is showing monitoring data of all remote probes on all cluster nodes. However, you cannot cluster a remote probe itself. To ensure gapless monitoring for a specific remote probe, install a second remote probe on a machine in your network next to the remote probe. Then create all devices and sensors of the original remote probe on the second remote probe by [cloning](#)<sup>[2714]</sup> the devices from the original remote probe, for example. The second remote probe is then a copy of the first remote probe and you can still monitor the desired devices if the original remote probe fails.
- ❗ Remote probes that send data to all cluster nodes result in increased bandwidth usage. Select Remote probe sends data only to primary master node in the [probe settings](#)<sup>[521]</sup> for one or more remote probes to lower bandwidth usage if necessary.
- ❗ Explicitly check on each cluster node if a remote probe is connected. PRTG does not notify you if a remote probe is disconnected from a cluster node. For example, log in to the PRTG web interface on a cluster node and check in the device tree if your remote probes are connected.

## More

### ■ KNOWLEDGE BASE

What is the clustering feature in PRTG?

- <https://kb.paessler.com/en/topic/6403>

What are the bandwidth requirements for running a cluster?

- <https://kb.paessler.com/en/topic/8223>

What is a failover master node and how does it behave?

- <https://kb.paessler.com/en/topic/7663>

I need help with my cluster configuration. Where do I find step-by-step instructions?

- <https://kb.paessler.com/en/topic/41913>

Cluster: How do I convert a (temporary) failover master node to be the primary master node?

- <https://kb.paessler.com/en/topic/34853>

Are there alternatives to the cluster when running a large installation?

- <https://kb.paessler.com/en/topic/75474>

I cannot log in to my failover node anymore. What can I do?

- <https://kb.paessler.com/en/topic/89878>

What is the multi-platform probe and how can I use it?

- <https://kb.paessler.com/en/topic/90140>

### ■ PAESSLER WEBSITE

How to connect PRTG through a firewall in 4 steps

- <https://www.paessler.com/support/how-to/firewall>

How to set up a failover cluster in PRTG in 6 steps

- <https://www.paessler.com/support/how-to/failover-cluster>

## 14.11 Data Storage

PRTG stores the monitoring configuration, monitoring data, logs, tickets, and reports, as well as support and debug data into different subfolders in the PRTG data directory on the PRTG core server system. Additionally, there is data in the PRTG program directory (for example, scripts for your [custom sensors](#)<sup>[3213]</sup>) and in the Windows registry.

☁ You cannot access these directories in PRTG Hosted Monitor.

In this section:

- [PRTG Program Directory](#)<sup>[3213]</sup>
- [Subfolders in the PRTG Program Directory](#)<sup>[3213]</sup>
- [PRTG Data Directory](#)<sup>[3214]</sup>
- [Files and Subfolders in the PRTG Data Directory](#)<sup>[3214]</sup>
- [Structure of the Logs Folder](#)<sup>[3216]</sup>
- [Windows Registry](#)<sup>[3217]</sup>
- [HTTP Full Web Page Sensor: Cached Files](#)<sup>[3217]</sup>
- [Auto-Update Files](#)<sup>[3217]</sup>

### PRTG Program Directory

32-bit systems:

```
%programfiles%\PRTG Network Monitor
```

64-bit systems:

```
%programfiles(x86)%\PRTG Network Monitor
```

ⓘ These are the default paths. If you specified a different installation directory, you can find your data there.

### Subfolders in the PRTG Program Directory

You can find the following folders in the PRTG program directory:

Folder	Description
\cert	Certificates used by PRTG
\Custom Sensors	Custom sensor templates, custom scripts, and example scripts
\devicetemplates	Default and custom device templates
\download	Downloads from PRTG

Folder	Description
\lookups	Standard lookup files maintained by PRTG ⓘ The \lookups subfolder contains the \custom subfolder to store your customized lookups.
\MIB	Management Information Base (MIB) files referenced by sensors
\notifications	Custom notifications and notification sounds
\PRTG Installer Archive	PRTG Network Monitor installers for the currently installed version and the previously installed version
\python	Python environment files
\Sensor System	Sensor configuration files
\snmplibs	SNMP library files and converted .oidlib files
\webroot	PRTG web interface data

## PRTG Data Directory

On supported Windows versions:

```
%programdata%\Paessler\PRTG Network Monitor
```

ⓘ These are the default paths, depending on your Windows version. If you specified a custom path for data storage, you need to look it up in the [PRTG Administration Tool](#)<sup>[3046]</sup> on the PRTG Core Server tab. You can find the path there.

ⓘ The Windows ProgramData folder is hidden by default. To display it, you need to enable hidden items in the View options of your Windows system.

ⓘ You can find the supported Windows versions in section [System Requirements](#)<sup>[26]</sup>.

## Files and Subfolders in the PRTG Data Directory

You can find the following files in the PRTG data directory:

File	Description
PRTG Configuration.dat	Monitoring configuration (for example probes, groups, devices, sensors, users, maps, reports, and more)

File	Description
	<p><b>i</b> This configuration file is the central storage for all your credentials, such as passwords and secrets used by PRTG for authentication. Handle all configuration files as sensitive, even if there are already security measures in place in your system.</p> <p><b>■</b> For recommendations on how to handle your configuration files in a secure manner, see <a href="#">Handling Configuration Files</a> <sup>[3216]</sup> below.</p>
PRTG Configuration.old	Backup of previous version of monitoring configuration
PRTG Graph Data Cache.dat	Precalculated data for the graphs throughout the PRTG web interface (if missing, this file is automatically recalculated from the files in the monitoring database)

You can find the following folders in the PRTG data directory:

Folder	Description
\Configuration Auto-Backups	Backup versions of the PRTG Configuration.dat file
\Log Database	Database with the recent event history for the whole system: menu option Logs in the PRTG web interface
\Logs	Text file based logs <b>■</b> For more information, see section <a href="#">Structure of the Logs Folder</a> <sup>[3216]</sup>
\Monitoring Database	Results of all monitoring requests for all sensors (required for historic reports)
\Report PDFs	Older PDF <a href="#">reports</a> <sup>[2754]</sup> stored in the file system
\System Information Database	Retrieved <a href="#">system information</a> <sup>[205]</sup> for the categories hardware, users (loggedonusers), processes, services, software, system (in according subfolders)
\Ticket Database	Database with all <a href="#">tickets</a> <sup>[213]</sup> (ticketdata.dat)
\ToDo Database	Database with all ToDo entries <b>i</b> The ToDo feature is deprecated as of <a href="#">PRTG 14.1.8</a>

## Handling Configuration Files


Configuration files are the central storage for all your credentials, such as passwords and secrets used by PRTG for authentication. When you create a support bundle within PRTG that contains the configuration file, all secrets are removed or masked before the file is included in the support bundle.

Administrators should not depend solely on PRTG and their operating system (OS) to secure the configuration files, but rather ensure that the security and access control for these files are maintained during transit, deployment, and storage (e.g. backups). Handle all configuration files as sensitive, even if there are already security measures in place in your system.

Scenario	Example	Recommendations
In transit	<ul style="list-style-type: none"> <li>Sharing files to customer support</li> <li>Migration to a new server</li> </ul>	<ul style="list-style-type: none"> <li>Always use an encrypted or an offline channel to share the configuration files.</li> <li>Do not share the configuration files with untrustworthy third parties.</li> <li>Use the support bundle feature and share the raw configuration file only when specifically requested by support.</li> </ul>
In deployment	<ul style="list-style-type: none"> <li>Storing data in non-default paths</li> </ul>	<ul style="list-style-type: none"> <li>Ensure that any custom data path restrict access to those files to only users with high privileges (e.g. administrators).</li> <li>Use the default path whenever possible.</li> </ul>
In storage	<ul style="list-style-type: none"> <li>Backups (which includes the configuration files) in the same or alternative location</li> </ul>	<ul style="list-style-type: none"> <li>Any backup containing files with sensitive information, like the configuration file, should be protected in the same manner as the live system.</li> <li>Storing backups may erase or change the current access rights and result in more users being able to access the stored data. Always maintain the same level of access control on the paths where configurations files are stored as used in deployment.</li> </ul>

## Structure of the Logs Folder

Folder	Description
\appserver	Currently not in use

Folder	Description
\core	Text file based logs of the PRTG core server system and the cluster system
\debug	Text file based debug logs of the PRTG core server system and probe system, and PRTG core server cache recalculation
\desktopclient	Currently not in use
\enterpriseconsole	Text file based logs of the deprecated Enterprise Console
\probe	Text file based logs of the probe system
\probeadapter	Text file based logs of the probe adapter  The probe adapter supports multi-platform probe connections.
\sensordeprecation	Text file based log of deprecated sensors
\sensors	Text file based logs of sensors
\serveradmin	Text file based logs of the administration system
\webserver	HTTP server log files of the PRTG web server

## Windows Registry

System settings on 32-bit systems:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Paessler\PRTG Network Monitor
```

System settings on 64-bit systems:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Paessler\PRTG Network Monitor
```

## HTTP Full Web Page Sensor: Cached Files

If you use the HTTP Full Web Page, files might be cached in this directory:

```
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
```

## Auto-Update Files

PRTG automatically saves downloaded software versions in the \download subfolder of the PRTG program directory. The compressed prtg.zip file that contains all necessary files is also cached there.

## More

### ■ KNOWLEDGE BASE

What is the best way to contact the Paessler support team?

- <https://kb.paessler.com/en/topic/57993>














# Part 15

## Appendix

# 15 Appendix

Find more information about PRTG and used terms in the following sections:

- [Abbreviations](#)  3221
- [Available Sensor Types](#)  3232
- [Default Ports](#)  3288
- [Differences between PRTG Network Monitor and PRTG Hosted Monitor](#)  3293
- [Escape Special Characters and Whitespaces in Parameters](#)  3312
- [Glossary](#)  3313
- [Icons](#)  3322
- [Legal Notices](#)  3323
- [Placeholders for Notifications](#)  3325
- [Standard Lookup Files](#)  3335
- [Supported AWS Regions and Their Codes](#)  3350

## 15.1 Abbreviations

See below for a list of abbreviations used in this documentation.

### A

ACL	access control list
AD	Active Directory
ADO	ActiveX Data Objects
ADSL	asymmetric digital subscriber line
AES	Advanced Encryption Standard
AET	Application Entity Title
AIM	AOL Instant Messenger
AJAX	Asynchronous JavaScript and XML
API	application programming interface
ARP	Address Resolution Protocol
ASN.1	Abstract Syntax Notation One
AWS	Amazon Web Services

### B

BA	basic authentication
BMC	Baseboard Management Controller

### C

CA	certificate authority
----	-----------------------

CBQoS	Class Based Quality of Service
CGI	Common Gateway Interface
CIFS	Common Internet File System
CLI	command-line interface
CLR	common language runtime
COM	component object model
CPG	Common Provisioning Group
CRC	cyclic redundancy check
CSP	cloud solution provider
CSV	comma-separated values

## D

DAE	disk-array enclosure
DAG	Database Availability Group
DBMS	database management system
DC	domain controller
DCS	domain components
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DICOM	Digital Imaging and Communications in Medicine
DN	distinguished name
DNS	Domain Name System
DoS	denial of service

DPE	disk processor enclosure
DSCP	Differentiated Services Code Point
DTU	Database Transaction Unit

## E

EBS	Elastic Block Store
EC2	Elastic Compute Cloud
ECC	Elliptic Curve Cryptography
eDTU	elastic Database Transaction Unit
ELB	Elastic Load Balancing
EVA	Enterprise Virtual Array

## F

FAT	file allocation table
FCP	Fibre Channel Protocol
FIPS	Federal Information Processing Standards
Flow	Flow (NetFlow, jFlow, sFlow, IPFIX)
FQDN	fully qualified domain name
FTP	File Transfer Protocol
FTPS	FTP over SSL

## G

GID	global ID
GUID	globally unique identifier

H

HL7	Health Level 7
HTTP	Hypertext Transfer Protocol

I

I/O	input/output
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
ICPIF	Impairment Calculated Planning Impairment Factor
IDE	integrated development environment
iDRAC	Integrated Dell Remote Access Controller
IIS	Microsoft Internet Information Services
IKE	Internet Key Exchange
iLO	HPE Integrated Lights Out
IMAP	Internet Message Access Protocol
IMM	Integrated Management Module
IOPS	input/output operations per second
IoT	Internet of Things
IPC	Industrial PC
IPFIX	Internet Protocol Flow Information Export
IPMI	Intelligent Platform Management Interface
IPsec	Internet Protocol Security
IRC	Internet Relay Chat

iRMC	integrated Remote Management Controller
iSCSI	Internet Small Computer System Interface

## J

JSON	JavaScript Object Notation
JWKS	JSON Web Key Set

## L

L2L	LAN-to-LAN
LCU	load balancer capacity units
LDAP	Lightweight Directory Access Protocol
LIF	logical interface
LUN	logical unit number

## M

MD5	message-digest algorithm 5
MIB	Management Information Base
MOID	managed object identifier
MOS	mean opinion score
MQTT	Message Queue Telemetry Transport
ms	milliseconds
msec	milliseconds
MSH	message header
MSMQ	Microsoft Message Queuing

MSP	managed service provider
mutex	mutual exclusion
MWL	Modality Worklist

## N

NAS	network-attached storage
NAT	network address translation
NFS	network file system
NIC	network interface card
Nmap	Network Mapper
NSA	Network Security Appliance
NTFS	New Technology File System
NTLM	NT LAN Manager

## O

OAuth2	Open Authorization 2
ODBC	Open Database Connectivity
OID	object identifier
OLE DB	Object Linking and Embedding, Database
OMSA	OpenManage Server Administrator
ONTAPI	DATA ONTAP API
OPC UA	OPC Unified Architecture
OSPF	Open Shortest Path First



OU	organizational unit
----	---------------------

**P**

P2P	Peer-to-Peer
PACS	picture archiving and communication system
PAP	Password Authentication Protocol
PCRE	Perl Compatible Regular Expression
PDV	packet delay variation
PEM	Privacy-Enhanced Mail
PMPP	PRTG Mini Probe Protocol
POP3	Post Office Protocol version 3

**Q**

QNAP	Quality Network Appliance Provider
QoS	Quality of Service

**R**

RADIUS	Remote Authentication Dial-In User Service
RAID	redundant array of independent disks
RDP	Remote Desktop Protocol
RDS	Relational Database Service
Redfish	Redfish Scalable Platforms Management API
regex	regular expression
REST	Representational State Transfer

RMON	Remote Monitoring
RODC	Read-only Domain Controllers
RPC	remote procedure call
RPM	revolutions per minute
RST	number of reset
RTT	round-trip time
RTU	Remote Terminal Unit

## S

S.M.A.R.T.	Self-Monitoring, Analysis and Reporting Technology
SaaS	software as a service
SAN	storage area network
SASL	Simple Authentication and Security Layer
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SID	Oracle System ID
SIP	Session Initiation Protocol
SMB	server message block
SMTP	Simple Mail Transfer Protocol
SNI	Server Name Indication
SNMP	Simple Network Management Protocol
SNR	signal-to-noise ratio
SNS	Simple Notification Service

Sntp	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SPA	Single Page Application
SPAN	Switched Port Analyzer
SPN	Service Principal Name
SQL	Structured Query Language
SRP	Secure Remote Password
SSD	solid-state drive
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	single sign-on
SVC	switched virtual circuit

## T

TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
ToS	Type of Service
TOTP	Time-based One-time Password algorithm

## U

UAC	User Account Control
UCS	Unified Computing System

UDF	User-defined Function
UDP	User Datagram Protocol
UID	Unique Identifier
UNC	Universal Naming Convention
UPS	uninterruptible power supplies
URI	uniform resource identifier
UTC	Coordinated Universal Time
UUID	universally unique identifier

## V

vCore	virtual core
VM	virtual machine
VoIP	Voice over IP
VPN	virtual private network

## W

WBEM	Web-based Enterprise Management
WMI	Windows Management Instrumentation
WQL	Windows Management Instrumentation Query Language
WSAPI	Web Services API
WSUS	Windows Server Update Services
WWN	World Wide Name

X

XML	Extensible Markup Language
-----	----------------------------

## 15.2 Available Sensor Types

Here you can find a list of all available sensors, including their category, the version they were introduced in, their performance impact, IP version, meta-scan capability, device template capability, notification triggers, and what they monitor.

**i** In the [Add a Sensor](#) assistant, you have various options to filter for suitable sensors. You can also filter for device template capability, IP version, and meta-scan functionality, among others, via /sensorlist.htm, for example <https://yourserver/sensorlist.htm>.

In this section:

<ul style="list-style-type: none"> <li><a href="#">General</a></li> <li><a href="#">Backup and replication monitoring</a></li> <li><a href="#">Bandwidth monitoring</a></li> <li><a href="#">Beta sensors</a></li> <li><a href="#">Cloud service</a></li> <li><a href="#">Custom</a></li> <li><a href="#">Database server</a></li> <li><a href="#">eHealth</a></li> </ul>	<ul style="list-style-type: none"> <li><a href="#">EXE</a></li> <li><a href="#">Hardware parameter</a></li> <li><a href="#">IoT and IIoT</a></li> <li><a href="#">Linux/Unix/macOS</a></li> <li><a href="#">Mail server</a></li> <li><a href="#">New sensors</a></li> <li><a href="#">PRTG internal</a></li> <li><a href="#">PRTG Sensor Hub</a></li> </ul>	<ul style="list-style-type: none"> <li><a href="#">SNMP</a></li> <li><a href="#">Storage and file server</a></li> <li><a href="#">Various server</a></li> <li><a href="#">Virtual server</a></li> <li><a href="#">VoIP and QoS</a></li> <li><a href="#">Web server (HTTP)</a></li> <li><a href="#">Windows WMI/performance counter</a></li> </ul>
---	---	---

### General

General sensors let you monitor the basic parameters of your network.






Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Beckhoff IPC System Health</a>	21.3.71		No	No	Yes	State Threshold
<a href="#">Cloud HTTP v2</a>	20.3.62		No	No	No	State Threshold
<a href="#">Cloud Ping v2</a>	20.3.62		Yes	No	No	State Threshold
<a href="#">HTTP</a>	7		No	No	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Ping</a>	7		No	No	Yes	State Threshold
<a href="#">Port</a>	7		No	No	Yes	State Threshold
<a href="#">Port Range</a>	12.x.4		No	No	Yes	State Threshold Change
<a href="#">SNMP Traffic</a>	7		No	Yes	Yes	State Speed Volume
<a href="#">SSL Certificate</a>	15.x.19		No	No	Yes	State Threshold
<a href="#">SSL Security Check</a>	14.x.12		No	No	Yes	State Threshold
<a href="#">Windows Network Card</a>	7		No	Yes	Yes	State Speed Volume

## Backup and replication monitoring



Backup and replication monitoring sensors let you monitor backup and replication jobs.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Active Directory Replication Errors</a>	8.3.0		No	Yes	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Change
<a href="#">File</a>	7		No	No	Yes	State Threshold Change
<a href="#">Folder</a>	7		No	No	Yes	State Threshold Change
<a href="#">IMAP</a>	7		Yes	No	Yes	State Threshold
<a href="#">Veeam Backup Job Status</a>	20.4.64		No	No	Yes	State Threshold
<a href="#">Veeam Backup Job Status Advanced</a>	21.x.69		No	Yes	Yes	State Threshold

## Bandwidth monitoring

Bandwidth monitoring sensors let you analyze your network bandwidth.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">IPFIX</a>	13.x.7		Yes	No	No	State Speed Volume
<a href="#">IPFIX (Custom)</a>	13.x.7		Yes	No	No	State Speed Volume



Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">jFlow v5</a>	8.2.0		Yes	No	No	State Speed Volume
<a href="#">jFlow v5 (Custom)</a>	8.2.0		Yes	No	No	State Speed Volume
<a href="#">NetFlow v5</a>	7		No	No	No	State Speed Volume
<a href="#">NetFlow v5 (Custom)</a>	7		No	No	No	State Speed Volume
<a href="#">NetFlow v9</a>	7		No	No	No	State Speed Volume
<a href="#">NetFlow v9 (Custom)</a>	7		No	No	No	State Speed Volume
<a href="#">Packet Sniffer</a>	7		No	No	No	State Speed Volume
<a href="#">Packet Sniffer (Custom)</a>	7		No	No	No	State Speed Volume
<a href="#">sFlow</a>	7		Yes	No	No	State Speed

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Volume
<a href="#">sFlow (Custom)</a>	7		Yes	No	No	State Speed Volume
<a href="#">SNMP Cisco ADSL</a>	12.x.1		No	Yes	Yes	State Threshold
<a href="#">SNMP Cisco ASA VPN Traffic</a>	12.x.1		No	Yes	Yes	State Speed Volume
<a href="#">SNMP HPE ProLiant Network Interface</a>	12.x.4		No	Yes	Yes	State Speed Volume
<a href="#">SNMP Library</a>	7		No	Yes	Yes	State Threshold Change
<a href="#">SNMP NetApp Network Interface</a>	12.x.3		No	Yes	Yes	State Speed Volume
<a href="#">SNMP RMON</a>	12.x.1		No	Yes	Yes	State Speed Volume
<a href="#">SNMP SonicWall VPN Traffic</a>	13.x.6		No	Yes	Yes	State Speed Volume
<a href="#">SNMP Traffic</a>	7		No	Yes	Yes	State

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Speed Volume
<a href="#">Windows Network Card</a>	7		No	Yes	Yes	State Speed Volume

### Beta sensors

Here you can find a list of sensors that are currently in the beta status.










**i** To use beta sensors, enable the Beta Sensors experimental feature of PRTG. For more information, see the Knowledge Base: [What are beta sensors and how can I use them?](#)






Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Cisco WLC Access Point Overview</a>	N/A		No	Yes	No	State Threshold
<a href="#">Port v2</a>	N/A		No	No	Yes	State Threshold
<a href="#">REST Custom v2</a>	N/A		No	Yes	No	State Threshold
<a href="#">SNMP Custom v2</a>	N/A		No	No	No	State Threshold
<a href="#">SNMP Disk Free v2</a>	N/A		No	Yes	No	State Threshold
<a href="#">SNMP Traffic v2</a>	N/A		No	Yes	No	State Speed

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Volume

## Cloud service

Cloud service sensors let you get a quick overview of all cloud services.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">AWS Alarm v2</a>	22.x.76		No	Yes	Yes	State Threshold
<a href="#">AWS Cost</a>	20.1.56		No	No	Yes	State Threshold
<a href="#">AWS EBS v2</a>	22.x.76		No	Yes	Yes	State Threshold
<a href="#">AWS EC2 v2</a>	22.x.76		No	Yes	Yes	State Threshold
<a href="#">AWS ELB v2</a>	22.x.76		No	Yes	Yes	State Threshold
<a href="#">AWS RDS v2</a>	22.x.77		No	No	Yes	State Threshold
<a href="#">Common SaaS</a>	15.x.19		No	No	Yes	State Threshold
<a href="#">Microsoft 365 Mailbox</a>	22.x.79		No	Yes	No	State Threshold
<a href="#">Microsoft 365 Service Status</a>	20.3.61		No	No	Yes	State







Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Threshold
<a href="#">Microsoft 365 Service Status Advanced</a>	20.3.61		No	Yes	Yes	State Threshold
<a href="#">Microsoft Azure SQL Database</a>	21.x.70		No	Yes	Yes	State Threshold
<a href="#">Microsoft Azure Storage Account</a>	21.x.70		No	Yes	Yes	State Threshold
<a href="#">Microsoft Azure Subscription Cost</a>	20.4.64		No	No	Yes	State Threshold
<a href="#">Zoom Service Status</a>	20.3.61		No	No	Yes	State Threshold

## Custom

Custom sensors let you enhance the monitoring task far beyond the standard sensor set.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Business Process</a>	15.x.20		No	No	No	State Threshold
<a href="#">EXE/Script</a>	7		No	Yes	Yes	State Threshold Change
<a href="#">EXE/Script Advanced</a>	7		No	Yes	Yes	State Threshold Change

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">IPFIX (Custom)</a>	13.x.7		Yes	No	No	State Speed Volume
<a href="#">jFlow v5 (Custom)</a>	8.2.0		Yes	No	No	State Speed Volume
<a href="#">NetFlow v5 (Custom)</a>	7		No	No	No	State Speed Volume
<a href="#">NetFlow v9 (Custom)</a>	7		No	No	No	State Speed Volume
<a href="#">Packet Sniffer (Custom)</a>	7		No	No	No	State Speed Volume
<a href="#">Python Script Advanced</a>	15.x.19		No	Yes	Yes	State Threshold
<a href="#">REST Custom</a>	17.3.33		No	Yes	No	State Threshold
<a href="#">Sensor Factory</a>	7		No	No	No	State Threshold
<a href="#">sFlow (Custom)</a>	7		Yes	No	No	State Speed Volume
<a href="#">SNMP Custom</a>	7		No	No	Yes	State

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Threshold Change
<a href="#">SNMP Custom Advanced</a>	15.x.18		No	No	Yes	State Threshold
<a href="#">SNMP Custom String</a>	9.1.0		No	No	Yes	State Threshold Change
<a href="#">SNMP Custom String Lookup</a>	14.x.14		No	Yes	Yes	State Threshold
<a href="#">SNMP Custom Table</a>	15.x.18		No	Yes	Yes	State Threshold
<a href="#">SSH Script</a>	12.x.1		Yes	Yes	Yes	State Threshold Change
<a href="#">SSH Script Advanced</a>	12.x.6		Yes	Yes	Yes	State Threshold Change

## Database server

Database server sensors let you monitor the most common databases.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">ADO SQL v2</a>	16.x.24		No	Yes	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Change
<a href="#">Microsoft SQL v2</a>	14.x.12		No	Yes	Yes	State Threshold Change
<a href="#">MySQL v2</a>	14.x.12		No	Yes	Yes	State Threshold Change
<a href="#">Oracle SQL v2</a>	14.x.13		No	Yes	Yes	State Threshold Change
<a href="#">Oracle Tablespace</a>	15.x.18		No	Yes	Yes	State Threshold Change
<a href="#">PostgreSQL</a>	14.x.12		No	Yes	Yes	State Threshold Change
<a href="#">WMI Microsoft SQL Server 2005</a>	8.1.0		No	No	Yes	State Threshold
<a href="#">WMI Microsoft SQL Server 2008</a>	8.1.0		No	Yes	Yes	State Threshold
<a href="#">WMI Microsoft SQL Server 2012</a>	12.x.6		No	Yes	Yes	State Threshold
<a href="#">WMI Microsoft SQL Server 2014</a>	14.x.13		No	Yes	Yes	State Threshold



Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">WMI Microsoft SQL Server 2016</a>	16.x.26		No	Yes	Yes	State Threshold
<a href="#">WMI Microsoft SQL Server 2017</a>	18.x.42		No	Yes	Yes	State Threshold
<a href="#">WMI Microsoft SQL Server 2019</a>	20.3.62		No	Yes	Yes	State Threshold

## eHealth

eHealth sensors let you monitor medical equipment.



Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">DICOM Bandwidth</a>	18.1.38		No	No	No	State Threshold Change
<a href="#">DICOM C-ECHO</a>	18.1.38		No	No	No	State Threshold Change
<a href="#">DICOM Query/Retrieve</a>	18.1.38		No	No	No	State Threshold Change
<a href="#">HL7</a>	18.1.38		No	Yes	No	State Threshold Change
<a href="#">Soffico Orchestra Channel Health</a>	20.4.63		No	Yes	No	State

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Threshold

## EXE

EXE sensors let you carry out a wide range of different operations.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Active Directory Replication Errors</a>	8.3.0		No	Yes	Yes	State Threshold Change
<a href="#">ADO SQL v2</a>	16.x.24		No	Yes	Yes	State Threshold Change
<a href="#">Citrix XenServer Host</a>	12.x.1		Yes	Yes	Yes	State Threshold Change
<a href="#">Citrix XenServer Virtual Machine</a>	8.1.0		Yes	Yes	Yes	State Threshold Change
<a href="#">Dell PowerVault MDi Logical Disk</a>	12.x.1		Yes	Yes	Yes	State Threshold
<a href="#">Dell PowerVault MDi Physical Disk</a>	14.x.13		No	Yes	Yes	State Threshold
<a href="#">DICOM Bandwidth</a>	18.1.38		No	No	No	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Change
<a href="#">DICOM C-ECHO</a>	18.1.38		No	No	No	State Threshold Change
<a href="#">DICOM Query/Retrieve</a>	18.1.38		No	No	No	State Threshold Change
<a href="#">Enterprise Virtual Array</a>	13.x.6		No	Yes	No	State Threshold
<a href="#">Exchange Backup (PowerShell)</a>	13.x.5		Yes	Yes	No	State Threshold Change
<a href="#">Exchange Database (PowerShell)</a>	13.x.5		Yes	Yes	No	State Threshold Change
<a href="#">Exchange Database DAG (PowerShell)</a>	15.x.18		Yes	Yes	No	State Threshold Change
<a href="#">Exchange Mail Queue (PowerShell)</a>	13.x.5		Yes	Yes	No	State Threshold Change
<a href="#">Exchange Mailbox (PowerShell)</a>	13.x.5		Yes	Yes	No	State Threshold Change

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Exchange Public Folder (PowerShell)</a>	13.x.5		Yes	Yes	No	State Threshold Change
<a href="#">EXE/Script</a>	7		No	Yes	Yes	State Threshold Change
<a href="#">EXE/Script Advanced</a>	7		No	Yes	Yes	State Threshold Change
<a href="#">FTP</a>	7		Yes	No	Yes	State Threshold
<a href="#">HL7</a>	18.1.38		No	Yes	No	State Threshold Change
<a href="#">HTTP Full Web Page</a>	7		No	No	Yes	State Threshold
<a href="#">HTTP XML/REST Value</a>	8.3.0		No	No	Yes	State Threshold Change
<a href="#">Hyper-V Cluster Shared Volume Disk Free</a>	12.3.4		No	Yes	Yes	State Threshold Change
<a href="#">IP on DNS Blacklist</a>	8.3.0		No	No	Yes	State Threshold Change










Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">IPMI System Health</a>	14.x.11		No	Yes	No	State Threshold Change
<a href="#">Microsoft SQL v2</a>	14.x.12		No	Yes	Yes	State Threshold Change
<a href="#">NetApp Physical Disk</a>	17.3.33		No	Yes	No	State Speed Volume Threshold Change
<a href="#">Oracle SQL v2</a>	14.x.13		No	Yes	Yes	State Threshold Change
<a href="#">Oracle Tablespace</a>	15.x.18		No	Yes	Yes	State Threshold Change

## Hardware parameter

Hardware parameter sensors let you monitor the status of hardware components.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Dell PowerVault MDi Logical Disk</a>	12.x.1		Yes	Yes	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Dell PowerVault MDi Physical Disk</a>	14.x.13		No	Yes	Yes	State Threshold
<a href="#">Enterprise Virtual Array</a>	13.x.6		No	Yes	No	State Threshold
<a href="#">FortiGate System Statistics</a>	22.x.79		No	No	Yes	State Threshold
<a href="#">NetApp Aggregate</a>	17.3.33		No	Yes	No	State Threshold Change
<a href="#">NetApp I/O</a>	17.3.33		No	Yes	No	State Speed Volume Change
<a href="#">NetApp LIF</a>	17.3.33		No	Yes	No	State Speed Volume Change
<a href="#">NetApp LUN</a>	17.3.33		No	Yes	No	State Threshold Change
<a href="#">NetApp NIC</a>	17.3.33		No	Yes	No	State Speed Volume Threshold Change

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">NetApp Physical Disk</a>	17.3.33		No	Yes	No	State Speed Volume Threshold Change
<a href="#">NetApp SnapMirror</a>	17.4.35		No	Yes	No	State Threshold Change
<a href="#">NetApp System Health</a>	17.3.33		No	Yes	No	State Threshold Change
<a href="#">NetApp Volume</a>	17.3.33		No	Yes	No	State Threshold Change
<a href="#">Redfish Power Supply</a>	22.x.76		No	Yes	Yes	State Threshold
<a href="#">Redfish System Health</a>	22.x.76		No	Yes	No	State Threshold
<a href="#">SNMP APC Hardware</a>	9.1.0		No	Yes	Yes	State Threshold Change
<a href="#">SNMP Buffalo TS System Health</a>	17.1.29		No	No	Yes	State Threshold
<a href="#">SNMP Cisco System Health</a>	12.x.4		No	Yes	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">SNMP Cisco UCS Blade</a>	15.x.14		No	Yes	Yes	State Threshold
<a href="#">SNMP Cisco UCS Chassis</a>	14.x.8		No	Yes	Yes	State Threshold
<a href="#">SNMP Cisco UCS Physical Disk</a>	14.2.10		No	Yes	Yes	State Threshold
<a href="#">SNMP Cisco UCS System Health</a>	14.1.8		No	No	Yes	State Threshold
<a href="#">SNMP CPU Load</a>	12.x.4		No	No	Yes	State Threshold
<a href="#">SNMP Dell EqualLogic Logical Disk</a>	16.x.24		No	Yes	Yes	State Threshold
<a href="#">SNMP Dell EqualLogic Member Health</a>	16.x.24		No	Yes	Yes	State Threshold
<a href="#">SNMP Dell EqualLogic Physical Disk</a>	16.x.24		No	Yes	Yes	State Threshold
<a href="#">SNMP Dell Hardware</a>	7		No	Yes	Yes	State Threshold Change
<a href="#">SNMP Dell PowerEdge Physical Disk</a>	12.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP Dell PowerEdge System Health</a>	12.x.4		No	Yes	Yes	State Threshold



Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">SNMP Disk Free</a>	12.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP Fujitsu System Health v2</a>	19.x.53		No	Yes	Yes	State Threshold
<a href="#">SNMP Hardware Status</a>	13.x.5		No	Yes	Yes	State Threshold
<a href="#">SNMP HP LaserJet Hardware</a>	9.1.0		No	Yes	Yes	State Threshold Change
<a href="#">SNMP HPE BladeSystem Blade</a>	15.x.18		No	Yes	Yes	State Threshold
<a href="#">SNMP HPE BladeSystem Enclosure Health</a>	15.x.18		No	No	Yes	State Threshold
<a href="#">SNMP HPE ProLiant Logical Disk</a>	12.x.6		No	Yes	Yes	State Threshold
<a href="#">SNMP HPE ProLiant Memory Controller</a>	12.x.6		No	Yes	Yes	State Threshold
<a href="#">SNMP HPE ProLiant Network Interface</a>	12.x.4		No	Yes	Yes	State Speed Volume
<a href="#">SNMP HPE ProLiant Physical Disk</a>	12.x.6		No	Yes	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">SNMP HPE ProLiant System Health</a>	12.x.4		No	No	Yes	State Threshold
<a href="#">SNMP IBM System X Logical Disk</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP IBM System X Physical Disk</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP IBM System X Physical Memory</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP IBM System X System Health</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP interSector Pro Environment</a>	14.1.10		No	Yes	Yes	State Threshold
<a href="#">SNMP Juniper NS System Health</a>	15.2.16		No	No	Yes	State Threshold
<a href="#">SNMP LenovoEMC Physical Disk</a>	13.x.8		No	Yes	Yes	State Threshold
<a href="#">SNMP LenovoEMC System Health</a>	13.x.8		No	No	Yes	State Threshold
<a href="#">SNMP Library</a>	7		No	Yes	Yes	State Threshold Change
<a href="#">SNMP Memory</a>	12.x.4		No	Yes	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">SNMP NetApp Enclosure</a>	12.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP NetApp I/O</a>	12.x.3		No	No	Yes	State Speed Volume
<a href="#">SNMP NetApp Logical Unit</a>	13.x.7		No	Yes	Yes	State Speed Volume Threshold
<a href="#">SNMP NetApp Network Interface</a>	12.x.3		No	Yes	Yes	State Speed Volume
<a href="#">SNMP NetApp System Health</a>	12.x.3		No	No	Yes	State Threshold
<a href="#">SNMP QNAP Logical Disk</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP QNAP Physical Disk</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP QNAP System Health</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP SonicWall System Health</a>	13.x.5		No	No	Yes	State Threshold
<a href="#">SNMP SonicWall VPN Traffic</a>	13.x.6		No	Yes	Yes	State Speed Volume

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">SNMP Synology Logical Disk</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP Synology Physical Disk</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP Synology System Health</a>	13.x.4		No	No	Yes	State Threshold
<a href="#">SSH SAN Enclosure</a>	14.x.12		Yes	Yes	Yes	State Threshold
<a href="#">SSH SAN Logical Disk</a>	14.1.9		Yes	Yes	Yes	State Threshold
<a href="#">SSH SAN Physical Disk</a>	14.1.9		Yes	Yes	Yes	State Threshold
<a href="#">SSH SAN System Health</a>	14.1.9		Yes	Yes	Yes	State Threshold
<a href="#">Windows Physical Disk I/O</a>	16.x.24		No	Yes	Yes	State Threshold
<a href="#">WMI Battery</a>	19.x.52		No	Yes	Yes	State Threshold
<a href="#">WMI Disk Health</a>	19.4.54		No	Yes	Yes	State Threshold
<a href="#">WMI HDD Health</a>	12.x.1		Yes	Yes	Yes	State
<a href="#">WMI Vital System Data v2</a>	7		No	Yes	Yes	State Threshold

## IoT and IIoT

IoT and IIoT sensors let you monitor IoT-capable and IIoT-capable devices.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Beckhoff IPC System Health</a>	21.x.71		No	No	Yes	State Threshold
<a href="#">HTTP IoT Push Data Advanced</a>	18.3.43		No	No	Yes	State
<a href="#">Modbus RTU Custom</a>	21.x.71		No	No	Yes	State Speed Volume
<a href="#">Modbus TCP Custom</a>	20.4.63		No	No	Yes	State Threshold
<a href="#">MQTT Round Trip</a>	20.2.59		No	No	Yes	State Threshold
<a href="#">MQTT Statistics</a>	20.2.59		No	No	Yes	State Threshold
<a href="#">MQTT Subscribe Custom</a>	20.3.61		No	No	Yes	State Threshold
<a href="#">OPC UA Certificate</a>	21.1.66		No	No	Yes	State Threshold
<a href="#">OPC UA Custom</a>	21.1.66		No	No	Yes	State Threshold
<a href="#">OPC UA Server Status</a>	20.4.63		No	No	Yes	State Threshold
<a href="#">SNMP Rittal CMC III Hardware Status</a>	22.x.76		No	No	Yes	State

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Threshold

## Linux/Unix/macOS










Linux/Unix/macOS sensors let you monitor Linux-based networks.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Python Script Advanced</a>	15.x.19		No	Yes	Yes	State Threshold
<a href="#">SFTP Secure File Transfer Protocol</a>	12.x.6		Yes	No	Yes	State Threshold
<a href="#">SNMP Linux Disk Free</a>	8.1.0		No	No	Yes	State Threshold
<a href="#">SNMP Linux Load Average</a>	8.1.0		No	No	Yes	State Threshold
<a href="#">SNMP Linux Meminfo</a>	8.1.0		No	No	Yes	State Threshold
<a href="#">SNMP Linux Physical Disk</a>	13.x.5		No	Yes	Yes	State Speed Volume Threshold
<a href="#">SSH Disk Free</a>	8.1.0		Yes	Yes	Yes	State Threshold
<a href="#">SSH INodes Free</a>	8.1.1		Yes	No	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">SSH Load Average</a>	8.1.0		Yes	No	Yes	State Threshold
<a href="#">SSH Meminfo</a>	8.1.0		Yes	No	Yes	State Threshold
<a href="#">SSH Remote Ping</a>	12.x.1		Yes	No	Yes	State Threshold
<a href="#">SSH SAN Enclosure</a>	14.x.12		Yes	Yes	Yes	State Threshold
<a href="#">SSH SAN Logical Disk</a>	14.1.9		Yes	Yes	Yes	State Threshold
<a href="#">SSH SAN Physical Disk</a>	14.1.9		Yes	Yes	Yes	State Threshold
<a href="#">SSH SAN System Health</a>	14.1.9		Yes	Yes	Yes	State Threshold
<a href="#">SSH Script</a>	12.x.1		Yes	Yes	Yes	State Threshold Change
<a href="#">SSH Script Advanced</a>	12.x.6		Yes	Yes	Yes	State Threshold Change

## Mail server

Mail server sensors let you monitor different parameters of mail servers.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Exchange Backup (PowerShell)</a>	13.x.5		Yes	Yes	No	State Threshold Change
<a href="#">Exchange Database (PowerShell)</a>	13.x.5		Yes	Yes	No	State Threshold Change
<a href="#">Exchange Database DAG (PowerShell)</a>	15.x.18		Yes	Yes	No	State Threshold Change
<a href="#">Exchange Mail Queue (PowerShell)</a>	13.x.5		Yes	Yes	No	State Threshold Change
<a href="#">Exchange Mailbox (PowerShell)</a>	13.x.5		Yes	Yes	No	State Threshold Change
<a href="#">Exchange Public Folder (PowerShell)</a>	13.x.5		Yes	Yes	No	State Threshold Change
<a href="#">IMAP</a>	7		Yes	No	Yes	State Threshold
<a href="#">IP on DNS Blacklist</a>	8.3.0		No	No	Yes	State Threshold Change
<a href="#">POP3</a>	7		Yes	No	Yes	State Threshold



Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">SMTP</a>	7		Yes	Yes	Yes	State Threshold
<a href="#">SMTP&amp;IMAP Round Trip</a>	7		Yes	Yes	Yes	State Threshold
<a href="#">SMTP&amp;POP3 Round Trip</a>	7		Yes	Yes	Yes	State Threshold
<a href="#">SSL Security Check</a>	14.x.12		No	No	Yes	State Threshold
<a href="#">Windows SMTP Service Received</a>	8.1.0		No	No	Yes	State Speed Volume
<a href="#">Windows SMTP Service Sent</a>	8.1.0		No	No	Yes	State Speed Volume
<a href="#">WMI Exchange Server</a>	9		No	Yes	Yes	State Threshold
<a href="#">WMI Exchange Transport Queue</a>	12.x.1		No	Yes	Yes	State Threshold

## New sensors

Here you can find a list of sensors that are new. Sensors are **new** for a few versions after the Stable release.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">AWS Alarm v2</a>	22.2.76		No	Yes	Yes	State Threshold
<a href="#">AWS EBS v2</a>	22.2.76		No	Yes	Yes	State Threshold
<a href="#">AWS EC2 v2</a>	22.2.76		No	Yes	Yes	State Threshold
<a href="#">AWS ELB v2</a>	22.2.76		No	Yes	Yes	State Threshold
<a href="#">AWS RDS v2</a>	22.2.76		No	Yes	Yes	State Threshold
<a href="#">Cisco Meraki License</a>	22.1.75		No	Yes	Yes	State Threshold
<a href="#">Cisco Meraki Network Health</a>	22.1.75		No	Yes	Yes	State Threshold
<a href="#">FortiGate VPN Overview</a>	22.1.74		No	No	Yes	State Threshold
<a href="#">HPE 3PAR Drive Enclosure</a>	22.2.76		No	Yes	Yes	State Threshold
<a href="#">HTTP v2</a>	22.4.81		No	No	Yes	State Threshold
<a href="#">Local Folder</a>	21.3.70		No	No	Yes	State Threshold
<a href="#">Microsoft 365 Mailbox</a>	22.3.79		No	Yes	No	State Threshold





Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Modbus RTU Custom</a>	21.3.71		No	No	Yes	State Speed Volume
<a href="#">Multi-Platform Probe Health</a>	24.1.92		No	No	No	State Threshold
<a href="#">NetApp Aggregate v2</a>	23.2.84		No	Yes	Yes	State Threshold
<a href="#">NetApp I/O v2</a>	23.2.84		No	Yes	Yes	State Threshold
<a href="#">NetApp LIF v2</a>	23.2.84		No	Yes	Yes	State Threshold
<a href="#">NetApp LUN v2</a>	23.2.84		No	Yes	Yes	State Threshold
<a href="#">NetApp NIC v2</a>	23.2.84		No	Yes	Yes	State Threshold
<a href="#">NetApp Physical Disk v2</a>	23.2.84		No	Yes	Yes	State Threshold
<a href="#">NetApp SnapMirror v2</a>	23.2.84		No	Yes	Yes	State Threshold
<a href="#">NetApp System Health v2</a>	23.2.84		No	Yes	Yes	State Threshold
<a href="#">NetApp Volume v2</a>	23.2.84		No	Yes	Yes	State Threshold
<a href="#">Network Share</a>	21.4.73		No	No	Yes	State

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Threshold
<a href="#">Ping v2</a>	22.4.81		No	No	Yes	State Threshold
<a href="#">Redfish Virtual Disk</a>	21.3.71		No	Yes	Yes	State Threshold
<a href="#">Script v2</a>	24.2.97		No	Yes	Yes	State Threshold
<a href="#">SNMP Rittal CMC III Hardware Status</a>	22.2.76		No	No	Yes	State Threshold
<a href="#">SNMP Uptime v2</a>	23.2.84		No	No	No	State Threshold
<a href="#">Soffico Orchestra Scenario</a>	23.3.88		No	Yes	Yes	State Threshold
<a href="#">System Health v2</a>	24.1.92		No	No	No	State Threshold

## PRTG internal

PRTG internal sensors let you monitor internal parameters of PRTG.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Application Server Health (Autonomous)</a>	21.x.73		No	No	No	State Threshold
<a href="#">Cluster Health</a>	9.1.0		No	No	No	State

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Threshold
<a href="#">Core Health</a>	9.1.0		No	No	No	State Threshold
<a href="#">Core Health (Autonomous)</a>	21.2.67		No	No	No	State Threshold
<a href="#">Probe Health</a>	9.1.0		No	No	No	State Threshold
<a href="#">System Health</a>	9.1.0		No	No	No	State Threshold



## PRTG Sensor Hub

In addition to the built-in sensors, you can create your own. You can write a script or a program and use it with a [custom sensor](#)<sup>[3150]</sup>. There are already many free, useful scripts, plugins, and add-ons for PRTG in the [PRTG Sensor Hub](#). You can also directly open the PRTG Sensor Hub from the [Add Sensor](#)<sup>[414]</sup> dialog in the PRTG web interface.

- To use the sensors in the PRTG Sensor Hub, go to <https://www.paessler.com/sensor-hub> and follow the instructions there.

## SNMP

SNMP sensors let you monitor a wide range of devices via SNMP.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Cisco IP SLA</a>	7		Yes	Yes	Yes	State Threshold
<a href="#">SNMP APC Hardware</a>	9.1.0		No	Yes	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Change
<a href="#">SNMP Buffalo TS System Health</a>	17.1.29		No	No	Yes	State Threshold
<a href="#">SNMP Cisco ADSL</a>	12.x.1		No	Yes	Yes	State Threshold
<a href="#">SNMP Cisco ASA VPN Connections</a>	12.x.1		No	No	Yes	State Threshold
<a href="#">SNMP Cisco ASA VPN Traffic</a>	12.x.1		No	Yes	Yes	State Speed Volume
<a href="#">SNMP Cisco ASA VPN Users</a>	12.x.5		No	No	Yes	State Threshold
<a href="#">SNMP Cisco CBQoS</a>	13.x.5		Yes	Yes	Yes	State Speed Volume
<a href="#">SNMP Cisco System Health</a>	12.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP Cisco UCS Blade</a>	15.x.14		No	Yes	Yes	State Threshold
<a href="#">SNMP Cisco UCS Chassis</a>	14.x.8		No	Yes	Yes	State Threshold
<a href="#">SNMP Cisco UCS Physical Disk</a>	14.2.10		No	Yes	Yes	State Threshold
<a href="#">SNMP Cisco UCS System Health</a>	14.1.8		No	No	Yes	State

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Threshold
<a href="#">SNMP CPU Load</a>	12.x.4		No	No	Yes	State Threshold
<a href="#">SNMP Custom</a>	7		No	No	Yes	State Threshold Change
<a href="#">SNMP Custom Advanced</a>	15.x.18		No	No	Yes	State Threshold
<a href="#">SNMP Custom String</a>	9.1.0		No	No	Yes	State Threshold Change
<a href="#">SNMP Custom String Lookup</a>	14.x.14		No	Yes	Yes	State Threshold
<a href="#">SNMP Custom Table</a>	15.x.18		No	Yes	Yes	State Volume
<a href="#">SNMP Dell EqualLogic Logical Disk</a>	16.x.24		No	Yes	Yes	State Threshold
<a href="#">SNMP Dell EqualLogic Member Health</a>	16.x.24		No	Yes	Yes	State Threshold
<a href="#">SNMP Dell EqualLogic Physical Disk</a>	16.x.24		No	Yes	Yes	State Threshold
<a href="#">SNMP Dell Hardware</a>	7		No	Yes	Yes	State Threshold Change

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">SNMP Dell PowerEdge Physical Disk</a>	12.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP Dell PowerEdge System Health</a>	12.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP Disk Free</a>	12.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP Fujitsu System Health v2</a>	19.x.53		No	Yes	Yes	State Threshold
<a href="#">SNMP Hardware Status</a>	13.x.5		No	Yes	Yes	State Threshold
<a href="#">SNMP HP LaserJet Hardware</a>	9.1.0		No	Yes	Yes	State Threshold Change
<a href="#">SNMP HPE BladeSystem Blade</a>	15.x.18		No	Yes	Yes	State Threshold
<a href="#">SNMP HPE BladeSystem Enclosure Health</a>	15.x.18		No	No	Yes	State Threshold
<a href="#">SNMP HPE ProLiant Logical Disk</a>	12.x.6		No	Yes	Yes	State Threshold
<a href="#">SNMP HPE ProLiant Memory Controller</a>	12.x.6		No	Yes	Yes	State Threshold
<a href="#">SNMP HPE ProLiant Network Interface</a>	12.x.4		No	Yes	Yes	State Speed



Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Volume
<a href="#">SNMP HPE ProLiant Physical Disk</a>	12.x.6		No	Yes	Yes	State Threshold
<a href="#">SNMP HPE ProLiant System Health</a>	12.x.4		No	No	Yes	State Threshold
<a href="#">SNMP IBM System X Logical Disk</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP IBM System X Physical Disk</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP IBM System X Physical Memory</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP IBM System X System Health</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP interSector Pro Environment</a>	14.1.10		No	Yes	Yes	State Threshold
<a href="#">SNMP Juniper NS System Health</a>	15.2.16		No	No	Yes	State Threshold
<a href="#">SNMP LenovoEMC Physical Disk</a>	13.x.8		No	Yes	Yes	State Threshold
<a href="#">SNMP LenovoEMC System Health</a>	13.x.8		No	No	Yes	State Threshold
<a href="#">SNMP Library</a>	7		No	Yes	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Change
<a href="#">SNMP Linux Disk Free</a>	8.1.0		No	No	Yes	State Threshold
<a href="#">SNMP Linux Load Average</a>	8.1.0		No	No	Yes	State Threshold
<a href="#">SNMP Linux Meminfo</a>	8.1.0		No	No	Yes	State Threshold
<a href="#">SNMP Linux Physical Disk</a>	13.x.5		No	Yes	Yes	State Speed Volume Threshold
<a href="#">SNMP Memory</a>	12.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP NetApp Disk Free</a>	12.x.3		No	Yes	Yes	State Threshold
<a href="#">SNMP NetApp Enclosure</a>	12.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP NetApp I/O</a>	12.x.3		No	No	Yes	State Speed Volume
<a href="#">SNMP NetApp License</a>	12.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP NetApp Logical Unit</a>	13.x.7		No	Yes	Yes	State Speed Volume

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Threshold
<a href="#">SNMP NetApp Network Interface</a>	12.x.3		No	Yes	Yes	State Speed Volume
<a href="#">SNMP NetApp System Health</a>	12.x.3		No	No	Yes	State Threshold
<a href="#">SNMP Nutanix Cluster Health</a>	20.1.55		No	Yes	Yes	State Threshold
<a href="#">SNMP Nutanix Hypervisor</a>	20.1.55		No	Yes	Yes	State Threshold
<a href="#">SNMP Poseidon Environment</a>	13.x.5		No	Yes	Yes	State Threshold
<a href="#">SNMP Printer</a>	14.x.11		No	No	Yes	State Threshold
<a href="#">SNMP QNAP Logical Disk</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP QNAP Physical Disk</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP QNAP System Health</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP Rittal CMC III Hardware Status</a>	22.x.76		No	No	Yes	State Threshold
<a href="#">SNMP RMON</a>	12.x.1		No	Yes	Yes	State Speed








Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Volume
<a href="#">SNMP SonicWall System Health</a>	13.x.5		No	No	Yes	State Threshold
<a href="#">SNMP SonicWall VPN Traffic</a>	13.x.6		No	Yes	Yes	State Speed Volume
<a href="#">SNMP Synology Logical Disk</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP Synology Physical Disk</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP Synology System Health</a>	13.x.4		No	No	Yes	State Threshold
<a href="#">SNMP System Uptime</a>	7		No	No	Yes	State Threshold
<a href="#">SNMP Traffic</a>	7		No	Yes	Yes	State Speed Volume
<a href="#">SNMP Trap Receiver</a>	7		No	No	No	State Speed Volume
<a href="#">SNMP Windows Service</a>	13.x.8		No	Yes	Yes	State Threshold

## Storage and file server

Storage and file server sensors let you monitor different parameters of storage and file servers.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Dell EMC Unity Enclosure Health v2</a>	20.4.64		No	Yes	Yes	State Threshold
<a href="#">Dell EMC Unity File System v2</a>	20.3.62		No	Yes	Yes	State Threshold
<a href="#">Dell EMC Unity Storage Capacity v2</a>	20.3.62		No	No	Yes	State Threshold
<a href="#">Dell EMC Unity Storage LUN v2</a>	20.3.61		No	Yes	Yes	State Threshold
<a href="#">Dell EMC Unity Storage Pool v2</a>	20.3.62		No	Yes	Yes	State Threshold
<a href="#">Dell EMC Unity VMware Datastore v2</a>	20.4.63		No	Yes	Yes	State Threshold
<a href="#">Dell PowerVault MDi Logical Disk</a>	12.x.1		Yes	Yes	Yes	State Threshold
<a href="#">Dell PowerVault MDi Physical Disk</a>	14.x.13		No	Yes	Yes	State Threshold
<a href="#">Enterprise Virtual Array</a>	13.x.6		No	Yes	No	State Threshold
<a href="#">File</a>	7		No	No	Yes	State Threshold Change
<a href="#">File Content</a>	7		No	No	Yes	State Threshold Change

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Folder</a>	7		No	No	Yes	State Threshold Change
<a href="#">FTP</a>	7		Yes	No	Yes	State Threshold
<a href="#">FTP Server File Count</a>	8.3.0		No	No	Yes	State Threshold Change
<a href="#">HPE 3PAR Common Provisioning Group</a>	21.x.70		No	Yes	Yes	State Threshold
<a href="#">HPE 3PAR Drive Enclosure</a>	22.x.76		No	Yes	Yes	State Threshold
<a href="#">HPE 3PAR Virtual Volume</a>	22.x.76		No	Yes	Yes	State Threshold
<a href="#">Hyper-V Cluster Shared Volume Disk Free</a>	12.3.4		No	Yes	Yes	State Threshold Change
<a href="#">Hyper-V Virtual Storage Device</a>	12.4.4		No	Yes	Yes	State Threshold
<a href="#">NetApp Aggregate</a>	17.3.33		No	Yes	No	State Threshold Change
<a href="#">NetApp I/O</a>	17.3.33		No	Yes	No	State Speed Volume

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Change
<a href="#">NetApp LIF</a>	17.3.33		No	Yes	No	State Speed Volume Change
<a href="#">NetApp LUN</a>	17.3.33		No	Yes	No	State Threshold Change
<a href="#">NetApp NIC</a>	17.3.33		No	Yes	No	State Speed Volume Threshold Change
<a href="#">NetApp Physical Disk</a>	17.3.33		No	Yes	No	State Speed Volume Threshold Change
<a href="#">NetApp SnapMirror</a>	17.4.35		No	Yes	No	State Threshold Change
<a href="#">NetApp System Health</a>	17.3.33		No	Yes	No	State Threshold Change
<a href="#">NetApp Volume</a>	17.3.33		No	Yes	No	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Change
<a href="#">SFTP Secure File Transfer Protocol</a>	12.x.6		Yes	No	Yes	State Threshold
<a href="#">Share Disk Free</a>	7		No	Yes	Yes	State Threshold
<a href="#">SNMP Buffalo TS System Health</a>	17.1.29		No	No	Yes	State Threshold
<a href="#">SNMP Cisco UCS Physical Disk</a>	14.2.10		No	Yes	Yes	State Threshold
<a href="#">SNMP Dell EqualLogic Logical Disk</a>	16.x.24		No	Yes	Yes	State Threshold
<a href="#">SNMP Dell EqualLogic Member Health</a>	16.x.24		No	Yes	Yes	State Threshold
<a href="#">SNMP Dell EqualLogic Physical Disk</a>	16.x.24		No	Yes	Yes	State Threshold
<a href="#">SNMP Dell PowerEdge Physical Disk</a>	12.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP HPE ProLiant Logical Disk</a>	12.x.6		No	Yes	Yes	State Threshold
<a href="#">SNMP HPE ProLiant Physical Disk</a>	12.x.6		No	Yes	Yes	State Threshold
<a href="#">SNMP IBM System X Logical Disk</a>	13.x.4		No	Yes	Yes	State Threshold



Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">SNMP IBM System X Physical Disk</a>	13.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP LenovoEMC Physical Disk</a>	13.x.8		No	Yes	Yes	State Threshold
<a href="#">SNMP LenovoEMC System Health</a>	13.x.8		No	No	Yes	State Threshold
<a href="#">SNMP Linux Disk Free</a>	8.1.0		No	No	Yes	State Threshold
<a href="#">SNMP Linux Physical Disk</a>	13.x.5		No	Yes	Yes	State Speed Volume Threshold
<a href="#">SNMP NetApp Disk Free</a>	12.x.3		No	Yes	Yes	State Threshold
<a href="#">SNMP NetApp Enclosure</a>	12.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP NetApp I/O</a>	12.x.3		No	No	Yes	State Speed Volume
<a href="#">SNMP NetApp License</a>	12.x.4		No	Yes	Yes	State Threshold
<a href="#">SNMP NetApp Logical Unit</a>	13.x.7		No	Yes	Yes	State Speed Volume Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">SNMP NetApp Network Interface</a>	12.x.3		No	Yes	Yes	State Speed Volume
<a href="#">SNMP NetApp System Health</a>	12.x.3		No	No	Yes	State Threshold
<a href="#">IFTP</a>	8.1.0		Yes	No	Yes	State Threshold

## Various server

Various server sensors let you monitor a wide range of server parameters.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">DHCP</a>	8.2.0		Yes	Yes	No	State Threshold Change
<a href="#">DNS v2</a>	20.2.59		No	No	Yes	State Threshold
<a href="#">IPMI System Health</a>	14.x.11		No	Yes	No	State Threshold Change
<a href="#">LDAP</a>	8.1.0		Yes	No	Yes	State Threshold
<a href="#">OPC UA Certificate</a>	21.1.66		No	No	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">OPC UA Custom</a>	21.1.66		No	No	Yes	State Threshold
<a href="#">OPC UA Server Status</a>	20.4.63		No	No	Yes	State Threshold
<a href="#">Ping</a>	7		No	No	Yes	State Threshold
<a href="#">Ping Jitter</a>	8.3.0		No	No	Yes	State Threshold Change
<a href="#">Port</a>	7		No	No	Yes	State Threshold
<a href="#">Port Range</a>	12.x.4		No	No	Yes	State Threshold Change
<a href="#">RADIUS v2</a>	14.x.13		Yes	No	Yes	State Threshold Change
<a href="#">RDP (Remote Desktop)</a>	7		No	No	Yes	State Threshold
<a href="#">SNMP Trap Receiver</a>	7		No	No	No	State Speed Volume
<a href="#">SNTP</a>	8.1.0		No	No	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">SSL Security Check</a>	14.x.12		No	No	Yes	State Threshold
<a href="#">Syslog Receiver</a>	7		No	No	No	State Speed Volume
<a href="#">Traceroute Hop Count</a>	8.3.0		No	No	Yes	State Threshold Change

## Virtual server

Virtual server sensors let you monitor your virtualized IT infrastructure.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Citrix XenServer Host</a>	12.x.1		Yes	Yes	Yes	State Threshold Change
<a href="#">Citrix XenServer Virtual Machine</a>	8.1.0		Yes	Yes	Yes	State Threshold Change
<a href="#">Dell EMC Unity VMware Datastore v2</a>	20.4.63		No	Yes	Yes	State Threshold
<a href="#">Docker Container Status</a>	16.x.22		Yes	Yes	No	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Hyper-V Cluster Shared Volume Disk Free</a>	12.3.4		No	Yes	Yes	State Threshold Change
<a href="#">Hyper-V Host Server</a>	7		No	No	Yes	State Threshold
<a href="#">Hyper-V Virtual Machine</a>	7		No	Yes	Yes	State Threshold
<a href="#">Hyper-V Virtual Network Adapter</a>	9.1.0		No	Yes	Yes	State Threshold
<a href="#">Hyper-V Virtual Storage Device</a>	12.4.4		No	Yes	Yes	State Threshold
<a href="#">Microsoft Azure Virtual Machine</a>	20.4.63		No	Yes	Yes	State Threshold
<a href="#">SNMP Nutanix Cluster Health</a>	20.1.55		No	Yes	Yes	State Threshold
<a href="#">SNMP Nutanix Hypervisor</a>	20.1.55		No	Yes	Yes	State Threshold
<a href="#">VMware Datastore (SOAP)</a>	15.x.19		No	Yes	Yes	State Threshold Change
<a href="#">VMware Host Hardware (WBEM)</a>	8.1.0		Yes	Yes	Yes	State Threshold
<a href="#">VMware Host Hardware Status (SOAP)</a>	12.x.1		No	Yes	Yes	State Threshold Change

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">VMware Host Performance (SOAP)</a>	12.x.1		No	Yes	Yes	State Threshold Change
<a href="#">VMware Virtual Machine (SOAP)</a>	7		No	Yes	Yes	State Threshold Change

## VoIP and QoS

VoIP and QoS sensors let you monitor the QoS in a network and all VoIP-relevant network parameters.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Cisco IP SLA</a>	7		Yes	Yes	Yes	State Threshold
<a href="#">QoS (Quality of Service) One Way</a>	7		Yes	No	No	State Threshold
<a href="#">QoS (Quality of Service) Round Trip</a>	9.1.0		Yes	No	No	State Threshold
<a href="#">SIP Options Ping</a>	12.x.1		No	Yes	Yes	State Threshold Change
<a href="#">SNMP Cisco CBQoS</a>	13.x.5		Yes	Yes	Yes	State Speed Volume

## Web server (HTTP)

Web server (HTTP) sensors let you monitor server parameters with HTTP.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Cloud HTTP v2</a>	20.3.62		No	No	No	State Threshold
<a href="#">Common SaaS</a>	15.x.19		No	No	Yes	State Threshold
<a href="#">HTTP</a>	7		No	No	Yes	State Threshold
<a href="#">HTTP Advanced</a>	7		No	No	Yes	State Threshold Change
<a href="#">HTTP Apache ModStatus PerfStats</a>	12.x.3		No	No	Yes	State Threshold
<a href="#">HTTP Apache ModStatus Totals</a>	12.x.3		No	No	Yes	State Speed Volume
<a href="#">HTTP Content</a>	7		No	No	Yes	State Threshold Change
<a href="#">HTTP Data Advanced</a>	15.x.16		No	No	Yes	State Change
<a href="#">HTTP Full Web Page</a>	7		No	No	Yes	State Threshold
<a href="#">HTTP IoT Push Data Advanced</a>	18.3.43		No	No	Yes	State

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">HTTP Push Count</a>	13.4.8		No	No	Yes	State Speed Threshold
<a href="#">HTTP Push Data</a>	14.1.9		No	No	Yes	State Threshold
<a href="#">HTTP Push Data Advanced</a>	14.1.10		No	No	Yes	State
<a href="#">HTTP Transaction</a>	7		No	No	Yes	State Threshold
<a href="#">HTTP XML/REST Value</a>	8.3.0		No	No	Yes	State Threshold Change
<a href="#">REST Custom</a>	17.3.33		No	Yes	No	State Threshold
<a href="#">SSL Certificate</a>	15.x.19		No	No	Yes	State Threshold
<a href="#">SSL Security Check</a>	14.x.12		No	No	Yes	State Threshold
<a href="#">Windows IIS Application</a>	12.x.1		No	Yes	Yes	State Speed Volume Threshold

### Windows WMI/performance counter

Windows WMI/performance counter sensors let you monitor Windows systems via WMI and Windows performance counters.



Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Active Directory Replication Errors</a>	8.3.0		No	Yes	Yes	State Threshold Change
<a href="#">Event Log (Windows API)</a>	7		No	No	Yes	State Speed Volume Change
<a href="#">PerfCounter Custom</a>	12.x.3		No	No	Yes	State Threshold
<a href="#">PerfCounter IIS Application Pool</a>	12.x.6		No	Yes	Yes	State Threshold
<a href="#">Windows CPU Load</a>	7		No	No	Yes	State Threshold
<a href="#">Windows IIS Application</a>	12.x.1		No	Yes	Yes	State Speed Volume Threshold
<a href="#">Windows MSMQ Queue Length</a>	8.3.0		No	Yes	Yes	State Threshold Change
<a href="#">Windows Network Card</a>	7		No	Yes	Yes	State Speed Volume
<a href="#">Windows Pagefile</a>	12.x.4		No	No	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
<a href="#">Windows Physical Disk I/O</a>	16.x.24		No	Yes	Yes	State Threshold
<a href="#">Windows Print Queue</a>	8.3.0		No	Yes	Yes	State Threshold Change
<a href="#">Windows Process</a>	7		No	No	Yes	State Threshold
<a href="#">Windows SMTP Service Received</a>	8.1.0		No	No	Yes	State Speed Volume
<a href="#">Windows SMTP Service Sent</a>	8.1.0		No	No	Yes	State Speed Volume
<a href="#">Windows System Uptime</a>	8.1.0		No	No	Yes	State Threshold
<a href="#">Windows Updates Status (PowerShell)</a>	13.x.6		No	Yes	Yes	State Threshold Change
<a href="#">WMI Battery</a>	19.x.52		No	Yes	Yes	State Threshold
<a href="#">WMI Custom</a>	7		No	Yes	Yes	State Threshold Change
<a href="#">WMI Custom String</a>	12.x.4		No	Yes	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Change
<a href="#">WMI Disk Health</a>	19.4.54		No	Yes	Yes	State Threshold
<a href="#">WMI Event Log</a>	7		No	Yes	Yes	State Speed Volume Change
<a href="#">WMI Exchange Server</a>	9		No	Yes	Yes	State Threshold
<a href="#">WMI Exchange Transport Queue</a>	12.x.1		No	Yes	Yes	State Threshold
<a href="#">WMI File</a>	7		No	No	Yes	State Threshold Change
<a href="#">WMI Free Disk Space (Multi Disk)</a>	7		No	No	Yes	State Threshold
<a href="#">WMI HDD Health</a>	12.x.1		Yes	Yes	Yes	State
<a href="#">WMI Logical Disk I/O</a>	16.x.24		No	Yes	Yes	State Threshold
<a href="#">WMI Memory</a>	7		No	No	Yes	State Threshold
<a href="#">WMI Microsoft SQL Server 2005</a>	8.1.0		No	No	Yes	State Threshold
<a href="#">WMI Microsoft SQL Server 2008</a>	8.1.0		No	Yes	Yes	State

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Threshold
<a href="#">WMI Microsoft SQL Server 2012</a>	12.x.6		No	Yes	Yes	State Threshold
<a href="#">WMI Microsoft SQL Server 2014</a>	14.x.13		No	Yes	Yes	State Threshold
<a href="#">WMI Microsoft SQL Server 2016</a>	16.x.26		No	Yes	Yes	State Threshold
<a href="#">WMI Microsoft SQL Server 2017</a>	18.x.42		No	Yes	Yes	State Threshold
<a href="#">WMI Microsoft SQL Server 2019</a>	20.3.62		No	Yes	Yes	State Threshold
<a href="#">WMI Remote Ping</a>	12.x.1		No	No	Yes	State Threshold
<a href="#">WMI Security Center</a>	9		No	Yes	Yes	State Threshold Change
<a href="#">WMI Service</a>	7		No	Yes	Yes	State Threshold Change
<a href="#">WMI Share</a>	8.1.0		No	Yes	Yes	State Threshold
<a href="#">WMI SharePoint Process</a>	12.x.1		No	Yes	Yes	State Threshold
<a href="#">WMI Storage Pool</a>	19.4.54		No	Yes	Yes	State

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
						Threshold
<a href="#">WMI Terminal Services (Windows 2008+)</a>	8.1.0		No	No	Yes	State Threshold
<a href="#">WMI Terminal Services (Windows XP/Vista/2003)</a>	8.1.0		No	No	Yes	State Threshold
<a href="#">WMI UTC Time</a>	9.2.0		Yes	No	Yes	State Threshold
<a href="#">WMI Vital System Data v2</a>	7		No	Yes	Yes	State Threshold
<a href="#">WMI Volume</a>	7		No	Yes	Yes	State Threshold
<a href="#">WSUS Statistics</a>	9.1.0		No	No	Yes	State Change

## More

### ■ KNOWLEDGE BASE

What are beta sensors and how can I use them?

- <https://kb.paessler.com/en/topic/88697>

## 15.3 Default Ports

Here you can find lists for all default ports used in PRTG:

- [Ports Used by Sensors](#) <sup>3288</sup>
- [Ports Used in Other Contexts](#) <sup>3291</sup>

### Ports Used by Sensors

Sensors	Default Port Numbers	Description
Cloud HTTP v2 and Cloud Ping v2	443	Port for the communication via the PRTG Cloud
Cloud Ping v2	80	Port for the TCP ping
Dell EMC	443	Port for the connection to the Dell EMC system
DICOM	104	Port for the connection to the DICOM interface
<a href="#">DNS v2</a>	53	Port for the connection to the device that runs the DNS service
<a href="#">Docker Container Status</a>	2376 (Docker over TLS)	Port for the connection to the Docker container
FortiGate	443	Port for the connection to the FortiGate system
<a href="#">FTP</a>	21	Port for the connection to the file server
<a href="#">HL7</a>	104	Port for the connection to the HL7 interface
HPE 3PAR	WSAPI port: <ul style="list-style-type: none"> <li>▪ 8080 (secure)</li> <li>▪ 8008 (unsecure)</li> </ul> SSH port: <ul style="list-style-type: none"> <li>▪ 22 (secure)</li> </ul>	WSAPI and SSH port for the connections to the HPE 3PAR system
HTTP	8080	Port of the proxy


Sensors	Default Port Numbers	Description
<a href="#">HTTP IoT Push Data Advanced</a>	5051	Port on which the sensor listens for incoming HTTPS requests  <b>i</b> This port is fixed. You cannot change it.
HTTP Push	<ul style="list-style-type: none"> <li>▪ 5051 (secure)</li> <li>▪ 5050 (unsecure)</li> </ul>	Port on which the sensor listens for incoming HTTP or HTTPS requests
<a href="#">IMAP</a>	<ul style="list-style-type: none"> <li>▪ 993 (secure)</li> <li>▪ 143 (unsecure)</li> </ul>	Port for the IMAP connection
<a href="#">LDAP</a>	<ul style="list-style-type: none"> <li>▪ 636 (secure)</li> <li>▪ 389 (unsecure)</li> </ul>	Port for the connection to the LDAP server
NetApp	443	Port for the NetApp API access
<a href="#">Microsoft SQL v2</a>	1433	Port for the connection to the Microsoft SQL database
<a href="#">MySQL v2</a>	3306	Port for the connection to the MySQL database
<a href="#">Modbus TCP Custom</a>	502	Port for the connection to the Modbus TCP server
MQTT	<ul style="list-style-type: none"> <li>▪ 8883 (secure)</li> <li>▪ 1883 (unsecure)</li> </ul>	Port for the MQTT connection
OPC UA	4840	Port for the connection to the OPC UA server
Oracle	1521	Port for the connection to the Oracle SQL database
<a href="#">POP3</a>	<ul style="list-style-type: none"> <li>▪ 995 (secure)</li> <li>▪ 110 (unsecure)</li> </ul>	Port for the POP3 connection
<a href="#">Port v2</a>	443	Port for the TCP connection
<a href="#">PostgreSQL</a>	5432	Port for the connection to the PostgreSQL database

Sensors	Default Port Numbers	Description
QoS	50000	Port on which the sensor listens for the UDP packets
<a href="#">RADIUS v2</a>	1812	Port for the connection to the RADIUS server
<a href="#">RDP (Remote Desktop)</a>	3389	Port for the RDP connection
Redfish	443	Port for the Redfish connection
REST	8080	Port for the proxy
<a href="#">SIP Options Ping</a>	5060	Port for the UDP connection
SMTP	<ul style="list-style-type: none"> <li>▪ 465 or 587 (secure)</li> <li>▪ 25 (unsecure)</li> </ul>	Port used to send an email via SMTP
<a href="#">SMTP&amp;IMAP Round Trip</a>	<ul style="list-style-type: none"> <li>▪ 993 (secure)</li> <li>▪ 143 (unsecure)</li> </ul>	Port for the IMAP connection
<a href="#">SMTP&amp;POP3 Round Trip</a>	<ul style="list-style-type: none"> <li>▪ 995 (secure)</li> <li>▪ 110 (unsecure)</li> </ul>	Port for the POP3 connection
SNMP	161	Port for the SNMP connection
<a href="#">SNMP Trap Receiver</a>	162	Port on which the sensor listens for SNMP traps and on which trap messages are sent
<a href="#">Soffico Orchestra Channel Health</a>	<ul style="list-style-type: none"> <li>• 8443 (secure)</li> <li>• 8019 (unsecure)</li> </ul>	Port for the connection to the Orchestra platform
SSH	22	Port for the connection via SSH
SSL	443	Port for the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) connection
<a href="#">Syslog Receiver</a>	514	Port on which the sensor listens for Syslog messages and on which Syslog messages are sent



Sensors	Default Port Numbers	Description
<a href="#">TFTP</a>	69	Port of the device on which the TFTP service runs
Veeam Backup Job Status	9398	Port for the connection to the Veeam Backup Enterprise Manager
VMware (SOAP)	443	Port for the VMware (SOAP) connection
WBEM	<ul style="list-style-type: none"> <li>▪ 5988 (unsecure)</li> <li>▪ 5989 (secure)</li> </ul>	Port for the communication via WBEM
<a href="#">Windows Updates Status (PowerShell)</a>	5985	Port for the connection to Microsoft or to the local WSUS server
WMI	135	Port for the RPC server connection via WMI
<a href="#">WSUS Statistics</a>	8530	Port for the connection to the device on which the WSUS server service runs

### Ports Used in Other Contexts

Context	Default Port Numbers	Description
Active Directory integration	<ul style="list-style-type: none"> <li>▪ 389 (unsecure)</li> <li>▪ 636 (secure)</li> </ul>	The LDAP port for Active Directory integration
Auto-update and activation	443	Port for auto-update and activation  For more information, see the Knowledge Base: <a href="#">Which servers does PRTG connect to for software auto-update, activation, etc.?</a>
Cluster communication	23570	Port for the communication between cluster nodes
Incoming probe connections	23560	Port on which PRTG listens for incoming remote probe connections
Multi-platform probe and PRTG core server	23562	Port for the connections between multi-platform probes and the PRTG core server

Context	Default Port Numbers	Description
Notifications	<ul style="list-style-type: none"> <li>▪ 443 (push)</li> <li>▪ 25 (SMTP)</li> <li>▪ 162 (SNMP trap)</li> <li>▪ 514 (Syslog)</li> </ul>	<p>Port for the notifications</p> <p><b>i</b> The target URL for push is <a href="https://api.prtgcloud.com:443">https://api.prtgcloud.com:443</a>.</p>
PRTG application server and PRTG core server	23580	Port for the connections between the PRTG application server and the PRTG core server
PRTG Cloud	443	Port used by the PRTG Cloud for support tickets, for example
PRTG MultiBoard File Transfer	44387	Port used to transfer files between PRTG core servers
PRTG web server	<ul style="list-style-type: none"> <li>▪ 443 (secure)</li> <li>▪ 80 (unsecure)</li> </ul> <p>Fallbacks:</p> <ul style="list-style-type: none"> <li>▪ 8443 and 8443+ (secure)</li> <li>▪ 8080+ (unsecure)</li> </ul>	<p>Port used by the PRTG web server</p> <p><b>i</b> PRTG app for desktop, PRTG MultiBoard, and the PRTG mobile apps also use this port to connect to the PRTG web server.</p>
Remote probes and PRTG core server	23560	<p>Port for the connections between remote probes and the PRTG core server</p> <p><b>■</b> It is sufficient to open or forward this TCP port only on the PRTG core server. If you need to change it, see the Knowledge Base: <a href="#">How can I customize ports for core-probe connections used by PRTG?</a></p>
Report generation	8085 (PDF)	Port for the report generation
Update check and download	80	<p>Port for the update check and download</p> <p><b>■</b> For more information, see the Knowledge Base: <a href="#">Which servers does PRTG connect to for software auto-update, activation, etc.?</a></p>

## 15.4 Differences between PRTG Network Monitor and PRTG Hosted Monitor

See below for the differences between the settings and features that PRTG Network Monitor and PRTG Hosted Monitor have to offer.

### Licensing, Payment, Infrastructure

Topic	PRTG Network Monitor	PRTG Hosted Monitor
Trial period	30 days	10 days
Freeware edition	Freeware (100 sensors) available	No freeware available, smallest edition is Hosted 500
Payment	Annual subscription	Monthly or annual subscription
Change of subscription or license size	Up only	Up and down, anytime
Maximum installation size	Max. 10,000 sensors recommended	10,000 sensors
PRTG update management	Done by user	Done by Paessler

### Features

Feature	PRTG Network Monitor	PRTG Hosted Monitor
Local probe	Yes	No
Hosted probe	No	Yes
Multi-platform probe	Yes	Yes
Cluster	Yes	No
Freeware edition (100 sensors)	Yes	No

Feature	PRTG Network Monitor	PRTG Hosted Monitor
Remote Desktop Protocol (RDP) access to PRTG core server	Yes	No
Historic data purging (manually defined)	Yes	No
Active Directory integration	Yes	No
License/subscription settings via PRTG web interface	Yes	No
Recommended sensors on local probe/hosted probe	Yes	No
Auto-discovery for groups on local probe/hosted probe	Yes	No
Mini probes	Yes	No
Device tools on local probe/hosted probe	Yes	No
Proxy server settings	Yes	No
System information on local probe/hosted probe	Yes	No
PRTG Administration Tool on PRTG core server	Yes	No
Notification methods:		
▪ Send Email	Yes	Yes
▪ Send SMS/Pager Message	Yes	Yes
▪ Execute HTTP Action	Yes	Yes
▪ Send Amazon Simple Notification Service Message	Yes	Yes
▪ Assign Ticket	Yes	Yes

Feature	PRTG Network Monitor	PRTG Hosted Monitor
▪ Send Push Notification	Yes	Yes
▪ Send Microsoft Teams Message	Yes	Yes
▪ Send Slack Message	Yes	Yes
▪ Send MQTT Publish Notification	Yes	Yes
▪ Send OPC UA Notification	Yes	Yes
▪ Add Entry to Event Log	Yes	No
▪ Send Syslog Message	Yes	No
▪ Send SNMP Trap	Yes	No
▪ Execute Program	Yes	No
Re-login request on setup pages after 15 minutes	Yes	No
IPv6 on local probe/hosted probe	Yes	No
Multi-factor authentication	No*	Yes

\* PRTG Network Monitor supports multi-factor authentication with Microsoft Entra ID and Okta.

- For more information, see the Knowledge Base: [How can I enable Microsoft Entra ID multifactor authentication?](#)
- For more information, see the Knowledge Base: [How can I enable Okta multi-factor authentication?](#)

### Sensors on the Hosted Probe of PRTG Hosted Monitor

You can use the following sensors on the hosted probe of PRTG Hosted Monitor:

Supported Sensors
AWS Alarm v2 sensor
AWS Cost sensor

Supported Sensors
AWS EBS v2 sensor
AWS EC2 v2 sensor
AWS ELB v2 sensor
AWS RDS v2 sensor
Beckhoff IPC System Health sensor
Business Process sensor
Cisco IP SLA sensor
Citrix XenServer Host sensor
Citrix XenServer Virtual Machine sensor
Cloud HTTP v2 sensor
Cloud Ping v2 sensor
Cluster Health sensor
Common SaaS sensor
Core Health sensor
Dell EMC Unity Enclosure Health v2 sensor
Dell EMC Unity File System v2 sensor
Dell EMC Unity Storage Capacity v2 sensor
Dell EMC Unity Storage LUN v2 sensor
Dell EMC Unity Storage Pool v2 sensor
Dell EMC Unity VMware Datastore v2 sensor
DICOM Bandwidth sensor

Supported Sensors
DICOM C-ECHO sensor
DICOM Query/Retrieve sensor
DNS v2 sensor
Docker Container Status sensor
FortiGate System Statistics sensor
FTP sensor
FTP Server File Count sensor
HL7 sensor
HPE 3PAR Common Provisioning Group sensor
HPE 3PAR Drive Enclosure sensor
HPE 3PAR Virtual Volume sensor
HTTP sensor
HTTP Advanced sensor
HTTP Apache ModStatus PerfStats sensor
HTTP Apache ModStatus Totals sensor
HTTP Content sensor
HTTP Data Advanced sensor
HTTP IoT Push Data Advanced sensor
HTTP Transaction sensor
HTTP XML/REST Value sensor
IMAP sensor

Supported Sensors
IP on DNS Blacklist sensor
LDAP sensor
Microsoft 365 Mailbox sensor
Microsoft 365 Service Status sensor
Microsoft 365 Service Status Advanced sensor
Microsoft Azure SQL Database sensor
Microsoft Azure Storage Account sensor
Microsoft Azure Subscription Cost sensor
Microsoft Azure Virtual Machine sensor
Modbus TCP Custom sensor
MQTT Round Trip sensor
MQTT Statistics sensor
MQTT Subscribe Custom sensor
NetApp Aggregate sensor
NetApp I/O sensor
NetApp LIF sensor
NetApp LUN sensor
NetApp NIC sensor
NetApp Physical Disk sensor
NetApp SnapMirror sensor
NetApp System Health sensor



Supported Sensors
NetApp Volume sensor
NetApp Volume v2
OPC UA Certificate sensor
OPC UA Custom sensor
OPC UA Server Status sensor
Ping sensor
Ping Jitter sensor
POP3 sensor
Probe Health sensor
RADIUS v2 sensor
RDP (Remote Desktop) sensor
Redfish Power Supply sensor
Redfish System Health sensor
REST Custom sensor
Sensor Factory sensor
SFTP Secure File Transfer Protocol sensor
SIP Options Ping sensor
SMTP&IMAP Round Trip sensor
SMTP&POP3 Round Trip sensor
SNMP APC Hardware sensor
SNMP Buffalo TS System Health sensor

Supported Sensors
SNMP Cisco ADSL sensor
SNMP Cisco ASA VPN Connections sensor
SNMP Cisco ASA VPN Traffic sensor
SNMP Cisco ASA VPN Users sensor
SNMP Cisco CBQoS sensor
SNMP Cisco System Health sensor
SNMP Cisco UCS Blade sensor
SNMP Cisco UCS Chassis sensor
SNMP Cisco UCS Physical Disk sensor
SNMP Cisco UCS System Health sensor
SNMP CPU Load sensor
SNMP Custom sensor
SNMP Custom Advanced sensor
SNMP Custom String sensor
SNMP Custom String Lookup sensor
SNMP Custom Table sensor
SNMP Dell EqualLogic Logical Disk sensor
SNMP Dell EqualLogic Member Health sensor
SNMP Dell EqualLogic Physical Disk sensor
SNMP Dell Hardware sensor
SNMP Dell PowerEdge Physical Disk sensor

Supported Sensors
SNMP Dell PowerEdge System Health sensor
SNMP Disk Free sensor
SNMP Fujitsu System Health v2 sensor
SNMP Hardware Status sensor
SNMP HP LaserJet Hardware sensor
SNMP HPE BladeSystem Blade sensor
SNMP HPE BladeSystem Enclosure Health sensor
SNMP HPE ProLiant Logical Disk sensor
SNMP HPE ProLiant Memory Controller sensor
SNMP HPE ProLiant Network Interface sensor
SNMP HPE ProLiant Physical Disk sensor
SNMP HPE ProLiant System Health sensor
SNMP IBM System X Logical Disk sensor
SNMP IBM System X Physical Disk sensor
SNMP IBM System X Physical Memory sensor
SNMP IBM System X System Health sensor
SNMP interSeptor Pro Environment sensor
SNMP Juniper NS System Health sensor
SNMP LenovoEMC Physical Disk sensor
SNMP LenovoEMC System Health sensor
SNMP Library sensor


Supported Sensors
SNMP Linux Disk Free sensor
SNMP Linux Load Average sensor
SNMP Linux Meminfo sensor
SNMP Linux Physical Disk sensor
SNMP Memory sensor
SNMP NetApp Disk Free sensor
SNMP NetApp Enclosure sensor
SNMP NetApp I/O sensor
SNMP NetApp License sensor
SNMP NetApp Logical Unit sensor
SNMP NetApp Network Interface sensor
SNMP NetApp System Health sensor
SNMP Nutanix Cluster Health sensor
SNMP Nutanix Hypervisor sensor
SNMP Poseidon Environment sensor
SNMP Printer sensor
SNMP QNAP Logical Disk sensor
SNMP QNAP Physical Disk sensor
SNMP QNAP System Health sensor
SNMP Rittal CMC III Hardware Status sensor
SNMP RMON sensor

Supported Sensors
SNMP SonicWall System Health sensor
SNMP SonicWall VPN Traffic sensor
SNMP Synology Logical Disk sensor
SNMP Synology Physical Disk sensor
SNMP Synology System Health sensor
SNMP System Uptime sensor
SNMP Traffic sensor
SNMP Windows Service sensor
SNTP sensor
Soffico Orchestra Channel Health sensor
SSH Disk Free sensor
SSH INodes Free sensor
SSH Load Average sensor
SSH Meminfo sensor
SSH Remote Ping sensor
SSH SAN Enclosure sensor
SSH SAN Logical Disk sensor
SSH SAN Physical Disk sensor
SSH SAN System Health sensor
SSH Script sensor
SSH Script Advanced sensor

Supported Sensors
SSL Certificate sensor
SSL Security Check sensor
System Health sensor
TFTP sensor
Traceroute Hop Count sensor
Veeam Backup Job Status sensor
Veeam Backup Job Status Advanced sensor
VMware Datastore (SOAP) sensor
VMware Host Hardware (WBEM) sensor
VMware Host Hardware Status (SOAP) sensor
VMware Host Performance (SOAP) sensor
VMware Virtual Machine (SOAP) sensor
Zoom Service Status sensor

## Sensors on a Classic Remote Probe Device

You can use the following sensors only on a [classic remote probe](#) [3198] device.

 For performance reasons, you cannot add these sensors to the hosted probe of PRTG Hosted Monitor.

Supported Sensors
Active Directory Replication Errors sensor
ADO SQL v2 sensor
Dell PowerVault MDi Logical Disk sensor

Supported Sensors
Dell PowerVault MDi Physical Disk sensor
DHCP sensor
Enterprise Virtual Array sensor
Event Log (Windows API) sensor
Exchange Backup (PowerShell) sensor
Exchange Database DAG (PowerShell) sensor
Exchange Database (PowerShell) sensor
Exchange Mailbox (PowerShell) sensor
Exchange Mail Queue (PowerShell) sensor
Exchange Public Folder (PowerShell) sensor
EXE/Script sensor
EXE/Script Advanced sensor
File sensor
File Content sensor
Folder sensor
HTTP Full Web Page sensor
HTTP Push Count sensor
HTTP Push Data sensor
HTTP Push Data Advanced sensor
Hyper-V Cluster Shared Volume Disk Free sensor
Hyper-V Host Server sensor

Supported Sensors
Hyper-V Virtual Machine sensor
Hyper-V Virtual Network Adapter sensor
Hyper-V Virtual Storage Device sensor
IPFIX sensor
IPFIX (Custom) sensor
IPMI System Health sensor
jFlow v5 sensor
jFlow v5 (Custom) sensor
Microsoft SQL v2 sensor
MySQL v2 sensor
NetFlow v5 sensor
NetFlow v5 (Custom) sensor
NetFlow v9 sensor
NetFlow v9 (Custom) sensor
Oracle SQL v2 sensor
Oracle Tablespace sensor
Packet Sniffer sensor
Packet Sniffer (Custom) sensor
PerfCounter Custom sensor
PerfCounter IIS Application Pool sensor
Port sensor



Supported Sensors
Port Range sensor
PostgreSQL sensor
Python Script Advanced sensor
QoS (Quality of Service) One Way sensor
QoS (Quality of Service) Round Trip sensor
sFlow sensor
sFlow (Custom) sensor
Share Disk Free sensor
SMTP sensor
SNMP Trap Receiver sensor
Syslog Receiver sensor
Windows CPU Load sensor
Windows IIS Application sensor
Windows MSMQ Queue Length sensor
Windows Network Card sensor
Windows Pagefile sensor
Windows Physical Disk I/O sensor
Windows Print Queue sensor
Windows Process sensor
Windows SMTP Service Received sensor
Windows SMTP Service Sent sensor

Supported Sensors
Windows System Uptime sensor
Windows Updates Status (PowerShell) sensor
WMI Battery sensor
WMI Custom sensor
WMI Custom String sensor
WMI Disk Health sensor
WMI Event Log sensor
WMI Exchange Server sensor
WMI Exchange Transport Queue sensor
WMI File sensor
WMI Free Disk Space (Multi Disk) sensor
WMI HDD Health sensor
WMI Logical Disk I/O sensor
WMI Memory sensor
WMI Microsoft SQL Server 2005 sensor (Deprecated)
WMI Microsoft SQL Server 2008 sensor
WMI Microsoft SQL Server 2012 sensor
WMI Microsoft SQL Server 2014 sensor
WMI Microsoft SQL Server 2016 sensor
WMI Microsoft SQL Server 2017 sensor
WMI Microsoft SQL Server 2019 sensor

Supported Sensors
WMI Remote Ping sensor
WMI Security Center sensor
WMI Service sensor
WMI Share sensor
WMI SharePoint Process sensor
WMI Storage Pool sensor
WMI Terminal Services (Windows 2008+) sensor
WMI Terminal Services (Windows XP/Vista/2003) sensor
WMI UTC Time sensor
WMI Vital System Data v2 sensor
WMI Volume sensor
WSUS Statistics sensor

## Settings

 These settings are only available in PRTG Network Monitor.

Setting Title	Setting Name
Auto-Update	When a New Version is Available
	Installation Time
	Release Channel
Notification Templates	Add Entry to Event Log
	Send Syslog Message

Setting Title	Setting Name
	Send SNMP Trap
	Execute Program
Core & Probes	Proxy Configuration
	Probe Connection IP Addresses
	Mini Probes
	Mini Probe Port
Administrative Tools For Probes	Restart Probe (local probe)
Scanning Intervals	Available Intervals (definition of individual intervals)
Notification Delivery	SMTP Delivery (everything but sender email address and name)
Recommended Sensors Detection	Detection Handling
User Interface (PRTG Web Interface)	DNS Name
	Google Analytics Tracking ID
User Interface (PRTG Web Server)	IP Address for PRTG Web Server
	TCP Port for PRTG Web Server
	PRTG Web Server Port
	PRTG Web Server Security
	Connection Security
	Active IP Address/Port Combinations
User Accounts	Login Name
	Password

Setting Title	Setting Name
	Passhash
Administrative Tools For The PRTG Core Server	Create Configuration Snapshot
	Write Core Status File
	Clear Caches
	Load Lookups and File Lists
	Recalculate PRTG Graph Data Cache
	Restart PRTG Core Server Service
	Reload Logging Configuration
Advanced Network Analysis	System Information
Scheduled Restart Settings (Local Probe)	Restart Options
	Restart Schedule
	Specify Day
	Specify Hour

## 15.5 Escape Special Characters and Whitespaces in Parameters

You must escape special characters in parameters that you pass to an executable or script and surround them with quotation marks to make sure that the characters are correctly interpreted. PowerShell scripts in particular require adequate escaping so that the parameters are passed in a valid PowerShell syntax. PRTG automatically does most of the escaping for you.

Follow these rules to escape special characters and whitespaces in the parameters fields:

- Use double (") or single (') quotation marks for parameters that contain whitespaces.

```
-name "Mr John Q Public"
-name 'Mr John Q Public'
```

- Use double quotation marks (") for parameters that already contain single quotation marks (').

```
-name "Mr 'John Q' Public"
```

- Use single quotation marks (') for parameters that already contain double quotation marks (").

```
-name 'Mr "John Q" Public'
```

- Use a backslash (\) to escape and pass a literal double quotation mark.

```
-name pub\"lic
```

- Use double quotation marks (") for parameters that contain double (") and single (') quotation marks and escape double quotation marks (").

```
-name "pu'b\"lic"
```

**i** In SSH scripts, you can use alphanumeric characters and the special characters ".", "\_", "-", "=", and "/" outside of quoted strings.

**i** We recommend that you do not pass passwords in parameters. Use placeholders instead. For more information, see section [Custom Sensors](#) <sup>3148</sup>.

## 15.6 Glossary

This section explains PRTG-specific terminology.

### A

Alarms	The <a href="#">alarms</a> list shows all <a href="#">sensors</a> that are in the Down, Down (Partial), Down (Acknowledged), Warning, or Unusual <a href="#">status</a> . The alarms list shows you all irregularities in your network.
Auto-discovery	The <a href="#">auto-discovery</a> process uses ping to scan your network for <a href="#">devices</a> (for <a href="#">groups</a> only). It assesses the device type for all discovered devices, and it creates <a href="#">sensor</a> sets that match the discovered device types based on built-in templates or your custom <a href="#">device templates</a> .

### C

Channel	The monitoring data of a <a href="#">sensor</a> is shown in <a href="#">channels</a> . For example, sensors that measure network traffic have one channel each for traffic <a href="#">in</a> , traffic <a href="#">out</a> , and traffic <a href="#">total</a> . You can set various <a href="#">triggers</a> for each channel to define <a href="#">sensor status</a> changes or <a href="#">notifications</a> based on the monitoring data received.
Classic remote probe	A <a href="#">classic remote probe</a> is a small piece of software that is installed on a Windows system in the local or remote network. It is one of three types of <a href="#">remote probes</a> . It scans the network and sends monitoring results to the <a href="#">PRTG core server</a> . Once the connection has been established, the classic remote probe is shown in the <a href="#">device tree</a> . You can add <a href="#">groups</a> and <a href="#">devices</a> to the classic remote probe.
Cluster	A <a href="#">cluster</a> consists of two or more <a href="#">PRTG core servers</a> that work together to form a high availability monitoring system. A cluster consists of a <a href="#">master node</a> and one or more <a href="#">failover nodes</a> . Every <a href="#">cluster node</a> can monitor every <a href="#">device</a> in a network for fail-safe monitoring.
Cluster node	<a href="#">Cluster nodes</a> make up a cluster. Cluster nodes can be <a href="#">master nodes</a> or <a href="#">failover nodes</a> .
Cluster probe	When you create or join a <a href="#">cluster</a> , PRTG automatically creates a <a href="#">cluster probe</a> . All <a href="#">objects</a> that you create on the cluster probe (or below in the <a href="#">device tree</a> ) are monitored by all <a href="#">cluster nodes</a> . Create or move <a href="#">objects</a> there for fail-safe monitoring. If one cluster node fails, the other cluster nodes continue to monitor all objects. You can add <a href="#">groups</a> and <a href="#">devices</a> to the cluster probe. The cluster probe runs as part of the <a href="#">local probe</a> .

Cluster probe device	The <a href="#">cluster probe device</a> is an internal system device that PRTG automatically adds to the <a href="#">cluster probe</a> <sup>[3313]</sup> . It has access to the <a href="#">cluster node</a> <sup>[3313]</sup> system and monitors its health parameters using several <a href="#">sensors</a> <sup>[3320]</sup> .
----------------------	---

## D

Dashboard	A preconfigured sample <a href="#">dashboard</a> is available in the Home menu of the PRTG web interface. Dashboards provide an overview of the overall status of your monitoring configuration. You can create custom dashboards using the <a href="#">Maps</a> <sup>[3316]</sup> feature.
Device	A <a href="#">device</a> represents a physical or virtual component in your network that is reachable via an IP address. For a clear <a href="#">device tree</a> <sup>[3314]</sup> structure, you usually create one device for each physical or virtual component that you want to monitor. You can add one or more <a href="#">sensors</a> <sup>[3320]</sup> to a device.
Device template	If you want to add a specific <a href="#">device</a> <sup>[3314]</sup> several times, you can create a <a href="#">device template</a> from a device in the <a href="#">device tree</a> <sup>[3314]</sup> . When you create a device template, PRTG saves information for nearly all <a href="#">sensors</a> <sup>[3320]</sup> on the device to a template file. You can later use the template file in combination with the <a href="#">auto-discovery</a> <sup>[3313]</sup> (restrictions apply for a few sensor types).
Device tree	The configuration of PRTG is represented in a hierarchical tree structure called the <a href="#">device tree</a> , which contains all monitoring <a href="#">objects</a> <sup>[3317]</sup> . While building the device tree, you can relate to your network's topology to make your monitoring setup more understandable.

## F

Failover master node	If the <a href="#">primary master node</a> <sup>[3317]</sup> of a <a href="#">cluster</a> <sup>[3313]</sup> fails, a <a href="#">failover node</a> <sup>[3314]</sup> becomes a <a href="#">failover master node</a> . The failover master node takes over the role of the primary master node until it reconnects to the cluster.
Failover node	In a <a href="#">cluster</a> <sup>[3313]</sup> , a <a href="#">failover node</a> monitors all <a href="#">sensors</a> <sup>[3320]</sup> on the <a href="#">cluster probe</a> <sup>[3313]</sup> and it provides monitoring data for the <a href="#">PRTG core server</a> <sup>[3318]</sup> . Additionally, it serves as a backup in case the <a href="#">master node</a> <sup>[3316]</sup> fails.
Flows	PRTG supports NetFlow v5, NetFlow v9, IPFIX, sFlow v5, and jFlow v5.



G

Gauge	A <a href="#">gauge</a> is a type of visual representation of the values of a <a href="#">channel</a> <sup>[3313]</sup> . The gauge needle points to the current value of the channel. Other types of visual representations are <a href="#">toggles</a> <sup>[3320]</sup> and <a href="#">switches</a> <sup>[3320]</sup> .
Geo Maps	The <a href="#">Geo Maps</a> feature shows the different locations of your <a href="#">devices</a> <sup>[3314]</sup> on a geographical map using the location data that you provide in the settings of <a href="#">probes</a> <sup>[3317]</sup> , <a href="#">groups</a> <sup>[3315]</sup> , or devices. The status icons on the geographical maps that represent your devices also show the overall status of a location. This is useful for monitoring distributed networks.
Group	A <a href="#">group</a> is an organizational unit in the <a href="#">device tree</a> <sup>[3314]</sup> . You can add <a href="#">devices</a> <sup>[3314]</sup> or subgroups to groups. This way, you can model your physical network's topology within the PRTG configuration. You can use groups to arrange similar objects so that they inherit the same settings.

H

Hosted probe	The <a href="#">hosted probe</a> in PRTG Hosted Monitor is like the <a href="#">local probe</a> <sup>[3316]</sup> in PRTG Network Monitor. When you create a PRTG Hosted Monitor instance, the system automatically adds the hosted probe. The hosted probe runs on the <a href="#">PRTG core server system</a> <sup>[3318]</sup> that we host for you and it shows the monitoring values of your PRTG Hosted Monitor instance. You can use the hosted probe to monitor <a href="#">devices</a> <sup>[3314]</sup> , servers, and services that are publicly available on the internet like, for example, websites. To monitor your LAN, you need at least one <a href="#">remote probe</a> <sup>[3319]</sup> installation in your network. The local probe and the multi-platform probe are not available in PRTG Hosted Monitor.
--------------	---

L

Library	A <a href="#">library</a> enables you to create additional views of your <a href="#">device tree</a> <sup>[3314]</sup> . These views are updated in the same scanning interval as your device tree and show the same monitoring data, but arranged the way you want. This is useful if you want to display data in different ways, like depending on target groups or a specific use case.
Library node	<a href="#">Libraries</a> <sup>[3315]</sup> use <a href="#">library nodes</a> to reference <a href="#">objects</a> <sup>[3317]</sup> in your monitoring setup. Library nodes can show a subtree of the <a href="#">device tree</a> <sup>[3314]</sup> or they can show a collection of filtered <a href="#">sensors</a> <sup>[3320]</sup> .
Limit	<a href="#">Limits</a> let you define thresholds for <a href="#">channel</a> <sup>[3313]</sup> values. When the value of a channel is above or below the defined limit, the sensor can show the Warning or Down status.

Local probe	When installing PRTG Network Monitor, the <a href="#">local probe</a> is installed together with the <a href="#">PRTG core server</a> . All <a href="#">objects</a> created on the local probe, or underneath it in the <a href="#">device tree</a> , are monitored by the local PRTG core server system. You can add <a href="#">groups</a> and <a href="#">devices</a> to the local probe. If you use PRTG Hosted Monitor, the <a href="#">hosted probe</a> replaces the local probe.
Local probe device	The <a href="#">local probe device</a> is an internal system device that PRTG automatically adds to the <a href="#">local probe</a> . It has access to the <a href="#">local probe system</a> and monitors its health parameters using several <a href="#">sensors</a> .
Lookup	PRTG uses <a href="#">lookups</a> for some <a href="#">sensor</a> types and for some sensors with custom <a href="#">channels</a> . In general, lookups map status values as returned by a <a href="#">device</a> (usually integers) to more informative expressions in words.

**M**

Maps	The <a href="#">Maps</a> feature lets you present monitoring data the way you want it. An editor is available that lets you create maps (sometimes referred to as <a href="#">dashboards</a> ) directly in your browser. Using maps, you can also make overviews of live data publicly available.
Master node	In a <a href="#">cluster</a> , the <a href="#">master node</a> controls the settings and cluster management. It also takes over notifications. All changes to the monitoring configuration are made on the master node, which distributes the changes among all other cluster nodes in real time. There are two types of master nodes: <a href="#">primary master node</a> and <a href="#">failover master node</a> .
Meta-scan	Sensors that use the <a href="#">meta-scan</a> feature, for example SNMP sensors, first look at the according <a href="#">device</a> to find what they can monitor. This can be tables, object identifiers (OID), or disks, for example. When the meta-scan is finished, the second step of the <a href="#">Add Sensor</a> dialog shows you the parameters that you can monitor. Some sensors require basic information before they can perform a meta-scan. Provide the requested information, such as credentials, in the appearing dialog box. PRTG then scans and recognizes all parameters that are available for monitoring based on your input.
Mini probe	With a <a href="#">mini probe</a> , you can create small <a href="#">probes</a> on any <a href="#">device</a> (not only on Windows systems). It is one of three types of <a href="#">remote probes</a> .
Multi-platform probe	A <a href="#">multi-platform probe</a> is a small piece of software that is installed on a Linux system in a remote network. It is one of three types of <a href="#">remote probes</a> . It scans the network and sends monitoring results to the <a href="#">PRTG core server</a> via a NATS server. Once the connection has been established, the multi-platform probe is shown in the <a href="#">device tree</a> . You can add <a href="#">groups</a> and <a href="#">devices</a> to the multi-platform probe.

N

Notification	PRTG uses <a href="#">notifications</a> to send you alerts whenever it discovers a defined status, such as slow <a href="#">sensors</a> <sup>[3320]</sup> , or when <a href="#">channels</a> <sup>[3313]</sup> breach threshold values. You can define an unlimited number of notifications. You can use one or more of several notification methods like email, text messaging, push notifications to Android and iOS devices, and more.
Notification trigger	PRTG sends a <a href="#">notification</a> <sup>[3317]</sup> when a defined event triggers it. These events are known as <a href="#">notification triggers</a> . The following events can trigger notifications: <a href="#">sensor status</a> <sup>[3320]</sup> changes, <a href="#">sensor</a> <sup>[3320]</sup> value threshold breaches, speed threshold breaches, volume threshold breaches, and sensor value changes.

O

Object	All types of items in the <a href="#">device tree</a> <sup>[3314]</sup> are generally referred to as <a href="#">objects</a> , or <a href="#">monitoring objects</a> . An object can be a <a href="#">probe</a> <sup>[3317]</sup> , a <a href="#">group</a> <sup>[3315]</sup> , a <a href="#">device</a> <sup>[3314]</sup> , or a <a href="#">sensor</a> <sup>[3320]</sup> .
Object hierarchy	All <a href="#">objects</a> <sup>[3317]</sup> are arranged in a hierarchical order called the <a href="#">object hierarchy</a> . The object hierarchy is used to define common settings for groups of objects.
Object selector	The <a href="#">object selector</a> lets you browse all <a href="#">objects</a> <sup>[3317]</sup> in your configuration and lets you select an object. The left-hand side shows the <a href="#">device tree</a> <sup>[3314]</sup> . If you have selected a <a href="#">device</a> <sup>[3314]</sup> , the right-hand side shows the <a href="#">sensors</a> <sup>[3320]</sup> on the device.

P

Primary group	Every user has to be a member of a <a href="#">primary group</a> to make sure there is no user without group membership. Membership in other user groups is optional.
Primary master node	In a <a href="#">cluster</a> <sup>[3313]</sup> , the <a href="#">primary master node</a> is the <a href="#">cluster node</a> <sup>[3313]</sup> that is the <a href="#">master node</a> <sup>[3316]</sup> by configuration.
Probe	A <a href="#">probe</a> is where the actual monitoring takes place. There are <a href="#">local probes</a> <sup>[3316]</sup> , <a href="#">cluster probes</a> <sup>[3313]</sup> , <a href="#">remote probes</a> <sup>[3319]</sup> , <a href="#">hosted probes</a> <sup>[3315]</sup> , and <a href="#">multi-platform probes</a> <sup>[3316]</sup> .
Probe device	The <a href="#">probe device</a> is an internal system device that PRTG automatically adds to the <a href="#">probe</a> <sup>[458]</sup> . It has access to the <a href="#">probe system</a> <sup>[3318]</sup> and monitors its health parameters using several <a href="#">sensors</a> <sup>[3320]</sup> .

<p>Probe system</p>	<p>A <a href="#">probe system</a> is the system, or Windows computer, that runs a <a href="#">probe</a>. A <a href="#">remote probe</a>, a <a href="#">cluster probe</a>, and the <a href="#">local probe</a> run on a probe system.</p>
<p>PRTG Administration Tool</p>	<p>The <a href="#">PRTG Administration Tool</a> is part of your PRTG installation. You can use it to edit the administrative settings of the <a href="#">local probe</a> and <a href="#">remote probe</a> installations. You can start the PRTG Administration Tool from the Windows Start menu on the <a href="#">PRTG core server system</a> or on the <a href="#">remote probe system</a>.</p>
<p>PRTG app for desktop</p>	<p>The <a href="#">PRTG app for desktop</a> is an alternative interface that you can use to connect to the <a href="#">PRTG core server</a> or a PRTG Hosted Monitor instance to configure your setup, view monitoring results, and keep an eye on your network. It is a cross-platform application for fast access to data and monitoring management.</p>
<p>PRTG Application Programming Interface (PRTG API)</p>	<p>The <a href="#">PRTG API</a> enables you to access monitoring data and to manipulate <a href="#">objects</a> using HTTP requests, to run your own written <a href="#">sensors</a> and <a href="#">notifications</a>, and to implement <a href="#">mini probes</a>.</p>
<p>PRTG Cloud</p>	<p><a href="#">PRTG Cloud</a> is used by the <a href="#">Cloud HTTP v2</a> sensor and the <a href="#">Cloud Ping v2</a> sensor to monitor the loading times of a web server via HTTP or the Transmission Control Protocol (TCP) ping times to a parent device from different locations worldwide. PRTG also sends push notifications and securely transmits support bundles to Paessler via PRTG Cloud.</p>
<p>PRTG core server</p>	<p>The <a href="#">PRTG core server</a> is the central unit of PRTG. It receives monitoring data from the <a href="#">probe</a> and handles reporting and notifications, provides the web server for the user interfaces, and much more. In a <a href="#">cluster</a>, one PRTG core server is installed on every <a href="#">cluster node</a>. The PRTG core server is configured as a Windows service that is permanently run by the Windows system without requiring a user that is logged in.</p>
<p>PRTG core server service</p>	<p>The <a href="#">PRTG core server service</a> is responsible for running the <a href="#">PRTG core server</a>. It is a Windows service that permanently runs on the <a href="#">PRTG core server system</a>.</p>
<p>PRTG core server system</p>	<p>The <a href="#">PRTG core server system</a> is the system, or Windows computer, that runs the <a href="#">PRTG core server</a>.</p>
<p>PRTG data directory</p>	<p>The <a href="#">PRTG data directory</a> is the directory on the <a href="#">PRTG core server system</a> or <a href="#">remote probe system</a> where PRTG stores monitoring data, configuration data, and logs.</p>
<p>PRTG Hosted Monitor</p>	<p><a href="#">PRTG Hosted Monitor</a> is the PRTG cloud solution where we at Paessler run the <a href="#">PRTG core server</a> and <a href="#">hosted probe</a> for you. PRTG Hosted Monitor does not require a PRTG core server installation inside your network.</p>

PRTG Network Monitor	<a href="#">PRTG Network Monitor</a> is a network monitoring application for Windows-based systems with which you can monitor your entire network. PRTG Network Monitor requires a <a href="#">PRTG core server</a> installation inside your network.
PRTG probe service	The <a href="#">PRTG probe service</a> is responsible for running a <a href="#">probe</a> . It is a Windows service that permanently runs on the <a href="#">probe system</a> .
PRTG program directory	The <a href="#">PRTG program directory</a> is the directory on the <a href="#">PRTG core server system</a> where PRTG stores all files that are required for it to run.
PRTG web interface	The <a href="#">PRTG web interface</a> is the Asynchronous JavaScript and XML (AJAX) based web interface of PRTG. It is the default interface for setting up your monitoring.

**R**

Recommended Sensors Detection	The <a href="#">Recommended Sensors Detection</a> feature enables PRTG to analyze <a href="#">devices</a> in your network and to suggest sensors that are still missing for a comprehensive monitoring setup. If enabled, the analysis runs in the background with low priority if you add a new device, if the last analysis was executed more than 30 days ago, or if you manually start it.
Release channel	PRTG updates are delivered in different <a href="#">release channels</a> . With PRTG Network Monitor, you can choose between maximum stability ( <a href="#">Stable</a> ), or most early access to new features ( <a href="#">Canary</a> or <a href="#">Preview</a> ). PRTG Hosted Monitor does not have release channels. Instead, we roll out the latest stable version to PRTG Hosted Monitor instances in stages, so your instance automatically updates to the latest stable version.
Remote probe	A <a href="#">remote probe</a> is a small piece of software that is installed on a computer, or <a href="#">remote probe system</a> , in the local or remote network. It scans the network and sends monitoring results to the <a href="#">PRTG core server</a> . Once the connection has been established, the remote probe is shown in the <a href="#">device tree</a> . All <a href="#">objects</a> that you create on the remote probe, or below it in the device tree, are monitored by the remote probe system. You can add <a href="#">groups</a> and <a href="#">devices</a> to the remote probe. In a <a href="#">cluster</a> , remote probes can connect to all cluster nodes so you can view monitoring data of a remote probe on all <a href="#">cluster nodes</a> .
Remote probe device	The <a href="#">remote probe device</a> is an internal system device that PRTG automatically adds to the <a href="#">remote probe</a> . It has access to the <a href="#">remote probe system</a> and monitors its health parameters using several <a href="#">sensors</a> .
Remote probe system	The <a href="#">remote probe system</a> is the system, such as a Windows or Linux computer, that runs a <a href="#">remote probe</a> .

Root group	The <a href="#">root group</a> is the topmost instance in the <a href="#">object hierarchy</a> [3317] in the device tree. It contains all <a href="#">objects</a> [3317] in your monitoring setup. All objects inherit the settings of the root group by default.
------------	---

## S

Schedule	You can use <a href="#">schedules</a> to pause monitoring or notifications for certain periods of time or at certain times. You can also use schedules to define the periods of time that are covered when creating reports.
Sensor	A <a href="#">sensor</a> monitors one aspect of a <a href="#">device</a> [3314]. For example, one sensor monitors if a device responds to a ping request. A different sensor monitors the traffic of one Ethernet port of a router, and so on. The data of sensors is shown in their respective <a href="#">channels</a> [3313]. Each sensor has at least one channel.
Sensor status	The color of a <a href="#">sensor</a> [3320] represents the <a href="#">sensor status</a> . There are 8 different sensor states: Down, Down (Partial), Down (Acknowledged), Warning, Unusual, Up, Paused, and Unknown.
Similar Sensors Detection	The <a href="#">Similar Sensors Detection</a> feature enables PRTG to analyze <a href="#">sensor</a> [3320] data for similarities. If enabled, the detection runs in the background with low priority. The recommended setting for the analysis depth is to let PRTG automatically decide how many <a href="#">channels</a> [3313] it analyzes.
Switch	A <a href="#">switch</a> is a type of visual representation of the values of a <a href="#">channel</a> [3313]. Switches represent boolean values when using <a href="#">lookups</a> [3316].

## T









Tickets	<a href="#">Tickets</a> are created by the system or by a user and contain important messages or action steps for the administrator or other users to take. You should view every <a href="#">ticket</a> [213] to take appropriate action. You can access the list of tickets from the main menu.
Toggle	A <a href="#">toggle</a> is a type of visual representation of the values of a <a href="#">channel</a> [3313]. Toggles represent bitfields when using <a href="#">lookups</a> [3316].
Toplist	Packet Sniffer and Flow (NetFlow, jFlow, sFlow, IPFIX) <a href="#">sensor</a> [3320] types can break down traffic by IP address, port, protocol, and other parameters. The results are shown in graphs that are called <a href="#">Toplists</a> .

## U

Unusual Detection	The <b>Unusual Detection</b> feature can set <a href="#">sensors</a> to the Unusual <a href="#">status</a> when it detects values that are not typical for the time span in which they are measured. If the detection is enabled, PRTG compares the current average values to the historic monitoring results for this purpose. If the current values show a big difference to the values that are normally retrieved by a sensor, this sensor indicates this with the Unusual status.
-------------------	--

## 15.7 Icons

See below for a list of icons used in this documentation.

	Notes that contain additional information.
	Notes that contain critical information on the functioning of PRTG. Pay close attention to this information to avoid serious consequences for PRTG.
	There is more information on this topic in a different section of the PRTG Manual or in the Knowledge Base.
	This feature is in beta status and might not function properly in all situations.
	There is a video on this topic.
	Examples on how to use a feature.
	This information is relevant for PRTG Hosted Monitor.
	This information is relevant for PRTG Network Monitor.
	There is a Paessler tool that you can use.
	There is more information on this topic in the PRTG Manual, the Knowledge Base, the Paessler Blog, on the Paessler website, or on other websites. This icon is only used in More sections.



## 15.8 Legal Notices

See below for an excerpt of the libraries and licenses that PRTG uses:

- Build using Indy Internet Direct (<https://www.indyproject.org/>).  
This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com))
- Uses the net-SNMP library, see [netsnmp-license.txt](#)
- Uses Python under the Python Software Foundation License (<https://docs.python.org/3.7/license.html#psf-license-agreement-for-python-release>)
- Uses NexusMM (<https://www.nexusdb.com/>)
- Delphi Chromium Embedded (<https://code.google.com/archive/p/delphichromiumembedded/>) under the Mozilla Public License 1.1 (MPL 1.1, available from <http://www.mozilla.org/en-US/MPL/1.1/>)
- Soundfiles from <https://www.soundsnap.com/>
- Uses Public Domain regional maps from "The World Factbook 2016-17" Washington, DC: Central Intelligence Agency, 2016 (<https://www.cia.gov/library/publications/the-world-factbook/docs/refmaps.html>)
- Icons from <https://www.androidicons.com/>
- Uses the IPMIUTIL library under the BSD 2.0 license, see [ipmi\\_bsd-2.0.txt](#)
- Uses PhantomJS, see [phantomjs-license.bsd](#)
- Uses the Npgsql .Net Data Provider for Postgresql library (for license information see [ipmi\\_bsd-2.0.txt](#))
- Uses NPcap (<https://nmap.org/npcap/oem/redist.html>)
- Uses GeoLite2 data created by MaxMind (<https://www.maxmind.com>)
- Uses OpenSSL developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)  
This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com))

Code libraries using

- MIT (<https://opensource.org/licenses/MIT>)
- MPL 1.1 (<https://www.mozilla.org/media/MPL/1.1/index.0c5913925d40.txt>)
- MPL 2.0 (<https://www.mozilla.org/media/MPL/2.0/index.815ca599c9df.txt>)
- APL 2.0 (<https://www.apache.org/licenses/LICENSE-2.0.txt>)
- BSD 2.0 license (<https://opensource.org/licenses/BSD-2-Clause>)
- BSD 3.0 license (<https://opensource.org/licenses/BSD-3-Clause>)

Licenses used in previous versions of PRTG:

- FastMM (<https://sourceforge.net/projects/fastmm/>)
- TPLockBox (<https://sourceforge.net/projects/tplockbox/>)
- "wkhtmltopdf" (<https://wkhtmltopdf.org/>) library distributed under the GNU LESSER GENERAL PUBLIC LICENSE (see [wkhtmltopdf\\_lgpl-3.0.txt](#))
- WinPcap (<https://www.winpcap.org/misc/copyright.htm>)

All product names, company names, and logos referenced to or depicted herein are the trademarks™, registered® trademarks, or service marks of the respective owners. Use of them, their occurrence, or references to their occurrence in graphical representations of the PRTG web interface herein is solely for informational purposes and does not imply any affiliation with or endorsement by the respective owners.

## Privacy Policy

<https://www.paessler.com/privacy-policy>

## Terms and Conditions

<https://www.paessler.com/terms-conditions>

Last manual export: Friday, July 26, 2024 5:17:48 AM

## 15.9 Placeholders for Notifications

Here you can find a list of all placeholders for notifications. You can use placeholders in different settings fields of a notification when editing [notification templates](#).

In this section:

- [Notification Settings Fields](#)
- [Placeholders in Summarized Notifications](#)
- [Available Placeholders](#)

### Notification Settings Fields

Notification	Settings field
Send Email	<ul style="list-style-type: none"> <li>▪ Subject</li> <li>▪ Custom Text if you select the option Custom text</li> </ul>
Add Entry to Event Log	Message
Send SMS/Pager Message	Message
Execute HTTP Action	Payload if you select the options POST, PUT, or PATCH
Execute Program	Parameters
Send Syslog Message	Message
Send SNMP Trap	Message
Send Amazon Simple Notification Service Message	Message
Assign Ticket	<ul style="list-style-type: none"> <li>▪ Subject</li> <li>▪ Content</li> </ul>
Send Push Notification	Message
Send Microsoft Teams Message	<ul style="list-style-type: none"> <li>▪ Title</li> <li>▪ Subtitle</li> </ul>

Notification	Settings field
Send Slack Message	<ul style="list-style-type: none"> <li>▪ Sender Name</li> <li>▪ Title</li> <li>▪ Subtitle</li> </ul>
Send MQTT Publish Notification	Message

❗ Placeholders are **not** case-sensitive.

❗ Depending on **where** you use a placeholder in a notification, PRTG might resolve the placeholder differently. A resolved placeholder in the **body** of a notification, for example, can contain more information compared to when PRTG resolves the same placeholder in the **subject** of a notification. The reason for this is to save space in the subject line.

## Placeholders in Summarized Notifications

Placeholders in summarized notifications have limited functionality:

- PRTG does **not** resolve placeholders in the subject field of summarized notifications if more than one trigger was evoked during the summarized time span. An exception are the placeholders %sitename and %summarycount. These are **always resolved** in summarized notifications.
- If only one event is triggered during the time span you defined, PRTG does not send a summarized notification, it only sends a common notification. A summarized notification requires at least two triggered events.

## Available Placeholders

Placeholder	Resolved Content	Synonym	Comment
%colorofstate	Color of the current object status (hex code)		Might not work in older versions.
%company	Copyright string of Paessler GmbH		
%comments	Comments entered for the sensor	%commentssensor	As of PRTG 15.4.21, resolved placeholders contain the heading <b>Sensor Comments</b> .

Placeholder	Resolved Content	Synonym	Comment
%commentssensor	Comments entered for the sensor	%comments	As of PRTG 15.4.21, resolved placeholders contain the heading <a href="#">Sensor Comments</a> .
%commentsdevice	Comments entered for the parent device		As of PRTG 15.4.21, resolved placeholders contain the heading <a href="#">Device Comments</a> .
%commentsgroup	Comments entered for the parent group		As of PRTG 15.4.21, resolved placeholders contain the heading <a href="#">Group Comments</a> .
%commentsprobe	Comments entered for the parent probe		Available as of PRTG 12.4. As of PRTG 15.4.21, resolved placeholders contain the heading <a href="#">Probe Comments</a> .
%coverage	Covered time span		Might not work in older versions.
%cumsince	Since when data has been accumulated		
%date	An event's date in the time zone of the PRTG core server system		
%datetime	An event's date and time in the time zone of the PRTG core server system		
%device	Name of the device in which the event was triggered	%server	
%deviceid	ID number of the device in which the event was triggered		







Placeholder	Resolved Content	Synonym	Comment
%down	Time the item was down		
%downtime	Accumulated downtime		
%elapsed_lastcheck	Elapsed time since the sensor's last scan		Available as of PRTG 20.1.57.
%elapsed_lastdown	Elapsed time since the sensor last showed a Down status		Available as of PRTG 20.1.57.
%elapsed_lastup	Elapsed time since the sensor last showed an Up status		Available as of PRTG 20.1.57.
%group	Group in which the event was triggered		
%groupid	ID number of the group in which the event was triggered		
%history	History of sensor events		
%home	URL of the PRTG web server		
%host	IP or DNS name of the device that triggered the event		As of PRTG 13.x.7, the placeholder can be used as Agent IP in SNMP trap notifications sent by PRTG.
%iconofstate	File name including the extension of the icon for the current object status		Might not work in older versions.



Placeholder	Resolved Content	Synonym	Comment
%lastcheck	Point in time of the sensor's last scan including time stamp		
%lastdown	Point in time when the sensor last showed a Down status, including the time stamp		
%lastmessage	Message that the sensor sent the last time	%message	
%laststatus	Current sensor status		Available as of PRTG 20.1.57.
%lastup	Point in time when the sensor last showed an Up status, including the time stamp		
%lastvalue	Value that the sensor sent the last time		
%linkprobe	URL of the probe that triggered the event		Might not work in older versions.
%linkgroup	URL of the group that triggered the event		Might not work in older versions.
%linkdevice	URL of the device that triggered the event		Might not work in older versions.
%linksensor	URL of the sensor that triggered the event		Might not work in older versions.

Placeholder	Resolved Content	Synonym	Comment
%location	Location of the device or server for which the event was triggered		
%message	Message that the sensor sent the last time	%lastmessage	
%name	Name of the sensor that triggered the event, including the sensor type	%sensor	
%nodename	Name of the node if PRTG runs in a cluster		Might not work in older versions.
%objecttags	All tags of a sensor		Available as of PRTG 20.1.56.
%parenttags	All tags of a sensor's parent objects		Available as of PRTG 20.1.56.
%prio	A sensor's priority setting	%priority	
%priority	A sensor's priority setting	%prio	
%probe	Probe under which the event was triggered		
%probeid	ID number of the probe under which the event was triggered		
%programname	Official name of PRTG		
%programversion	Program version of PRTG		



Placeholder	Resolved Content	Synonym	Comment
%sensor	Name of the sensor that triggered the event, including the sensor type	%name	
%sensorid	ID number of the sensor that triggered the event		
%server	Name of the device under which the event was triggered	%device	
%serviceurl	Service URL configured for the device under which the event was triggered		Available as of PRTG 9.1.
%settings	Miscellaneous sensor settings, such as the user name for Windows, HTTP, POP3 credentials, and so on		
%shortname	Name of the sensor that triggered the event		
%since	Point in time since the current object status has been active	%statesince	
%sitename	Name of the PRTG web server		
%statesince	Point in time since the current object status has been active	%since	

Placeholder	Resolved Content	Synonym	Comment
%status	Old sensor status and current sensor status		
%summarycount	Number of events triggered during the defined time span		<p> For summarized notifications only.</p>
%syslogerrors	Max. last 20 syslog entries before the notification trigger		<p>Available as of PRTG 14.x.10.</p> <p> Works only with <a href="#">Syslog Receiver</a>.</p> <p> Can only be used in the Custom Content field of Send Email notifications.</p>
%syslogmessages	Max. last 20 syslog entries before the notification trigger		<p>Available as of PRTG 14.x.10.</p> <p> Works only with <a href="#">Syslog Receiver</a>.</p> <p> Can only be used in the Custom Content field of Send Email notifications.</p>
%syslogwarnings	Max. last 20 syslog entries before the notification trigger		<p>Available as of PRTG 14.x.10.</p> <p> Works only with <a href="#">Syslog Receiver</a>.</p> <p> Can only be used in the Custom Content field of Send Email notifications.</p>
%systemdatetime	Date and time when the notification was sent in the time zone of the PRTG core server system		
%tags	All tags of a sensor and its parent objects		Available as of PRTG 20.1.56.

Placeholder	Resolved Content	Synonym	Comment
%time	An event's time in the time zone of the PRTG core server system		
%timezone	Time zone name of the PRTG core server system		
%toaddress	Address to which the notification was sent		
%traperrors	Max. last 20 SNMP trap entries before the notification trigger		<p>Available as of PRTG 14.x.10.</p> <p> Works only with <a href="#">SNMP Trap Receiver</a>.</p> <p> Can only be used in the Custom Content field of Send Email notifications.</p>
%trapmessages	Max. last 20 SNMP trap entries before the notification trigger		<p>Available as of PRTG 14.x.10.</p> <p> Works only with <a href="#">SNMP Trap Receiver</a>.</p> <p> Can only be used in the Custom Content field of Send Email notifications.</p>
%trapwarnings	Max. last 20 SNMP trap entries before the notification trigger		<p>Available as of PRTG 14.x.10.</p> <p> Works only with <a href="#">SNMP Trap Receiver</a>.</p> <p> Can only be used in the Custom Content field of Send Email notifications.</p>
%uptime	Accumulated uptime		

- ① As of PRTG 15.4.21, PRTG uses default content in HTML email notifications. You can still change the content of emails in plain text in the Send Email notification settings and also use placeholders there.
- ① As of PRTG 16.x.24, the placeholder `%state` has been deprecated. You can use the placeholder `%status` with the same functionality instead.
- For a list of placeholders that are available for EXE/Script and other custom sensors, as well as for command-line parameters, see section [Custom Sensors](#)<sup>B137</sup>.

## 15.10 Standard Lookup Files

Here you can find a list of all PRTG standard lookup files that are located in the \lookups subfolder of the [PRTG program directory](#) <sup>[3213]</sup>.

**i** The actual number of standard lookup files in the \lookups subfolder of your PRTG installation depends on your system configuration and might differ from this list.

**■** For more information, see section [Define Lookups](#) <sup>[3187]</sup>.

Standard Lookup	Used by
oid.paessler.hplaserjet.jamstatus.ovl	SNMP HP LaserJet Hardware
oid.paessler.hplaserjet.paperstatus.ovl	SNMP HP LaserJet Hardware
oid.paessler.hplaserjet.tonerstatus.ovl	SNMP HP LaserJet Hardware
prtg.standardlookups.access.status.ovl	N/A
prtg.standardlookups.activeinactive.stateactiveok.ovl	N/A
prtg.standardlookups.activeinactive.stateless.ovl	N/A
prtg.standardlookups.apc-mib.upsbattery.upsbatteryteststatus.ovl	Device template for APC UPS
prtg.standardlookups.boolean.statefalseok.ovl	N/A
prtg.standardlookups.boolean.statetrueok.ovl	N/A
prtg.standardlookups.buffalo.ts.nasarraystatus.ovl	Device template for Buffalo TeraStation
prtg.standardlookups.buffalo.ts.nasdisksmartstatus.ovl	Device template for Buffalo TeraStation
prtg.standardlookups.buffalo.ts.nasdiskstatus.ovl	Device template for Buffalo TeraStation
prtg.standardlookups.buffalo.ts.nasfailoverstatus.ovl	SNMP Buffalo TS System Health
prtg.standardlookups.buffalo.ts.nasiscsistatus.ovl	Device template for Buffalo TeraStation

Standard Lookup	Used by
prtg.standardlookups.buffalo.ts.nasisfwupdateavailable.ovl	SNMP Buffalo TS System Health
prtg.standardlookups.buffalo.ts.nasrpsustatus.ovl	SNMP Buffalo TS System Health
prtg.standardlookups.businessprocess.state.ovl	Business Process
prtg.standardlookups.cisco.ciscoenvmonstate.ovl	SNMP Cisco System Health
prtg.standardlookups.cisco.cucs.cucsequipmentchassisconfigstate.ovl	SNMP Cisco UCS Chassis
prtg.standardlookups.cisco.cucs.cucsequipmentchassispoweroperstate.ovl	SNMP Cisco UCS Chassis
prtg.standardlookups.cisco.cucs.cucslicensestate.ovl	SNMP Cisco UCS Chassis
prtg.standardlookups.cisco.cucs.equipmentoperability.ovl	SNMP Cisco UCS Blade SNMP Cisco UCS Chassis SNMP Cisco UCS Physical Disk
prtg.standardlookups.cisco.cucs.equipmentpowerstate.ovl	SNMP Cisco UCS Blade
prtg.standardlookups.cisco.cucs.equipmentpresence.ovl	SNMP Cisco UCS Physical Disk
prtg.standardlookups.cisco.cucs.equipmentsensorthresholdstatus.ovl	SNMP Cisco UCS Chassis SNMP Cisco UCS System Health
prtg.standardlookups.cisco.cucs.lsoperstate.ovl	SNMP Cisco UCS Blade
prtg.standardlookups.cisco.sensecode.ovl	Cisco IP SLA
prtg.standardlookups.cisco.truthvalue.ovl	SNMP Cisco System Health
prtg.standardlookups.commonsaas.services.ovl	N/A
prtg.standardlookups.connectionstate.bothok.ovl	SNMP Cisco ASA VPN Users
prtg.standardlookups.connectionstate.stateonlineok.ovl	SNMP NetApp Logical Unit
prtg.standardlookups.dell.dellstatus.ovl	SNMP Dell Hardware

Standard Lookup	Used by
	SNMP Dell PowerEdge Physical Disk SNMP Dell PowerEdge System Health
prtg.standardlookups.dell.diskstate.ovl	SNMP Dell PowerEdge Physical Disk
prtg.standardlookups.dell.diskstate_idrac.ovl	SNMP Dell PowerEdge Physical Disk
prtg.standardlookups.dell.equallogic.availability.ovl	SNMP Dell EqualLogic Logical Disk
prtg.standardlookups.dell.equallogic.diskhealth.ovl	SNMP Dell EqualLogic Physical Disk
prtg.standardlookups.dell.equallogic.diskstatus.ovl	SNMP Dell EqualLogic Physical Disk
prtg.standardlookups.dell.equallogic.memberhealthstatus.ovl	SNMP Dell EqualLogic Member Health
prtg.standardlookups.dell.equallogic.memberstatus.ovl	SNMP Dell EqualLogic Member Health
prtg.standardlookups.dell.equallogic.operstatus.ovl	SNMP Dell EqualLogic Logical Disk
prtg.standardlookups.dell.equallogic.powersupplystatus.ovl	SNMP Dell EqualLogic Member Health
prtg.standardlookups.dell.equallogic.raidstatus.ovl	SNMP Dell EqualLogic Member Health
prtg.standardlookups.dell.phydisk.mode.ovl	Dell PowerVault MDi Physical Disk
prtg.standardlookups.dell.phydisk.status.ovl	Dell PowerVault MDi Physical Disk
prtg.standardlookups.disabledenabled.stateenabledok.ovl	N/A
prtg.standardlookups.disabledenabled.stateless.ovl	N/A

Standard Lookup	Used by
prtg.standardlookups.docker.containerstatus.ovl	Docker Container Status
prtg.standardlookups.emc.health.ovl	N/A
prtg.standardlookups.emc.lenovo.diskstatus.ovl	SNMP LenovoEMC Physical Disk
prtg.standardlookups.emc.lenovo.raidstatus.ovl	SNMP LenovoEMC System Health
prtg.standardlookups.esxelementhealthsensor.healthstate.ovl	VMware Host Hardware (WBEM)
prtg.standardlookups.exampledevice.ovl	N/A
prtg.standardlookups.exchangedag.activationstatus.ovl	Exchange Database DAG (PowerShell)
prtg.standardlookups.exchangedag.contentindexstate.ovl	Exchange Database DAG (PowerShell)
prtg.standardlookups.exchangedag.status.ovl	Exchange Database DAG (PowerShell)
prtg.standardlookups.exchangedag.yesno.allstatesok.ovl	Exchange Backup (PowerShell)
prtg.standardlookups.exchangedag.yesno.statenook.ovl	N/A
prtg.standardlookups.exchangedag.yesno.stateyesok.ovl	Exchange Database (PowerShell)
prtg.standardlookups.exchangedag.yesno.stateyeswarning.ovl	Exchange Database DAG (PowerShell)
prtg.standardlookups.fujitsu.fsc-raid-mib.svrctrl.svrctrlbbustatusex.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-raid-mib.svrctrl.svrctrlstatus.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-raid-mib.svrlogicaldrive.svrlogicaldriveinitstatus.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-raid-mib.svrlogicaldrive.svrlogicaldrivestatusex.ovl	SNMP Fujitsu System Health v2



Standard Lookup	Used by
prtg.standardlookups.fujitsu.fsc-raid-mib.svrphysicaldevice.svrphysicaldeviceconfiguredisk.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-raid-mib.svrphysicaldevice.svrphysicaldeviceforeignconfig.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-raid-mib.svrphysicaldevice.svrphysicaldevicepowerstatus.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-raid-mib.svrphysicaldevice.svrphysicaldevicesmartstatus.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-raid-mib.svrphysicaldevice.svrphysicaldevicestatusex.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-raid-mib.svrstatus.svrstatusoverall.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-servercontrol2-mib.sc2cpu.sc2cpustatus.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-servercontrol2-mib.sc2managementprocessor.sc2spbatterystatus.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-servercontrol2-mib.sc2memorymodule.sc2memmoduleapproved.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-servercontrol2-mib.sc2memorymodule.sc2memmoduleconfiguration.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-servercontrol2-mib.sc2memorymodule.sc2memmodulestatus.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-servercontrol2-mib.sc2powersupply.sc2powersupplystatus.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-servercontrol2-mib.sc2powersupplyredundancyconfiguration.sc2psredundancy modeconfig.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-servercontrol2-mib.sc2powersupplyredundancyconfiguration.sc2psredundancy status.ovl	SNMP Fujitsu System Health v2

Standard Lookup	Used by
prtg.standardlookups.fujitsu.fsc-servercontrol2-mib.sc2psredundancymode.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.fsc-servercontrol2-mib.sc2statuscomponent.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.fujitsu.serverview-status-mib.siestsubsystem.siestsubsystemstatusvalue.ovl	SNMP Fujitsu System Health v2
prtg.standardlookups.Google.Gsa.Health.ovl	N/A
prtg.standardlookups.hl7.ackcode.ovl	HL7
prtg.standardlookups.hp.blade.enclosure.condition.ovl	SNMP HPE BladeSystem Enclosure Health
prtg.standardlookups.hp.blade.power.ovl	SNMP HPE BladeSystem Blade
prtg.standardlookups.hp.blade.status.ovl	SNMP HPE BladeSystem Blade
prtg.standardlookups.hp.condition.ovl	SNMP HPE ProLiant Memory Controller
prtg.standardlookups.hp.diskstatus.ovl	SNMP HPE ProLiant Physical Disk
prtg.standardlookups.hp.eva.state.ovl	Enterprise Virtual Array
prtg.standardlookups.hp.logicaldiskstatus.ovl	SNMP HPE ProLiant Logical Disk
prtg.standardlookups.hp.memorycontrollererrorstatus.ovl	SNMP HPE ProLiant Memory Controller
prtg.standardlookups.hp.memorymodulestatus.ovl	SNMP HPE ProLiant Memory Controller
prtg.standardlookups.hp.powersupplystatus.ovl	SNMP HPE ProLiant System Health
prtg.standardlookups.hp.smartstatus.ovl	SNMP HPE ProLiant Physical Disk
prtg.standardlookups.hp.status.ovl	SNMP HPE ProLiant Physical Disk

Standard Lookup	Used by
	SNMP HPE ProLiant System Health
prtg.standardlookups.hp.statuswarning.ovl	N/A
prtg.standardlookups.http.statuscode.ovl	N/A
prtg.standardlookups.http.statuscodedetailed.ovl	N/A
prtg.standardlookups.hyperv.clusternodestatus.ovl	N/A
prtg.standardlookups.hyperv.communicationstate.ovl	N/A
prtg.standardlookups.hyperv.computerstate.ovl	N/A
prtg.standardlookups.hyperv.hoststatus.ovl	N/A
prtg.standardlookups.hyperv.virtualserverstate.ovl	N/A
prtg.standardlookups.hyperv.vmsstatus.ovl	N/A
prtg.standardlookups.ibm.OperationalStatus.ovl	SNMP IBM System X Logical Disk SNMP IBM System X Physical Disk SNMP IBM System X Physical Memory
prtg.standardlookups.ibm.OverallStatus.ovl	SNMP IBM System X System Health
prtg.standardlookups.ibm.psstatus.ovl	SNMP IBM System X System Health
prtg.standardlookups.ipmi.powersupply.ovl	N/A
prtg.standardlookups.juniper.fanstatus.ovl	SNMP Juniper NS System Health
prtg.standardlookups.juniper.powerstatus.ovl	SNMP Juniper NS System Health
prtg.standardlookups.lanmanager.servicestate.ovl	SNMP Windows Service

Standard Lookup	Used by
prtg.standardlookups.liebert.lgppwrbattery.lgppwrbatterycharges.tatus.ovl	Device template for Liebert UPS
prtg.standardlookups.liebert.lgppwrbattery.capacitystatus.ovl	Device template for Liebert UPS
prtg.standardlookups.liebert.lgpsysstatus.lgpsysselftestresult.ovl	Device template for Liebert UPS
prtg.standardlookups.microsoft.applicationpoolstate.ovl	PerfCounter IIS Application Pool
prtg.standardlookups.mqtt.rttstate.ovl	MQTT Round Trip v1 (deprecated)
prtg.standardlookups.multiplatformprobeconnectionhealthsensor.natsconnectionstate	Multi-Platform Probe Connection Health (Autonomous)
prtg.standardlookups.netapp.aggrstate.ovl	NetApp Aggregate
prtg.standardlookups.netapp.batterystate.ovl	NetApp System Health
prtg.standardlookups.netapp.dfstatus.ovl	SNMP NetApp Disk Free
prtg.standardlookups.netapp.fsstatus.ovl	SNMP NetApp System Health
prtg.standardlookups.netapp.healthstate.ovl	NetApp System Health
prtg.standardlookups.netapp.lunalignment.ovl	SNMP NetApp Logical Unit
prtg.standardlookups.netapp.lunstate.ovl	NetApp LUN
prtg.standardlookups.netapp.mirrorstate.ovl	NetApp SnapMirror
prtg.standardlookups.netapp.nichealth.ovl	NetApp NIC
prtg.standardlookups.netapp.nodestorageconfiguration.ovl	NetApp System Health
prtg.standardlookups.netapp.notavailable.ovl	N/A
prtg.standardlookups.netapp.relationshipstate.ovl	NetApp SnapMirror
prtg.standardlookups.netapp.relationshipstatus.ovl	NetApp SnapMirror

Standard Lookup	Used by
prtg.standardlookups.netapp.sparestate.ovl	N/A
prtg.standardlookups.netapp.takeoverstatus.ovl	SNMP NetApp System Health
prtg.standardlookups.netapp.tempstate.ovl	NetApp System Health
prtg.standardlookups.nutanix-mib.clusterstaus.ovl	SNMP Nutanix Cluster Health
prtg.standardlookups.offon.stateless.ovl	N/A
prtg.standardlookups.offon.stateonok.ovl	SNMP IBM System X Physical Memory
prtg.standardlookups.oracle.tablespace.onlinestatus.ovl	Oracle Tablespace
prtg.standardlookups.oracle.tablespace.status.ovl	Oracle Tablespace
prtg.standardlookups.paessler.aws.lookup_alarm_status.ovl	AWS Alarm v2
prtg.standardlookups.paessler.aws.lookup_status_check.ovl	AWS EC2 v2
prtg.standardlookups.paessler.aws.lookup_volume_status.ovl	AWS EBS v2
prtg.standardlookups.paessler.cisco.operational_status	Cisco WLC Access Point Overview
prtg.standardlookups.paessler.ciscomeraki.lookup_license_model.ovl	Cisco Meraki License
prtg.standardlookups.paessler.dellemc.lookup_health_status.ovl	Dell EMC Unity Enclosure Health v2 Dell EMC Unity Storage LUN v2 Dell EMC Unity Storage Pool v2
prtg.standardlookups.paessler.dns.lookup_records_found.ovl	DNS v2
prtg.standardlookups.paessler.exe.status.ovl	Script v2
prtg.standardlookups.paessler.fortigate.lookup_conserve_mode.ovl	FortiGate System Statistics

Standard Lookup	Used by
prtg.standardlookups.paessler.hpe3par.lookup_state.ovl	HPE 3PAR Common Provisioning Group HPE 3PAR Drive Enclosure HPE 3PAR Virtual Volume
prtg.standardlookups.paessler.http.status_code.ovl	HTTP v2
prtg.standardlookups.paessler.icmp.reachability_state.ovl	Ping v2
prtg.standardlookups.paessler.icmp.reachability_state_reversed.ovl	Ping v2
prtg.standardlookups.paessler.microsoft365.overall_component_state.ovl	Microsoft 365 Service Status Advanced
prtg.standardlookups.paessler.microsoft365.service_component_state.ovl	Microsoft 365 Service Status Advanced
prtg.standardlookups.paessler.microsoftazure.virtual_machine_status.ovl	Microsoft Azure Virtual Machine
prtg.standardlookups.paessler.modbus.lookup_boolean.ovl	Modbus RTU Custom Modbus TCP Custom
prtg.standardlookups.paessler.mqtt.rttstate.ovl	MQTT Round Trip
prtg.standardlookups.paessler.netapp.aggregate_state.ovl	NetApp Aggregate v2
prtg.standardlookups.paessler.netapp.autogrow_state.ovl	NetApp Volume v2
prtg.standardlookups.paessler.netapp.container_state.ovl	NetApp LUN v2
prtg.standardlookups.paessler.netapp.container_type.ovl	NetApp Physical Disk v2
prtg.standardlookups.paessler.netapp.healthy.ovl	NetApp SnapMirror v2
prtg.standardlookups.paessler.netapp.is_home.ovl	NetApp LIF v2
prtg.standardlookups.paessler.netapp.lif_state.ovl	NetApp LIF v2
prtg.standardlookups.paessler.netapp.lun_state.ovl	NetApp LUN v2

Standard Lookup	Used by
prtg.standardlookups.paessler.netapp.mirror_state.ovl	NetApp SnapMirror v2
prtg.standardlookups.paessler.netapp.nic_state.ovl	NetApp NIC v2
prtg.standardlookups.paessler.netapp.node_health.ovl	NetApp System Health v2
prtg.standardlookups.paessler.netapp.nvram_battery.ovl	NetApp System Health v2
prtg.standardlookups.paessler.netapp.policy_type.ovl	NetApp SnapMirror v2
prtg.standardlookups.paessler.netapp.storage_configuration_path.ovl	NetApp System Health v2
prtg.standardlookups.paessler.netapp.temperature_state.ovl	NetApp System Health v2
prtg.standardlookups.paessler.netapp.transfer_status.ovl	NetApp SnapMirror v2
prtg.standardlookups.paessler.opcua.negative_boolean_lookup.ovl	OPC UA Custom
prtg.standardlookups.paessler.opcua.positive_boolean_lookup.ovl	OPC UA Custom
prtg.standardlookups.paessler.opcua.raid_controller_state	Beckhoff IPC System Health
prtg.standardlookups.paessler.opcua.self_signed_certificate.ovl	OPC UA Certificate
prtg.standardlookups.paessler.opcua.server_state.ovl	OPC UA Server Status
prtg.standardlookups.paessler.orchestra.lookup_adapter_state.ovl	Soffico Orchestra Channel Health
prtg.standardlookups.paessler.paecloud.cloud_status.ovl	Cloud HTTP v2 Cloud Ping v2
prtg.standardlookups.paessler.paecloud.status_code.ovl	Cloud HTTP v2 Cloud Ping v2
prtg.standardlookups.paessler.redfish.lookup_health.ovl	Redfish Power Supply Redfish System Health

Standard Lookup	Used by
prtg.standardlookups.paessler.redfish.lookup_powerstate.ovl	Redfish System Health
prtg.standardlookups.paessler.rest.status_code.ovl	REST Custom v2
prtg.standardlookups.paessler.rest.string_as_state.ovl	REST Custom v2
prtg.standardlookups.paessler.veeam.lookup_last_result.ovl	Veeam Backup Job Status Advanced
prtg.standardlookups.paessler.veeam.lookup_status.ovl	Veeam Backup Job Status Advanced
prtg.standardlookups.paessler.veeam.yesno_no_is_error.ovl	Veeam Backup Job Status Advanced
prtg.standardlookups.paessler.veeam.yesno_no_is_ok.ovl	Veeam Backup Job Status Advanced
prtg.standardlookups.paessler.zoom.lookup_service_states.ovl	Zoom Service Status
prtg.standardlookups.QNAP.HDStatus.ovl	SNMP QNAP Physical Disk
prtg.standardlookups.QNAP.SMARTStatus.ovl	SNMP QNAP Physical Disk
prtg.standardlookups.QNAP.VolStatus.ovl	SNMP QNAP Logical Disk
prtg.standardlookups.radius.status.ovl	RADIUS v2
prtg.standardlookups.rfc.hardwarestatus.ovl	SNMP Dell Hardware SNMP Hardware Status
prtg.standardlookups.rittal.cmc3.devicestatus.ovl	SNMP Rittal CMC III Hardware Status
prtg.standardlookups.rittal.cmc3.overallstatus.ovl	SNMP Rittal CMC III Hardware Status
prtg.standardlookups.sigfox.device.state.ovl	Device template for Sigfox
prtg.standardlookups.sigfox.device.token.state.ovl	Device template for Sigfox
prtg.standardlookups.sigfox.keepalive.ovl	REST Custom template for Sigfox



Standard Lookup	Used by
prtg.standardlookups.sip.statuscode.ovl	SIP Options Ping
prtg.standardlookups.snmpprinter.cartridgelevel.ovl	SNMP Printer
prtg.standardlookups.snmpprinter.coverstate.ovl	SNMP Printer
prtg.standardlookups.sshsan.health.ovl	SSH SAN Enclosure SSH SAN Logical Disk SSH SAN Physical Disk
prtg.standardlookups.sshsan.status.ovl	SSH SAN System Health
prtg.standardlookups.sslcertificatesensor.cncheck.ovl	SSL Certificate
prtg.standardlookups.sslcertificatesensor.publickey.ovl	SSL Certificate
prtg.standardlookups.sslcertificatesensor.publickeyecc.ovl	SSL Certificate
prtg.standardlookups.sslcertificatesensor.revoked.ovl	SSL Certificate
prtg.standardlookups.sslcertificatesensor.selfsigned.ovl	SSL Certificate
prtg.standardlookups.sslcertificatesensor.trustedroot.ovl	SSL Certificate
prtg.standardlookups.sslsensor.acceptokdeniednone.ovl	N/A
prtg.standardlookups.sslsensor.acceptwarndeniedok.ovl	N/A
prtg.standardlookups.sslsensor.security.ovl	SSL Security Check
prtg.standardlookups.sslsensor.security.compatibility.ovl	N/A
prtg.standardlookups.sslsensor.ssl.ovl	SSL Security Check
prtg.standardlookups.sslsensor.tls.ovl	SSL Security Check
prtg.standardlookups.Synology.DiskStatus.ovl	SNMP Synology Physical Disk
prtg.standardlookups.Synology.RaidStatus.ovl	SNMP Synology Logical Disk

Standard Lookup	Used by
prtg.standardlookups.Synology.Status.ovl	SNMP Synology System Health
prtg.standardlookups.ups-mib.upsbattery.upsbatterystatus.ovl	Device template for Liebert UPS Device template for generic UPS
prtg.standardlookups.ups-mib.upsoutput.upsoutputsource.ovl	Device template for generic UPS
prtg.standardlookups.ups-mib.upstest.upstestresultssummary.ovl	Device template for generic UPS
prtg.standardlookups.wmi.antivir.ovl	WMI Security Center
prtg.standardlookups.wmi.battery.ovl	WMI Battery
prtg.standardlookups.wmi.battery.ups.ovl	N/A
prtg.standardlookups.wmi.diskhealth.health.ovl	WMI Disk Health
prtg.standardlookups.wmi.diskhealth.operationalstatus.ovl	WMI Disk Health
prtg.standardlookups.wmi.service.staterunningok.ovl	Windows IIS Application
prtg.standardlookups.wmi.storagepool.health.ovl	WMI Storage Pool
prtg.standardlookups.wmi.storagepool.operationalstatus.ovl	WMI Storage Pool
prtg.standardlookups.yesno.statenook.ovl	Active Directory Replication Errors Enterprise Virtual Array NetApp System Health SNMP Dell PowerEdge Physical Disk SNMP HPE ProLiant Physical Disk SNMP NetApp System Health
prtg.standardlookups.yesno.statenookna.ovl	SNMP Cisco UCS System Health
prtg.standardlookups.yesno.stateyesok.ovl	Enterprise Virtual Array HL7 NetApp LIF

Standard Lookup	Used by
	NetApp LUN NetApp NIC NetApp SnapMirror VMware Datastore (SOAP)

## 15.11 Supported AWS Regions and Their Codes

Here you can find a list of all supported Amazon Web Services (AWS) regions and their codes. The following sensors support these AWS regions:

- [AWS Alarm v2 sensor](#)
- [AWS EBS v2 sensor](#)
- [AWS EC2 v2 sensor](#)
- [AWS ELB v2 sensor](#)
- [AWS RDS v2 sensor](#)

Region	Code
Africa (Cape Town)	af-south-1
Asia Pacific (Hong Kong)	ap-east-1
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Osaka)	ap-northeast-3
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Canada (Central)	ca-central-1
Europe (Frankfurt)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2
Europe (Milan)	eu-south-1
Europe (Paris)	eu-west-3
Europe (Stockholm)	eu-north-1

Region	Code
Middle East (Bahrain)	me-south-1
South America (São Paulo)	sa-east-1
US East (Northern Virginia)	us-east-1
US East (Ohio)	us-east-2
US West (Northern California)	us-west-1
US West (Oregon)	us-west-2

