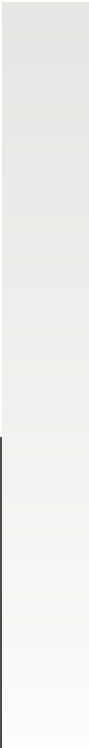
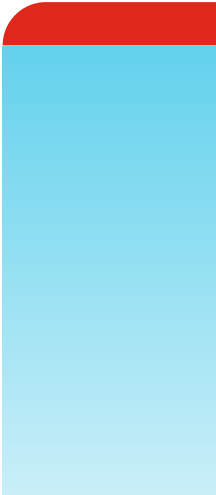


DEPLOYMENT GUIDE

Fortinet FortiGate and FireMon



Fortinet FortiGate and FireMon

- Overview 3
- Deployment Prerequisites 3
- FireMon Configuration 4
- Fortinet Configuration 7
- Summary12



Overview

The FireMon Security Manager Core Platform provides detailed, customizable IT risk analytics that allows network and security management to respond quickly to changing business demands and ensure protection, with real-time assessment of policy enforcement spanning from the specific rules and configurations of every individual device to the combined effectiveness of all defenses.

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security features without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks No. 1 in the most security appliances shipped worldwide and more than 400,000 customers trust Fortinet to protect their businesses. Learn more at <https://www.fortinet.com>, the Fortinet Blog, or FortiGuard Labs.

Deployment Prerequisites

1. Fortinet FortiGate version 4.x or newer
2. FireMon FMOS version 8.15.x or newer

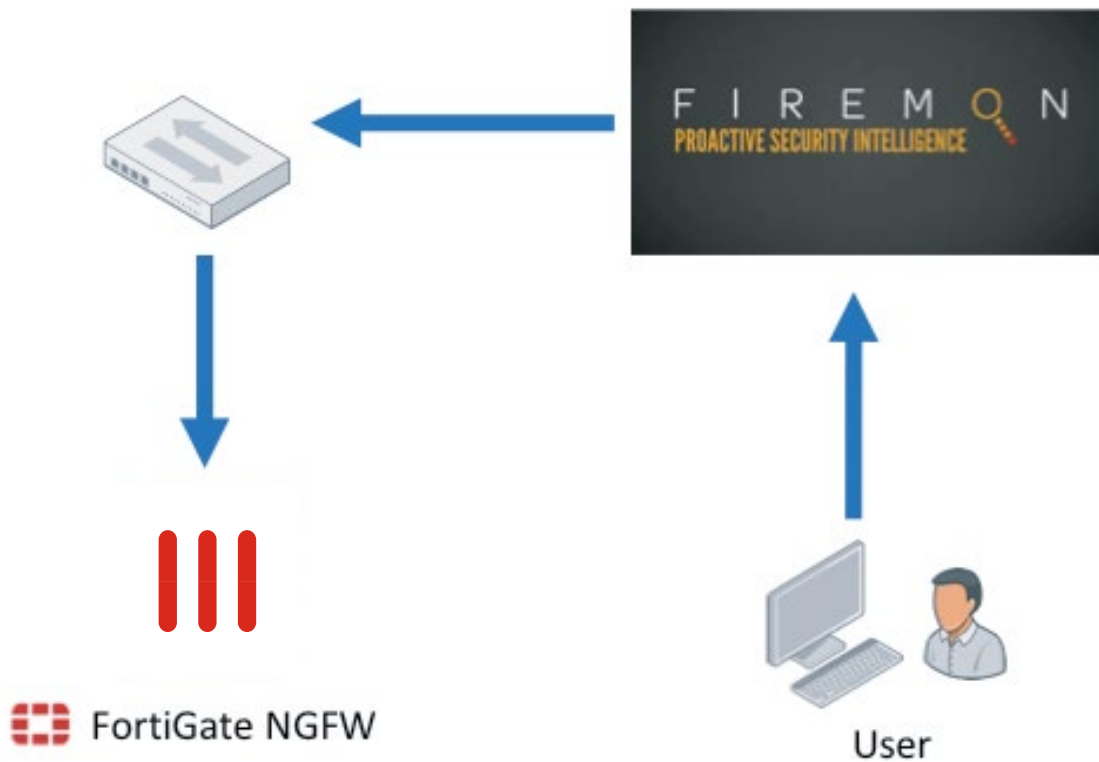
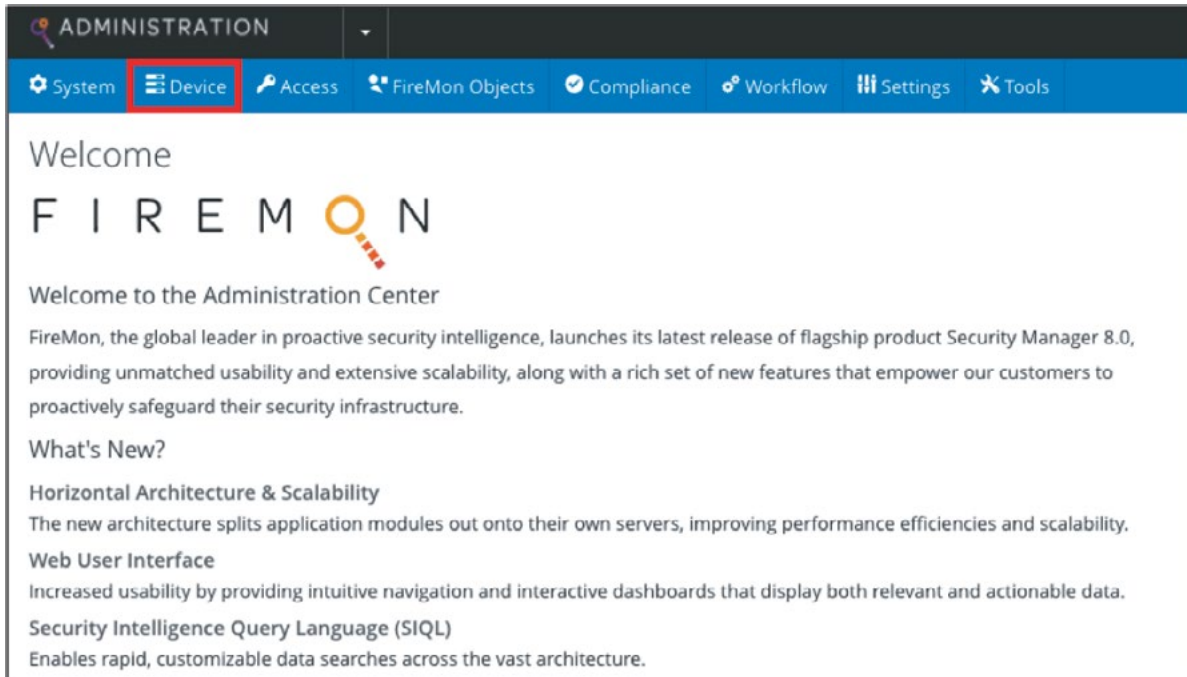


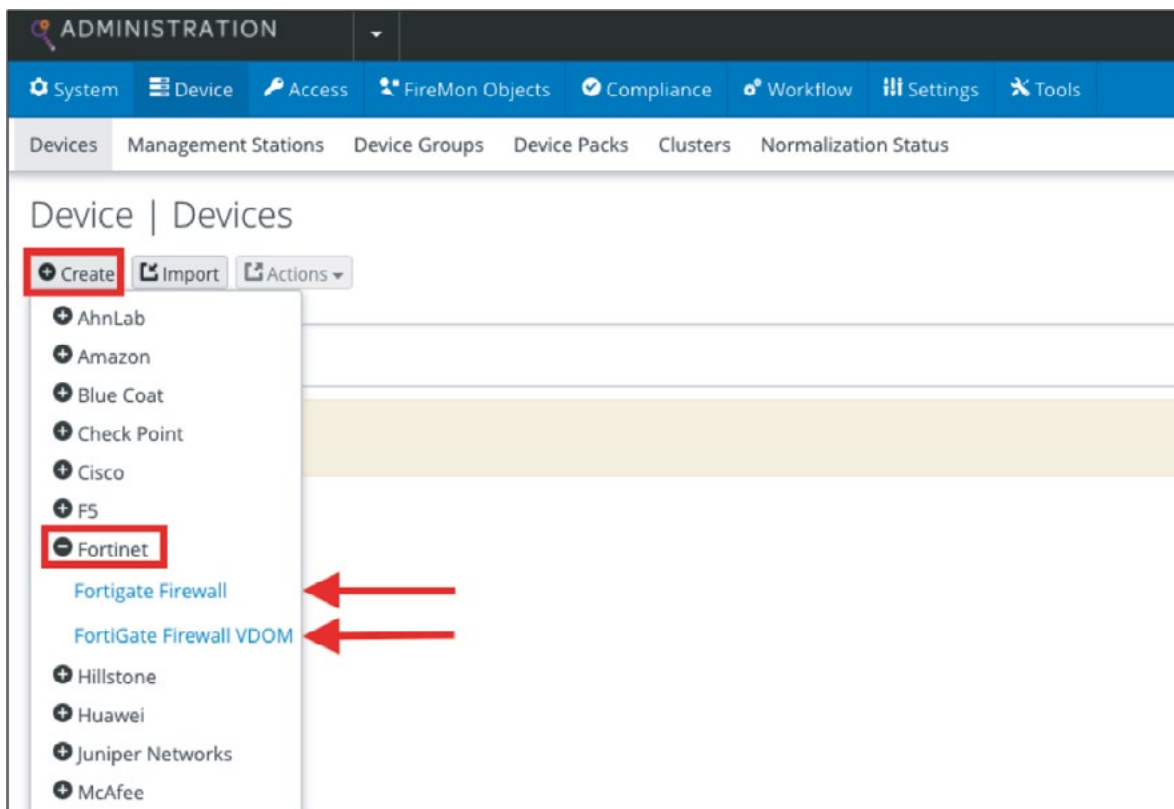
Figure 1: Architecture overview.

FireMon Configuration

1. From the Administration screen, click Device.



2. From the Devices screen, click Create > Fortinet.
3. Choose FortiGate Firewall or FortiGate Firewall VDOM if your deployment has VDOMs.
4. For VDOMs, be sure to input the correct VDOM name in the device property section.



5. Under General Properties, give the device a name and enter the IP Address.

The screenshot shows the 'Device | Devices | Create' configuration page. Under the 'General Properties' section, the 'Device Name' is 'FortiGate' and the 'Management IP Address' is '10.101.32.59'. The 'Data Collector' is set to 'firemon.fortinet.com'. Other fields are currently empty.

6. Under Device Settings, enter the password for the Admin user then re-enter the password.

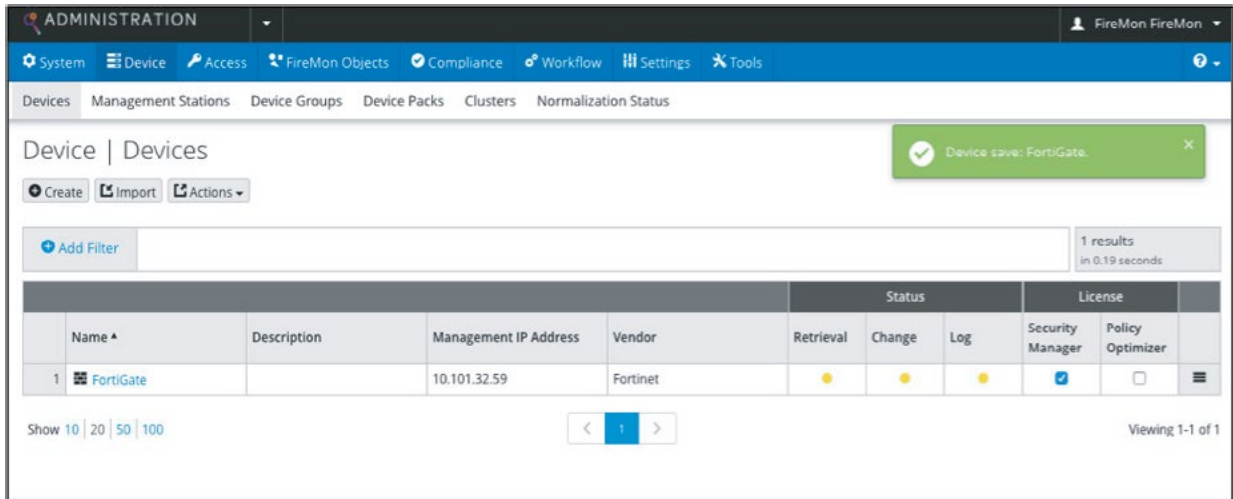
7. Click Save when done.

8. Please note: The Admin user will need to be configured with the super_admin profile on the FortiGate.

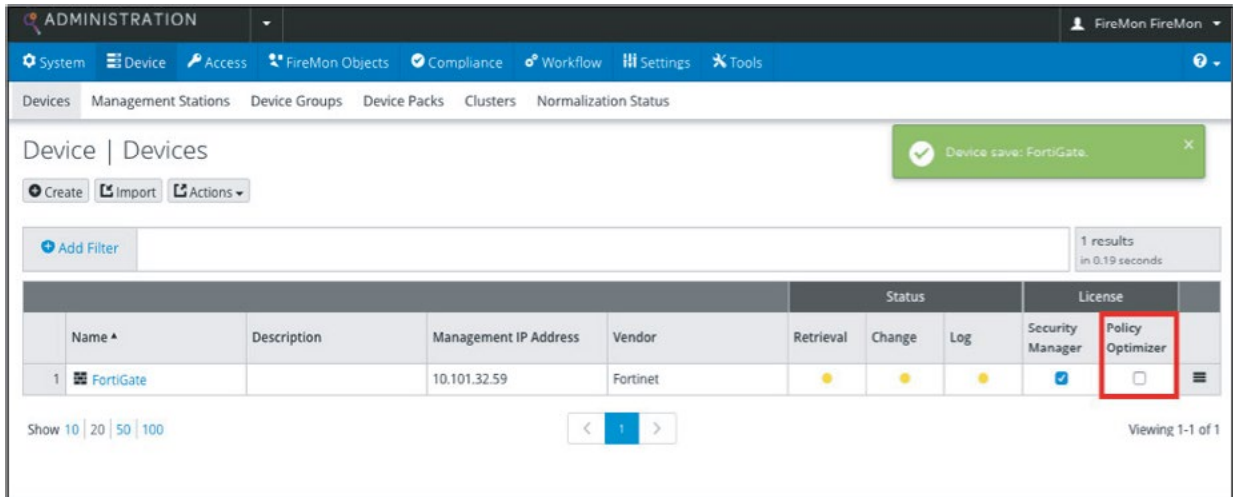
The screenshot shows the 'Device Settings' section. Under 'Credentials', the 'User Name' is 'admin'. The 'Password' and 'Re-enter Password' fields are filled with masked characters. Under 'Retrieval', the 'Protocol' is 'ssh' and the 'Port' is '22'. At the bottom, there are 'Save' and 'Cancel' buttons.



The next screen should look like this.

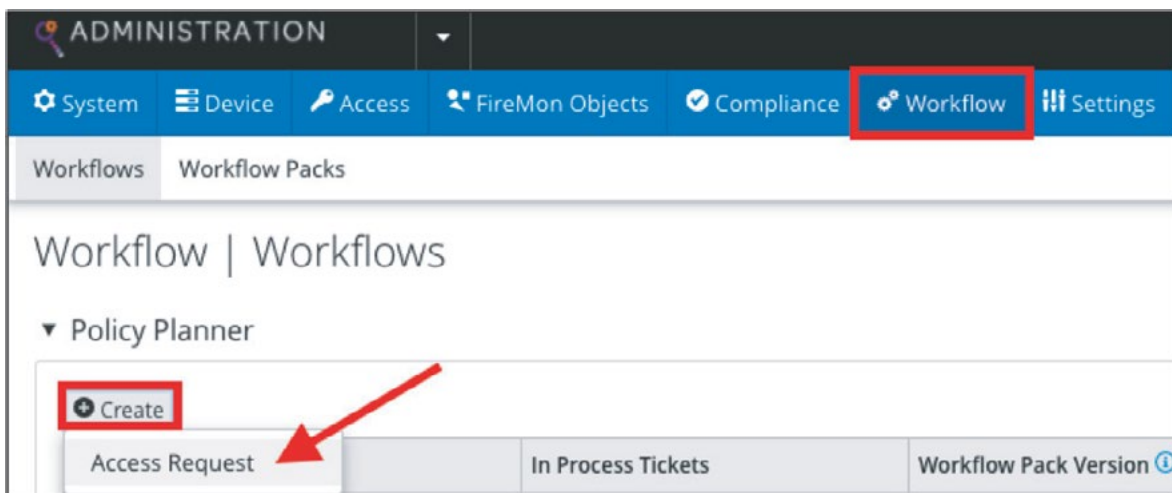


If you plan on using Policy Optimizer, make sure to check the box to enable the License.

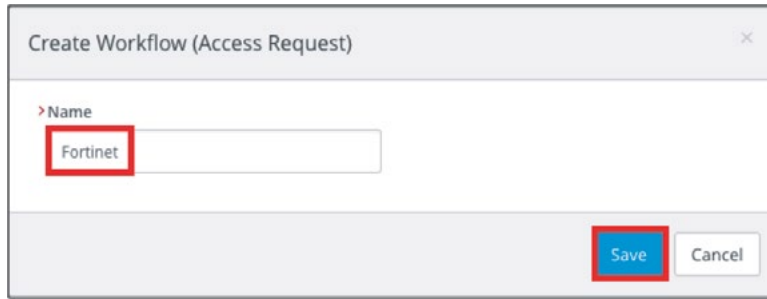


9. Then go to Workflow.

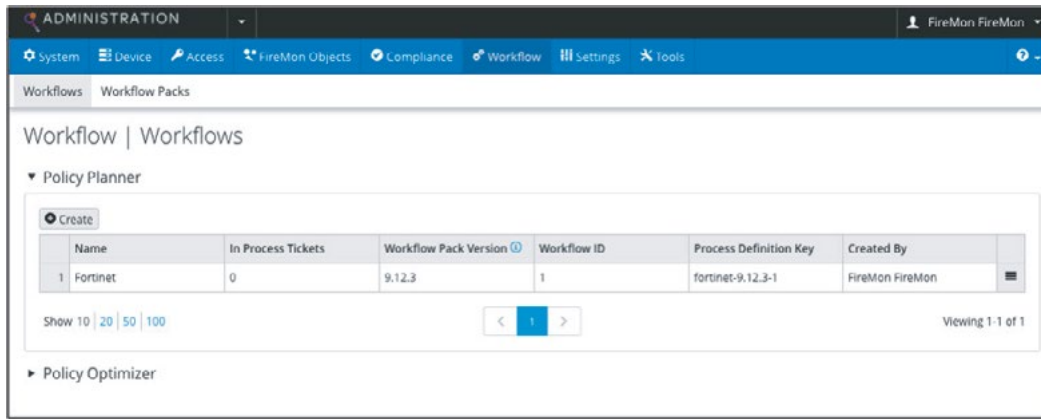
10. Under Policy Planner, click Create > Access Request.



11. Give it a Name, then click Save.

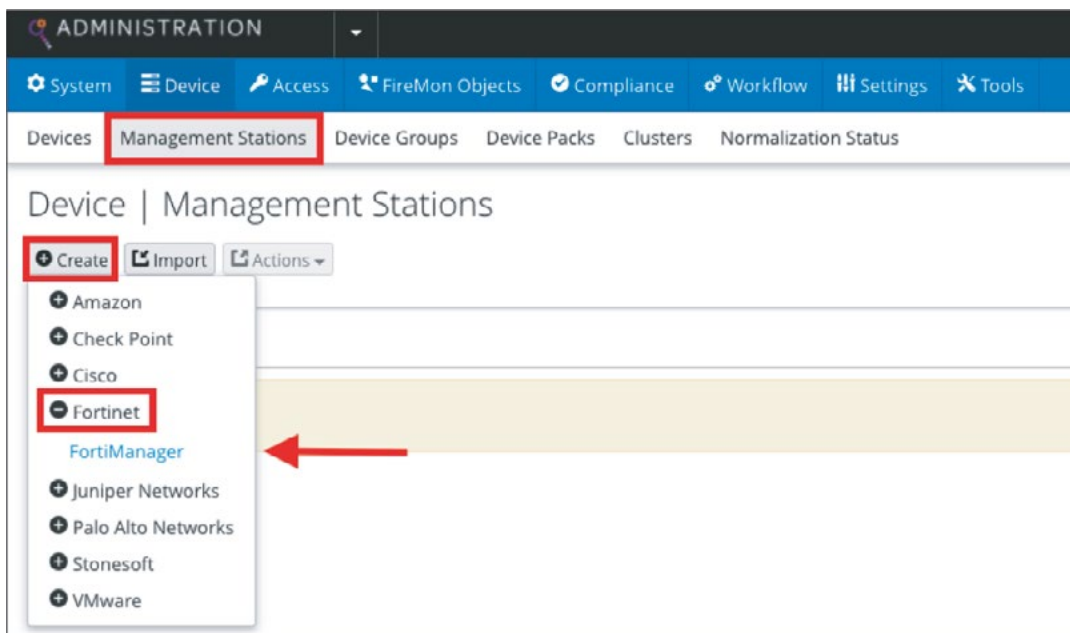


The Workflow screen should now look like the image below.



12. Do the same for the Policy Optimizer configuration.

Note: If adding FortiGate firewalls via FortiManager, do this from Devices > Management Stations. The Admin user will need access to all VDOMs enabled.



Fortinet Configuration

1. Ensure all Firewall rules are set to Log All Sessions.

Seq.#	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
lan - wan1 (1 - 1)										
1	Default-Policy	all	all	always	ALL	ACCEPT	Enabled	AV, WEB, APP, IPS, SSL	All	482.11 GB
vsw.dmz - wan1 (2 - 2)										
2	FSW	all	all	always	ALL	ACCEPT	Enabled	AV, WEB, APP, IPS, SSL	All	9.37 GB
wan1 - lan (3 - 3)										
3	RDP	all	RDP_Server	always	RDP	ACCEPT	Enabled		All	0 B
Implicit (4 - 4)										
4	Implicit Deny	all	all	always	ALL	DENY	Disabled		Disabled	229.40 MB

If not, enable this for each rule under Logging Options.

Logging Options

Log Allowed Traffic Security Events **All Sessions**

Generate Logs when Session Starts

Capture Packets

2. Configure FortiGate to send Syslog to the FireMon IP address.
3. Under Log & Report, click Log Settings.

FortiGate VM64 FGVM040000101072

- Dashboard
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WiFi & Switch Controller
- Log & Report**
 - Forward Traffic
 - Local Traffic
 - System Events
 - AntiVirus
 - Web Filter
 - Application Control
 - Security Fabric Audit
 - Security Audit Events
 - Learning Report
 - Log Settings**
 - Threat Weight

System Information

- Hostname: FGVM040000101072
- Serial Number: FGVM040000101072
- Firmware: v5.6.0 build1449 (GA)
- Mode: NAT (Proxy-based)
- System Time: 2017/07/27 09:40:35
- Uptime: 35:20:12:01
- WAN IP: 96.45.34.225 (Sunnyvale, California, United States)

Administrators

- admin super_admin
- 1 Logged in
- 3 Sessions

4. Enable Send Logs to Syslog.
5. Enter the IP Address or FQDN of the FireMon server.
6. Select the desired Log Settings.
7. Click Save.

- Security Fabric Audit
- Security Audit Events
- Learning Report
- Log Settings**
- Threat Weight
- Alert E-mail

Log Settings

Send Logs to Syslog

IP Address/FQDN

Event Logging **All** Customize

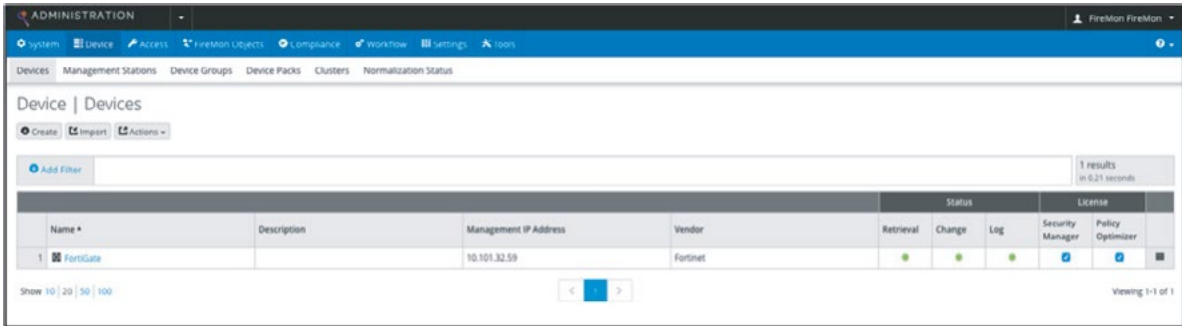
Local Traffic Log **All** Customize



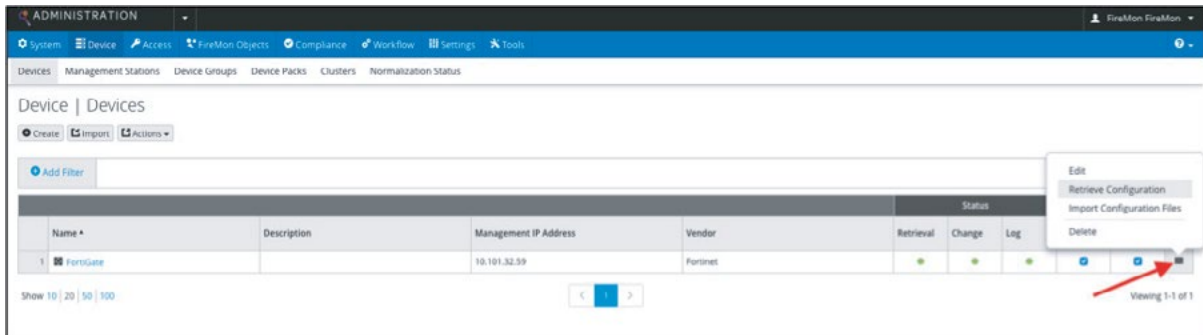
Note: If the primary Syslog is already configured, you can use the CLI to configure additional Syslog servers.

```
FortiGate-ESX2 # config log syslogd2 setting
FortiGate-ESX2 (setting) # set status enable
FortiGate-ESX2 (setting) # set server 1.2.3.4
FortiGate-ESX2 (setting) # end
FortiGate-ESX2 #
```

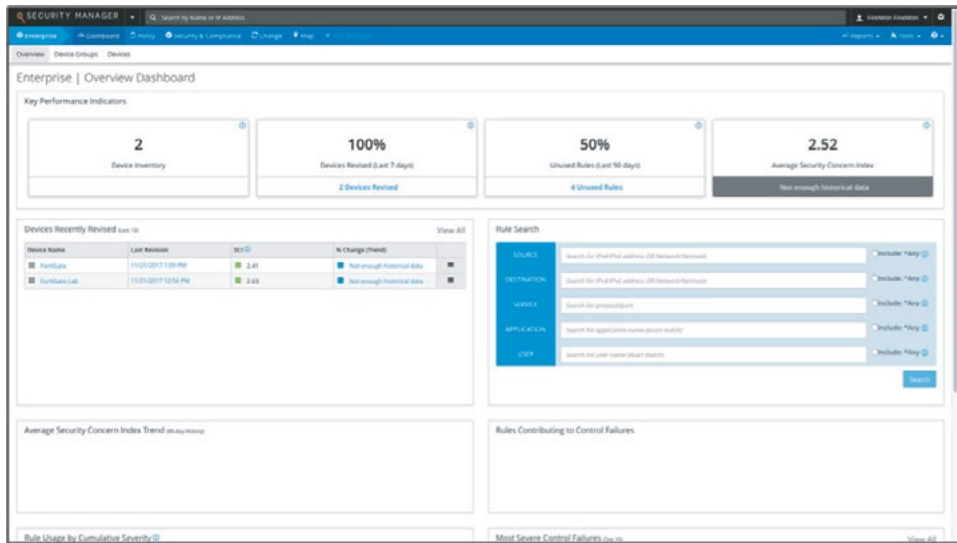
8. The configuration is now complete. Go back to the Devices screen in the FireMon interface. It should look like the image below once logs are received and the configuration has been retrieved.

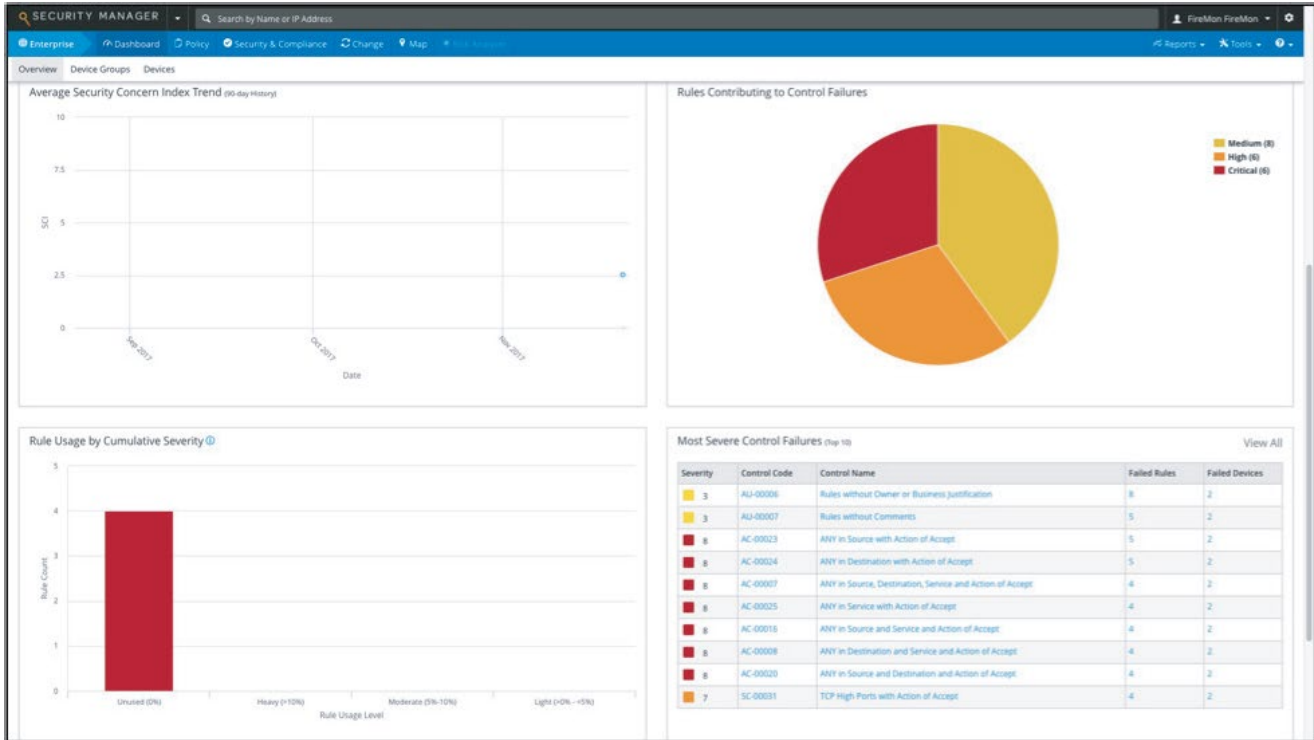


9. You can initiate a manual retrieval of the configuration by clicking the box on the far right.

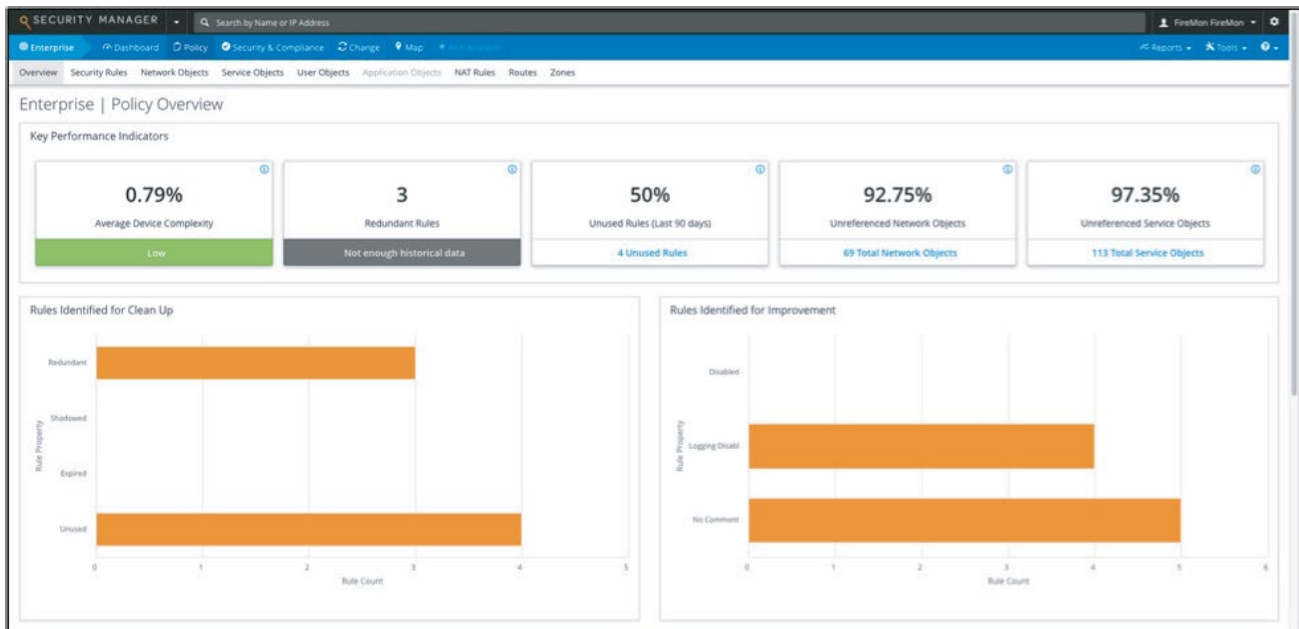


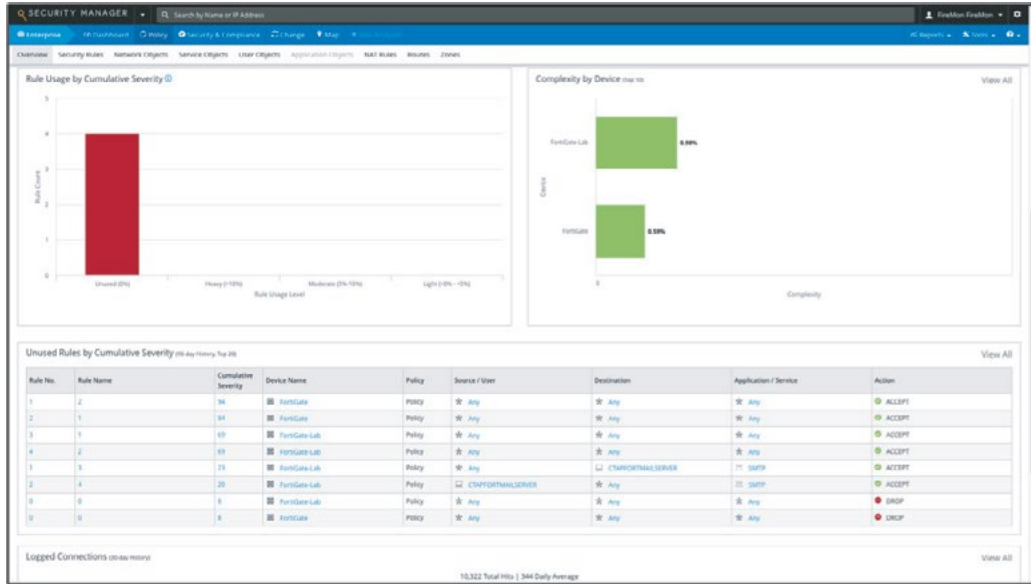
Security Manager Dashboard Views.



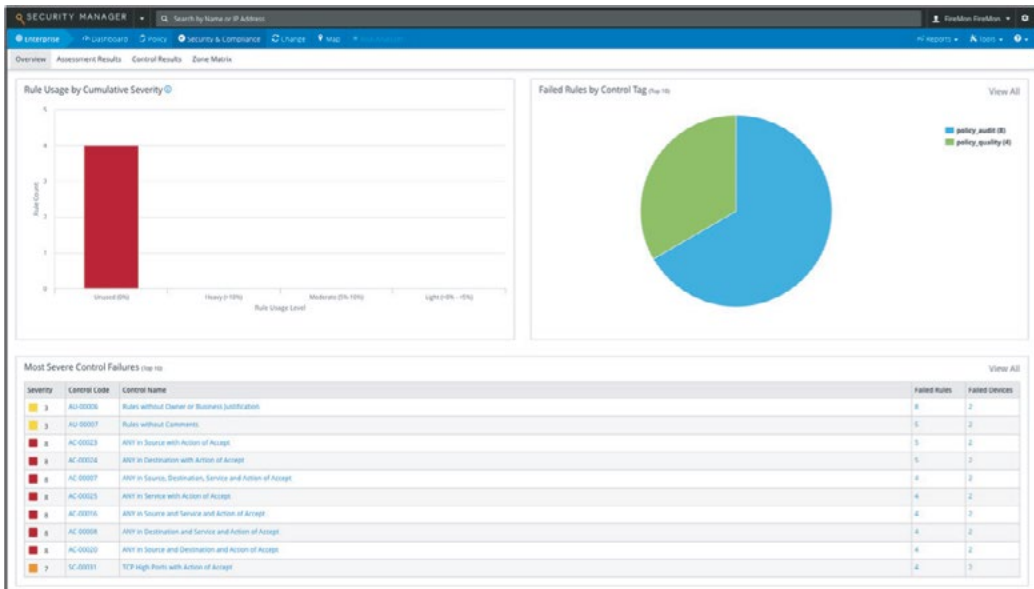
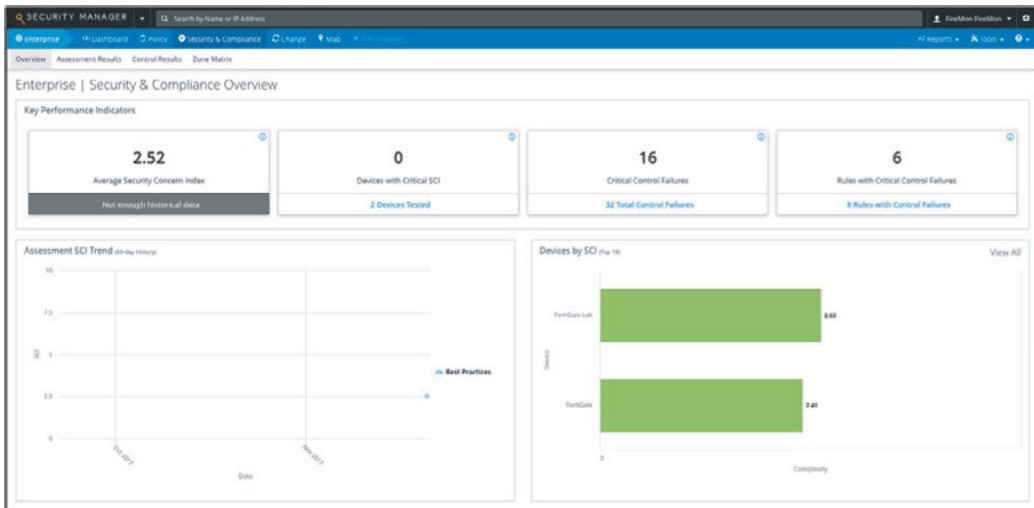


Security Manager Policy Views





Security Manager Security & Compliance Views



Security Manager Security & Change Views

Enterprise | Change Overview

Key Performance Indicators

- 9 Revisions (Last 7 days)
 7 Configuration Changes
- FortiGate
 Device Most Recently Revised
 At 11/21/2017 1:09 PM by admin@10.101.32.254
- 8 Rules with Changes
 Last 7 days

Revisions (Last 10)

Revision	Date/Time	User	No. of Changes	Device Name
15	11/21/2017 1:09 PM	admin@10.101.32.254	3	FortiGate
14	11/21/2017 1:07 PM	admin@10.101.32.254	0	FortiGate
13	11/21/2017 1:07 PM	admin@10.101.32.254	2	FortiGate
12	11/21/2017 1:06 PM	admin@10.101.32.254	2	FortiGate
11	11/21/2017 1:05 PM	admin@10.101.32.254	0	FortiGate
10	11/21/2017 12:56 PM	firemon	0	FortiGate-Lab
9	11/21/2017 12:55 PM	firemon	0	FortiGate-Lab
6	11/21/2017 10:36 AM	firemon	0	FortiGate
5	11/21/2017 10:35 AM	firemon	0	FortiGate

Devices Recently Revised (Last 10)

Device Name	Last Revision	SCI	% Change (Trend)
FortiGate	11/21/2017 1:09 PM	2.41	Not enough historical data
FortiGate-Lab	11/21/2017 12:56 PM	2.63	Not enough historical data

Changes (Last 20)

Device Name	Revision	Action	User	Date/Time	Object Type	Object	Summary
FortiGate	15	Modified	admin@10.101.32.254	11/21/2017 1:09 PM	Security Rule	2	Disabled changed from [true] to [false]. Log changed from [false]...
FortiGate	15	Modified	admin@10.101.32.254	11/21/2017 1:09 PM	Security Rule	1	Rule order changed in policy [Policy] from [1] to [2]
FortiGate	15	Modified	admin@10.101.32.254	11/21/2017 1:09 PM	Policy	Policy	Security rule(s) modified
FortiGate	13	Modified	admin@10.101.32.254	11/21/2017 1:07 PM	Security Rule	1	Disabled changed from [true] to [false]
FortiGate	13	Modified	admin@10.101.32.254	11/21/2017 1:07 PM	Policy	Policy	Security rule(s) modified
FortiGate	12	Modified	admin@10.101.32.254	11/21/2017 1:06 PM	Security Rule	1	Disabled changed from [false] to [true]
FortiGate	12	Modified	admin@10.101.32.254	11/21/2017 1:06 PM	Policy	Policy	Security rule(s) modified

Changes by User (1 Day History)

User	No. of Changes	Last Revision	Summary
admin@10.101.32.254	7	11/21/2017 1:09 PM	1 policies changed, 2 security rules changed
firemon	0	11/21/2017 12:56 PM	

Summary

FireMon helps keep Fortinet firewalls running smoothly with a complete configuration management solution, including full support for the FortiGate line of network security platforms and appliances. FireMon monitors each appliance, capturing event and traffic logs in real time. All change events trigger a full configuration capture including detailed change history and a full audit trail of operations. Fortinet devices can be monitored directly or indirectly if another event collection system is in place.

Solution Guide: <https://www.fortinet.com/content/dam/fortinet/assets/alliances/firemon-integration-brief-for-fortinet.pdf>

FortiGate 5.6 Handbook: <https://docs.fortinet.com/uploaded/files/3999/fortios-handbook-56.pdf>

