

Veriti Integration



Table of Contents

About Veriti
Deployment Prerequisite
Version Compatibility
Configuration
FortiManager Configuration
Standalone FortiGate Configuration
Standalone FortiAnalyzer Configuration
Veriti Configuration11
Integrating with FortiManager11
Integrating with Standalone FortiGate NGFW
Integrating with Standalone FortiAnalyzer
Known Limitations

About Veriti

Veriti is a fast-growing cybersecurity innovator that helps organizations maximize their security posture while ensuring business uptime. With Veriti, organizations can eliminate complexity and operational friction in managing multiple cybersecurity solutions with a consolidated, governing platform that proactively monitors and, in a single click, remediates security gaps and misconfigurations across the entire security infrastructure.

Version Compatibility

This deployment and integration guide applies to FortiManager, FortiGate, and FortiAnalyzer with FortiOS v6.4 or newer.

Deployment Prerequisite

- FortiGate
- FortiManager (Optional)
- FortiAnalyzer (Optional)
- Veriti Server with network access to Fortinet devices



Configuration

Fortinet configuration

Veriti supports the following Fortinet deployments:

- Fully managed architecture with FortiManager, FortiGate, and FortiAnalyzer
- Managed architecture with FortiManager and FortiGate and standalone FortiAnalyzer
- Managed architecture with FortiManager and FortiGates
- Standalone FortiGate and standalone FortiAnalyzer
- Standalone FortiGate

Configure a new user with the required permissions to initiate communication between Veriti and Fortinet devices, along with the remote utilization of API commands.

FortiManager Configuration:

1. Log in to FortiManager GUI.



2. Select an ADOM (if the ADOM feature is enabled).

				ADOM: root	📣 admin 👻
Select an ADOM			×		
			۹ ()		
root (1) FortiGate 7.2	adom_a (1) FortiGate 7.2	Global Database Global 7.2			
		+ Create New ADOM	Close		

3. Click on "System Settings."

					ADOM: root	- 0•	û 0 -	🔺 admin 🝷
III Device Manager	Policy & Objects	(()) AP Manager	VPN Manager	Fabric View				
Â			*					
FortiGuard	FortiSwitch Manager	Extender Manager	System Settings					

4. On the left panel, click on "Administrators."

🔝 System Settings 🗸								ADOM: root	• •	40-	A	admir
O Dashboard	Toggle Widget ~											_
All ADOMs												
Network	System Information		e	¥ :	; ≡~	License Information				e ¥	0 =	
₫ HA	Next Name	DIC VALUE AVEC-D				Bruthurt	104 Mater Free Jac	Onelland				
1 Admin v	Plost Name	PMG-YM04-AW3OnDemand			6	OPOrtiouard	VM Meter Service	W No Ocense			2	4
Administrators	Serial Number	FMGAWSTM23002209					Server Location	Servers located in US	only		6	1
Profile	Platform Type	FMG-VM64-AWSOnDemand				La! Management	Devices/VDOMs	2 / 30 (6.7%)				
Workspace	HA Status	Standalone			-		FortiGates/Logging Device	5 2				
Remote Authentication S	System Time	Thu Dec 07 03:06:13 2023 PST			ß	Update Server	AntiVirus and IPS	N/A				
Admin Settings	Firmware Version	v7.2.4-build1460 230926 (GA)			٢		Web and Email Filter	N/A				
SAML SSO	System Configuration	Last Backup : N/A		Ð	Ð		FortiClient Update	N/A				
B Certificates	Current Administrators	admin / 1 in total			E							
Event Log	Up Time	13 days 14 hours 9 minutes 45 seconds										
Task Monitor	Administrative Domain	•				' I						
Bo Advanced	Easti Analiseas Easterna	~										
	System Resources		0	¥ (; ≡~	Unit Operation				e ¥	0 =	I~
						FORTINET		FortiM	lanager-VI	464-AWS	OnDem	ind
	4%	17%	6%			ò			12			
	Average CPU U	sage Memory Usage	Disk Usage									
	More Detail	8										
							Destant	0				
						×	POESCAPE	0	Shutdowr			
	Alert Message Console			* :	; ≡~		Restart	U	Shutdown			

5. Click "Create New" at the top toolbar and choose "Administrator."

🕄 System Settings 🕶								ADOM: root	- 0-	4 0 -	🔥 admin	
C Darbbord A AdOMs A HuA A HA A HA A HA A HA A HA A HA A H	Craste New V Administrator EST APA Admin STA APA Admin Administrator	(2) (dd) (% Cours)	Data Water	I Table View> Profile 3 Super_Uter	JJON API Access 9	ADDMs 5 All ADDMs	Pulcy Packages 9 All Packages	Device Group #	Trusted	Search IPv4 Hosts [©]		
FUETOFT												

- 6. Fill the following details in the "Create New Administrator" menu:
 - a. Username
 - b. Admin Type (make sure it is "LOCAL")
 - c. New Password
 - d. Confirm Password
 - e. Administrative Domain (make sure it is "All ADOMs" if the ADOM feature is enabled)
 - f. Admin Profile create a new profile by clicking on "+" with the following data:
 - i. Profile Name
 - ii. Type (make sure it is "System Admin")
 - iii. Read-Write permissions:
 - 1. System Settings
 - 2. Device Manager (and its sub permissions)
 - 3. Policy & Objects (and its sub permissions) required only if remediations will be taken from Veriti
 - 4. Install Policy Package or Device Configuration required only if remediations will be taken from Veriti
 - iv. Read-Only permissions (all other permissions)

System Settings -					ADOM	root >_ @•	A 🛛 🔹 🔺	adm
Dashboard	+ Create New* Di Edit Se Clone	1 Delete Move		Edit Profile				
All ADOMs	Name 0		JSON API					
Network	Sustem Administrator			Profile Name	Veriti Profile			_
I. HA				Description	1			
Admin	Ag admin		None					
Administrators								
Profile				Туре	System Admin	Restricted Admin		
Workspace					Read-Write	Read-Only	None	
Remote Authentication S				System Settings	۲	0	0	
Admin Settings				Administrative Domain	0	۲	0	
SAML SSO				FortiGuard Center	0	۲	0	
Certificates	,			License Management	0	۲	0	
Event Log				Firmware Management	0	۲	0	
Task Monitor				Settings	0	۲	0	
 Advanced 	·			Device Manager	۲	0	0	
			1	Add/Delete/Edit Devices/Groups	۲	0	0	
				Retrieve Configuration from Devices	۲	0	0	
				Revert Configuration from Revision History	۲	0	0	
				Delete Device Revision	۲	0	0	
				Terminal Access	۲	0	0	
				Manage Device Configurations	۲	0	0	
				Provisioning Templates	۲	0	0	
				SD-WAN	۲	0	0	
				Script Access	۲	0	0	
				Policy & Objects	۲	0	0	
				Global Policy Packages & Objects	۲	0	0	
				Assignment	۲	0	0	
				Policy Package & Objects	۲	0	0	
				Policy Check	۲	0	0	
				Edit Installation Tunner		0	0	
FURTIDET				0	< Cancel			

g. JSON API Access (make sure it is "Read-Write").

🕄 System Settings 🕶								0- A0	• 🔥 admin 👻
O Dashboard	+ Create New * Edit Clone	Delete Move	Table View ~		Create New Administrator				×
All ADOMs	Name 0	Type 0	Profile ©	JSON API					
Network	System Administrator				User Name	Veriti			
L Admin Y	An admin	LOCAL	Super_User	None	Avatar	V + Add Photo - Remove Photo			
Administrators				1000	Description				
Profile									
Workspace									
Remote Authentication S					Admin Type	LOCAL			•
Admin Settings					New Password				0 0 0
SAMLSSO					Confirm Password				0 0 0
E Event Log					Forts loken Cloud	Disable FortiToken Mobile Email SMS			
Task Monitor					Administrative Domain	All ADOMs All ADOMs except specified or	nes Specify		-
B Advanced					Policy Package	Verio Pronie			•
					ISON API Access	Part-Write			-
					Theme Mode	Ike Global Theme Like Own Theme			
					Trusted Hosts				
						-			
					Meta Fields >				
					Advanced Options >				
FURTIDET						ОК Са	ncel		

7. Click "OK."

8. Verify the new user is presented in the "System Administrators" table.

🕄 System Settings 🗸									🗕 🔞 • 🛛 🗘 🗿 • 🕜 admin •
② Dashboard	+	Create New 🐃 🖾 Edit 🛸 Clone	1 Delete	Table View ~					Search
All ADOMs		Name 0	Type 0	Profile ©	JSON API Access ©	ADOMs 0	Policy Packages ©	Device Group ©	Trusted IPv4 Hosts 0
Network	•	System Administrator							
Admin ·	- 0	Ag admin	LOCAL	Super_User	None	All ADOMs	All Packages		0.0.0.0/0.0.0.0
Administrators Profile	0	V Veriti	LOCAL	Veriti Profile	Read & Write	All ADOMs	All Packages		0.0.0.0/0.0.0.0
Workspace Remote Authentication S Admin Settings									
SAMLSSO	>								
lo Advanced	>								
ELIBTIOET									

Standalone FortiGate Configuration:

1. Log in to FortiGate GUI.

Username
Password
Login

2. On the left panel, click "System" and choose "Administrators."

ark i					
	System Information	Licenses (173.243.141.6) 0	Virtual Machine I •	FortiGate Cloud	Security Fabric
	Hostname FGTAWS80TTM05SC9	FortiCare Support	FGTAWS License	Status A Not Activated	彭 🖲 🖪 🗎 🗙 (0
	Serial Number FGTAWS80TTM055C9 2	Firmware & General Updates	Allocated vCPUs 1		[T]
	Ermware v7.0.13 build0566 (Mature)		Allocated RAM 2 GB		
	Mode NAT	0 105			8
• ·		 AntiVirus 	Auto Scaling O Disabled		B FGTAWS80TTM05SC9
	System Time 2023/12/0704:14:17	Web Filtering			•
	Uptime 13:14:53:26	FortiToken 0/2			
	WAN IP 13253.87.128	0%			A Security Fabric Connection
	Administrators I-	CPU	1 minute • I •	Memory	1 min
	1 HTTPS 0 FortiExplorer	100%		100%	
	admin super_admin	75%		75%	
		134		104	
		50%		50%	
		254		200	
		2.77			
		0% 04:13:20 04:13:30 04:13:40	04:13:50 04:14:00 04:14:10	0% 04:13:20 04:13:30 04:13:40	04:13:50 04:14:00 0
Report :		Current	0%	Correction	20%
		Corrence	ender 076	Corrento	
	Sessions	1 minute • I •			
	250				
	200				
	150				
	100				

3. Click "Create New" at the top toolbar and choose "REST API Admin."

FAZVM64-AWSOnDemand	=						>_ 0•	4 0 • A admin •
Dashboard	+ Create New ~	🖾 Edit 🛸 Clone 🛙	Delete	Table View ~				Search
Device Manager	Administrator	1	Type 0	Profile 0	JSON API Access ©	ADOMs 0	Trusted IPv4 Hosts ©	•
FortiView >	REST API Admin	itor						
E Log View			LOCAL	Super_User	None	All ADOMs	0.0.0.0/0.0.0.0	
Incidents & Events	-							
Reports >								
 System Settings 								
ADOMs								
Administrators								
Admin Profiles								
Remote Authentication S								
Fabric Management								
Settings								
на								
Network								
Event Lors								
Certificates								
Advanced								
FRATIOET								

- 4. Fill in the following details on the "New REST API Admin" page:
 - a. Username
 - b. Administrator Profile create a new profile by clicking on "+ Create" with the following data:
 - i. Name
 - ii. Read/Write permissions:
 - 1. Log & Report
 - 2. System
 - 3. Security Profiles are required only if remediations are taken from Veriti; otherwise, they should be "Read"
 - iii. Read permissions:
 - 1. User & Device
 - 2. Firewall
 - 3. Network
 - iv. None Permissions (all other permissions)

FGTAWS80TTM05SC9 •	≡ Q.									16	≗ • >_	0· 0	- 🙂	admin •
Dashboard	New REST API Admin			New Admin Profile	e									×
Policy & Objects	Username			Name Ve	eriti Profile									
Security Profiles	Comments			Comments			0/255							
□ VPN >	Administrator profile		*											
🚨 User & Authentication 🔷	PKI Group			Access Permissio	ins									
♥ WIFI Controller >		admin_no_access		Access Contro	ol	Permi	ssions Set All *							
🗘 System 🗸 🗸														
Administrators 🛱	CORS Allow Origin			Security Fabric	0	None @ Read	Kead/Write							
Admin Profiles				FortiView	0	None @ Read								
Firmware	Restrict login to trusted	hosts												
Fabric Management	Trusted Hosts			User & Device	0	None @ Read	 Read/Write 							
Settings				Firewall	0	None @ Read		O Custom						
на														
SNMP				Log & Report	0	None @ Read	Read/Write	O Custom						
Replacement Messages				Network	0	None @ Read		O Custom						
FortiGuard														
Feature Visibility				System	0	None @ Read	Read/Write	O Custom						
Certificates				Security Profile	0	None @ Read		O Custom						
☆ Security Fabric >														
네 Log & Report 🔹 🔸				VPN	0	None @ Read	Read/Write							
				WAN Opt & Car	che Ø	None Read								
				WiFi & Switch	0	None @ Read	Read/Write							
				Permit usage of C	CLI diagnos	itic commands	D							
				Override Idle	Timeout									
								014	Grand					
								UK	Cancel					

- 5. Click "OK."
- 6. Copy the generated "API Key" and store it for later use.

FGTAWS80TTM05SC9	≣ ۹,			👷 - >_ 🛛 - 유 - 🙎 admin -
Dashboard	New REST API Admin		New API key	×
Network				
Policy & Objects	Username		New API key for Veriti kdzN5dwd1b7g8fQw574kw0bNjf4rqr 😢	
A Security Profiles	Comments			
II VPN	Administrator profile	Veriti Profile 👻	This is the only place this key will be provided. Keep this information or secure. The bearer of this API key will be granted all access privileges	
LUser & Authentication	API key	M Regenerate	assigned to this account.	
♥ WiFi Controller	PKI Group			
🗘 System	CORS Allow Origin (2)			
Administrators 1	Restrict login to trusted		Close	
Admin Profiles	Tourisd Harts (7)			
Firmware	Indiated Plosts Car			
Fabric Management				
Settings				
HA				
SNMP				
Replacement Messages				
FortiGuard				
Feature Visibility				
Certificates				
⊗ Security Fabric >				
Let Log & Report				

Standalone FortiAnalyzer Configuration:

1. Log in to FortiAnalyzer GUI.

FortiAnalyzer-VM64-AWSOnDemand	

2. Click "System Settings" on the left panel and choose "Administrators."

FAZVM64-AWSOnDemand	=											0+ A 🛛 + 🔥
Dashboard	Toggle Widget ~											
Device Manager												
	System Information	on @¥C	≣~	License Informatio	n Ø	* 0	≣~	System Resources	8	: :: ≡~	Unit Operation	Ø ¥ C ≡
	Host Name	FAZVM64-	ß	FortiGuard			1.1					FortiAnalyzer-VM64-
		AWSOnDemand	_	Indicators of Com	C Licensed (Exp	vires 2095	-12-				FORTINET	AWSOnDemand
Incidents & Events	Serial Number	FAZAWSTA23002262	- 1		31)							
Reports >	Platform Type	FAZVM64-AWSOnDeman	nd	Outbreak Detectio.	A Not Licensed		- 11					5 6 7 8 mm mm mm
System Settings 🗸 👻	HA Status	Standalone		Security Automatio	Not Licensed		7	25%	51%	7%		teal heat heat heat
	System Time	Thu Dec 07 04:46:58	ß	Industrial Security	C Licensed (Exp	pires 2038	3-01-			10 A 1	m m	
Administrators		2023 PST			03)			Average CPU Usage Me	mory Usage	Disk Usage	1.4 1.4	and and
	Firmware Version	v7.2.1-build2308 230831	٢	Security Rating Up.	A Not Licensed		π	More Details				
Remote Authentication S		(GA)		Server Location	Servers locat	ed in US	ß					
	System Configuration	Last Backup: N/A	÷Ð		only						🌣 Restart	③ Shutdown
							-				1	
	Log Receive Moni	tor			8	* 0	=~	Alert Message Conso	ble LLI & A	k C ≡*		
на	1	Av	erage Ral	te (0 Logs/Sec)				Time 0	Message 0	•		
Network	Law							Dec 7, 03:56:57	'admin' login fa	iled from		
	1							Dec 7, 03:38:01	'gitlab-runner'	login faile		
event Logs								Dec 7. 03:21:25	'arrow' login fa	iled from		
Leroncates								Dec 7.02-02-48	Sagrant' Ingin	failed fro		
								Dec 7.01:47:00	'munt' lonio fa	led from		
								Dec 7, 01, 22,02	issent toget to	falled fo		
	0			in the time of	in the si			Dec 7,01.02.00	loople to all a feat	ind former		
	00.50	0.55 04.00 04.05 0	7440741	0.15 0420 0425 0	130 04:30 040			Dec 7, 01:17:04	Caziz login fai	ed from s		
			-2/1101/10	Soverse						0/6 10		
	Disk I/O				0	x /1	=~	Insert Pate us Receiv	e Rate			a x n =
					~			instant to receiv				
	1.00%							30			\$	lustained Log Rate(30)
	0.80%							25				
FURTIDET								20				

3. Click "Create New" at the top left toolbar and choose "Administrator."

E FAZVM64-AWSOnDemand	=						>_ 0+	
Dashboard	+ Create New ~	🖾 Edit 🖄 Clone 🗄	Delete	Table View				Search
Device Manager	Administrator		Type ©	Profile 0	JSON API Access 0	ADOMS 0	Trusted IPv4 Hosts 0	•
D Log View	REST API Admin	itor						
Fabric View	🗆 🖉 admin		LOCAL	Super_User	None	All ADOMs	0.0.0.0/0.0.0.0	
🚦 Incidents & Events 💦 🔸								
Reports >								
System Settings								
ADOMS								
Administrators Admin Profiles								
Remote Authentication S								
Fabric Management								
SAML SSO								
Settings								
НА								
Network								
Event Logs								
Advanced								
FERTIDET								

- 4. Fill the following details in the "Create New Administrator" menu:
 - a. Username
 - b. Admin Type (make sure it is "LOCAL")
 - c. New Password
 - d. Confirm Password
 - e. Administrative Domain (make sure it is "All ADOMs" if the ADOM feature is enabled)
 - f. Admin Profile create a new profile by clicking on "+" with the following:
 - i. Profile Name
 - ii. Read-Write permissions:
 - 1. System Settings
 - iii. Read-Only permissions:
 - 1. Administrative Domain
 - 2. Device Manager (and its sub permissions)
 - 3. LogView/FortiView
 - iv. None Permissions (all other permission)



5. Click "OK."

FAZVM64-AWSOnDemand	=						>_ @• /	4 0 •	A admin •
Dashboard	+0	Create New Y	1 Delete	Table View ~	Create New Administrator				×
Device Manager		Name 0	Type 0	Profile 0					
FortiView		ustern Administrator			User Name	Veriti			
Log View			_		Avatar	V + Add Photo - Remove Photo			
Fabric View		Age admin	LOCAL	Super_User	Description				
Incidents & Events									
Reports >									
System Settings ·					Admin Tune	1054			
ADOMS					New Passaged				0.0.0
Administrators					Confern Destanded				
Admin Profiles					EastiTaken Claud				000
Remote Authentication S					Porti loken Clobo	Disable FortiToken Mobile Email SMS			
Fabric Management					Administrative Domain	All ADOMs All ADOMs except specified ones Specify			
SAML SSO					Admin Profile	Veriti Profile			•
Settings					JSON API Access	Read-Write			٠
на					Theme Mode	Use Global Theme Use Own Theme			
Network					Trusted Hosts	0			
Event Logs					Meta Fields >				
Certificates									
Advanced					Advanced Options >				
FURTIDET						OK Cancel			

6. Verify the new user is presented in the "System Administrators" table.

63 F	AZVM64-AWSOnDemand							>_ @• ∴ <mark>0</mark> •	🔥 admin 👻
0		+0	eate New 🖌 🖾 Edit 🖄 Clone 🗄	Delete	Table View ~			Search	
80	Device Manager		Name 0	Type 0	Profile 0	JSON API Access 0	ADOMs 0	Trusted IPv4 Hosts 0	0
	ort/View >	∎ Syr	stem Administrator						
	abric View		Ag admin	LOCAL	Super_User	None	All ADOMs	0.0.0.0/0.0.0	
81		-	M at at	1054	Mariti Drofile	Read & Write	ALL ADOMA	0000/0000	
	Reports >		* Venb	LOCAL		Nead of Thine	ALACANS	000000000	
•	vstem Settings								
É									
	idmin Profiles								
F									
s									
5	ettings								
F									
<u>,</u>	letwork								
	vent Logs								
	idvanced								
	FURTIDET								

Veriti Configuration

The Veriti platform requires that you initialize connections with the relevant device to fetch the relevant data from your security products.

Integrating with FortiManager:

1. Log in to Veriti Portal via <a href="https://<veriti_server_ip>:30002">https://<veriti_server_ip>:30002 and enter your credentials.



2. On the left panel, click on "Settings."



3. Click on "Integrations."

4	Settings			
8				
8		Alerts & Notifications		>
÷		Audit Trails		>
æ		Q Custom Protections		>
0		 Important Assets 		>
		Integrations		2
°		Meports		,
۰		VERITI © 2023	Up-to-date	0 1
1				

4. On the top panel, click "Network" and choose "Fortinet."

Settings >	> Integrations					
e -	All Network	Endpoint Vulnerability assessm	ent			
		-				
Check	Point Palo Alto I	Networks Fortinet	F5 BIG-IP Advanced	Cloudflare		
Network	k Network	Network	Network	Network		

5. On the connector page, click "Connect" and choose "FortiManager" as the registration type.

*	Settings > Integrations > 🔛 Fortin	ot			
25	Default Connector				B Save
	About connector	Inspected assets			
	Default Connector		New Connection	×	III ~ O Rems 1
	Connector type		Basistar bas		
			FortiManager		
	Not connected		O Standalone FortiGate / FortiCluster		
	Server IP address Not available		Standalone FortiAnalyzer		
			Username Enter Username		
	🖇 Connect. 🥒 Edit		Password		
			Enter Password	6	
			Enter host name		
			Port (Optional)	nection	
			a construction of the second s		
				Cancel Connect	
-					
0					

- 6. Fill in the following details in the "New Connection" menu:
 - a. Username
 - b. Password
 - c. FortiManager IP Address
 - d. Port (optional by default, it is 443)
- 7. Click "Connect."
- 8. Verify your FortiManager and managed devices are presented in the "Inspected Assets" table.
- 9. Click "Save" on the top right to start fetching data from your devices.

Integrating with Standalone FortiGate NGFW:

1. Log in to Veriti Portal via :30002">https://cveriti_server_ip>:30002 and enter your credentials.



2. On the left panel, click on "Settings."

4	Welcome, Shay						0 logs analyzed 🛢
 8	Security Posture	stoure triagets		Cyber Attacks O O		Exposed Vulnerabilities	
• • •	NEW PROVIS	No new insights found! Keep up the good work	TRLINE PLANE	BUSINESS CONTINUITY * 0			
0 1		No new remodulations found! Cito: to start	THE LEGEL CONTRACTOR	REMEDIATIONS DISTRIBUTION	No new remediation Cick to set	found!	

3. Click on "Integrations."

^	Settings			
85				
8		Alerts & Notifications		>
÷		Audit Trails		>
æ		Q Custom Protections		>
Č		 Important Assets 		>
Ŷ		Integrations		>
۰		Reports		,
		L Osers		,
0		VERITI © 2023	Up-to-date	0 1
1				

4. On the top panel, click "Network" and choose "Fortinet."

4	Settings > Integrations						
- 88	AI	Network Endpo	int Vulnerability ass	essment			
8	e.	-		æ			
•	Check Point	Palo Alto Networks	Fortinet	F5 BIG-IP Advanced WAF	Cloudflare		
φ				Network	191990		
•							
۲							
0							

5. On the connector page, click "Connect" and choose "Standalone FortiGate" as the registration type.

Note: If multiple standalone devices exist, each one will require a new connector.

6. Fill in the following details in the "New Connection" menu:

a. API Token

- b. FortiGate IP Address
- c. Port (optional by default, it is 443)
- d. Choose the type of the Log Server:
 - i. Local If security logs are saved on FortiGate
 - ii. FortiAnalyzer If security logs are sent and saved on FortiAnalyzer, fill in the following details of the FortiAnalyzer:
 - 1. Username
 - 2. Password
 - 3. FortiAnalyzer IP Address
 - 4. Port (optional by default, it is 443)

<u> </u>	Settings > Integrations > [2] Fortin	et			
	Default Connector				B Sec.
8	About connector Connector name	Inspected assets			∏ v 01mm
9	Default Connector Connector type		5 New Connection	×	
φ	Not available Connector status Not connected		Register type FortiManager		
9	Server IP address Not available		Standaione Fortikiate / Fortikiater Standaione Fortikinalyzer		
۲			API Token Enter API token	0	
	• connet		P Address Enter host name		
			Port (Optional) Enter port		
			Logs Server Eccal		
			 FortiAnalyzer 		
				Cancel Connect	
0					
£					

- 7. Click "Connect."
- 8. Verify your FortiGate or FortiAnalyzer is presented in the "Inspected Assets" table.
- 9. Click "Save" on the top right to start fetching data from your devices.

Integrating with Standalone FortiAnalyzer:

1. Log in to Veriti Portal via <u>https://<veriti_server_ip>:30002</u> and enter your credentials.

VERITI Security Controls Optimization Platform	
	Welcome! Le deplantentente Messal Messal Messal Septi Septi Septi Messal Septi Sept

2. On the left panel, click on "Settings."



3. Click on "Integrations."

4	Settings				
-					
8		& Alerts	& Notifications		
٠		Audit Audit	Trails		
φ		Q, Custo	m Protections		
•		+ Impor	tant Assets		
		Report	15		
Ĩ		1 Users			
-		VERITI © 21	923 Up-to-date	0	,
1					

4. On the top panel, click "Network" and choose "Fortinet."

4	Settings > Integrations				
85	AI	Network Endpo	int Vulnerability asse	esement	
8	6	-	o	G	
*	Check Point Network	Palo Alto Networks Network	Fortinet Network	F5 BIG-IP Advanced WAF Network	Cloudflare Network
*				a man compto se	
č					
•					
+					

- 5. On the connector page, click "Connect" and choose "Standalone FortiAnalyzer" as the registration type.
- 6. Fill in the following details in the "New Connection" menu:
 - a. Username
 - b. Password
 - c. FortiAnalyzer IP Address
 - d. Port (optional by default, it is 443)

*	Settings > Integrations > El Fortine		
13	Default Connector		B See
8	About connector Connector name	Inspected assets) Rems I
9		New Connection X	
φ	Not available Connector status	Register type Ö FortMunager	
0	Not connected Server IP address	Standalore FortGate / FortGate e Standalore FortGate e	
	Not available	Userane Entro Userane	
	∮ Connect 🖉 Edit	Pessent Date Person	
		P Address Draw host name	
		Port (Contrau) exection Enter port	
		Const Connet	
•			
1			

- 7. Click "Connect."
- 8. Verify your FortiAnalyzer is presented in the "Inspected Assets" table.
- 9. Click "Save" on the top right to start fetching data from your device.

Known Limitations

- In the absence of FortiManager, remediation of global VDOMs is not supported.
- ADOMs in FortiAnalyzer are currently not supported.



www.fortinet.com

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet^{*}, FortiGate^{*}, Fortinet^{*}, FortiGate^{*}, Fortinet^{*}, FortiGate^{*}, Fortinet^{*}, Forti^{*}, Fortinet^{*}, Fortinet^{*}, Fortinet^{*}, Fortinet^{*}, Fo

February 8, 2024 10:50 AM 2546153-0-0-EN