

Examples

FortiManager 7.0.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



August 1, 2021

FortiManager 7.0.0 Examples

02-700-735790-20201216

TABLE OF CONTENTS

Change Log	4
Introduction	5
Device Manager	6
Exporting a policy package from one FortiManager to another	6
VPN Manager	8
Configuring a full mesh VPN topology within a VPN console	8
FortiSwitch Manager	15
Using central management	15
Enabling FortiSwitch central management	15
Importing and editing FortiSwitch templates	16
Creating FortiSwitch templates	17
Assigning templates to FortiSwitch devices	19
Using per-device management	20
Enabling FortiSwitch per-device management	20
Configuring FortiSwitch profiles	20
Configuring FortiSwitch ports	22
Installing changes to FortiSwitch devices	23
Upgrading FortiSwitch firmware	24
Using zero touch deployment for FortiSwitch	25
System Settings	27
Configuring and debugging FortiManager HA clusters	27
Configuring the primary FortiManager unit in an HA cluster	27
Configuring backup FortiManager units in an HA cluster	28
Generating and downloading HA debug logs	28
Creating administrator accounts with restricted access	29
Restricting administrator access to ADOMs	29
Restricting administrator access to device groups	31
Restricting administrator access to policy packages	32
Others	34
Managing FortiAnalyzer from FortiManager	34
Adding FortiAnalyzer to FortiManager	34
Viewing managed FortiAnalyzer behavior	38
Centrally configuring FortiGate to send logs to managed FortiAnalyzer	39
Viewing logs and reports for managed FortiAnalyzer units	39
Managing multiple FortiAnalyzer units	40
Troubleshooting managed FortiAnalyzer units	41
Creating a third party blocklist provider workflow	42

Change Log

Date	Change Description
2021-08-01	Initial release.

Introduction

This document serves as a reference guide to common FortiManager 7.0 configuration and deployment scenarios. The scope of this document is to explain specific examples and include information required for those examples to work. The examples rely on the other documents to provide full product information.



For further FortiManager information, refer to the [FortiManager Administration Guides](#) available on the [Fortinet Docs Library](#).

This section includes configuration examples for FortiManager 7.0:

- [Device Manager on page 6](#)
- [VPN Manager on page 8](#)
- [FortiSwitch Manager on page 15](#)
- [System Settings on page 27](#)
- [Others on page 34](#)

Device Manager

This section contains the following topics:

- [Exporting a policy package from one FortiManager to another](#) on page 6

Exporting a policy package from one FortiManager to another

In this example, you will learn how to export a policy package from one FortiManager to another FortiManager.

To export a policy package from one FortiManager to another FortiManager:

1. Select a FortiManager policy package and installation target you want to export:
 - a. Select a FortiManager policy package and its installation target.
For example,
Policy Package: PP_001
Installation Target: Device1
2. Download the latest revision:
 - a. Go to *Device Manager > Device & Groups >* and double-click the installation target device (Device1 in this example).
 - b. Go to *Dashboard > Configuration and Installation Status > Total Revisions*.
 - c. Download the latest revision (for example, Revision 1).
3. Add the device to the second FortiManager:
 - a. Go to your second FortiManager.
 - b. Go to *Device Manager > Device & Groups >* and click *Add Device*. The Add Device wizard displays.
Its SN must be similar to the one you got the revision from. It can be the same as the original SN, or you can take the SN prefix (the first six characters) and append 10 digits to it.
For example, FG200D12345985242 is the original SN.
Prefix: FG200D
Appended 10 Digits: 0000000001
The new SN will be: FG200D0000000001.
 - c. Select *Add Model Device* and complete the wizard.
4. Import the revision to the second FortiManager:
 - a. On your second FortiManager device, go to *Device Manager > Device & Groups* and double-click the model device. The Device Dashboard displays.
 - b. Go to *Dashboard > Configuration and Installation Status > Total Revisions*.
 - c. Right-click the empty revision list and select *Import Revision > Revision 1*.
 - d. Go to *Device Manager > Device & Groups*.
 - e. Right-click your model device and select *Import Policy*. The wizard displays.

- f. Complete the wizard.
- g. Go to *Policy & Objects*. The policy package and its used objects are displayed.



For further FortiManager information, refer to the [FortiManager Administration Guides](#) available on the [Fortinet Document Library](#).

VPN Manager

This section contains the following topics:

- [Configuring a full mesh VPN topology within a VPN console on page 8](#)

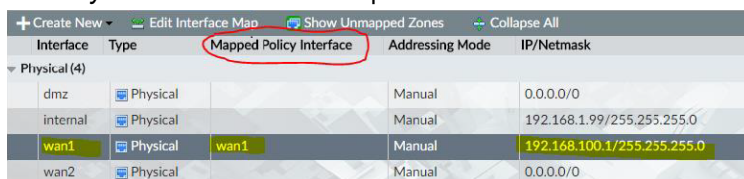
Configuring a full mesh VPN topology within a VPN console

This is an example on how to configure a simple full mesh VPN with:

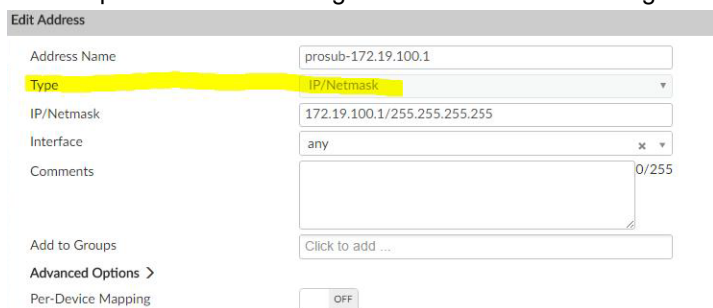
- Three FortiGate (FGT) devices
- A pre-shared key for authentication
- An auto-up tunnel setting
- Static routes

To configure a full mesh VPN topology within a VPN console:

1. Add FortiGate devices and map all interfaces:
 - a. Go to *Device Manager*. Add three FortiGate devices by clicking *Add Device*. Follow the wizard to add each device.
 - b. Go to *Policy & Objects > Policy Packages* and define the *Zone* interfaces.
 - c. Go to *Device Manager* and select a device.
 - d. Go to *System > Interface* and map the interfaces to the *Zone* interfaces.
2. Create firewall addresses for protected subnets:
 - a. Go to *Policy & Objects > Object Configurations > Firewall Objects > Address* to manage the firewall addresses.
 - b. VPNs only support firewall addresses with the type set to *subnet (IP/Netmask)*. The firewall addresses will be used as protected subnets to generate static routes among the FortiGate devices.



Interface	Type	Mapped Policy Interface	Addressing Mode	IP/Netmask
dmz	Physical		Manual	0.0.0.0/0
internal	Physical		Manual	192.168.1.99/255.255.255.0
wan1	Physical	wan1	Manual	192.168.100.1/255.255.255.0
wan2	Physical		Manual	0.0.0.0/0



Edit Address

Address Name: prosub-172.19.100.1

Type: IP/Netmask

IP/Netmask: 172.19.100.1/255.255.255.255

Interface: any

Comments: 0/255

Add to Groups: Click to add ...

Advanced Options >

Per-Device Mapping: OFF

3. Create a VPN community:

- a. Go to *VPN Manager > IPsec VPN > VPN Community list > Create New*.
- b. Set the *VPN Topology* type to *Full Meshed*.

VPN Topology Setup Wizard

fullmesh
demo for full mesh topology

Choose VPN Topology

Full Meshed Star Dial up

< Back Next > Cancel

- c. Define the *Authentication* method with a *Pre-shared Key*.
- d. Specify the encryption and hash methods.

VPN Topology Setup Wizard

Authentication & Encryption Settings:

Authentication Certificates Pre-shared Key

☐ Generate(random)

☒ Specify *****

Encryption

IKE Security (Phase 1) Properties

1-Encryption	3DES	Authentication	SHA-1	+	🗑
2-Encryption	3DES	Authentication	MD5	+	🗑

IPsec Security (Phase 2) Properties

1-Encryption	3DES	Authentication	SHA-1	+	🗑
2-Encryption	3DES	Authentication	MD5	+	🗑

< Back Next > Cancel

- e. After defining the authentication methods and encryption properties, click *Next*.

f. Configure the *VPN Phase 1* and *Phase 2* settings.

VPN Topology Setup Wizard

VPN Zone ☒ ON

☒ Create Default Zones
☐ Use Custom Zone

IKE Security Phase 1 Advanced Properties

Diffie Hellman Group(s) ☐ 2 ☒ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17
☐ 18 ☐ 19 ☐ 20 ☐ 21

Exchange Mode ☐ Aggressive ☒ Main(ID Protection)

Key Life (120-172800 seconds)

Dead Peer Detection ☒ ON

IPsec Security Phase 2 Advanced Properties

Diffie Hellman Group(s) ☐ 2 ☒ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17
☐ 18 ☐ 19 ☐ 20 ☐ 21

Replay Detection ☒ ON

Perfect Forward ☒ ON

< Back Next > Cancel

g. For the *IPSec Phase 2* setting, set the tunnel to *Auto-Negotiate*.

VPN Topology Setup Wizard

Dead Peer Detection ☒ ON

IPsec Security Phase 2 Advanced Properties

Diffie Hellman Group(s) ☐ 2 ☒ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17
☐ 18 ☐ 19 ☐ 20 ☐ 21

Replay Detection ☒ ON

Perfect Forward Secrecy(PFS) ☒ ON

Key Life ☒ Seconds ☐ KB ☐ Both
 seconds KB

Autokey Keep Alive ☒ ON

Auto-Negotiate ☐ OFF

NAT-traversal ☒ Enable ☐ Disable ☐ Forced

Keep Alive Frequency (10-900 seconds)

Advanced Options >

< Back Next > Cancel

VPN configuration summary:

The screenshot shows the 'Edit VPN Community' configuration page in FortiManager. The left sidebar contains navigation options: Full, Star, Monitor, and Map View. The main configuration area includes the following sections:

- Name:** Full
- Description:** test full mesh
- Topology:** Full Meshed
- Authentication:** Certificates (selected), Pre-shared Key, Generate(random), Specify
- Encryption:**
 - IKE Security (Phase 1) Properties:**
 - 1-Encryption: DES, Authentication: SHA-1
 - 2-Encryption: DES, Authentication: MD5
 - IPsec Security (Phase 2) Properties:**
 - 1-Encryption: DES, Authentication: SHA-1
 - 2-Encryption: DES, Authentication: MD5
- VPN Zone:** ON, Create Default Zones (selected), Use Custom Zone
- IKE Security Phase 1 Advanced Properties:**
 - Diffie Hellman Group(s): 2, 5, 14, 15, 16, 17, 18, 19, 20, 21

4. Add a VPN gateway:

- Go to *VPN Manager > IPsec VPN > VPN Communities* and select your VPN community.
- In the content pane, from the *Create New* menu, select *Managed Gateway*.
- Add a *Protected Network*. There can be more than one protected networks.






The screenshot shows the 'VPN Gateway Setup Wizard - Full' in FortiManager. The wizard progress bar indicates the following steps: Protected Network, Device, Default VPN Interface, Local Gateway, and Advanced. The 'Protected Network' step is currently active, showing a list of protected subnets:

- prosub
- IP/Netmask:172.19.100.104/255.255.255...
- prosub-172.19.100.2
- IP/Netmask:172.19.100.2/255.255.255...
- prosub-172.19.100.3
- IP/Netmask:172.19.100.3/255.255.255...
- prosub-172.19.100.4
- IP/Netmask:172.19.100.4/255.255.255...
- prosub-172.19.100.5

At the bottom of the wizard, there are three buttons: '< Back', 'Next >', and 'Cancel'.

d. Select a *Device*.

VPN Gateway Setup Wizard - Full






    

Protected Network **Device** Default VPN Interface Local Gateway Advanced

Device

e. Select a *Default VPN Interface*. The default VPN interface should have a valid IP and be mapped.

VPN Gateway Setup Wizard - Full

Protected Network Device **Default VPN Interface** Local Gateway Advanced

Default VPN Interface

- i. Optionally, specify the *Local Gateway*. This option can be left blank in most cases.

VPN Gateway Setup Wizard - ☒ Full

Protected Network Device Default VPN Interface **Local Gateway** Advanced

Local Gateway IP Address

< Back Next > Cancel

- f. Go to *Routing* and select *Automatic* to generate static routes.

VPN Gateway Setup Wizard - ☒ Full

Routing ☐ Manual (via Device Manager)
☒ Automatic

Local ID

Advanced Options ▾

authpasswd

authuser

banner

dns-mode

domain

public-ip

route-overlap

< Back OK Cancel

- i. If *Manual* is selected, go to the *Device Manager* to set the IP on the relevant IPsec interfaces and define the routings manually.

VPN gateway configuration settings summary:

Edit Gateway

Protected Subnet	* prosub-172.19.100.1
Device	FGT-168-100-1[root]
Default VPN Interface	wan1
Local Gateway	IP Address
Routing	<input type="radio"/> Manual (via Device Manager) <input checked="" type="radio"/> Automatic
Local ID	<input type="text"/>
Advanced Options	>

5. Create firewall policies:

- a. Go to *Policy & Objects > Policy Package* to create policies among the default VPN zones and protected-subnet interfaces.

- b. Use the *Install On* option to restrict policies applied on specific FortiGate devices.

Interface Pair View By Sequence											
Seq#	From	To	Source	Destinat...	Schedule	Service	Action	Log	NAT	Install On	
1	loop1	vpnmgc_Full_rm	all	all	always	ALL	Accept	Log Security Ev	Disabled	<input type="checkbox"/> FGT-168-100-4 (root) <input type="checkbox"/> FGT-168-100-2 (root) <input type="checkbox"/> FGT-168-100-3 (root) <input type="checkbox"/> FGT-168-100-1 (root) <input type="checkbox"/> FGT-168-100-5 (root)	
2	vpnmgc_Full_rm	loop1	all	all	always	ALL	Accept	Log Security Ev	Disabled	<input type="checkbox"/> FGT-168-100-4 (root) <input type="checkbox"/> FGT-168-100-2 (root) <input type="checkbox"/> FGT-168-100-3 (root) <input type="checkbox"/> FGT-168-100-1 (root) <input type="checkbox"/> FGT-168-100-5 (root)	
3	loop1	vpnmgc_Full_rm	prosub-172.19.100.22 prosub-172.19.100.23 prosub-172.19.100.24 prosub-172.19.100.25 prosub-172.19.100.26 prosub-172.19.100.27 prosub-172.19.100.28 prosub-172.19.100.29 prosub-172.19.100.30	all	always	ALL	Accept	Log All Sessions	Disabled	<input type="checkbox"/> FGT-168-100-22 (root) <input type="checkbox"/> FGT-168-100-23 (root) <input type="checkbox"/> FGT-168-100-24 (root) <input type="checkbox"/> FGT-168-100-25 (root) <input type="checkbox"/> FGT-168-100-26 (root) <input type="checkbox"/> FGT-168-100-27 (root) <input type="checkbox"/> FGT-168-100-28 (root) <input type="checkbox"/> FGT-168-100-29 (root) <input type="checkbox"/> FGT-168-100-30 (root)	

- c. Remember to create policies for bi-directional traffic.



For further FortiManager information, refer to the [FortiManager Administration Guide](#) available on the [Fortinet Document Library](#).

FortiSwitch Manager

FortiSwitch Manager is used to manage and monitor FortiSwitch units. Managed FortiSwitch units are connected to FortiGate units that are managed by FortiManager. This chapter contains the following topics:

- [Using central management on page 15](#)
- [Using per-device management on page 20](#)
- [Installing changes to FortiSwitch devices on page 23](#)
- [Upgrading FortiSwitch firmware on page 24](#)
- [Using zero touch deployment for FortiSwitch on page 25](#)

Using central management

You can use *FortiSwitch Manager* for central management or per-device management of managed FortiSwitch units. This section describes how to use central management.

Following is a high-level summary of how to use central management:

1. Enable central management. See [Enabling FortiSwitch central management on page 15](#).
2. Create templates.
You can import templates from managed switches, or you can create new templates. See [Importing and editing FortiSwitch templates on page 16](#) or [Creating FortiSwitch templates on page 17](#).
3. Assign templates to managed switches. See [Assigning templates to FortiSwitch devices on page 19](#).
4. Install changes to managed switches. See [Installing changes to FortiSwitch devices on page 23](#).

Enabling FortiSwitch central management

When central management is enabled, you can create templates for a variety of switch configurations, and assign templates to multiple managed switches of the same type.

To enable central management:

1. Go to *System Settings > All ADOMs*.
2. Double-click the ADOM to open it for editing.

3. Beside *Central Management*, select the *FortiSwitch* checkbox, and click *OK*.

Edit ADOM

Name: root

Type: FortiGate 7.0

Description:

Devices

Name	IP Address	Platform
Branch_Office_01	10.0.11.2	FortiGate-VM64-KVM
Branch_Office_02	10.0.12.3	FortiGate-VM64-KVM
Enterprise_First_Floor	10.100.88.101	FortiGate-VM64-KVM
Enterprise_Second_Floor	10.100.88.102	FortiGate-VM64-KVM
FGT_Root	10.100.88.1	FortiGate-VM64-KVM

Central Management ☒ VPN ☒ FortiAP ☒ FortiSwitch

Default Device Selection for Install ☒ Select All ☐ Deselect All

Perform Policy Check Before Every Install ☐

Auto-Push Policy Packages When Device Back Online ☐ Enable ☒ Disable

Central management is enabled for FortiSwitch.

Importing and editing FortiSwitch templates

You can import a template of settings from a managed FortiSwitch unit, and then use FortiManager to edit the template before installing the changes back to the switch or assigning the template to other switches of the same type.

To import FortiSwitch templates:

1. Go to *FortiSwitch Manager > FortiSwitch Templates*.
2. In the tree menu, select *FortiSwitch Template*, and click *Import* in the toolbar. The *Import* dialog box opens.

Import

FortiGate: Click to select

FortiSwitch: None

OK Cancel

3. Set the following options, and click *OK*.
 - a. In the *FortiGate* list, select a FortiGate.
 - b. In the *FortiSwitch* list, select the FortiSwitch from which to import the template.

- c. (Optional) In the *New Name* box, type a name for the template.

When you leave this option blank, the template is named by using the default naming pattern.

The template is imported and displayed on the content pane.

+ Create New Edit Delete Where Used Import Column Settings -			
<input type="checkbox"/> Name	Description	Platform	Last Modified
<input checked="" type="checkbox"/> Test	Imported from switch S424DN3X17000097	FortiSwitch-424D	admin/2019-11-20 12:06:41
<input type="checkbox"/> template-287	Imported from switch S448DN3X16000287	FortiSwitch-448D	admin/2019-11-20 10:45:53

To edit a template:

1. Go to *FortiSwitch Manager > FortiSwitch Templates*.
2. In the tree menu, select *FortiSwitch Templates*.

The available templates are displayed.

+ Create New Edit Delete Where Used Import Column Settings -			
<input type="checkbox"/> Name	Description	Platform	Last Modified
<input checked="" type="checkbox"/> Test	Imported from switch S424DN3X17000097	FortiSwitch-424D	admin/2019-11-20 12:06:41
<input type="checkbox"/> template-287	Imported from switch S448DN3X16000287	FortiSwitch-448D	admin/2019-11-20 10:45:53

3. Select a template, and click *Edit*.
The template opens for editing.
4. Edit the options, and click *OK*.

Creating FortiSwitch templates

Instead of importing a template of settings from FortiSwitch units to FortiManager, you can create templates on the *FortiSwitch Manager* pane in FortiManager.

You can create the following components, and then create a variety of templates that select different combinations of the components:

- VLANs
- Security policies
- LLDP profiles
- QoS policies

This topic describes how to create a security policy and a template.

To create security policies:

1. Go to *FortiSwitch Manager > FortiSwitch Templates*.
2. Click *Security Policy*, and click *Create New*.
The *Create New Security Policies* pane opens.

Create New Security Policies

Name

Security mode **Port-based** MAC-based

User groups

Guest VLAN ☐ OFF

Guest authentication delay second(s)

Authentication fail VLAN ☐ OFF

MAC authentication bypass ☐ OFF

EAP pass-through ☒ ON

Override RADIUS timeout ☐ OFF

- Set the options, and click **OK**.
The security policy is created.

To create FortiSwitch templates:

- Go to *FortiSwitch Manager > FortiSwitch Templates*.
- Ensure that you have created all of the following components that you want to use in one or more templates: VLANs, security policies, LLDP profiles, and QoS profiles.
- Click *FortiSwitch Templates*, and click *Create New*.
The *Create New FortiSwitch Template* pane opens.

Create New FortiSwitch Template

Template Name Name is required

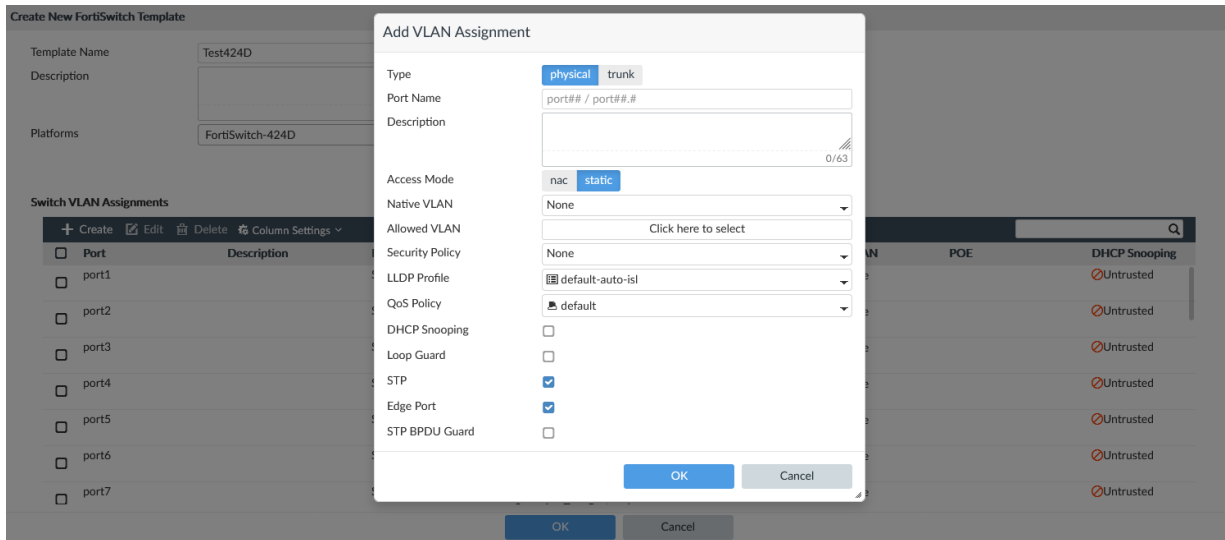
Description 0/63

Platforms Platform is required...

Switch VLAN Assignments

<input type="checkbox"/> Port	Description	Mode	Enabled Features	Native VLAN	Allowed VLAN	POE	DHCP Snooping
No record found.							

- Set the following options, and click **OK**.
 - In the *Template Name* box, type a name for the template.
 - In the *Platforms* list, select the FortiSwitch platform.
 - Under *Switch VLAN Assignments*, click *Create*.
The *Add VLAN Assignment* dialog box opens.



- d. In the *Allowed VLAN* box, select the VLAN configuration that you created.
 - e. In the *Security Policy* box, select the security policy that you created.
 - f. In the *LLDP Profile* box, select the LLDP profile that you created.
 - g. In the *QoS Policy* box, select the QoS policy that you created.
 - h. Set the remaining options as required.
5. Click **OK**.

Assigning templates to FortiSwitch devices

Use the *FortiSwitch Manager* pane to assign templates of settings to switches.

To assign templates:

1. Go to *FortiSwitch Manager > Device & Groups > Managed FortiGate*.
2. In the tree menu, select a FortiGate to list its managed switches, or select *All_FortiGate* to list all switches. The list of managed FortiSwitch units is displayed in the content pane.
3. Use the quick status bar to filter the list of switches in the content pane and help locate the switch.
4. Select the switch, and click *Assign Template* from the toolbar. The *Assign FortiSwitch Template* dialog box opens.
5. Select a FortiSwitch template, and click **OK** to assign it.



Only templates that apply to the specific device model are available for selection



You also assign templates when editing a FortiSwitch device.

6. Install the template settings. See [Installing changes to FortiSwitch devices on page 23](#).

Using per-device management

You can use *FortiSwitch Manager* for central management or per-device management of managed FortiSwitch units. This section describes how to use per-device management.

Following is a high-level summary of how to use per-device management:

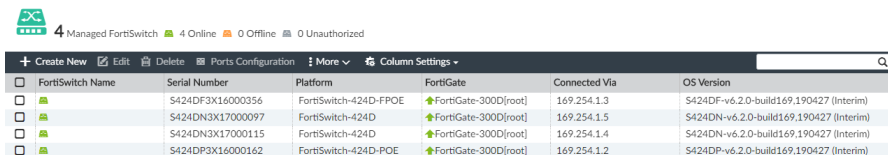
1. Enable per-device management. See [Enabling FortiSwitch per-device management on page 20](#).
2. Configure profiles for managed switches.
You can configure VLANs, security policies, LLDP profiles, and QoS policies, and the changes are saved to the FortiGate database. See [Configuring FortiSwitch profiles on page 20](#).
3. Configure ports for managed switches by assigning profiles.
When you configure ports, you can assign the profiles and policies that you created. See [Configuring FortiSwitch ports on page 22](#).
4. Install changes to managed switches. See [Installing changes to FortiSwitch devices on page 23](#).

Enabling FortiSwitch per-device management

When per-device management is enabled, you can configure changes on each managed switch.

To enable FortiSwitch per-device management:

1. Go to *System Settings > All ADOMs*.
2. Double-click the ADOM to open it for editing.
3. Beside *Central Management*, clear the *FortiSwitch* checkbox, and click *OK*.
Central management is disabled, and per-device management is enabled for FortiSwitch.
4. Go to *FortiSwitch Manager*, and notice that *Per-device Management* is displayed in the top-right corner.



FortiSwitch Name	Serial Number	Platform	FortiGate	Connected Via	OS Version
<input type="checkbox"/>	S424DF3X16000356	FortiSwitch-424D-FPOE	FortiGate-300D[root]	169.254.1.3	S424DF-v6.2.0-build169.190427 (Interim)
<input type="checkbox"/>	S424DN3X17000097	FortiSwitch-424D	FortiGate-300D[root]	169.254.1.5	S424DN-v6.2.0-build169.190427 (Interim)
<input type="checkbox"/>	S424DN3X17000115	FortiSwitch-424D	FortiGate-300D[root]	169.254.1.4	S424DN-v6.2.0-build169.190427 (Interim)
<input type="checkbox"/>	S424DP3X16000162	FortiSwitch-424D-POE	FortiGate-300D[root]	169.254.1.2	S424DP-v6.2.0-build169.190427 (Interim)

Configuring FortiSwitch profiles

When per-device management is enabled, you can use the *FortiSwitch Manager* pane to configure profile and policy settings for each managed switch. The settings are saved to the FortiGate database, but not yet assigned or installed to switches.

You can configure the following types of profiles and policies:

- VLANs
- Security policies
- LLDP profiles
- QoS policies

After you create the profiles and policies, you can configure ports for managed switches to select the VLANs, policies, and profiles you created, and then assign and install the settings to managed switches.

To configure VLANs:

1. Go to *FortiSwitch Manager*.
2. In the tree menu, select a FortiGate.
3. Select *FortiSwitch Profiles > VLAN* from the toolbar.

The *VLAN* page is displayed.

+ Create New Edit Delete Where Used Column Settings							
<input type="checkbox"/>	Name	Alias	VLAN ID	IP/Netmask	Access	Last Modified	Created Time
<input type="checkbox"/>	FortiLink Interface (1)						
<input type="checkbox"/>	fortilink		0	169.254.1.1/255.255.255.0	PING, CAPWAP	admin/2019-11-20 10:40:47	2019-11-20 10:40:47
<input type="checkbox"/>	VLANs (6)						
<input type="checkbox"/>	www.fortilink		1	0.0.0.0/0.0.0.0		admin/2019-11-20 10:40:47	2019-11-20 10:40:47
<input type="checkbox"/>	qtn.fortilink		4093	10.254.254.254/255.255.255.0		admin/2019-11-20 10:40:47	2019-11-20 10:40:47
<input type="checkbox"/>	vol.fortilink		4091	0.0.0.0/0.0.0.0		admin/2019-11-20 10:40:47	2019-11-20 10:40:47
<input type="checkbox"/>	cam.fortilink		4090	0.0.0.0/0.0.0.0		admin/2019-11-20 10:40:47	2019-11-20 10:40:47
<input type="checkbox"/>	snf.fortilink		4092	10.254.253.254/255.255.254.0	PING	admin/2019-11-20 10:40:47	2019-11-20 10:40:47
<input type="checkbox"/>	VLAN1		2	0.0.0.0/0.0.0.0		admin/2019-11-21 15:30:05	2019-11-21 15:30:05

4. Double-click a VLAN to open it for editing, or click *Create New* to create a new VLAN.
 5. Edit the options, and click *OK*.
- The VLAN settings are saved to the FortiGate database.

To configure Security Policies:

1. Go to *FortiSwitch Manager*.
 2. In the tree menu, select a FortiGate.
 3. Select *FortiSwitch Profiles > Security Policy* from the toolbar.
- The *Security Policy* page is displayed.
4. Double-click a security policy to open it for editing, or click *Create New* to create a new policy.
 5. Edit the options, and click *OK*.
- The policy is saved to the FortiGate database.

To configure LLDP Profiles:

1. Go to *FortiSwitch Manager*.
 2. In the tree menu, select a FortiGate.
 3. Select *FortiSwitch Profiles > LLDP Profile* from the toolbar.
- The *LLDP Profile* page is displayed.
4. Double-click an LLDP profile to open it for editing, or click *Create New* to create a new profile.
 5. Edit the options, and click *OK*.
- The profile is saved to the FortiGate database.

To configure QoS policies:

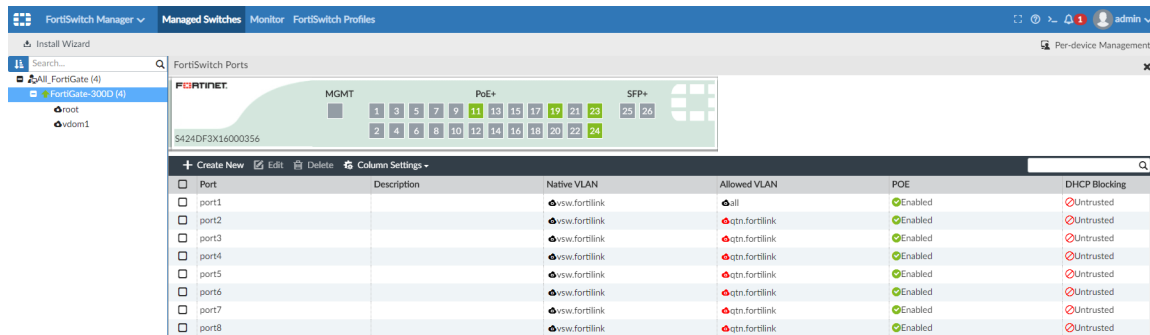
1. Go to *FortiSwitch Manager*.
 2. In the tree menu, select a FortiGate.
 3. Select *FortiSwitch Profiles* from the toolbar and select a QoS policy type.
- The corresponding policy page is displayed, for example *QoS Policy*.
4. Double-click the policy to open it for editing, or click *Create New* to create a new policy.
 5. Edit the options, and click *OK*.
- The policy is saved to the FortiGate database.

Configuring FortiSwitch ports

When per-device management is enabled, you can use the *FortiSwitch Manager* pane to configure ports for each managed switch. When you configure ports, you can assign the VLANs, security policies, LLDP profiles, and QoS policies that you created by using the *FortiSwitch Profiles* tab.

To configure switch ports:

1. Go to *FortiSwitch Manager > Managed Switches*.
2. In the tree menu, select a FortiGate.
The list of managed switches is displayed in the content pane.
3. Double-click a switch.
The *FortiSwitch Ports* pane is displayed.



4. Double-click a port to open it for editing.
The *Edit Port* dialog box is displayed.

Edit Port

Port Name: port1

Description: 0/63

Native VLAN: vsw.fortilink

Allowed VLAN: all (1 Entry Selected)

Security Policy: 802-1X-policy-default

LLDP Profile: default-auto-isl

QoS Policy: default

PoE Status: ☒

DHCP Blocking: ☐

IGMP Snooping: ☒

Loop Guard: ☐

STP: ☒

Edge Port: ☒

OK Cancel

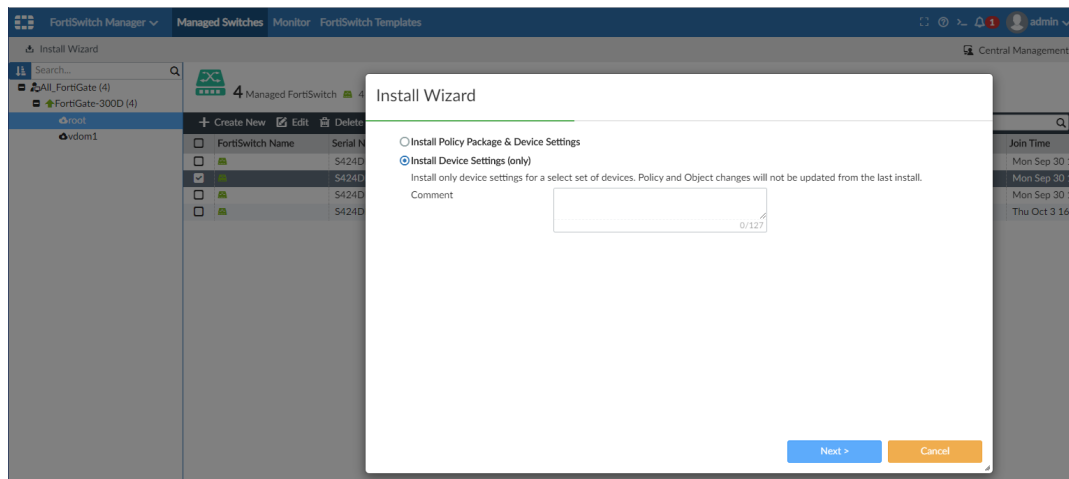
5. Edit the options and click **OK**.
The changes are saved to the FortiGate database.
6. Install the changes. See [Installing changes to FortiSwitch devices on page 23](#).

Installing changes to FortiSwitch devices

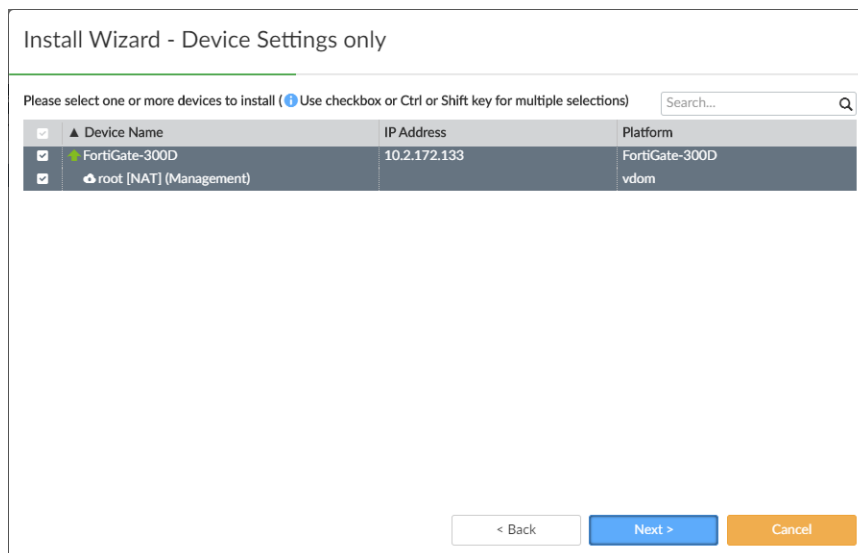
You can install changes to managed FortiSwitch devices directly from the *FortiSwitch Manager* pane. Alternately you can install changes when you install a configuration to the FortiGate that manages the switch.

To install changes to switches:

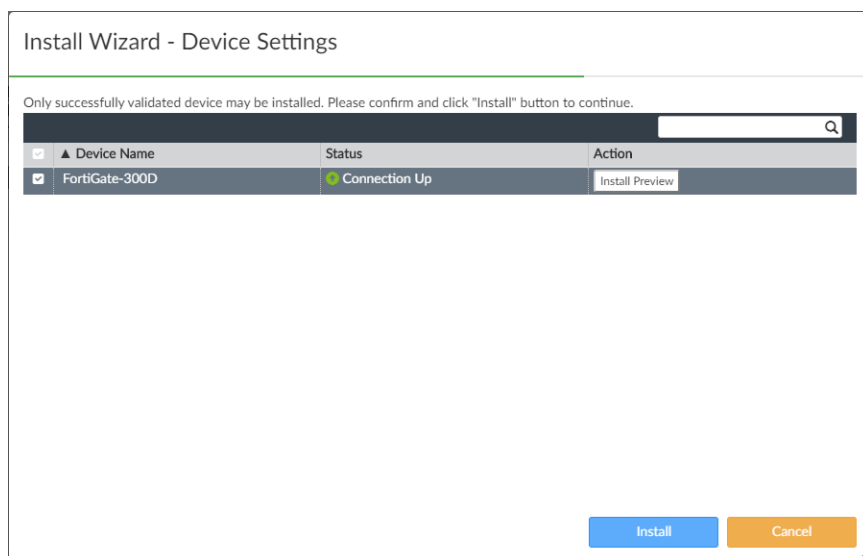
1. Go to *FortiSwitch Manager > Managed Switches*.
2. In the tree menu, select the FortiGate device that controls the FortiSwitch.
The managed switches are displayed in the content pane.
3. In the content pane, select the switch, and click *Install Wizard*.
The *Install Wizard* is displayed.



4. Select *Install Device Settings (only)*, and click *Next*.
The *Device Settings only* pane is displayed.



5. Select the device, and click *Next*.
The *Device Settings* pane is displayed.



6. (Optional) Click *Install Preview* to review the changes.
7. Click *Install*.

Upgrading FortiSwitch firmware

You can use FortiManager to upgrade firmware for FortiSwitch units. By default, FortiManager retrieves the firmware from FortiGuard.

You can also optionally import special firmware images for FortiSwitch to the FortiGuard module, and then use them to upgrade FortiSwitch units.

To upgrade FortiSwitch firmware:

1. Go to *FortiSwitch Manager > Managed Switches*.
2. In the tree menu, select a FortiGate.
The managed FortiSwitches are displayed in the content pane.
3. Right-click a FortiSwitch, and select *Upgrade*.
The *FortiSwitch Firmware Upgrade* dialog box is displayed.

FortiSwitch Firmware Upgrade

Selected FortiSwitches S448DN3X16000287

<input type="checkbox"/> Firmware	Release Date
▼ Official Images (15)	
<input type="checkbox"/> Firmware 6.2.2 build(194)	
<input type="checkbox"/> Firmware 6.2.1 build(176)	
<input type="checkbox"/> Firmware 6.2.0 build(168)	
<input type="checkbox"/> Firmware 6.0.4 build(64)	
<input type="checkbox"/> Firmware 6.0.3 build(52)	
<input type="checkbox"/> Firmware 6.0.2 build(46)	
<input type="checkbox"/> Firmware 6.0.1 build(36)	
<input type="checkbox"/> Firmware 6.0.0 build(27)	
<input type="checkbox"/> Firmware 3.6.9 build(426)	
<input type="checkbox"/> Firmware 3.6.8 build(424)	
<input type="checkbox"/> Firmware 3.6.7 build(418)	
<input type="checkbox"/> Firmware 3.6.6 build(416)	

☐ Let Device Download Firmware from FortiGuard ⓘ

Upgrade Now **Cancel**

4. Select the firmware, and click *Upgrade Now*.

Using zero touch deployment for FortiSwitch

You can configure FortiSwitch on FortiManager by using its serial number. Then you can use zero touch deployment of FortiSwitch devices across the network. After configuring FortiSwitch on FortiManager, you can deploy remote FortiSwitch devices by plugging them into remote FortiGate devices.

Requirements:

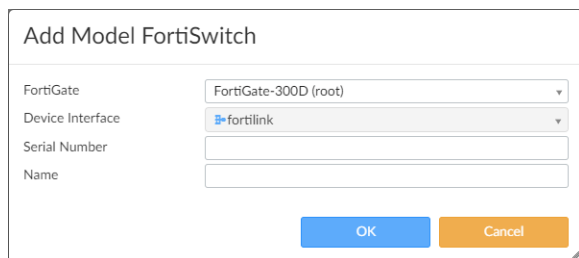
- FortiManager version 5.6 ADOM or later.
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with FortiSwitch.
- The FortiSwitch serial number is available.



You can also use the zero touch deployment process to deploy FortiGate devices.

To prepare FortiSwitch for zero touch deployment:

1. Go to *FortiSwitch Manager > Managed Switches*.
2. Click *Create New*.
The *Add Model FortiSwitch* pane is displayed.

A dialog box titled "Add Model FortiSwitch". It contains four fields: "FortiGate" with a dropdown menu showing "FortiGate-300D (root)", "Device Interface" with a dropdown menu showing "fortilink", "Serial Number" with an empty text box, and "Name" with an empty text box. At the bottom right are two buttons: "OK" (blue) and "Cancel" (orange).

Add Model FortiSwitch	
FortiGate	FortiGate-300D (root)
Device Interface	fortilink
Serial Number	
Name	
<div>OK Cancel</div>	

3. Configure the following settings, and click *OK*:

FortiGate	Select the FortiGate device or VDOM from the drop-down.
Device Interface	Select the port where the FortiSwitch will be connected.
Serial Number	Specify the FortiSwitch serial number.
Name	Specify a name.

A model FortiSwitch is created and added to the managed FortiGate.

4. Click *Close* to close the *Add Model FortiSwitch* pane.
5. Configure the switch.
 - For *FortiSwitch Manager* with central management enabled, see [Assigning templates to FortiSwitch devices on page 19](#).
 - For *FortiSwitch Manager* with per-device management enabled, see [Configuring FortiSwitch ports on page 22](#).Because this is a model device, FortiManager saves the changes to the FortiGate database.
6. Connect the FortiSwitch to FortiGate.

The FortiSwitch settings are deployed to FortiSwitch.

System Settings

This section contains the following topics:

- [Configuring and debugging FortiManager HA clusters on page 27](#)
- [Creating administrator accounts with restricted access on page 29](#)

Configuring and debugging FortiManager HA clusters

You can configure two or more FortiManager units in a high availability (HA) cluster. You can also generate and download a debug log for each unit in a FortiManager HA cluster.

The following is an overview of configuring FortiManager units in an HA cluster:

1. Configure the primary FortiManager unit. See [Configuring the primary FortiManager unit in an HA cluster on page 27](#)
2. Configure one or more backup FortiManager units. See [Configuring backup FortiManager units in an HA cluster on page 28](#)
3. If you encounter problems, review the debug log for each unit in an HA cluster. See [Generating and downloading HA debug logs on page 28](#).

Configuring the primary FortiManager unit in an HA cluster

You can configure one FortiManager unit to be the primary unit in a high availability (HA) cluster. You must know the IP address and serial number of the FortiManager units that will be configured as backup (also called secondary or peer) units in the HA cluster to complete this procedure.

To configure the primary FortiManager unit:

1. Go to *System Settings > HA*.
2. Set *Operation Mode* to *Primary*.
3. In the *Peer IP* box, enter the IP address of the backup FortiManager unit.
4. In the *Peer SN* box, enter the serial number of the backup (secondary or peer) FortiManager unit.

- Click + to add additional backup FortiManager units to the HA cluster.

System Settings ▾

Dashboard All ADOMs Network **HA** Admin ▾ Administrators Profile Workspace Remote Authentication Server Admin Settings SAML SSO Certificates > Event Log Task Monitor Advanced >

Cluster Settings

Operation Mode: Standalone **Primary** Secondary

Peer IP and Peer SN	IP Type	Peer IP	Peer SN
	IPv4	192.168.48.61	FM200D3A15000236 +

Cluster ID: 1 (1-64)

Group Password: [Empty]

File Quota: 4096 (2048-20480) MB

Heart Beat Interval: 5 Seconds

Failover Threshold: 3 (1-255)

Download Debug Log: [Download]

Apply

- Click *Apply*.

Configuring backup FortiManager units in an HA cluster

You can configure up to four FortiManager units as backup (also called secondary or peer) units in an HA cluster. You must know the IP address and serial number of the primary FortiManager unit in the HA cluster to complete this procedure.

To configure the backup FortiManager unit:

- Go to *System Settings > HA*.
- Beside *Operation Mode*, select *Secondary*.
- In the *Peer IP* box, enter the IP address of the primary FortiManager unit.
- In the *Peer SN* box, enter the serial number of the primary FortiManager unit.
- Click *Apply*.

Generating and downloading HA debug logs

You can run a command to generate a debug log for each FortiManager unit in an HA cluster, and then you can download the logs using the GUI.

To generate a debug log:

- On the primary or backup (secondary) FortiManager unit in an HA cluster, enter the following command:

```
diagnose debug application ha 255
```

To download a debug log:

- Go to *System Settings > HA*.
- Next to *Download Debug Log*, click *Download*.
- Save the log file (`ha-<date>.log`) to your local computer. It can be opened in a text editor.

Creating administrator accounts with restricted access

When you create an administrator account in FortiManager, by default the account grants access to all ADOMs and all policy packages. However, you can configure administrator accounts with restricted access to the following items:

- ADOMs - see [Restricting administrator access to ADOMs on page 29](#)
- Device groups - see [Restricting administrator access to device groups on page 31](#)
- Policy packages - see [Restricting administrator access to policy packages on page 32](#)

Restricting administrator access to ADOMs


When you create an administrator account, you can specify which ADOMs that users of the account can access. This topic describes the different methods you can use to restrict access.

To create an administrator account and specify ADOM access:

1. Go to *System Settings > Admin > Administrators*.
2. Click *Create New*.
3. Beside *Administrative Domain*, click *Specify*, and then select the ADOMs that the administrator account can access.

Create New Administrator

User Name: ADOM-admin

Avatar:  +Add Photo -Remove Photo

Description:

Admin Type: LOCAL

New Password:

Confirm Password:

Admin Profile: Restricted_User

Administrative Domain: All ADOMs All ADOMs except specified

Policy Package Access: All Packages Specify

JSON API Access: None

Theme Mode: Use Global Theme Use Own Theme

Trusted Hosts:

OK

Select Entries (Total: 20)

- ☐ Chassis
- ☐ FortiAnalyzer
- ☐ FortiAuthenticator
- ☐ FortiCache
- ☐ FortiCarrier
- ☐ FortiClient
- ☐ FortiDDoS
- ☐ FortiDeceptor
- ☐ FortiFirewall
- ☐ FortiMail
- ☐ FortiManager
- ☐ FortiNAC

OK Cancel

For example, select only the *root* and 56 ADOMs.

Create New Administrator

User Name

ADOM-admin

Avatar

A

+ Add Photo

- Remove Photo

Description

Admin Type

LOCAL

New Password

Confirm Password

Admin Profile

Restricted_User

Administrative Domain

All ADOMs

All ADOMs except specified ones

Specify

root

56

2 Entries Selected

Policy Package Access

All Packages

Specify

JSON API Access

None

OK

Cancel

4. Set the remaining options, and click **OK**.

When the administrator logs in to FortiManager, they can only access the specified ADOMs. In this example, the specified ADOMs are *root* and *56*.

Select an ADOM

root (5)

FortiGate 7.0

56

FortiGate 7.0

To create an administrator account and exclude access to specific ADOMs:

1. Go to *System Settings > Admin > Administrators*.
2. Click *Create New*.
3. Beside *Administrative Domain*, click *All ADOMs except specified ones*, and then select the ADOMs that you do not want the administrator account to access.
In this example, the *root* and *56* ADOMs are excluded from access.

Edit Administrator

User Name: ADOM-admin

Avatar: +Add Photo -Remove Photo

Description:

Admin Type: LOCAL

Admin Profile: Restricted_User

Administrative Domain: All ADOMs All ADOMs except specified ones Specify

Policy Package Access: All Packages Specify

JSON API Access: None

Theme Mode: Use Global Theme Use Own Theme

Trusted Hosts: ☐

OK Cancel

4. Set the remaining options, and click **OK**.

When the administrator logs in to FortiManager, they can access all ADOMs except for the ones specified. In this example, they can access all ADOMs except *root* and *56*.

Select an ADOM

Production FortiGate 6.4 Test FortiGate 7.0

Restricting administrator access to device groups

On the *Device Manager* pane, you can create device groups and add devices to the different groups. If you are using ADOMs, select the ADOM, and then create the device group.

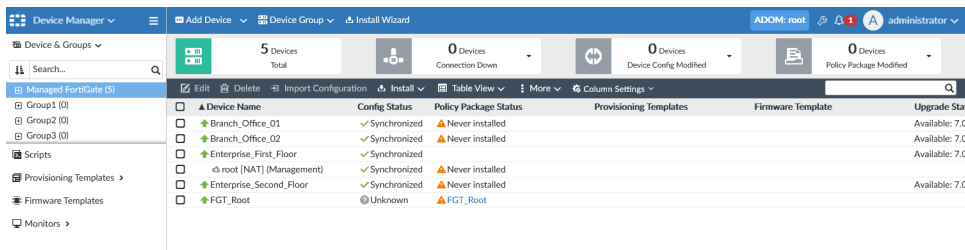
When you create an administrator account, you can specify which ADOMs the account can access, and which device groups can be accessed in those ADOMs.

This topic describes how to create a device group and how to restrict administrator access to device groups.

To create a device group:

1. Go to *Device Manager > Device & Groups*.
2. If you are using ADOMs, select the ADOM that you are creating a device group in. Otherwise skip this step.
3. In the *Device Group* dropdown menu, click *Create New Group*.
4. Enter a name for the group and add devices to it, then click **OK**.

In this example, the root ADOM contains *group1*, *group2*, and *group3*.



To specify admin access to device groups:

1. Go to *System Settings > Admin > Administrators*.
2. Click *Create New*.
3. Beside *Administrative Domain*, click *Specify*.
4. Select the ADOM that contains the device group. Select only one ADOM.
5. Select *Specify Device Group to Access*, and then select the device group.
In this example, *group1* is specified.

Create New Administrator

User Name: Devicegrp-admin

Avatar: Add Photo Remove Photo

Description:

Admin Type: LOCAL

New Password:

Confirm Password:

Admin Profile: Restricted_User

Administrative Domain: All ADOMs | All ADOMs except specified ones Specify

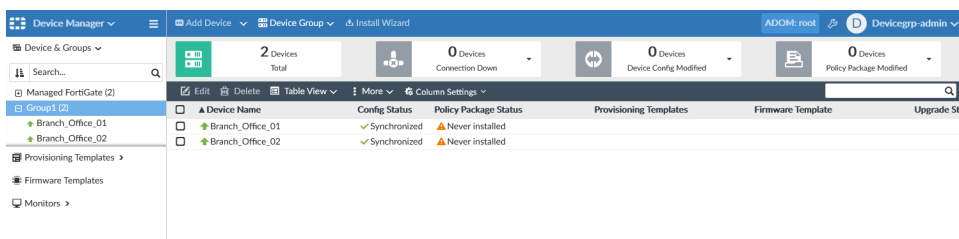
Specify Device Group to Access: ☒ Group1

Policy Package Access: All Packages Specify

OK Cancel

6. Click *OK*.

When the administrator logs in to FortiManager, they can only access the specified device group on the *Device Manager* pane. In this example, they can only access *group1*.



Restricting administrator access to policy packages

When you create an administrator account, you can specify which policy packages that administrator can access.

To specify admin access to policy packages:

1. Go to *System Settings > Admin > Administrators*.
2. Click *Create New*.

3. Beside *Policy Package Access*, click *Specify*, and specify which policy packages can be accessed. In the following example, administrators can access the *root* and *60* policy packages.

The screenshot shows the 'New Administrator' configuration window in FortiManager. The left sidebar is expanded to 'System Settings' > 'Administrators'. The main form contains the following fields and values:

- User Name: Package-admin
- Avatar: P (with '+ Change Photo' and '- Remove Photo' buttons)
- Comments: (empty text box, 0/127 characters)
- Admin Type: LOCAL (dropdown menu)
- New Password: (empty text box with eye icon)
- Confirm Password: (empty text box with eye icon)
- Admin Profile: Restricted_User (dropdown menu)
- Administrative Domain: All ADOMs (selected), All ADOMs except specified ones, Specify
- Policy Package Access: All Packages, Specify (selected)
- Trusted Hosts: OFF (checkbox)
- Meta Fields: >

At the bottom of the form, there are two buttons: 'OK' (blue) and 'Cancel' (orange). The 'Specify' button for 'Policy Package Access' is highlighted, and the selected packages are 'root:default' and '60:default'.

4. Set the remaining options, and click *OK*.
When the administrator logs in to FortiManager, they can only access the specified policy packages. In this example, the specified policy packages are *root:default* and *60:default*.

Others

This section contains the following topics:

- [Managing FortiAnalyzer from FortiManager on page 34](#)
- [Creating a third party blocklist provider workflow on page 42](#)

Managing FortiAnalyzer from FortiManager

This section contains the following topics:

- [Adding FortiAnalyzer to FortiManager on page 34](#)
- [Viewing managed FortiAnalyzer behavior on page 38](#)
- [Centrally configuring FortiGate to send logs to managed FortiAnalyzer on page 39](#)
- [Viewing logs and reports for managed FortiAnalyzer units on page 39](#)
- [Managing multiple FortiAnalyzer units on page 40](#)
- [Troubleshooting managed FortiAnalyzer units on page 41](#)

Adding FortiAnalyzer to FortiManager

You can add a FortiAnalyzer unit to FortiManager and use FortiManager to manage FortiAnalyzer, but you must add the FortiAnalyzer unit to an ADOM used for central management, which is similar to adding FortiGate units to FortiManager for central management.

You can use the following methods to add FortiAnalyzer units to FortiManager:

- In FortiManager, use the *Add FortiAnalyzer* wizard in the *Device Manager* pane.
- In FortiAnalyzer, enable central management, and then go to FortiManager to authorize the device for central management.

This topic includes the following sections:

- [Preparing to add FortiAnalyzer to FortiManager on page 34](#)
- [Using the wizard to add FortiAnalyzer to FortiManager on page 35](#)
- [Additional information on page 36](#)

Preparing to add FortiAnalyzer to FortiManager

When using FortiManager to manage FortiAnalyzer, it is recommended to use a FortiAnalyzer unit with factory settings or a FortiAnalyzer unit that has been reset to the factory settings (`factory-reset`). A FortiAnalyzer unit with factory settings helps avoid conflicts when FortiManager synchronizes the device database to FortiAnalyzer.

To prepare FortiAnalyzer for management by FortiManager:

1. On the FortiAnalyzer unit, enable fgfm access on the interface used to connect to FortiManager.

```
config system interface
edit "port1"
set ip 10.3.121.142 255.255.0.0
set allowaccess fgfm
next
end
```
2. Create an ADOM with the same name as the ADOM in FortiManager, such as *manage_remote_faz*.
FortiAnalyzer and FortiManager must have an ADOM of the same name. When you add FortiAnalyzer to FortiManager, add it to the ADOM of the same name.
3. Set storage settings for the ADOM.

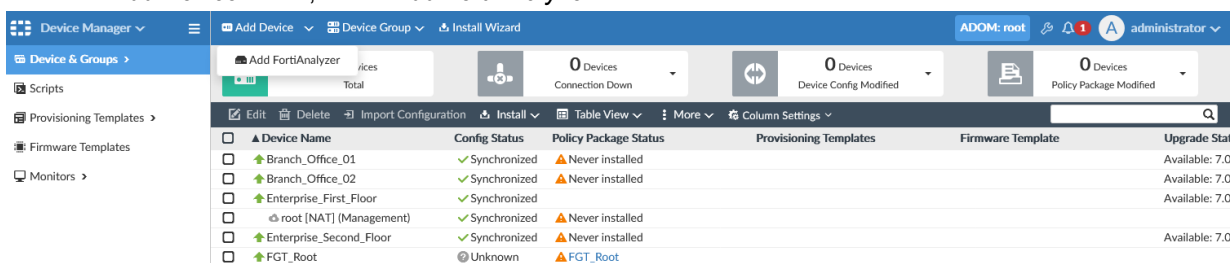
Using the wizard to add FortiAnalyzer to FortiManager

This section describes how to use the *Add FortiAnalyzer* wizard to add FortiAnalyzer to FortiManager.

To add FortiAnalyzer to FortiManager:

1. On FortiManager, ensure that FortiAnalyzer Features are disabled.
 - a. Go to *System Settings > Dashboard*.
 - b. In the *System Information* widget, ensure that *FortiAnalyzer Features* are toggled *Off*.
2. Ensure that the ADOM mode is set to normal by using the following CLI command:

```
config system global
set adom-mode normal
end
```
3. Go to *Device Manager*, and select a central management ADOM, such as *manage_remote_faz*.
The FortiAnalyzer unit should contain an ADOM of the same name. In this example, both FortiAnalyzer and FortiManager have an ADOM named *manage_remote_faz*.
4. On the *Device & Groups* tab, add the FortiAnalyzer unit.
 - a. From the *Add Device* menu, select *Add FortiAnalyzer*.



The *Add FortiAnalyzer* wizard is displayed.

- b. Type the FortiAnalyzer IP address, username, password, and click *Next*.

Add FortiAnalyzer

Discover
Device will be probed using a provided IP address and credentials to determine model type and other important information.

IP: 10.3.121.142

Username: root

Password: [Masked]

Next Cancel

After FortiManager discovers the device, device information is displayed.

Add FortiAnalyzer

The following information has been discovered from the device:

IP Address	10.3.121.142
Host Name	FAZ1000E
SN	FG14E2B1A000004
Model	FortiAnalyzer-1000E
Firmware Version	6.0.4 build292 (GA)
HA Status	Standalone
Administrator	Pat

Please input the following information to complete addition of the device:

Name:

Description:

- c. Click **Next** to continue.

Add FortiAnalyzer

Status: Comparing ADOM and devices on both sides...

FortiManager automatically compares ADOMs and devices on both FortiAnalyzer and FortiManager and provides the comparison and verification results.

Add FortiAnalyzer

Status: Verifying managed/logging devices on both sides...

Status	Device Name	Platform
FortiManager Only	FGVMD2000008807	FortiGate-VN64
FortiManager Only	FGVMD2000008808	FortiGate-VN64
FortiManager Only	EQH	FortiGate-VN64
FortiManager Only	Central	FortiGate-VN64
FortiManager Only	NAM	FortiGate-VN64
FortiManager Only	FGVMD2010100073	FortiGate-VN64

- d. Click **Synchronize ADOM and Devices** to continue.

Devices are synchronized between FortiAnalyzer and FortiManager, and FortiAnalyzer is added to FortiManager. The synchronized devices are added to FortiAnalyzer as logging-mode FortiGates.

Add FortiAnalyzer

Status: FortiAnalyzer Added Successfully

FortiAnalyzer is added to FortiManager.

- e. Click **Finish**.

5. Go to **Device Manager > Device & Groups** to view FortiAnalyzer in the *Managed FortiAnalyzer* group.

Device Name	IP Address	Platform	Description
FAZ1000E	10.3.121.142	FortiAnalyzer-1000E	

Additional information

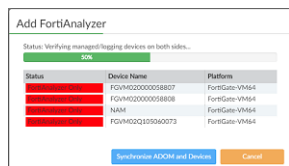
This section describes some of the other scenarios you might encounter when adding FortiAnalyzer units to FortiManager.

Missing ADOM

If the current ADOM in FortiManager does not exist on FortiAnalyzer, FortiManager automatically creates an ADOM with same name and version on FortiAnalyzer before starting to synchronize the device list.

Unknown or mismatched FortiGate devices

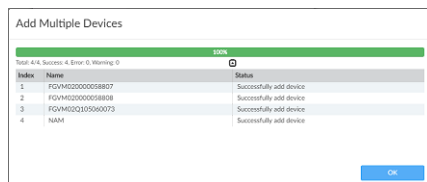
If FortiAnalyzer is receiving logs from FortiGate devices that do not exist on FortiManager, FortiManager identifies the devices.



FortiManager automatically attempts to discover the FortiGates.

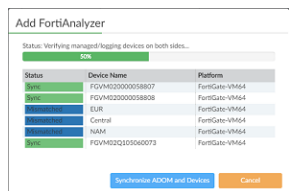


FortiManager can add the FortiGates and retrieve configurations for the FortiGates when adding the FortiAnalyzer unit.

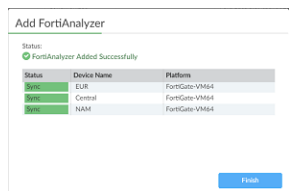


If one device fails to add or retrieve, FortiManager fails to add FortiAnalyzer.

If the same FortiGate device exists on both FortiManager and FortiAnalyzer, but with differences, FortiManager considers the device to be *Mismatched*.



FortiManager tries to synchronize the device settings to FortiAnalyzer.



If any errors occur during the synchronization step, FortiManager fails to add FortiAnalyzer.

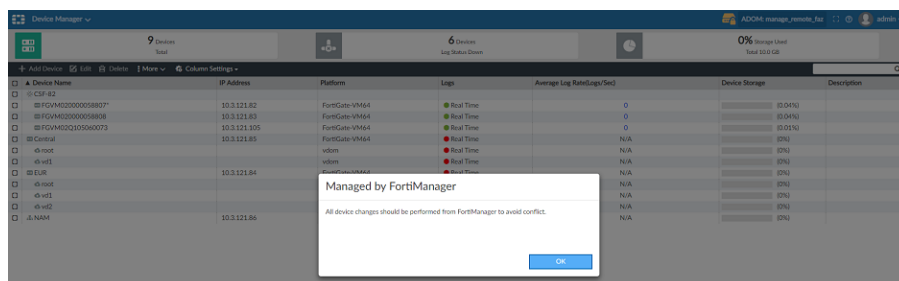
Viewing managed FortiAnalyzer behavior

After FortiManager manages the ADOM with FortiAnalyzer in it, you should use FortiManager to perform changes on all devices in the ADOM. This topic describes the behavior you will view in the GUI for a FortiAnalyzer unit that is managed by FortiManager.

To view managed FortiAnalyzer behavior:

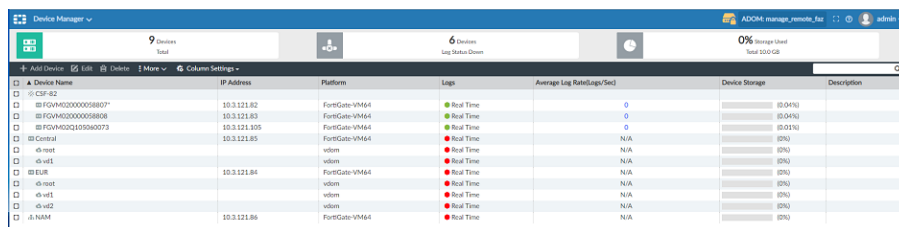
1. Log in to the FortiAnalyzer unit.
2. Go to the *Device Manager* pane.

The *Managed by FortiManager* message is displayed.



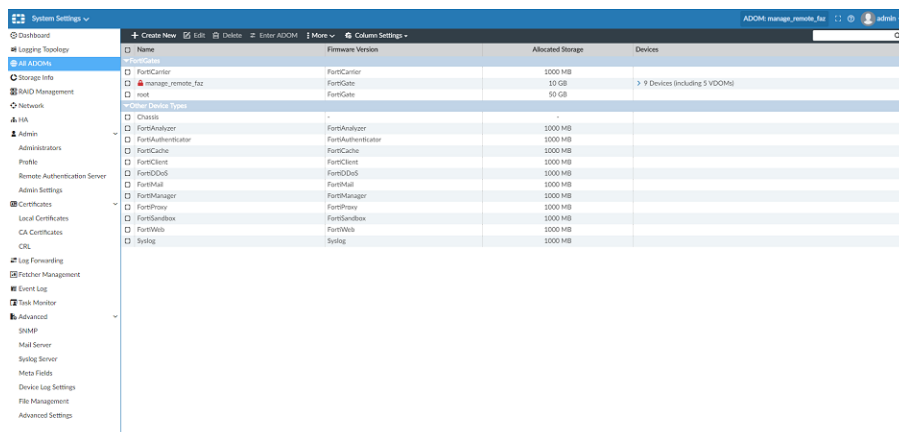
3. Click *OK*.

Notice the *Lock* icon displayed on top bar, and notice that the *Add Device*, *Edit*, and *Delete* buttons are unavailable.



4. Go to *System Settings > All ADOMs*.

Notice the lock icon beside the ADOM that is managed by FortiManager. You can no longer edit devices in the ADOM.

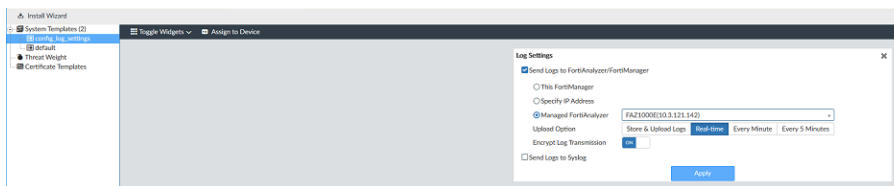


Centrally configuring FortiGate to send logs to managed FortiAnalyzer

After adding FortiAnalyzer to FortiManager, the device list is also synchronized to FortiAnalyzer. To make these FortiGate devices send log to FortiAnalyzer, you can use provisioning templates to centrally configure the log settings for FortiGates.

To centrally configure logging:

1. In FortiManager, go to *Device Manager > Provisioning templates*.
2. Create a new blank system template.
 - a. In the content pane, click *Create New*.
 - b. Type a name for the system template, and click *OK*.
The system template is created.
 - c. Select the system template, and click *Edit*.
The template opens for editing. You can enable the *Log Settings* widget by selecting it from the *Toggle Widgets* dropdown.



- d. In the *Log Settings* widget, select *Send Logs to FortiAnalyzer/FortiManager*.
 - e. Select *Managed FortiAnalyzer*, and select the unit from the drop-down list.
 - f. Click *Apply*.
3. Assign the system template to FortiGates.
4. Install the system template to FortiGates.

Viewing logs and reports for managed FortiAnalyzer units

After you add FortiAnalyzer to the ADOM in FortiManager, the following FortiAnalyzer panes are available in FortiManager:

- FortiView
- Log View
- FortiSoC
- Reports

All FortiAnalyzer functionality is available, except for the following:

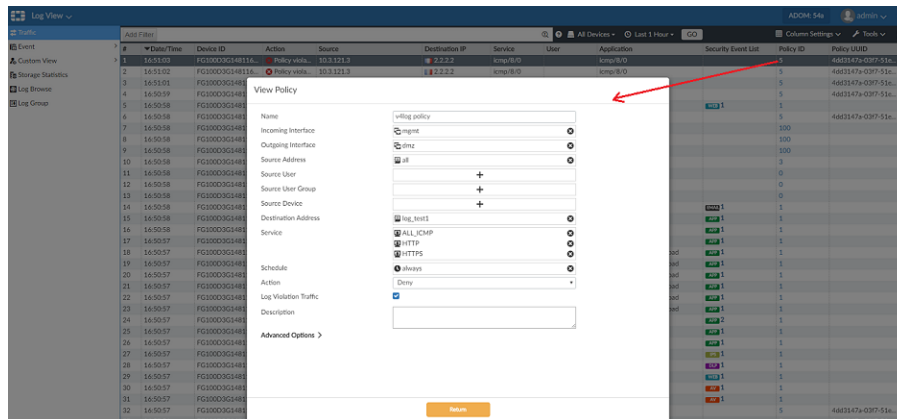
- Importing and exporting a report template
- Importing and exporting a chart
- Importing and downloading a log file

In FortiManager, when you create a report and run it, and the same report is generated in the managed FortiAnalyzer.

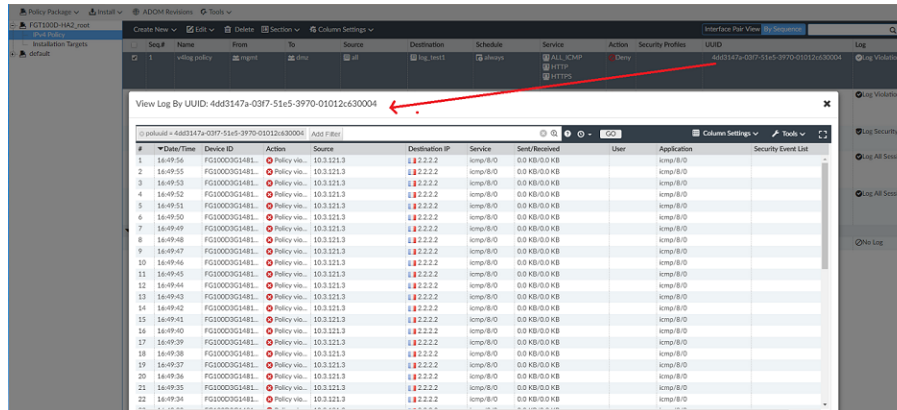
To view logs and reports:

1. On FortiManager, go to **Log View**.
You can view all logs received and stored on FortiAnalyzer.
2. Click the **Policy ID**.
The policy rule opens.

If the policy rule doesn't open, ensure that you have imported the policy rules to the ADOM.



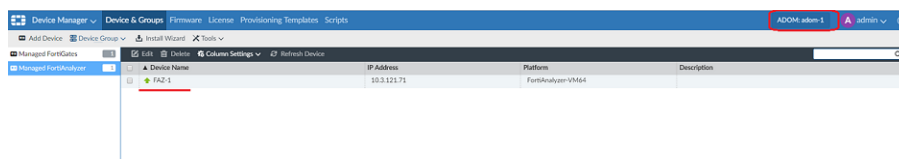
3. Go to **Policy & Objects > Policy Packages**, and right-click the policy UUID to search the related policy logs.



Managing multiple FortiAnalyzer units

FortiManager can manage multiple FortiAnalyzer units, but each FortiAnalyzer must be in its own ADOM. You cannot add a second FortiAnalyzer unit to an ADOM.

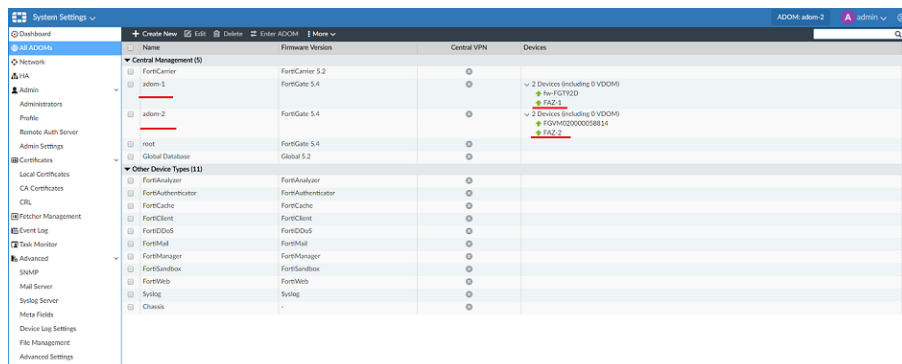
For example, FortiManager can contain the following ADOMs: *adom-1* and *adom-2*, and *adom-1* manages FAZ-1:



The other ADOM, *adom-2*, manages FAZ-2:



Following is another view of the ADOMs with FortiAnalyzer units:



Troubleshooting managed FortiAnalyzer units

This topic describes how to troubleshoot several situations.

Adding FortiAnalyzer failed

If adding FortiAnalyzer failed, enable the following debug command, which will provide error or information in a debug log, and then try adding FortiAnalyzer again.

```
diagnose debug application depmanager 255
diagnose debug enable
```

example: add_faz_dep_debug.txt

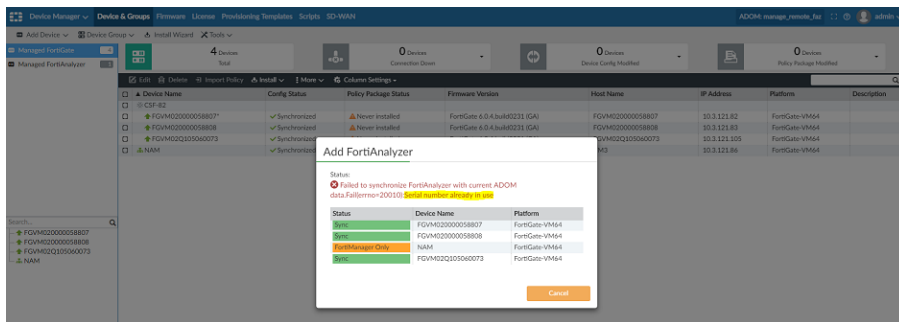
ADOM remains locked on FortiAnalyzer

When you delete FortiAnalyzer from FortiManager, the ADOM on FortiAnalyzer should be unlocked. If the ADOM remains locked, you can use the following command on the FortiAnalyzer unit to unlock the ADOM:

```
FAZ1000E # diag dvm adom unlock
adom ADOM name.
FAZ1000E # diag dvm adom unlock remote-faz
---Deleting DVM lock by remote FortiManager succeeded---
FAZ1000E#
```

Serial number already in use

The Alert console might display the *Serial number already in use* message. FortiManager might also display the *Serial number already in use* message after failing to add FortiAnalyzer.



You can use the `diagnose dvm device list` command on the FortiAnalyzer unit and on the FortiManager unit to see if the same FortiGate unit already exists on the FortiAnalyzer unit, but in different ADOM.

```

FGM000 Login: admin
Password:
FGM000 # diagnose dvm device list
... There are currently 4 device/adoms managed ...

TYPE      QID  SN      HA      IP      NAME      ADOM      IPS      FIRMWARE
mgmt/faz enabled 501  FQVM020000058807  10.3.121.82  FQVM020000058807  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dev: retrieved; com: up
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/faz enabled 513  FQVM020000058808  10.3.121.83  FQVM020000058808  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dev: retrieved; com: up
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/faz enabled 489  FQVM020105060073  10.3.121.105  FQVM020105060073  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dev: retrieved; com: up
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/faz enabled 476  FQVM020000058811  10.3.121.88  N/A      root      6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dev: retrieved; com: up
HA cluster member: FQVM020000058811 (master)
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]

... There are currently 0 FortiAP managed ...

... There are currently 0 FortiSwitch managed ...

... There are currently 0 FortiExtender managed ...

... End device list ...

FGM000 #

FGM1000 Login: admin
Password:
FGM1000 # diagnose dvm device list
... There are currently 4 device/adoms managed ...

TYPE      QID  SN      HA      IP      NAME      ADOM      IPS      FIRMWARE
mgmt/faz enabled 273  FQVM020000058807  10.3.121.82  FQVM020000058807  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dev: unknown; com: unknown
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/faz enabled 271  FQVM020000058808  10.3.121.83  FQVM020000058808  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dev: unknown; com: unknown
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/faz enabled 272  FQVM020105060073  10.3.121.105  FQVM020105060073  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dev: unknown; com: unknown
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/faz enabled 308  FQVM020000058811  10.3.121.88  N/A      root      6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dev: unknown; com: unknown
HA cluster member: FQVM020000058811 (master)
|- vdom:[1]root flags:0 adom:root pkg:[never-installed]

... There are currently 0 FortiAP managed ...

... There are currently 0 FortiSwitch managed ...

... There are currently 0 FortiExtender managed ...

... End device list ...

FGM1000 #
  
```

Compare the device list on FGM and FAZ. Both FGM and FAZ have device "FQVM020000058811" but it is in different ADOM (on FGM it is in ADOM "manage_remote_faz" on FAZ it is in ADOM "root"). That is why we saw the error "Failed to sync devdb to FAZ: Serial number already in use".

To solve the problem, manually move the device "FQVM020000058811" to ADOM "manage_remote_faz" on FAZ. You may need to rebuild the DB if want to view the old log after move the device.

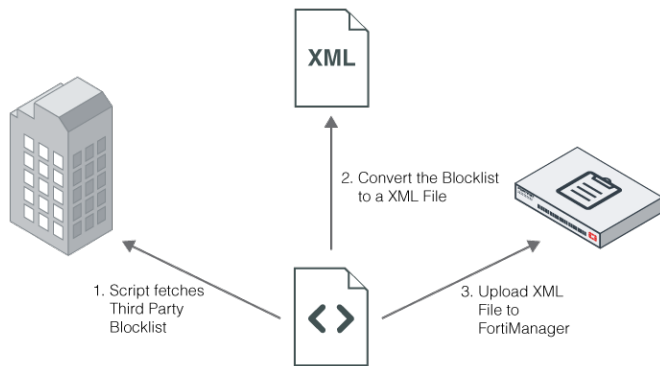
Creating a third party blocklist provider workflow

In this example, you will learn how to use your FortiManager to create a third party blocklist provider workflow.

Overview

You must create a script that will handle the entire workflow. Make sure the script can convert the third party blocklist into a FortiManager XML file.

From an external server, you must schedule the periodic execution of that script. Using the communication tools provided by the third party blocklist provider, the script will fetch the blocklist from the third party.



To create a script to handle a third party blocklist provider workflow:

1. Convert the blocklist to a FortiManager XML file:

The script will convert the blocklist to a FortiManager XML file. This XML file allows you to assign a category to each URL in the list, in addition to a default category. The default category is used as the return value when there is no match.

Example of the FortiManager XML file format:

```
<custom_url_list version="1.0">
  <head>
    <default_cate>142</default_cate>
    <description>the description</description>
  </head>
  <body>
    <url_entry>
      <url>http://www.url-0000001.com</url>
      <cate>79</cate>
    </url_entry>
    <url_entry>
      <url>http://www.url-0000001.com</url>
      <cate>28</cate>
    </url_entry>
  </body>
</custom_url_list>
```

The category value in `<cate></cate>` could be either a normal web filter category or a local category.

2. Upload the XML file into FortiManager:

The script uses SSH to connect to FortiManager and upload the XML file.

CLI command:

```
execute fmupdate <ftp|scp|tftp> import custom-url <xml filename> <ftp|scp|tftp details>
```

Example:

```
# execute fmupdate scp import custom-url 20M-custom-url.xml 000.000.000.000 00
  tmp/FORTIGUARD my_login my_password
```

This operation will replace the current <custom-url> package!

Do you want to continue? (y/n)y

Start getting file from remote SCP Host...

SCP transfer successful.

Packing installation is in process...This could take some time.

lccclient command result:Response=202|

Update successfully

In this example, FortiManager will upload the file from the following file:

```
scp://my_login:my_password@000.000.000.000:00/temp/FORTIGUARD/20M-custom-url.xml
```

3. Configure FortiManager to only use its local FortiGuard database or local blocklist database:

a. Select one of the following:

- Local FortiGuard database
- Local blocklist database
- Or both

```
config fmupdate custom-url-list
  set db_selection <fortiguard-db|custom-url|both>
end
```

4. Test custom URLs managed by FortiManager:

a. Use the CLI in FortiManager to send categorization requests for custom URLs managed by FortiManager.

Example of the CLI command set:

```
# diagnose fmupdate fgd-url-rating FGT SN 1 www.foo.com
url rating flags: 0x2 (2:EXACT_MATCH, 1:PREFIX_MATCH)
rates according to url: 0x37 0x00 0x00 0x00
rates according to ip: 0x00 0x00 0x00 0x00
num_dots:-1, num_slash:-1
database version: 16.45562
0 ms
```

The *FGT SN* can be any FortiGate SN.

The returned category is in a hexadecimal output: *0x37*.

In decimal format, the category is *56* or *Web Hosting*.



The memory capacity of the unit determines the number of URLs FortiManager can manage.

5. Specify FortiManager as the FortiGuard server in FortiGate

a. Go to your FortiGate CLI console and execute the following commands:

```
config system centralmanagement
  set type fortimanager
  set {<IP_address> | <FQDN_address>}
  config serverlist
    edit 1
      set servertype
      update rating
      set serveraddress {<IP_address> | <FQDN_address>}
    next
  end
  set includedefaultservers disable
end
```



For further FortiManager information, refer to the [FortiManager Administration Guides](#) available on the [Fortinet Document Library](#).



www.fortinet.com

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.