



# FortiManager - Cookbook

Version 6.2

**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://fortiguard.com/>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



July 29, 2020

FortiManager 6.2 Cookbook

02-620-594254-20200729

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>SD-WAN</b>	<b>6</b>
SD-WAN/ADVPN configuration	6
Adding FortiGate devices to FortiManager	7
Creating the overlay configuration	9
Configuring dynamic routing	22
Configuring SD-WAN	27
Using Intelligent Application Steering and Link Fail-over	32
<b>Device Manager</b>	<b>34</b>
Exporting a policy package from one FortiManager to another	34
<b>VPN Manager</b>	<b>36</b>
Configuring a full mesh VPN topology within a VPN console	36
<b>FortiSwitch Manager</b>	<b>42</b>
Using central management	42
Enabling FortiSwitch central management	42
Importing and editing FortiSwitch templates	43
Creating FortiSwitch templates	44
Assigning templates to FortiSwitch devices	47
Using per-device management	47
Enabling FortiSwitch per-device management	48
Configuring FortiSwitch profiles	48
Configuring FortiSwitch ports	49
Installing changes to FortiSwitch devices	50
Upgrading FortiSwitch firmware	52
Using zero touch deployment for FortiSwitch	53
<b>System Settings</b>	<b>55</b>
Configuring and debugging FortiManager HA clusters	55
Configuring the primary FortiManager unit in an HA cluster	55
Configuring backup FortiManager units in an HA cluster	55
Generating and downloading HA debug logs	56
Creating administrator accounts with restricted access	56
Restricting administrator access to ADOMs	57
Restricting administrator access to device groups	59
Restricting administrator access to policy packages	61
<b>Others</b>	<b>62</b>
Managing FortiAnalyzer from FortiManager	62
Adding FortiAnalyzer to FortiManager	62
Viewing managed FortiAnalyzer behavior	66
Centrally configuring FortiGate to send logs to managed FortiAnalyzer	67
Viewing logs and reports for managed FortiAnalyzer units	67
Managing multiple FortiAnalyzer units	69
Troubleshooting managed FortiAnalyzer units	69
Creating a third party blocklist provider workflow	71

---

Overview .....71

## Change Log

Date	Change Description
2019-11-18	Initial release.
2019-12-03	Added <a href="#">FortiSwitch Manager</a> on page 42.
2020-07-29	Added <a href="#">SD-WAN</a> on page 6.

# SD-WAN

This chapter contains the following topics:

- [SD-WAN/ADVPN configuration on page 6](#)

## SD-WAN/ADVPN configuration

This section provides an understanding of the Fortinet Secure SD-WAN configuration.

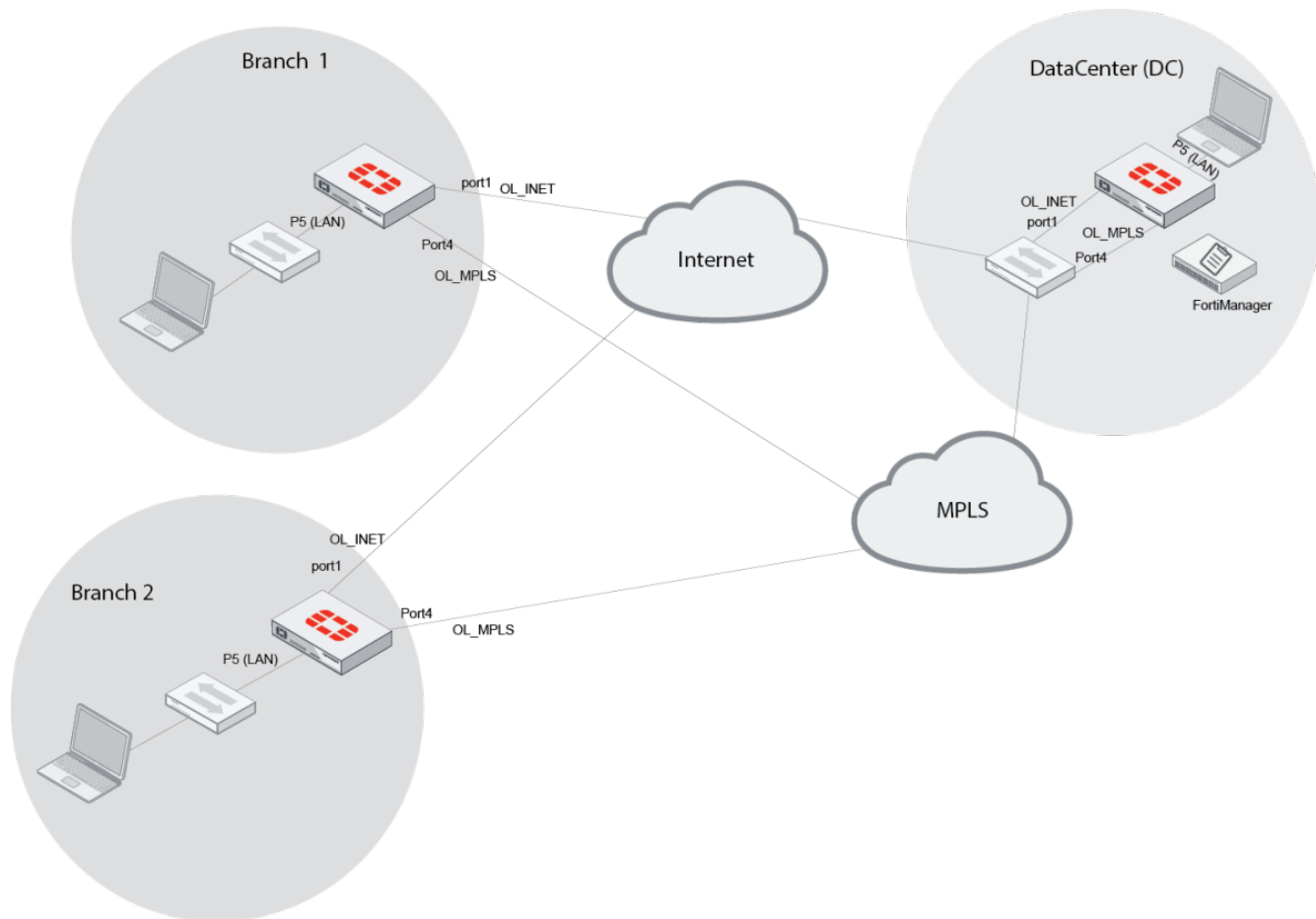
The main objective of this section is to provide details on how to configure SD-WAN to cover the following use cases:

- ADVPN
- QoS

The following topics consider one FortiGate as datacenter and two FortiGates as branch offices. All the FortGates have two links:

- MPLS: To simulate a private connection from branch to datacenter
- INET: To simulate the local internet breakout

From the branches you will create an IPsec tunnel to the FortiGate datacenter for both the INET and MPLS links.



**To configure a SDWAN/ADVPN deployment:**

1. [Add the devices to FortiManager.](#)
2. [Create the overlay configuration.](#)
3. [Configure the dynamic routes.](#)
4. [Enable central management.](#)
5. [Create SD-WAN rules for Intelligent Application Steering and Link Fail-over.](#)

## Adding FortiGate devices to FortiManager

Add the datacenter FortiGate and two branch office FortiGates to FortiManager.

**To add a device with Discover mode:**

1. Go to *Device Manager > Device & Groups*.
2. In the toolbar, click *Add Device*.  
The *Add Device* window opens.
3. Select *Discover*, and then follow the prompts to configure the device settings.

For information about adding devices, go to the [FortiManager Document Library](#) > [FortiManager Administration Guide](#) > [Firewall Devices](#) > [Adding Devices](#).

### To retrieve the configuration:

1. Go to *Device Manager* > *Device & Groups*, and select a device group.
2. In the tree menu, select a device.  
The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*.
5. In the *Configuration Revision History* dialog box, click *Retrieve Config*.  
View the current configuration running on the device. If there are differences between the configuration file on the device and the configuration file in the repository, a new revision is created and assigned a new ID number.

For information about retrieving configuration, go to the [FortiManager Document Library](#) > [FortiManager Administration Guide](#) > [Firewall Devices](#) > [Managing device configurations](#) > [Managing configuration history](#).

### To synch the devices:

1. Go to *Device Manager* > *Device & Groups*.
2. In the device pane, right-click a device, and select *Import Policy* to launch the *Import Policy* wizard.  
This wizard allows you to import interface maps, policy databases, and objects. Default or per-device mapping must exist or the installation will fail.



After initially importing policies from the device, make all changes related to policies and objects in the *Policy & Objects* module in the FortiManager.

Making changes directly on the FortiGate device will require reimporting policies to resynchronize the policies and objects.

For information about importing policies, go to the [FortiManager Document Library](#) > [FortiManager Administration Guide](#) > [Firewall Devices](#) > [Adding devices](#) > [Import policy Wizard](#).

The screenshot shows the FortiManager Device Manager interface. The top navigation bar includes tabs for Device Manager, Device & Groups, Firmware, License, Provisioning Templates, Scripts, and SD-WAN. The main content area displays a table of managed devices. The table has columns for Device Name, Config Status, Policy Package Status, Firmware Version, and Host Name. The devices listed are DC5, root [NAT] (Management), FortiGate-VM64-154, and FortiGate-VM64-155. All devices show a 'Synchronized' status. A left sidebar shows a tree view of the device hierarchy, including DC5 (1), root, and the two FortiGate-VM64 devices.

Device Name	Config Status	Policy Package Status	Firmware Version	Host Name
DC5	✓ Synchronized		FortiGate 6.2.2.build1010 (GA)	FortiGate-VM64
root [NAT] (Management)	✓ Synchronized	✓ DC5_root	FortiGate 6.2.2.build1010 (GA)	FortiGate-VM64
FortiGate-VM64-154	✓ Synchronized	✓ SD-WAN-154	FortiGate 6.2.2.build1010 (GA)	FortiGate-VM64
FortiGate-VM64-155	✓ Synchronized	✓ SD-WAN-154	FortiGate 6.2.2.build1010 (GA)	FortiGate-VM64



## Creating the overlay configuration

Create dynamic interfaces to map port2, port3, port10, INET and MPLS of the three FortiGates.

**To create the overlay:**

1. [Configure the VPN Manager.](#)
2. [Map the underlay interfaces.](#)
3. [Create the policy packages.](#)
4. [Install the configurations and policies.](#)
5. [Configure the tunnel interfaces and dynamic mapping.](#)

## Adding the dynamic interfaces to map underlay interfaces

Create dynamic interfaces to map the overlay with the underlay topologies. Interface mapping allows the new interface to be used when creating policies.

Create the following dynamic interfaces:

- OL\_INET\_0
- OL\_MPLS\_0
- Port10
- Port2
- Port3

**To create a dynamic interface:**

1. Go to *Policy & Objects > Object Configurations*.
2. In the tree menu, select *Zone/Interface > Interface*.
3. In the toolbar, click *Create New > Dynamic interface*.
4. Enter a name and description for the dynamic interface.
5. Enable *Per-Device Mapping*.
6. Click *Create New*. The *Per-Device Mapping* dialog box is displayed.
  - a. Select a *Mapped Device* from the dropdown.
  - b. Select a *Device Interface* from the dropdown.
  - c. Repeat these steps for all of the hub and branch devices.
7. Click *OK* to create the new dynamic interface object.

The mapped interface can now be used when creating policies.

Policy & Objects ▾ Policy Packages Object Configurations ADOM: SD-WAN-622						
ADOM Revisions Tools ▾						
Zone/Interface ▾						
Interface						
Firewall Objects ▾						
Security Profiles ▾						
Fabric Connectors ▾						
User & Device ▾						
WAN Optimize ▾						
Dynamic Object ▾						
Advanced ▾						
CLI Only Objects ▾						
<div> <div>+</div> <div>Create New ▾</div> <div>Edit</div> <div>Delete</div> <div>Column Settings ▾</div> <div>More ▾</div> </div> <div>View ▾</div> <div></div>						
Interface		Default Mapping	Per-Device Mapping	Description	Created Time	Last Modified
Interface (18)						
<input type="checkbox"/>	any		> 0 out of 3			
<input type="checkbox"/>	sslvpn_tun_intf		> 0 out of 3			
<input type="checkbox"/>	sd-wan		> 0 out of 3			
<input checked="" type="checkbox"/>	OL_INET_0		✓ 3 out of 3 DC5 (root): OL_INET_0 FortiGate-VM64-154 (r FortiGate-VM64-155 (r		2020-01-02 14:49:29	admin/2020-01-02 14
<input checked="" type="checkbox"/>	OL_MPLS_0		✓ 3 out of 3 DC5 (root): OL_MPLS_0 FortiGate-VM64-154 (r FortiGate-VM64-155 (r		2020-01-02 14:49:58	admin/2020-01-02 14
<input type="checkbox"/>	loopback		> 0 out of 3		2019-12-12 14:02:27	admin/2019-12-12 14
<input type="checkbox"/>	loopback1		> 1 out of 3		2019-11-13 11:00:02	admin/2019-11-13 11
<input type="checkbox"/>	port1		> 3 out of 3		2019-11-01 11:36:07	admin/2019-11-01 11
<input checked="" type="checkbox"/>	port10		✓ 3 out of 3 DC5 (root): port10 FortiGate-VM64-154 (r FortiGate-VM64-155 (r		2019-11-01 11:36:07	admin/2019-11-01 11
<input checked="" type="checkbox"/>	port2		✓ 3 out of 3 DC5 (root): port2 FortiGate-VM64-154 (r FortiGate-VM64-155 (r		2019-11-01 11:36:07	admin/2019-11-01 11
<input checked="" type="checkbox"/>	port3		✓ 3 out of 3 DC5 (root): port3 FortiGate-VM64-154 (r FortiGate-VM64-155 (r		2019-11-01 11:36:07	admin/2019-11-01 11
<input type="checkbox"/>	port4		> 3 out of 3		2019-11-01 11:36:07	admin/2019-11-01 11
<input type="checkbox"/>	port5		> 3 out of 3		2019-11-01 11:36:07	admin/2019-11-01 11
<input type="checkbox"/>	port6		> 3 out of 3		2019-11-01 11:36:07	admin/2019-11-01 11

## Configuring the VPN manager

Create two overlays, one for the internet connection and one for the MPLS network. This is to create two secure links to the datacenter and to implement SDWAN among those links.

VPN Manager ▾ IPsec VPN Monitor Map View SSL VPN ADOM: SD-WAN-622				
VPN Community ▾ Install Wizard				
All VPN Communities				
<div> <div>+</div> <div>Create New ▾</div> <div>Edit</div> <div>Delete</div> <div>Column Settings ▾</div> </div> <div></div>				
<input type="checkbox"/>	Name	Gateways	Authentication	Description
<input type="checkbox"/>	OL_INET	✓ 3 Gateways DC5 [root] FortiGate-VM64-154 [root] FortiGate-VM64-155 [root]	Pre-shared Key	
<input checked="" type="checkbox"/>	OL_MPLS	✓ 3 Gateways DC5 [root] FortiGate-VM64-154 [root] FortiGate-VM64-155 [root]	Pre-shared Key	

**To create a dial-up topology:**

1. Go to *VPN Manager > IPsec VPN*.
2. In the toolbar, click *Create New*. The *VPN Topology Setup Wizard* is displayed.
  - a. Enter a name for the topology, such as *OL\_INET* and *OL\_MPLS*.
  - b. In the *Choose VPM topology* section, select *Dial up*.
  - c. Click *Next*.
3. Complete the steps in the wizard, and click *OK*.
4. After you create the MPLS and INET overlays, select the topology and click *Edit*. Ensure *VPN Zone* is disabled.

**Edit VPN Community**

Name:

Description:

Topology: ☒ Dial up

Authentication: ☒ Pre-shared Key ☐ Certificates

☐ Generate (random)

☒ Specify:

**Encryption**

IKE Security (Phase 1) Properties

IKE Version:

#	Encryption	Authentication	
1	<input type="text" value="AES128"/>	<input type="text" value="SHA256"/>	+ <input type="button" value="X"/>
2	<input type="text" value="AES256"/>	<input type="text" value="SHA256"/>	+ <input type="button" value="X"/>

IPsec Security (Phase 2) Properties

#	Encryption	Authentication	
1	<input type="text" value="AES128"/>	<input type="text" value="SHA256"/>	+ <input type="button" value="X"/>
2	<input type="text" value="AES256"/>	<input type="text" value="SHA256"/>	+ <input type="button" value="X"/>

VPN Zone: ☐ OFF

**IKE Security Phase 1 Advanced Properties**

Diffie-Hellman Group(s):

<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input checked="" type="checkbox"/> 5	<input checked="" type="checkbox"/> 14	<input type="checkbox"/> 15	<input type="checkbox"/> 16
<input type="checkbox"/> 17	<input type="checkbox"/> 18	<input type="checkbox"/> 19	<input type="checkbox"/> 20	<input type="checkbox"/> 21	<input type="checkbox"/> 27
<input type="checkbox"/> 28	<input type="checkbox"/> 29	<input type="checkbox"/> 30	<input type="checkbox"/> 31	<input type="checkbox"/> 32	



Enabling *VPN Zone* and setting it to *Create Default Zones*, creates a dynamic interface by default.

SDWAN does not support dynamic interfaces.

For information about creating VPN communities, go to the [Fortinet Document Library > FortiManager Administration Guide > IPsec VPN Communities > Creating IPsec VPN communities](#).

**To add the branches:**

1. Go to *VPN Manager > IPsec VPN*.
2. In the tree menu, select one of the dial-up topologies you created.
3. In the toolbar, click *Create New > Managed Gateway*. The *VPN Gateway Setup Wizard<Name>* is displayed.
  - a. Select a *Protected Subnet*, and click *Next*.
  - b. Set the *Role* to *Spoke* and select a branch FortiGate from the dropdown, then click *Next*.
  - c. Proceed through the steps in the wizard, and then click *OK*.
4. After you complete the steps in the wizard, select a branch device, and click *Edit*.  
Configure the following settings for all of the branch devices:

text

text

Property	Setting
Enable IP Assignment	Toggle OFF.
Add Route	Toggle OFF.
DHCP	Toggle OFF.
Advanced Options	
net-device	Toggle OFF.
tunnel-search	Select <i>nexthop</i> from the dropdown.

5.

Edit VPN Gateway

Protected Subnet

all  
IP/Netmask:0.0.0.0/0.0.0.0

1 Entry Selected

Role

Hub

Spoke

Device

FGT-1

Default VPN Interface

port1

Local Gateway

0.0.0.0

Local ID

Routing

Manual (via Device Manager)

Automatic

XAUTH Type

Disable

Client

Enable IKE Configuration Method ("mode config")

OFF

Enable IP Assignment

OFF

Add Route

OFF

Advanced Options

banner

dns-mode

manual

domain

exchange-interface-ip

OFF

hub-public-ip

net-device

OFF

public-ip

route-overlap

spoke-zone

None

tunnel-search

nexthop

For information about creating gateways, go to the [Fortinet Document Library](#) > *FortiManager Administration Guide* > *VPN* > *IPSec VPN gateways* > *Creating managed gateways*.

**To create the hub:**

1. Go to *VPN Manager* > *IPsec VPN*.
2. In the tree menu, select one of the dial-up topologies you created.
3. In the toolbar, click *Create New* > *Managed Gateway*. The *VPN Gateway Setup Wizard*<Name> is displayed.
  - a. Select a *Protected Subnet*, and click *Next*.
  - b. Set the *Role* to *Hub* and select a FortiGate from the dropdown, then click *Next*.
  - c. Proceed through the steps in the wizard, and then click *OK*.
4. After you add the hub to both of the overlay communities, select the hub device and click *Edit*.  
Configure the following settings for both hub devices:

Property	Setting
Peer Type	Select <i>Accept any peer ID</i> from the dropdown.
Enable IKE configuration Method ("mode config")	Toggle <i>OFF</i> .
DHCP	Toggle <i>OFF</i> .
Advanced Options	
net-device	Toggle <i>OFF</i> .
tunnel-search	Select <i>nexthop</i> from the dropdown.

Protected Subnet

all

IP/Netmask:0.0.0.0/0.0.0.0

1 Entry Selected

Role

☒ Hub ☐ Spoke

Device

FGT-DC-5

Default VPN Interface

port1

Hub-to-Hub Interface

None

(Required for multiple Hubs)

Local Gateway

0.0.0.0

Local ID

Routing

☒ Manual (via Device Manager) ☐ Automatic

Summary Network(s)

Seq#	Network	Priority
1		1

Peer Type

☒ Accept any peer ID  
☐ Accept this peer ID  
☐ Accept a dialup group  
☐ Accept peer  
☐ Accept peer group

XAUTH Type

☒ Disable ☐ PAP Server ☐ CHAP Server ☐ AUTO Server

Enable IKE Configuration Method ("mode config")

OFF

DHCP Server

OFF

Default Gateway

0.0.0.0

DNS Service

☐ Use System DNS Setting ☒ Specify

DNS Server #1

0.0.0.0

DNS Server #2

0.0.0.0

DNS Server #3

0.0.0.0

Netmask

255.255.255.255

OK

Cancel

## Verifying ADVPN configuration in FortiGate

When configuring the VPN manager, take into account that the final outcome you want to have on the FortiGate is shown the configurations below.

The configuration will be available on the FortiGates only after they are installed from FortiManager. The installation is described later in the guide. These configurations are required for ADVPN to work. At this point you don't need to install the configurations on the FortiGates.

### Example configurations

```
FGT-1 # show vpn ipsec phase1-interface
config vpn ipsec phase1-interface
edit "OL_MPLS_0"
```

```
set interface "port4"
set ike-version 2
set keylife 28800
set peertype any
set net-device disable
set proposal aes128-sha256 aes256-sha256
set add-route disable
set auto-discovery-receiver enable
set tunnel-search nexthop
set remote-gw 172.16.2.5
set psksecret xxx
next
edit "OL_INET_0"
set interface "port1"
set ike-version 2
set keylife 28800
set peertype any
set net-device disable
set proposal aes128-sha256 aes256-sha256
set add-route disable
set auto-discovery-receiver enable
set tunnel-search nexthop
set remote-gw 100.64.1.5
set psksecret xxx
next
end
```

#### FGT-DC-5 # show vpn ipsec phasel-interface

```
config vpn ipsec phasel-interface
edit "OL_MPLS_0"
set type dynamic
set interface "port4"
set ike-version 2
set keylife 28800
set peertype any
set net-device disable
set proposal aes128-sha256 aes256-sha256
set add-route disable
set auto-discovery-sender enable
set tunnel-search nexthop
set psksecret xxx
next
edit "OL_INET_0"
set type dynamic
set interface "port1"
set ike-version 2
set keylife 28800
set peertype any
set net-device disable
set proposal aes128-sha256 aes256-sha256
set add-route disable
set auto-discovery-sender enable
set tunnel-search nexthop
set psksecret xxx
next
end
```

## Creating policy packages

Create the firewall policies to install on the FortiGates. You create two policy packages: one for the branches and one for the hub.

### To create a policy package:

1. Go to *Policy & Objects > Policy Packages*.
2. In the toolbar, click *Policy Package > New*.
3. Configure the policy package settings, then click *OK*.

For information about creating policy packages, go to the [FortiManager Document Library > FortiManager Administration Guide > Firewall Policy & Objects > Managing policy packages > Create new policy packages](#).

### To create a firewall policy:

1. Go to *Policy & Objects > Policy Packages*.
2. In the tree menu, select a policy package.
3. In the tree menu, select a policy package. click *Create New*. By default, policies will be added to the bottom of the list, but above the *Implicit* policy.
4. Configure the firewall policy settings, and click *OK*.

Create the following set of policies for the branches:

- Branch to overlay
- Overlay to branch

#	Name	From	To	Source	Destination	Schedule	Service	Users	Action
1		any	OL_INET_0 OL_MPLS_0 port2 port3	all	all	always	ALL		Accept
2	To-client	OL_INET_0 OL_MPLS_0 port2 port3	port10	all	all	always	ALL		Accept
Implicit (3-3 / Total: 1)									
3	Implicit Deny	any	any	all	all	always	ALL		Deny

Create the following set of policies for the hub:

- Overlay to hub
- Overlay to INET
- Branch to branch



#	Name	From	To	Source	Destination	Schedule	Service	Users	Action
1	Overlay to DC	OL_INET_0 OL_MPLS_0	port10	all	all	always	ALL		Accept
2	To Internet Traf	OL_INET_0 OL_MPLS_0	port1	all	all	always	ALL		Accept
3	allow_internet2	port2 port3	port10	all	all	always	ALL		Accept
4	ADVPN	OL_INET_0 OL_MPLS_0	OL_INET_0 OL_MPLS_0	all	all	always	ALL		Accept
▼ Implicit (5-5 / Total: 1)									
5	Implicit Deny	any	any	all	all	always	ALL		Deny

For information about creating firewall policies, go to the [FortiManager Document Library](#) > [FortiManager Administration Guide](#) > [Firewall Policy & Objects](#) > [Managing policies](#) > [Create new Firewall Policy](#).

## Installing policy packages

Install the policy packages on the hub and branch FortiGates.

### To install a policy package:

1. Go to *Policy & Objects* > *Policy Packages*.
2. In the toolbar, click *Install* > *Install Wizard*.
3. Follow the steps in the install wizard to install the policy package.

For information about installing policy packages, go to the [FortiManager Document Library](#) > [FortiManager Administration Guide](#) > [Firewall Policy & Objects](#) > [Managing policy packages](#) > [Install a policy package](#).



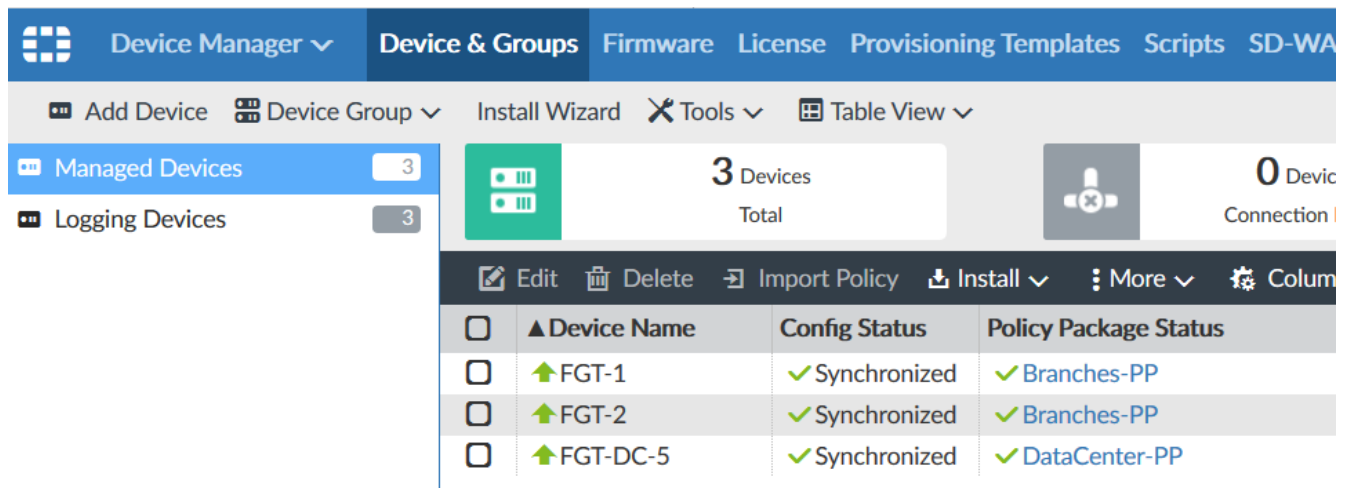
After the policies are installed on the devices, FortiManager may make the following modifications to the FortiGate configurations:

- The *tunnel-search* property will no longer be set to *nexthop* on the spokes.
- The *auto-discovery-sender* and *auto-discovery-receiver* properties will no longer be enabled on the hub and spokes

You can use the GUI or scripts to correct the configuration; however, you should first complete the following step, [Configuring tunnel interfaces and dynamic mapping on page 18](#)

### To verify the policy packages were installed in the GUI:

1. Go to *Device Manager* > *Device & Groups*.
2. In the tree menu, click *Managed Devices*. In the *Policy Package Status* column, a check mark appears next to the package you installed.



Device Name	Config Status	Policy Package Status
FGT-1	✓ Synchronized	✓ Branches-PP
FGT-2	✓ Synchronized	✓ Branches-PP
FGT-DC-5	✓ Synchronized	✓ DataCenter-PP

## Configuring tunnel interfaces and dynamic mapping

After the policy packages are installed on the FortiGates, ensure the tunnel interfaces for Port 2 and Port 3 are configured correctly.



After completing this task, you can fix the settings that were modified when [Installing policy packages on page 17](#) See [Fixing the settings in the policy package on page 20](#).

### To configure the tunnel interface address in the GUI:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, select the device you want to configure.
3. Hover over the *System* tab and select *Interface*.
4. Select the tunnel interface, and click *Edit*.
5. Enter the tunnel address in the *IP/Netmask* and *Remote/IP* fields.

The screenshot shows the FortiManager GUI with the 'Device & Groups' tab selected. The left sidebar shows a tree view with 'DC5 (1)' and 'root' under 'Managed Devices'. The main panel is titled 'Edit Interface' for 'FortiGate-VM64-154'. The configuration fields are as follows:

- Interface Name:** OL\_INET\_0
- Alias Name:** (empty)
- Type:** Tunnel
- Interface:** port2
- Role:** Undefined
- Addressing Mode:** Manual
- IP/Netmask:** 10.254.40.2/255.255.255.255
- Remote IP:** 10.254.40.1/255.255.255.0
- Shaping Profile:** OFF
- Restrict Access:**
  - Override Default MTU Value: OFF
  - Administrative Access:
    - ☐ CAPWAP
    - ☐ HTTP
    - ☐ Probe Response
    - ☐ SSH
    - ☐ FMG-Access
    - ☐ HTTPS
    - ☐ RADIUS Accounting
    - ☐ TELNET
    - ☐ FTM
    - ☒ PING
    - ☐ SNMP
    - ☐ FortiTelemetry
- DHCP Server:** OFF (Server, Relay)
- Security Mode:** None
- Device Management:**
  - Device Detection: OFF
  - Broadcast Discovery Messages: OFF
  - Explicit Web Proxy: OFF
  - Explicit FTP Proxy: OFF

Buttons at the bottom: OK, Cancel.

### To configure the branch devices in the CLI:

```
FGT1: config system interface
edit "OL_MPLS_0"
    set vdom "root"
    set ip 10.254.41.2 255.255.255.255
    set allowaccess ping
    set type tunnel
    set remote-ip 10.254.41.1 255.255.255.0
    set estimated-upstream-bandwidth 1500
    set estimated-downstream-bandwidth 500
    set snmp-index 113
    set interface "port3"
next
edit "OL_INET_0"
    set vdom "root"
    set ip 10.254.40.2 255.255.255.255
    set allowaccess ping
    set type tunnel
    set remote-ip 10.254.40.1 255.255.255.0
    set estimated-upstream-bandwidth 100
    set estimated-downstream-bandwidth 50
    set snmp-index 114
    set interface "port2"
next
end

FGT2: config system interface
```

```
edit "OL_MPLS_0"
set vdom "root"
set ip 10.254.41.3 255.255.255.255
set allowaccess ping
set type tunnel
set remote-ip 10.254.41.1 255.255.255.0
set estimated-upstream-bandwidth 1500
set estimated-downstream-bandwidth 500
set snmp-index 113
set interface "port3"
next
edit "OL_INET_0"
set vdom "root"
set ip 10.254.40.3 255.255.255.255
set allowaccess ping
set type tunnel
set remote-ip 10.254.40.1 255.255.255.0
set estimated-upstream-bandwidth 100
set estimated-downstream-bandwidth 50
set snmp-index 114
set interface "port2"
next
end
```

### To configure the hub device in the CLI:

```
FGTDC: config system interface
edit "OL_MPLS_0"
set vdom "root"
set ip 10.254.41.1 255.255.255.255
set allowaccess ping
set type tunnel
set remote-ip 10.254.41.254 255.255.255.0
set snmp-index 114
set interface "port3"
next
edit "OL_INET_0"
set vdom "root"
set ip 10.254.40.1 255.255.255.255
set allowaccess ping
set type tunnel
set remote-ip 10.254.40.254 255.255.255.0
set snmp-index 115
set interface "port2"
next
end
```

## Fixing the settings in the policy package

After you have verified the configurations in the tunnel interfaces and dynamic mapping, fix the settings that were modified when you installed the configurations and policies. After you have fixed the configurations, ensure the devices are *Up*.



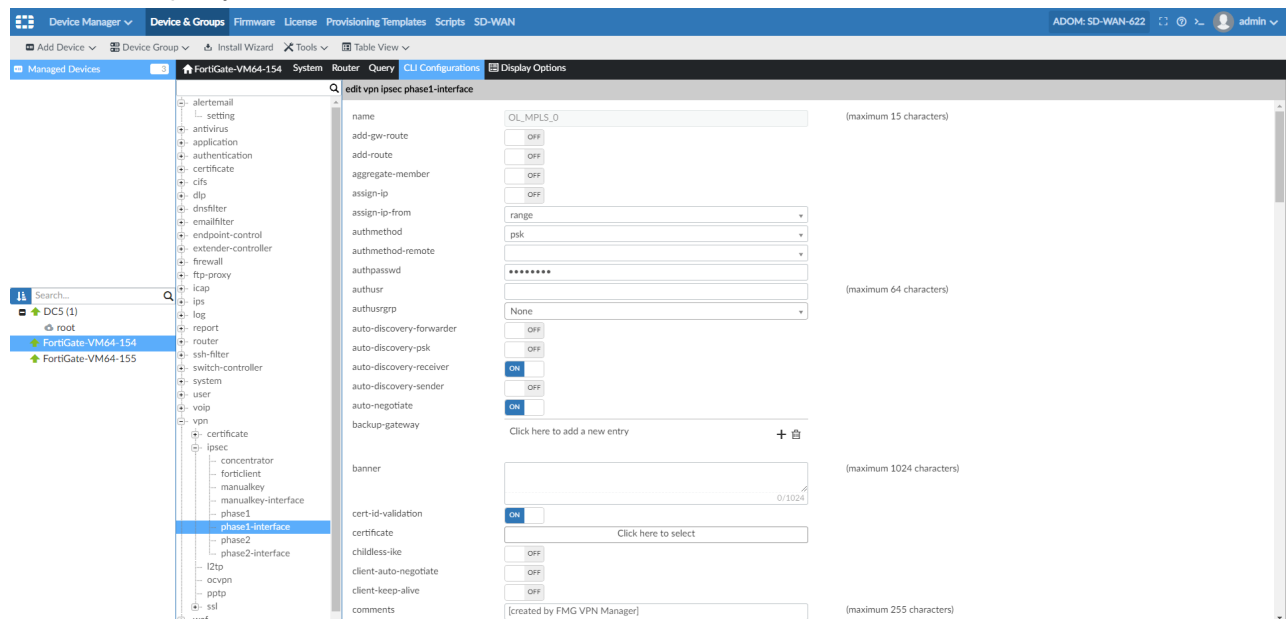
To complete this task, enable *CLI Configurations* in each device you want to configure.

### To enable CLI configurations:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, click *Managed Devices*, and then select a device from the list.
3. In the toolbar, click *Display Options*.
4. Click *Customize*.
5. Enable *CLI configurations*.

### To fix the configurations:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, click *Managed Devices*, and then select a device from the list.
3. In the toolbar, click *CLI configuration*.
4. Go to *vpn > ipsec > phase1-interface*.
5. Select a policy from the list, and click *Edit*.
  - a. On the hub device, enable *auto-discovery-forwarder* and *auto-discovery-sender*, then configure the required parameters.
  - b. On the branch devices, enable *auto-discovery-reciever*, and then configure the required parameters.
  - c. Install the policy on the hub and branches.



### To ensure the devices are up:

1. Go to *VPN Manager > Monitor*.
2. In the tree menu, click *All VPN Communities*.

3. In the *Status* column, ensure the device status is *Up*.

Status	Device	P1 Name	Type	Remote Gateway	Uptime	P2 Name	Incoming Data
Down	DC5[root]	OL_INET_0		0.0.0.0			382.0 MB
Up	DC5[root]	OL_INET_0_0	dialup	172.20.11.4	1d 3h 28m 08s	OL_INET_0_0	191.1 MB
Up	DC5[root]	OL_INET_0_1	dialup	172.20.11.5	1d 3h 28m 08s	OL_INET_0_0	190.9 MB
Down	DC5[root]	OL_MPLS_0		0.0.0.0			370.3 MB
Up	DC5[root]	OL_MPLS_0_0	dialup	172.20.12.4	1d 3h 28m 08s	OL_MPLS_0_0	185.4 MB
Up	DC5[root]	OL_MPLS_0_1	dialup	172.20.12.5	1d 3h 28m 08s	OL_MPLS_0_0	184.9 MB
Up	FortiGate-VM64-1	OL_INET_0	automatic	172.20.10.6	1d 3h 28m 06s	OL_INET_0_0	201.1 MB
Up	FortiGate-VM64-1	OL_MPLS_0	automatic	172.20.9.6	1d 3h 28m 06s	OL_MPLS_0_0	193.4 MB
Up	FortiGate-VM64-1	OL_INET_0	automatic	172.20.10.6	1d 3h 28m 06s	OL_INET_0_0	200.8 MB
Up	FortiGate-VM64-1	OL_MPLS_0	automatic	172.20.9.6	1d 3h 28m 06s	OL_MPLS_0_0	192.9 MB

## Configuring dynamic routing

BGP configurations are required to ensure ADVPN works properly. We recommend using FortiManager to create CLI templates with meta data fields or scripts to execute advanced BGP configurations on the branches and hubs.

**To configure dynamic routing:**

1. Configure the router-bgp in the branches.
2. Configure the router BGP on the hub.
3. Verify the BGP routes.
4. Configure the ADVPN policy route on the hub.

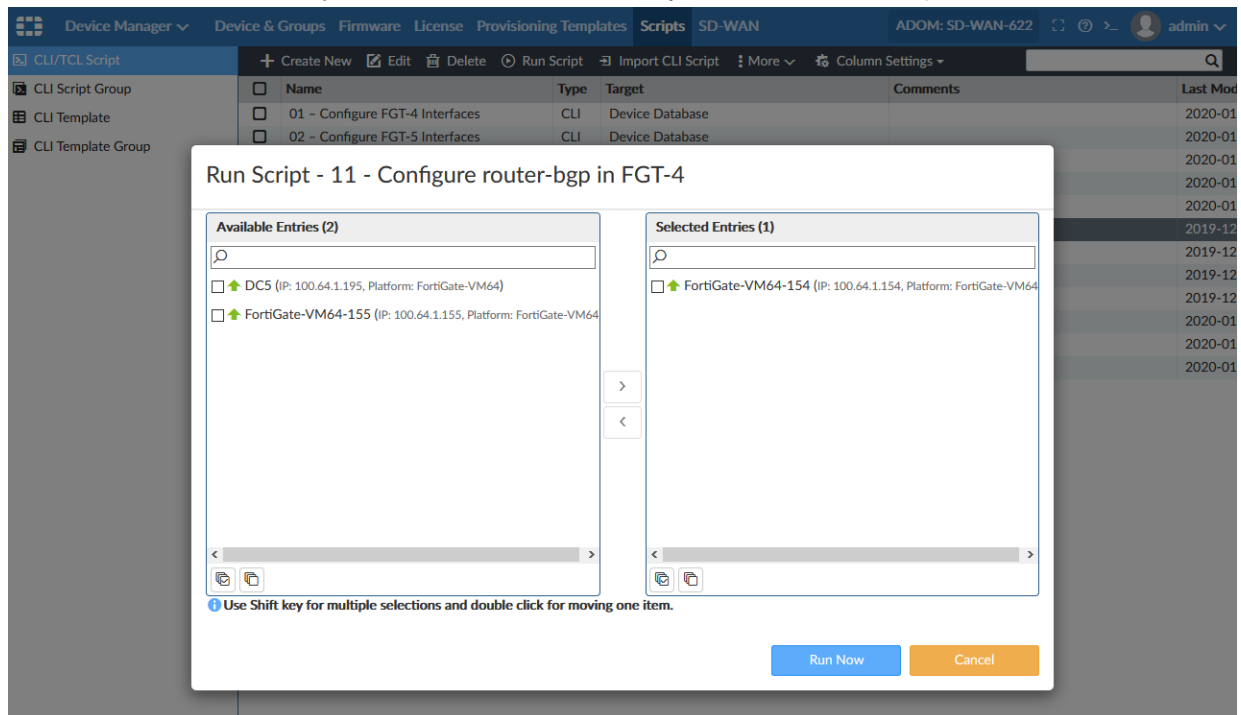
### Configuring the router-bgp on the branches

Use a script to configure the router-bgp in the branches.

**To create the CLI script:**

1. Go to *Device Manager > Scripts*.
2. In the toolbar, click *Create New*.
3. Enter the script details such as the *Script Name*, *Type*, and *Run script on*.
4. In the *Script details* field, paste the script:

5. In the toolbar, click *Run Script*, and then select the devices you want to run the script on. Click *Run Now*.



### Branch script example

```
config router bgp
  set as 65501
  set router-id 10.254.40.2
  set keepalive-timer 1
  set holdtime-timer 3
  set ebgp-multipath enable
  set scan-time 5
  set distance-external 1
config neighbor
  edit "10.254.40.1"
    set advertisement-interval 1
    set link-down-failover enable
    set soft-reconfiguration enable
    set remote-as 65500
    set keep-alive-timer 1
    set holdtime-timer 3
  next
  edit "10.254.41.1"
    set advertisement-interval 1
    set link-down-failover enable
    set soft-reconfiguration enable
    set remote-as 65500
    set keep-alive-timer 1
    set holdtime-timer 3
  next
end
config network
  edit 1
    set prefix 10.100.4.0 255.255.255.0
```

```

    next
end
end

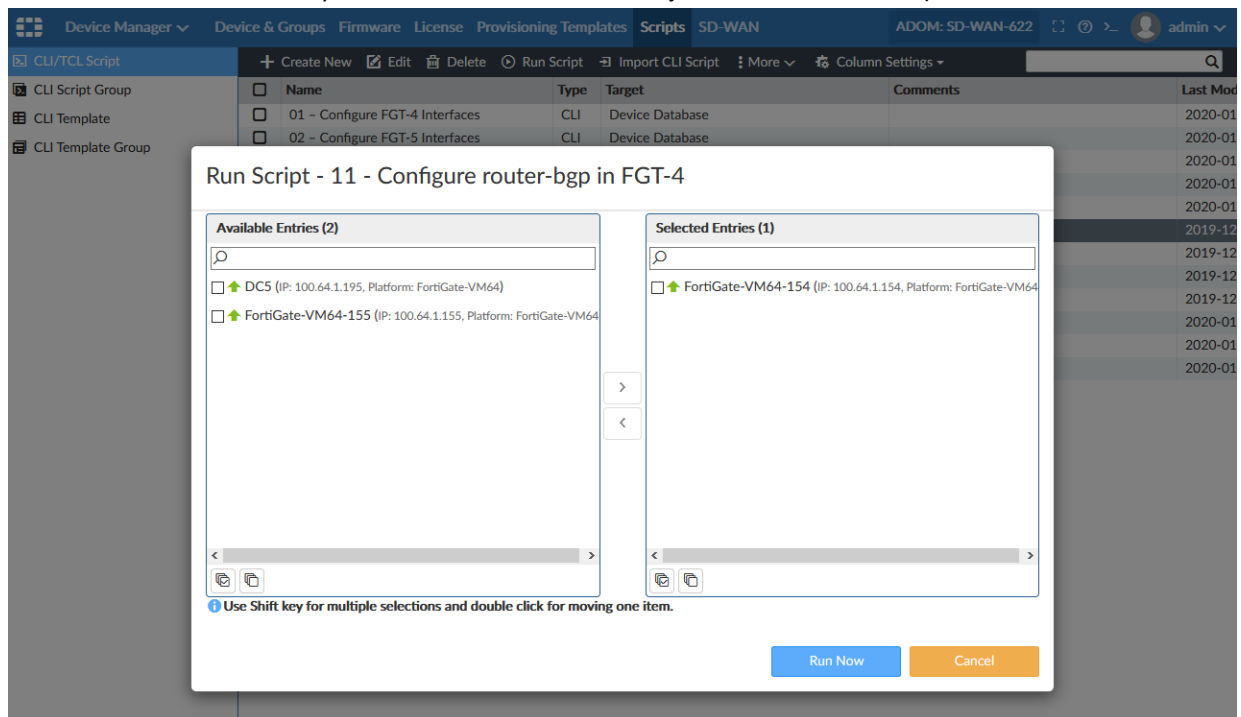
```

## Configuring the router BGP on the hub

Create and run a script to configure the router-bgp on the hub.

### To configure the router BGP on the hub:

1. Go to *Device Manager > Scripts*.
2. In the toolbar, click *Create New*.
3. Enter the script details such as the *Script Name*, *Type*, and *Run script on*.
4. In the *Script details* field, paste the script:
5. In the toolbar, click *Run Script*, and then select the devices you want to run the script on. Click *Run Now*.



## Example hub script

```

config vdom
  edit root

config router bgp
  set as 65500
  set router-id 10.10.40.1
  set ebgp-multipath enable
  set scan-time 5
  set graceful-restart enable

config aggregate-address

```



```
edit 1
    set prefix 10.100.0.0 255.255.0.0
    set summary-only enable
next
end
config neighbor
    edit "10.200.1.2"
        set remote-as 65500
    next
end

config neighbor-group
    edit "branch-peers-1"
        set advertisement-interval 1
        set link-down-failover enable
        set soft-reconfiguration enable
        set remote-as 65501
        set keep-alive-timer 1
        set holdtime-timer 3
    next
end

config neighbor-range
    edit 1
        set prefix 10.254.40.0 255.255.255.0
        set neighbor-group "branch-peers-1"
    next

edit 2
    set prefix 10.254.41.0 255.255.255.0
    set neighbor-group "branch-peers-1"
next
end

config network
    edit 1
        set prefix 10.200.1.0 255.255.255.0
    next

edit 2
    set prefix 10.200.0.0 255.255.255.0
next

edit 3
    set prefix 10.200.3.0 255.255.255.0
next
end

end

end
```

## Verifying the BGP routes

After you have configured the BGP routes in the hub and branches, use the routing table to verify the routes.

## Example BGP routes

### Branch 1:

```
FGT-4 # get router info routing-table bgp
Routing table for VRF=0
B      10.100.0.0/16 [1/0] via 10.254.41.1, OL_MPLS_0, 01:17:15
[1/0] via 10.254.40.1, OL_INET_0, 01:17:15
B      10.200.1.0/24 [1/0] via 10.254.41.1, OL_MPLS_0, 01:17:15
[1/0] via 10.254.40.1, OL_INET_0, 01:17:15
```

### Branch 2:

```
FGT-5 # get router info routing-table bgp
Routing table for VRF=0
B      10.100.0.0/16 [1/0] via 10.254.41.1, OL_MPLS_0, 00:23:24
[1/0] via 10.254.40.1, OL_INET_0, 00:23:24
B      10.200.1.0/24 [1/0] via 10.254.41.1, OL_MPLS_0, 00:23:24
[1/0] via 10.254.40.1, OL_INET_0, 00:23:24
```

### Hub

```
FGT-DC-5 # get router info routing-table bgp
Routing table for VRF=0
B      10.100.0.0/16 [200/0] is a summary, Null, 1d03h30m
B      10.100.4.0/24 [20/0] via 10.254.41.2, OL_MPLS_0, 01:18:57
[20/0] via 10.254.40.2, OL_INET_0, 01:18:57
B      10.100.5.0/24 [20/0] via 10.254.41.3, OL_MPLS_0, 00:23:52
[20/0] via 10.254.40.3, OL_INET_0, 00:23:52
```

## Configuring the ADVPN policy route on the FortiGate hub

In ADVPN, the hub devices forward the data packets to the spokes before the shortcut is established. To prevent the hub from using ECMP to send traffic to the spokes, create and implement a route policy.

### To configure the policy route in FortiManager:

```
config router policy
  edit 1
    set input-device "OL_MPLS_0"
    set output-device "OL_MPLS_0"
  next
  edit 2
    set input-device "OL_INET_0"
    set output-device "OL_INET_0"
```

next  
end

## Configuring SD-WAN

After you have configured the overlay and tunnel routes, enable SD-WAN for central management.

**To configure central management:**

1. [Enable central management.](#)
2. [Test ADVPN.](#)
3. [Add health-check servers.](#)
4. [Create SD-WAN templates for the branches.](#)
5. [Configure the static routes.](#)

### Enabling central management

Enable central management so you can configure the settings once, and install them to one or more devices.

**To enable Central Management:**

1. Go to *System Settings > All ADOMs*. Select the SDWAN network.
2. In the toolbar, click *Edit*.
3. Next to *Central Management*, select *SD-WAN*, and click *OK*.

### Configuring branch interfaces

You can use basic SD-WAN configurations on the branches to test ADVPN.

**To configure the branch interface members:**

1. Go to *Device Manager > SD-WAN*.
2. In the tree menu, click *Interface Members*.
3. In the toolbar, click *Create New*.

Create the following interface members:

- OL\_MPLS
- OL\_INET
- port2
- port3

Device Manager

Device & Groups

Firmware

License

Provisioning Templates

Scripts

SD-WAN

ADOM: SD-WAN-622

admin

Install Wizard

Central Management

SD-WAN Templates

Interface Members

Health-Check Servers

BGP Neighbors

Input Interfaces

Monitor

Create New

Edit

Delete

Where Used

Column Settings

Interface Name	Per Device Mapping	Description
<input type="checkbox"/> OL_INET_0	√ 2 out of 3 FortiGate-VM64-154 (root): OL_INET_0 FortiGate-VM64-155 (root): OL_INET_0	
<input type="checkbox"/> OL_MPLS_0	√ 2 out of 3 FortiGate-VM64-154 (root): OL_MPLS_0 FortiGate-VM64-155 (root): OL_MPLS_0	
<input type="checkbox"/> port2	√ 2 out of 3 FortiGate-VM64-154 (root): port2 FortiGate-VM64-155 (root): port2	
<input type="checkbox"/> port3	√ 2 out of 3 FortiGate-VM64-154 (root): port3 FortiGate-VM64-155 (root): port3	

4. Configure the interface settings keeping the following considerations in mind:

Property	Description
<b>Gateway</b>	Make sure to specify the remote gateway for the overlay interfaces.
<b>Default interface</b>	Make sure to specify the suffix <code>_0</code> for <code>OL_MPLS</code> and <code>OL_INET</code> . For example, <code>OL_MPLS_0</code> and <code>OL_INET_0</code> .
<b>Per-Device Mapping</b>	Toggle <i>ON</i> .
<b>Advanced Options</b>	
<b>Priority</b>	<p>Make sure to specify the priority for the <code>OL_MPLS</code> and <code>OL_INET</code> interfaces is higher than <code>port2</code> and <code>port3</code>.</p> <p>This will redirect the traffic that does not match an SD-WAN rule to the underlays in <code>port2</code> and <code>port3</code>, instead of using ECMP for all the interface members of the SD-WAN.</p>

## OL\_INET\_0 configuration:

Device Manager ▾ Device & Groups Firmware License Provisioning Templates Scripts **SD-WAN**

Install Wizard

SD-WAN Templates

**Interface Members**

Health-Check Servers

BGP Neighbors

Input Interfaces

Monitor

### Edit WAN Interface OL\_INET\_0

Name: OL\_INET\_0

Description:

Default Interface: OL\_INET\_0

Gateway: 0.0.0.0

Weight: 1

Cost: 1

Volume Ratio: 1

Per-Device Mapping: ☒ ON

	Name	VDOM	Interface	Gateway	Weight	Cost	Volume Ratio
<input type="checkbox"/>	FortiGate-VM64-154	root	OL_INET_0	10.254.40.2	1	1	1
<input type="checkbox"/>	FortiGate-VM64-155	root	OL_INET_0	10.254.40.3	1	1	1

Advanced Options ▾

gateway6: ::

ingress-spillover-threshold: 0

priority: 1

source: 0.0.0.0

source6: ::

spillover-threshold: 0

status: ☒ ON

## OL\_MPLS\_0 interface configuration:

Device Manager ▾ Device & Groups Firmware License Provisioning Templates Scripts **SD-WAN**

Install Wizard

SD-WAN Templates

**Interface Members**

Health-Check Servers

BGP Neighbors

Input Interfaces

Monitor

### Edit WAN Interface OL\_MPLS\_0

Name: OL\_MPLS\_0

Description:

Default Interface: OL\_MPLS\_0

Gateway: 0.0.0.0

Weight: 1

Cost: 1

Volume Ratio: 1

Per-Device Mapping: ☒ ON

	Name	VDOM	Interface	Gateway	Weight	Cost	Volume Ratio
<input type="checkbox"/>	FortiGate-VM64-154	root	OL_MPLS_0	10.254.41.2	1	1	1
<input type="checkbox"/>	FortiGate-VM64-155	root	OL_MPLS_0	10.254.41.3	1	1	1

Advanced Options ▾

gateway6: ::

ingress-spillover-threshold: 0

priority: 1

source: 0.0.0.0

source6: ::

spillover-threshold: 0

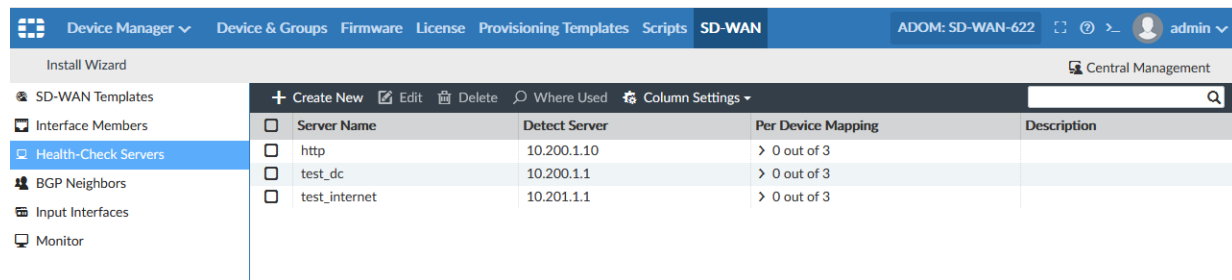
status: ☒ ON

## Creating health-check servers

Create health-check servers to verify that real servers are able respond to network connection attempts. You will need to create a health-check server for the overlay and underlay topologies.

### To create a health-check server:

1. Go to *Device Manager > SD-WAN*.
2. In the tree menu, click *Health-Check Servers*.
3. In the toolbar, click *Create New*. The *Create New WAN Detect Server* page opens.
4. Configure the Health-Check server settings, and click *OK*.



## Creating SD-WAN templates for the branches

Create an SD-WAN template, and then assign it to the branch devices.

### To create an SD-WAN template:

1. Go to *Device Manager > SD-WAN > SD-WAN Template*.
2. In the toolbar, click *Create New*. The *Create New* page opens.
3. Configure the SD-WAN template settings, and then click *OK*.

### To assign the SD-WAN template to the branch devices:

1. In the *SD-WAN Templates* content pane, select the SD-WAN template.
2. In the toolbar, click *Assign to Device*. The *Assign to Device* window appears.
3. Select the branch devices, and click *OK*.

## Configuring the static routes

Create static routes for IPv4 and IPv6, and then assign them to the branches.

To view the routing tables, go to *System Settings > Network*, and click *Routing Table* or *IPv6 Routing Table*.

### To add a static route:

1. From the IPv4 or IPv6 routing table, click *Create New* in the toolbar. The *Create New Network Route* dialog is displayed.
2. Enter the *Destination IP/Mask*.
3. Enter the *Gateway*.
4. From the *Interface* dropdown, select the network interface that connects to the gateway .
5. Click *OK*.

## Using Intelligent Application Steering and Link Fail-over

You can use FortiGate to load balance traffic depending on the application type and on the SLA. To do this, create application-based SD-WAN rules in FortiManager and then install the configurations on the branches.

### To use Intelligent Application Steering and Link Fail-over:

1. Create the following SD-WAN rules:
  - *Business Critical Cloud APP (Office365 and Azure and AWS)*: This traffic should always favor the INET underlay, in case SLA is not met or the underlay link fails, it can go through an overlay.
  - *Non-Business Critical Cloud APP (Facebook and Twitter)*: This traffic should only go through the underlay, in case of link failure, the traffic can stop working.
2. Enable FortiAnalyzer on the branches using CLI scripts
3. Install the configurations on the branches

### To create SD-WAN rules in the GUI:

1. Go to *Device Manager > SD-WAN > SD-WAN Template*.
2. Click *Create New* in the content pane toolbar, or right-click and select *Create New*. The *Create New* page opens.
3. In the SD-WAN Rules toolbar, click *Create New*. The *Create New SD-WAN Rule* dialog-box opens.
4. Configure the SD-WAN rule settings, then click *OK*.



In the SD-WAN policy for Business Critical and Non-Business Critical Cloud App, make sure to enable the *Gateway* option. This allows FortiGate to redirect correctly.

---

For information about creating SD-WAN rules, go to the [FortiManager Document Library > FortiManager Administration Guide > SD-WAN > SD-WAN templates](#).

### To enable FortiAnalyzer on the branches:


```
config log fortianalyzer setting
  set status enable
  set server "192.168.0.15"
  set upload-option realtime
  set serial <FMG_Serial Number>
  set certificate-verification disable
  set reliable enable
end
```

### To configure a FortiGate unit:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, select a device group.
3. In the content pane, select a device.
4. From the Install menu, select *Install Config*.
5. When the installation configuration is complete, click *Finish*.



After the installation is complete you will see the logs are on FortiAnalyzer. If you log in to the FortiGate WebUI you will notice an error message in the *Security Fabric Settings* page:



FortiAnalyzer Logging

Use FortiManager ☒

IP address

Storage usage

Upload option ☒ Real Time ☐ Every Minute ☐ Every 5 Minutes

SSL encrypt log transmission ☒

Allow access to FortiGate REST API ☒

Verify FortiAnalyzer certificate ☐

FortiGate not authorized to send any log types. Please grant permission on logging device.

Run the following command on FortiManager CLI:

```
exe log device permission ALL all ena
```

# Device Manager

This section contains the following topics:

- [Exporting a policy package from one FortiManager to another on page 34](#)

## 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 *System: 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.

The image shows two side-by-side screenshots of the FortiManager 'Add Device' wizard. The left screenshot is the 'Add Model Device' step, where the 'Add Model Device' radio button is selected. It includes input fields for Name, Link Device By (set to Serial Number), Serial Number, Device Model (set to 'Input SN to see available version...'), and Firmware Version (set to 5.4). The right screenshot is the 'Finish' step, showing a success message 'Device Added Successfully' and a list of completed steps: 'Creating device database', 'Retrieving high availability status', 'Initializing configuration database', 'Updating group membership', and 'Successfully add device'.

4. Import the revision to the second FortiManager:
- On your second FortiManager device, go to *Device Manager > Device & Groups* and double-click the model device. The Device Dashboard displays.
  - Go to *System: Dashboard > Configuration and Installation Status > Total Revisions*.
  - Right-click the empty revision list and select *Import Revision > Revision 1*.
  - Go to *Device Manager > Device & Groups*.
  - Right-click your model device and select *Import Policy*. The wizard displays.
  - Complete the wizard.
  - Go to *Policy & Objects*. The policy package and its used objects are displayed.



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

# VPN Manager

This section contains the following topics:

- [Configuring a full mesh VPN topology within a VPN console on page 36](#)

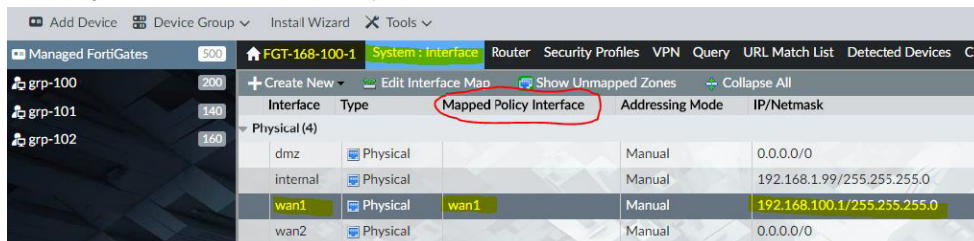
## Configuring a full mesh VPN topology within a VPN console

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.



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

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.

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

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

- 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

i. Optionally, under *Advanced Options*, the *IKE version* must be set to *two* in order to use IPv6 over tunnels.

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 is titled 'Edit VPN Community' and 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 (checked), 5 (checked), 14, 15, 16, 17, 18, 19, 20, 21

#### 4. Add a VPN gateway:

- Go to *VPN Manager > 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' in FortiManager, specifically the 'Protected Network' step. The wizard has five steps: Protected Network, Device, Default VPN Interface, Local Gateway, and Advanced. The 'Protected Network' step is currently active, showing a list of protected subnets. A dropdown menu is open, displaying the following options:

- 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
- IP/Netmask:172.19.100.5/255.255.255...

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:

< Back   Next >   Cancel

**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:

< Back   Next >   Cancel

**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:

< 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:

VPN Manager ▾ IPsec VPN SSL-VPN

VPN Community ▾ Install Wizard

All VPN Communities

- Full
- Star
- Monitor
- Map View

Edit Gateway

Protected Subnet

Device

Default VPN Interface

Local Gateway

Routing ☐ Manual (via Device Manager) ☒ Automatic

Local ID

Advanced Options >

## 5. Create firewall policies:

- Go to *Policy & Objects > Policy Package* to create policies among the default VPN zones and protected-subnet interfaces.
- Use the *Install On* option to restrict policies applied on specific FortiGate devices.

Policy Package ▾ Install ▾ ADOM Revisions ▾ Tools ▾

Create New ▾ Edit ▾ Delete ▾ Section ▾ Column Settings ▾

Seq.#	From	To	Source	Destination	Schedule	Service	Action	Log	NAT	Install On
1	loop1	vpnmgmt_full_mn	all	all	all	always	ALL	Accept	Log Security Ev	Disabled
2	vpnmgmt_full_mn	loop1	all	all	all	always	ALL	Accept	Log Security Ev	Disabled
3	loop1	vpnmgmt_full_sp	prosub-172.19.100.22	all	all	always	ALL	Accept	Log All Sessions	Disabled

Interface Pair View By Sequence

- FGT-168-100-4 (root)
- FGT-168-100-2 (root)
- FGT-168-100-3 (root)
- FGT-168-100-1 (root)
- FGT-168-100-5 (root)
- FGT-168-100-4 (root)
- FGT-168-100-2 (root)
- FGT-168-100-3 (root)
- FGT-168-100-1 (root)
- FGT-168-100-5 (root)
- FGT-168-100-22 (root)
- FGT-168-100-23 (root)
- FGT-168-100-24 (root)
- FGT-168-100-25 (root)
- FGT-168-100-26 (root)
- FGT-168-100-27 (root)
- FGT-168-100-28 (root)
- FGT-168-100-29 (root)
- FGT-168-100-30 (root)

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



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

# FortiSwitch Manager

*FortiSwitch Manager* is used to manage and monitor managed 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 42](#)
- [Using per-device management on page 47](#)
- [Installing changes to FortiSwitch devices on page 50](#)
- [Upgrading FortiSwitch firmware on page 52](#)
- [Using zero touch deployment for FortiSwitch on page 53](#)

## 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 42](#).
2. Create templates.  
You can import templates from managed switches, or you can create new templates. See [Importing and editing FortiSwitch templates on page 43](#) or [Creating FortiSwitch templates on page 44](#).
3. Assign templates to managed switches. See [Assigning templates to FortiSwitch devices on page 47](#).
4. Install changes to managed switches. See [Installing changes to FortiSwitch devices on page 50](#).

## 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 6.2

Comments: 0/128

**Devices**

Name	IP Address	Platform
FortiGate-140E-POE	10.2.172.153	FortiGate-140E-POE
FortiGate-300D	10.2.172.133	FortiGate-300D

Mode: ☐ Normal ☐ Backup

Central Management: ☐ VPN ☒ FortiAP ☐ SD-WAN

☒ FortiSwitch

Default Device Selection for Install: ☒ Select All ☐ Deselect All

Perform Policy Check Before Every Install: ☐ OFF

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 Templates*, and click *Import* in the toolbar. The *Import* dialog box opens.

**FortiSwitch Manager** > **Managed Switches** > **Monitor** > **FortiSwitch Templates**

Install Wizard

FortiSwitch Templates

+ Create New Edit Delete Where Used Import Column Settings

Name	Description	Platform	Last Modified
template-287	Imported from switch S448DN3X16000287	FortiSwitch-448D	admin/2019-11-20 10:45:53

**Import**

FortiGate: Click to select

FortiSwitch:

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.

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.

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:

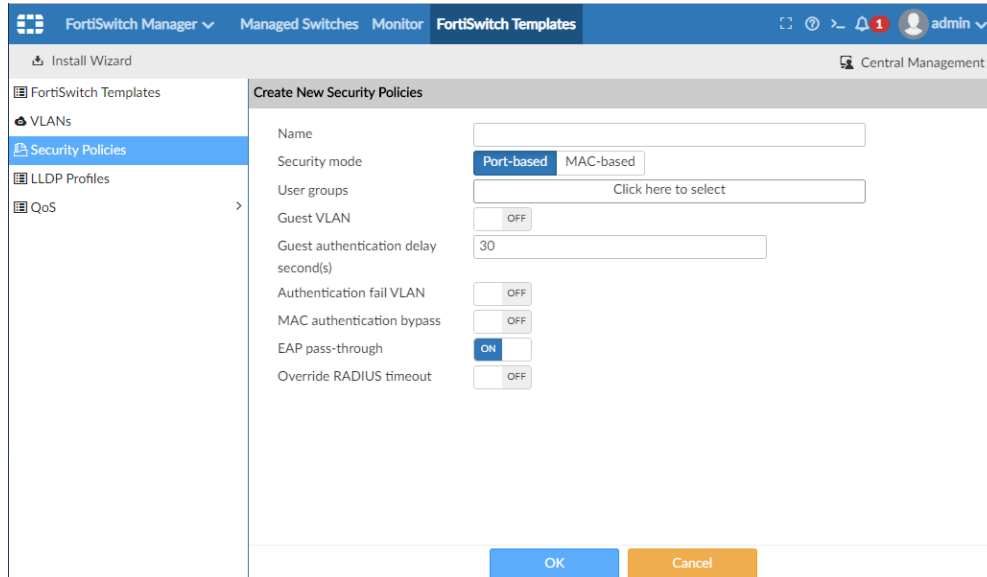
- VLANs
- Security policies
- LLDP profiles
- QoS policies

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 Policies*, and click *Create New*.

The *Create New Security Policies* pane opens.



The screenshot shows the FortiSwitch Manager interface. The top navigation bar includes 'FortiSwitch Manager', 'Managed Switches', 'Monitor', and 'FortiSwitch Templates'. The left sidebar has a tree view with 'FortiSwitch Templates', 'VLANs', 'Security Policies' (selected), 'LLDP Profiles', and 'QoS'. The main area is titled 'Create New Security Policies'. It contains the following fields and controls:

- Name: A text input field.
- Security mode: Two tabs, 'Port-based' (selected) and 'MAC-based'.
- User groups: A dropdown menu with the text 'Click here to select'.
- Guest VLAN: A dropdown menu with 'OFF' selected.
- Guest authentication delay second(s): A text input field with '30'.
- Authentication fail VLAN: A dropdown menu with 'OFF' selected.
- MAC authentication bypass: A dropdown menu with 'OFF' selected.
- EAP pass-through: A dropdown menu with 'ON' selected.
- Override RADIUS timeout: A dropdown menu with 'OFF' selected.

At the bottom of the pane are 'OK' and 'Cancel' buttons.

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

**To create FortiSwitch templates:**

1. Go to *FortiSwitch Manager > FortiSwitch Templates*.
2. 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.
3. Click *FortiSwitch Templates*, and click *Create New*.  
The Create New FortiSwitch Template pane opens.

4. Set the following options, and click **OK**.
  - a. In the *Template Name* box, type a name for the template.
  - b. In the *Platforms* list, select the FortiSwitch platform.
  - c. 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 > Managed Switches*.
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 can also assign templates when editing a FortiSwitch device.

- 
6. Install the template settings. See [Installing changes to FortiSwitch devices on page 50](#).

## 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:

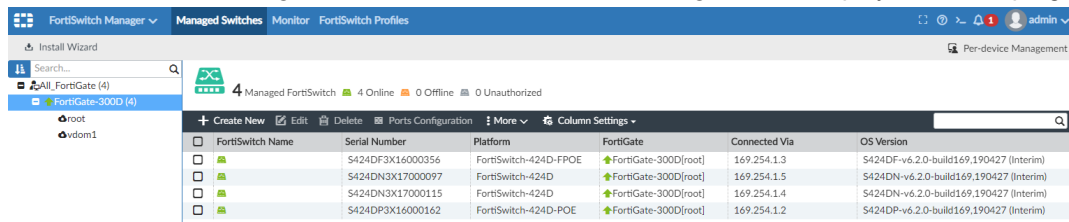
1. Enable per-device management. See [Enabling FortiSwitch per-device management on page 48](#).
2. Configure profiles for managed switches.  
You can configure VLANs, security policies, LLDP profiles, and QoS policies, and the changes are saved to the FortiGate database. See [Configuring FortiSwitch profiles on page 48](#).
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 49](#).
4. Install changes to managed switches. See [Installing changes to FortiSwitch devices on page 50](#).

## 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.



## 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.

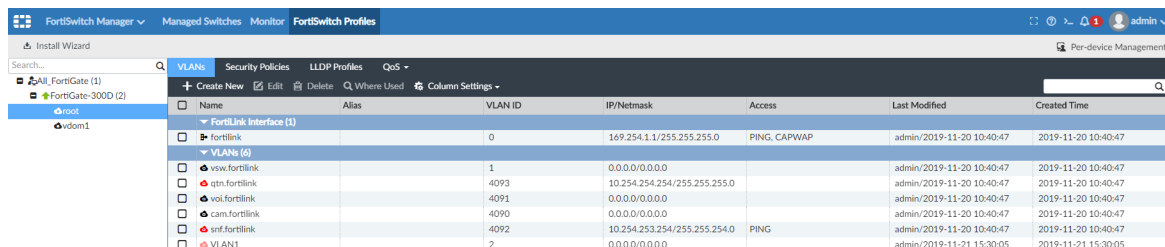
You can configure the following types of profiles and policies:

- 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 > FortiSwitch Profiles*.
2. In the tree menu, select a FortiGate.  
The *VLAN* tab is displayed.



3. Double-click a VLAN to open it for editing, or click *Create New* to create a new VLAN.



4. Edit the options, and click *OK*.  
The VLAN settings are saved to the FortiGate database.

**To configure Security Policies:**

1. Go to *FortiSwitch Manager > FortiSwitch Profiles*.
2. In the tree menu, select a FortiGate.  
The *VLAN* tab is displayed.
3. Click the *Security Policies* tab.
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 > FortiSwitch Profiles*.
2. In the tree menu, select a FortiGate.  
The *VLAN* tab is displayed.
3. Click the *LLDP Profiles* tab.
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:**

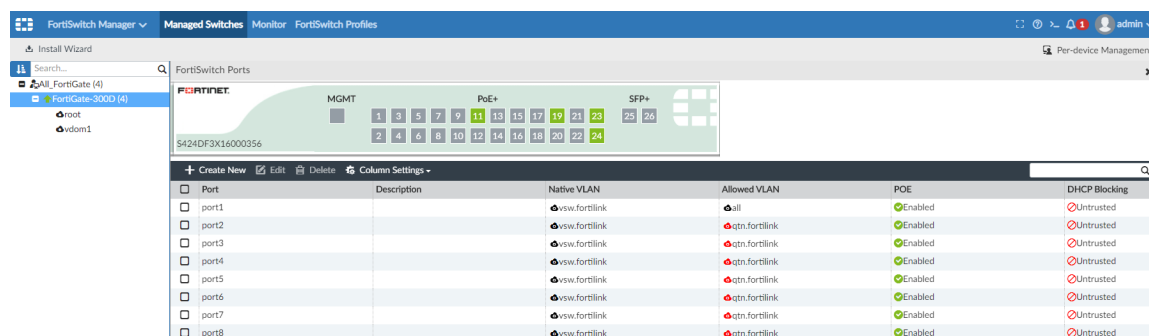
1. Go to *FortiSwitch Manager > FortiSwitch Profiles*.
2. In the tree menu, select a FortiGate.  
The *VLAN* tab is displayed.
3. From the *QoS* menu, select a type of policy.
4. Double-click the policy to open it for editing, or click *Create New* to create a new policy.
5. Edit the options, and click *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.



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

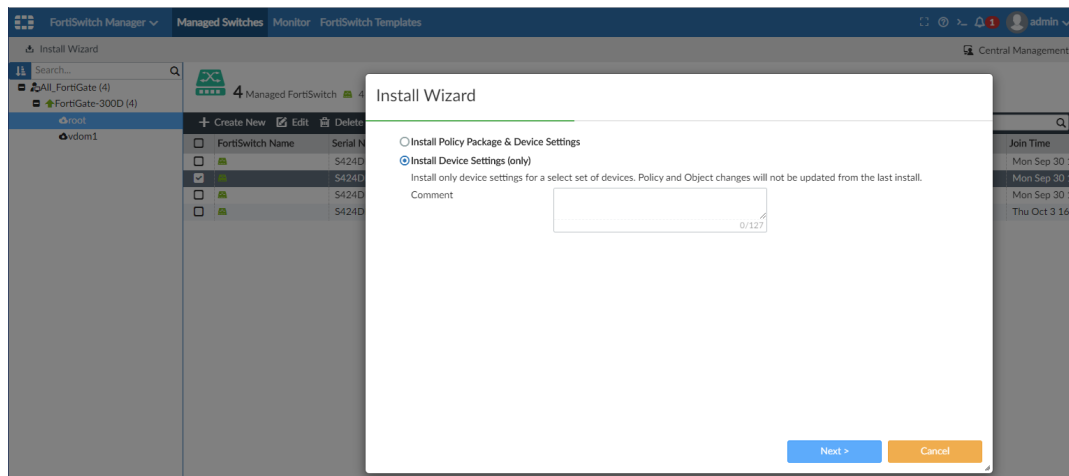
- Edit the options and click **OK**.  
The changes are saved to the FortiGate database.
- Install the changes. See [Installing changes to FortiSwitch devices on page 50](#).

## Installing changes to FortiSwitch devices

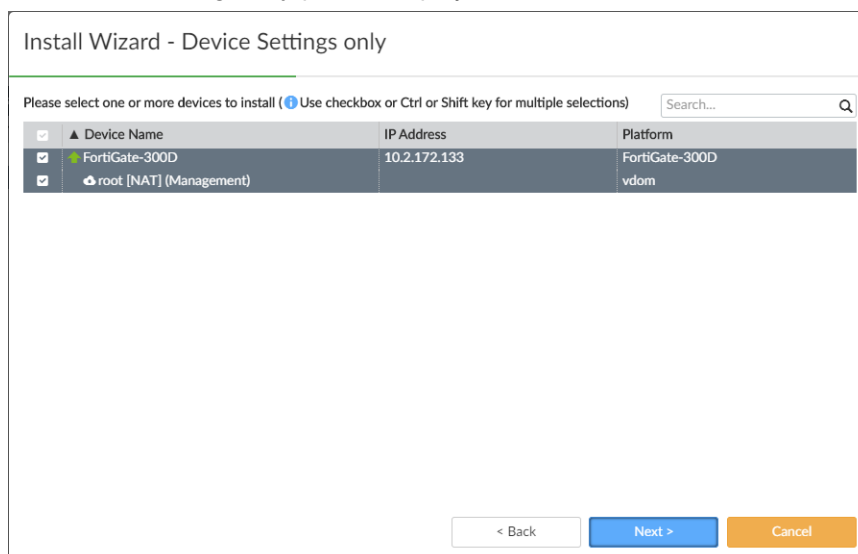
You can install changes to managed FortiSwitch devices directly from the *FortiSwitch Manager* pane. Alternately you can install changes when you install a configuration to the FortiGate that manages the switch.

### To install changes to switches:

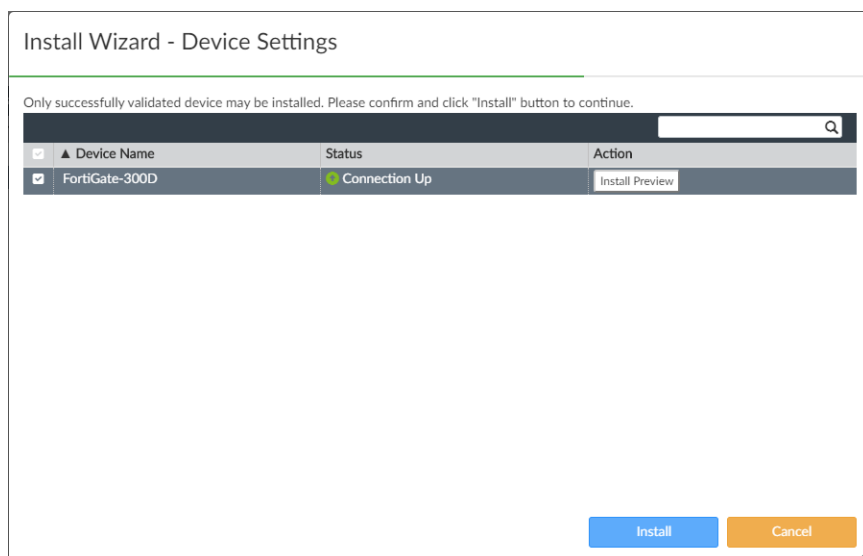
- Go to *FortiSwitch Manager > Managed Switches*.
- In the tree menu, select the FortiGate device that controls the FortiSwitch.  
The managed switches are displayed in the content pane.
- In the content pane, select the switch, and click *Install Wizard*.  
The *Install Wizard* is displayed.



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*.

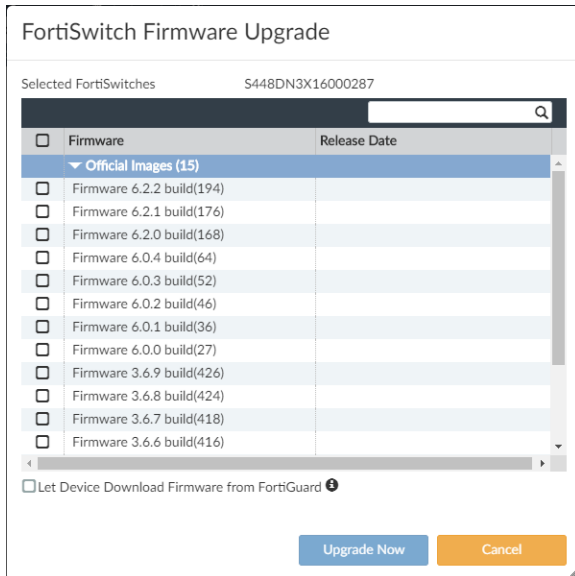
## Upgrading FortiSwitch firmware

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.



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:

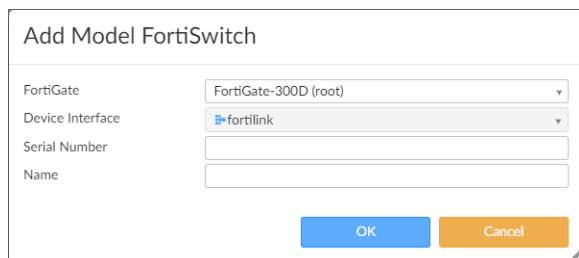
- FortiManager version 5.6 ADOM or later.
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with FortiSwitch.
- The FortiSwitch serial number is available.



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 input 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).

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

<b>FortiGate</b>	Select the FortiGate device or VDOM from the drop-down.
<b>Device Interface</b>	Select the port where the FortiSwitch will be connected.
<b>Serial Number</b>	Specify the FortiSwitch serial number.
<b>Name</b>	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 47](#).
  - For *FortiSwitch Manager* with per-device management enabled, see [Configuring FortiSwitch ports on page 49](#).

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 55](#)
- [Creating administrator accounts with restricted access on page 56](#)

## 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.](#)
2. [Configure one or more backup FortiManager units.](#)
3. [If you encounter problems, review the debug log for each unit in an HA cluster.](#)

### 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 (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 (or peer) FortiManager unit.
5. Click the + icon to add additional backup FortiManager units to the HA cluster.

Peer SN  +-

6. Click *Apply*.

### Configuring backup FortiManager units in an HA cluster

You can configure up to four FortiManager units as backup (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:**

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

Peer IP	<input type="text" value="IPv4 192.168.48.60"/>	Peer SN	<input type="text" value="FM200D3A15000056"/>
Cluster ID	<input type="text" value="1"/> (1-64)		
Group Password	<input type="password"/>		
File Quota	<input type="text" value="4096"/> (2048-20480) MB		
Heart Beat Interval	<input type="text" value="5"/> Seconds		
Fallover Threshold	<input type="text" value="3"/> (1-255)		
Download Debug Log	<input type="button" value="Download"/>		

5. 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:**

1. On the primary or backup FortiManager unit in an HA cluster, enter the following command:  
`diagnose debug application ha 255`

**To download a debug log:**

1. Go to *System Settings > HA*.
2. Next to *Download Debug Log*, click *Download*.

Cluster ID	<input type="text" value="1"/> (1-64)
Group Password	<input type="password"/>
File Quota	<input type="text" value="4096"/> (2048-20480) MB
Heart Beat Interval	<input type="text" value="5"/> Seconds
Fallover Threshold	<input type="text" value="3"/> (1-255)
Download Debug Log	<input type="button" value="Download"/>

3. 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 57](#)
- Device groups - see [Restricting administrator access to device groups on page 59](#)
- Policy packages - see [Restricting administrator access to policy packages on page 61](#)



## 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 > Administrators*.
2. Click *Create New*.
3. Beside *Administrative Domain*, click *Specify*, and then select the ADOMs that the administrator account can access.

The screenshot shows the 'New Administrator' configuration page in FortiManager. The left sidebar contains the 'System Settings' menu with 'Administrators' selected. The main form fields are: User Name (ADOM-admin), Avatar (A), Comments (0/127), Admin Type (LOCAL), New Password, Confirm Password, Admin Profile (Restricted\_User), Administrative Domain (All ADOMs, All ADOMs except specified ones, Specify), Policy Package Access, Trusted Hosts, and Meta Fields. The 'Specify' button for Administrative Domain is highlighted, and a dropdown menu is open showing a list of ADOMs: FortiManager, FortiProxy, FortiSandbox, FortiWeb, Syslog, root, and Global Database. The 'root' ADOM is selected.

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

The screenshot shows the 'New Administrator' configuration window in FortiManager. The left sidebar lists various system settings, with 'Administrators' selected under the 'Admin' category. The main form contains the following fields and options:

- User Name:** ADOM-admin
- Avatar:** A purple circle with the letter 'A'. Buttons: + Change Photo, - Remove Photo
- Comments:** Text area with a character count of 0/127.
- Admin Type:** LOCAL (dropdown)
- New Password:** Password field with an eye icon to toggle visibility.
- Confirm Password:** Password field with an eye icon to toggle visibility.
- Admin Profile:** Restricted\_User (dropdown)
- Administrative Domain:**
  - Buttons: All ADOMs, All ADOMs except specified ones, Specify
  - Selected ADOMs: root, 56
- Policy Package Access:**
  - Buttons: All Packages, Specify
- Trusted Hosts:** OFF (toggle)
- Meta Fields:** Expandable section.

At the bottom right are 'OK' and 'Cancel' buttons.

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*.

The screenshot shows a 'Select an ADOM' dialog box with a search bar at the top. Below the search bar is a list of ADOMs:

ADOM Name	Version
root (2)	FortiGate 6.0
56	FortiGate 5.6

The 'root (2)' entry is highlighted in blue. A 'Close' button is located at the bottom right of the dialog.

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

1. Go to *System Settings > 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.

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*.

## 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.

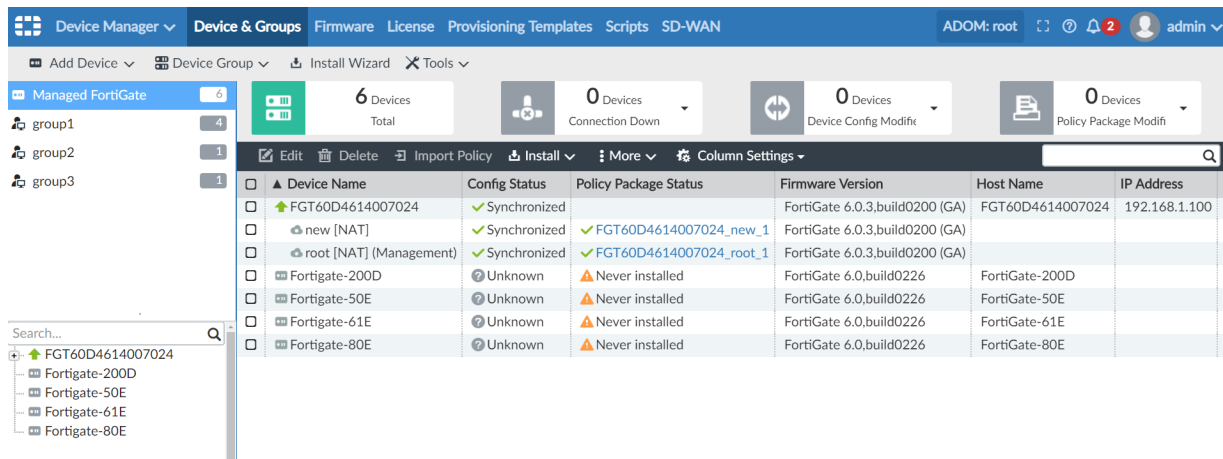
When you create an administrator account, you can specify which ADOMs the account can access, and which device groups can be accessed in those ADOMs.

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

### To create a device group:

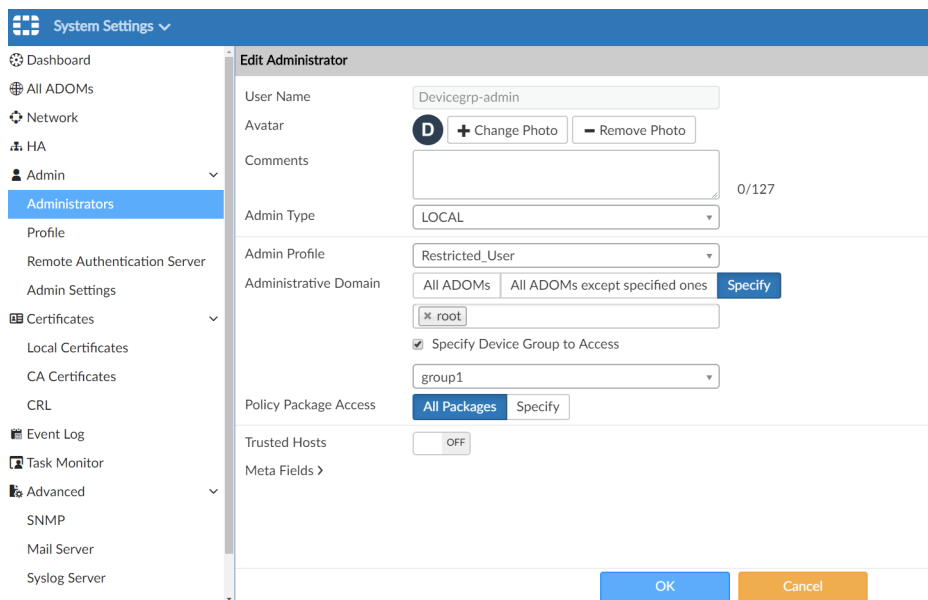
1. Go to *Device Manager > Device & Groups*.
2. If you are using ADOMs, select the ADOM that you are creating a device group in. Otherwise skip this step.
3. In the *Device Group* menu, click *Create New*.
4. Enter a name for the group and add devices to it, then click **OK**.

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



### To specify admin access to device groups:

1. Go to **System Settings > 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.



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*.

Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	IP Address
FGT60D4614007024	✓ Synchronized	✓ FGT60D4614007024_new_1	FortiGate 6.0.3,build0200 (GA)	FGT60D4614007024	192.168.1.100
new [NAT]	✓ Synchronized	✓ FGT60D4614007024_new_1	FortiGate 6.0.3,build0200 (GA)		
root [NAT] (Management)	✓ Synchronized	✓ FGT60D4614007024_root_1	FortiGate 6.0.3,build0200 (GA)		
Fortigate-200D	⚠ Unknown	⚠ Never installed	FortiGate 6.0,build0226	FortiGate-200D	
Fortigate-50E	⚠ Unknown	⚠ Never installed	FortiGate 6.0,build0226	FortiGate-50E	

## 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 > 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.

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 62](#)
- [Creating a third party blocklist provider workflow on page 71](#)

## Managing FortiAnalyzer from FortiManager

This section contains the following topics:

- [Adding FortiAnalyzer to FortiManager on page 62](#)
- [Viewing managed FortiAnalyzer behavior on page 66](#)
- [Centrally configuring FortiGate to send logs to managed FortiAnalyzer on page 67](#)
- [Viewing logs and reports for managed FortiAnalyzer units on page 67](#)
- [Managing multiple FortiAnalyzer units on page 69](#)
- [Troubleshooting managed FortiAnalyzer units on page 69](#)

## 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 62](#)
- [Using the wizard to add FortiAnalyzer to FortiManager on page 63](#)
- [Additional information on page 65](#)

### 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. Ensure that FortiManager Features are disabled.  

```
config system global
set fmg-status disable
end
```
3. 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.
4. Set storage settings for the ADOM.

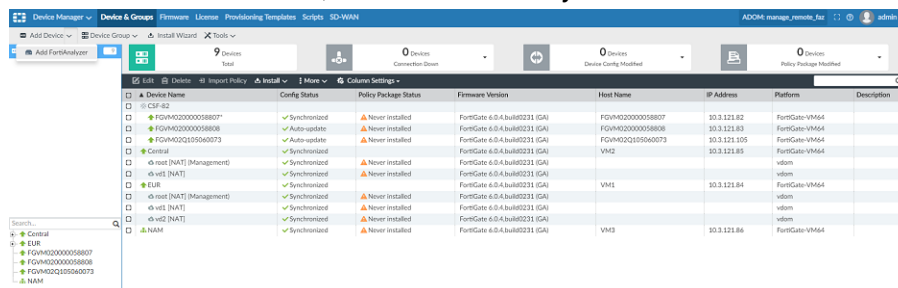
### Using the wizard to add FortiAnalyzer to FortiManager

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*.

After FortiManager discovers the device, device information is displayed.

- c. Click *Next* to continue.

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

Status	Device Name	Platform
FortiManager Only	FGM4020000058807	FortiGate-V4000
FortiManager Only	FGM4020000058808	FortiGate-V4000
FortiManager Only	SQL	FortiGate-V4000
FortiManager Only	Control	FortiGate-V4000
FortiManager Only	NAM	FortiGate-V4000
FortiManager Only	FGM4020000058809	FortiGate-V4000

- 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.

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

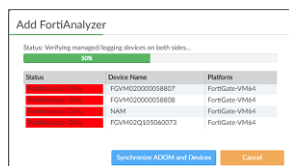
This section describes some of the other scenarios you might encounter when adding FortiAnalyzer units to FortiManager.

### 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

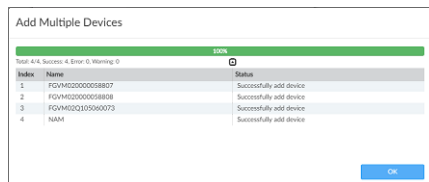
If FortiAnalyzer is receiving logs from FortiGate devices that do not exist on FortiManager, FortiManager identifies the devices.



FortiManager automatically attempts to discover the FortiGates.

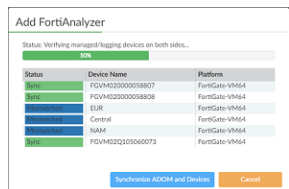


FortiManager can add the FortiGates and retrieve configurations for the FortiGates when adding the FortiAnalyzer unit.

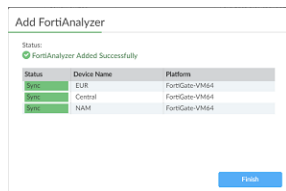


If one device fails to add or retrieve, FortiManager fails to add FortiAnalyzer.

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.



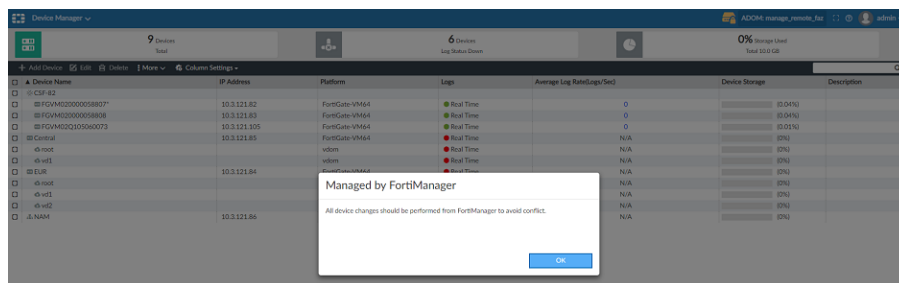
If any errors occur during the synchronization step, FortiManager fails to add FortiAnalyzer.

## Viewing managed FortiAnalyzer behavior

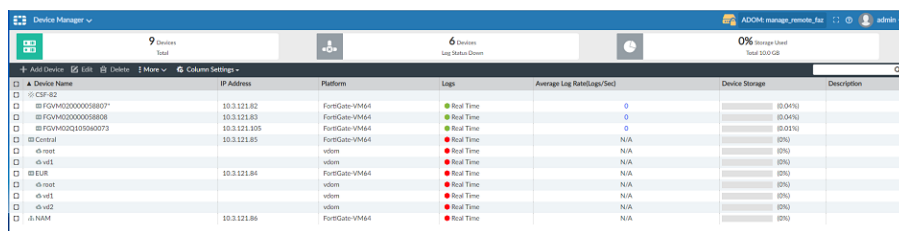
After FortiManager manages the ADOM with FortiAnalyzer in it, you should use FortiManager to perform changes on all devices in the ADOM. This topic describes the behavior you will view in the GUI for a FortiAnalyzer unit that is managed by FortiManager.

**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.

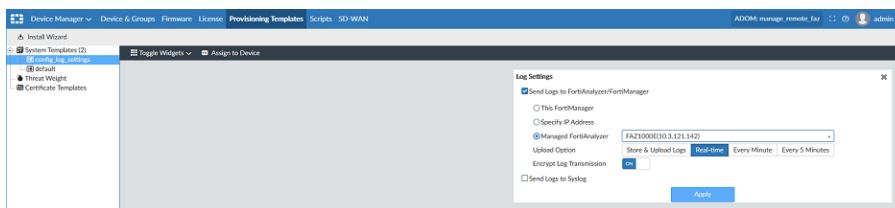
Name	Firmware Version	Allocated Storage	Devices
FortiAnalyzer	FortiAnalyzer	1000 MB	
FortiAuthenticator	FortiAuthenticator	1000 MB	
FortiCache	FortiCache	1000 MB	
FortiClient	FortiClient	1000 MB	
FortiDDoS	FortiDDoS	1000 MB	
FortiMail	FortiMail	1000 MB	
FortiManager	FortiManager	1000 MB	
FortiProxy	FortiProxy	1000 MB	
FortiSandBox	FortiSandBox	1000 MB	
FortiWeb	FortiWeb	1000 MB	
Syslog	Syslog	1000 MB	

## 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 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 close all the unneeded widgets.



- 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
- NOC-SOC
- Log View
- Event Manager
- 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:

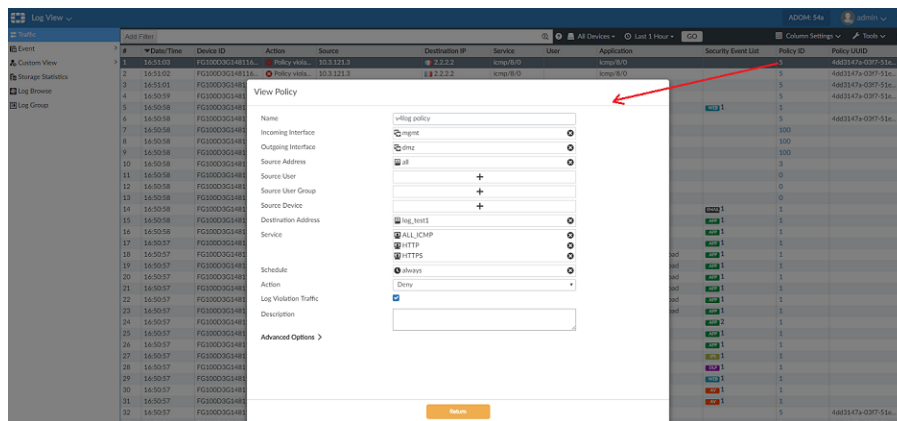
#### 1. On FortiManager, go to *Log View*.

You can view all logs received and stored on FortiAnalyzer.

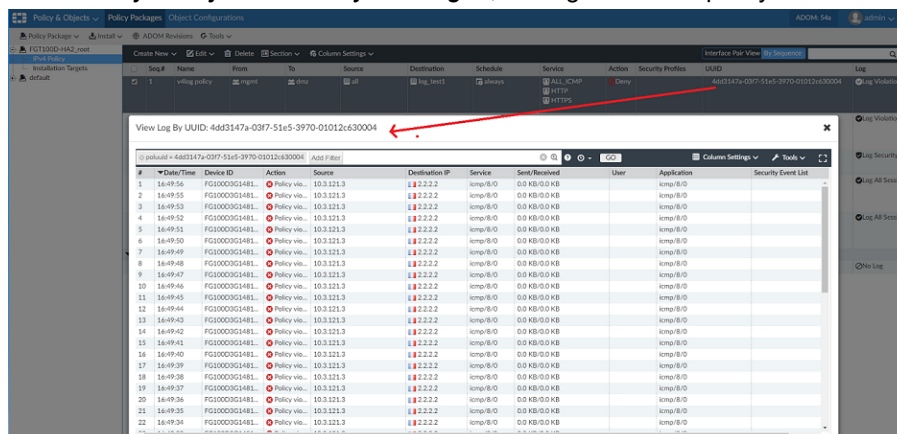
#### 2. Click the *Policy ID*.

The policy rule opens.

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



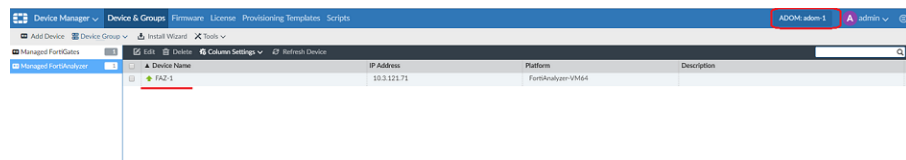
#### 3. Go to *Policy & Objects > Policy Packages*, and right-click the policy UUID to search the related policy logs.



## 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.

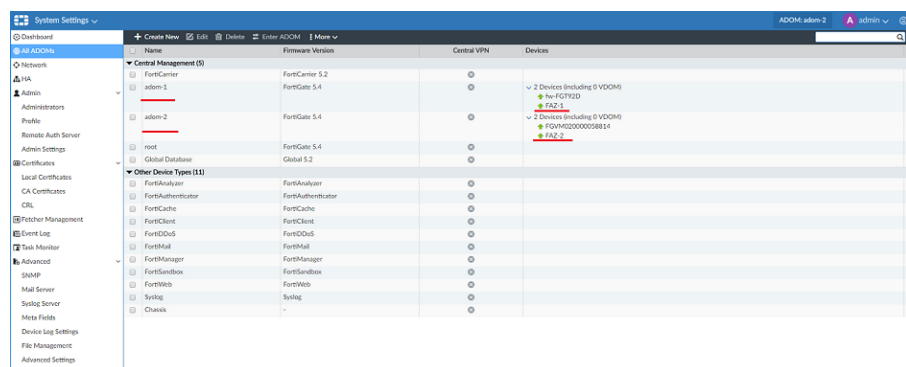
For example, FortiManager can contain the following ADOMs: *adom-1* and *adom-2*, and *adom-1* manages FAZ-1:



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`

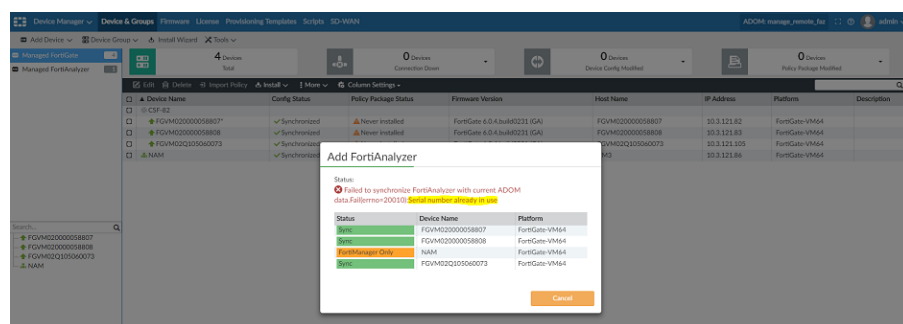
## ADOM remains locked on FortiAnalyzer

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.

```
FG3000 login: admin
Password:
FG3000 # diagnose dvm device list
... There are currently 4 devices/vdoms managed ...

TYPE  QID  SN              HA  IP  NAME                                ADOM              IPS
-----
mg/faz enabled 501  FGVMD2000058807  10.3.121.82  FGVMD2000058807  manage_remote_faz  6.00741 (regular)  FTMware2
mg/faz enabled 513  FGVMD2000058808  10.3.121.83  FGVMD2000058808  manage_remote_faz  6.00741 (regular)  6.0 HBB (231)
mg/faz enabled 400  FGVMD2000058807  10.3.121.82  FGVMD2000058807  manage_remote_faz  6.00741 (regular)  6.0 HBB (231)
mg/faz enabled 476  FGVMD2000058811  10.3.121.85  N/A              manage_remote_faz  6.00741 (regular)  6.0 HBB (231)

HA cluster members: (from FGVMD20058811) (failed)
[- vdom:[J]root flags:0 admin: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 ...

FG3000 #

FAZ1000E login: admin
Password:
FAZ1000E # diagnose dvm device list
... There are currently 4 devices/vdoms managed ...

TYPE  QID  SN              HA  IP  NAME                                ADOM              IPS
-----
faz enabled 273  FGVMD2000058807  10.3.121.82  FGVMD2000058807  manage_remote_faz  6.00741 (regular)  FTMware2
faz enabled 271  FGVMD2000058808  10.3.121.83  FGVMD2000058808  manage_remote_faz  6.00741 (regular)  6.0 HBB (231)
faz enabled 272  FGVMD2000058807  10.3.121.82  FGVMD2000058807  manage_remote_faz  6.00741 (regular)  6.0 HBB (231)
faz enabled 508  FGVMD2000058811  10.3.121.85  N/A              root              6.00741 (regular)  6.0 HBB (231)

HA cluster members: (from FGVMD20058811) (failed)
[- vdom:[J]root flags:0 admin: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 ...

FAZ1000E #
```

Compare the device list on FMG and FAZ. Both FMG and FAZ have device "FGVMD2000058811" but it is in different ADOM (on FMG it is in ADOM "manage\_remote\_faz", on FAZ it is in ADOM "root"). That is why we saw the error "Failed to sync device to FAZ: Serial number already in use".

To solve the problem, manually move the device "FGVMD2000058811" 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.

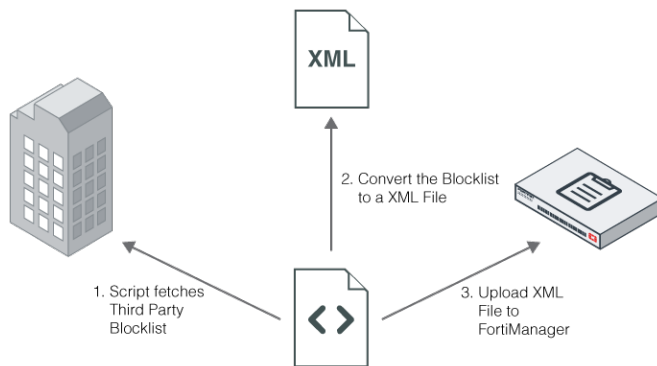
## Creating a third party blocklist provider workflow

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
```

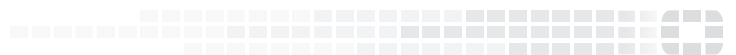


For further FortiManager information, refer to the [FortiManager Administration Guides](#) available in the [Fortinet Document Library](#).

---



**FORTINET®**



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.