FortiManager - Examples

Version 6.4.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

December 15, 2022
FortiManager 6.4.0 Examples
02-640-682453-20221215

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-12-16	Initial release.
2021-08-23	Added SD-WAN with ADVPN - dual hub on page 37.
2022-12-15	Updated Adding gateways to VPN communities on page 47.

Introduction

This document serves as a reference guide to common FortiManager 6.4 configuration and deployment scenarios. The scope of this document is to explain specific examples and include information required for those examples to work. The examples rely on the other documents to provide full product information.

For further FortiManager information, refer to the FortiManager Administration Guides available on the Fortinet Docs Library.

This section includes configuration examples for FortiManager 6.4:

SD-WAN with ADVPN - single hub

You can use this section with FortiManager 6.4.1. and later that supports normalized interfaces and zones.

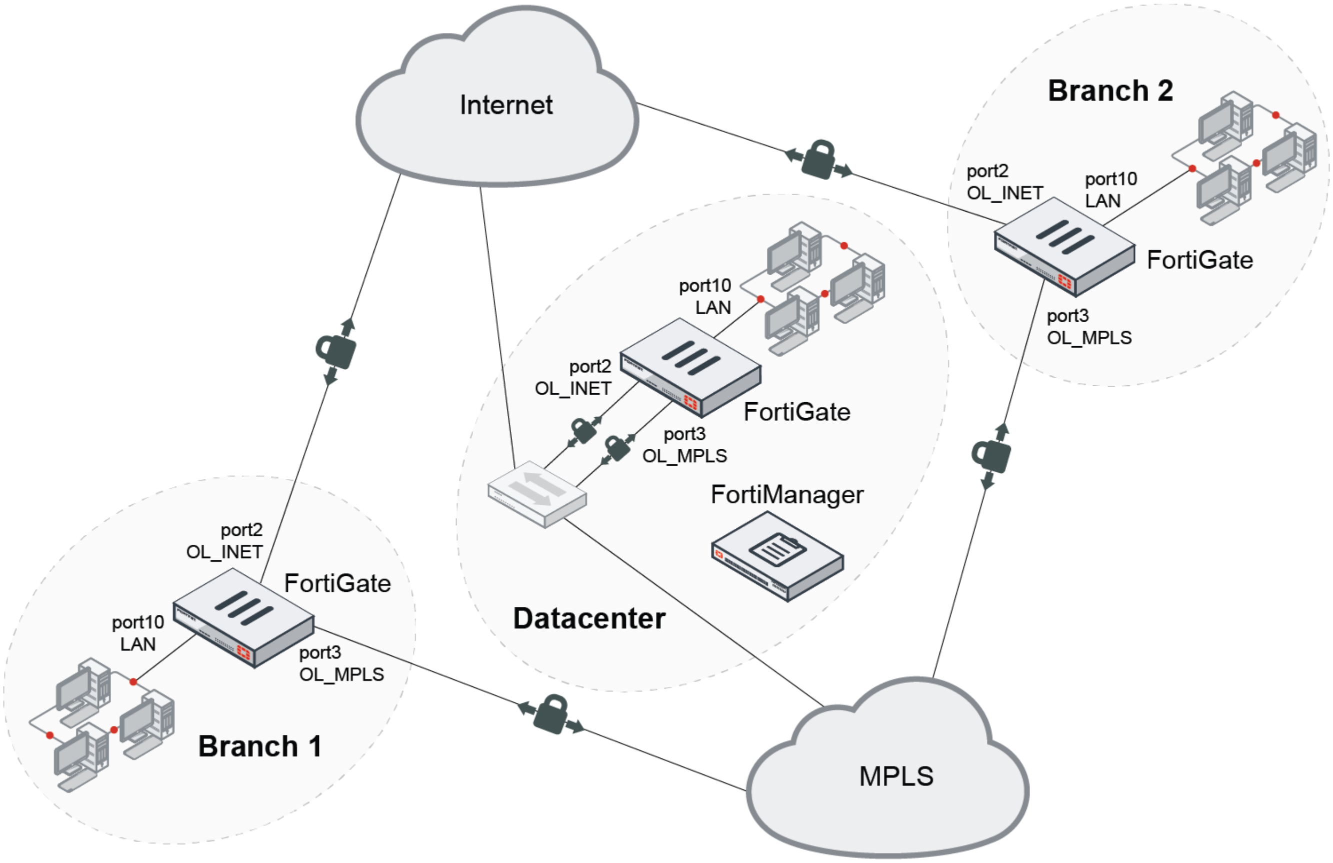
This section provides an understanding of the Fortinet secure SD-WAN configuration. The main objective of this section is to provide details on how to configure SD-WAN to cover the following use cases:

- ADVPN
- SD-WAN

In our example, we have a FortiGate at the Datacenter (FGT-DC6), another FortiGate at Branch 1 (FGT-6), and one more FortiGate at Branch 2 (FGT-7). All the FortGates have two links:

- INET: To simulate a connection from the branch to the datacenter
- MPLS: To simulate a backup connection from the branch to the datacenter

From both the branch FortiGates you will create IPsec tunnels OL_INET (over port2) and OL_MPLS (over port3) to the datacenter FortiGate.



The configuration in this example uses the following interfaces and IP addresses:

FortiGate	INET	MPLS	LAN	OL_INET	OL_MPLS
Datacenter (FGT-DC6)	port2: 172.20.10.5 /24 Default Gateway: 172.20.10.254	port3: 172.20.9.5 /24 Default Gateway: 172.20.9.254	port10: 10.200.1.6/24	10.254.50.1	10.254.51.1
Branch 1 (FGT-6)	port2: 172.20.11.6/24 Default Gateway: 172.20.11.254	port3: 172.20.12.6 /24 Default Gateway: 172.20.12.254	port10: 10.100.6.1/24	10.254.50.2	10.254.51.2
Branch 2 (FGT-7)	port2: 172.20.11.7/24 Default Gateway: 172.20.11.254	port3: 172.20.12.7 /24 Default Gateway: 172.20.12.254	port10: 10.100.7.1/24	10.254.50.3	10.254.51.3

This section describes the following steps to configure a SD-WAN with ADVPN for a single hub deployment:

1. Adding FortiGate devices to FortiManager on page 9.
2. Configuring overlay connections on page 10.
3. Configuring dynamic routing on page 25.
4. Configuring SD-WAN on page 29.
5. Using Intelligent Application Steering and Link Fail-over on page 34.

Adding FortiGate devices to FortiManager

Adding the datacenter FortiGate and the two branch office FortiGates to FortiManager involves the following steps:

1. Adding the FortiGates to FortiManager.
2. Retrieving the FortiGate device configuration settings.
3. Importing the FortiGate device policies and establishing synchronization.

To add a FortiGate device using the *Discover* mode on FortiManager:

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

To retrieve the FortiGate device configuration settings:

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.

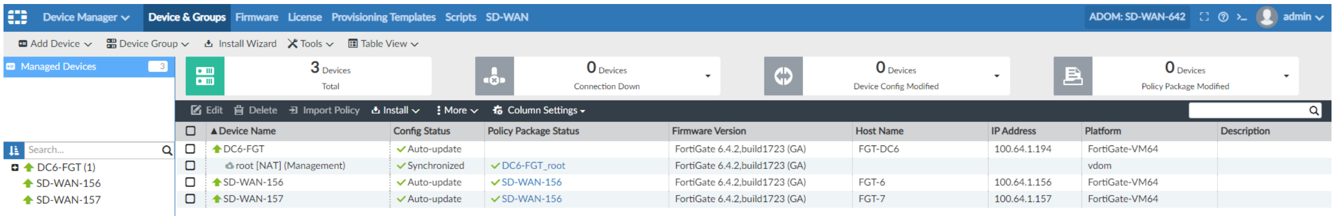
To import the FortiGate device policies:

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 the changes related to policies and objects in the *Policy & Objects* module.

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

After you have successfully added the FortiGates, retrieved the configuration settings, and imported the policies to synchronize, go to *Device Manager* > *Device & Groups* to view the registered FortiGates:



Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	IP Address	Platform	Description
DC6-FGT	✓ Auto-update		FortiGate 6.4.2,build1723 (GA)	FGT-DC6	100.64.1.194	FortiGate-VM64	
root [NAT] (Management)	✓ Synchronized	✓ DC6-FGT_root	FortiGate 6.4.2,build1723 (GA)			vdom	
SD-WAN-156	✓ Auto-update	✓ SD-WAN-156	FortiGate 6.4.2,build1723 (GA)	FGT-6	100.64.1.156	FortiGate-VM64	
SD-WAN-157	✓ Auto-update	✓ SD-WAN-156	FortiGate 6.4.2,build1723 (GA)	FGT-7	100.64.1.157	FortiGate-VM64	

Configuring overlay connections

Creating and configuring overlay connections involves the following steps:

1. Configuring VPN Manager on page 11.
2. Mapping underlay interfaces on page 18.
3. Creating policy packages on page 19.
4. Installing policy packages on page 21.
5. Configuring tunnel interfaces and dynamic mapping on page 21.
6. Fixing the settings in the policy package on page 23.

Configuring VPN Manager

We need to create two overlay connections to create two secure links to the datacenter and then implement SD-WAN among those links. In order to create the two overlay connections, we need to create VPN communities and add nodes to those communities, from the *VPN Manager*.

This section involves the following steps:

1. Creating VPN communities on page 11
2. Adding nodes to VPN communities on page 12

Creating VPN communities

We will use the dial-up topology to create the two overlays, one for the internet connection (OL_INET) and one for the MPLS network (OL_MPLS), by creating two VPN communities.

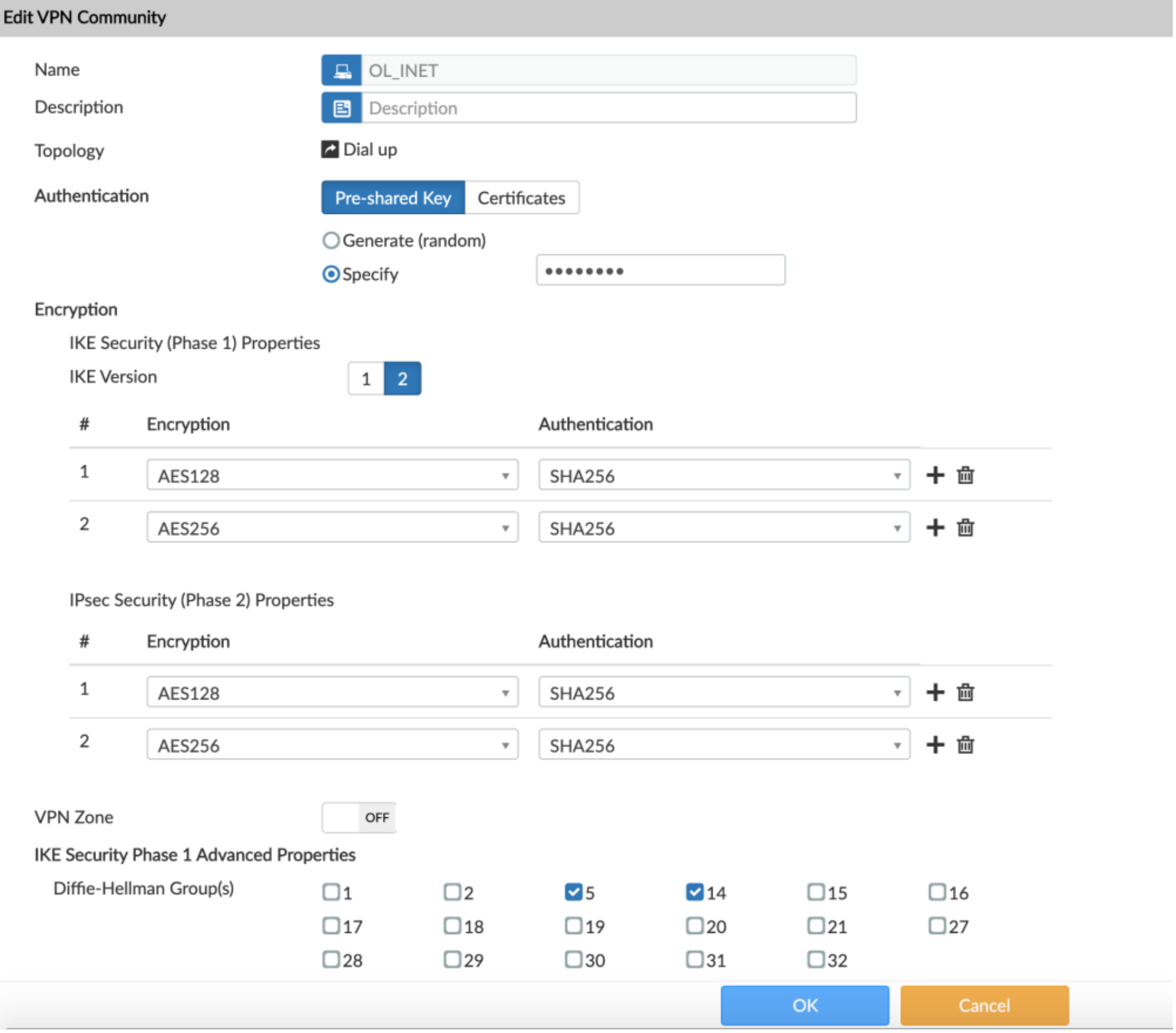
To create a VPN Community from the GUI:

1. Go to *VPN Manager > IPsec VPN*.
2. In the toolbar, click *Create New*. The *VPN Topology Setup Wizard* dialog appears.
3. Enter a name for the topology, such as *OL_INET*.
4. In the *Choose VPN topology* field, select *Dial up*.
5. Click *Next*.
6. Complete the setup as required in the wizard.

Ensure that *VPN Zone* is disabled while completing the dial-up topology setup. Enabling *VPN Zone* and setting it to *Create Default Zones*, creates a dynamic interface by default.

SD-WAN does not support dynamic interfaces.

7. Click *OK*. The VPN community is created.



Edit VPN Community

Name: OL_INET

Description: Description

Topology: Dial up

Authentication: Pre-shared Key | Certificates

○ Generate (random)

● Specify ••••••••

Encryption

IKE Security (Phase 1) Properties

IKE Version: 1 | 2

#	Encryption	Authentication
1	AES128	SHA256
2	AES256	SHA256

IPsec Security (Phase 2) Properties

#	Encryption	Authentication
1	AES128	SHA256
2	AES256	SHA256

VPN Zone: OFF

IKE Security Phase 1 Advanced Properties

Diffie-Hellman Group(s)

□1	□2	☑5	☑14	□15	□16
□17	□18	□19	□20	□21	□27
□28	□29	□30	□31	□32	

Similarly, create another VPN community called *OL_MPLS* for the MPLS network.

Adding nodes to VPN communities

Once we have created the *OL_INET* and *OL_MPLS* VPN communities, we need to add hub and spoke nodes to both these communities. The datacenter will act as a hub and the branches will act as spokes.

To add a branch to the *OL_INET* VPN community from the GUI:

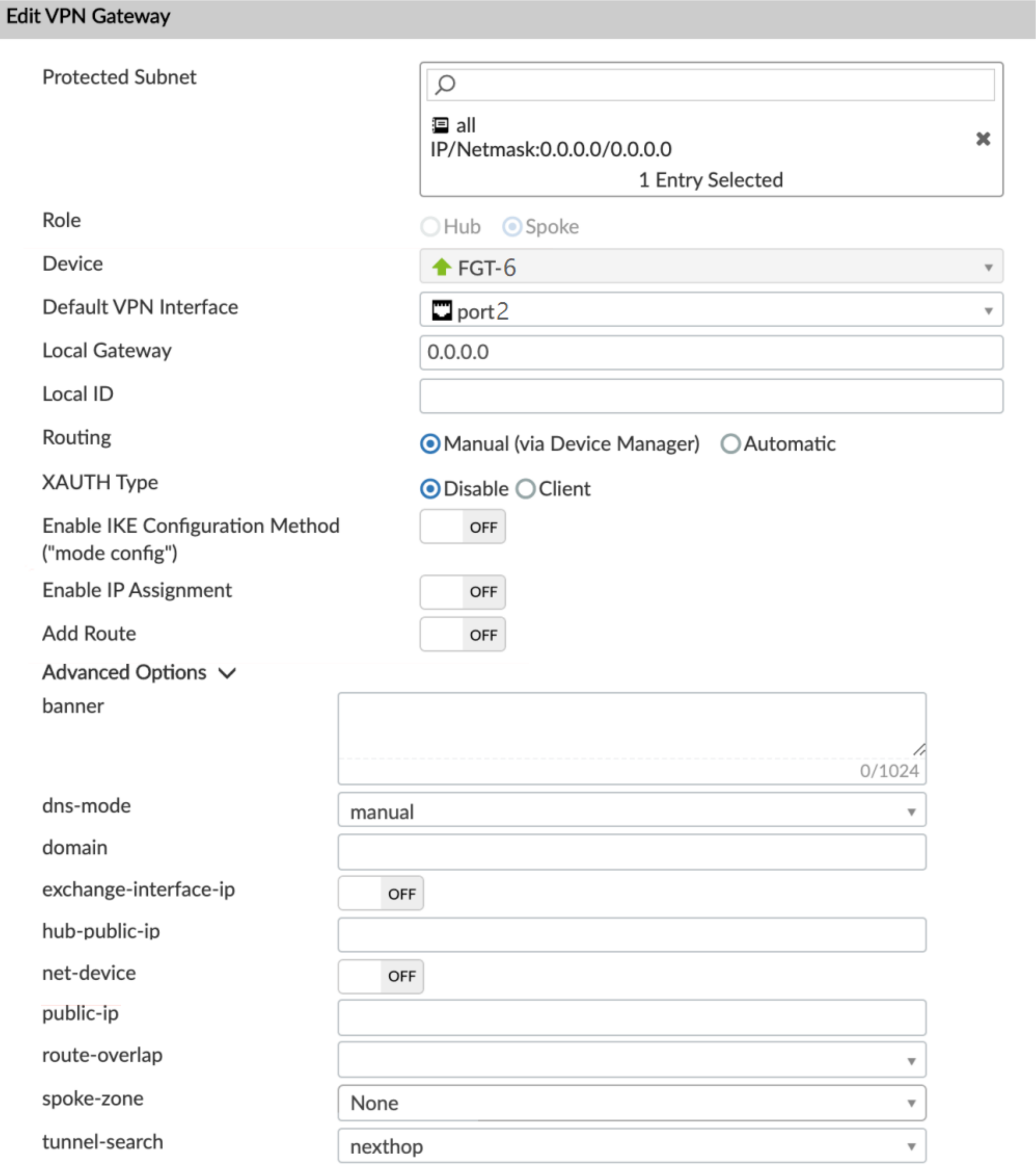
1. Go to *VPN Manager* > *IPsec VPN*.
2. In the tree menu, click *OL_INET*.
3. In the toolbar, click *Create New* > *Managed Gateway*. The *VPN Gateway Setup Wizard - OL_INET* dialog appears.
4. Select a *Protected Subnet*, and click *OK*.
5. Set the *Role* field to *Spoke*.

6. Select a branch FortiGate from the *Device* dropdown, and click *Next*.
7. Complete the setup as required in the wizard.

While completing the managed gateway setup:

- Ensure to toggle *Enable IP Assignment* to *OFF*.
- Ensure to toggle *Add Route* to *OFF*.
- Under *Advanced Options*, ensure to toggle *net-device* to *OFF*, and set the *tunnel-search* setting to *nexthop*.

8. Click *OK*. The branch is added to the *OL_INET* VPN community.



Edit VPN Gateway

Protected Subnet	all IP/Netmask:0.0.0.0/0.0.0.0 1 Entry Selected
Role	○ Hub ● Spoke
Device	FGT-6
Default VPN Interface	port2
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	0/1024
dns-mode	manual
domain	
exchange-interface-ip	OFF
hub-public-ip	
net-device	OFF
public-ip	
route-overlap	
spoke-zone	None
tunnel-search	nexthop

Similarly, add the other branch to the *OL_INET* VPN community.

To add a hub to the *OL_INET* VPN community from the GUI:

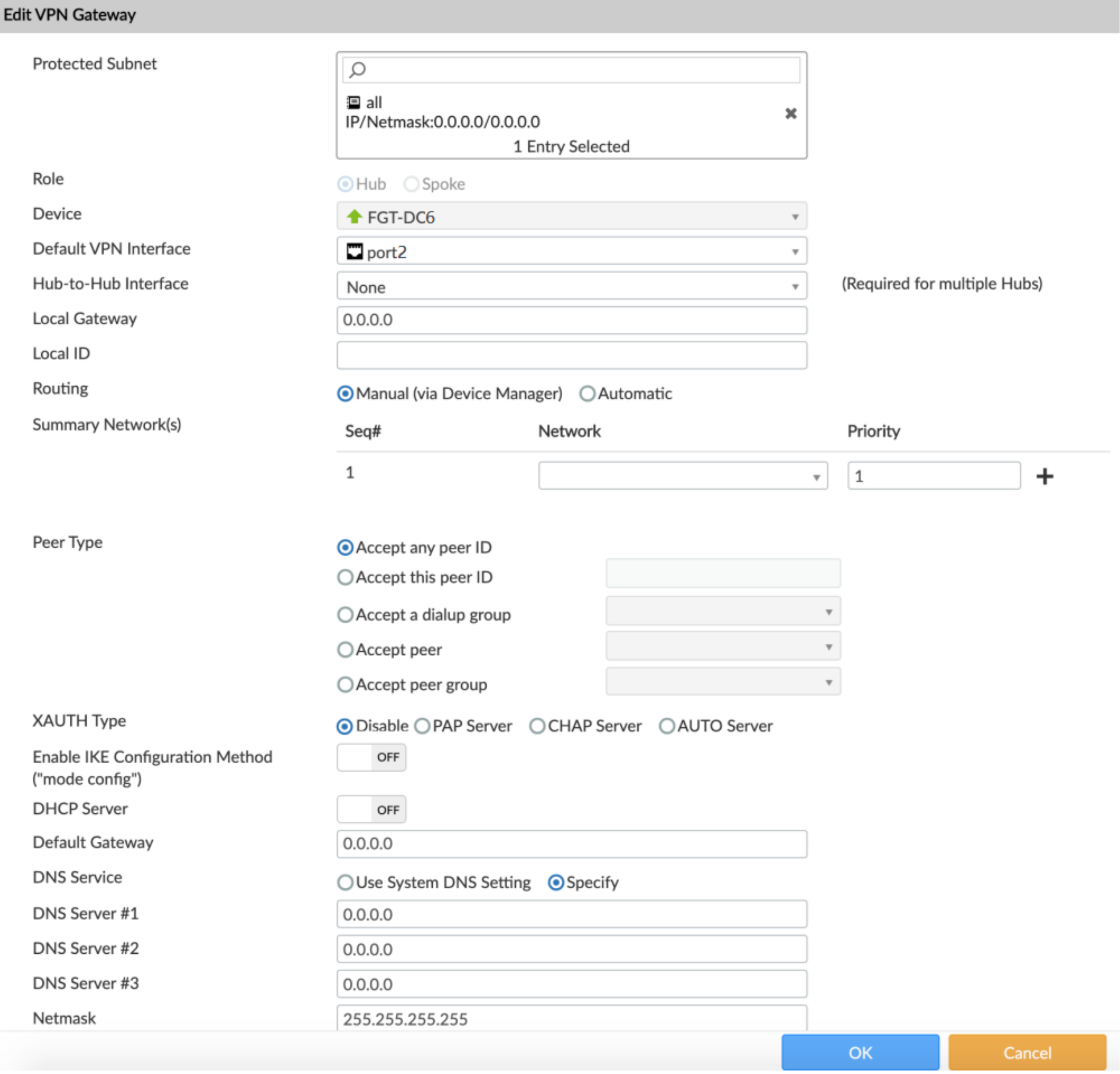
1. Go to *VPN Manager > IPsec VPN*.
2. In the tree menu, click *OL_INET*.

3. In the toolbar, click *Create New > Managed Gateway*. The *VPN Gateway Setup Wizard - OL_INET* dialog appears.
4. Select a *Protected Subnet*, and click *OK*.
5. Set the *Role* field to *Hub*.
6. Select the datacenter FortiGate from the *Device* dropdown, and click *Next*.
7. Complete the setup as required in the wizard.

While completing the managed gateway setup:

- Ensure to select *Accept any peer ID* for *Peer Type*.
- Ensure to toggle both *Enable IKE Configuration Method* and *DHCP Server* settings to *OFF*.
- Under *Advanced Options*, ensure to toggle *net-device* to *OFF*, and set the *tunnel-search* setting to *nexthop*.

8. Click *OK*. The hub is added to the *OL_INET* VPN community.



Edit VPN Gateway

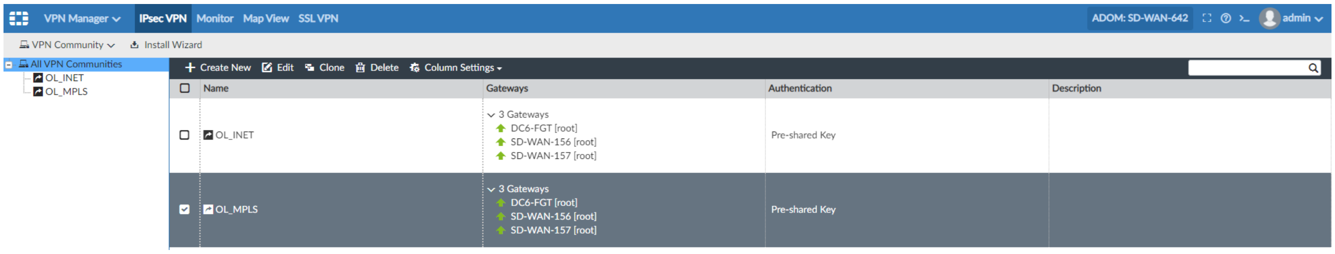
Protected Subnet	all IP/Netmask:0.0.0.0/0.0.0.0 ✖ 1 Entry Selected
Role	● Hub ○ Spoke
Device	FGT-DC6
Default VPN Interface	port2
Hub-to-Hub Interface	None (Required for multiple Hubs)
Local Gateway	0.0.0.0
Local ID	
Routing	● Manual (via Device Manager) ○ Automatic
Summary Network(s)	

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

Once you have added both the branches and the hub to the *OL_INET* VPN community, do the same for *OL_MPLS* VPN community as well.

Once you have configured the *VPN Manager*, your configuration should appear as follows:



	Name	Gateways	Authentication	Description
□	OL_INET	3 Gateways DC6-FGT [root] SD-WAN-156 [root] SD-WAN-157 [root]	Pre-shared Key	
☑	OL_MPLS	3 Gateways DC6-FGT [root] SD-WAN-156 [root] SD-WAN-157 [root]	Pre-shared Key	

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

Branch FGT-6

```
config vpn ipsec phase1-interface
   edit "OL_MPLS_0"
      set interface "port3"
      set ike-version 2
      set comments "[created by FMG VPN Manager]"
      set proposal aes128-sha256 aes256-sha256
      set keylife 28800
      set peertype any
      set remote-gw 172.20.9.5
      set net-device disable
      set psksecret ENC ***
   next
      edit "OL_INET_0"
      set interface "port2"
      set ike-version 2
      set comments "[created by FMG VPN Manager]"
      set proposal aes128-sha256 aes256-sha256
      set keylife 28800
      set peertype any
      set remote-gw 172.20.10.5
      set net-device disable
      set psksecret ENC ***
   next
end
```

Branch FGT-7

Similar configuration as FGT-6

Datacenter DC-6

```
config vpn ipsec phase1-interface
   edit "OL_MPLS_0"
      set type dynamic
      set interface "port3"
      set ike-version 2
      set dpd on-idle
      set comments "[created by FMG VPN Manager]"
      set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
           chacha20poly1305-prfsha256
      set keylife 28800
```

```
     set peertype any
     set dpd-retryinterval 60
     set net-device disable
     set tunnel-search nexthop
     set add-route disable
     set psksecret ENC ***
   next
     edit "OL_INET_0"
     set type dynamic
     set interface "port2"
     set ike-version 2
     set dpd on-idle
     set comments "[created by FMG VPN Manager]"
     set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
           chacha20poly1305-prfsha256
     set keylife 28800
     set peertype any
     set dpd-retryinterval 60
     set net-device disable
     set tunnel-search nexthop
     set add-route disable
     set psksecret ENC ***
   next
end
```

Mapping underlay interfaces

We need to create normalized interfaces to map the overlay links to the underlay links. Normalized interfaces allows the new interfaces to be used when creating policies.

Create the following normalized interfaces:

- OL_INET_0
- OL_MPLS_0

Normalized interfaces for the following ports should have been created by default when you imported the policy package from FortiGate:

- Port10
- Port2
- Port3

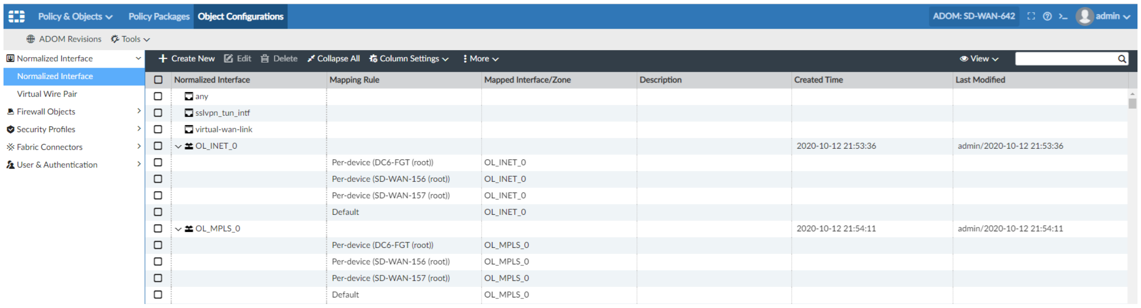
To create a normalized interface:

1. Go to *Policy & Objects* > *Object Configurations*.
2. In the tree menu, go to *Normalized Interface* > *Normalized Interface*.
3. In the toolbar, click *Create New*. The *Create New Normalized Interface* dialog box is displayed.
4. In the *Name* box, type *OL_INET_0* for the normalized interface.
5. Under *Per-Device Mapping*, click *Create New*. The *Per-Device Mapping* dialog box is displayed.
    a. In the *Mapped Device* list, select a device.
    b. In the *Mapped Interface Name* list, select an interface.
    c. Click *OK*.
       The mapped interface is added.

- **d.** Repeat this procedure to add a mapping for each device.

6. Click *OK*.
The normalized interface is created.

7. Repeat this procedure to create a normalized interface named *OL_MPLS_0*.
You can use the mapped interfaces in policies.



	Normalized Interface	Mapping Rule	Mapped Interface/Zone	Description	Created Time	Last Modified
□	any					
□	sslvpn_tun_intf					
□	virtual-wan-link					
□	OL_INET_0				2020-10-12 21:53:36	admin/2020-10-12 21:53:36
□		Per-device (DC6-FGT (root))	OL_INET_0			
□		Per-device (SD-WAN-156 (root))	OL_INET_0			
□		Per-device (SD-WAN-157 (root))	OL_INET_0			
□		Default	OL_INET_0			
□	OL_MPLS_0				2020-10-12 21:54:11	admin/2020-10-12 21:54:11
□		Per-device (DC6-FGT (root))	OL_MPLS_0			
□		Per-device (SD-WAN-156 (root))	OL_MPLS_0			
□		Per-device (SD-WAN-157 (root))	OL_MPLS_0			
□		Default	OL_MPLS_0			

Creating policy packages

Create the following policy packages to install on the FortiGates:

- Policy package for the hub
- Policy package for the branches

After you create policy packages, you'll add firewall policies to each policy package.

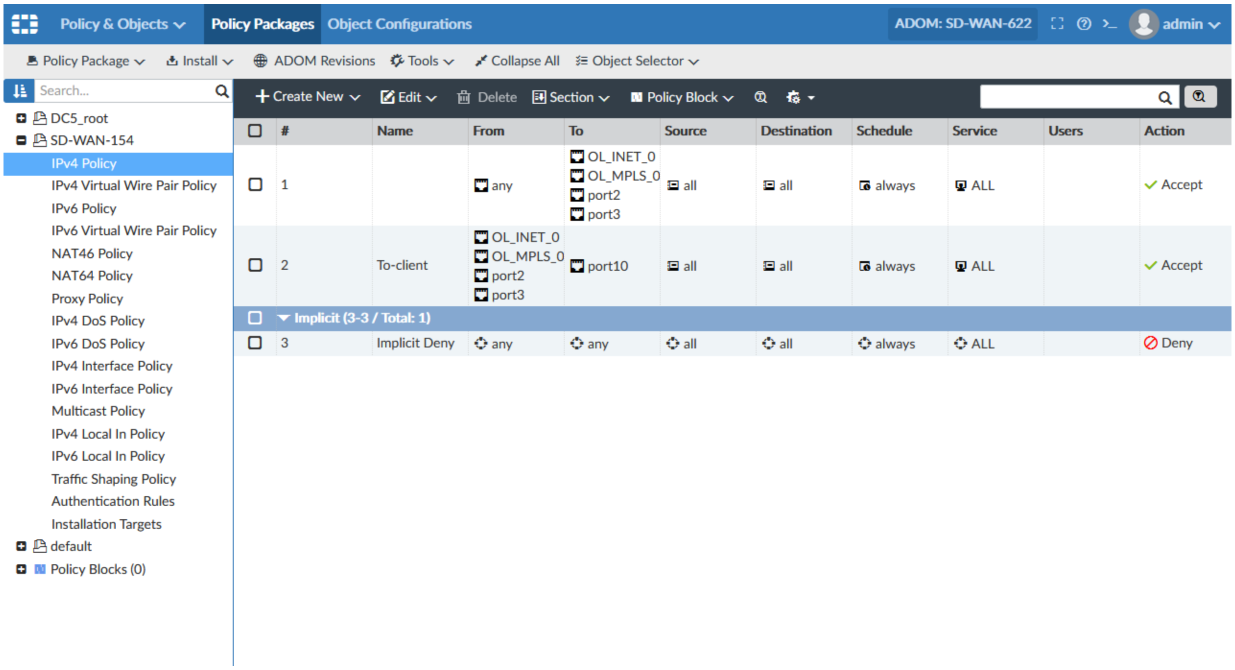
To create a policy package:

1. Go to *Policy & Objects* > *Policy Packages*.
2. In the toolbar, click *Policy Package* > *New*.
3. In the *Name* box, type *DC6*, and click *OK*.
4. Repeat this procedure to create a policy package named *SD-WAN-156* for branches.

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 add firewall policies to policy packages:

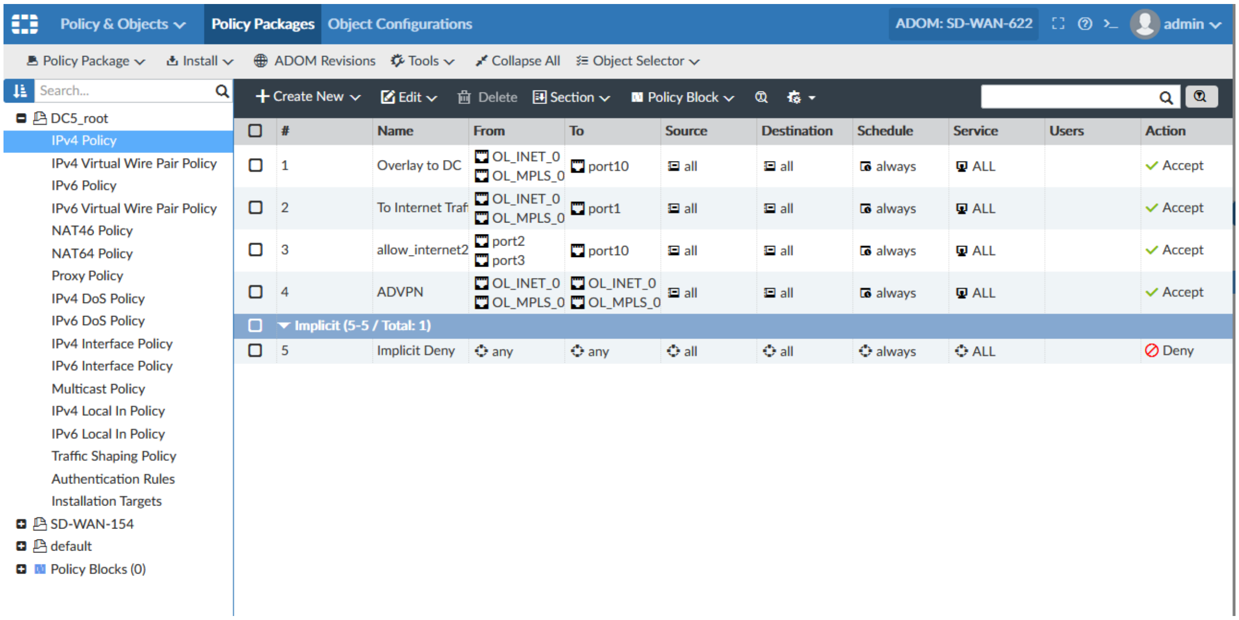
1. Go to *Policy & Objects* > *Policy Packages*.
2. In the tree menu, select a policy package.
3. In the content pane, click *Create New*. By default, policies will be added to the bottom of the list, but above the *Implicit* policy.
4. Configure the firewall policy settings, and click *OK*.
   Create 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 DC
- 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 21

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.

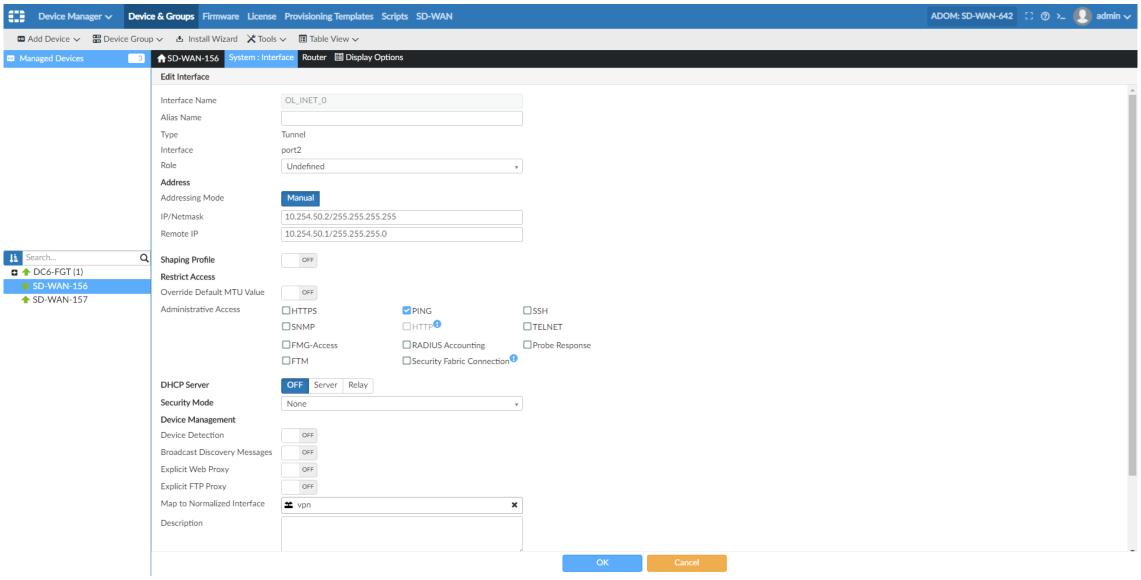
Configuring tunnel interfaces and dynamic mapping

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 21See Fixing the settings in the policy package on page 23.

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.



Edit Interface

Interface Name: OL_INET_0

Alias Name:

Type: Tunnel

Interface: port2

Role: Undefined

Address

Addressing Mode: Manual

IP/Netmask: 10.254.50.2/255.255.255.255

Remote IP: 10.254.50.1/255.255.255.0

Shaping Profile: OFF

Restrict Access

Override Default MTU Value: OFF

Administrative Access: □HTTPS ☑PING □SSH □SNMP □HTTP □TELNET □FMG-Access □RADIUS Accounting □Probe Response □FTM □Security Fabric Connection

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

Map to Normalized Interface: vpn

Description:

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.

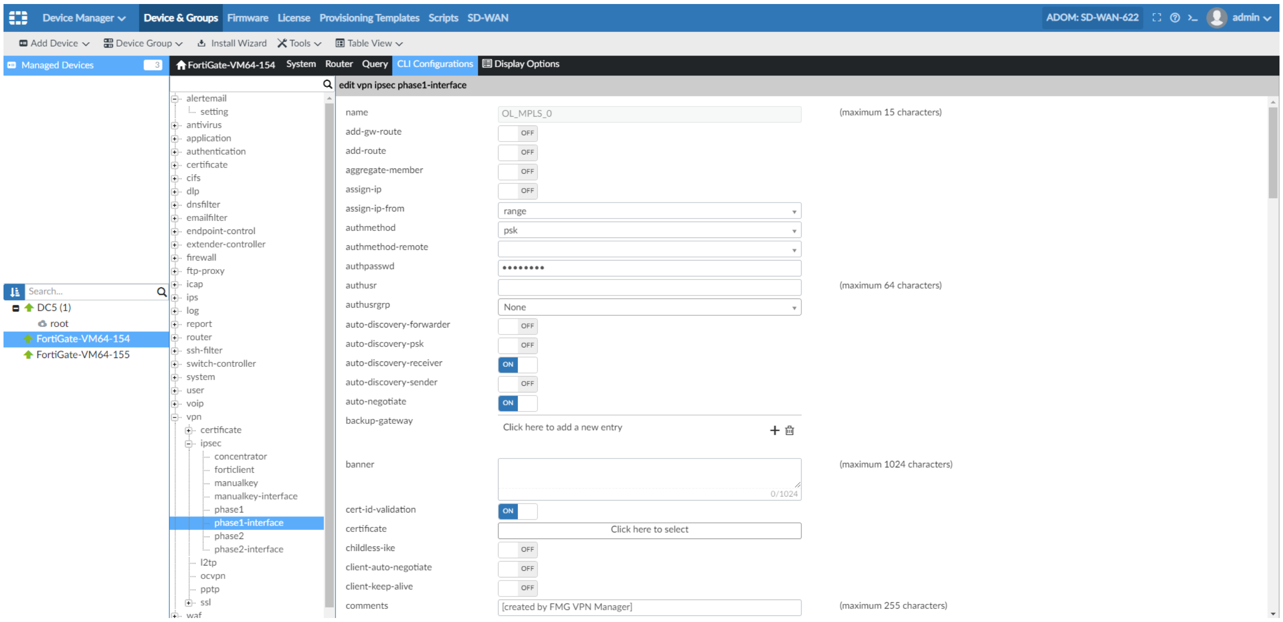
To enable CLI configurations:

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.

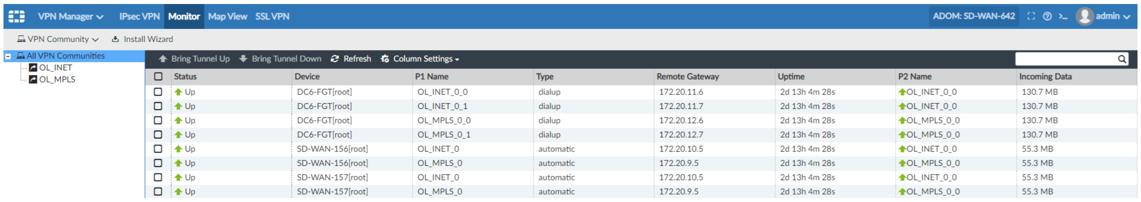


edit vpn ipsec phase1-interface

name	OL_MPLS_0	(maximum 15 characters)
add-gw-route	OFF	
add-route	OFF	
aggregate-member	OFF	
assign-ip	OFF	
assign-ip-from	range	
authmethod	psk	
authmethod-remote		
authpasswd	••••••••	
authusr		(maximum 64 characters)
authusrgrp	None	
auto-discovery-forwarder	OFF	
auto-discovery-psk	OFF	
auto-discovery-receiver	ON	
auto-discovery-sender	OFF	
auto-negotiate	ON	
backup-gateway	Click here to add a new entry	
banner	0/1024	(maximum 1024 characters)
cert-id-validation	ON	
certificate	Click here to select	
childless-ike	OFF	
client-auto-negotiate	OFF	
client-keep-alive	OFF	
comments	[created by FMG VPN Manager]	(maximum 255 characters)

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
□	Up	DC6-FGT[root]	OL_INET_0_0	dialup	172.20.11.6	2d 13h 4m 28s	OL_INET_0_0	130.7 MB
□	Up	DC6-FGT[root]	OL_INET_0_1	dialup	172.20.11.7	2d 13h 4m 28s	OL_INET_0_0	130.7 MB
□	Up	DC6-FGT[root]	OL_MPLS_0_0	dialup	172.20.12.6	2d 13h 4m 28s	OL_MPLS_0_0	130.7 MB
□	Up	DC6-FGT[root]	OL_MPLS_0_1	dialup	172.20.12.7	2d 13h 4m 28s	OL_MPLS_0_0	130.7 MB
□	Up	SD-WAN-156[root]	OL_INET_0	automatic	172.20.10.5	2d 13h 4m 28s	OL_INET_0_0	55.3 MB
□	Up	SD-WAN-156[root]	OL_MPLS_0	automatic	172.20.9.5	2d 13h 4m 28s	OL_MPLS_0_0	55.3 MB
□	Up	SD-WAN-157[root]	OL_INET_0	automatic	172.20.10.5	2d 13h 4m 28s	OL_INET_0_0	55.3 MB
□	Up	SD-WAN-157[root]	OL_MPLS_0	automatic	172.20.9.5	2d 13h 4m 28s	OL_MPLS_0_0	55.3 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.

Configuring dynamic routing involves the following steps:

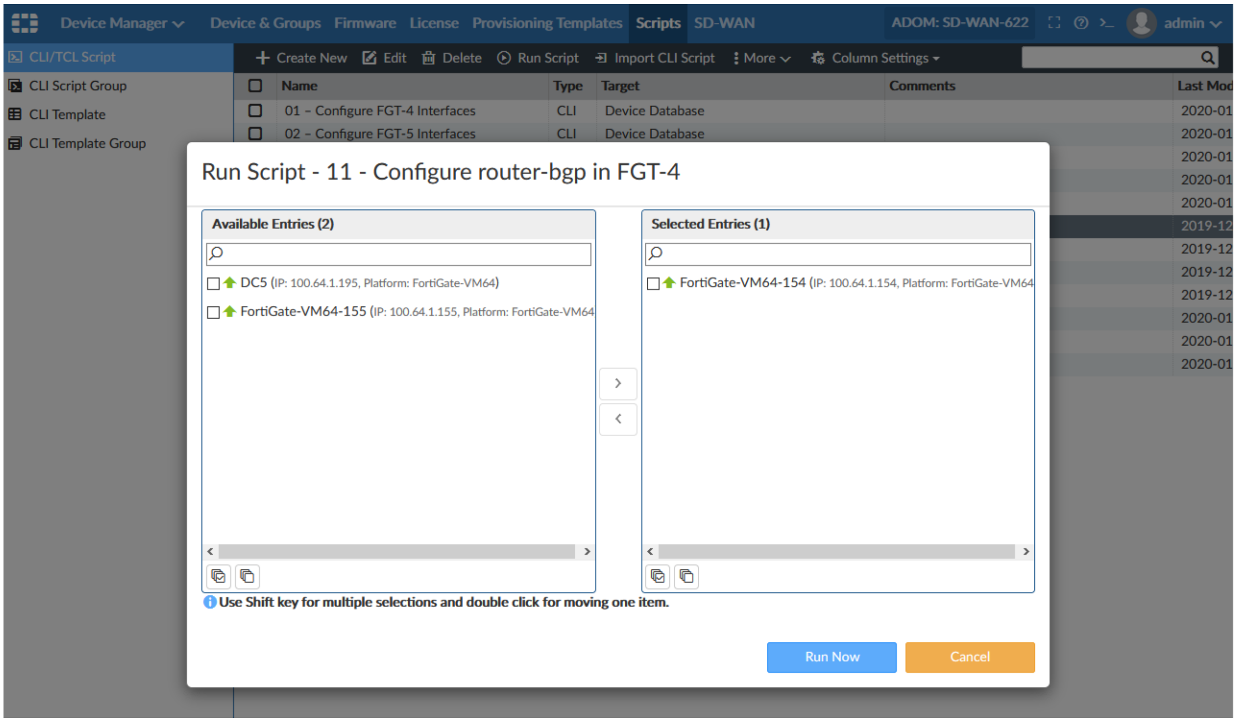
1. Configuring the router-bgp on the branches on page 25.
2. Configuring the router BGP on the hub on page 26.
3. Verifying the BGP routes on page 28.
4. Configuring the ADVPN policy route on the FortiGate hub on page 29.

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*.



01 - Configure FGT-4 Interfaces CLI Device Database 2020-01

02 - Configure FGT-5 Interfaces CLI Device Database 2020-01

Run Script - 11 - Configure router-bgp in FGT-4

Available Entries (2)

□ DC5 (IP: 100.64.1.195, Platform: FortiGate-VM64)

□ FortiGate-VM64-155 (IP: 100.64.1.155, Platform: FortiGate-VM64

Selected Entries (1)

□ FortiGate-VM64-154 (IP: 100.64.1.154, Platform: FortiGate-VM64

Use Shift key for multiple selections and double click for moving one item.

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
```

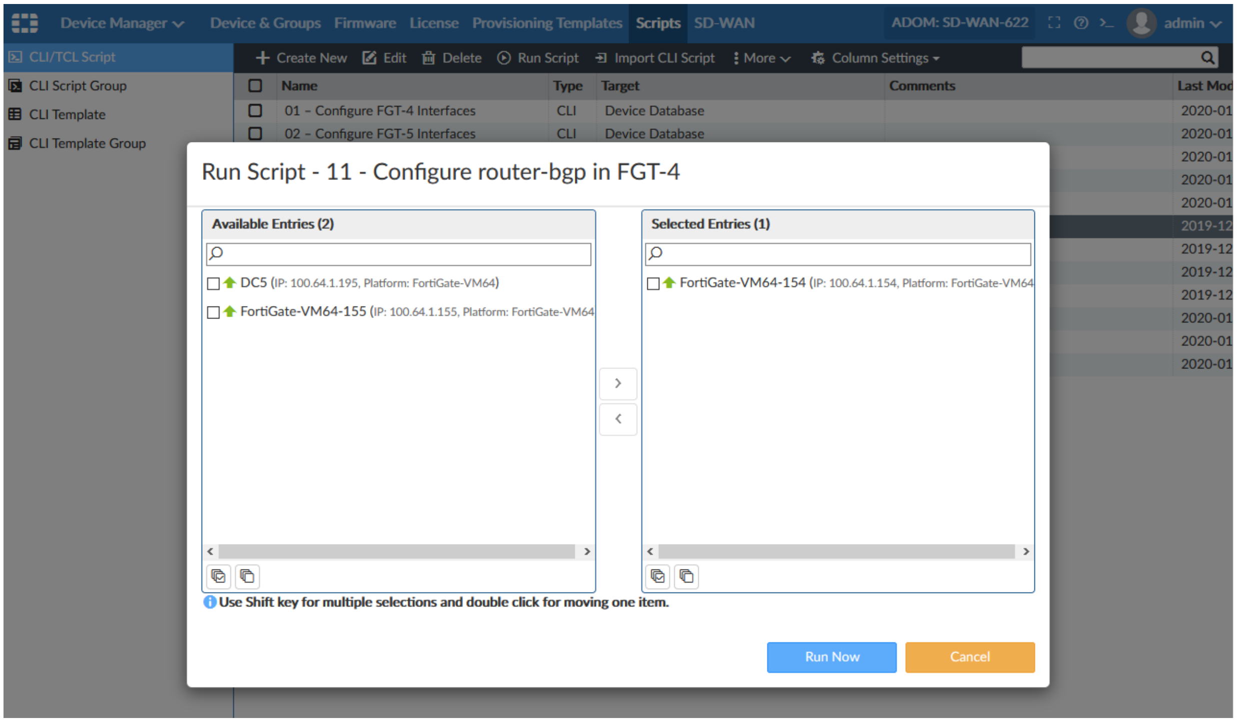
Configuring the router BGP on the hub

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*.



Name	Type	Target	Comments	Last Mod
01 – Configure FGT-4 Interfaces	CLI	Device Database		2020-01
02 – Configure FGT-5 Interfaces	CLI	Device Database		2020-01

Run Script - 11 - Configure router-bgp in FGT-4

Available Entries (2):

- DC5 (IP: 100.64.1.195, Platform: FortiGate-VM64)
- FortiGate-VM64-155 (IP: 100.64.1.155, Platform: FortiGate-VM64

Selected Entries (1):

- FortiGate-VM64-154 (IP: 100.64.1.154, Platform: FortiGate-VM64

Use Shift key for multiple selections and double click for moving one item.

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, configure SD-WAN for branches. Configuring SD-WAN involves the following steps:

1. Enabling central management on page 30.
2. Creating SD-WAN interface members on page 30.

3. Creating health-check servers on page 32.
4. Creating SD-WAN templates on page 32.
5. Adding SD-WAN zones to policies on page 34.

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*.
2. Double-click the ADOM to open it for editing.
3. Next to *Central Management*, select *SD-WAN*, and click *OK*.

Creating SD-WAN interface members

Create the following SD-WAN interface members:

- OL_MPLS
- OL_INET
- port2
- port3

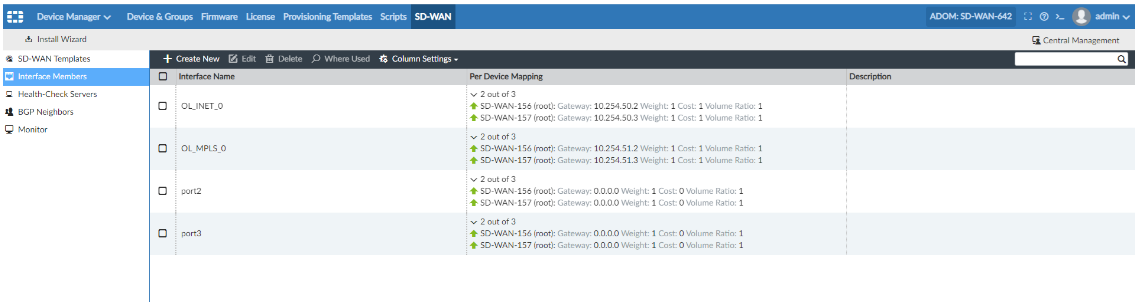
Keep the following considerations in mind:

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

To add SD-WAN interface members:

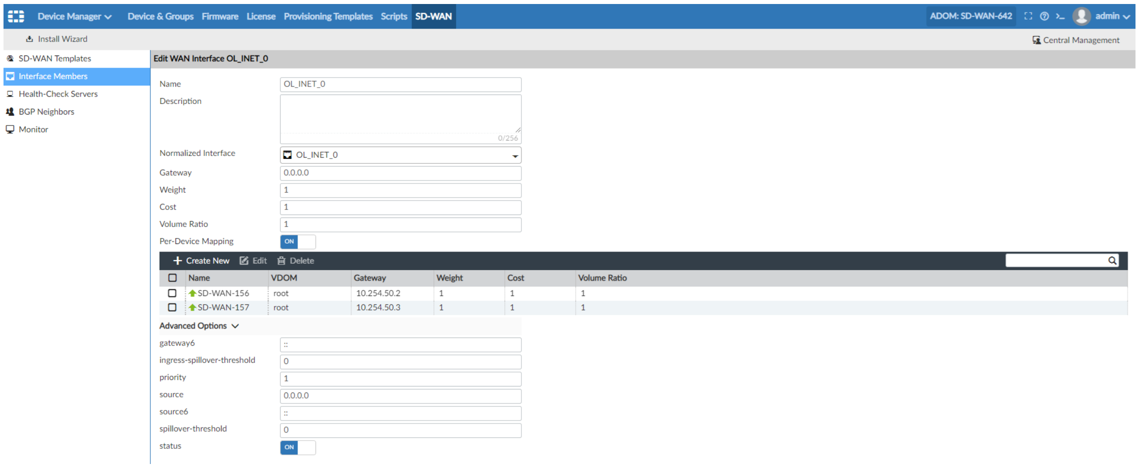
1. Go to *Device Manager* > *SD-WAN*.
2. In the tree menu, click *Interface Members*.
3. In the toolbar, click *Create New*.
   The *Create New WAN Interface* pane opens.
4. In the *Name* box, type a name for the interface, such as *OL_MPLS_0*.

5. In the *Normalized Interface* list, select the normalized interface.
6. Toggle *Per-Device Mapping* to *ON*.
7. Add per-device mappings:
   a. Under *Per-Device Mapping*, click *Create New*.
   b. In the *Mapped Device* list, select a device.
   c. In the *Gateway* box, type the remote gateway.
   d. Under *Advanced Options*, set *priority*.
   e. Click *OK*.
   The per-device mapping is added.
   f. Repeat this step to add all devices.
8. Expand *Advanced Options*, and set *priority*.
9. Click *OK*.
   The interface member is added.
10. Repeat this procedure to add all the interface members.



□	Interface Name	Per Device Mapping	Description
□	OL_INET_0	2 out of 3 SD-WAN-156 (root): Gateway: 10.254.50.2 Weight: 1 Cost: 1 Volume Ratio: 1 SD-WAN-157 (root): Gateway: 10.254.50.3 Weight: 1 Cost: 1 Volume Ratio: 1	
□	OL_MPLS_0	2 out of 3 SD-WAN-156 (root): Gateway: 10.254.51.2 Weight: 1 Cost: 1 Volume Ratio: 1 SD-WAN-157 (root): Gateway: 10.254.51.3 Weight: 1 Cost: 1 Volume Ratio: 1	
□	port2	2 out of 3 SD-WAN-156 (root): Gateway: 0.0.0.0 Weight: 1 Cost: 0 Volume Ratio: 1 SD-WAN-157 (root): Gateway: 0.0.0.0 Weight: 1 Cost: 0 Volume Ratio: 1	
□	port3	2 out of 3 SD-WAN-156 (root): Gateway: 0.0.0.0 Weight: 1 Cost: 0 Volume Ratio: 1 SD-WAN-157 (root): Gateway: 0.0.0.0 Weight: 1 Cost: 0 Volume Ratio: 1	

OL_INET_0 configuration:



Edit WAN Interface OL_INET_0

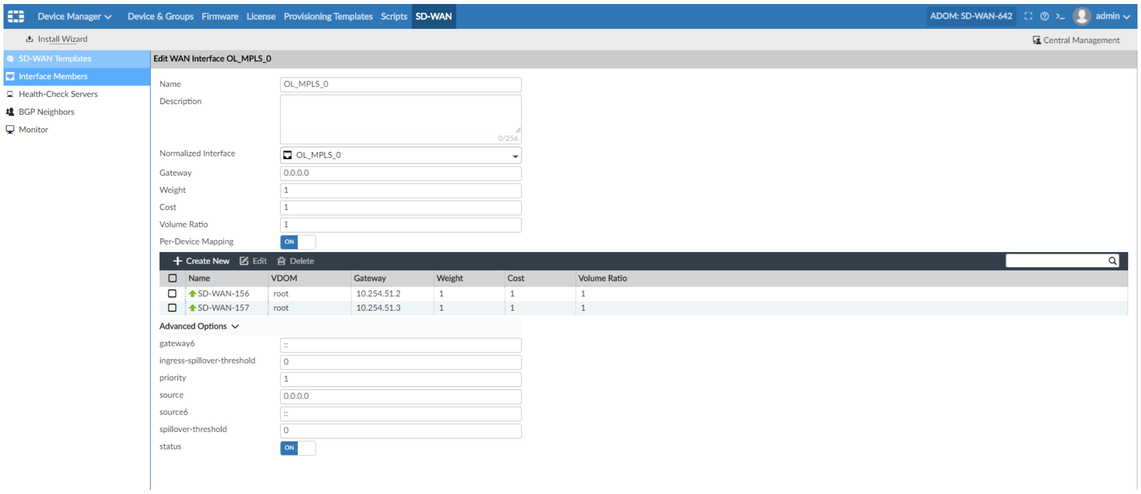
Name	OL_INET_0
Description	0/256
Normalized Interface	OL_INET_0
Gateway	0.0.0.0
Weight	1
Cost	1
Volume Ratio	1
Per-Device Mapping	ON

□	Name	VDOM	Gateway	Weight	Cost	Volume Ratio
□	SD-WAN-156	root	10.254.50.2	1	1	1
□	SD-WAN-157	root	10.254.50.3	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:



Edit WAN Interface OL_MPLS_0

Name	OL_MPLS_0
Description	0/256
Normalized Interface	OL_MPLS_0
Gateway	0.0.0.0
Weight	1
Cost	1
Volume Ratio	1
Per-Device Mapping	ON

☐	Name	VDOM	Gateway	Weight	Cost	Volume Ratio
☐	SD-WAN-156	root	10.254.51.2	1	1	1
☐	SD-WAN-157	root	10.254.51.3	1	1	1

Advanced Options

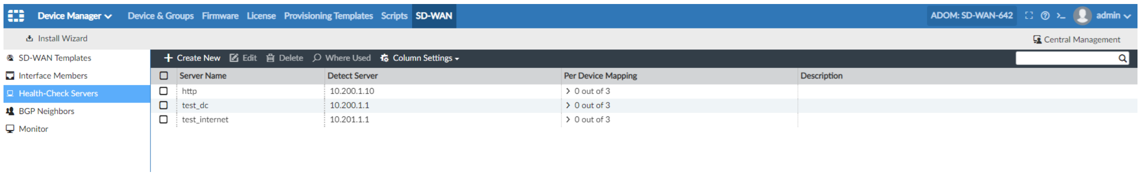
gateway6	::
ingress-spillover-threshold	0
priority	1
source	0.0.0.0
source6	::
spillover-threshold	0
status	ON

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*.



☐	Server Name	Detect Server	Per Device Mapping	Description
☐	http	10.200.1.10	0 out of 3	
☐	test_dc	10.200.1.1	0 out of 3	
☐	test_internet	10.201.1.1	0 out of 3	

Creating SD-WAN templates

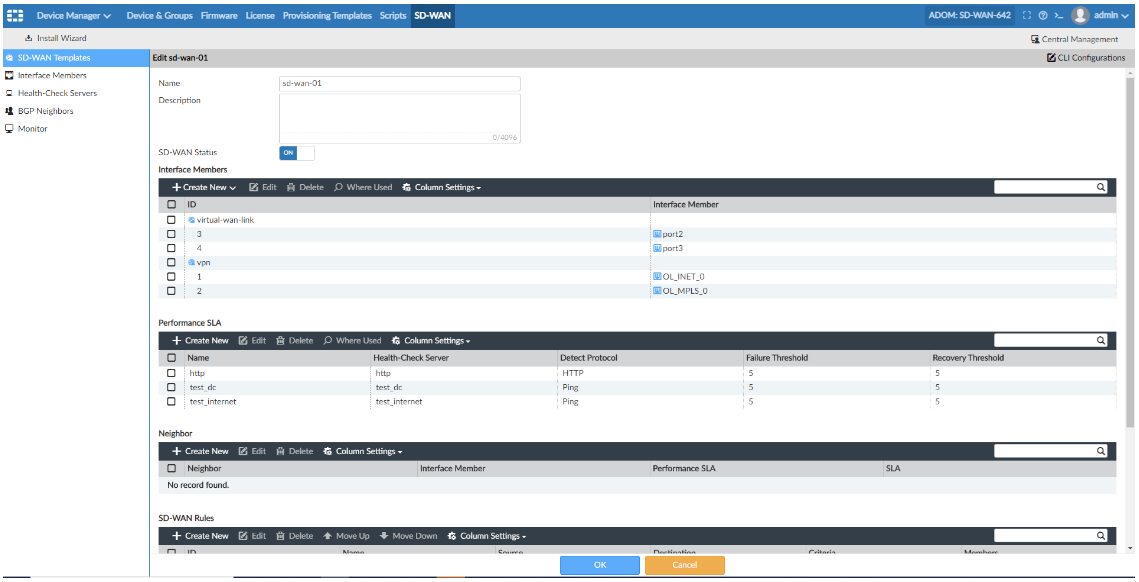
Create an SD-WAN template with the following zones and interface members for branch devices:

Zone	Interface members
virtual-wan-link	port2 port3
vpn	OL_INET_0 OL_MPLS_0

After you create the template, assign the template to the branch devices.

To create an SD-WAN template for branch devices:

1. Go to *Device Manager > SD-WAN > SD-WAN Template*.
2. In the toolbar, click *Create New*. The *Create New* page opens.
3. In the *Name* box, type a name for the template, such as *sd-wan-01*.
4. Create an SD-WAN zone named *vpn*:
   a. Under *Interface Members*, click *Create New > SD-WAN Zone*.
   b. In the *Name* box, type a name, such as *VPN*, and click *OK*.
      The zone is created
5. Add SD-WAN members to the *vpn* zone:
   a. Under *Interface Members*, click *Create New > SD-WAN Member*.
   b. In the *Sequence Number* box, type a number for the interface.
   c. In the *Interface Member* box, select the interface member, such as *OL_INET_0*.
   d. In the *SD-WAN Zone* box, select *vpn*, and click *OK*.
      The interface member is added to the zone.
   e. Repeat this procedure to add the *OL_MPLS_0* interface member to the zone.
6. Add the following SD-WAN members to the virtual-wan-link zone: *port2*, *port3*.



Edit sd-wan-01

Name: sd-wan-01

Description: 0/4096

SD-WAN Status: ON

Interface Members

ID	Interface Member
virtual-wan-link	
3	port2
4	port3
vpn	
1	OL_INET_0
2	OL_MPLS_0

Performance SLA

Name	Health-Check Server	Detect Protocol	Failure Threshold	Recovery Threshold
http	http	HTTP	5	5
test_dc	test_dc	Ping	5	5
test_internet	test_internet	Ping	5	5

Neighbor

Neighbor	Interface Member	Performance SLA	SLA
No record found.			

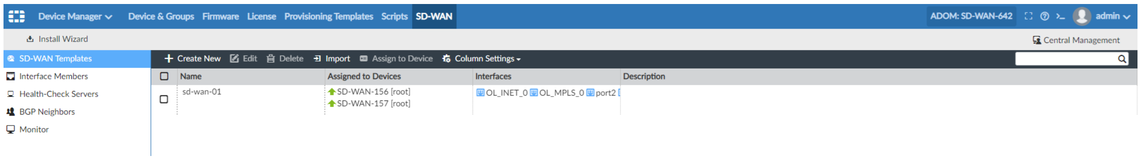
SD-WAN Rules

ID	Name	Source	Destination	Criteria	Members

7. Click *OK* to save the template.

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*.



Name	Assigned to Devices	Interfaces	Description
sd-wan-01	SD-WAN-156 [root] SD-WAN-157 [root]	OL_INET_0 OL_MPLS_0 port2	

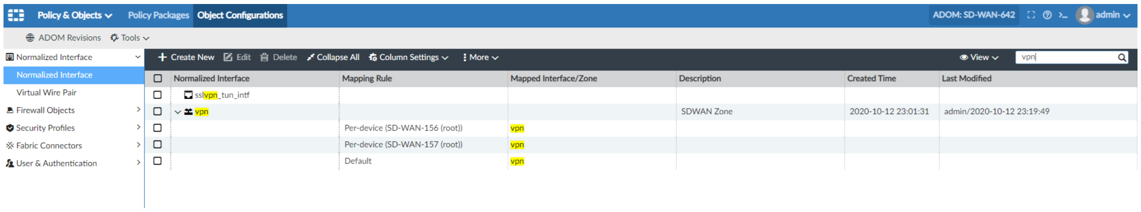
Adding SD-WAN zones to policies

You can select SD-WAN zones in a policy. However, you cannot select SD-WAN interface members in a policy.

When you create an SD-WAN zone on the *Device Manager* > *SD-WAN* pane, a normalized interface should be automatically created on the *Policy & Objects* > *Object Configurations* > *Normalized Interfaces* pane. The description identifies it as an *SD-WAN Zone*.

To view normalized interfaces for SD-WAN zones:

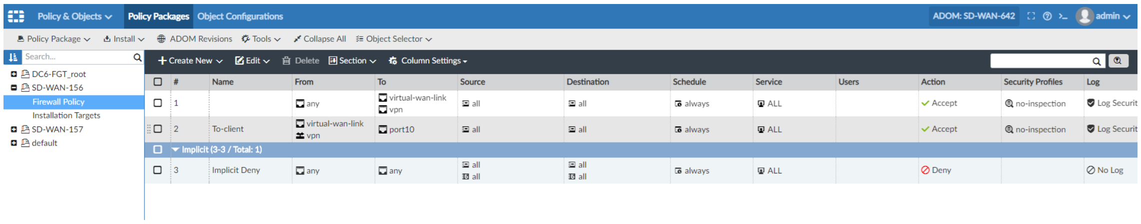
1. Go to *Policy & Objects* > *Object Configurations*.
2. In the tree menu, go to *Normalized Interface* > *Normalized Interface*.
   The normalized interface named *vpn* is displayed that you created on the *Device Manager* > *SD-WAN* pane.



☐	Normalized Interface	Mapping Rule	Mapped Interface/Zone	Description	Created Time	Last Modified
☐	sslvpn_tun_intf					
☐	vpn			SDWAN Zone	2020-10-12 23:01:31	admin/2020-10-12 23:19:49
☐		Per-device (SD-WAN-156 (root))	vpn			
☐		Per-device (SD-WAN-157 (root))	vpn			
☐		Default	vpn			

To add SD-WAN zones to policies:

1. Go to *Policy & Objects* > *Policy Packages*.
2. Expand the policy package, and click the firewall policy.
   The firewall policy displays in the content pane.
3. In the content pane, double-click the firewall policy to open it for editing, and add the SD-WAN zones.



☐	#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profiles	Log
☐	1		any	virtual-wan-link vpn	all	all	always	ALL		✓ Accept	no-inspection	Log Securit
☐	2	To-client	virtual-wan-link vpn	port10	all	all	always	ALL		✓ Accept	no-inspection	Log Securit
☐	Implicit (3-3 / Total: 1)											
☐	3	Implicit Deny	any	any	all all	all all	always	ALL		⊘ Deny		⊘ No Log

4. Install the policy package to branch devices.

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 in 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 to 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*.

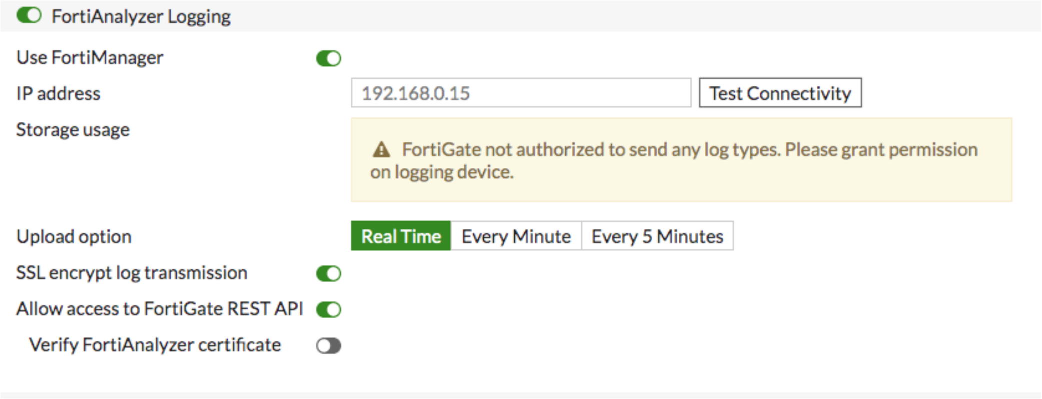
To enable FortiAnalyzer on the branches:

```
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: 192.168.0.15 [Test Connectivity]

Storage usage: ⚠ FortiGate not authorized to send any log types. Please grant permission on logging device.

Upload option: [✓ Real Time] Every Minute Every 5 Minutes

SSL encrypt log transmission

Allow access to FortiGate REST API

Verify FortiAnalyzer certificate

Run the following command on FortiManager CLI:

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

SD-WAN with ADVPN - dual hub

You can use the examples in this section with FortiManager 6.4.2 and later, which supports normalized interfaces and zones.

This section provides an example of configuring a dual hub SD-WAN topology with the following functionality:

- SD-WAN Zones
- SD-WAN for Internal Traffic (with ADVPN)
- SD-WAN for Internet Access (DIA / RIA)
- End-to-End Segmentation using VRFs on Hubs and Spokes
- ADVPN Shortcut Monitoring
- IKE Config Mode
- Reusable configuration using CLI Templates

This section includes the following topics about configuring SD-WAN with ADVPN for a dual hub deployment:

- Topology on page 37
- Naming conventions on page 38
- Adding FortiGate devices to FortiManager on page 39
- Creating underlay WAN links on page 43
- Configuring overlay connections on page 44
- Configuring dynamic routing on page 55
- Configuring SD-WAN for internal traffic on page 59
- Configuring SD-WAN for Internet traffic on page 67
- Interconnecting data centers on page 74

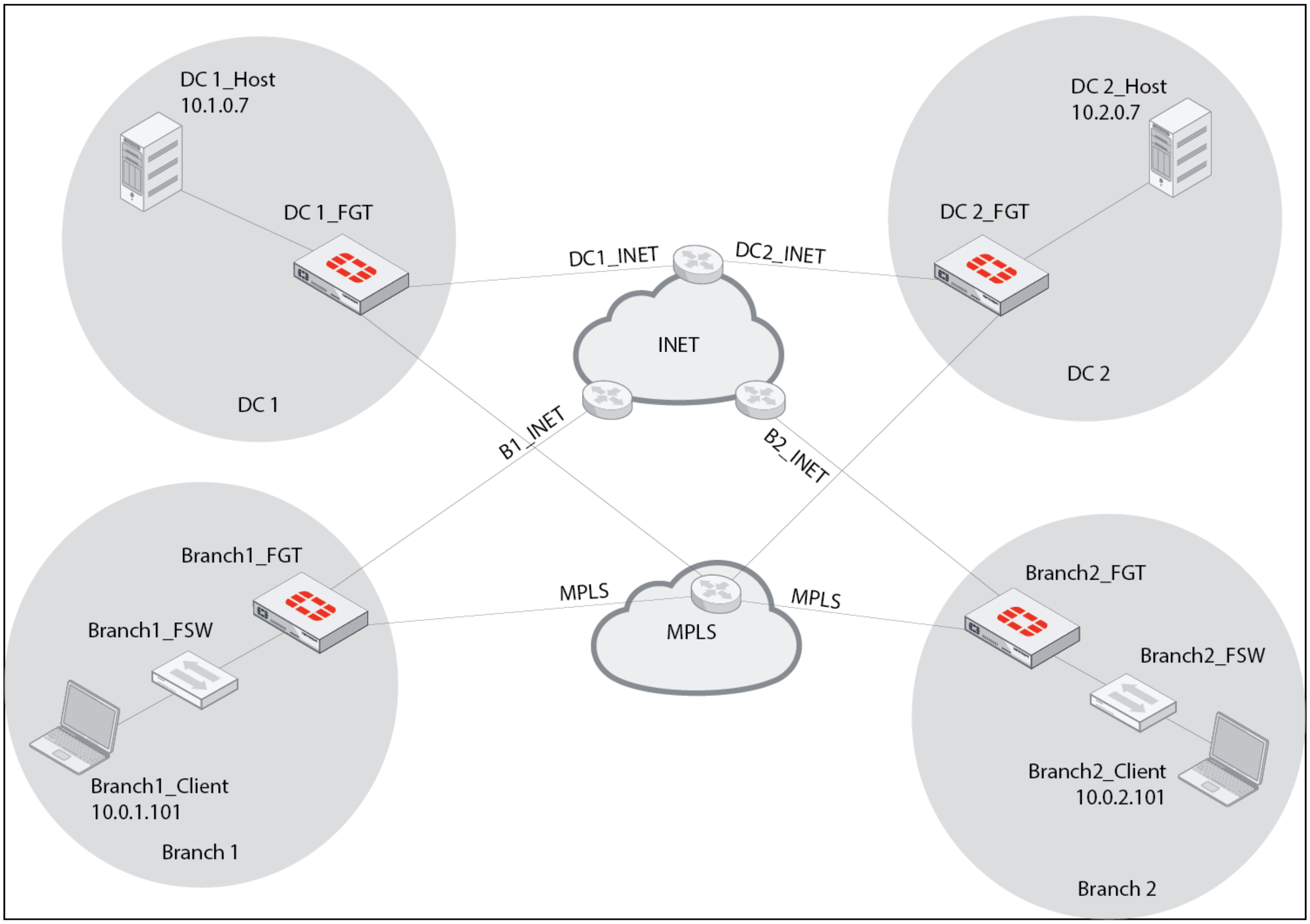
Topology

This example includes two FortiGates acting as hubs (DC1_Host and DC2_Host) and two FortiGates acting as spokes (Branch1_FGT and Branch2_FGT).

Each FortiGate has two underlay WAN links:

- INET: simulates a local Internet breakout on each FortiGate
- MPLS: simulates a private connection between branches and datacenters

Overlay networks will be built on top of the underlay WAN links.



Naming conventions

The examples in this guide often use the following variables:

Variable	Description	Value
ul-id	Underlay ID	1 for INET 2 for MPLS
branch-id	Branch ID	1 for Branch1 2 for Branch2
dc-id	Datacenter ID	1 for DC1 2 for DC2
overlay-id	Overlay ID	<ul-id><dc-id>

The `overlay-id` variable deserves a bit of an explanation. Because Spokes will build tunnels to each of the Hubs over each of the underlays, effectively we will have 4 separate overlay networks. And we will identify them by the combination of the other two variables (`<ul-id><dc-id>`):

Underlay	Hub	Overlay ID
INET	DC1_FGT	11
INET	DC2_FGT	12
MPLS	DC1_FGT	21
MPLS	DC2_FGT	22

As you will see, all these variables will be often used in naming and IP addressing, which will be particularly crucial when we define CLI templates.

To begin with, LAN subnets on each site are defined as follows:

Site Type	LAN Subnet
Branch	10.0.<branch-id>.0/24
DC	10.<dc-id>.0.0/24

Adding FortiGate devices to FortiManager

In this section, you will add two FortiGate devices to use for the datacenters and two FortiGate devices to use for the branch offices.

Adding FortiGate devices to FortiManager involves the following steps:

1. Creating device groups on page 39
2. Adding FortiGates to device groups on page 40
3. Retrieving FortiGate device configuration on page 41
4. Importing device policies and mapping interfaces on page 41
5. Creating meta fields on page 42
6. Setting meta field values for all FortiGates on page 43

Creating device groups

Create two device groups with the following names:

- *Hubs*
- *Spokes*

To create device groups:

1. Go to *Device Manager* > *Device & Groups*.
2. From the *Device Group* menu, select *Create New Group*.
3. In the *Group Name* box, type a name for the group, such as *Hubs*, and click *OK*.
4. Repeat this procedure, and create a device group named *Spokes*.

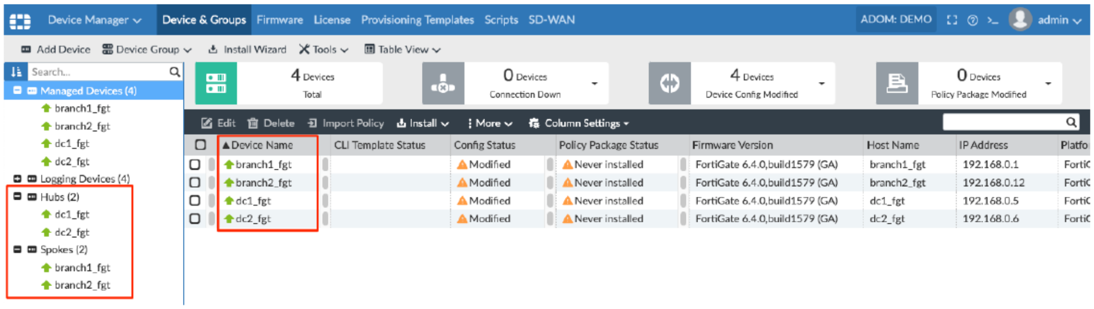
Adding FortiGates to device groups

Add each FortiGate to FortiManager by using the *Add Device* wizard and *Discover* mode. When you add FortiGates to FortiManager, you can name each device and add it to a device group. Name and add devices to the device groups as follows:

FortiGate	Device Group
dc1_fgt	Hubs
dc2_fgt	Hubs
branch1_fgt	Spokes
branch1_fgt	Spokes

To add FortiGate devices by using the *Discover* mode on FortiManager:

1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, click *Add Device*. The *Add Device* wizard opens.
3. Select *Discover*.
4. Enter the following information, and click *Next*. IP address, user name, and password for the first device, and click *Next*.
   a. In the *IP address* box, type the IP address for the device.
   b. In the *User Name* box, type the user name for the FortiGate.
   c. In the *Password* box, type the password for the FortiGate.
   The device is discovered, and you can specify additional details.
5. Complete the following options, and click *Next*.
   a. In the *Name* box, type a name for the device.
   b. In the *Add to Groups* box, select *Specify* and select the device group.
6. When prompted whether to import policies and objects, you can click *Import Later*.
   The device is added to FortiManager and displays in the device group.
7. Repeat this procedure to add all devices to FortiManager and a device group.



☐	Device Name	CLI Template Status	Config Status	Policy Package Status	Firmware Version	Host Name	IP Address	Platfo
☐	branch1_fgt		Modified	Never installed	FortiGate 6.4.0,build1579 (GA)	branch1_fgt	192.168.0.1	FortiG
☐	branch2_fgt		Modified	Never installed	FortiGate 6.4.0,build1579 (GA)	branch2_fgt	192.168.0.12	FortiG
☐	dc1_fgt		Modified	Never installed	FortiGate 6.4.0,build1579 (GA)	dc1_fgt	192.168.0.5	FortiG
☐	dc2_fgt		Modified	Never installed	FortiGate 6.4.0,build1579 (GA)	dc2_fgt	192.168.0.6	FortiG

Retrieving FortiGate device configuration

To retrieve the FortiGate device configuration settings:

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.

Importing device policies and mapping interfaces

When you import the policy from a FortiGate device, you can import all policies and objects or select policies and objects. All enabled FortiGate device interfaces are imported and mapped to a normalized interface, and you can choose whether to import and map unused interfaces.

To import FortiGate device policies:

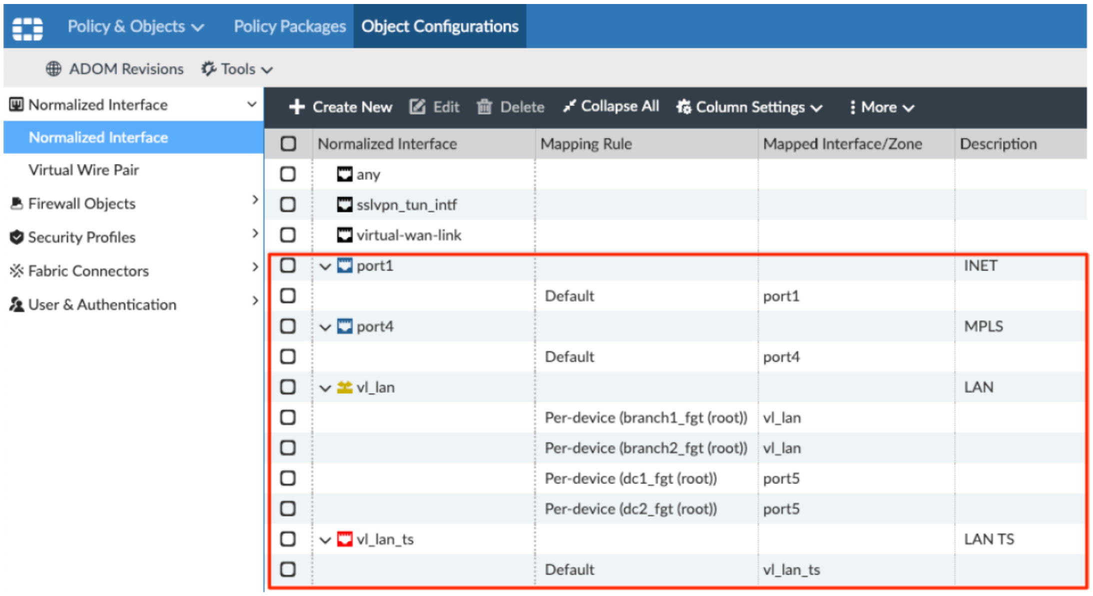
1. Go to *Device Manager* > *Device & Groups*.
2. Click a device group. The devices in the group display in the content pane.
3. In the content pane, right-click a device, and select *Import Policy* to launch the *Import Policy* wizard.
   For device interfaces, select *Per-Device* mapping type. Device interfaces are imported and mapped to normalized interfaces.
4. Complete the wizard.

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

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

To view mapped interfaces:

1. Go to *Policy & Objects* > *Object Configurations*.
2. In the tree menu, go to *Normalized Interface* > *Normalized Interface*. The mapped interfaces display in the content pane.



Normalized Interface	Mapping Rule	Mapped Interface/Zone	Description
any			
sslvpn_tun_intf			
virtual-wan-link			
port1			INET
	Default	port1	
port4			MPLS
	Default	port4	
vl_lan			LAN
	Per-device (branch1_fgt (root))	vl_lan	
	Per-device (branch2_fgt (root))	vl_lan	
	Per-device (dc1_fgt (root))	port5	
	Per-device (dc2_fgt (root))	port5	
vl_lan_ts			LAN TS
	Default	vl_lan_ts	

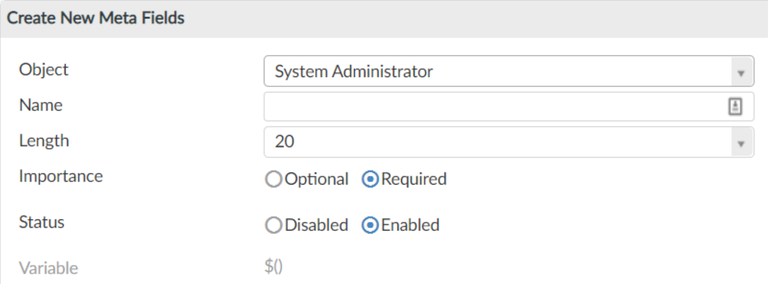
Creating meta fields

Create the following meta fields:

- *branch-id*
- *dc-id*
- *overlay-id*
- *remote-dc-id*
- *ul-id*

To create meta fields:

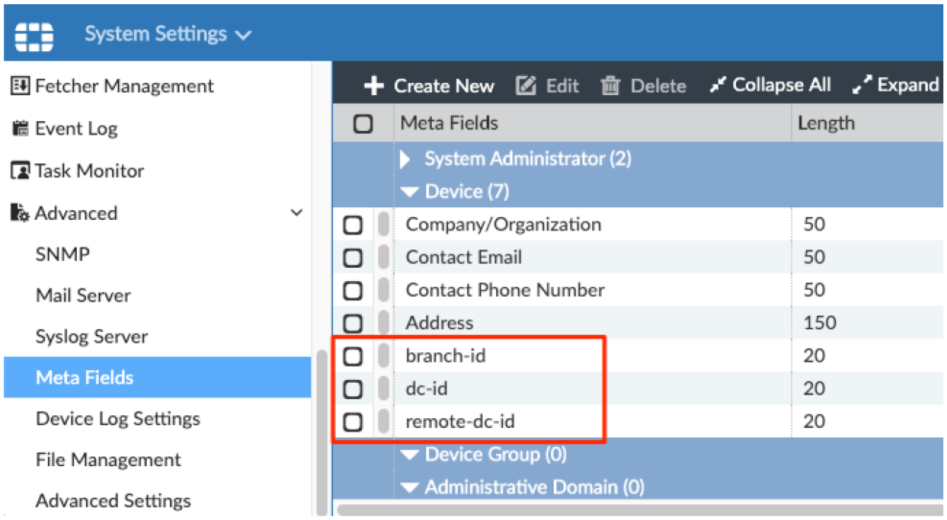
1. Go to *System Settings* > *Advanced* > *Meta Fields*, and click *Create New*.
   The *Create New Meta Fields* pane is displayed.



Create New Meta Fields

Object	System Administrator
Name	
Length	20
Importance	○ Optional ● Required
Status	○ Disabled ● Enabled
Variable	$()

2. In the *Object* list, select *Device*.
3. In the *Name* box, type a name such as *branch-id*.
4. Beside *Importance*, select *Optional*.
5. Click *OK*.
6. Repeat this procedure until you create all meta fields.



Meta Fields	Length
System Administrator (2)	
Device (7)	
Company/Organization	50
Contact Email	50
Contact Phone Number	50
Address	150
branch-id	20
dc-id	20
remote-dc-id	20
Device Group (0)	
Administrative Domain (0)	

Setting meta field values for all FortiGates

Edit each FortiGate, and set the following meta field values:

FortiGate	Meta Field	Value
dc1_fgt	dc-id	1
dc2_fgt	dc-id	2
branch1_fgt	branch-id	1
branch2_fgt	branch-id	2

To set meta field values for all FortiGates:

1. Go to *Device Manager* > *Device & Groups*.
2. In the tree menu, select a group. The devices in the group are displayed in the content pane.
3. Right-click a device, and select *Edit*.
4. Enter the value for the meta field, and click *OK*.
5. Repeat this procedure to edit each device and set the meta field value.

Creating underlay WAN links

Each FortiGate utilizes two underlay WAN links:

- INET: simulates a local Internet breakout on each FortiGate
- MPLS: simulates a private connection between branches and datacenters

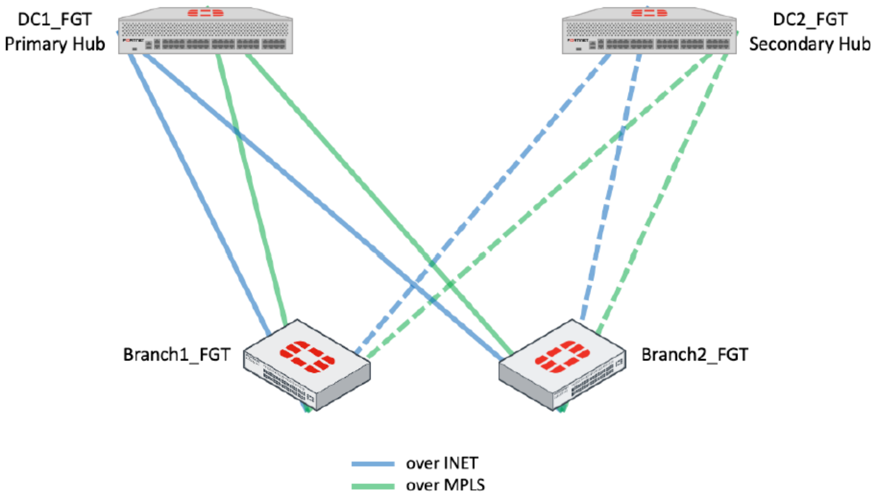
The following table summarizes the configuration:

FortiGate	MPLS	INET	LAN
Datacenter 1 **(DC1_FGT)**	port4: 172.16.1.5 /24 Default Gateway: 172.16.1.6	port1: 100.64.1.5 /24 Default Gateway: 100.64.1.100	port5: 10.1.0.1/24
Datacenter 2 **(DC2_FGT)**	port4: 172.16.2.5 /24 Default Gateway: 172.16.2.6	port1: 100.64.2.5 /24 Default Gateway: 100.64.2.100	port5: 10.2.0.1/24
Branch 1 **(Branch1_FGT)**	port4: 172.16.0.1 /30 Default Gateway: 172.16.0.2	port1: 192.2.0.1 /30 Default Gateway: 192.2.0.2	vl_lan: 10.0.1.1 /24
Branch 2 **(Branch2_FGT)**	port4: 172.16.0.5 /30 Default Gateway: 172.16.0.6	port1: 203.0.113.2 /30 Default Gateway: 203.0.113.1	vl_lan: 10.0.2.1 /24

Configuring overlay connections

This section describes how to build topology with two hubs and two spokes. The spokes will connect to both hubs and use them in Active/Passive mode.

The following diagram illustrates this:



FortiManager uses the term *VPN Community* for a set of interconnected gateways. FortiGates will be interconnected over two separate underlay networks, so we will create the following separate VPN communities:

- One VPN community over the Internet (OL_INET)
- Another VPN community over MPLS (OL_MPLS)

Creating and configuring overlay connections involves the following steps:

1. Creating VPN communities on page 45
2. Adding gateways to VPN communities on page 47
3. Installing default policy packages on page 51
4. Enabling ADVPN and adding overlay IDs on page 52

Creating VPN communities

Create the following separate VPN communities:

- One VPN community over the Internet named *OL_INET*
- One VPN community over MPLS named *OL_MPLS*

FortiManager supports having two Hubs within the same community.

The following parameters will be used for each VPN community. Any parameters not mentioned in the table can be left to use default values:

Parameter	Value
VPN Topology	Dial-Up
Authentication	Pre-shared Key = 123Fortinet!@#
IKE Version	2

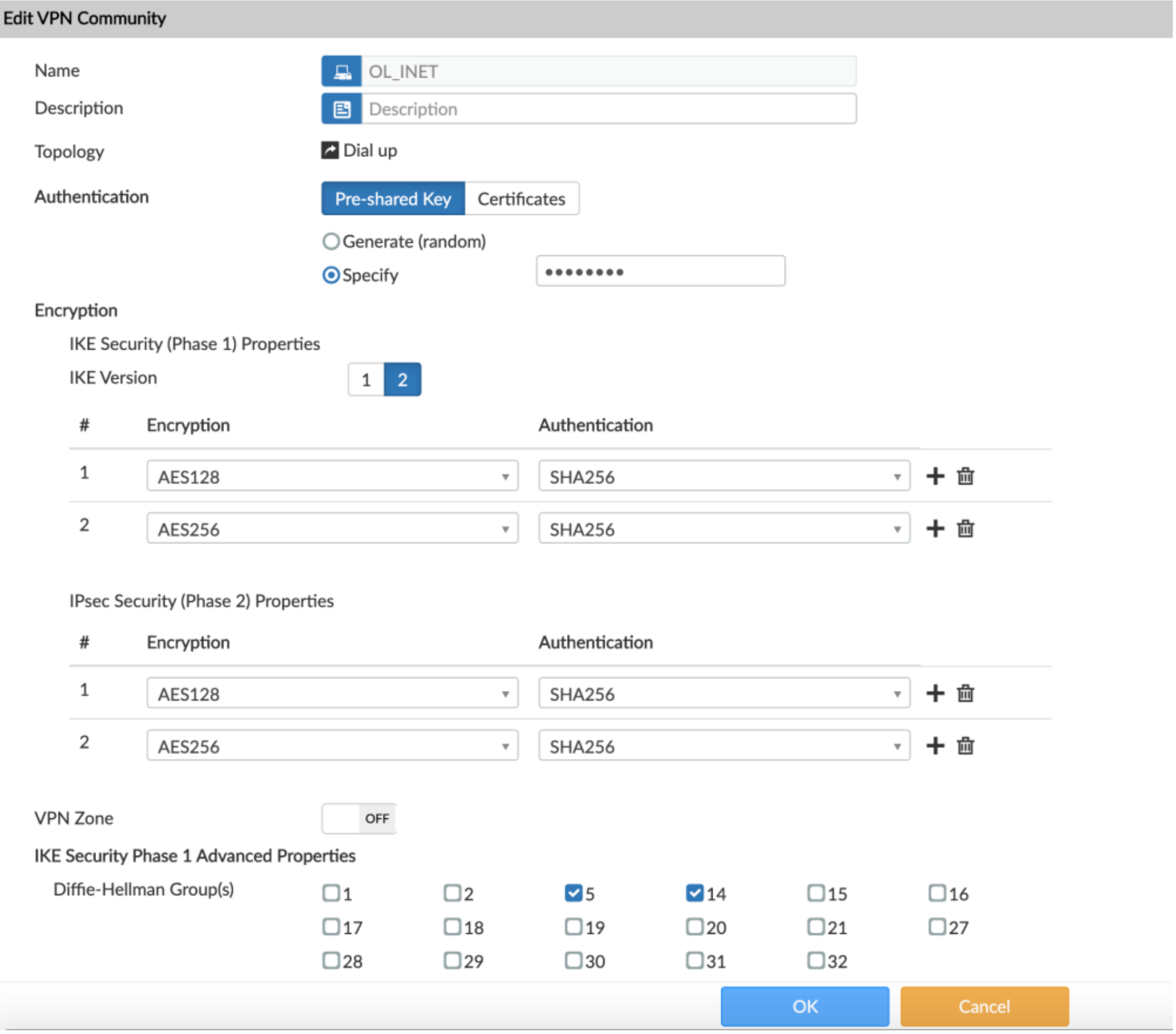
Parameter	Value
IKE SA Proposals	AES256/SHA256, AES256GCM/PRFSHA384
IPSEC SA Proposals	AES256/SHA256, AES256GCM
VPN Zone	OFF
Dead Peer Detection	On Idle
dpd-retrycount	2
dpd-retryinterval	10

To create a VPN Community from the GUI:

1. Go to *VPN Manager* > *IPsec VPN*.
2. In the toolbar, click *Create New*. The *VPN Topology Setup Wizard* dialog appears.
3. Enter a name for the topology, such as *OL_INET*.
4. In the *Choose VPN topology* field, select *Dial up*, and click *Next*.
5. Complete the setup as required in the wizard.

Ensure that *VPN Zone* is disabled while completing the dial-up topology setup. Enabling *VPN Zone* and setting it to *Create Default Zones*, creates a dynamic interface by default. SD-WAN does not support dynamic interfaces.

6. Click *OK*. The VPN community is created.



Edit VPN Community

Name	OL_INET
Description	Description
Topology	Dial up
Authentication	Pre-shared Key / Certificates
	○ Generate (random)
	● Specify ••••••••

Encryption

IKE Security (Phase 1) Properties

IKE Version: 1 **2**

#	Encryption	Authentication
1	AES128	SHA256
2	AES256	SHA256

IPsec Security (Phase 2) Properties

#	Encryption	Authentication
1	AES128	SHA256
2	AES256	SHA256

VPN Zone: OFF

IKE Security Phase 1 Advanced Properties

Diffie-Hellman Group(s)

□1	□2	☑5	☑14	□15	□16
□17	□18	□19	□20	□21	□27
□28	□29	□30	□31	□32	

7. Similarly, create another VPN community called *OL_MPLS* for the MPLS network.

Adding gateways to VPN communities

After you create the VPN communities named *OL_INET* and *OL_MPLS*, the next step is to add managed gateways to the communities.

Add the following gateways to each VPN community:

- branch1_fgt
- branch2_fgt
- dc1_fgt
- dc2_fgt

Add the hub devices one by one to each community. Each hub device has different IP ranges defined for the IKE Config Mode (see the table below).

Use the following parameters for each hub device:

Parameter	Value
Protected Subnet	All
Role	Hub
Default VPN Interface	Underlay port port1 for OL_INET and port4 for OL_MPLS
Routing	Manual
Peer Type	Accept any peer type
IKE Config Mode	ON Hubs will assign tunnel IP addresses to Spokes
IPv4 Start/End/Mask	10.200.<overlay-id>.1-9/24
Add Route	OFF No static route injection. Routing will be handled by BGP.
net-device	OFF
tunnel-search	nexthop

Use the following parameters for each spoke device:

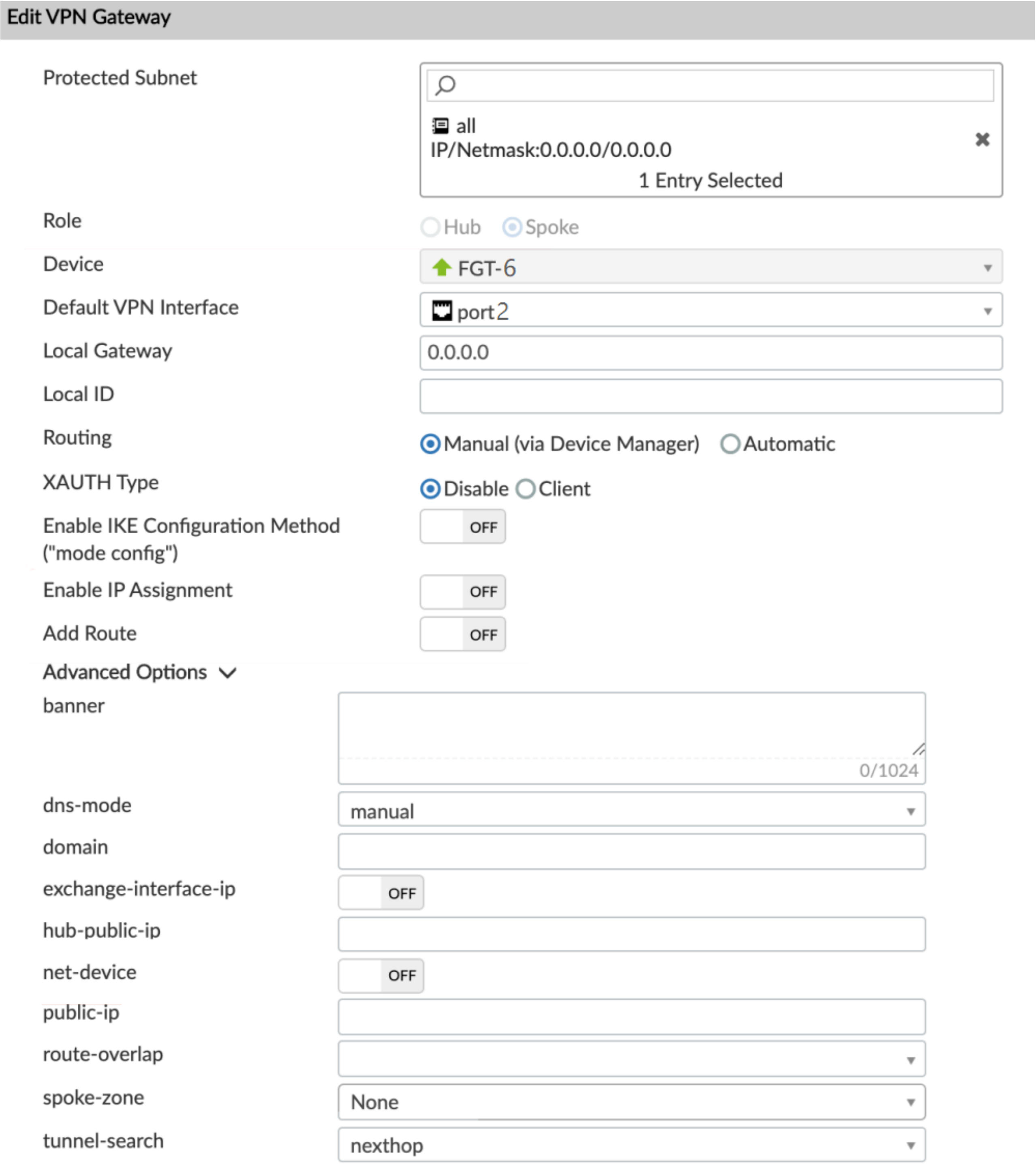
Parameter	Value
Protected Subnet	All
Role	Spoke
Default VPN Interface	Underlay port port1 for OL_INET and port4 for OL_MPLS
Routing	Manual
IKE Config Mode	ON Hubs will assign tunnel IP addresses to Spokes
Add Route	OFF No static route injection. Routing will be handled by BGP.
net-device	OFF

To add a gateway to the *OL_INET* VPN community from the GUI:

1. Go to *VPN Manager > IPsec VPN*.
2. In the tree menu, double-click *OL_INET* to open it for editing.
3. In the toolbar, click *Create New > Managed Gateway*.
   The *VPN Gateway Setup Wizard - OL_INET* is displayed.
4. On the *Protected Network* tab, set the following options, and click *Next*:
   a. Click *Protected Subnet*, select *all*, and click *OK*.

5. On the *Device* tab, set the following options, and click *Next*.
   a. Set the *Role* field to *Spoke*.
   b. From the *Device* list, select a branch FortiGate.
6. On the *Default VPN Interface* tab, set the following options, and click *Next*.
   a. In the *Default VPN Interface* list, select an underlay port.
7. On the *Local Gateway* tab, click *Next* to accept the defaults.
8. On the *Advanced* tab, set the following options, and click *OK*:
   a. Beside *Routing*, select *Manual (via Device Manager)*.
   b. Beside *Enable IKE Configuration Method ("mode config")*, toggle *ON*.
   c. Beside *Add Route*, toggle *OFF*.
   d. Under *Advanced Options*, set *net-device* to *OFF*.

   The branch is added to the *OL_INET* VPN community.



Edit VPN Gateway

Protected Subnet	all IP/Netmask:0.0.0.0/0.0.0.0 1 Entry Selected
Role	○ Hub ● Spoke
Device	FGT-6
Default VPN Interface	port2
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	0/1024
dns-mode	manual
domain	
exchange-interface-ip	OFF
hub-public-ip	
net-device	OFF
public-ip	
route-overlap	
spoke-zone	None
tunnel-search	nexthop

Similarly, add the other branch to the *OL_INET* VPN community.

To add a hub to the *OL_INET* VPN community from the GUI:

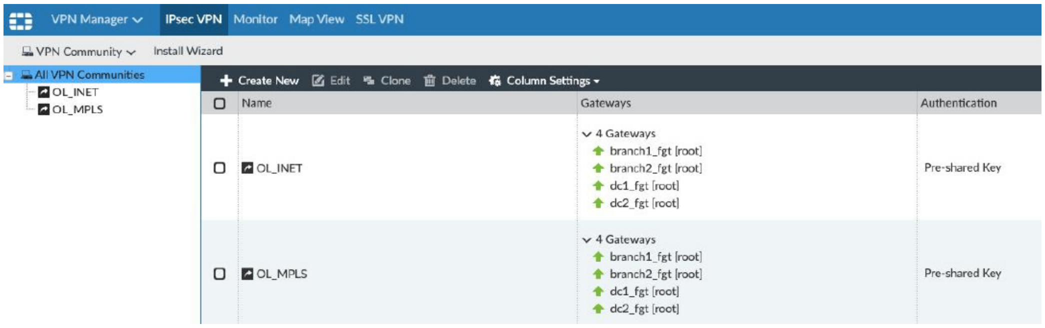
1. Go to *VPN Manager > IPsec VPN*.
2. In the tree menu, click *OL_INET*.

3. In the toolbar, click *Create New* > *Managed Gateway*.
   The *VPN Gateway Setup Wizard - OL_INET* is displayed.
4. On the *Protected Network* tab, set the following options, and click *Next*:
   a. Click *Protected Subnet*, select *all*, and click *OK*.
5. On the *Device* tab, set the following options, and click *Next*.
   a. Set the *Role* field to *Hub*.
   b. From the *Device* list, select a hub FortiGate.
6. On the *Default VPN Interface* tab, set the following options, and click *Next*.
   a. In the *Default VPN Interface* list, select an underlay port.
7. On the *Local Gateway* tab, click *Next* to accept the defaults.
8. On the *Advanced* tab, set the following options, and click *OK*:
   a. Beside *Routing*, select *Manual (via Device Manager)*.
   b. Beside *Peer Type*, select *Accept any peer ID*.
   c. Beside *Enable IKE Configuration Method ("mode config")*, toggle *ON*.
   d. In the *IPv4 Start IP* box, type the start of the IP range.
   e. In the *IPv4 End IP* box, type the end of the IP range.
   f. Beside *Add Route*, toggle *OFF*.
   g. Under *Advanced Options*, set *net-device* to *OFF*.
   h. Set *tunnel-search* to *nexthop*.
   The hub is added to the *OL_INET* VPN community.

Similarly, add the other hub to the *OL_INET* VPN community.

Once you have added both the branches and both hubs to the *OL_INET* VPN community, do the same for *OL_MPLS* VPN community as well.

Once you have configured the *VPN Manager*, your configuration should appear as follows:



☐	Name	Gateways	Authentication
☐	OL_INET	4 Gateways branch1_fgt [root] branch2_fgt [root] dc1_fgt [root] dc2_fgt [root]	Pre-shared Key
☐	OL_MPLS	4 Gateways branch1_fgt [root] branch2_fgt [root] dc1_fgt [root] dc2_fgt [root]	Pre-shared Key

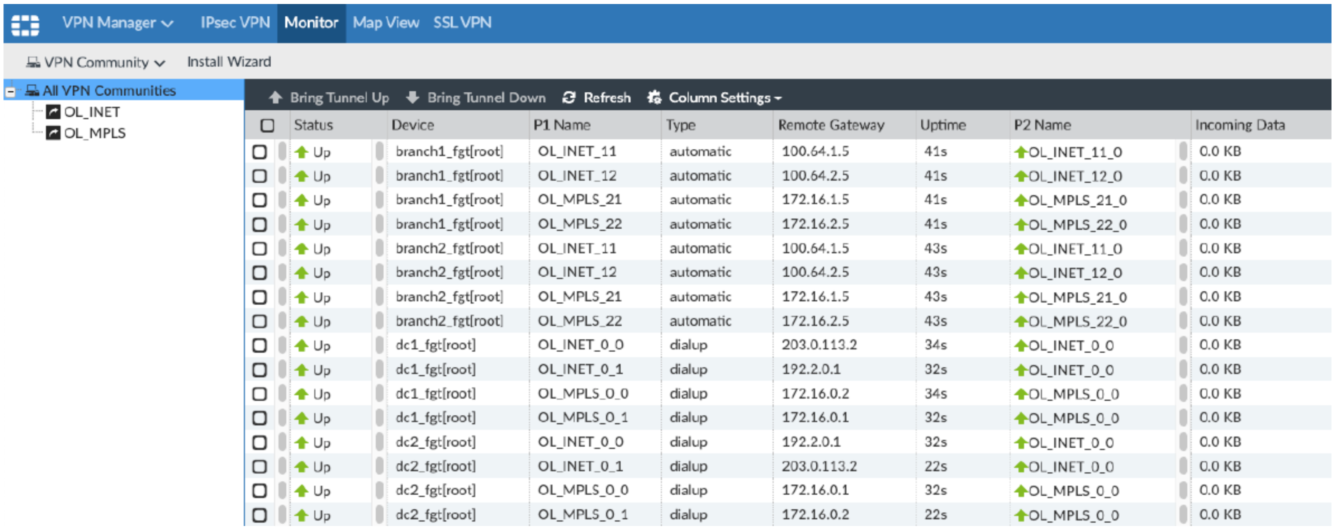
Installing default policy packages

After configuring the VPN communities, install the default policy package to all devices to push the VPN configuration to all devices, and then view the online tunnels.

To install default policy packages:

1. Go to *Device Manager* > *Device & Groups*, and select the devices.
2. From the *Install* menu, select *Install Wizard*. The *Install Wizard* is displayed.
3. Select *Install Policy Package & Device Settings*.

4. From the *Policy Package* list, select *Default*, and click *Next*.
5. Follow the steps to complete the wizard.
6. After installation completes, go to *VPN Manager* > *Monitor* to view the tunnels.



□	Status	Device	P1 Name	Type	Remote Gateway	Uptime	P2 Name	Incoming Data
□	Up	branch1_fgt[root]	OL_INET_11	automatic	100.64.1.5	41s	OL_INET_11_0	0.0 KB
□	Up	branch1_fgt[root]	OL_INET_12	automatic	100.64.2.5	41s	OL_INET_12_0	0.0 KB
□	Up	branch1_fgt[root]	OL_MPLS_21	automatic	172.16.1.5	41s	OL_MPLS_21_0	0.0 KB
□	Up	branch1_fgt[root]	OL_MPLS_22	automatic	172.16.2.5	41s	OL_MPLS_22_0	0.0 KB
□	Up	branch2_fgt[root]	OL_INET_11	automatic	100.64.1.5	43s	OL_INET_11_0	0.0 KB
□	Up	branch2_fgt[root]	OL_INET_12	automatic	100.64.2.5	43s	OL_INET_12_0	0.0 KB
□	Up	branch2_fgt[root]	OL_MPLS_21	automatic	172.16.1.5	43s	OL_MPLS_21_0	0.0 KB
□	Up	branch2_fgt[root]	OL_MPLS_22	automatic	172.16.2.5	43s	OL_MPLS_22_0	0.0 KB
□	Up	dc1_fgt[root]	OL_INET_0_0	dialup	203.0.113.2	34s	OL_INET_0_0	0.0 KB
□	Up	dc1_fgt[root]	OL_INET_0_1	dialup	192.2.0.1	32s	OL_INET_0_0	0.0 KB
□	Up	dc1_fgt[root]	OL_MPLS_0_0	dialup	172.16.0.2	34s	OL_MPLS_0_0	0.0 KB
□	Up	dc1_fgt[root]	OL_MPLS_0_1	dialup	172.16.0.1	32s	OL_MPLS_0_0	0.0 KB
□	Up	dc2_fgt[root]	OL_INET_0_0	dialup	192.2.0.1	32s	OL_INET_0_0	0.0 KB
□	Up	dc2_fgt[root]	OL_INET_0_1	dialup	203.0.113.2	22s	OL_INET_0_0	0.0 KB
□	Up	dc2_fgt[root]	OL_MPLS_0_0	dialup	172.16.0.1	32s	OL_MPLS_0_0	0.0 KB
□	Up	dc2_fgt[root]	OL_MPLS_0_1	dialup	172.16.0.2	22s	OL_MPLS_0_0	0.0 KB

Enabling ADVPN and adding overlay IDs

After creating VPN communities and gateways, you must also:

- Enable ADVPN
- Configure tunnel interface IP addresses

You must enable ADVPN on both hubs and on both spokes.

However you can configure tunnel IP addresses on only the hub devices. Because IKE Config Mode is enabled, the hub devices automatically assign tunnel IP addresses to spokes.

Each hub requires a network overlay ID.

You must use the CLI to enable ADVPN. You cannot enable ADVPN by using the GUI.

It is not possible to establish two IPSEC tunnels between the same two FGT IPs, unless the Network Overlay ID differs between these two tunnels. In our case, this can happen if DC1 Hub triggers a shortcut between two Spokes and then there is a failover to DC2 Hub which also triggers a shortcut between the same two Spokes. This second shortcut will fail to establish, as long as the first one is still there. To avoid this problem, we must ensure that the IPSEC tunnels towards each Hub have different Network Overlay IDs.

You must use the CLI to enable ADVPN and configure tunnel interface IP addresses. In this example, we use CLI script templates to enable these settings.

To create a CLI script template for hubs:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*.
2. Click *Create New* > *CLI Template*.

3. In the *Template Name* box, type *Hub-Overlay*.
4. In the script details box, copy and paste the following commands, and click *OK* to create the CLI script.

```
# Configure tunnel interface IPs
config system interface
   edit "OL_INET_0"
      set ip 10.200.1$(dc-id).10 255.255.255.255
      set remote-ip 10.200.1$(dc-id).254 255.255.255.0
      set allowaccess ping
   next
   edit "OL_MPLS_0"
      set ip 10.200.2$(dc-id).10 255.255.255.255
      set remote-ip 10.200.2$(dc-id).254 255.255.255.0
      set allowaccess ping
   next
end

# Enable ADVPN
config vpn ipsec phase1-interface
   edit "OL_INET_0"
      set auto-discovery-sender enable
      set network-overlay enable
      set network-id 1$(dc-id)
   next
   edit "OL_MPLS_0"
      set auto-discovery-sender enable
      set network-overlay enable
      set network-id 2$(dc-id)
   next
end
```

To create a CLI script template for spokes:

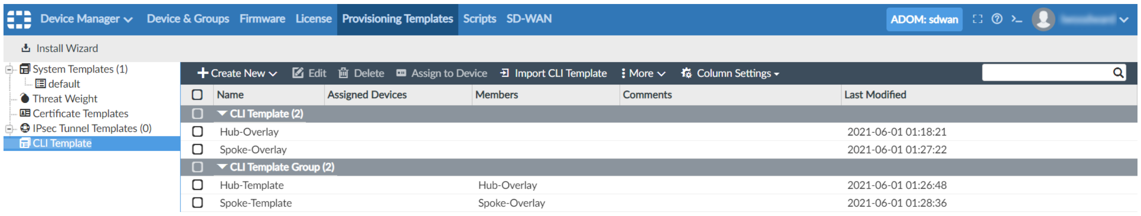
1. Go to *Device Manager > Provisioning Templates > CLI Template*.
2. Click *Create New > CLI Template*.
3. In the *Template Name* box, type *Spoke-Overlay*.
4. In the script details box, copy and paste the following commands, and click *OK* to create the CLI script.

```
# Enable ADVPN
config vpn ipsec phase1-interface
   edit "OL_INET_11"
      set auto-discovery-receiver enable
      set idle-timeout enable
      set idle-timeoutinterval 5
      set network-overlay enable
      set network-id 11
   next
   edit "OL_INET_12"
      set auto-discovery-receiver enable
      set idle-timeout enable
      set idle-timeoutinterval 5
      set network-overlay enable
      set network-id 12
   next
   edit "OL_MPLS_21"
      set auto-discovery-receiver enable
      set idle-timeout enable
      set idle-timeoutinterval 5
      set network-overlay enable
      set network-id 21
   next
   edit "OL_MPLS_22"
      set auto-discovery-receiver enable
      set idle-timeout enable
      set idle-timeoutinterval 5
      set network-overlay enable
      set network-id 22
   next
end
# Allow shortcut monitoring (ping)
config system interface
   edit "OL_INET_11"
      set allowaccess ping
   next
   edit "OL_INET_12"
      set allowaccess ping
   next
   edit "OL_MPLS_21"
      set allowaccess ping
   next
   edit "OL_MPLS_22"
      set allowaccess ping
   next
end
```

To create CLI template groups:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*.
2. Click *Create New* > *CLI Template Group*.
3. In the *Template Group Name* box, type *Hub-Template*.
4. Beside *Members*, click *Add* (+), select *Hub-Overlay*, and click *OK*.
5. Click *OK* to create the CLI Template Group named *Hub-Template*.
6. Repeat this procedure to create a CLI Template Group named *Spoke-Template* and select the script named *Spoke-Overlay*.

The following example shows the CLI scripts and CLI template groups.

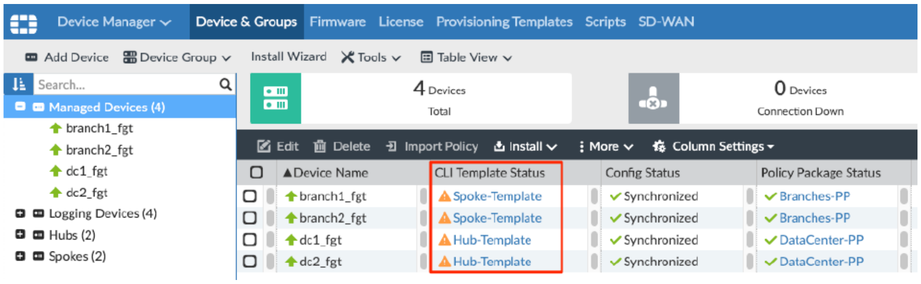


Name	Assigned Devices	Members	Comments	Last Modified
CLI Template (2)				
Hub-Overlay				2021-06-01 01:18:21
Spoke-Overlay				2021-06-01 01:27:22
CLI Template Group (2)				
Hub-Template		Hub-Overlay		2021-06-01 01:26:48
Spoke-Template		Spoke-Overlay		2021-06-01 01:28:36

To assign CLI template groups to devices:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*.
2. Select the template group, and click *Assign to Device*. The *Assign to Device* dialog box is displayed.
3. In the *Available Entries* list, select one or more devices, and click the right arrow (>) to move the devices to the *Selected Entries* list.

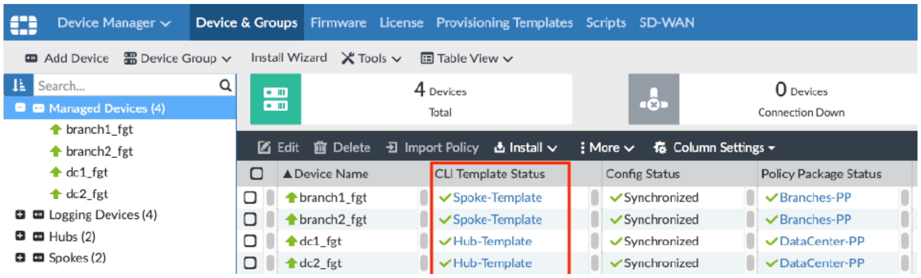
4. Click *OK*. The template group is assigned to the devices in the *Selected Entries* list.



Device Name	CLI Template Status	Config Status	Policy Package Status
branch1_fgt	⚠ Spoke-Template	✓ Synchronized	✓ Branches-PP
branch2_fgt	⚠ Spoke-Template	✓ Synchronized	✓ Branches-PP
dc1_fgt	⚠ Hub-Template	✓ Synchronized	✓ DataCenter-PP
dc2_fgt	⚠ Hub-Template	✓ Synchronized	✓ DataCenter-PP

To install the CLI templates to assigned devices:

1. Go to *Device Manager* > *Device & Groups*.
2. In the tree menu, select the group. The devices in the group are displayed in the content pane.
3. Select the devices, and from the *Install* menu, select *Quick Install (Device DB)*. A confirmation dialog box is displayed.
4. Click *OK* to install the CLI templates.
5. Repeat this procedure for the other device group.



Device Name	CLI Template Status	Config Status	Policy Package Status
branch1_fgt	✓ Spoke-Template	✓ Synchronized	✓ Branches-PP
branch2_fgt	✓ Spoke-Template	✓ Synchronized	✓ Branches-PP
dc1_fgt	✓ Hub-Template	✓ Synchronized	✓ DataCenter-PP
dc2_fgt	✓ Hub-Template	✓ Synchronized	✓ DataCenter-PP

Configuring dynamic routing

It's time to add BGP to this topology. We will be doing this with CLI Templates again. Spokes will establish IBGP peering with both Hubs, and the Hubs will act as Route Reflectors.

Configuring dynamic routing involves the following steps:

1. Configure BGP on spoke devices. See Configuring BGP on spokes on page 55
2. Configure BGP on hub devices. See Configuring BGP on hubs on page 56.
3. Verity BGP routing. See Verifying the BGP routes on page 58.

Configuring BGP on spokes

Use a CLI template to configure the router-bgp in the branches.

To create the CLI template:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*.
2. In the toolbar, click *Create New* > *CLI Template*.

3. In the *Template Name* box, type *Spoke-Routing-BGP*.
4. In the *Script details* field, paste the commands, and click *OK*.

To add the CLI template to the CLI template group:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*.
2. Under CLI Template Group, select *Spoke-Template*, and click *Edit*.
3. Beside *Members*, click *Add* (+), and select the CLI template named *Spoke-Routing-BGP*, and click *OK*.
4. Click *OK* to save changes to the CLI template group.
5. Install the CLI template to all spokes by using *Install* > *Quick Install (Device DB)*.

Example of spoke script details

```
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 BGP on hubs

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

To create the CLI template:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*.
2. In the toolbar, click *Create New* > *CLI Template*.
3. In the *Template Name* box, type *Hub-Routing-BGP*.
4. In the *Script details* field, paste the commands, and click *OK*.

To add the CLI template to the CLI template group:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*.
2. Under CLI Template Group, select *Hub-Template*, and click *Edit*.
3. Beside *Members*, click *Add* (+), and select the CLI template named *Hub-Routing-BGP*, and click *OK*.
4. Click *OK* to save changes to the CLI template group.
5. Install the CLI template to all spokes by using *Install* > *Quick Install (Device DB)*.

Example of hub script details

```
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 spokes, 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 SD-WAN for internal traffic

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

Configuring SD-WAN for internal traffic involves the following steps:

1. Enable SD-WAN central management. See Enabling SD-WAN central management on page 59.
2. Configure normalized interfaces. See Configuring normalized interfaces on page 59.
3. Configure SD-WAN interfaces. See Configuring SD-WAN interface members on page 60.
4. Create a loopback interface to use as a health-check server. See Creating a loopback interface on page 61.
5. Create a health check server for the loopback interface. See Creating health check servers on page 61.
6. Create SD-WAN templates. See Creating SD-WAN templates for branches on page 61.
7. Add SD-WAN rules to SD-WAN templates. See Configuring SD-WAN rules on page 62.
   SD-WAN rules define how traffic flows in the network.
8. Configure firewall policies. See Configuring firewall policies on page 65.
   Firewall policies define whether traffic is permitted to flow and how to inspect flowing traffic.
9. Disable stateful inspection on hubs. See Disabling stateful inspection on hubs on page 66.

Enabling SD-WAN central management

Enable SD-WAN 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*.
2. Select the ADOM, and click *Edit*.
3. Next to *Central Management*, select *SD-WAN*, and click *OK*.

Configuring normalized interfaces

We must create normalized interfaces (previously known as dynamic interfaces) on FortiManager, and map the interfaces to the tunnel interfaces on our FortiGates.

For spokes, create the following normalized interfaces:

Normalized interface	Default mapping
OL_INET_DC1	OL_INET_11
OL_INET_DC2	OL_INET_12
OL_MPLS_DC1	OL_MPLS_21
OL_MPLS_DC2	OL_MPLS_22

For hubs, create the following normalized interfaces:

Normalized interface	Default mapping
OL_INET	OL_INET_0
OL_MPLS	OL_MPLS_0

To create normalized interfaces:

1. Go to *Policy & Objects* > *Object Configurations*.
2. In the tree menu, click *Normalized Interface* > *Normalized Interface*.
3. In the toolbar, click *Create New*. The *Create New Normalized Interface* is displayed.
4. In the *Name* box, type *OL_INET_DC1*.
5. Under *Per-Platform Mapping*, click *Create New*. The *Create New Per-Platform Mapping* dialog box is displayed.
6. In the *Matched Platform* list, select *all*.
7. In the *Mapped Interface Name* box, type *OL_INET_11*, and click *OK*.
8. Click *OK*.
   The normalized interface is created.
9. Repeat this procedure to create all needed normalized interfaces.

Configuring SD-WAN interface members

We need to create SD-WAN interface members and map them to the normalized interfaces. Create the following SD-WAN interface members:

Interface member	Normalized interface
OL_INET_DC1	OL_INET_DC1
OL_INET_DC2	OL_INET_DC2
OL_MPLS_DC1	OL_MPLS_DC1
OL_MPLS_DC2	OL_MPLS_DC2

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*. The Create New WAN Interface dialog box is displayed.
4. In the *Name* box, type *OL_INET_DC1*.

5. In the *Normalized Interface* list, select the interface with the same name.
6. Click *OK*.
7. Repeat this procedure to create all

Creating a loopback interface

We can configure a loopback interface on each Hub. Both interfaces will have the same IP address, which can be used as a health-check server. As a result, we can configure just a single health-check server, while in fact the probes will be reaching different Hubs.

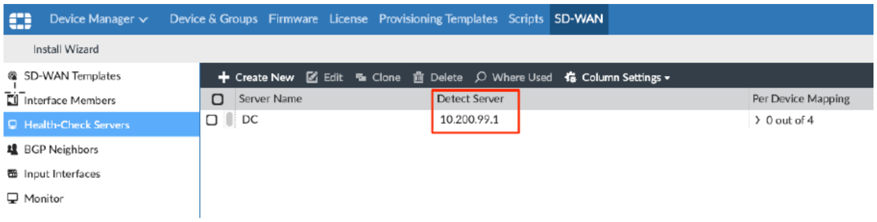
To create a loopback interface to use as a health-check server:

```
config system interface
   edit "lo-HC"
      set vdom "root"
      set vrf 1
      set ip 10.200.99.1 255.255.255.255
      set allowaccess ping
      set type loopback
   next
end
```

Creating health check servers

To create a health check server:

1. Go to *Device Manager* > *SD-WAN* > *Health-Check Servers*.
2. In the toolbar, click *Create New*. The *Create New* page opens.
3. In the *Name* box, type a name for the health check server, such as *DC*.
4. Under *Detect Server*, type the IP address for the loopback interface, and click *OK*.



□	Server Name	Detect Server	Per Device Mapping
□	DC	10.200.99.1	› 0 out of 4

Creating SD-WAN templates for branches

When you create an SD-WAN template, you can create an SD-WAN zone, and assign SD-WAN interface members to the zone.

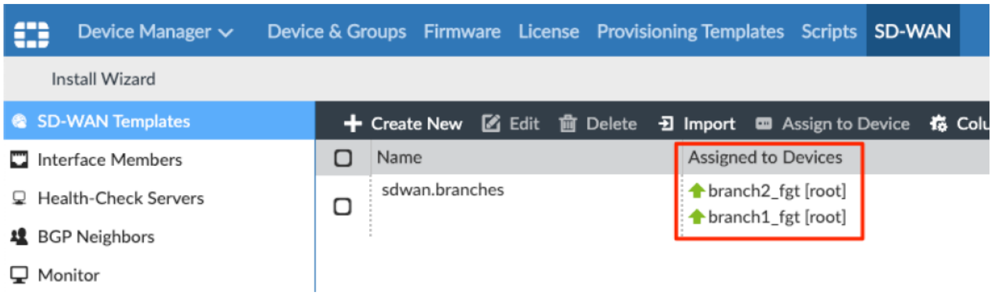
After the template is configured, assign the template to the branch devices.

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. In the *Name* box, type a name for the template, such as *sdwan.branches*.
4. Create an SD-WAN zone:
   a. Under *Interface Members*, click *Create New* > *SD-WAN Zone*.
   b. In the *Name* box, type *overlay*, and click *OK*.
      The zone is created
5. Add SD-WAN members to the zone:
   a. Under *Interface Members*, click *Create New* > *SD-WAN Member*.
   b. In the *Sequence Number* box, type a number for the interface.
   c. In the *Interface Member* box, select the SD-WAN interface member.
   d. In the *SD-WAN Zone* box, select *overlay*, and click *OK*.
      The interface member is added to the zone.
   e. Repeat this procedure to add all interface members to the zone.
6. Define performance SLA:
   a. Under *Performance SLA*, click *Create New*.
   b. In the *Name* box, type a name for the SLA, such as *DC*.
   c. In the *Health-Check Server* list, select the health-check server.
   d. Beside *Participants*, select *Specify*, and click *Click here to select*
   e. Select the SD-WAN members, and click *OK*.
      The interface members are specified.
   f. Under *SLA*, click *Create New*. The Create New SLA dialog box is displayed.
   g. Specify the options, and click *OK*.
7. Click *OK* to save the template.

To assign the SD-WAN template to the spoke 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 spoke devices, and click *OK*.The template is assigned to the devices.



	Name	Assigned to Devices
□	sdwan.branches	branch2_fgt [root] branch1_fgt [root]

Configuring SD-WAN rules

The SD-WAN rules define how the traffic flows. This section describes how to configure SD-WAN rules for internal (corporate) traffic, so that:

1. The traffic prefers OL_INET, as long as it meets the SLA. If the traffic doesn’t meet the SLA, the traffic switches over to OL_MPLS.
2. The traffic should always use DC1_FGT, as long as it is available. DC2_FGT should be used only as a backup Hub. In other words, DC2_FGT should only be used when DC1_FGT is completely out of service.

This topic describes how to create one rule for the primary hub and one rule for the secondary hub.

Creating SD-WAN rules for the primary hub

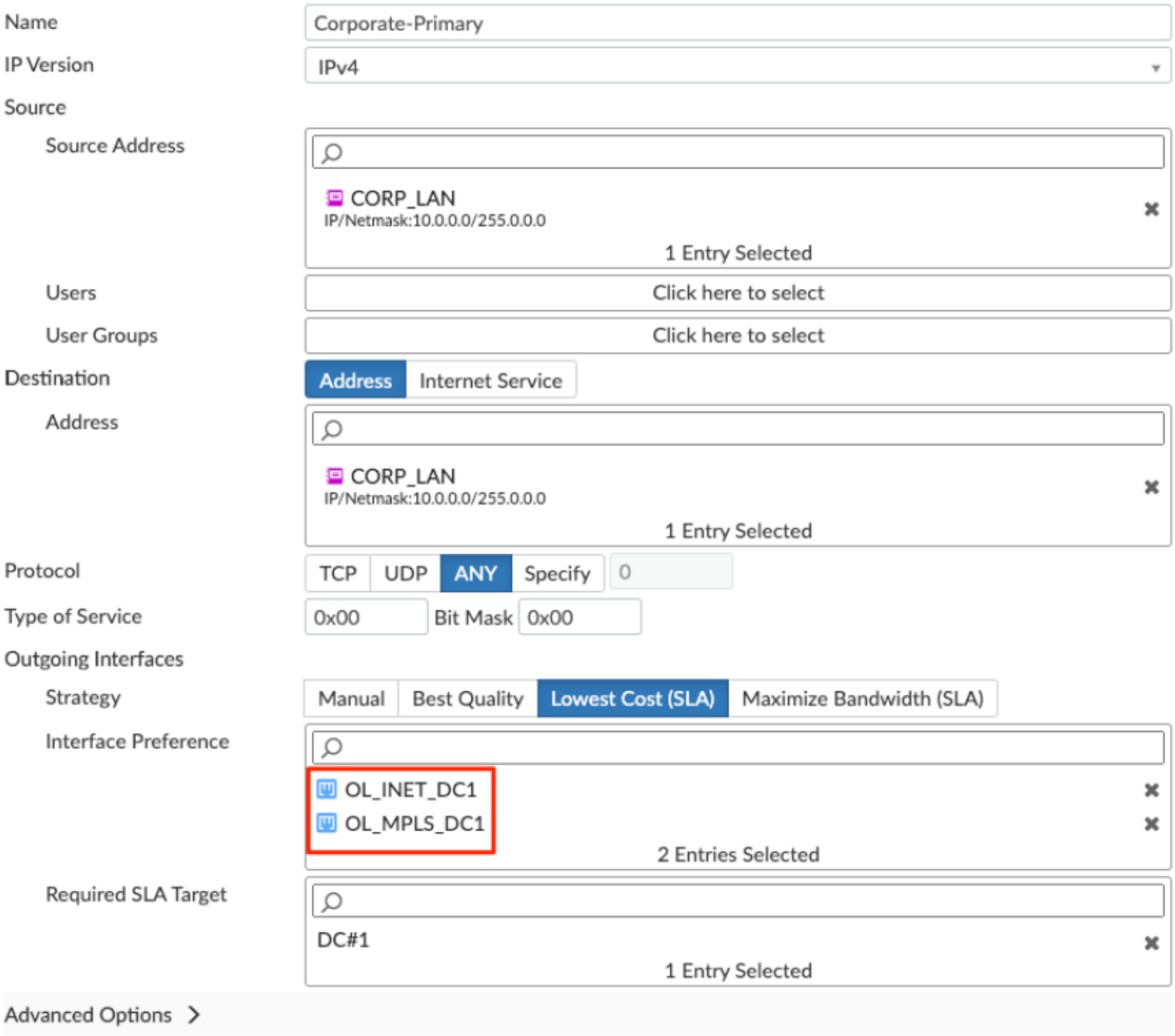
In the SD-WAN rule for the primary hub, we specify only the interface members connecting to the Primary Hub (DC1), and OL_INET_DC1 comes first in the list.

When using the *Lowest Cost (SLA)* strategy, preference is defined by configuration order, among others. The first interface that matches the SLA will be selected, which is precisely what we want to achieve here.

To create an SD-WAN rule for the primary hub:

1. Go to *Device Manager* > *SD-WAN* > *SD-WAN templates*.
2. Double-click the template named *sdwan.branches* to open it for editing.
3. In the SD-WAN rules section, click *Create New*.
4. Set the following options, and click *OK*.
   a. In the *Name* box, type *Corporate-Primary*.
   b. Under *Source*, click *Source Address*, and select the corporate network.
   c. Under *Destination*, click *Source*, and click *Click here to select* to select the corporate network.
   d. Under *Outgoing Interfaces*, click *Lowest Cost (SLA)*.
   e. Beside *Interface Preference*, click *Click here to select*, and select *OL_INET_DC1*, and then *OL_MPLS_DC1*.

f. Beside *Required SLA Target*, click *Click here to select*, and select *DC#1*.



Name	Corporate-Primary
IP Version	IPv4
Source	
Source Address	CORP_LAN IP/Netmask:10.0.0.0/255.0.0.0 1 Entry Selected
Users	Click here to select
User Groups	Click here to select
Destination	Address / Internet Service
Address	CORP_LAN IP/Netmask:10.0.0.0/255.0.0.0 1 Entry Selected
Protocol	TCP / UDP / ANY / Specify / 0
Type of Service	0x00 Bit Mask 0x00
Outgoing Interfaces	
Strategy	Manual / Best Quality / Lowest Cost (SLA) / Maximize Bandwidth (SLA)
Interface Preference	OL_INET_DC1 OL_MPLS_DC1 2 Entries Selected
Required SLA Target	DC#1 1 Entry Selected

Advanced Options >

The rule is created.

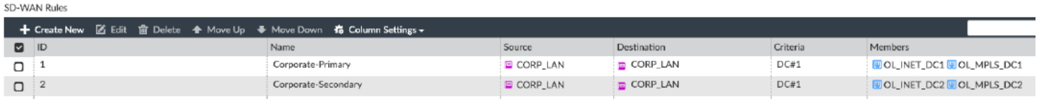
5. Click *OK* to save the SD-WAN template.

Creating SD-WAN rules for the secondary hub

In the SD-WAN rule for the secondary hub, we specify only the interface members connecting to the Secondary Hub (DC2), and OL_INET_DC2 comes first in the list.

Open the SD-WAN template named *sdwan.branches* for editing, and create a rule for the secondary hub.

When you are done, you will have the following rules in the SD-WAN template:



SD-WAN Rules

ID	Name	Source	Destination	Criteria	Members
1	Corporate-Primary	CORP_LAN	CORP_LAN	DC#1	OL_INET_DC1 OL_MPLS_DC1
2	Corporate-Secondary	CORP_LAN	CORP_LAN	DC#1	OL_INET_DC2 OL_MPLS_DC2

Configuring firewall policies

While SD-WAN rules define where the traffic should flow, the firewall policy defines whether the traffic is permitted to flow and how traffic should be inspected.

This topic describes how to create the following policy packages with firewall policies:

- A policy package named *Branches-PP* for spoke devices
- A policy package named *DataCenter-PP* for hub devices

After you create the policy package, assign it to the target devices, and install the policy packages.

> With the introduction of SD-WAN Zones concept, it is no longer possible to use individual tunnel interfaces in firewall policies! We must group them into SD-WAN Zones and use these zones in the policies.
>
> We have assigned all our SD-WAN members to the newly created zone named *overlay*, which automatically created a corresponding normalized interface. Use the normalized interface in the policies.

To create a policy package and firewall policy rules for spokes:

1. Go to *Policy & Objects* > *Policy Packages*.
2. Create a policy package for spoke devices:
   a. Click *Policy Package* > *New*. The *Create New Policy Package* dialog box is displayed.
   b. In the *Name* box, type a name, such as *Branches-PP*.
   c. Leave *Central NAT* toggled *OFF*.
   d. Beside *NGFW Mode*, select *Profile-based*.
   e. Click *OK*. The policy package is created.
3. In the tree menu, select the policy package for spokes named, for example, *Branches-PP*. The firewall policies in the policy package are displayed.
4. Add policies to the firewall policy:
   a. In the toolbar, click *Create New*. The *Create New Firewall Policy* pane is displayed.
   b. Create the following policy for spokes, and click *OK*.

Name	From	To	Src	Dst	Service	NAT	Action
Corporate	vl_lan overlay	overlay vl_lan	CORP_LAN	CORP_LAN	All	No	Accept

   The rule is added to the firewall policy.
5. Set the installation targets to spoke devices, and install the policy package.

To create a policy package and firewall policy rules for hubs:

1. Go to *Policy & Objects* > *Policy Packages*.
2. Create a policy package for spoke devices:
   a. Click *Policy Package* > *New*. The *Create New Policy Package* dialog box is displayed.
   b. In the *Name* box, type a name, such as *DataCenter-PP*.
   c. Leave *Central NAT* toggled *OFF*.

d. Beside *NGFW Mode*, select *Profile-based*.
e. Click *OK*. The policy package is created.

3. In the tree menu, select the policy package for spokes named, for example, *DataCenter-PP*. The firewall policies in the policy package are displayed.
4. Add policies to the firewall policy:
   a. In the toolbar, click *Create New*. The *Create New Firewall Policy* pane is displayed.
   b. Create the following policy for spokes, and click *OK*.

Name	From	To	Src	Dst	Service	NAT	Action
Branch to Branch	OL_INET OL_MPLS	OL_INET OL_MPLS	all	all	All	No	Accept
Branch to DC	OL_INET OL_MPLS	vl_lan	all	all	All	No	Accept
Health-check	OL_INET OL_MPLS	any	all	HC	PING	NO	Accept

On the Hub devices, individual interfaces are used in the firewall policy because SD-WAN is not configured on the Hub devices. As a result, there are no SD-WAN zones either.

Also incoming health probes must be explicitly permitted. Traffic towards loopback is not permitted by default.

5. Set the installation targets to hub devices, and install the policy package.

Disabling stateful inspection on hubs

When ADVPN is used, it is possible for a session to switch over from one overlay to another in the middle. For example, if the health of a link changes, it can cause a switchover. A certain TCP session might switch over from ADVPN shortcut to Spoke-to-Hub tunnel. Since the Hub is not aware of this TCP session, it will be dropped by the stateful inspection, which is not desired. As a result, when ADVPN is in use and session switchover is needed, it is important to disable stateful inspection on the Hubs for the Spoke-to-Spoke traffic. This is done as follows:

To disable stateful inspection on hub devices:

1. Globally enable TCP sessions without SYN:

```
config system settings
   set tcp-session-without-syn enable
end
```

2. Go to *Policy & Objects* > *Policy Package*s, and select the policy package for hubs.
3. Double-click the *Branch to Branch* policy to open it for editing.
4. Expand the *Advanced Options*, and set the following options:
   - Toggle *anti-replay* to *OFF*. (TCP sequence number validation.)
   - Set *tcp-session-without-syn* to *all*.
5. Click *OK* to save the changes.

No reason to worry: Spokes still provide stateful inspection for all the Spoke-to-Spoke traffic! And Hubs still provide it for all the other traffic, since we have only disabled it on a particular firewall rule.

Configuring SD-WAN for Internet traffic

This chapter describes how to extend SD-WAN to the Internet access as well. We will implement a hybrid Local + Remote Breakout, also known as Direct Internet Access (DIA) + Remote Internet Access (RIA). Our overlays over MPLS network will be used for RIA, when the DIA quality is not acceptable.

Configuring SD-WAN for Internet traffic involves the following steps:

1. Add a new SD-WAN interface member. See Configuring SD-WAN interface members on page 67.
2. Create a health check server. See Creating health-check servers on page 67.
3. Edit SD-WAN template for branches to add a new underlay zone. See Editing SD-WAN templates for branches on page 68.
4. Create new performance SLA. See Configuring performance SLA on page 69.
5. Create SD-WAN rules for DIA/RIA. See Creating SD-WAN rules for DIA/RIA on page 71.
6. Update firewall policies. See Updating firewall policies on page 73.
7. Configure a static route. See Configuring the static routes on page 74.

Configuring SD-WAN interface members

We are going to add our underlay port (Internet-facing WAN link) to the list of SD-WAN members. In our topology, this is port1.

To configure the interface members:

1. Go to *Device Manager* > *SD-WAN*.
2. In the tree menu, click *Interface Members*.
3. In the toolbar, click *Create New*. The *Create New WAN Interface* dialog box is displayed.
4. In the *Name* box, type *ul_inet*.
5. In the *Normalized Interface* list, select *port1*.
6. Click *OK*.

Creating health-check servers

Add a new health-check server: www.fortinet.com.

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*.

Editing SD-WAN templates for branches

Edit our existing SD-WAN template (“sdwan.branches”). Create a new SD-WAN Zone “underlay”, adding the new member to it

When you create an SD-WAN template, you can create an SD-WAN zone, and assign SD-WAN interface members to the zone.

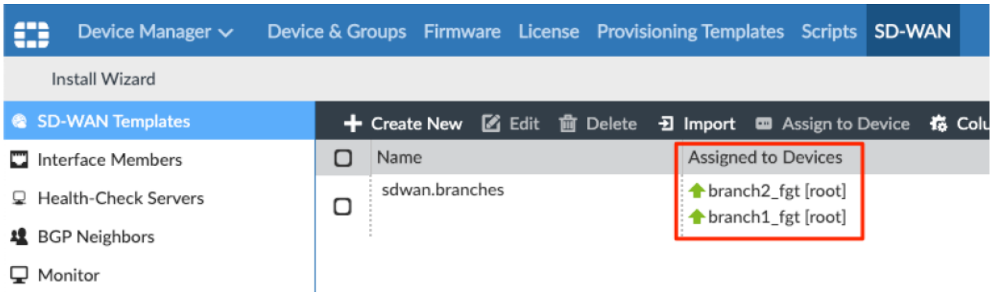
After the template is configured, assign the template to the branch devices.

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. In the *Name* box, type a name for the template, such as *sdwan.branches*.
4. Create an SD-WAN zone:
   a. Under *Interface Members*, click *Create New* > *SD-WAN Zone*.
   b. In the *Name* box, type *overlay*, and click *OK*.
      The zone is created
5. Add SD-WAN members to the zone:
   a. Under *Interface Members*, click *Create New* > *SD-WAN Member*.
   b. In the *Sequence Number* box, type a number for the interface.
   c. In the *Interface Member* box, select the SD-WAN interface member.
   d. In the *SD-WAN Zone* box, select *overlay*, and click *OK*.
      The interface member is added to the zone.
   e. Repeat this procedure to add all interface members to the zone.
6. Define performance SLA:
   a. Under *Performance SLA*, click *Create New*.
   b. In the *Name* box, type a name for the SLA, such as *DC*.
   c. In the *Health-Check Server* list, select the health-check server.
   d. Beside *Participants*, select *Specify*, and click *Click here to select*
   e. Select the SD-WAN members, and click *OK*.
      The interface members are specified.
   f. Under *SLA*, click *Create New*. The Create New SLA dialog box is displayed.
   g. Specify the options, and click *OK*.
7. Click *OK* to save the template.

To assign the SD-WAN template to the spoke 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 spoke devices, and click *OK*.The template is assigned to the devices.



Name	Assigned to Devices
sdwan.branches	branch2_fgt [root] branch1_fgt [root]

Configuring performance SLA

This section describes how to create a new Performance SLA measured over ul-inet, OL_MPLS_DC1 and OL_MPLS_DC2.

Define two separate SLA targets:

- Target #1: 200 ms latency
- Target #2: 300 ms latency

We are going to use these two targets to demonstrate how you can apply different thresholds to different applications.

For a proper logging and reporting, always set the values for sla-fail-log-period and sla-pass-log-period in each Performance SLA that you configure (see under “Advanced Options”)! By default, they are both set to 0, which means that FGTs will not send periodic SLA logs to FAZ. This will result in a lot of missing data in your reports and widgets!

Creating SD-WAN rules for the primary hub

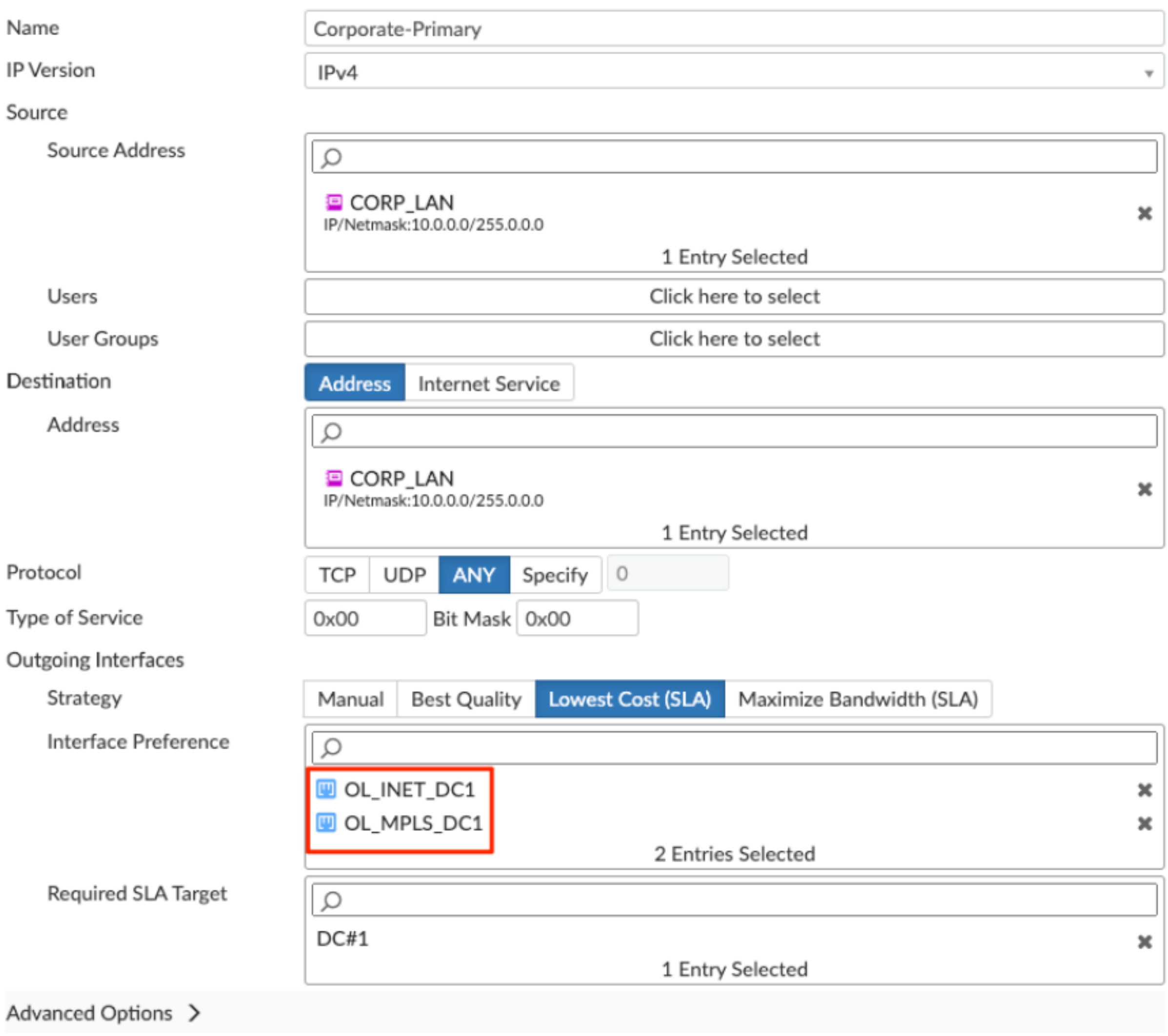
In the SD-WAN rule for the primary hub, we specify only the interface members connecting to the Primary Hub (DC1), and OL_INET_DC1 comes first in the list.

When using the *Lowest Cost (SLA)* strategy, preference is defined by configuration order, among others. The first interface that matches the SLA will be selected, which is precisely what we want to achieve here.

To create an SD-WAN rule for the primary hub:

1. Go to *Device Manager* > *SD-WAN* > *SD-WAN templates*.
2. Double-click the template named *sdwan.branches* to open it for editing.
3. In the SD-WAN rules section, click *Create New*.
4. Set the following options, and click *OK*.
   a. In the *Name* box, type *Corporate-Primary*.
   b. Under *Source*, click *Source Address*, and select the corporate network.
   c. Under *Destination*, click *Source*, and click *Click here to select* to select the corporate network.
   d. Under *Outgoing Interfaces*, click *Lowest Cost (SLA)*.
   e. Beside *Interface Preference*, click *Click here to select*, and select *OL_INET_DC1*, and then *OL_MPLS_DC1*.

f. Beside *Required SLA Target*, click *Click here to select*, and select *DC#1*.



Name	Corporate-Primary
IP Version	IPv4
Source	
Source Address	CORP_LAN IP/Netmask:10.0.0.0/255.0.0.0 1 Entry Selected
Users	Click here to select
User Groups	Click here to select
Destination	Address / Internet Service
Address	CORP_LAN IP/Netmask:10.0.0.0/255.0.0.0 1 Entry Selected
Protocol	TCP / UDP / ANY / Specify 0
Type of Service	0x00 Bit Mask 0x00
Outgoing Interfaces	
Strategy	Manual / Best Quality / Lowest Cost (SLA) / Maximize Bandwidth (SLA)
Interface Preference	OL_INET_DC1 OL_MPLS_DC1 2 Entries Selected
Required SLA Target	DC#1 1 Entry Selected

The rule is created.

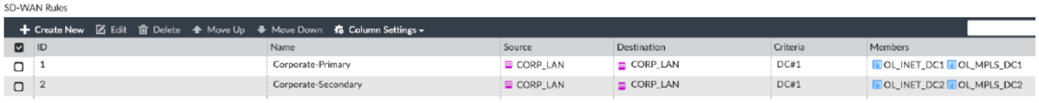
5. Click *OK* to save the SD-WAN template.

Creating SD-WAN rules for the secondary hub

In the SD-WAN rule for the secondary hub, we specify only the interface members connecting to the Secondary Hub (DC2), and OL_INET_DC2 comes first in the list.

Open the SD-WAN template named *sdwan.branches* for editing, and create a rule for the secondary hub.

When you are done, you will have the following rules in the SD-WAN template:



SD-WAN Rules

☑	ID	Name	Source	Destination	Criteria	Members
□	1	Corporate-Primary	CORP_LAN	CORP_LAN	DC#1	OL_INET_DC1 OL_MPLS_DC1
□	2	Corporate-Secondary	CORP_LAN	CORP_LAN	DC#1	OL_INET_DC2 OL_MPLS_DC2

Creating SD-WAN rules for DIA/RIA

Our strategy for Internet access will be as follows:

- We will prefer the Local Breakout (DIA) via the underlay port (ul-inet).
- For business-critical traffic, we will use OL_MPLS overlays as a secondary path (RIA), when DIA quality is not acceptable. The thresholds will be different for different applications.
- For non-business-critical traffic, we will keep using DIA as long as it is alive, disregarding its current quality.

Let’s configure three SD-WAN rules for this:

- Business-Critical-HighPriority: This rule will be matching GoToMeeting and Salesforce traffic, with SLA Target #1.
- Business-Critical-MedPriority: This rule will be matching Office365 traffic, with SLA Target #2.
- Non-Business-Critical: This rule will be matching all other Internet traffic.

Creating SD-WAN rules for the primary hub

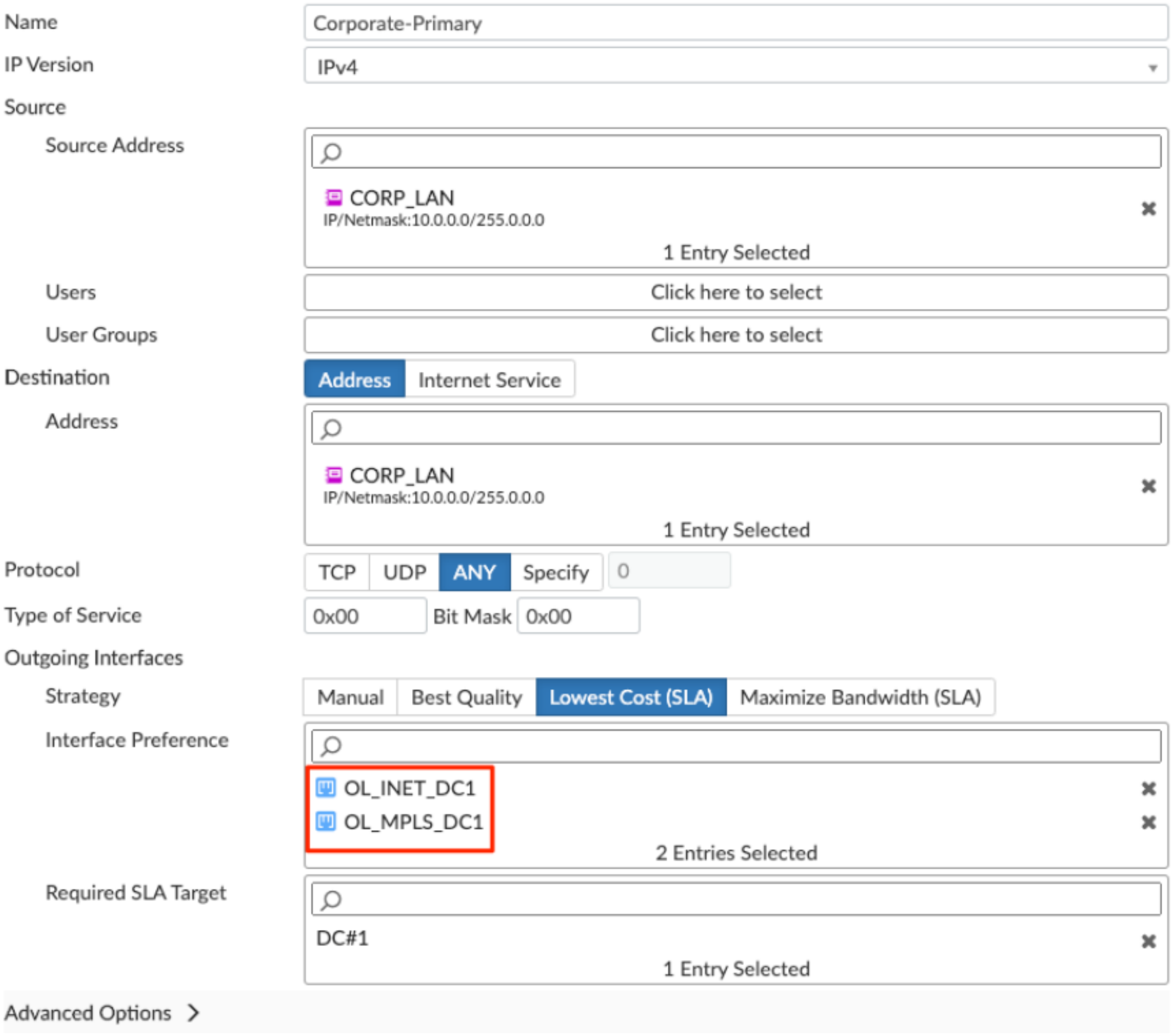
In the SD-WAN rule for the primary hub, we specify only the interface members connecting to the Primary Hub (DC1), and OL_INET_DC1 comes first in the list.

When using the *Lowest Cost (SLA)* strategy, preference is defined by configuration order, among others. The first interface that matches the SLA will be selected, which is precisely what we want to achieve here.

To create an SD-WAN rule for the primary hub:

1. Go to *Device Manager* > *SD-WAN* > *SD-WAN templates*.
2. Double-click the template named *sdwan.branches* to open it for editing.
3. In the SD-WAN rules section, click *Create New*.
4. Set the following options, and click *OK*.
   a. In the *Name* box, type *Corporate-Primary*.
   b. Under *Source*, click *Source Address*, and select the corporate network.
   c. Under *Destination*, click *Source*, and click *Click here to select* to select the corporate network.
   d. Under *Outgoing Interfaces*, click *Lowest Cost (SLA)*.
   e. Beside *Interface Preference*, click *Click here to select*, and select *OL_INET_DC1*, and then *OL_MPLS_DC1*.

f. Beside *Required SLA Target*, click *Click here to select*, and select *DC#1*.



Name	Corporate-Primary
IP Version	IPv4
Source	
Source Address	CORP_LAN IP/Netmask:10.0.0.0/255.0.0.0 1 Entry Selected
Users	Click here to select
User Groups	Click here to select
Destination	Address / Internet Service
Address	CORP_LAN IP/Netmask:10.0.0.0/255.0.0.0 1 Entry Selected
Protocol	TCP / UDP / ANY / Specify / 0
Type of Service	0x00 Bit Mask 0x00
Outgoing Interfaces	
Strategy	Manual / Best Quality / Lowest Cost (SLA) / Maximize Bandwidth (SLA)
Interface Preference	OL_INET_DC1 OL_MPLS_DC1 2 Entries Selected
Required SLA Target	DC#1 1 Entry Selected

Advanced Options >

The rule is created.

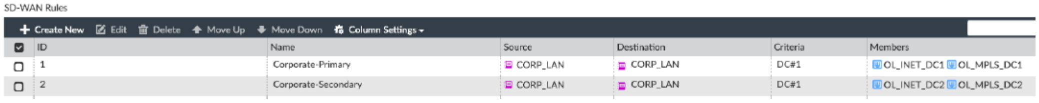
5. Click *OK* to save the SD-WAN template.

Creating SD-WAN rules for the secondary hub

In the SD-WAN rule for the secondary hub, we specify only the interface members connecting to the Secondary Hub (DC2), and OL_INET_DC2 comes first in the list.

Open the SD-WAN template named *sdwan.branches* for editing, and create a rule for the secondary hub.

When you are done, you will have the following rules in the SD-WAN template:



SD-WAN Rules

☑	ID	Name	Source	Destination	Criteria	Members
□	1	Corporate-Primary	CORP_LAN	CORP_LAN	DC#1	OL_INET_DC1 OL_MPLS_DC1
□	2	Corporate-Secondary	CORP_LAN	CORP_LAN	DC#1	OL_INET_DC2 OL_MPLS_DC2

Updating firewall policies

Let’s now add firewall policies to permit Internet traffic. Different treatment is required, depending whether it is DIA or RIA:

- For DIA, since the traffic leaves our network directly from the Branch, we must ensure advanced protection. In this lab, we are going to apply full SSL inspection (while this alone is not particularly advanced, it is enough to demonstrate our point). In addition, this traffic must be NATed on the Spokes.
- For RIA, the traffic will be backhauled via the DC, hence advanced security can be applied there, as it would happen in a legacy network. In this lab, DIA traffic will leave our network via the Hub, so we are going to apply full SSL inspection on the Hub, but not on Spokes. In addition, this traffic must be NATed on the Hubs, but not on the Spokes.

After you update the policy packages, install them.

We must enable Application Control on all these firewall rules, since our SD-WAN rules rely on it!

To create a policy package and firewall policy rules for spokes:

1. Go to *Policy & Objects* > *Policy Packages*.
2. In the tree menu, select the policy package for spokes, for example, *Branches-PP*. The firewall policies in the policy package are displayed.
3. Add policies to the firewall policy:
   a. In the toolbar, click *Create New*. The *Create New Firewall Policy* pane is displayed.
   b. Create the following policy for spokes, and click *OK*.

Name	From	To	Service	NAT	Action
DIA	vl_lan	underlay	All	Yes	Accept + App Control + SSL deep-inspection
RIA	vl_lan	overlay	ALL	No	Accept + App Control

SD-WAN Zones on Spokes are used to configure different treatment for the traffic flowing to underlay versus overlay. Remember that this will be exactly the same type of traffic, and the actual path for each session will be determined by the SD-WAN rules

The rules are added to the firewall policy.

4. Install the policy package.

To create a policy package and firewall policy rules for hubs:

1. Go to *Policy & Objects* > *Policy Packages*.
2. In the tree menu, select the policy package for hubs, for example, *DataCenter-PP*. The firewall policies in the policy package are displayed.

3. Add policies to the firewall policy:
   a. In the toolbar, click *Create New*. The *Create New Firewall Policy* pane is displayed.
   b. Create the following policy for spokes, and click *OK*.

Name	From	To	Service	NAT	Action
Branch RIA	OL_MPLS	port1	All	Yes	Accept + App Control + SSL deep-inspection

4. Install the policy package.

Configuring the static routes

The default (and most used) behavior on FOS is that SD-WAN will not forward the traffic without a feasible route! We have already seen this in the previous chapter. In other words: A valid route to the destination must exist via an SD-WAN member, for that member to be chosen!

Why do we explicitly set priority? We would like to ensure that port1 will still be preferred for Internet access by any traffic that is not handled by SD-WAN. The best example of such traffic is the one locally originated by Branch FGT itself (e.g. IKE or Fortiguard or even a ping that you initiate from CLI). We would like this traffic to always use port1. The default route via port1 has the default priority (0), so we set a higher value (lower priority) for these newly added routes, while still installing them into the routing table.

Note that you cannot use other attributes, such as “distance”. Higher distance would result in these new routes not being installed into the routing table at all. That would not solve our original routing caveat for SD-WAN.

To add static routes to the spoke FortiGates:

1. Create a CLI template.
2. Add the CLI script to the CLI template
3. Install the changes to FortiGate.

```
config router static
   edit 21
      set priority 10
      set device "OL_MPLS_21"
   next
   edit 22
      set priority 10
      set device "OL_MPLS_22"
   next
end
```

Interconnecting data centers

You can use the underlays to interconnect the data centers via the hubs.

Configuring inter-connection between data centers involves the following steps:

1. Configure hub to hub tunnels. See Configuring hub to hub tunnels on page 75.
2. Update the firewall policy to allow tunnel traffic. See Updating firewall policies on page 75.
3. Configure hub to hub routing. See Configuring hub to hub routing on page 76.

Configuring hub to hub tunnels

FortiManager VPN Manager supports building Hub-to-Hub tunnels, when VPN Community contains two Hubs. All we need to do is to specify a Hub-to-Hub underlay port for each Hub.

Edit each Hub in both communities and set the right Hub-to-Hub port (port1 for OL_INET Hubs, port4 for OL_MPLS Hubs):

Now run Install Wizard for the DC policy package and, right before completing the installation, click on “Install Preview”:

You will see how FMG creates two Site-to-Site IPSEC tunnels, one over each underlay. Note the naming: FMG is using the ID of the remote Hub for each tunnel, so it is again predictable, since we have manually set the Hub IDs via Postman.

Complete policy installation.

Updating firewall policies

Let’s not forget to add a firewall rule for this traffic! The tunnel interface name is different on each Hub (since it includes the ID of the remote Hub).

We will use per-device mapping when defining our normalized interfaces in FMG:

Normalized Interface	Per-Device Mapping
OL_INET_DC2DC	DC1_FGT: OL_INET_12 DC2_FGT: OL_INET_11
OL_MPLS_DC2DC	DC1_FGT: OL_MPLS_22 DC2_FGT: OL_MPLS_21

To update firewall policies for hubs:

1. Go to *Policy & Objects* > *Policy Packages*.
2. In the tree menu, select the policy package for hubs, for example, *DataCenter-PP*. The firewall policies in the policy package are displayed.
3. Add policies to the firewall policy:
   a. In the toolbar, click *Create New*. The *Create New Firewall Policy* pane is displayed.
   b. Create the following policy, and click *OK*.

Name	From	To	Src	Dst	Service	NAT	Action
DC to DC	vl_lan OL_INET_DC2DC OL_MPLS_DC2DC	vl_lan OL_INET_DC2DC OL_MPLS_DC2DC	all	all	ALL	No	Accept

4. Install the *DataCenter-PP* policy package to hub devices.

Configuring hub to hub routing

This topic describes how to add BGP peering over the tunnels.

Note that we do NOT need to enable ADVPN forwarding on these tunnels. Spoke traffic will never be forwarded between the Hubs, because each Spoke connects to each of the Hubs directly. The sole purpose of these tunnels is to forward inter-DC traffic! We also need to keep this in mind when configuring BGP!

We are going to configure IBGP between the Hubs with the sole purpose to advertise DC prefixes.

We will not advertise any Spoke prefixes between the Hubs!

We will not use SD-WAN here either. Instead, we will do it the “conventional” way, preferring Internet connection with BGP local-preference attribute.

BGP configuration will be done as usual, using CLI Templates.

- We configure Hub-to-Hub tunnel IPs (note how we use the meta variables here)
- We configure prefix-list for the local DC LAN:
  ```
  config router prefix-list
     edit "LAN_DC$(dc-id)"
        config rule
           edit 1
              set prefix 10.$(dc-id).0.0 255.255.255.0
              unset ge
              unset le
           next
        end
     next
  end
  ```
- We configure route-map to advertise only the DC LAN subnet:
  ```
  config router route-map
     edit "DC2DC_OUT"
        config rule
           edit 1
              set match-ip-address "LAN_DC$(dc-id)"
           next
           edit 2
              set action deny
           next
        end
     next
  end
  ```
- We configure route-map to prefer the link over the Internet:
  ```
  config router route-map
     edit "DC2DC_INET_IN"
        config rule
           edit 1
              set local-preference 200
           next
        end
  ```

```
      next
   end
```

- We configure BGP neighbors, applying the above route-maps:

```
   config router bgp
      config neighbor
         edit "10.200.10.$(remote-dc-id)"
            set route-map-in "DC2DC_INET_IN"
            set route-map-out "DC2DC_OUT"
         next
         edit "10.200.20.$(remote-dc-id)"
            set route-map-out "DC2DC_OUT"
         next
      end
   end
```

To create a CLI script template for hubs:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*.
2. Click *Create New* > *CLI Template*.
3. In the *Template Name* box, type *Hub-Routing-InterDC*.
4. In the script details box, copy and paste the above commands, and click *OK* to create the CLI script.

To add the CLI script to the CLI template group:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*.
2. Under *CLI Template Group*, double-click *Hub-Template* to open the group for editing.
3. Beside *Members*, click *Add* (+), select *Hub-Routing-InterDC*, and click *OK*.
   The CLI script is added to the CLI template group.
4. Install the changes to hub devices.

Device Manager

This section contains the following topics:

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.

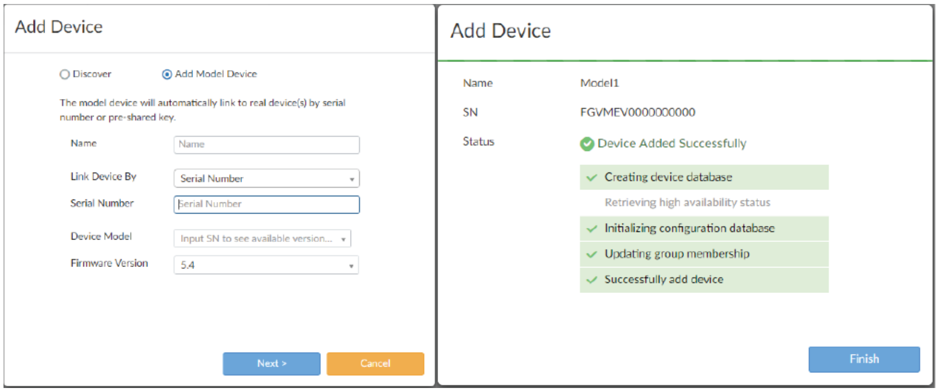
      For example, FG200D12345985242 is the original SN.

      Prefix: FG200D

      Appended 10 Digits: 0000000001

      The new SN will be: FG200D0000000001.

c. Select *Add Model Device* and complete the wizard.



Add Device

○ Discover ● Add Model Device

The model device will automatically link to real device(s) by serial number or pre-shared key.

Name	Name
Link Device By	Serial Number
Serial Number	Serial Number
Device Model	Input SN to see available version...
Firmware Version	5.4

Add Device

Name	Model1
SN	FGVMEV0000000000
Status	✓ Device Added Successfully

✓ Creating device database
Retrieving high availability status
✓ Initializing configuration database
✓ Updating group membership
✓ Successfully add device

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

For further FortiManager information, refer to the FortiManager Administration Guides available on the Fortinet Document Library.

VPN Manager

This section contains the following topics:

- Configuring a full mesh VPN topology within a VPN console on page 80

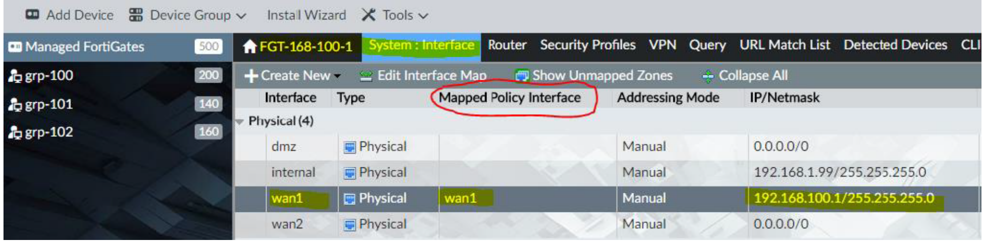
Configuring a full mesh VPN topology within a VPN console

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:

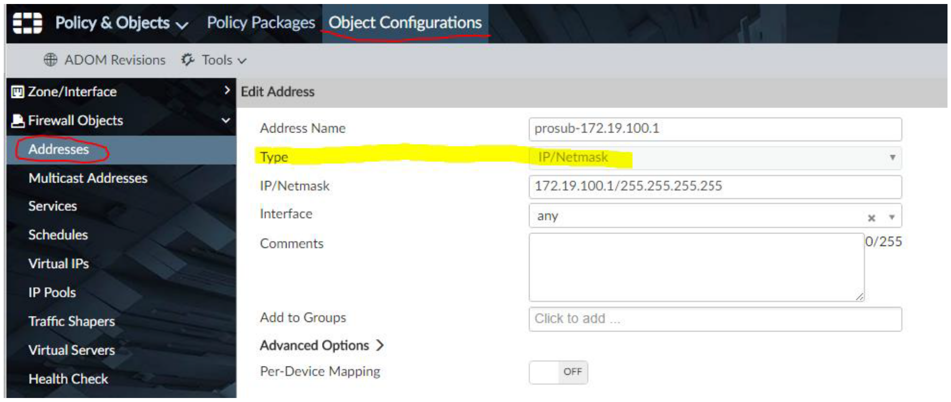
1. Add FortiGate devices and map all interfaces:
   a. Go to *Device Manager*. Add three FortiGate devices by clicking *Add Device*. Follow the wizard to add each device.
   b. Go to *Policy & Objects* > *Policy Packages* and define the *Zone* interfaces.
   c. Go to *Device Manager* and select a device.
   d. Go to *System: Interface* and map the interfaces to the *Zone* interfaces.



Interface	Type	Mapped Policy Interface	Addressing Mode	IP/Netmask
Physical (4)				
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

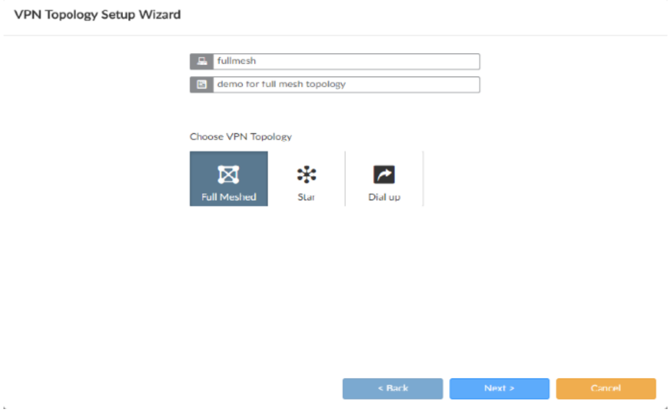
2. Create firewall addresses for protected subnets:
   a. Go to *Policy & Objects* > *Object Configurations* > *Firewall Objects* > *Address* to manage the firewall addresses.
   b. VPNs only support firewall addresses with the type set to *subnet (IP/Netmask)*. The firewall addresses will be

used as protected subnets to generate static routes among the FortiGate devices.



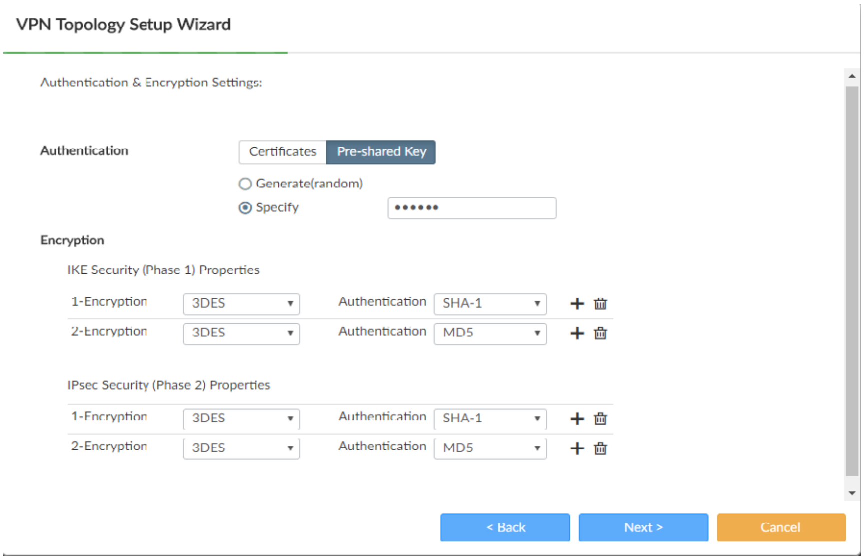
Address Name: prosub-172.19.100.1
Type: IP/Netmask
IP/Netmask: 172.19.100.1/255.255.255.255
Interface: any
Comments: 0/255
Add to Groups: Click to add ...
Per-Device Mapping: OFF

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



fullmesh
demo for full mesh topology

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


VPN Topology Setup Wizard
Authentication & Encryption Settings:
Certificates
Pre-shared Key
< Back
Next >
Cancel

Authentication: Pre-shared Key
○ Generate(random)
● Specify ••••••

Encryption

IKE Security (Phase 1) Properties

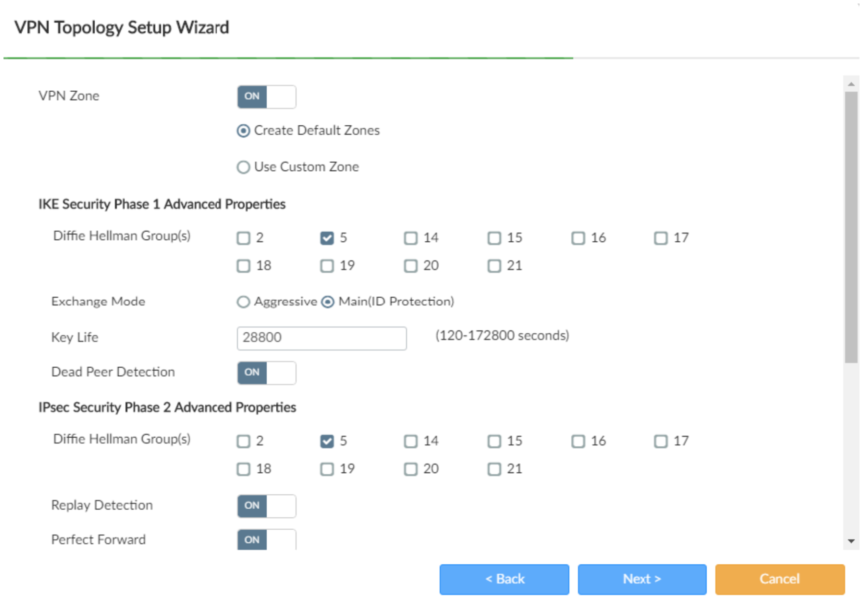
1-Encryption	3DES	Authentication	SHA-1
2-Encryption	3DES	Authentication	MD5

IPsec Security (Phase 2) Properties

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

   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 28800 (120-172800 seconds)

Dead Peer Detection ON

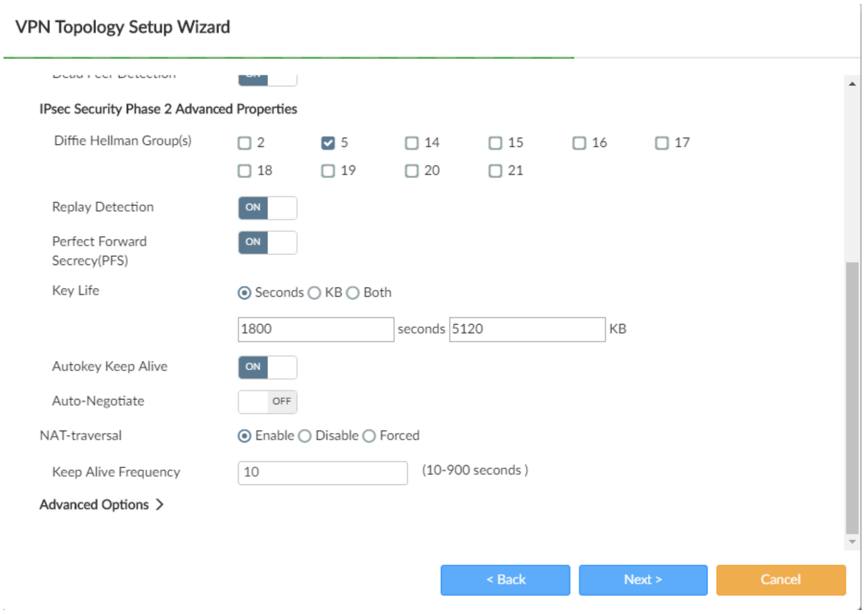
IPsec Security Phase 2 Advanced Properties

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

Replay Detection ON

Perfect Forward ON

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



VPN Topology Setup Wizard

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

1800 seconds 5120 KB

Autokey Keep Alive ON

Auto-Negotiate OFF

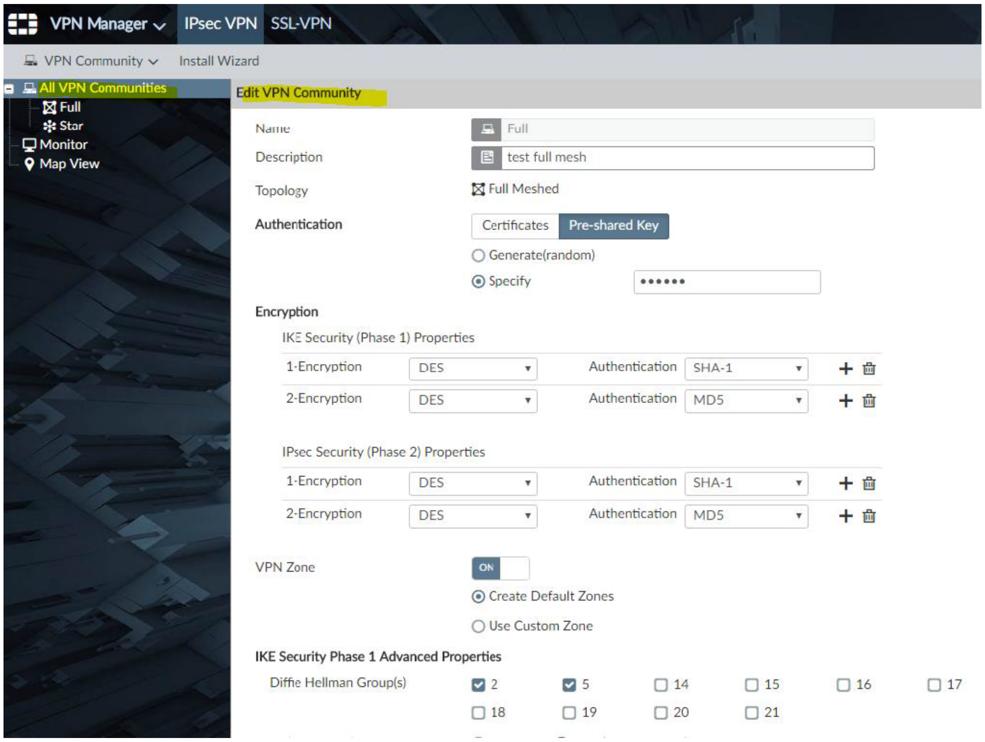
NAT-traversal ● Enable ○ Disable ○ Forced

Keep Alive Frequency 10 (10-900 seconds)

Advanced Options >

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

VPN configuration summary:



Edit VPN Community

Name: Full

Description: test full mesh

Topology: ☒ Full Meshed

Authentication: Certificates | 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

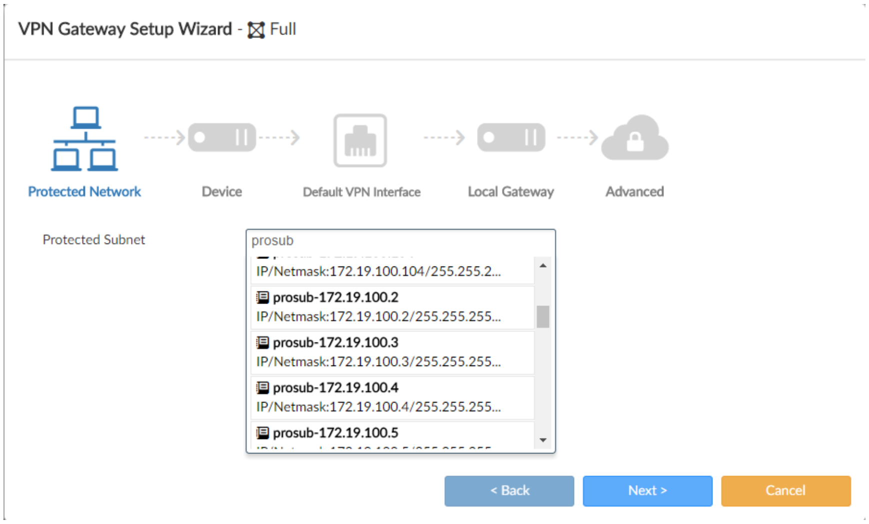
● Create Default Zones

○ Use Custom Zone

IKE Security Phase 1 Advanced Properties

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

4. Add a VPN gateway:
   a. Go to *VPN Manager* > *VPN Community*.
   b. In the content pane, from the *Create New* menu, select *Managed Gateway*.
   c. Add a *Protected Network*. There can be more than one protected networks.



VPN Gateway Setup Wizard - ☒ Full

Protected Subnet: prosub

IP/Netmask:172.19.100.104/255.255.2...

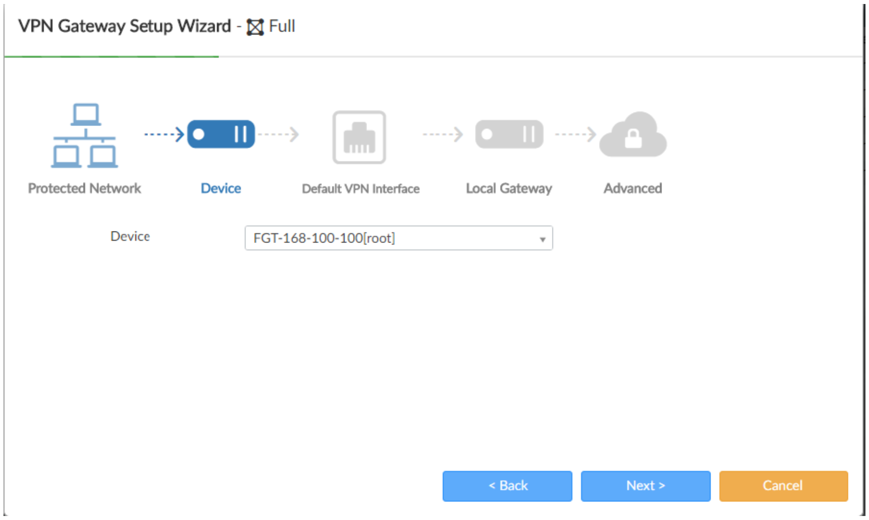
prosub-172.19.100.2
IP/Netmask:172.19.100.2/255.255.255...

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...

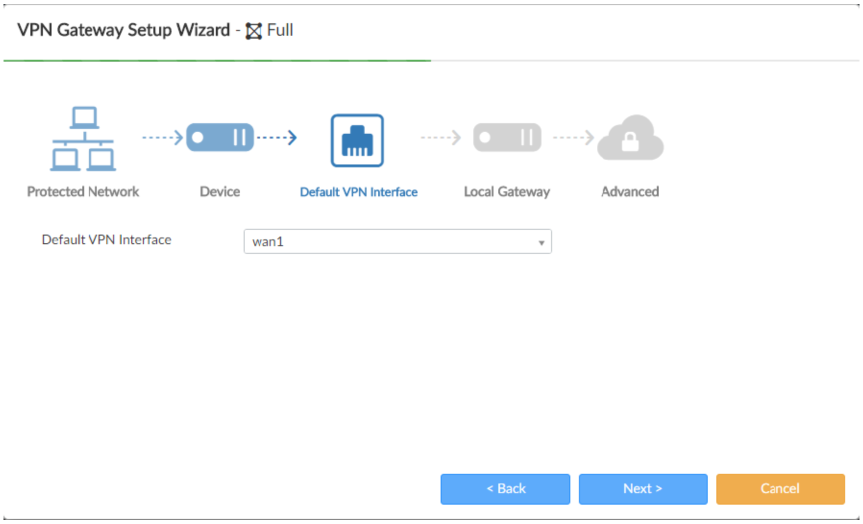
prosub-172.19.100.5

d. Select a *Device*.



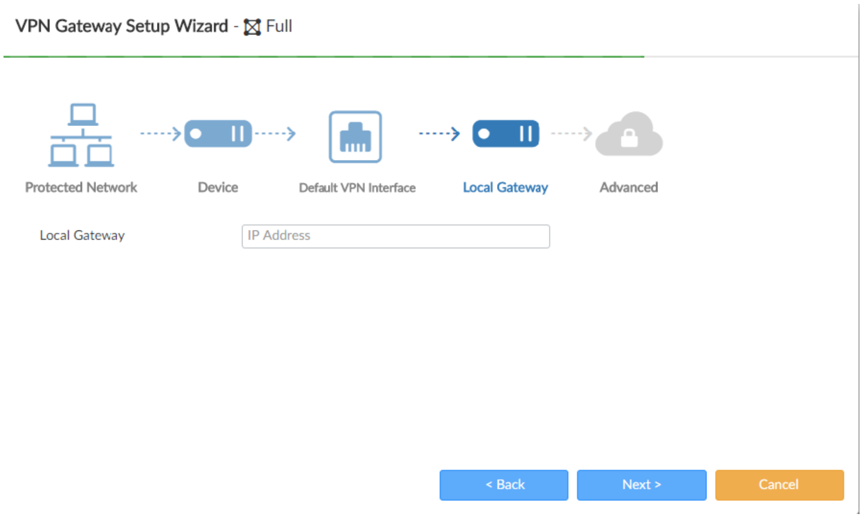
Device: FGT-168-100-100[root]

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



Default VPN Interface: wan1

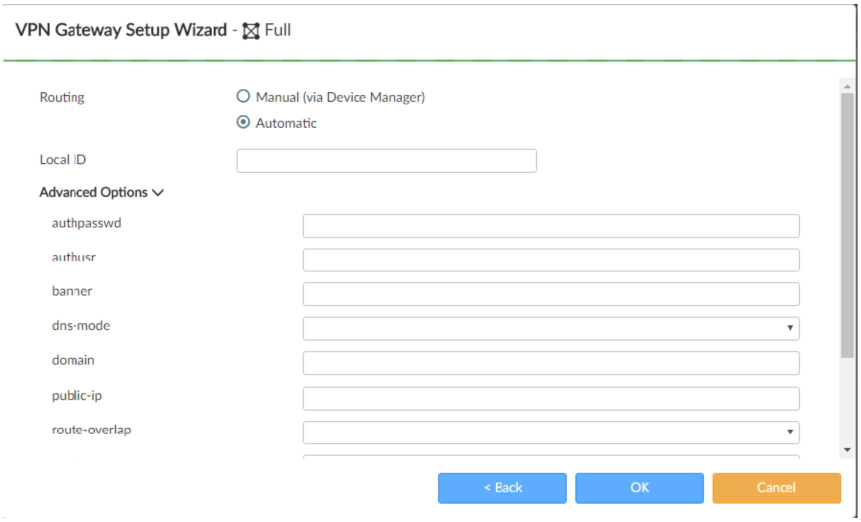
i. Optionally, specify the *Local Gateway*. This option can be left blank in most cases.



VPN Gateway Setup Wizard - ☒ Full

Local Gateway: IP Address

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:

authusr:

banner:

dns-mode: ▾

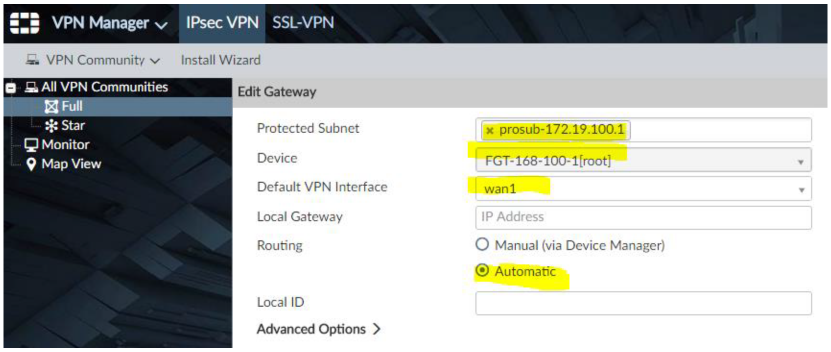
domain:

public-ip:

route-overlap: ▾

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

VPN gateway configuration settings summary:



Edit Gateway

Protected Subnet: × prosub-172.19.100.1

Device: FGT-168-100-1[root]

Default VPN Interface: wan1

Local Gateway: IP Address

Routing: ○ Manual (via Device Manager) ● Automatic

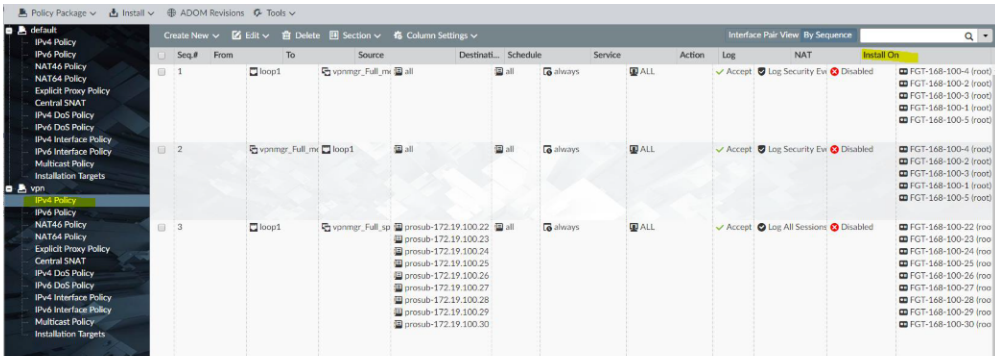
Local ID:

Advanced Options >

5. Create firewall policies:

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

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



□	Seq.#	From	To	Source	Destinati...	Schedule	Service	Action	Log	NAT	Install On
□	1	loop1	vpnmgr_Full_mı	all	all	always	ALL	✓ Accept	Log Security Evı	Disabled	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)
□	2	vpnmgr_Full_mı	loop1	all	all	always	ALL	✓ Accept	Log Security Evı	Disabled	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)
□	3	loop1	vpnmgr_Full_sp	prosub-172.19.100.22 prosub-172.19.100.23 prosub-172.19.100.24 prosub-172.19.100.25 prosub-172.19.100.26 prosub-172.19.100.27 prosub-172.19.100.28 prosub-172.19.100.29 prosub-172.19.100.30	all	always	ALL	✓ Accept	Log All Sessions	Disabled	FGT-168-100-22 (roo FGT-168-100-23 (roo FGT-168-100-24 (roo FGT-168-100-25 (roo FGT-168-100-26 (roo FGT-168-100-27 (roo FGT-168-100-28 (roo FGT-168-100-29 (roo FGT-168-100-30 (roo

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

For further FortiManager information, refer to the FortiManager Administration Guide available on the Fortinet Document Library.

FortiSwitch Manager

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

- Using central management on page 87
- Using per-device management on page 92
- Installing changes to FortiSwitch devices on page 95
- Upgrading FortiSwitch firmware on page 97
- Using zero touch deployment for FortiSwitch on page 98

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 87.
2. Create templates.
   You can import templates from managed switches, or you can create new templates. See Importing and editing FortiSwitch templates on page 88 or Creating FortiSwitch templates on page 89.
3. Assign templates to managed switches. See Assigning templates to FortiSwitch devices on page 92.
4. Install changes to managed switches. See Installing changes to FortiSwitch devices on page 95.

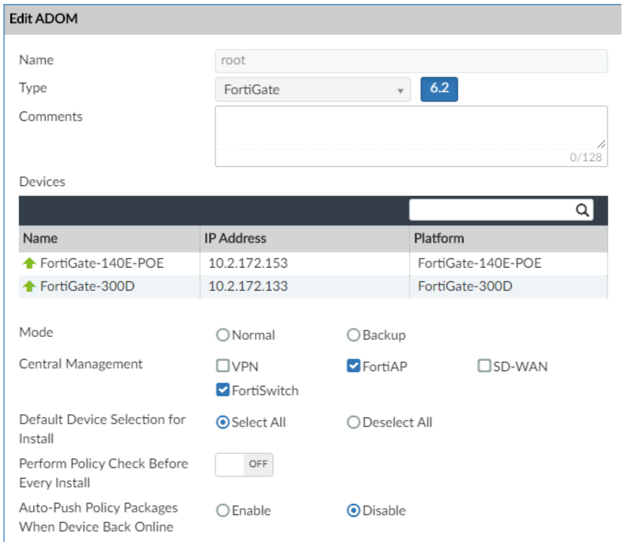
Enabling FortiSwitch central management

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 ☑ FortiSwitch	☑ FortiAP	□ SD-WAN
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	

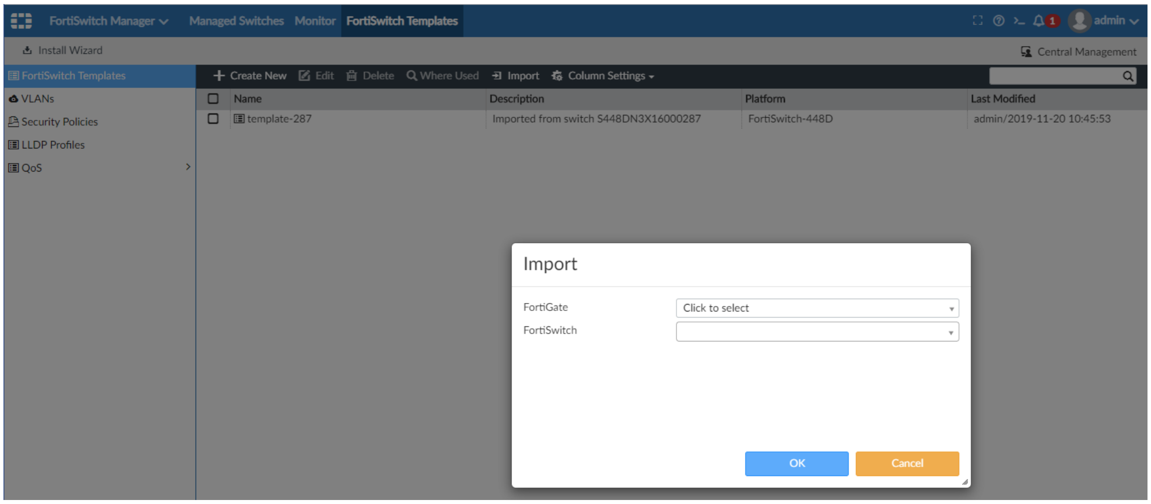
Central management is enabled for FortiSwitch.

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.



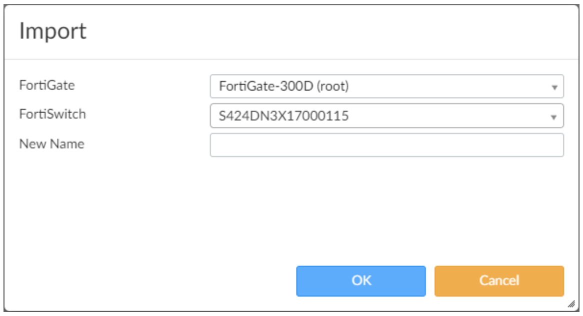
Name	Description	Platform	Last Modified
template-287	Imported from switch S448DN3X16000287	FortiSwitch-448D	admin/2019-11-20 10:45:53

Import

FortiGate	Click to select
FortiSwitch	

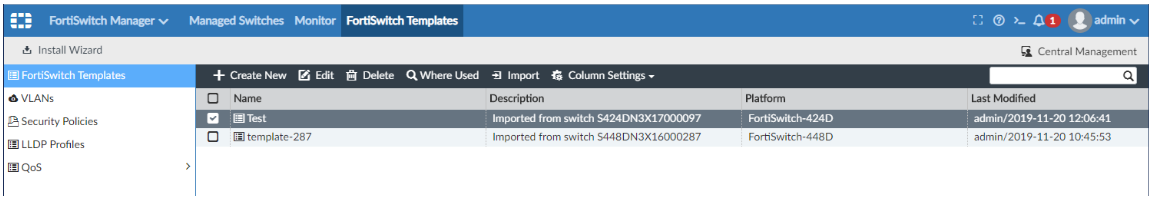
3. Set the following options, and click *OK*.
   a. In the *FortiGate* list, select a FortiGate.
   b. In the *FortiSwitch* list, select the FortiSwitch from which to import the template.

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.



FortiGate	FortiGate-300D (root)
FortiSwitch	S424DN3X17000115
New Name	

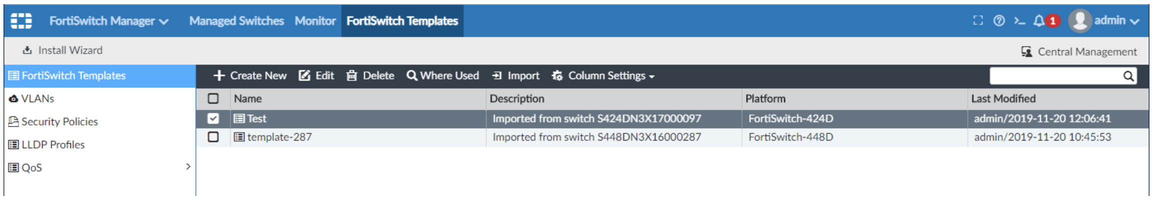
The template is imported and displayed on the content pane.



	Name	Description	Platform	Last Modified
☑	Test	Imported from switch S424DN3X17000097	FortiSwitch-424D	admin/2019-11-20 12:06:41
□	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
☑	Test	Imported from switch S424DN3X17000097	FortiSwitch-424D	admin/2019-11-20 12:06:41
□	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.

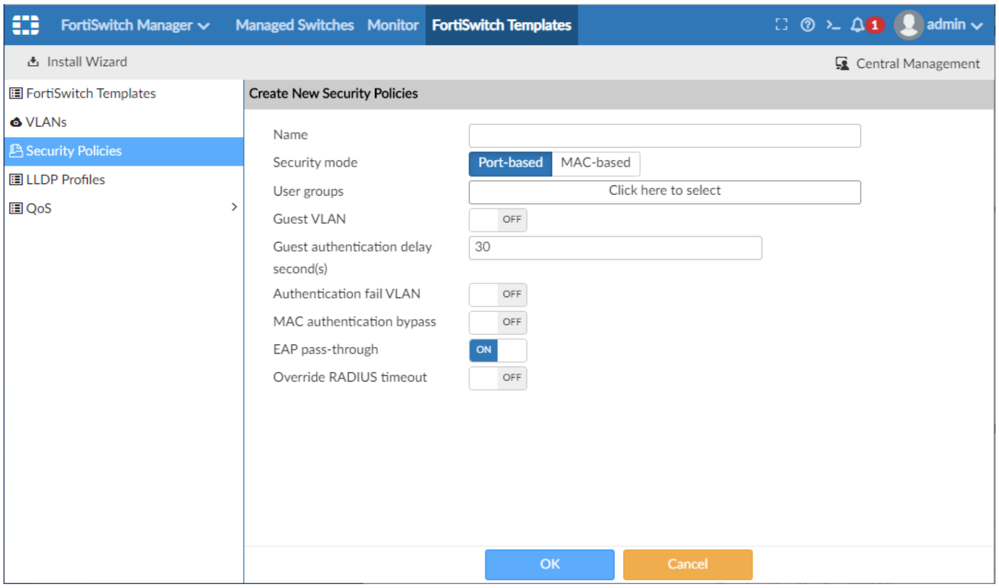
You can create the following components, and then create a variety of templates that select different combinations of the components:

- 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.



Create New Security Policies

Name

Security mode: Port-based | MAC-based

User groups: Click here to select

Guest VLAN: OFF

Guest authentication delay second(s): 30

Authentication fail VLAN: OFF

MAC authentication bypass: OFF

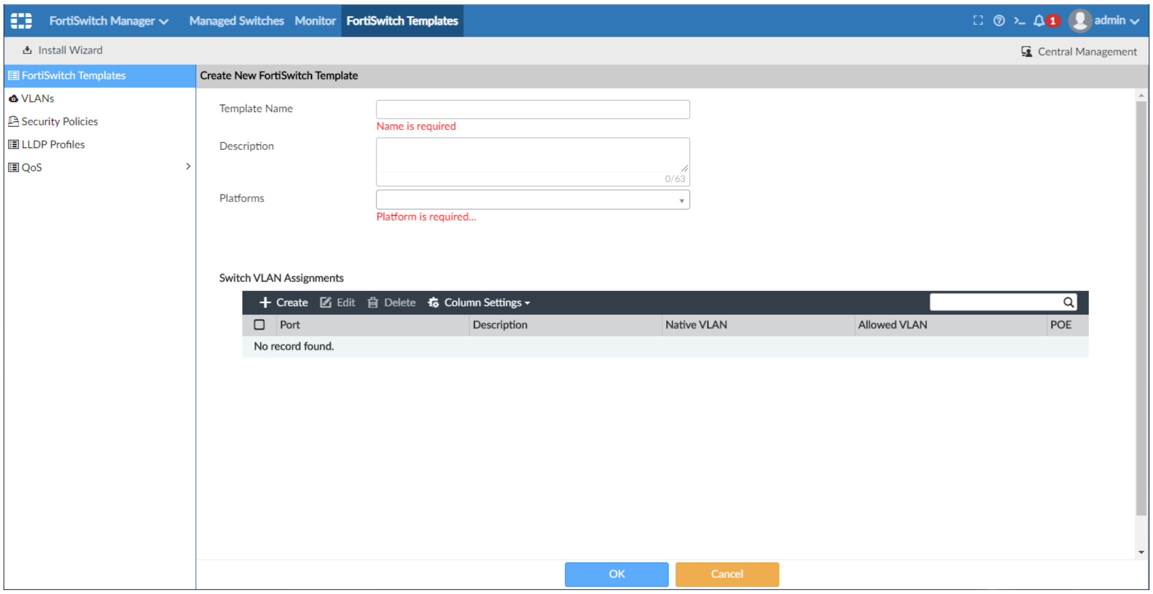
EAP pass-through: ON

Override RADIUS timeout: OFF

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.



Create New FortiSwitch Template

Template Name
Name is required

Description
0/63

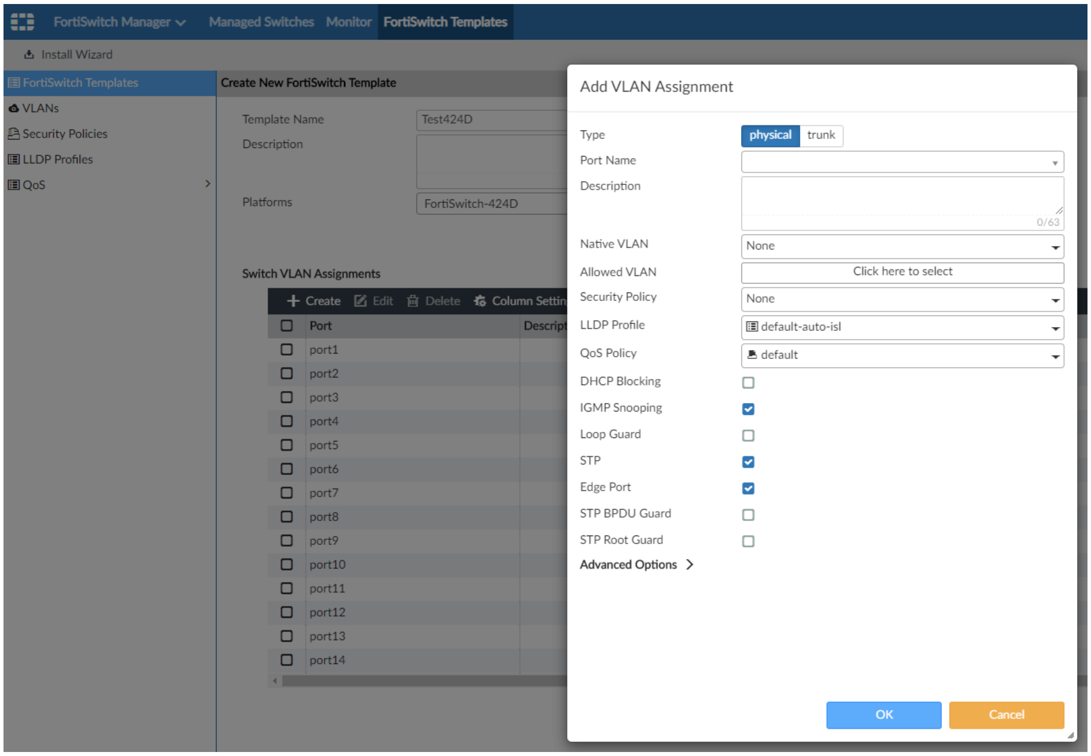
Platforms
Platform is required...

Switch VLAN Assignments

Create | Edit | Delete | Column Settings

Port	Description	Native VLAN	Allowed VLAN	POE
No record found.				

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.



Create New FortiSwitch Template

Template Name: Test424D
Description
Platforms: FortiSwitch-424D

Add VLAN Assignment

Type	physical | trunk
Port Name	
Description	0/63
Native VLAN	None
Allowed VLAN	Click here to select
Security Policy	None
LLDP Profile	default-auto-isl
QoS Policy	default
DHCP Blocking	□
IGMP Snooping	☑
Loop Guard	□
STP	☑
Edge Port	☑
STP BPDU Guard	□
STP Root Guard	□

   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 also assign templates when editing a FortiSwitch device.

6. Install the template settings. See Installing changes to FortiSwitch devices on page 95.

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:

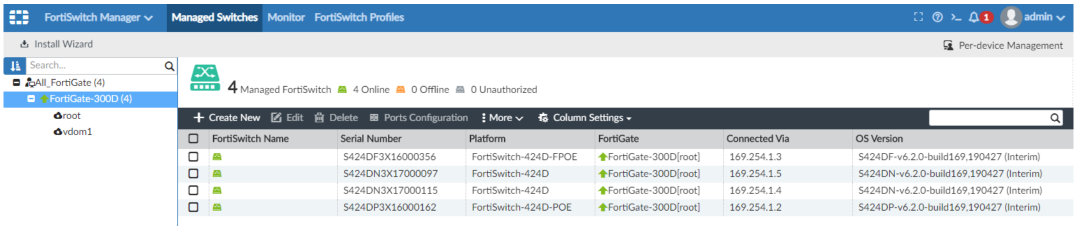
1. Enable per-device management. See Enabling FortiSwitch per-device management on page 93.
2. Configure profiles for managed switches.
   You can configure VLANs, security policies, LLDP profiles, and QoS policies, and the changes are saved to the FortiGate database. See Configuring FortiSwitch profiles on page 93.
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 94.
4. Install changes to managed switches. See Installing changes to FortiSwitch devices on page 95.

Enabling FortiSwitch per-device management

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

To enable FortiSwitch per-device management:

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



□	FortiSwitch Name	Serial Number	Platform	FortiGate	Connected Via	OS Version
□		S424DF3X16000356	FortiSwitch-424D-FPOE	FortiGate-300D[root]	169.254.1.3	S424DF-v6.2.0-build169,190427 (Interim)
□		S424DN3X17000097	FortiSwitch-424D	FortiGate-300D[root]	169.254.1.5	S424DN-v6.2.0-build169,190427 (Interim)
□		S424DN3X17000115	FortiSwitch-424D	FortiGate-300D[root]	169.254.1.4	S424DN-v6.2.0-build169,190427 (Interim)
□		S424DP3X16000162	FortiSwitch-424D-POE	FortiGate-300D[root]	169.254.1.2	S424DP-v6.2.0-build169,190427 (Interim)

Configuring FortiSwitch profiles

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

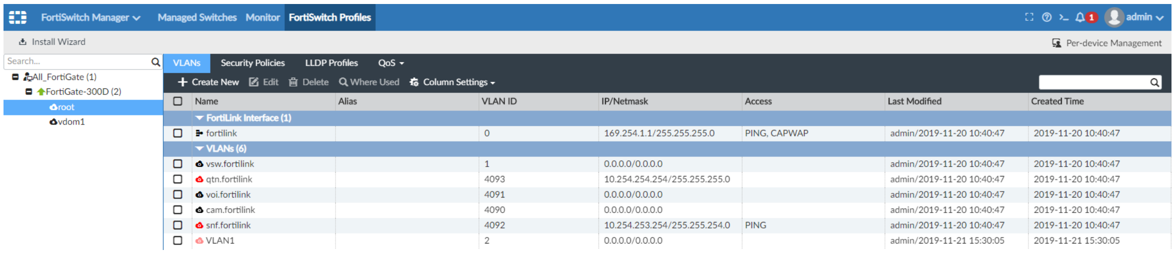
You can configure the following types of profiles and policies:

- VLANs
- Security policies
- LLDP profiles
- QoS policies

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

To configure VLANs:

1. Go to *FortiSwitch Manager > FortiSwitch Profiles*.
2. In the tree menu, select a FortiGate.
   The *VLAN* tab is displayed.



□	Name	Alias	VLAN ID	IP/Netmask	Access	Last Modified	Created Time
	FortiLink Interface (1)						
□	fortilink		0	169.254.1.1/255.255.255.0	PING, CAPWAP	admin/2019-11-20 10:40:47	2019-11-20 10:40:47
	VLANs (6)						
□	vsw.fortilink		1	0.0.0.0/0.0.0.0		admin/2019-11-20 10:40:47	2019-11-20 10:40:47
□	qtn.fortilink		4093	10.254.254.254/255.255.255.0		admin/2019-11-20 10:40:47	2019-11-20 10:40:47
□	voi.fortilink		4091	0.0.0.0/0.0.0.0		admin/2019-11-20 10:40:47	2019-11-20 10:40:47
□	cam.fortilink		4090	0.0.0.0/0.0.0.0		admin/2019-11-20 10:40:47	2019-11-20 10:40:47
□	snf.fortilink		4092	10.254.253.254/255.255.254.0	PING	admin/2019-11-20 10:40:47	2019-11-20 10:40:47
□	VLAN1		2	0.0.0.0/0.0.0.0		admin/2019-11-21 15:30:05	2019-11-21 15:30:05

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:

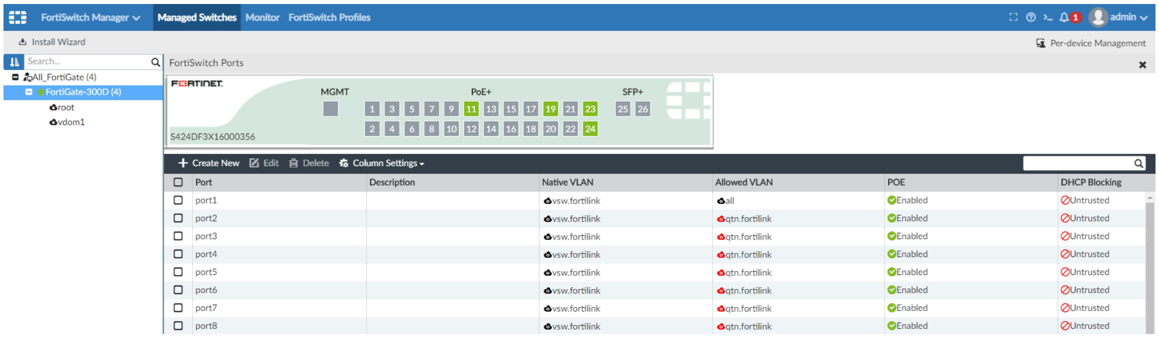
1. Go to *FortiSwitch Manager* > *FortiSwitch Profiles*.
2. In the tree menu, select a FortiGate.
   The *VLAN* tab is displayed.
3. From the *QoS* menu, select a type of policy.
4. Double-click the policy to open it for editing, or click *Create New* to create a new policy.
5. Edit the options, and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

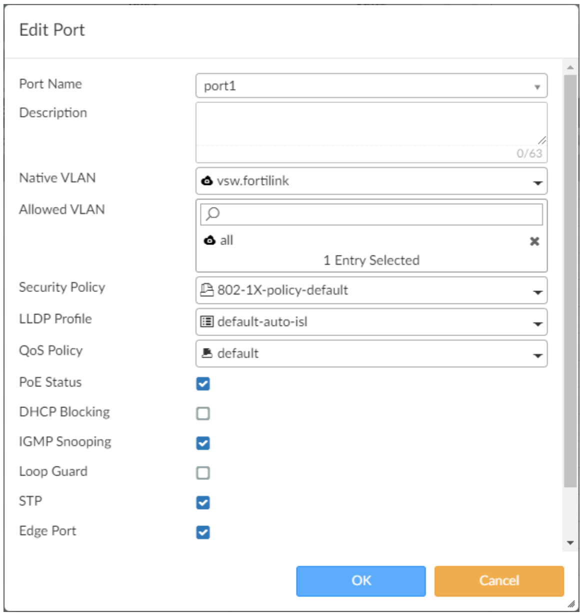
To configure switch ports:

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.



□	Port	Description	Native VLAN	Allowed VLAN	POE	DHCP Blocking
□	port1		vsw.fortilink	all	Enabled	Untrusted
□	port2		vsw.fortilink	qtn.fortilink	Enabled	Untrusted
□	port3		vsw.fortilink	qtn.fortilink	Enabled	Untrusted
□	port4		vsw.fortilink	qtn.fortilink	Enabled	Untrusted
□	port5		vsw.fortilink	qtn.fortilink	Enabled	Untrusted
□	port6		vsw.fortilink	qtn.fortilink	Enabled	Untrusted
□	port7		vsw.fortilink	qtn.fortilink	Enabled	Untrusted
□	port8		vsw.fortilink	qtn.fortilink	Enabled	Untrusted

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



Edit Port

Port Name	port1
Description	0/63
Native VLAN	vsw.fortilink
Allowed VLAN	all 1 Entry Selected
Security Policy	802-1X-policy-default
LLDP Profile	default-auto-isl
QoS Policy	default
PoE Status	☑
DHCP Blocking	□
IGMP Snooping	☑
Loop Guard	□
STP	☑
Edge Port	☑

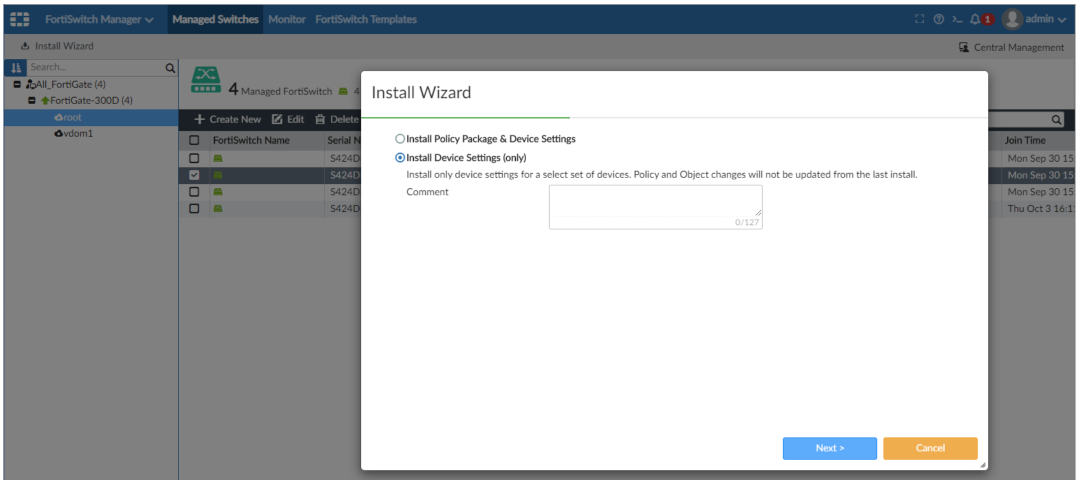
5. Edit the options and click *OK*.
   The changes are saved to the FortiGate database.
6. Install the changes. See Installing changes to FortiSwitch devices on page 95.

Installing changes to FortiSwitch devices

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

To install changes to switches:

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



Install Wizard

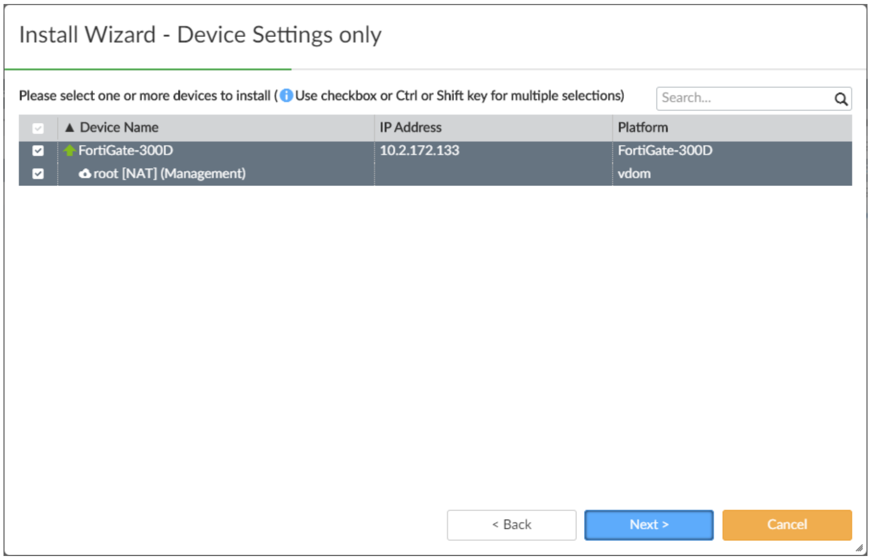
○ Install Policy Package & Device Settings

● Install Device Settings (only)

Install only device settings for a select set of devices. Policy and Object changes will not be updated from the last install.

Comment 0/127

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

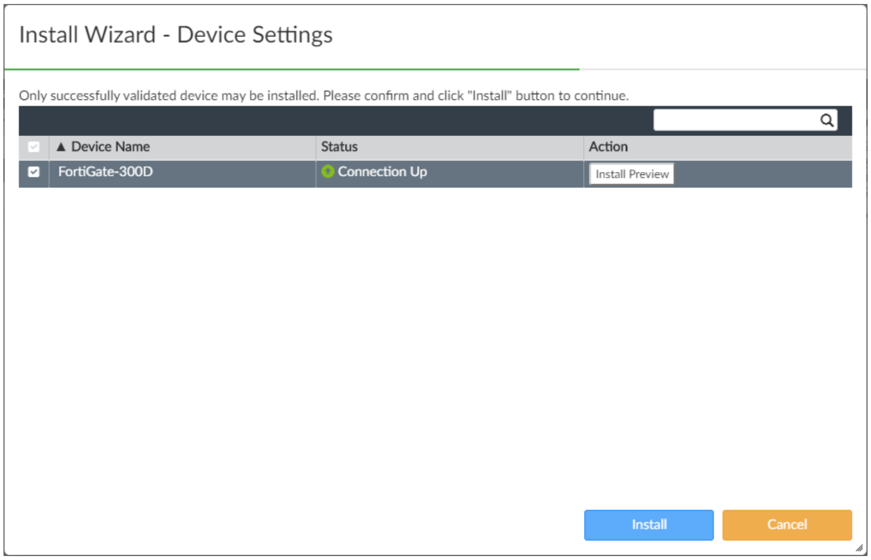


Install Wizard - Device Settings only

Please select one or more devices to install (Use checkbox or Ctrl or Shift key for multiple selections)

□	▲ Device Name	IP Address	Platform
☑	FortiGate-300D	10.2.172.133	FortiGate-300D
☑	root [NAT] (Management)		vdom

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



Install Wizard - Device Settings

Only successfully validated device may be installed. Please confirm and click "Install" button to continue.

☑	▲ Device Name	Status	Action
☑	FortiGate-300D	● Connection Up	Install Preview

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

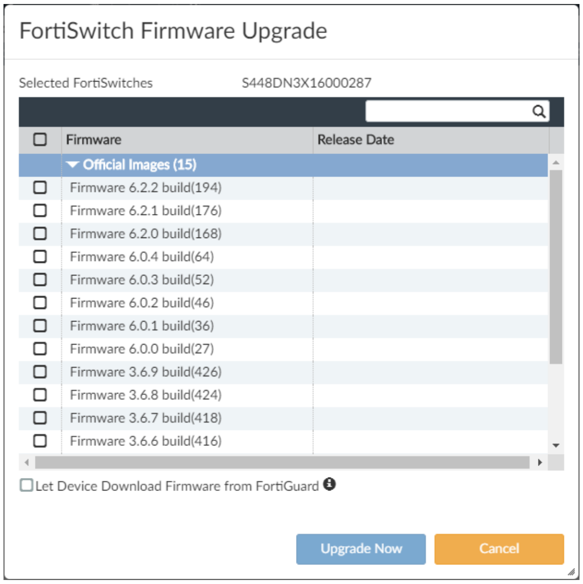
Upgrading FortiSwitch firmware

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

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

To upgrade FortiSwitch firmware:

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



FortiSwitch Firmware Upgrade

Selected FortiSwitches S448DN3X16000287

□	Firmware	Release Date
	Official Images (15)	
□	Firmware 6.2.2 build(194)	
□	Firmware 6.2.1 build(176)	
□	Firmware 6.2.0 build(168)	
□	Firmware 6.0.4 build(64)	
□	Firmware 6.0.3 build(52)	
□	Firmware 6.0.2 build(46)	
□	Firmware 6.0.1 build(36)	
□	Firmware 6.0.0 build(27)	
□	Firmware 3.6.9 build(426)	
□	Firmware 3.6.8 build(424)	
□	Firmware 3.6.7 build(418)	
□	Firmware 3.6.6 build(416)	

□ Let Device Download Firmware from FortiGuard

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.

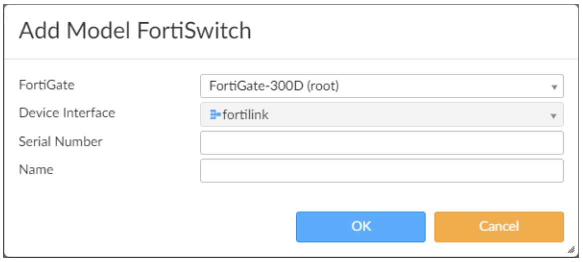
Requirements:

- 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.



Add Model FortiSwitch

FortiGate: FortiGate-300D (root)

Device Interface: fortilink

Serial Number:

Name:

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

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

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

4. Click *Close* to close the *Add Model FortiSwitch* pane.
5. Configure the switch.
   - For *FortiSwitch Manager* with central management enabled, see Assigning templates to FortiSwitch devices on page 92.
   - For *FortiSwitch Manager* with per-device management enabled, see Configuring FortiSwitch ports on page 94.

   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 100
- Creating administrator accounts with restricted access on page 102

Configuring and debugging FortiManager HA clusters

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

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

1. Configure the primary FortiManager unit. See Configuring the primary FortiManager unit in an HA cluster on page 100
2. Configure one or more backup FortiManager units. See Configuring backup FortiManager units in an HA cluster on page 101
3. If you encounter problems, review the debug log for each unit in an HA cluster. See Generating and downloading HA debug logs on page 101.

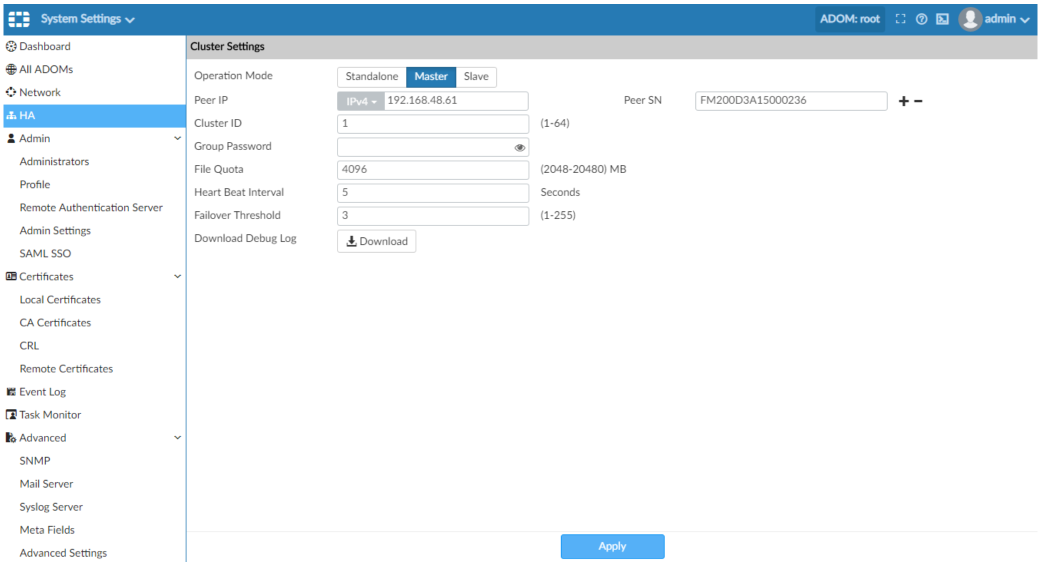
Configuring the primary FortiManager unit in an HA cluster

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

To configure the primary FortiManager unit:

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

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



Operation Mode: Standalone | **Master** | Slave

Peer IP: IPv4 192.168.48.61 Peer SN: FM200D3A15000236 + −

Cluster ID: 1 (1-64)

Group Password:

File Quota: 4096 (2048-20480) MB

Heart Beat Interval: 5 Seconds

Failover Threshold: 3 (1-255)

Download Debug Log: Download

6. Click *Apply*.

Configuring backup FortiManager units in an HA cluster

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

To configure the backup FortiManager unit:

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.
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 (secondary) 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*.

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:

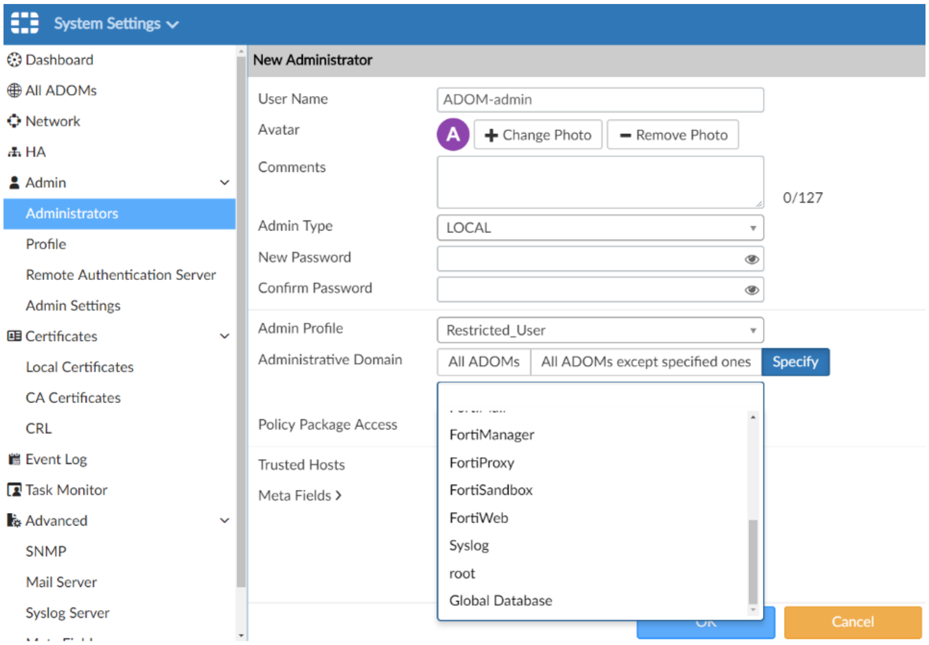
- ADOMs - see Restricting administrator access to ADOMs on page 102
- Device groups - see Restricting administrator access to device groups on page 104
- Policy packages - see Restricting administrator access to policy packages on page 106

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:

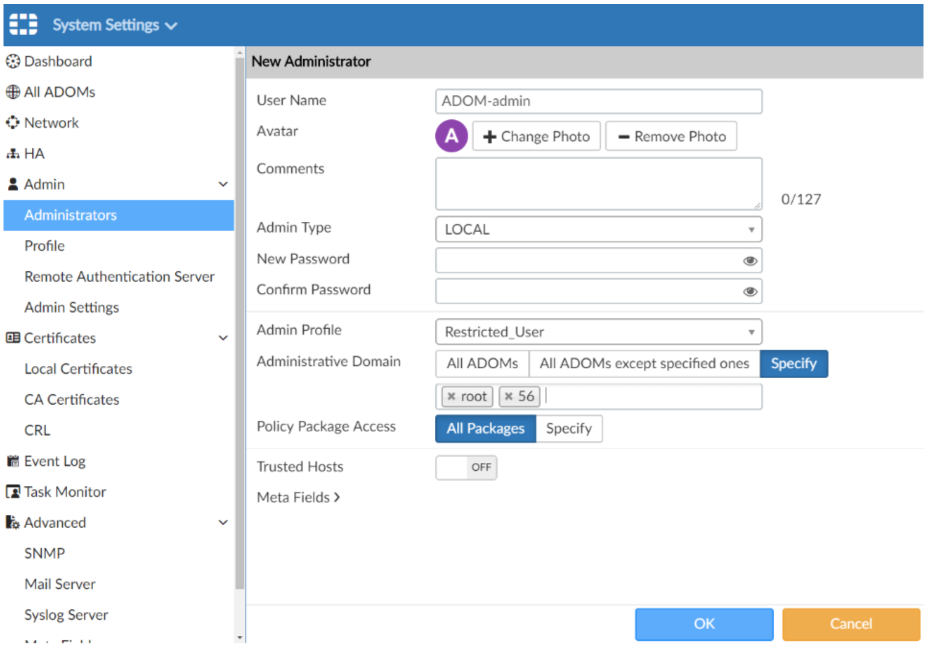
1. Go to *System Settings* > *Administrators*.
2. Click *Create New*.
3. Beside *Administrative Domain*, click *Specify*, and then select the ADOMs that the administrator account can access.



New Administrator

User Name: ADOM-admin
Comments: 0/127
Admin Type: LOCAL
Admin Profile: Restricted_User
Administrative Domain: Specify

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



User Name: ADOM-admin

Avatar

Comments

Admin Type: LOCAL

New Password

Confirm Password

Admin Profile: Restricted_User

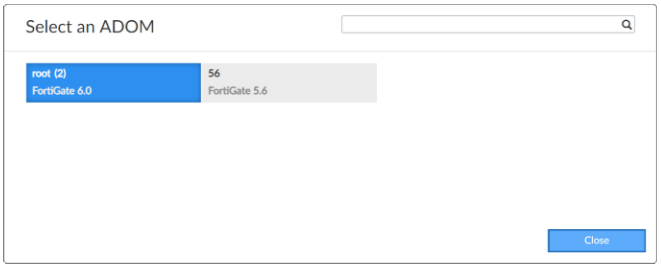
Administrative Domain: Specify

× root × 56

Policy Package Access: All Packages

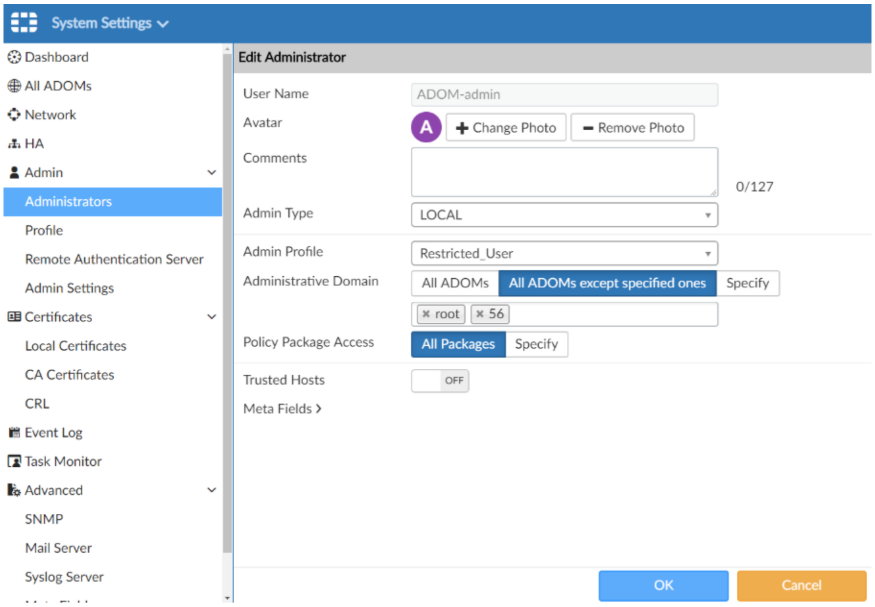
Trusted Hosts: OFF

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*.



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

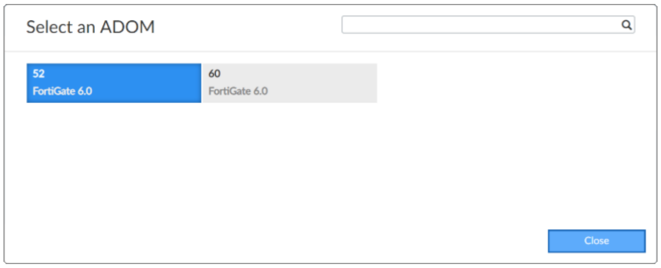
1. Go to *System Settings > Administrators*.
2. Click *Create New*.
3. Beside *Administrative Domain*, click *All ADOMs except specified ones*, and then select the ADOMs that you do not want the administrator account to access.
   In this example, the *root* and *56* ADOMs are excluded from access.



Edit Administrator

User Name: ADOM-admin
Avatar: A
Comments: 0/127
Admin Type: LOCAL
Admin Profile: Restricted_User
Administrative Domain: All ADOMs | All ADOMs except specified ones | Specify
× root × 56
Policy Package Access: All Packages | Specify
Trusted Hosts: OFF
Meta Fields ›

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



Select an ADOM

52
FortiGate 6.0

60
FortiGate 6.0

Restricting administrator access to device groups

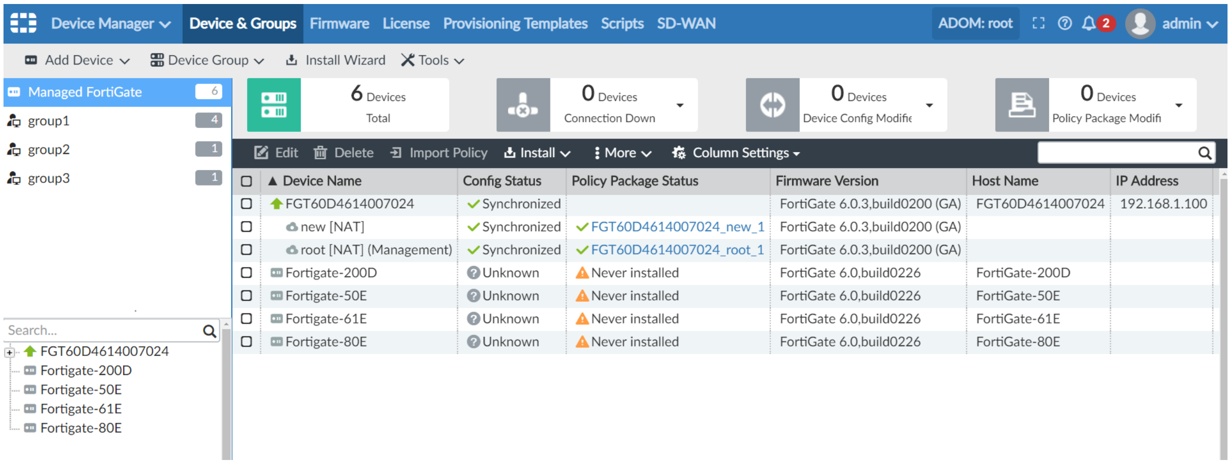
On the *Device Manager* pane, you can create device groups and add devices to the different groups. If you are using ADOMs, select the ADOM, and then create the device group.

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

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

To create a device group:

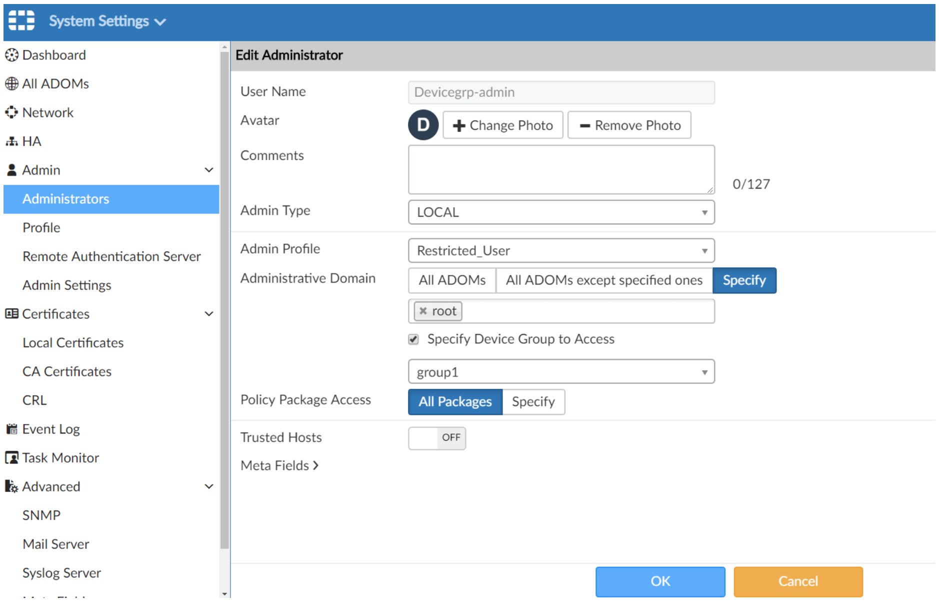
1. Go to *Device Manager* > *Device & Groups*.
2. If you are using ADOMs, select the ADOM that you are creating a device group in. Otherwise skip this step.
3. In the *Device Group* menu, click *Create New*.
4. Enter a name for the group and add devices to it, then click *OK*.
   In this example, the root ADOM contains *group1*, *group2*, and *group3*.



Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	IP Address
FGT60D4614007024	✓ Synchronized		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	
Fortigate-61E	Unknown	Never installed	FortiGate 6.0,build0226	FortiGate-61E	
Fortigate-80E	Unknown	Never installed	FortiGate 6.0,build0226	FortiGate-80E	

To specify admin access to device groups:

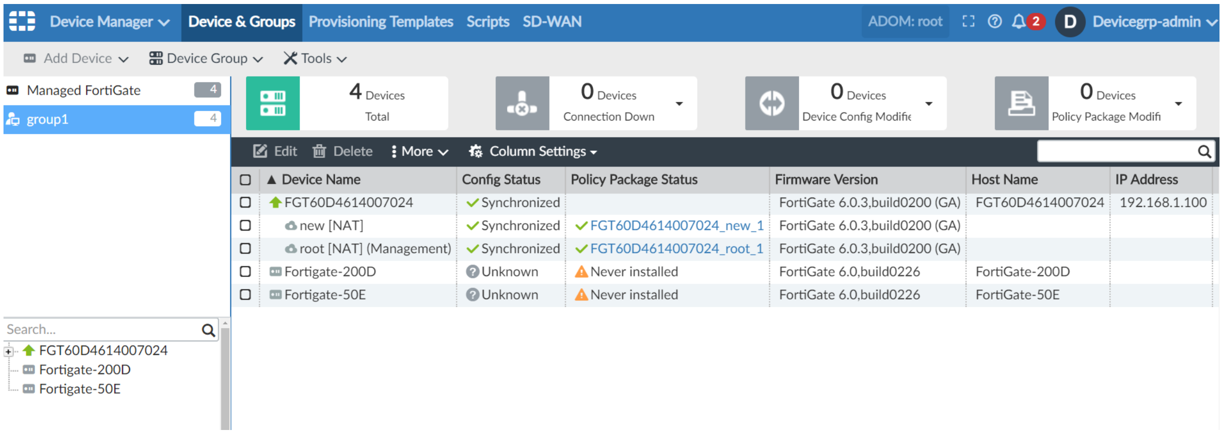
1. Go to *System Settings > Administrators*.
2. Click *Create New*.
3. Beside *Administrative Domain*, click *Specify*.
4. Select the ADOM that contains the device group. Select only one ADOM.
5. Select *Specify Device Group to Access*, and then select the device group.
   In this example, *group1* is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



Edit Administrator

User Name: Devicegrp-admin
Avatar: D
Comments: 0/127
Admin Type: LOCAL
Admin Profile: Restricted_User
Administrative Domain: All ADOMs | All ADOMs except specified ones | Specify
root
☑ Specify Device Group to Access
group1
Policy Package Access: All Packages | Specify
Trusted Hosts: OFF
Meta Fields

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*.



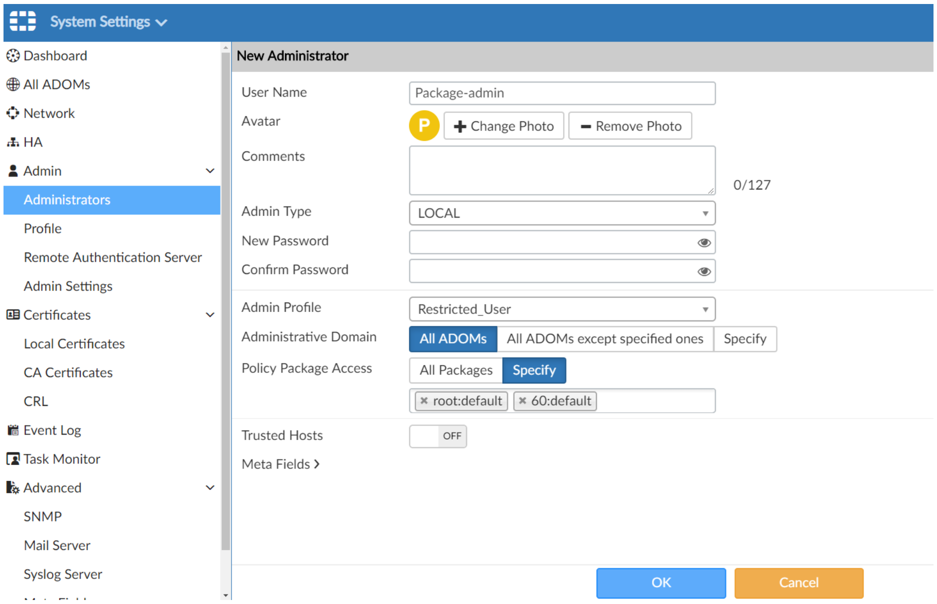
Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	IP Address
FGT60D4614007024	✓ Synchronized		FortiGate 6.0.3,build0200 (GA)	FGT60D4614007024	192.168.1.100
new [NAT]	✓ Synchronized	✓ FGT60D4614007024_new_1	FortiGate 6.0.3,build0200 (GA)		
root [NAT] (Management)	✓ Synchronized	✓ 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.



New Administrator

User Name	Package-admin
Avatar	P
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	All Packages / Specify root:default, 60:default
Trusted Hosts	OFF
Meta Fields ›	

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

This section contains the following topics:

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

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:

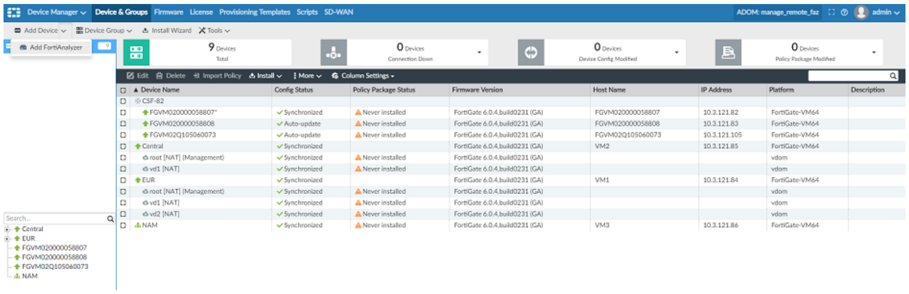
1. On the FortiAnalyzer unit, enable fgfm access on the interface used to connect to FortiManager.
   ```
   config system interface
   edit "port1"
   set ip 10.3.121.142 255.255.0.0
   set allowaccess fgfm
   next
   end
   ```
2. Ensure that FortiManager Features are disabled.
   ```
   config system 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.

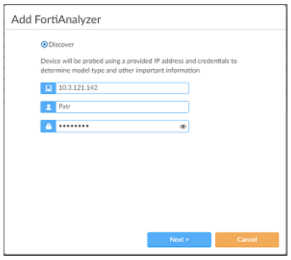
To add FortiAnalyzer to FortiManager:

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*.



Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	IP Address	Platform	Description
CSF-82							
FGVM020000058807*	✓ Synchronized	Never installed	FortiGate 6.0.4,build0231 (GA)	FGVM020000058807	10.3.121.82	FortiGate-VM64	
FGVM020000058808	✓ Auto-update	Never installed	FortiGate 6.0.4,build0231 (GA)	FGVM020000058808	10.3.121.83	FortiGate-VM64	
FGVM02Q105060073	✓ Auto-update	Never installed	FortiGate 6.0.4,build0231 (GA)	FGVM02Q105060073	10.3.121.105	FortiGate-VM64	
Central	✓ Synchronized		FortiGate 6.0.4,build0231 (GA)	VM2	10.3.121.85	FortiGate-VM64	
root [NAT] (Management)	✓ Synchronized	Never installed	FortiGate 6.0.4,build0231 (GA)			vdom	
vd1 [NAT]	✓ Synchronized	Never installed	FortiGate 6.0.4,build0231 (GA)			vdom	
EUR	✓ Synchronized		FortiGate 6.0.4,build0231 (GA)	VM1	10.3.121.84	FortiGate-VM64	
root [NAT] (Management)	✓ Synchronized	Never installed	FortiGate 6.0.4,build0231 (GA)			vdom	
vd1 [NAT]	✓ Synchronized	Never installed	FortiGate 6.0.4,build0231 (GA)			vdom	
vd2 [NAT]	✓ Synchronized	Never installed	FortiGate 6.0.4,build0231 (GA)			vdom	
NAM	✓ Synchronized	Never installed	FortiGate 6.0.4,build0231 (GA)	VM3	10.3.121.86	FortiGate-VM64	

   The *Add FortiAnalyzer* wizard is displayed.
   b. Type the FortiAnalyzer IP address, username, password, and click *Next*.



Add FortiAnalyzer

◉ Discover

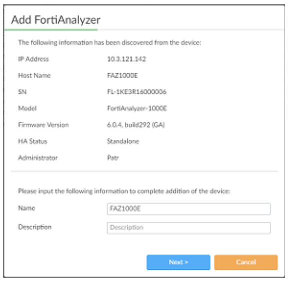
Device will be probed using a provided IP address and credentials to determine model type and other important information

10.3.121.142

Patr

•••••••••

After FortiManager discovers the device, device information is displayed.



Add FortiAnalyzer

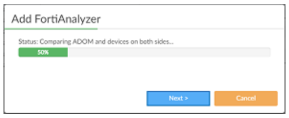
The following information has been discovered from the device:

IP Address	10.3.121.142
Host Name	FAZ1000E
SN	FL-1KE3R16000006
Model	FortiAnalyzer-1000E
Firmware Version	6.0.4, build292 (GA)
HA Status	Standalone
Administrator	Patr

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

Name	FAZ1000E
Description	Description

c. Click *Next* to continue.

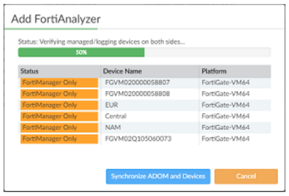


Add FortiAnalyzer

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

50%

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



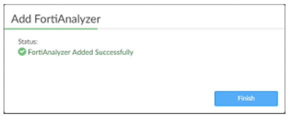
Add FortiAnalyzer

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

50%

Status	Device Name	Platform
FortiManager Only	FGVM020000058807	FortiGate-VM64
FortiManager Only	FGVM020000058808	FortiGate-VM64
FortiManager Only	EUR	FortiGate-VM64
FortiManager Only	Central	FortiGate-VM64
FortiManager Only	NAM	FortiGate-VM64
FortiManager Only	FGVM02Q105060073	FortiGate-VM64

d. Click *Synchronize ADOM and Devices* to continue.
Devices are synchronized between FortiAnalyzer and FortiManager, and FortiAnalyzer is added to FortiManager.The synchronized devices are added to FortiAnalyzer as logging-mode FortiGates.



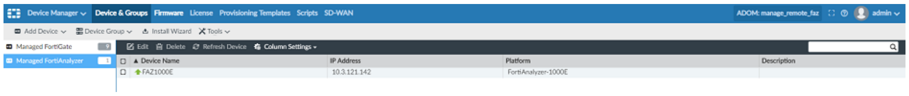
Add FortiAnalyzer

Status:
✓ FortiAnalyzer Added Successfully

FortiAnalyzer is added to FortiManager.

e. Click *Finish*.

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



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

Additional information

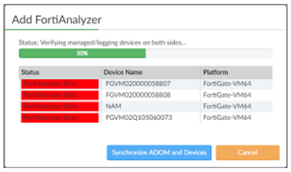
This section describes some of the other scenarios you might encounter when adding FortiAnalyzer units to FortiManager.

Missing ADOM

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

Unknown or mismatched FortiGate devices

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

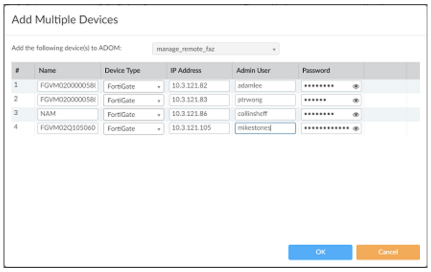

Add FortiAnalyzer

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

50%

Status	Device Name	Platform
FortiAnalyzer Only	FGVM020000058807	FortiGate-VM64
FortiAnalyzer Only	FGVM020000058808	FortiGate-VM64
FortiAnalyzer Only	NAM	FortiGate-VM64
FortiAnalyzer Only	FGVM02Q105060073	FortiGate-VM64

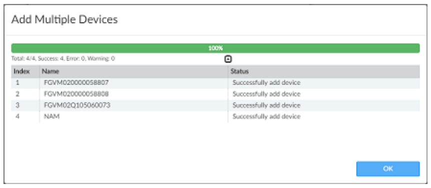
FortiManager automatically attempts to discover the FortiGates.


Add Multiple Devices

Add the following device(s) to ADOM: manage_remote_faz

#	Name	Device Type	IP Address	Admin User	Password
1	FGVM020000058	FortiGate	10.3.121.82	adamlee	•••••••••
2	FGVM02000005	FortiGate	10.3.121.83	ptrwong	••••••
3	NAM	FortiGate	10.3.121.86	collinsheff	•••••••••
4	FGVM02Q105060	FortiGate	10.3.121.105	mikestones	•••••••••••••

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


Add Multiple Devices

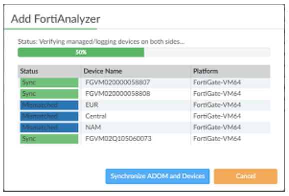
100%

Total: 4/4, Success: 4, Error: 0, Warning: 0

Index	Name	Status
1	FGVM020000058807	Successfully add device
2	FGVM020000058808	Successfully add device
3	FGVM02Q105060073	Successfully add device
4	NAM	Successfully add device

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*.

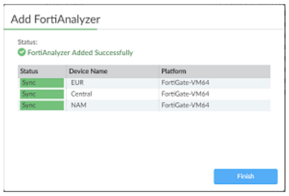

Add FortiAnalyzer

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

50%

Status	Device Name	Platform
Sync	FGVM020000058807	FortiGate-VM64
Sync	FGVM020000058808	FortiGate-VM64
Mismatched	EUR	FortiGate-VM64
Mismatched	Central	FortiGate-VM64
Mismatched	NAM	FortiGate-VM64
Sync	FGVM02Q105060073	FortiGate-VM64

FortiManager tries to synchronize the device settings to FortiAnalyzer.


Add FortiAnalyzer

Status:

✓ FortiAnalyzer Added Successfully

Status	Device Name	Platform
Sync	EUR	FortiGate-VM64
Sync	Central	FortiGate-VM64
Sync	NAM	FortiGate-VM64

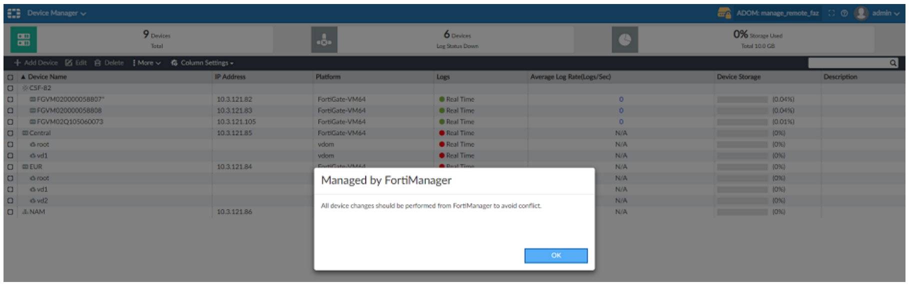
If any errors occur during the synchronization step, FortiManager fails to add FortiAnalyzer.

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.

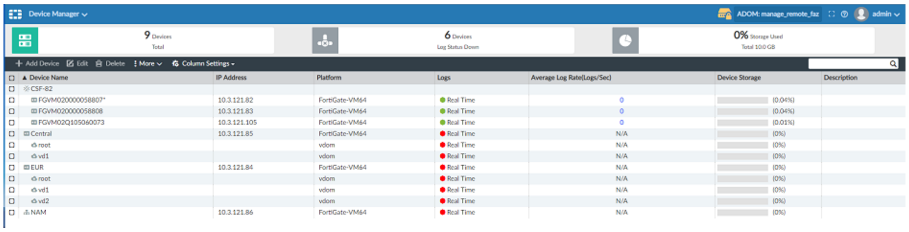


	▲ Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)	Device Storage	Description
□	CSF-82						
□	FGVM020000058807*	10.3.121.82	FortiGate-VM64	● Real Time	0	(0.04%)	
□	FGVM020000058808	10.3.121.83	FortiGate-VM64	● Real Time	0	(0.04%)	
□	FGVM02Q105060073	10.3.121.105	FortiGate-VM64	● Real Time	0	(0.01%)	
□	Central	10.3.121.85	FortiGate-VM64	● Real Time	N/A	(0%)	
□	root		vdom	● Real Time	N/A	(0%)	
□	vd1		vdom	● Real Time	N/A	(0%)	
□	EUR	10.3.121.84	FortiGate-VM64	● Real Time	N/A	(0%)	
□	root				N/A	(0%)	
□	vd1				N/A	(0%)	
□	vd2				N/A	(0%)	
□	NAM	10.3.121.86			N/A	(0%)	

Managed by FortiManager

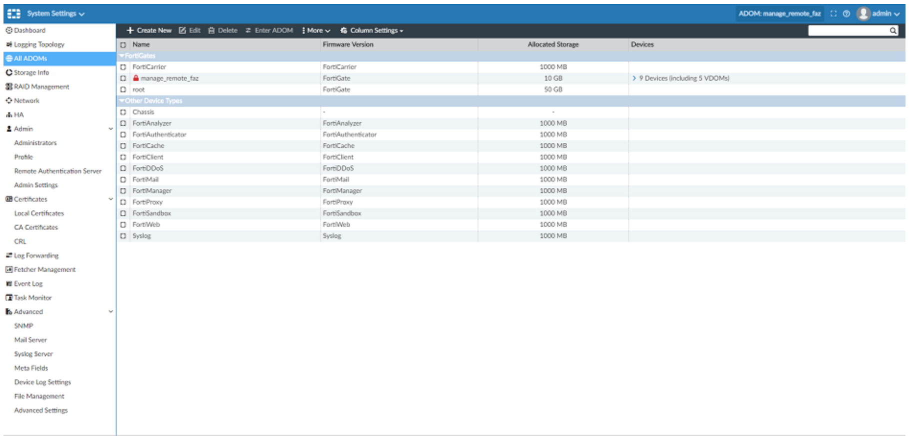
All device changes should be performed from FortiManager to avoid conflict.

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



	▲ Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)	Device Storage	Description
□	CSF-82						
□	FGVM020000058807*	10.3.121.82	FortiGate-VM64	● Real Time	0	(0.04%)	
□	FGVM020000058808	10.3.121.83	FortiGate-VM64	● Real Time	0	(0.04%)	
□	FGVM02Q105060073	10.3.121.105	FortiGate-VM64	● Real Time	0	(0.01%)	
□	Central	10.3.121.85	FortiGate-VM64	● Real Time	N/A	(0%)	
□	root		vdom	● Real Time	N/A	(0%)	
□	vd1		vdom	● Real Time	N/A	(0%)	
□	EUR	10.3.121.84	FortiGate-VM64	● Real Time	N/A	(0%)	
□	root		vdom	● Real Time	N/A	(0%)	
□	vd1		vdom	● Real Time	N/A	(0%)	
□	vd2		vdom	● Real Time	N/A	(0%)	
□	NAM	10.3.121.86	FortiGate-VM64	● Real Time	N/A	(0%)	

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.



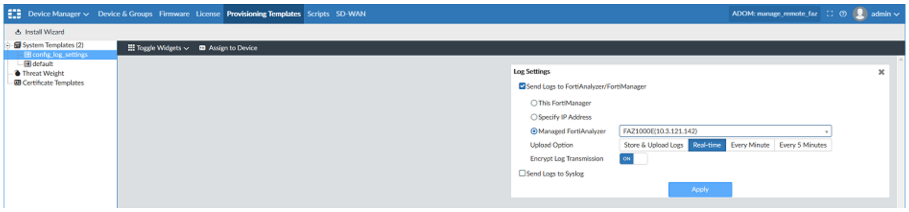
	Name	Firmware Version	Allocated Storage	Devices
	FortiGates			
□	FortiCarrier	FortiCarrier	1000 MB	
□	🔒 manage_remote_faz	FortiGate	10 GB	› 9 Devices (including 5 VDOMs)
□	root	FortiGate	50 GB	
	Other Device Types			
□	Chassis	-	-	
□	FortiAnalyzer	FortiAnalyzer	1000 MB	
□	FortiAuthenticator	FortiAuthenticator	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.



Log Settings

☑ Send Logs to FortiAnalyzer/FortiManager

○ This FortiManager
○ Specify IP Address
● Managed FortiAnalyzer: FAZ1000E(10.3.121.142)

Upload Option: Store & Upload Logs | **Real-time** | Every Minute | Every 5 Minutes

Encrypt Log Transmission: ON

□ Send Logs to Syslog

   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

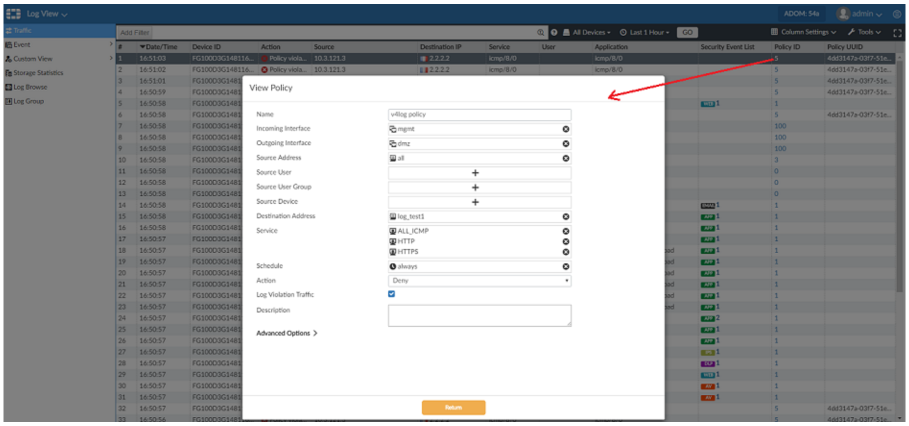
All FortiAnalyzer functionality is available, except for the following:

- 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.

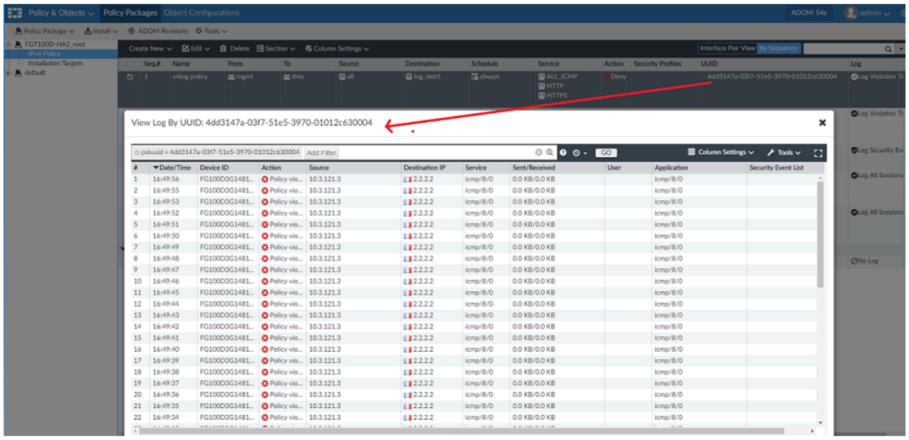


View Policy

Name	v4log policy
Incoming Interface	mgmt
Outgoing Interface	dmz
Source Address	all
Source User	+
Source User Group	+
Source Device	+
Destination Address	log_test1
Service	ALL_ICMP HTTP HTTPS
Schedule	always
Action	Deny
Log Violation Traffic	☑
Description	

Advanced Options >

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



	Seq.#	Name	From	To	Source	Destination	Schedule	Service	Action	Security Profiles	UUID	Log
☑	1	v4log policy	mgmt	dmz	all	log_test1	always	ALL_ICMP HTTP HTTPS	Deny		4dd3147a-03f7-51e5-3970-01012c630004	Log Violation Tr

View Log By UUID: 4dd3147a-03f7-51e5-3970-01012c630004

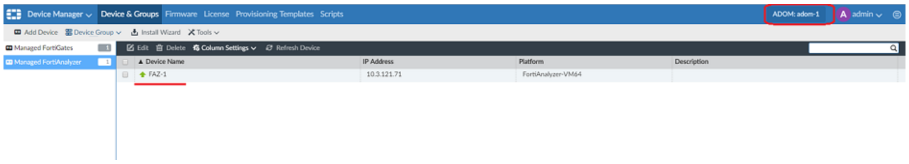
poluuid = 4dd3147a-03f7-51e5-3970-01012c630004

#	Date/Time	Device ID	Action	Source	Destination IP	Service	Sent/Received	User	Application	Security Event List
1	16:49:56	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
2	16:49:55	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
3	16:49:53	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
4	16:49:52	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
5	16:49:51	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
6	16:49:50	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
7	16:49:49	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
8	16:49:48	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
9	16:49:47	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
10	16:49:46	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
11	16:49:45	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
12	16:49:44	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
13	16:49:43	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
14	16:49:42	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
15	16:49:41	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
16	16:49:40	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
17	16:49:39	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
18	16:49:38	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
19	16:49:37	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
20	16:49:36	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
21	16:49:35	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	
22	16:49:34	FG100D3G1481...	Policy vio...	10.3.121.3	2.2.2.2	icmp/8/0	0.0 KB/0.0 KB		icmp/8/0	

Managing multiple FortiAnalyzer units

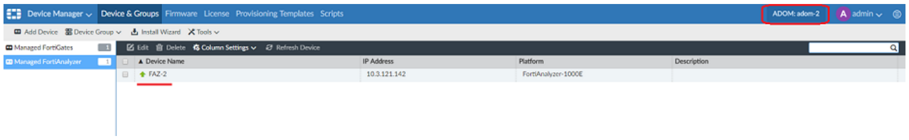
FortiManager can manage multiple FortiAnalyzer units, but each FortiAnalyzer must be in its own ADOM. You cannot add a second FortiAnalyzer unit to an ADOM.

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



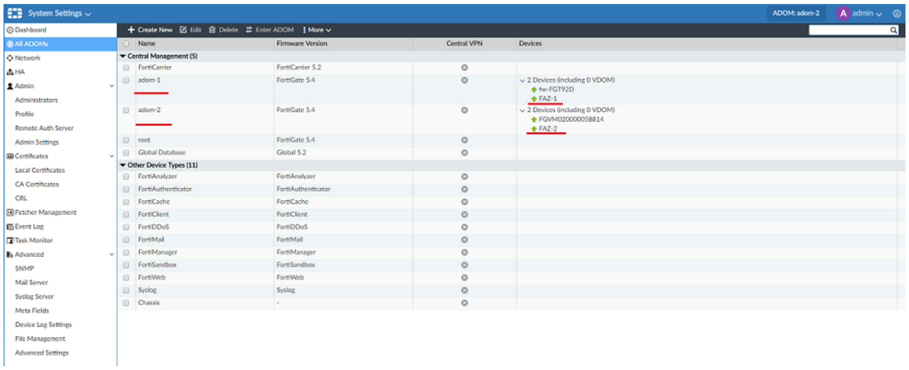
	Device Name	IP Address	Platform	Description
□	FAZ-1	10.3.121.71	FortiAnalyzer-VM64	

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



Device Name	IP Address	Platform	Description
FAZ-2	10.3.121.142	FortiAnalyzer-1000E	

Following is another view of the ADOMs with FortiAnalyzer units:



Name	Firmware Version	Central VPN	Devices
Central Management (5)			
FortiCarrier	FortiCarrier 5.2	⊗	
adom-1	FortiGate 5.4	⊗	2 Devices (including 0 VDOM) fw-FGT92D FAZ-1
adom-2	FortiGate 5.4	⊗	2 Devices (including 0 VDOM) FGVM020000058814 FAZ-2
root	FortiGate 5.4	⊗	
Global Database	Global 5.2	⊗	
Other Device Types (11)			
FortiAnalyzer	FortiAnalyzer	⊗	
FortiAuthenticator	FortiAuthenticator	⊗	
FortiCache	FortiCache	⊗	
FortiClient	FortiClient	⊗	
FortiDDoS	FortiDDoS	⊗	
FortiMail	FortiMail	⊗	
FortiManager	FortiManager	⊗	
FortiSandbox	FortiSandbox	⊗	
FortiWeb	FortiWeb	⊗	
Syslog	Syslog	⊗	
Chassis	-	⊗	

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`

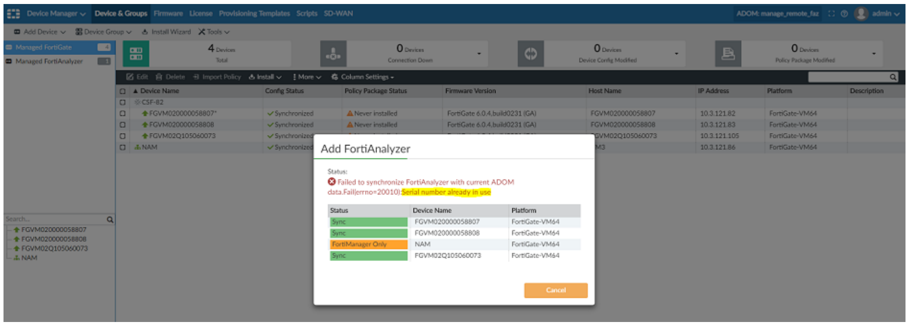
ADOM remains locked on FortiAnalyzer

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.



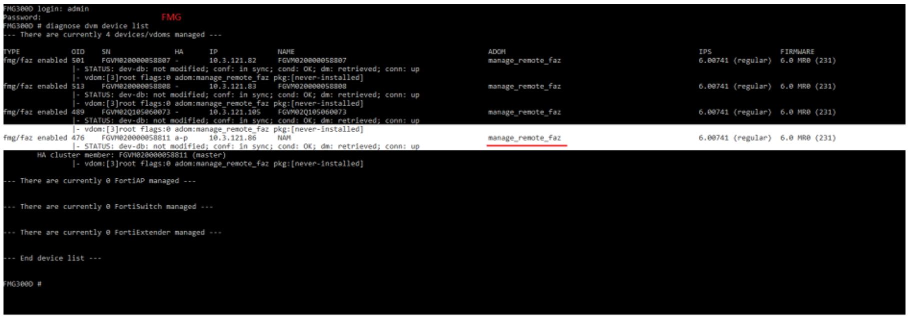
Add FortiAnalyzer

Status:

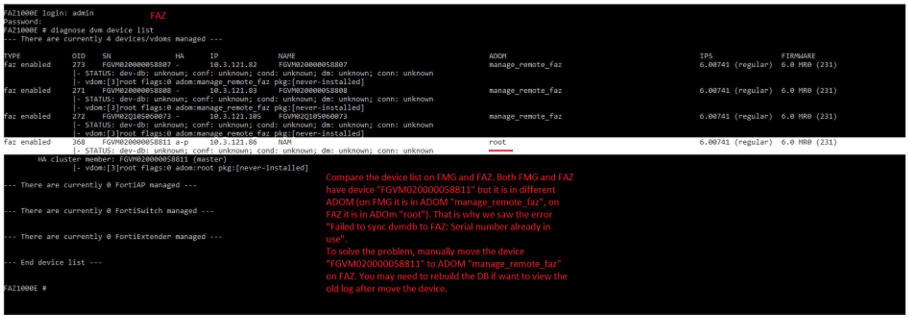
Failed to synchronize FortiAnalyzer with current ADOM data.Fail(errno=20010):Serial number already in use

Status	Device Name	Platform
Sync	FGVM020000058807	FortiGate-VM64
Sync	FGVM020000058808	FortiGate-VM64
FortiManager Only	NAM	FortiGate-VM64
Sync	FGVM02Q105060073	FortiGate-VM64

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.



```
FMG300D login: admin
Password:
FMG300D # diagnose dvm device list
--- There are currently 4 devices/vdoms managed ---

TYPE            OID    SN               HA      IP              NAME                                            ADOM                                                  IPS                 FIRMWARE
fmg/faz enabled 501    FGVM020000058807 -       10.3.121.82     FGVM020000058807                                manage_remote_faz                                     6.00741 (regular)  6.0 MR0 (231)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
                |- vdom:[3]root flags:0 adom:manage_remote_faz pkg:[never-installed]
fmg/faz enabled 513    FGVM020000058808 -       10.3.121.83     FGVM020000058808                                manage_remote_faz                                     6.00741 (regular)  6.0 MR0 (231)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
                |- vdom:[3]root flags:0 adom:manage_remote_faz pkg:[never-installed]
fmg/faz enabled 489    FGVM02Q105060073 -       10.3.121.105    FGVM02Q105060073                                manage_remote_faz                                     6.00741 (regular)  6.0 MR0 (231)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
                |- vdom:[3]root flags:0 adom:manage_remote_faz pkg:[never-installed]
fmg/faz enabled 476    FGVM020000058811 a-p     10.3.121.86     NAM                                             manage_remote_faz                                     6.00741 (regular)  6.0 MR0 (231)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
        HA cluster member: FGVM020000058811 (master)
                |- vdom:[3]root flags:0 adom:manage_remote_faz pkg:[never-installed]

--- There are currently 0 FortiAP managed ---


--- There are currently 0 FortiSwitch managed ---


--- There are currently 0 FortiExtender managed ---


--- End device list ---


FMG300D #
```



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

TYPE            OID    SN               HA      IP              NAME                                            ADOM                                                  IPS                 FIRMWARE
faz enabled     273    FGVM020000058807 -       10.3.121.82     FGVM020000058807                                manage_remote_faz                                     6.00741 (regular)  6.0 MR0 (231)
                |- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: unknown; conn: unknown
                |- vdom:[3]root flags:0 adom:manage_remote_faz pkg:[never-installed]
faz enabled     271    FGVM020000058808 -       10.3.121.83     FGVM020000058808                                manage_remote_faz                                     6.00741 (regular)  6.0 MR0 (231)
                |- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: unknown; conn: unknown
                |- vdom:[3]root flags:0 adom:manage_remote_faz pkg:[never-installed]
faz enabled     272    FGVM02Q105060073 -       10.3.121.105    FGVM02Q105060073                                manage_remote_faz                                     6.00741 (regular)  6.0 MR0 (231)
                |- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: unknown; conn: unknown
                |- vdom:[3]root flags:0 adom:manage_remote_faz pkg:[never-installed]
faz enabled     368    FGVM020000058811 a-p     10.3.121.86     NAM                                             root                                                  6.00741 (regular)  6.0 MR0 (231)
                |- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: unknown; conn: unknown
        HA cluster member: FGVM020000058811 (master)
                |- vdom:[3]root flags:0 adom:root pkg:[never-installed]

--- There are currently 0 FortiAP managed ---


--- There are currently 0 FortiSwitch managed ---


--- There are currently 0 FortiExtender managed ---


--- End device list ---


FAZ1000E #
```

Compare the device list on FMG and FAZ. Both FMG and FAZ have device "FGVM020000058811" 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 dvmdb to FAZ: Serial number already in use".
To solve the problem, manually move the device "FGVM020000058811" 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.

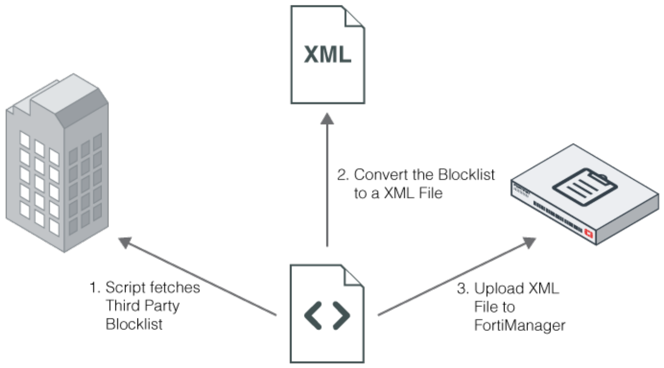
Creating a third party blocklist provider workflow

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.


XML
2. Convert the Blocklist to a XML File
1. Script fetches Third Party Blocklist
3. Upload XML File to FortiManager

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

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

   Example of the FortiManager XML file format:

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

   The category value in *<cate></cate>* could be either a normal web filter category or a local category.
2. Upload the XML file into FortiManager:
   The script uses SSH to connect to FortiManager and upload the XML file.

   CLI command:

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

     Example:
     #     execute fmupdate scp import custom-url 20M-custom-url.xml 000.000.000.000 00
          tmp/FORTIGUARD my_login my_password
     This operation will replace the current <custom-url> package!
     Do you want to continue? (y/n)y

     Start getting file from remote SCP Host...
     SCP transfer successful.
     Packing installation is in process...This could take some time.
     lccclient command result:Response=202|
   ```

```
  Update successfully
```

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

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

3. Configure FortiManager to only use its local FortiGuard database or local blocklist database:
   a. Select one of the following:
   - Local FortiGuard database
   - Local blocklist database
   - Or both

   ```
   config fmupdate custom-url-list
     set db_selection <fortiguard-db|custom-url|both>
     end
   ```
4. Test custom URLs managed by FortiManager:
   a. Use the CLI in FortiManager to send categorization requests for custom URLs managed by FortiManager.
   Example of the CLI command set:

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

   The *FGT SN* can be any FortiGate SN.

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

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

   The memory capacity of the unit determines the number of URLs FortiManager can manage.
5. Specify FortiManager as the FortiGuard server in FortiGate
   a. Go to your FortiGate CLI console and execute the following commands:

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

For further FortiManager information, refer to the FortiManager Administration Guides available on the Fortinet Document Library.

Copyright© 2022 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.