FortiManager - Cookbook

Version 5.4

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

June 3, 2019
FortiManager 5.4 Cookbook
02-540-560843-20190603

TABLE OF CONTENTS

Change Log

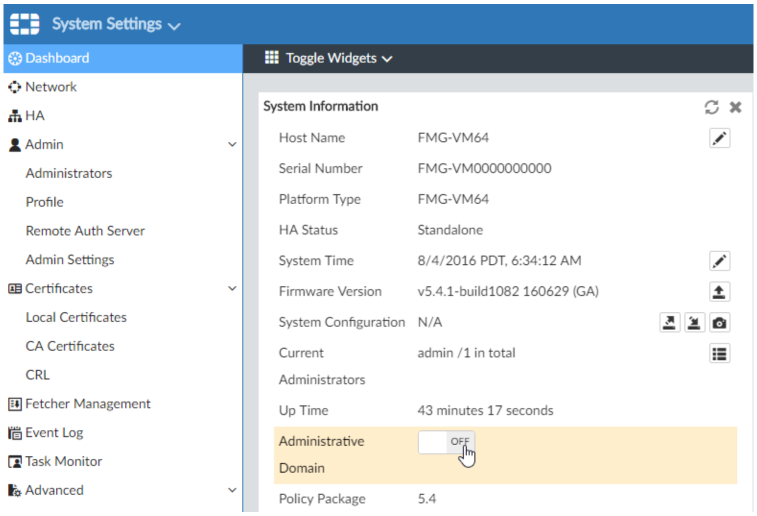
Date	Change Description
2019-06-03	Initial release.

Adding online FortiGates to FortiManager 5.4.1 ADOMs

This example illustrates how to enable administrative domains (ADOMs) in FortiManager, create an ADOM, and add an online FortiGate device to the ADOM.

To add an online FortiGate to FortiManager:

1. Enable ADOMs:
   a. Go to *System Settings > Dashboard*.
   b. In the System Information widget, go to *Administrative Domain*, and toggle *On*.

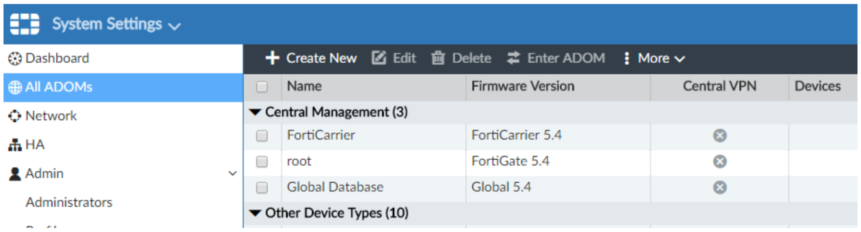


System Information

Host Name	FMG-VM64
Serial Number	FMG-VM0000000000
Platform Type	FMG-VM64
HA Status	Standalone
System Time	8/4/2016 PDT, 6:34:12 AM
Firmware Version	v5.4.1-build1082 160629 (GA)
System Configuration	N/A
Current Administrators	admin /1 in total
Up Time	43 minutes 17 seconds
Administrative Domain	OFF
Policy Package	5.4

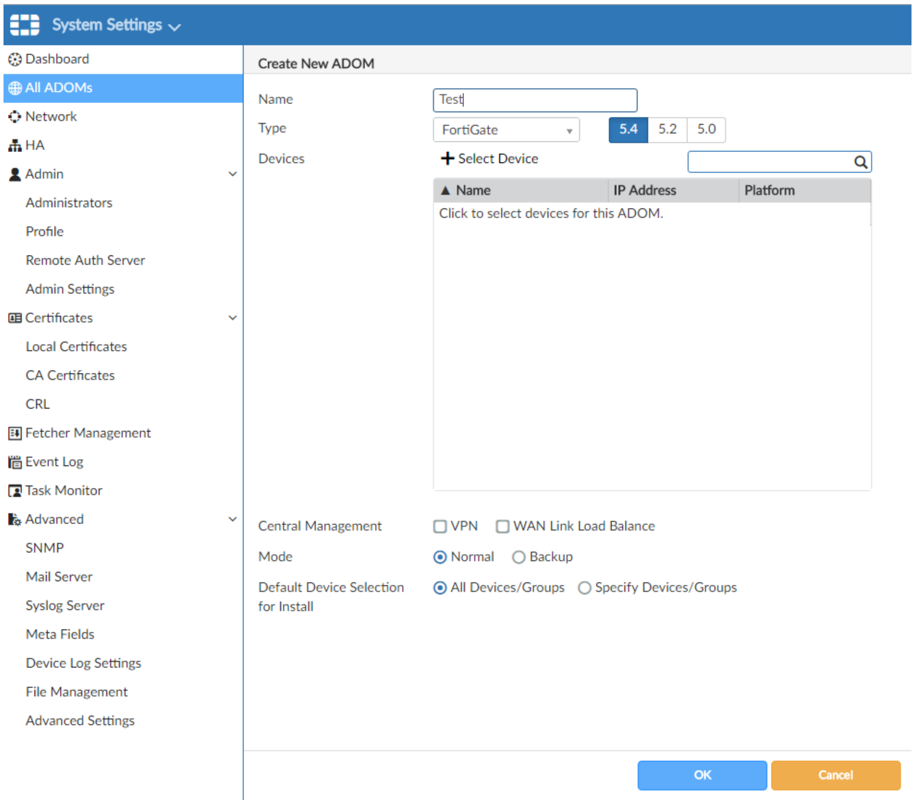
   c. Click *Yes* in the confirmation dialog box. FortiManager logs you out of the GUI.
   d. Log into the GUI, and select a default ADOM, such as *root*.

2. Create an ADOM:
   a. Go to *System Settings > All ADOMs*. Click *Create New*.



Name	Firmware Version	Central VPN	Devices
Central Management (3)			
FortiCarrier	FortiCarrier 5.4	⊗	
root	FortiGate 5.4	⊗	
Global Database	Global 5.4	⊗	
Other Device Types (10)			

b. Complete the options, and click *OK*.



Create New ADOM

Name: Test

Type: FortiGate [✓ 5.4] 5.2 5.0

Devices: + Select Device

▲ Name	IP Address	Platform
Click to select devices for this ADOM.		

Central Management: □ VPN □ WAN Link Load Balance

Mode: ● Normal ○ Backup

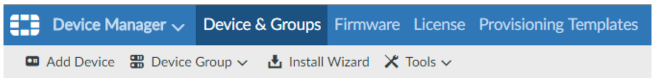
Default Device Selection for Install: ● All Devices/Groups ○ Specify Devices/Groups

The ADOM is created. In this example, the ADOM name is *Test*.

3. Add a FortiGate device to a FortiManager ADOM:

You are in the ADOM named *Test* that you just created, and the device will be added to the ADOM named *Test*. You can select a different ADOM by clicking *ADOM* in the top-right corner of the GUI.

a. Go to *Device Manager > Device & Groups* pane, and click *Add Device*.

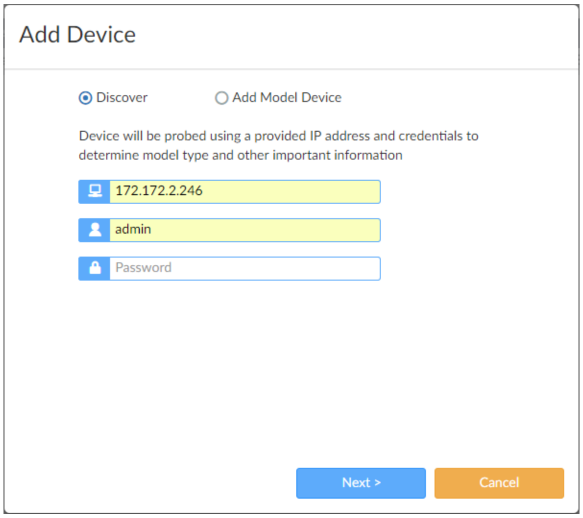


The Add Device wizard displays.

b. Select *Discover* to add an online FortiGate device.

c. In the *IP Address* box, type the IP address of the FortiGate.

d. In the *User Name* and *Password* boxes, type the username and password for the FortiGate, and click *Next*.



Add Device

● Discover ○ Add Model Device

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

172.172.2.246

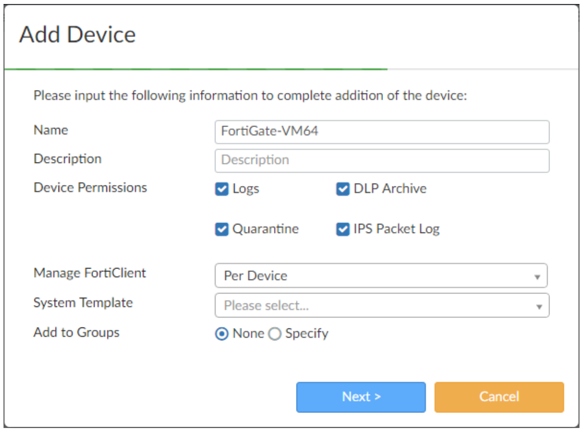
admin

Password

The wizard discovers the device and displays the configurable options.

e. Complete the options, and click *Next*.

The wizard adds the device.

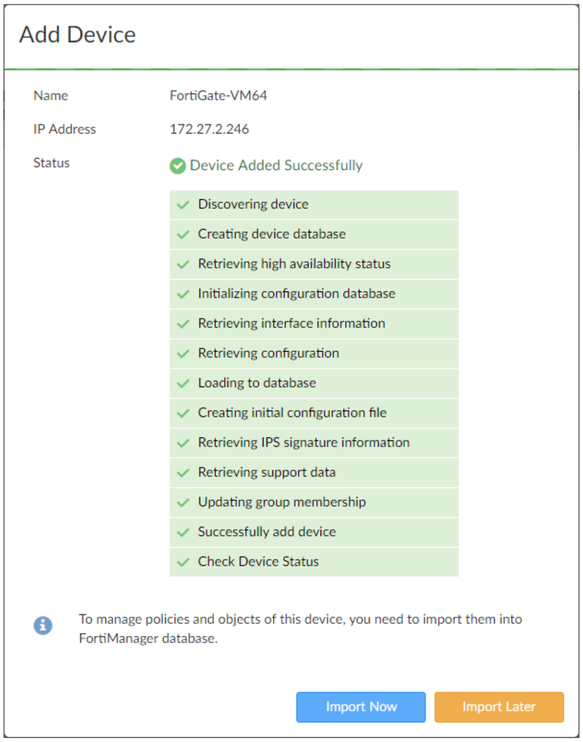


Add Device

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

Name	FortiGate-VM64
Description	Description
Device Permissions	☑ Logs ☑ DLP Archive ☑ Quarantine ☑ IPS Packet Log
Manage FortiClient	Per Device
System Template	Please select...
Add to Groups	● None ○ Specify

f. Click *Import Now* to import policies and objects from the FortiGate device.



Add Device

Name: FortiGate-VM64

IP Address: 172.27.2.246

Status: ✓ Device Added Successfully

- ✓ Discovering device
- ✓ Creating device database
- ✓ Retrieving high availability status
- ✓ Initializing configuration database
- ✓ Retrieving interface information
- ✓ Retrieving configuration
- ✓ Loading to database
- ✓ Creating initial configuration file
- ✓ Retrieving IPS signature information
- ✓ Retrieving support data
- ✓ Updating group membership
- ✓ Successfully add device
- ✓ Check Device Status

To manage policies and objects of this device, you need to import them into FortiManager database.

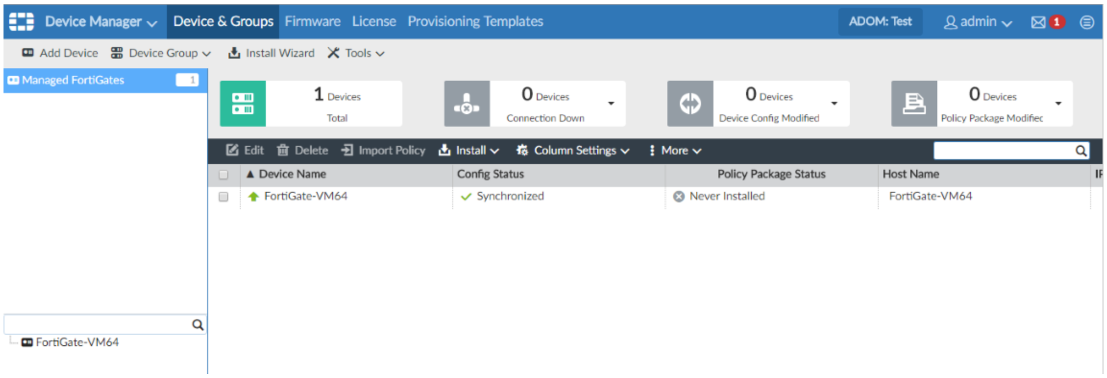
The wizard displays the list of policies and objects for the FortiGate device.

g. Click *Next* to import them.

h. Click *Finish* to close the Wizard.

The device is added to the FortiManager ADOM named Test.

4. On the *Device Manager > Device & Groups* pane, click *Managed FortiGates*.

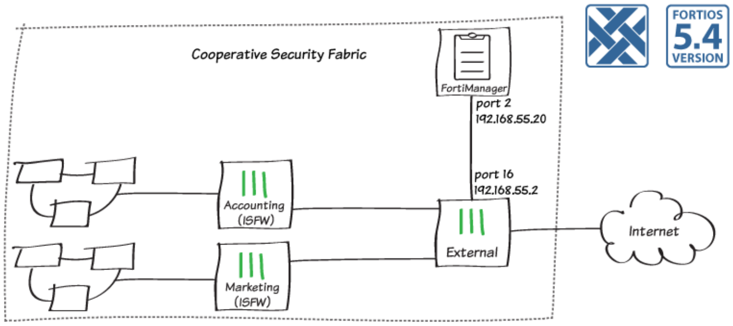


☐	▲ Device Name	Config Status	Policy Package Status	Host Name	IF
☐	FortiGate-VM64	✓ Synchronized	Never Installed	FortiGate-VM64	

The content pane displays the managed FortiGate devices.

Adding FortiManager to a Security Fabric

In this recipe, you will add a FortiManager to a network that is already configured as a Cooperative Security Fabric (CSF). This will simplify network administration because you can manage all of the FortiGates in the fabric from the FortiManager.

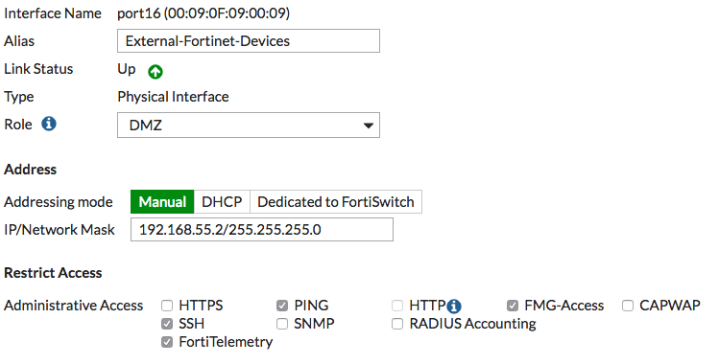


This recipe is part of the Cooperative Security Fabric collection. It can also be used as a standalone recipe.

In this example, the FortiManager is added to an existing security fabric. The FortiManager, as well as a FortiAnalyzer, both connect to the same port on the upstream FortiGate, called External, to provide services to the entire network.

To add a FortiManager to a security fabric:

1. Connect the External FortiGate and the FortiManager:
   In this example, the External FortiGate’s port 16 will connect to port 2 on the FortiManager.
   a. On the External FortiGate, go to *Network* > *Interfaces* and edit port 16. Set an *IP/Network Mask* for the interface (in the example, 192.168.55.2).
   b. Configure *Administrative Access* to allow *FMG-Access* and *FortiTelemetry*.



Interface Name port16 (00:09:0F:09:00:09)
Alias External-Fortinet-Devices
Link Status Up
Type Physical Interface
Role DMZ

Address

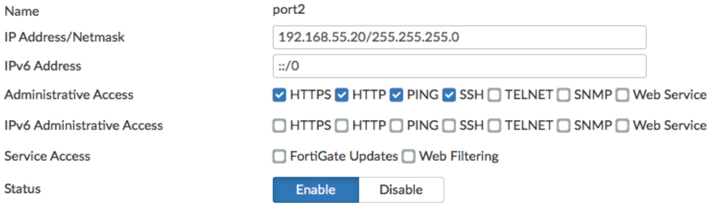
Addressing mode Manual | DHCP | Dedicated to FortiSwitch
IP/Network Mask 192.168.55.2/255.255.255.0

Restrict Access

Administrative Access □ HTTPS ☑ PING □ HTTP ☑ FMG-Access □ CAPWAP
☑ SSH □ SNMP □ RADIUS Accounting
☑ FortiTelemetry

   c. On the FortiManager, go to *System Settings* > *Network*, select *All Interfaces*, and edit *port2*.

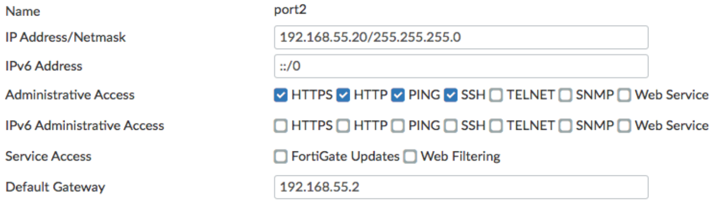
d. Set *IP Address/Netmask* to an internal IP (in the example, 192.168.55.20/255.255.255.0).



Name	port2
IP Address/Netmask	192.168.55.20/255.255.255.0
IPv6 Address	::/0
Administrative Access	☑ HTTPS ☑ HTTP ☑ PING ☑ SSH □ TELNET □ SNMP □ Web Service
IPv6 Administrative Access	□ HTTPS □ HTTP □ PING □ SSH □ TELNET □ SNMP □ Web Service
Service Access	□ FortiGate Updates □ Web Filtering
Status	Enable Disable

e. Connect the External FortiGate and the FortiManager.

f. On the FortiManager, go to *System Settings* > *Network*. Port 2 is now shown as the management interface. Add a *Default Gateway*, using the IP address of the External FortiGate's port 16.

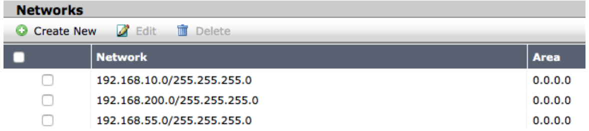


Name	port2
IP Address/Netmask	192.168.55.20/255.255.255.0
IPv6 Address	::/0
Administrative Access	☑ HTTPS ☑ HTTP ☑ PING ☑ SSH □ TELNET □ SNMP □ Web Service
IPv6 Administrative Access	□ HTTPS □ HTTP □ PING □ SSH □ TELNET □ SNMP □ Web Service
Service Access	□ FortiGate Updates □ Web Filtering
Default Gateway	192.168.55.2

If you previously configured a FortiAnalyzer using the recipe Adding a FortiAnalyzer to a security fabric, you may be able to skip the next two steps in this recipe, provided that the FortiAnalyzer and FortiManager both connect to the same port on the External FortiGate.

2. Configure OSPF routing to the FortiManager:

a. On the External FortiGate, go to *Network* > *OSPF* and create a new *Network*. Set *IP/Netmask* to 192.168.55.0/255.255.255.0 (the subnet that includes FortiManager's port 1) and *Area* to 0.0.0.0.

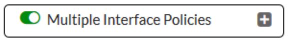


Networks

□	Network	Area
□	192.168.10.0/255.255.255.0	0.0.0.0
□	192.168.200.0/255.255.255.0	0.0.0.0
□	192.168.55.0/255.255.255.0	0.0.0.0

3. Allow internal FortiGates to access the FortiManager:

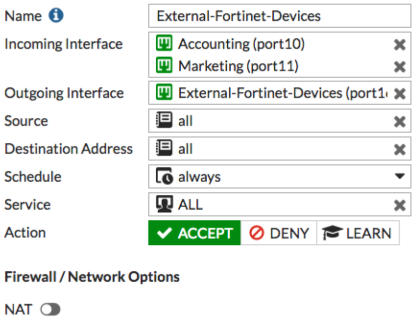
a. On the External FortiGate, go to *System* > *Feature Select*. Under *Additional Features*, select *Multiple Interface Policies*.



● Multiple Interface Policies

b. Go *to Policy & Objects* > *IPv4 Policy* and create a policy allowing the internal FortiGates (Accounting and Marketing) to access the FortiManager.

c. Do not enable *NAT*.



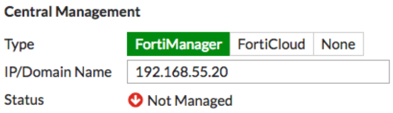
Name	External-Fortinet-Devices
Incoming Interface	Accounting (port10) Marketing (port11)
Outgoing Interface	External-Fortinet-Devices (port1
Source	all
Destination Address	all
Schedule	always
Service	ALL
Action	✓ ACCEPT ⊘ DENY LEARN

Firewall / Network Options

NAT ○

4. Configure central management:

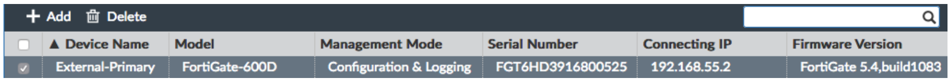
   a. On the External FortiGate, go to *System > Settings*. Under *Central Management*, select FortiManager and enter the *IP/Domain Name*.



Central Management

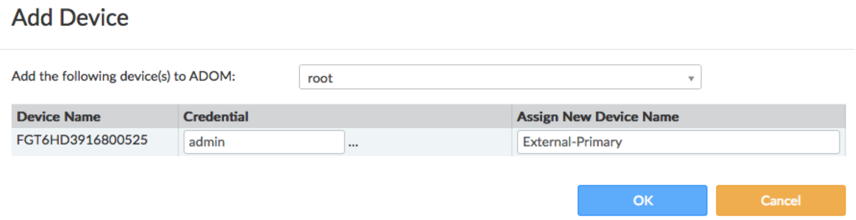
Type	FortiManager (selected) | FortiCloud | None
IP/Domain Name	192.168.55.20
Status	Not Managed

   b. On the FortiManager, go to *Device Manager > Unregistered Devices*. Select the External FortiGate, then select *+ Add*.



☐	▲ Device Name	Model	Management Mode	Serial Number	Connecting IP	Firmware Version
☑	External-Primary	FortiGate-600D	Configuration & Logging	FGT6HD3916800525	192.168.55.2	FortiGate 5.4,build1083

   c. Add the device to the root ADOM.

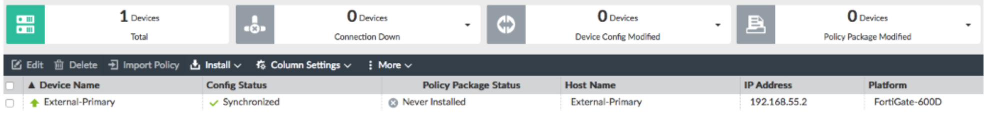


Add Device

Add the following device(s) to ADOM: root

Device Name	Credential	Assign New Device Name
FGT6HD3916800525	admin ...	External-Primary

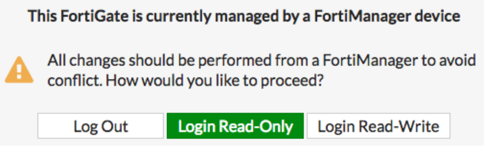
   d. The External FortiGate is now on the *Managed FortiGates* list.


1 Devices Total
0 Devices Connection Down
0 Devices Device Config Modified
0 Devices Policy Package Modified
Edit
Delete
Import Policy
Install
Column Settings
More

☐	▲ Device Name	Config Status	Policy Package Status	Host Name	IP Address	Platform
☐	External-Primary	✓ Synchronized	Never Installed	External-Primary	192.168.55.2	FortiGate-600D

   e. Connect to the External FortiGate. A warning message appears, stating that the FortiGate is now managed by a FortiManager.

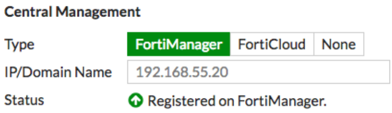
   f. Select *Login Read-Only*.



This FortiGate is currently managed by a FortiManager device

All changes should be performed from a FortiManager to avoid conflict. How would you like to proceed?

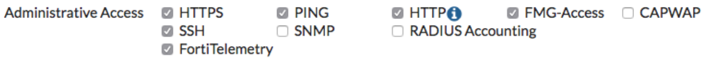
   g. Go to *System > Settings*. The *Central Management Status* is now *Registered on FortiManager*.



Central Management

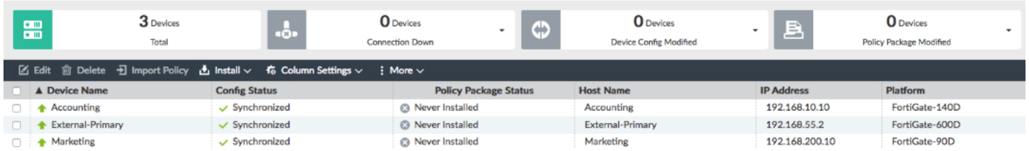
Type	FortiManager (selected) | FortiCloud | None
IP/Domain Name	192.168.55.20
Status	Registered on FortiManager.

   h. On the ISFW FortiGates, make sure that the interface connected to the External FortiGate allows *FMG-Access*. You can then repeat the above steps to configure central management for these FortiGates.



Administrative Access ☑ HTTPS ☑ PING ☑ HTTP ☑ FMG-Access ☐ CAPWAP ☑ SSH ☐ SNMP ☐ RADIUS Accounting ☑ FortiTelemetry

All three FortiGates are shown in the FortiManager's *Managed FortiGates* list.


3 Devices Total
0 Devices Connection Down
0 Devices Device Config Modified
0 Devices Policy Package Modified
Edit
Delete
Import Policy
Install
Column Settings
More

☐	▲ Device Name	Config Status	Policy Package Status	Host Name	IP Address	Platform
☐	Accounting	✓ Synchronized	Never Installed	Accounting	192.168.10.10	FortiGate-140D
☐	External-Primary	✓ Synchronized	Never Installed	External-Primary	192.168.55.2	FortiGate-600D
☐	Marketing	✓ Synchronized	Never Installed	Marketing	192.168.200.10	FortiGate-90D

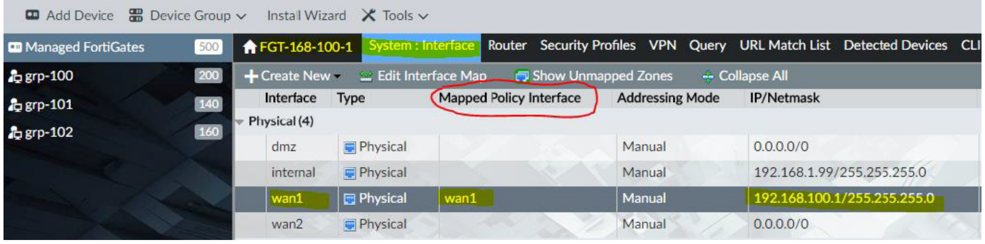
Configuring a full mesh VPN topology within a VPN console

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

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

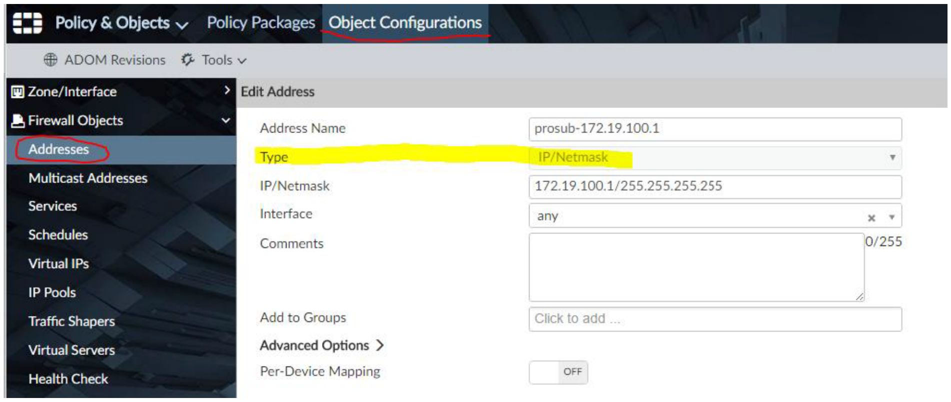
To configure a full mesh VPN topology within a VPN console:

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



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

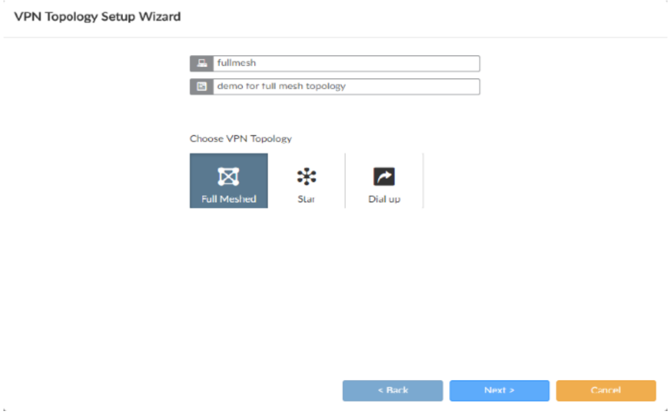
2. Create firewall addresses for protected subnets:
   a. Go to *Policy & Objects > Object Configurations > Firewall Objects > Address* to manage the firewall addresses.
   b. VPNs only support firewall addresses with the type set to *subnet (IP/Netmask)*. The firewall addresses will be used as protected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



Edit Address

Address Name	prosub-172.19.100.1
Type	IP/Netmask
IP/Netmask	172.19.100.1/255.255.255.255
Interface	any
Comments	0/255
Add to Groups	Click to add ...
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*.



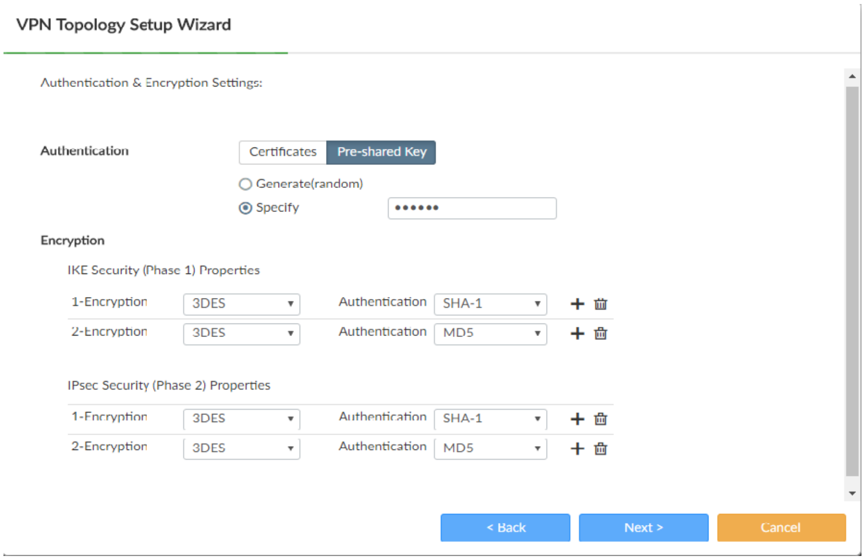
VPN Topology Setup Wizard

fullmesh

demo for full mesh topology

Choose VPN 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:

Authentication: Certificates | Pre-shared Key

○ Generate(random)

● Specify ••••••

Encryption

IKE Security (Phase 1) Properties

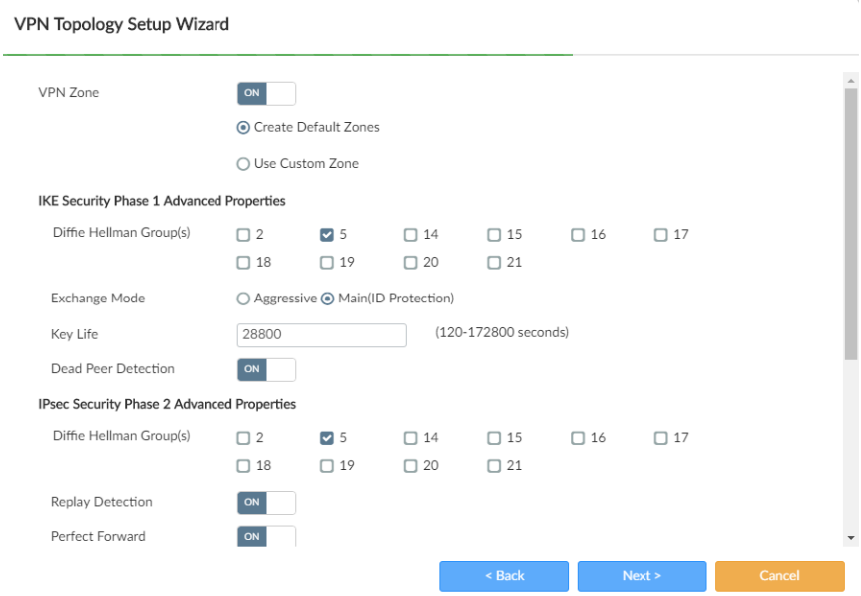
1-Encryption	3DES	Authentication	SHA-1
2-Encryption	3DES	Authentication	MD5

IPsec Security (Phase 2) Properties

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

   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

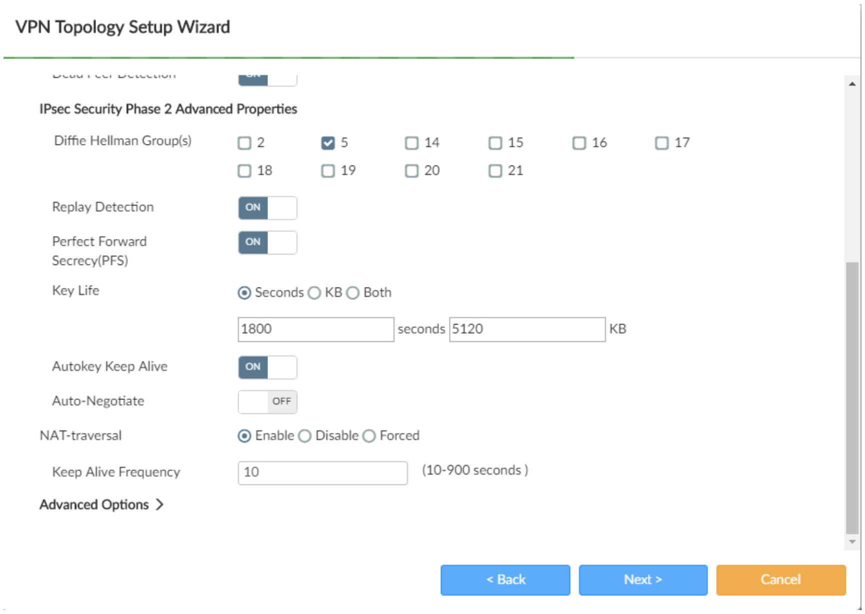
IPsec Security Phase 2 Advanced Properties

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

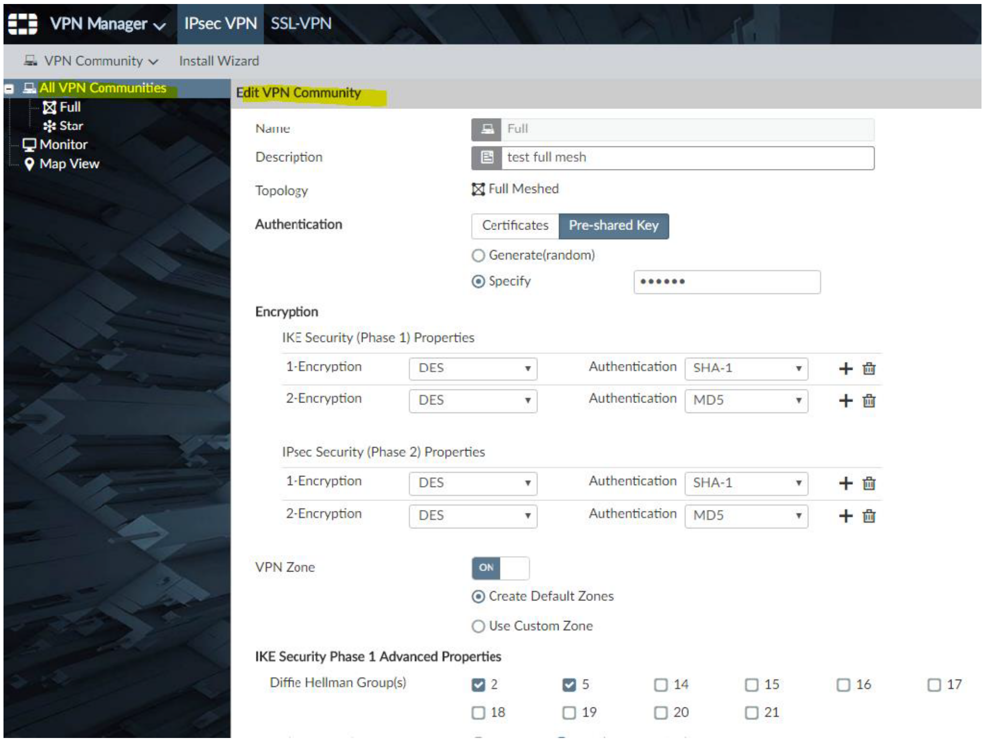
NAT-traversal: ● Enable ○ Disable ○ Forced

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:



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

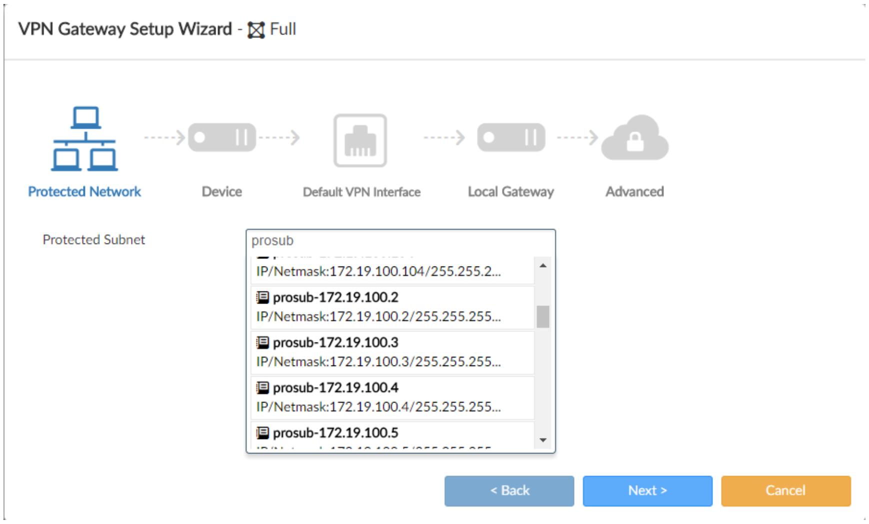
● Create Default Zones

○ 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.



Protected Subnet: prosub

IP/Netmask:172.19.100.104/255.255.2...

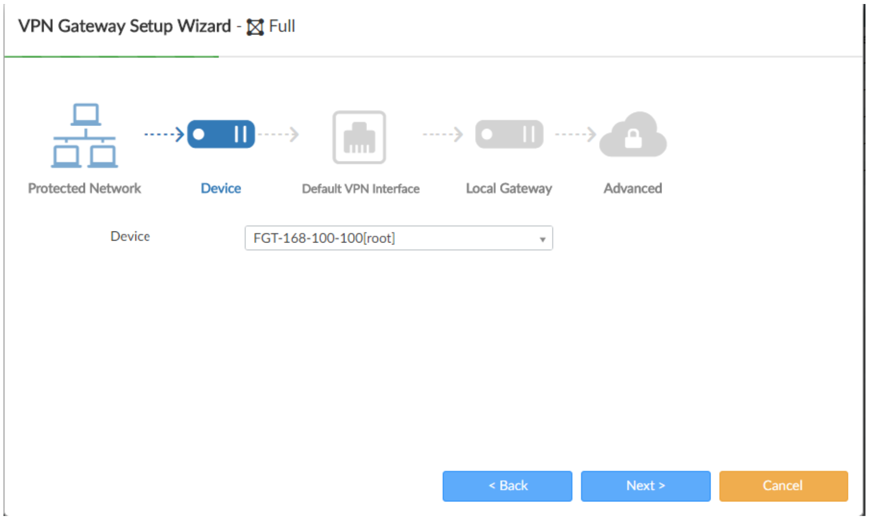
prosub-172.19.100.2
IP/Netmask:172.19.100.2/255.255.255...

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...

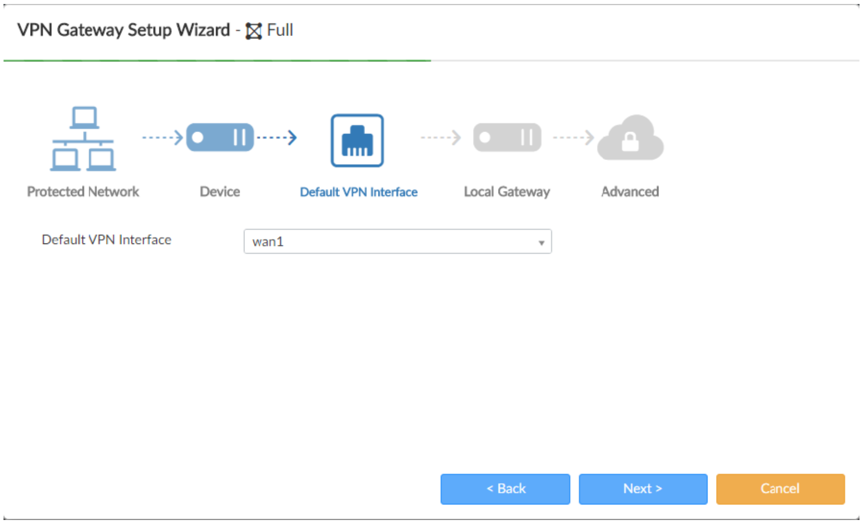
prosub-172.19.100.5

d. Select a *Device*.



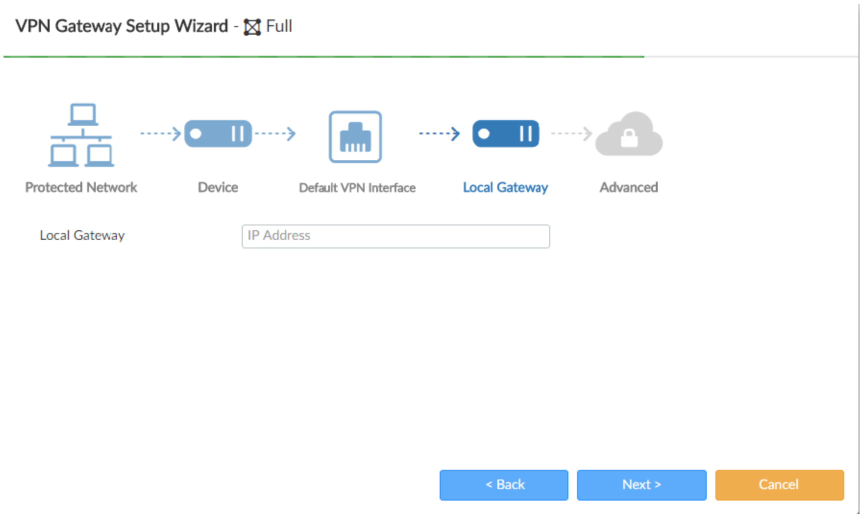
Device: FGT-168-100-100[root]

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



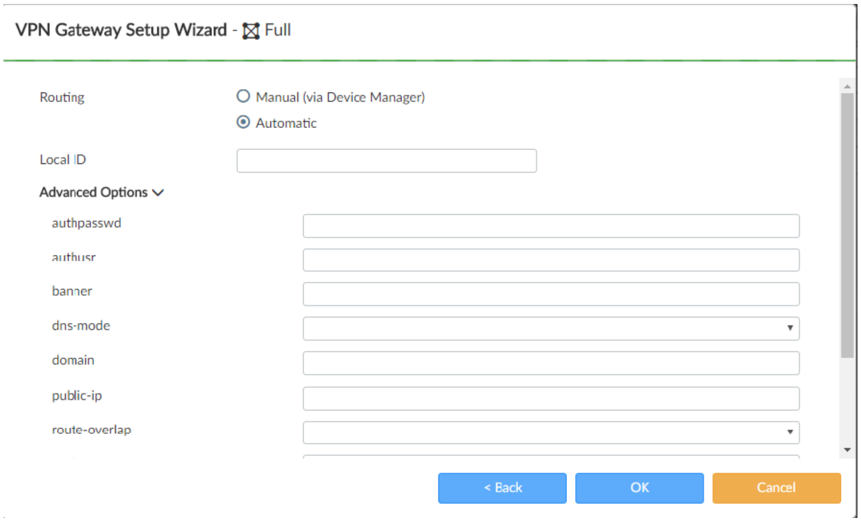
Default VPN Interface: wan1

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



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

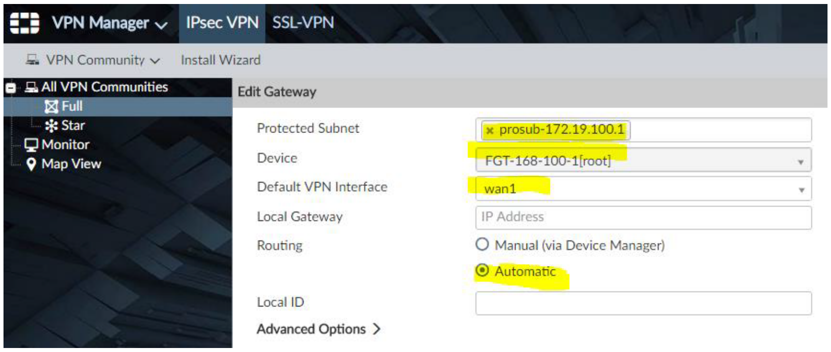
Local ID:

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:



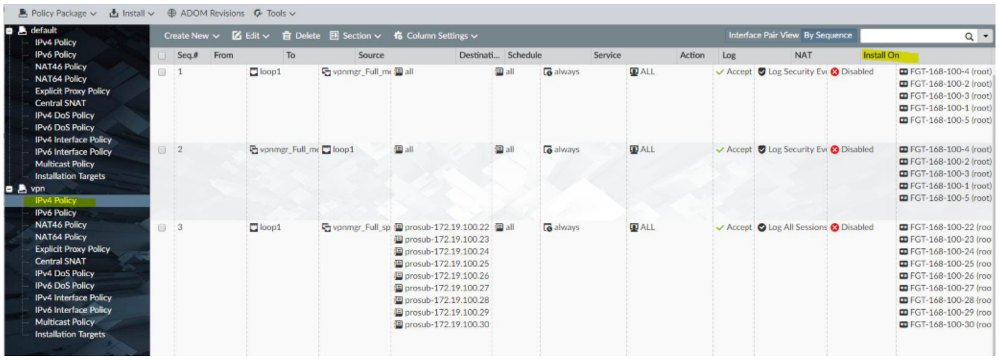
Edit Gateway

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_m	all	all	always	ALL	Accept	Log Security Ev	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_m	loop1	all	all	always	ALL	Accept	Log Security Ev	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 Administration Guides available in the Fortinet Document Library.

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

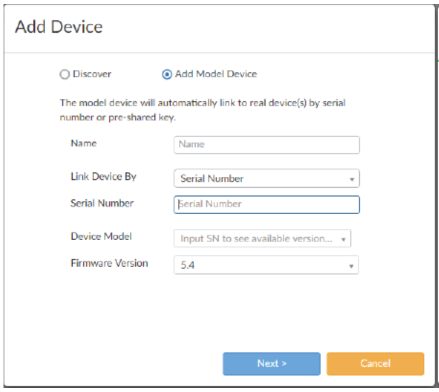
   Installation Target: Device1
2. Download the latest revision:
   a. Go to *Device Manager* > *Device & Groups* > and double-click the installation target device (Device1 in this example).
   b. Go to *System: Dashboard* > *Configuration and Installation Status* > *Total Revisions*.
   c. Download the 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.

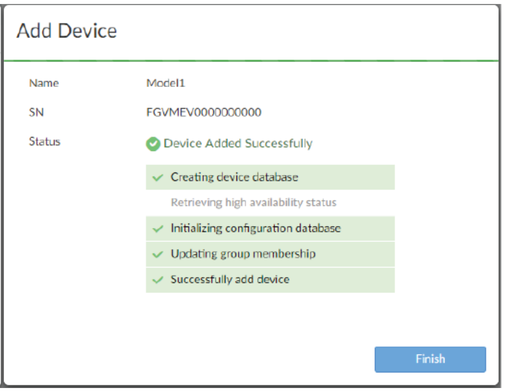


Add Device

○ 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 in the Fortinet Document Library.

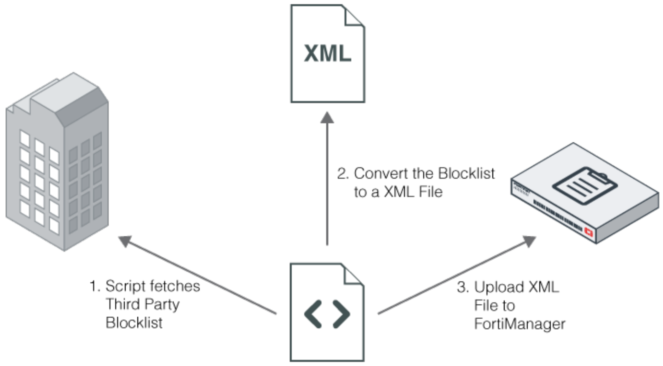
Creating a third party blocklist provider workflow

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 in the Fortinet Document Library.