



FortiManager - New Features Guide

Version 6.2.2

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



January 14, 2020

FortiManager 6.2.2 New Features Guide

02-622-528939-20200114

TABLE OF CONTENTS

Change Log	4
Fabric Connectors	5
VMware NSX-T connector	5
Enabling read-write JSON API access	5
Creating a fabric connector for VMware NSX-T	6
Downloading the FortiGate VM deployment image	9
Registering a service from FortiManager to VMware NSX-T	9
Deploying a FortiGate VM from VMware NSX-T	12
Creating and installing policy packages	12
SD-WAN	14
SD-WAN supports BGP neighbor configuration (central management mode)	14
Usability	17
API admin setup	17
FortiManager supports secured FortiGate update services	18
Directly use FSSO address group in firewall policies	19
Automatic multi-step firmware upgrade on FortiGate	21
Managed devices pull firmware from FortiGuard	23
FortiManager performs disk check on FortiGate before upgrading firmware	25
Support FQDN address objects in firewall policies	27
VPN Setup Wizard supports device groups	29
Creating device groups	30
Creating protected subnet firewall addresses	30
Creating VPN communities	32
Adding spoke FortiGate units to the VPN community	33
Adding the hub FortiGate unit to the VPN community	35
Installing firewall policies to hub and spoke devices	38
Removing a spoke member from a VPN community	39
Adding a spoke member to a VPN community	41
Other	43
Force admin password change	43
Acknowledgment of expired trial license	44

Change Log

Date	Change Description
2019-10-09	Initial release.
2019-10-16	Added SD-WAN supports BGP neighbor configuration (central management mode) on page 14.
2019-10-24	Added Support FQDN address objects in firewall policies on page 27.
2020-01-14	Added VPN Setup Wizard supports device groups on page 29.

Fabric Connectors

This section lists the new features added to FortiManager for Fabric Connectors.

List of new features:

- [VMware NSX-T connector on page 5](#)

VMware NSX-T connector

FortiManager supports VMware NSX-T connectors.

After configuration is complete, FortiManager can retrieve groups from VMware NSX-T manager and store them as dynamic firewall address objects, and a FortiGate that is deployed by the registered VMware NSX-T service can connect to FortiManager to receive dynamic objects for VMware NSX-T.

Following is an overview of the steps required to set up a VMware NSX-T connector:

1. [Enabling read-write JSON API access on page 5](#)
2. [Creating a fabric connector for VMware NSX-T on page 6](#)
3. [Downloading the FortiGate VM deployment image on page 9](#)
4. [Registering a service from FortiManager to VMware NSX-T on page 9](#)
5. [Deploying a FortiGate VM from VMware NSX-T on page 12](#)
6. [Creating and installing policy packages on page 12](#)

Enabling read-write JSON API access

A VMware NSX-T connector requires read-write access to the FortiManager JSON API.

The JSON API registers a service with VMware NSX-T manager and retrieves object updates from VMware NSX-T manager.

To enable read-write JSON API access:

1. On FortiManager, go to *System Settings > Administrators*.
2. Double-click an administrator account to open it for editing.

3. Beside *JSON API Access*, select *Read-Write*, and click *OK*.

System Settings ▾

- Dashboard
- All ADOMs
- Network
- HA
- Admin ▾
 - Administrators**
 - Profile
 - Remote Authentication Server
 - Admin Settings
 - SAML SSO
- Certificates ▾
 - Local Certificates
 - CA Certificates
 - CRL
 - Remote Certificates
- Event Log
- Task Monitor
- Advanced ▾
 - SNMP
 - Mail Server
 - Syslog Server
 - Meta Fields
 - Advanced Settings

Edit Administrator

User Name: admin

Avatar: + Change Photo - Remove Photo

Comments:

Admin Type: LOCAL

Admin Profile: Super_User

JSON API Access: Read-Write

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

Policy Package Access: All Packages | Specify

Trusted Hosts: OFF

Meta Fields >

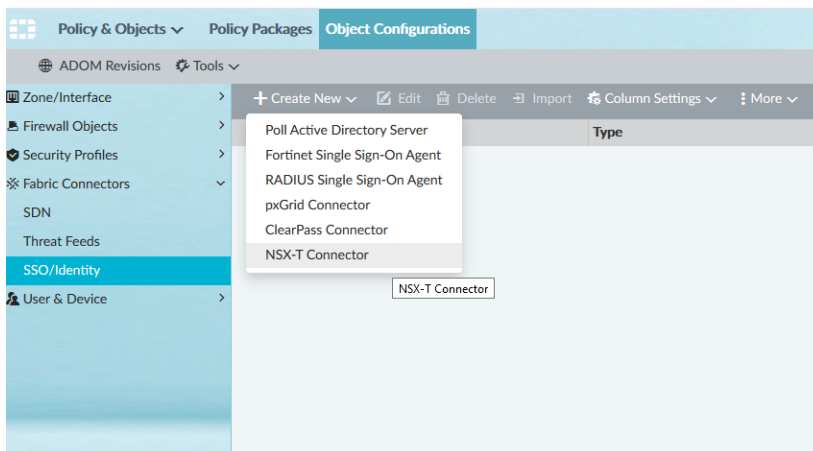
Advanced Options >

Creating a fabric connector for VMware NSX-T

In FortiManager, create a fabric connector for VMware NSX-T. You can configure a fabric connector for East-West or North-South traffic.

To create a fabric connector for VMware NSX-T:

1. On FortiManager, go to *Policy & Objects > Object Configurations > Fabric Connectors > SSO/Identity*.
2. Click *Create New* and select *NSX-T Connector*.



3. Complete the options, and click OK.

The screenshot shows the 'Object Configurations' tab in FortiManager. The left sidebar has 'SSO/Identity' selected. The main area is titled 'Create New NSX-T Connector'. It contains the following fields:

- Name: nsxt-2.4.2
- Status: OFF
- NSX-T Manager Configurations:
 - Server: 172.18.41.132
 - User Name: admin
 - Password: [masked]
- FortiManager Configurations:
 - IP Address: 172.18.37.142
 - User Name: qa
 - Password: [masked]

At the bottom right, there are three buttons: 'Apply & Refresh', 'OK', and 'Cancel'.

A fabric connector for VMware NSX-T is created and a connection to VMware NSX-T manager is established.

The screenshot shows the 'Object Configurations' tab with a table of NSX-T connectors. The table has columns for Name, Type, Details, Created Time, and Last Modified. The first row shows a connector named 'nsxt-2.4.2' of type 'NSX-T Connector' with details '172.18.41.132'.

Name	Type	Details	Created Time	Last Modified
nsxt-2.4.2	NSX-T Connector	172.18.41.132	2019-09-21 14:23:25	admin/2019-09-21 14:23:25

4. Double-click the VMware NSX-T connector to open it for editing.

5. Toggle *Status* to *On* and click *OK*.

Policy & Objects Policy Packages **Object Configurations**

ADOM Revisions Tools

Zone/Interface Firewall Objects Security Profiles Fabric Connectors SDN Threat Feeds SSO/Identity User & Device

Edit NSX-T Connector

Name nsxt-2.4.2

Status **ON**

NSX-T Manager Configurations

Server 172.18.41.132

User Name admin

Password

Registered Services (0)

+ Add Service

FortiManager Configurations

IP Address 172.18.37.142

User Name qa

Password

Connector Users Search...

No item.

Apply & Refresh OK Cancel

FortiManager retrieves the groups from VMware NSX-T manager and stores them as dynamic firewall address objects.

Policy & Objects Policy Packages **Object Configurations**

ADOM Revisions Tools

Zone/Interface Firewall Objects Security Profiles Fabric Connectors SDN Threat Feeds SSO/Identity User & Device

Edit NSX-T Connector

Name nsxt-2.4.2

Status **ON**

NSX-T Manager Configurations

Server 172.18.41.132

User Name admin

Password

Registered Services (0)

+ Add Service

FortiManager Configurations

IP Address 172.18.37.142

User Name qa

Password

Connector Users Search...

- nsx_nsxt-2.4.2_default/groups/group1 (6/6)
- nsx_nsxt-2.4.2_default/groups/group2 (8/8)
 - nsx (1.1.1.0)
 - nsx (1.1.1.0-4.4.0)
 - nsx (2.2.2.0)
 - nsx (3.3.3.0)
 - nsx (5.5.5.0)
 - nsx (6.6.6.0)
 - nsx (7.7.7.0)
 - nsx (8.8.8.0)
- nsx_nsxt-2.4.2_default/groups/group3 (8/8)

Apply & Refresh Disable Server Cancel

Downloading the FortiGate VM deployment image

You must download from the Fortinet Technical Support site a preconfigured deployment image for FortiGate VM and VMware NSX-T, and then place the image on a server that VMware NSX-T manager can access.

To download the FortiGate VM deployment image:

1. Go to the Fortinet Support site (<https://support.fortinet.com>), and download the following preconfigured FortiGate VM image to use for deployment:
`fortigate-vm64-nsxt.ovf`
2. Place the deployment image on a server that VMware NSX-T manager can access.
3. Identify the URL for the image. You will need to add the URL to FortiManager.

Registering a service from FortiManager to VMware NSX-T

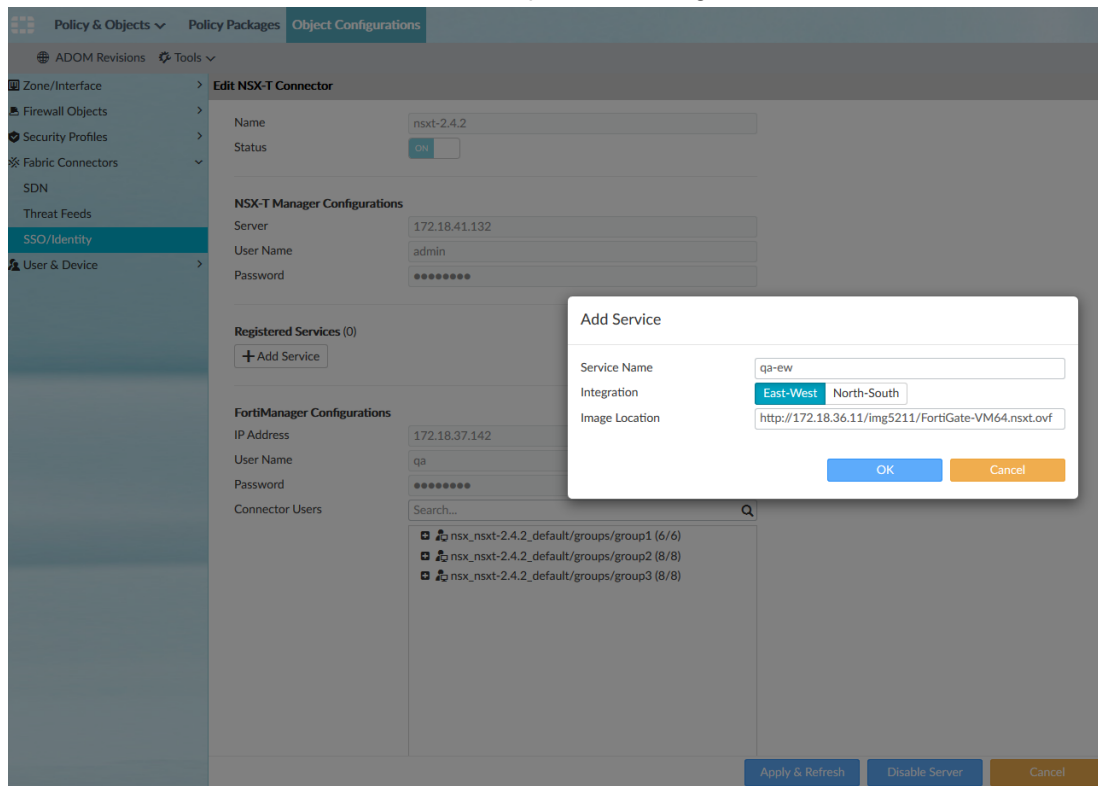
Before you can deploy a FortiGate VM from VMware NSX-T manager, you must register a service from FortiManager to the VMware NSX-T manager. The service includes the location of the preconfigured deployment image for the FortiGate VM.

The FortiManager JSON API registers the service with VMware NSX-T manager.

To register a service from FortiManager to VMware NSX-T:

1. Ensure that you know the URL for the location of the preconfigured deployment image for FortiGate VM and VMware NSX-T.
2. On FortiManager, go to *Policy & Objects > Object Configurations > Fabric Connectors > SSO/Identity*.

3. Double-click the VMware NSX-T connector to open it for editing, and click *Add Service*.



4. Complete the following options, and click *OK*:

- In the *Name* box, type a name for the service.
- Beside *Integration*, select *East-West* or *North-South* to identify the flow of traffic.
- In the *Image Location* box, type the URL of the location where the preconfigured FortiGate VM deployment image is located.

The service is added and registered with the VMware NSX-T manager.

Policy & Objects ▾ **Policy Packages** **Object Configurations**

ADOM Revisions Tools ▾

Zone/Interface ▾ **Firewall Objects** ▾ **Security Profiles** ▾ **Fabric Connectors** ▾

SDN
Threat Feeds
SSO/Identity
User & Device ▾

Edit NSX-T Connector

Name: nsxt-2.4.2
Status: ON

NSX-T Manager Configurations

Server: 172.18.41.132
User Name: admin
Password:

Registered Services (1)

Service Name: qa-ew [Delete Service](#)
Service ID: 47f318d9-2f6d-4ccc-918f-c6fc905b30b5
Implementations: EAST_WEST
[+ Add Service](#)

FortiManager Configurations

IP Address: 172.18.37.142
User Name: qa
Password:
Connector Users: Search...
nsx_nsxt-2.4.2_default/groups/group1 (6/6)
nsx_nsxt-2.4.2_default/groups/group2 (8/8)
nsx_nsxt-2.4.2_default/groups/group3 (8/8)

[Apply & Refresh](#) [Disable Server](#) [Cancel](#)

You can add multiple services.

Policy & Objects ▾ **Policy Packages** **Object Configurations**

ADOM Revisions Tools ▾

Zone/Interface ▾ **Firewall Objects** ▾ **Security Profiles** ▾ **Fabric Connectors** ▾

SDN
Threat Feeds
SSO/Identity
User & Device ▾

Edit NSX-T Connector

Name: nsxt-2.4.2
Status: ON

NSX-T Manager Configurations

Server: 172.18.41.132
User Name: admin
Password:

Registered Services (2)

Service Name: qa-ew [Delete Service](#)
Service ID: 47f318d9-2f6d-4ccc-918f-c6fc905b30b5
Implementations: EAST_WEST
Service Name: qa-ns [Delete Service](#)
Service ID: 49f3eb77-65d4-47ae-b4d2-4b7103c5714a
Implementations: EAST_WEST
[+ Add Service](#)

FortiManager Configurations

IP Address: 172.18.37.142
User Name: qa
Password:
Connector Users: Search...
nsx_nsxt-2.4.2_default/groups/group1 (6/6)
nsx_nsxt-2.4.2_default/groups/group2 (8/8)
nsx_nsxt-2.4.2_default/groups/group3 (8/8)

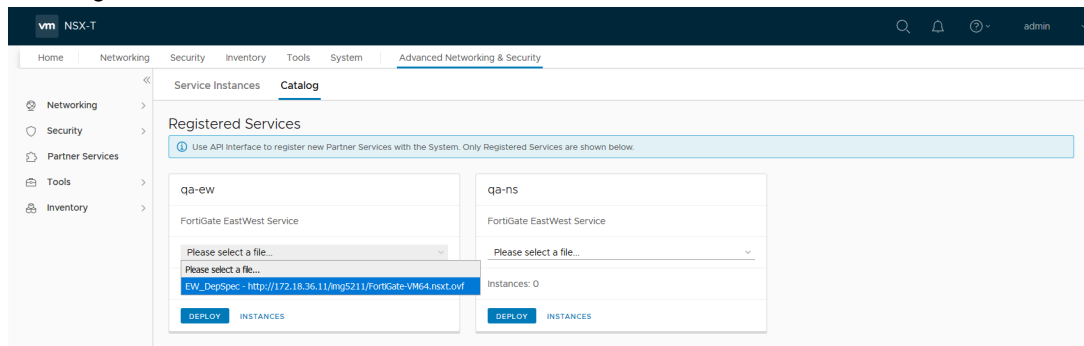
[Apply & Refresh](#) [Disable Server](#) [Cancel](#)

Deploying a FortiGate VM from VMware NSX-T

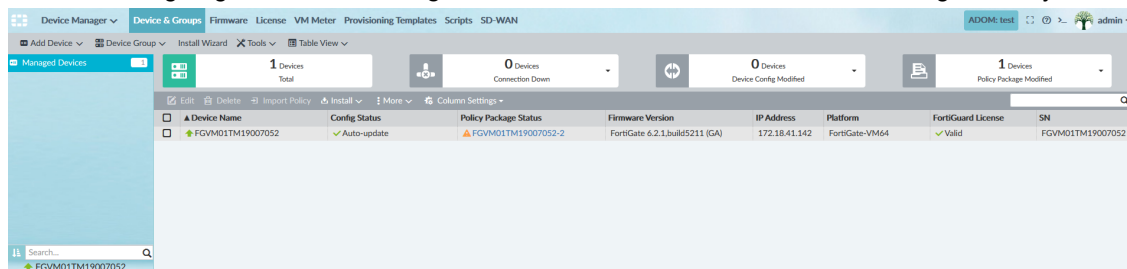
You must deploy the preconfigured FortiGate VM image from the VMware NSX-T manager, and then authorize FortiManager to centrally manage the FortiGate VM.

To deploy a FortiGate VM from VMware NSX-T:

1. On VMware NSX-T, ensure that the service is registered, and the *Deploy* option is available for FortiGate VMs via the image link.



2. On VMware NSX-T, deploy a FortiGate VM.
The FortiGate VM image is preconfigured to automatically enable central management by FortiManager.
3. When prompted by the deployment of FortiGate VM, enter the IP address of the FortiManager used for central management.
The FortiGate VM is deployed and displays in FortiManager on the *Device Manager* pane as an unauthorized device.
4. On FortiManager, go to *Device Manager*, and authorize the FortiGate VM for management by FortiManager.



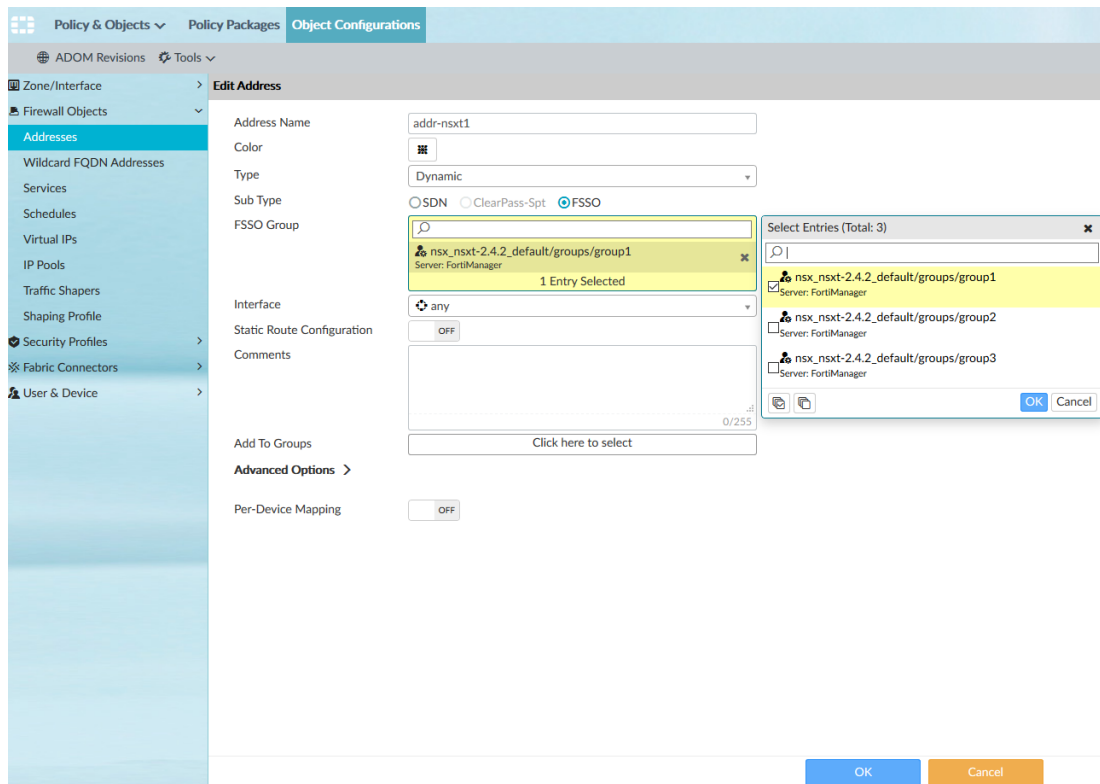
FortiManager can now manage FortiGate.

Creating and installing policy packages

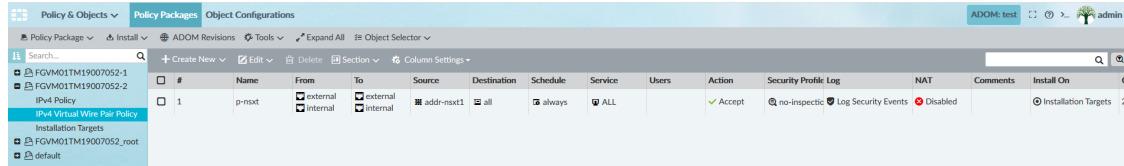
You must create an IPv4 virtual wire pair policy that contains the dynamic firewall address objects, and install the policy to FortiGate. Then FortiGate can use the dynamic address objects.

To create and install policy packages:

1. In FortiManager, go to *Policy & Objects > Object Configuration > Firewall Objects > Addresses*, and double-click an address to view the dynamic firewall address objects in the *FSSO Group*.



2. In the policy package in which you will be creating the new policy, create an IPv4 virtual wire pair policy and include the firewall address objects for VMware NSX-T.



3. Install the policy package to FortiGate.
FortiGate uses the information and FortiManager to communicate with VMware NSX-T to dynamically populate the firewall address objects with IP addresses.

SD-WAN

This section lists the new features added to FortiManager for SD-WAN.

List of new features:

- SD-WAN supports BGP neighbor configuration (central management mode) on page 14

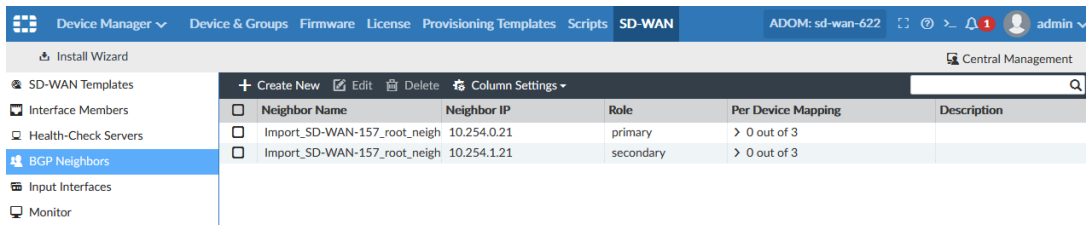
SD-WAN supports BGP neighbor configuration (central management mode)

SD-WAN supports BGP neighbor configuration in Central Management mode. You can also map input interfaces. You can use a default map or map to any interface in the database.

To view BGP neighbor options in central management mode:

1. Enable central management for SD-WAN.
 - a. Go to *System Settings > All ADOMs*.
 - b. Double-click the ADOM to open it for editing.
 - c. Beside *Central Management*, select *SD-WAN*, and click *OK*.
2. Go to *Device Manager > SD-WAN > BGP Neighbors*.

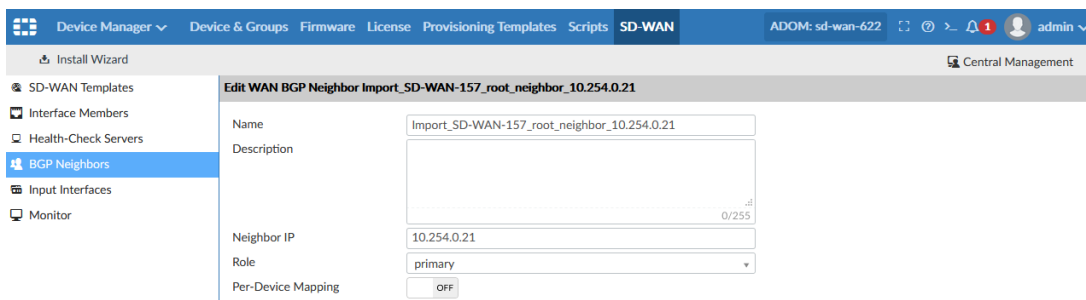
The list of BGP neighbors is displayed.



The screenshot shows the FortiManager interface in Central Management mode. The left sidebar has 'BGP Neighbors' selected. The main area displays a table of BGP neighbors.

Neighbor Name	Neighbor IP	Role	Per Device Mapping	Description
Import_SD-WAN-157_root_neigh	10.254.0.21	primary	> 0 out of 3	
Import_SD-WAN-157_root_neigh	10.254.1.21	secondary	> 0 out of 3	

You can double-click a BGP neighbor to open it for editing.

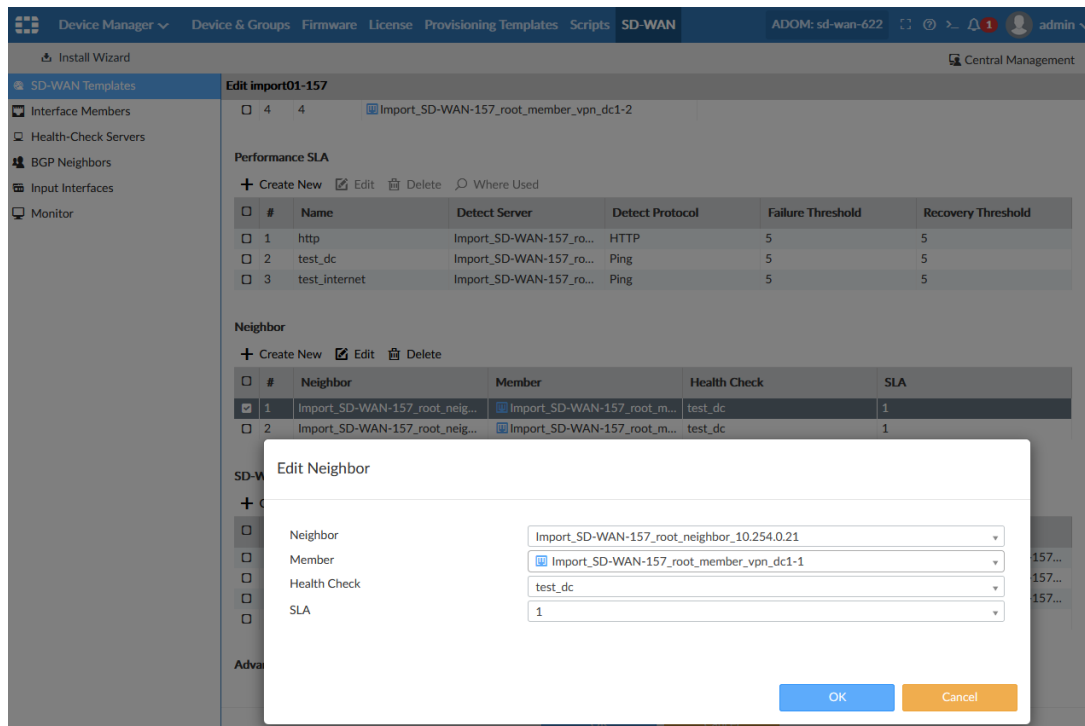


The screenshot shows the 'Edit WAN BGP Neighbor' form for the neighbor 'Import_SD-WAN-157_root_neigh_10.254.0.21'. The form fields are as follows:

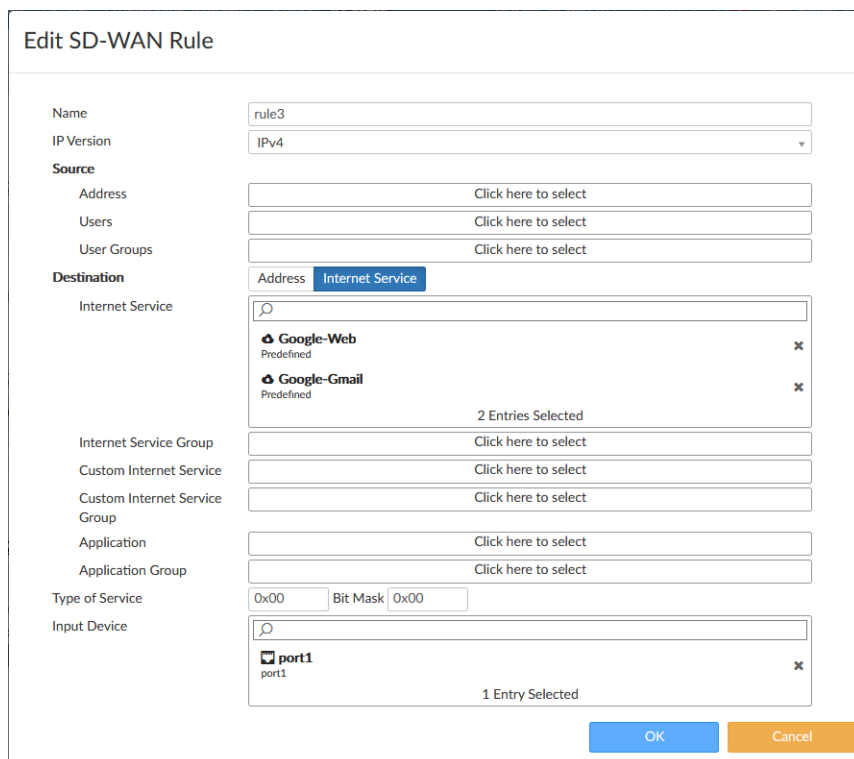
Name	Import_SD-WAN-157_root_neigh_10.254.0.21
Description	
Neighbor IP	10.254.0.21
Role	primary
Per-Device Mapping	off

3. Go to *Device Manager > SD-WAN > SD-WAN Templates*.

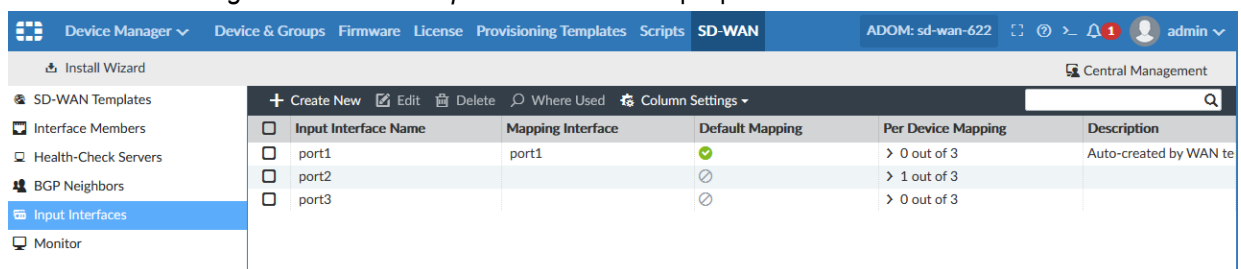
You can double-click a template to open it for editing.



In the SD-WAN Rules area, you can double-click a rule to open it for editing and edit input interfaces.



4. Go to *Device Manager > SD-WAN > Input Interfaces* to map input interfaces.



	Input Interface Name	Mapping Interface	Default Mapping	Per Device Mapping	Description
<input type="checkbox"/>	port1	port1	✓	> 0 out of 3	Auto-created by WAN te
<input type="checkbox"/>	port2		⊘	> 1 out of 3	
<input type="checkbox"/>	port3		⊘	> 0 out of 3	

Usability

This section lists the new features added to FortiManager for usability.

List of new features:

- [API admin setup on page 17](#)
- [FortiManager supports secured FortiGate update services on page 18](#)
- [Directly use FSSO address group in firewall policies on page 19](#)
- [Automatic multi-step firmware upgrade on FortiGate on page 21](#)
- [Managed devices pull firmware from FortiGuard on page 23](#)
- [FortiManager performs disk check on FortiGate before upgrading firmware on page 25](#)
- [Support FQDN address objects in firewall policies on page 27](#)
- [VPN Setup Wizard supports device groups on page 29](#)

API admin setup

JSON API access permission is now available from the main section of the Administrator's configuration page.

GUI changes for JSON API:

- JSON API Access which was under Advanced Options is moved to main configuration page of administrator.

The screenshot displays the FortiManager web interface for creating a new administrator. The left sidebar shows the navigation menu with 'System Settings' expanded and 'Administrators' selected. The main panel is titled 'New Administrator' and contains the following fields:

- User Name:** Test
- Avatar:** A placeholder icon with a red 'T' and buttons for '+ Change Photo' and '- Remove Photo'.
- Comments:** A text area with a character count of 0/127.
- Admin Type:** A dropdown menu set to 'LOCAL'.
- New Password:** A password field with a strength indicator.
- Confirm Password:** A password field with a strength indicator.
- Admin Profile:** A dropdown menu set to 'Restricted_User'.
- JSON API Access:** A dropdown menu set to 'Read-Write'.
- Administrative Domain:** A dropdown menu set to 'All ADOMs' with a 'Specify' button.
- Policy Package Access:** A dropdown menu set to 'All Packages' with a 'Specify' button.
- Trusted Hosts:** A toggle switch set to 'OFF'.
- Meta Fields:** A link to expand the meta fields section.
- Advanced Options:** A link to expand the advanced options section.

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

- In main page of administrator, JSON API Access column is added as well.

Name	Type	Profile	JSON API Access	ADOMs	Policy Package	Device Group	Comments	Trusted IPv4 Host	Trusted IPv6 Host
Test	LOCAL	Restricted_User	Read & Write	All ADOMs	All Packages			0.0.0.0/0.0.0.0 255.255.255.255/	0.0.0.0/0.0.0.0 255.255.255.255/
admin	LOCAL	Super_User	None	All ADOMs	All Packages			0.0.0.0/0.0.0.0 255.255.255.255/	0.0.0.0/0.0.0.0 255.255.255.255/

FortiManager supports secured FortiGate update services

FortiManager supports FortiOS generating HTTPS rating requests and AV/IPS updates on port 443 through the *Bind to IP Address* option.

Prerequisites of the Bind to IP Address feature:

- The FortiGate must be on the same subnet as the FortiManager interface IP.
- This feature is only for FortiGate 443 requests. Non-443 requests still use interface IP. For example, FortiGate still uses 8890 for update or TCP 8888/UDP for Web Filter query.
- Must configure with a different IP.

To enable secured FortiGate update services:

- Go to *System Settings > Network*.

System Network Management Interface

Name	port1
IP Address/Netmask	172.18.37.148/255.255.254.0
IPv6 Address	::/0
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input checked="" type="checkbox"/> Web Service
IPv6 Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> HTTP <input type="checkbox"/> PING <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> Web Service
Service Access	<input checked="" type="checkbox"/> FortiGate Updates
Bind to IP Address ⓘ	172.18.37.150/255.255.254.0
Web Filtering	<input checked="" type="checkbox"/> Web Filtering
Bind to IP Address ⓘ	172.18.37.149/255.255.254.0
Default Gateway	172.18.36.4
Primary DNS Server	208.91.112.52
Secondary DNS Server	208.91.112.53

- Select *FortiGate Updates* and specify the IP address in *Bind to IP Address*.
- Select *Web Filtering* and specify the IP address in *Bind to IP Address*
- Click *Apply*.

Directly use FSSO address group in firewall policies

Administrators can now directly use FSSO address group in firewall policies.

Case 1:

1. FortiManager has an FSSO Agent with 46 Active Directory groups.

Create New Fortinet Single Sign-On Agent

Name: fss1

Type: Active Directory / FortiAuthenticator

FSSO Agent

IP/Name: 10.3.113.103 Password: ***** Port: 8000

User Group Source: Collector Agent Via FortiGate Local

User Groups (46)

- FSSOTEST/ACCESS CONTROL ASSISTANCE OPERATORS
- FSSOTEST/ACCOUNT OPERATORS
- FSSOTEST/ADMINISTRATORS
- FSSOTEST/ALLOWED RODC PASSWORD REPLICATION GROUP
- FSSOTEST/BACKUP OPERATORS
- FSSOTEST/CERT PUBLISHERS
- FSSOTEST/CERTIFICATE SERVICE DCOM ACCESS
- FSSOTEST/CLONEABLE DOMAIN CONTROLLERS
- FSSOTEST/CRYPTOGRAPHIC OPERATORS
- FSSOTEST/DENIED RODC PASSWORD REPLICATION GROUP
- FSSOTEST/DISTRIBUTED COM USERS
- FSSOTEST/DNSADMIN
- FSSOTEST/DNSUPDATEPROXY
- FSSOTEST/DOMAIN ADMIN
- FSSOTEST/DOMAIN COMPUTERS
- FSSOTEST/DOMAIN CONTROLLERS
- FSSOTEST/DOMAIN GUESTS
- FSSOTEST/DOMAIN USERS
- FSSOTEST/ENTERPRISE ADMIN
- FSSOTEST/ENTERPRISE READ-ONLY DOMAIN CONTROLLERS
- FSSOTEST/EVENT LOG READERS
- FSSOTEST/GROUP POLICY CREATOR OWNERS
- FSSOTEST/GUESTS
- FSSOTEST/HYPER-V ADMINISTRATORS
- FSSOTEST/IIS_IUSRS
- FSSOTEST/INCOMING FOREST TRUST BUILDERS
- FSSOTEST/NETWORK CONFIGURATION OPERATORS

Buttons: Apply & Refresh, OK, Cancel

2. In the *Edit Policy* page, Active Directory groups can be directly used under FSSO groups, and there is no need to create an FSSO type user group.

Create New IPv4 Policy

Name:

Incoming Interface: any

Outgoing Interface: any

Source Internet Service: OFF

FSSO Groups: FSSOTEST/ACCESS CONTROL ASSISTANCE OPERATORS, FSSOTEST/ACCOUNT OPERATORS

Source Address: all

Source User: +

Source User Group: +

Destination Internet Service: OFF

Destination Address: all

Service: ALL

Schedule: always

Action: Deny, Accept, IPSEC

Log Traffic: No Log, Log Security Events, Log All Sessions

NAT: ☐

Security Profiles: ☐

Shared Shaper: ☐

Reverse Shaper: ☐

Per-IP Shaper: ☐

Comments:

Advanced Options >

Object Selector

Search...

FSSO GROUP (46)

- FSSOTEST/ACCESS CONTROL ASSISTANCE OPERATORS
- FSSOTEST/ACCOUNT OPERATORS
- FSSOTEST/ADMINISTRATORS
- FSSOTEST/ALLOWED RODC PASSWORD REPLICATION GROUP
- FSSOTEST/BACKUP OPERATORS
- FSSOTEST/CERT PUBLISHERS
- FSSOTEST/CERTIFICATE SERVICE DCOM ACCESS
- FSSOTEST/CLONEABLE DOMAIN CONTROLLERS
- FSSOTEST/CRYPTOGRAPHIC OPERATORS
- FSSOTEST/DENIED RODC PASSWORD REPLICATION GROUP
- FSSOTEST/DISTRIBUTED COM USERS
- FSSOTEST/DNSADMIN
- FSSOTEST/DNSUPDATEPROXY
- FSSOTEST/DOMAIN ADMIN
- FSSOTEST/DOMAIN COMPUTERS
- FSSOTEST/DOMAIN CONTROLLERS
- FSSOTEST/DOMAIN GUESTS

Total: 46

Case 2:**1. FortiManager has an LDAP server named *ldap1*.**

The screenshot shows the 'Edit LDAP' configuration page in FortiManager. The left sidebar has 'LDAP Servers' selected. The main configuration area includes the following fields:

- Name: ldap1
- Server Name/IP: 10.2.78.8
- Server Port: 389
- Common Name Identifier: cn
- Distinguished Name: dc=fssotest,dc=com
- Bind Type: Regular
- User DN: cn=administrator,cn=users,dc=fssotest,dc=com
- Password: (masked with asterisks)
- Secure Connection: None
- Advanced Options: Per-Device Mapping is OFF.

2. Under FSSO Agent, configure the following:

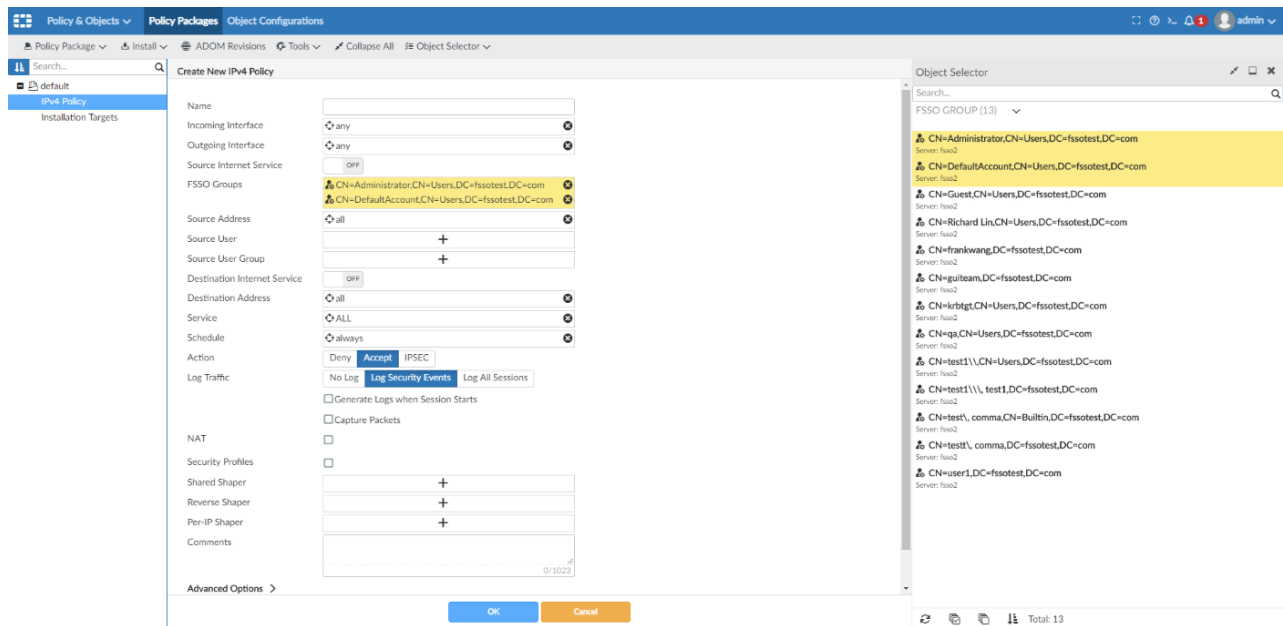
- User Group source: *Local*
- LDAP Server : *ldap1*

3. Specify the search filter as (*objectCategory=group*).

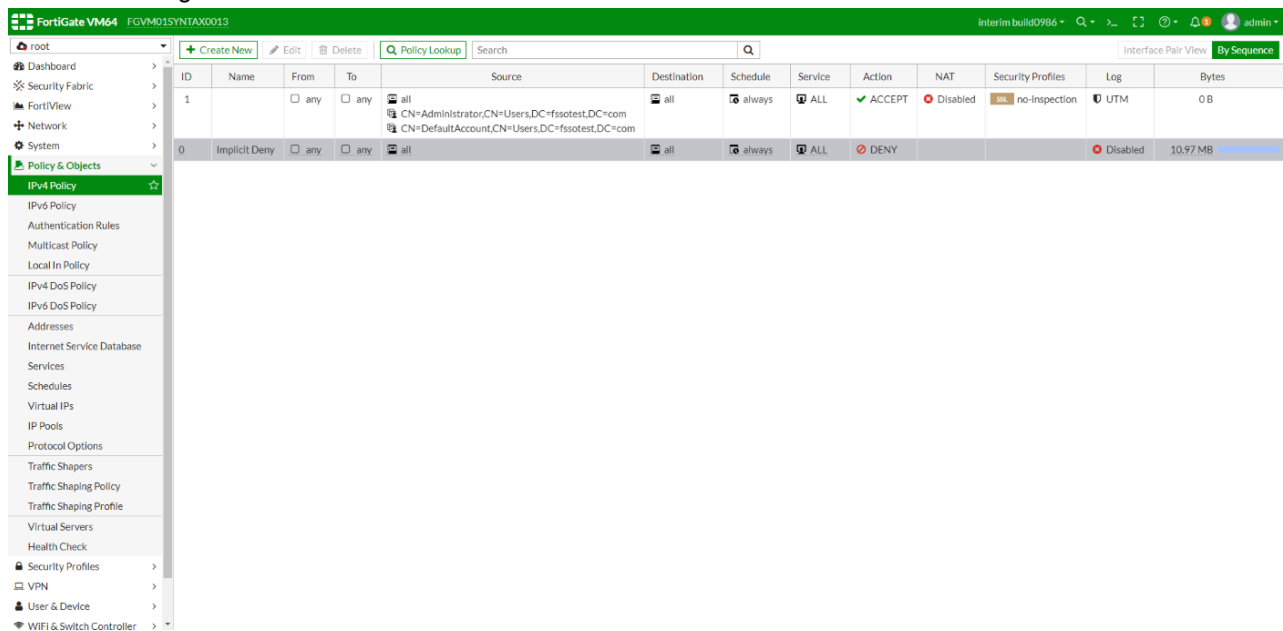
The screenshot shows the 'Create New Fortinet Single Sign-On Agent' configuration page in FortiManager. The left sidebar has 'SSO/Identity' selected. The main configuration area includes the following fields:

- Name: fss2
- Type: Active Directory / FortiAuthenticator
- FSSO Agent: IP/Name (10.2.78.8), Password (masked), Port (8000)
- User Group Source: Collector Agent | Via FortiGate | **Local**
- LDAP Server: ldap1
- Proactively Retrieve from LDAP Server: (checkbox)
- Search Filter: (objectCategory=group)
- Interval (minutes): 180
- SSL: OFF
- Per-Device Mapping: OFF
- Advanced Options: (expandable)

4. In the policy create/edit page, you can view all the user groups from the LDAP server as Active Directory Group for FSSO Groups.



5. Install the changes to FortiGate.



Automatic multi-step firmware upgrade on FortiGate

When using FortiManager to upgrade firmware on FortiGate, FortiManager can choose the shortest upgrade path based on the FortiGate upgrade matrix.

You can use the CLI to view and check the shortest upgrade path for a managed device by using the `diagnose fwmanager` command:

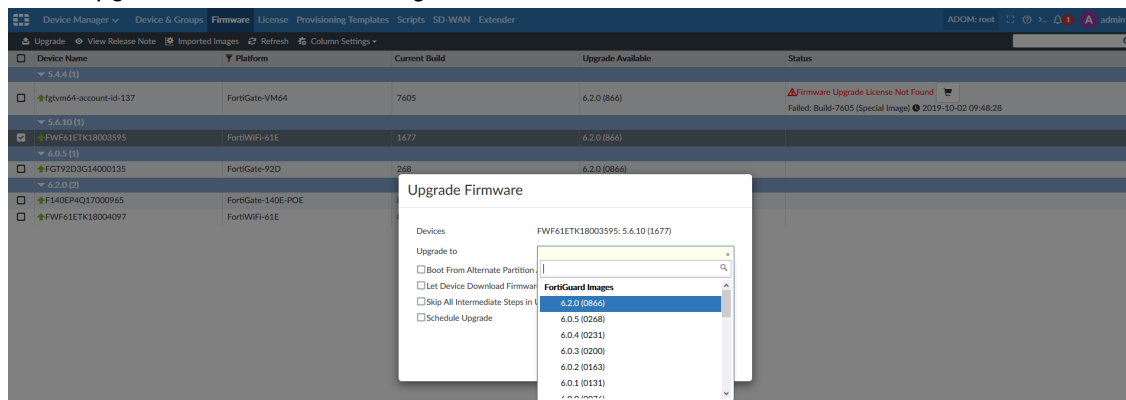
```
# diagnose fwmanager show-dev-upgrade-path 318 6.2.0
```

device FWF61ETK18003595(318), platform FWF61E, upgrade path from 5.6.10-1677 to 6.2.0-866 is:
[6.0.0-76 --> 6.0.2-163 --> 6.0.3-200 --> 6.2.0-866]

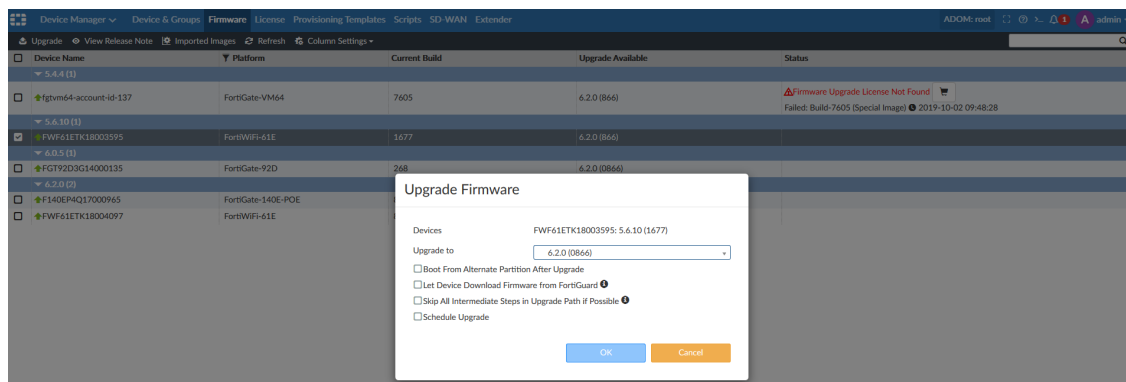
In this example, the device ID is 318, and you want to upgrade the device to FortiOS 6.2.0. The device is currently running FortiOS 5.6.10 build 1677, and the shortest upgrade path to FortiOS 6.2.0 is displayed.

To upgrade using the GUI:

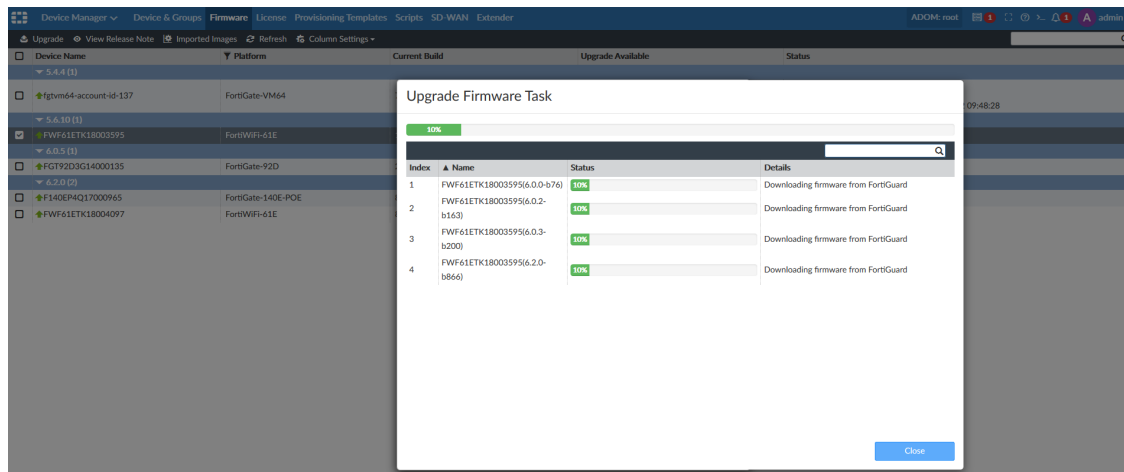
1. Go to *Device Manager > Firmware*.
2. Select a device, and click *Upgrade*.
The *Upgrade Firmware* dialog box is displayed.
3. In the *Upgrade to* box, select an image.



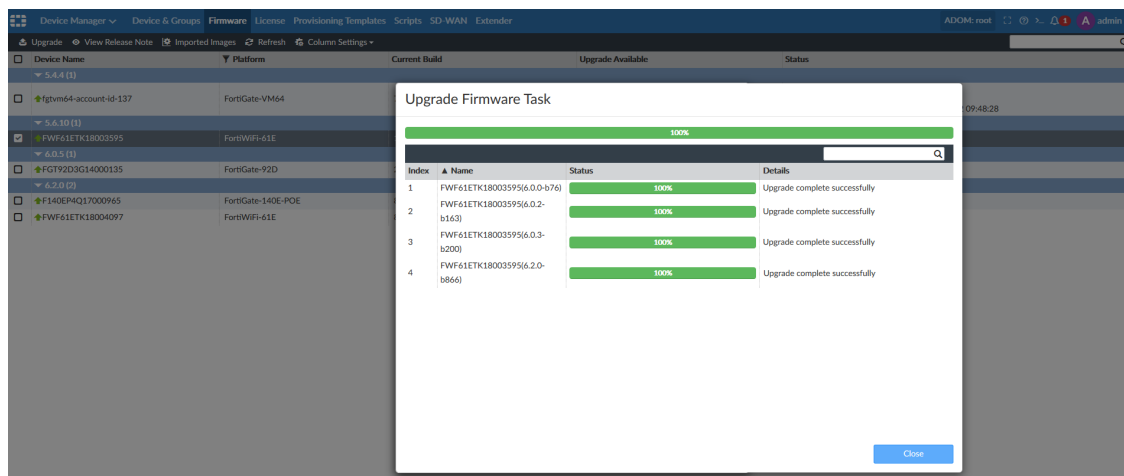
In this example, the FortiGate is running FortiOS 5.6.10, and we are going to upgrade to 6.2.0 (0866).



4. Click *OK*.
FortiManager starts the upgrade. Each upgrade is a subtask.



When all the subtasks reach a status of 100%, the upgrade completes.



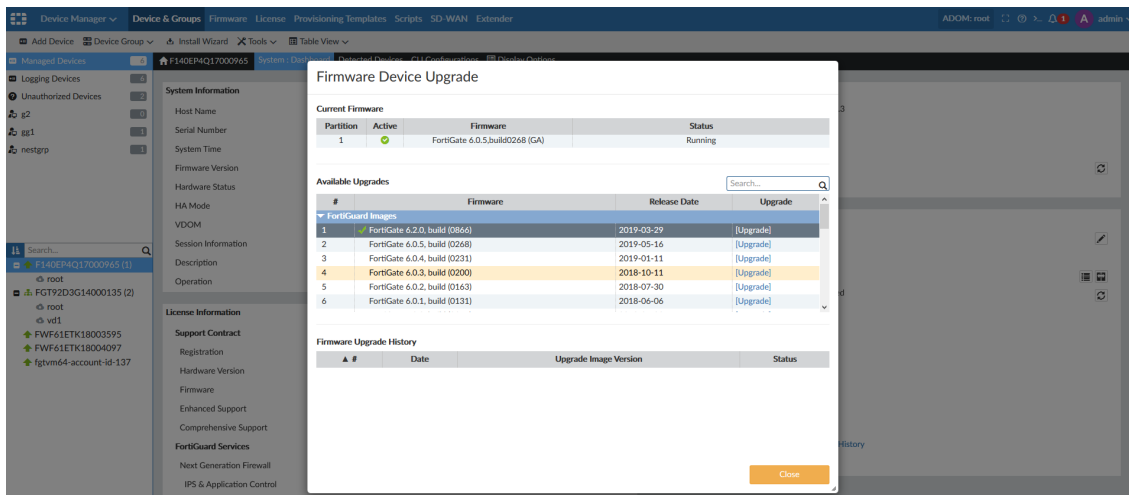
5. When the upgrade completes, click *Close*.

Managed devices pull firmware from FortiGuard

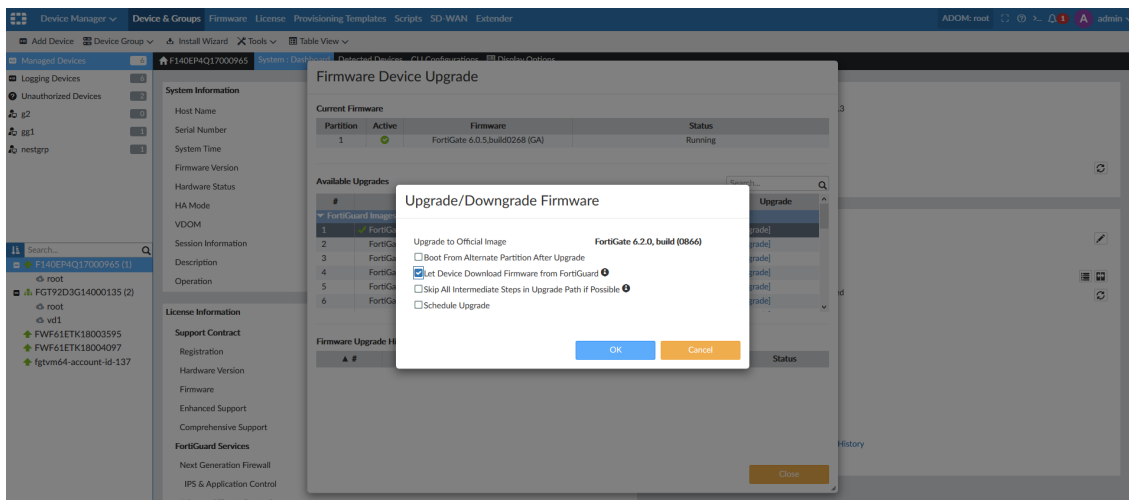
FortiManager retrieves firmware for managed devices from FortiGuard, and you can choose to use the images to upgrade firmware on managed devices.

To upgrade firmware using images retrieved from FortiGuard:

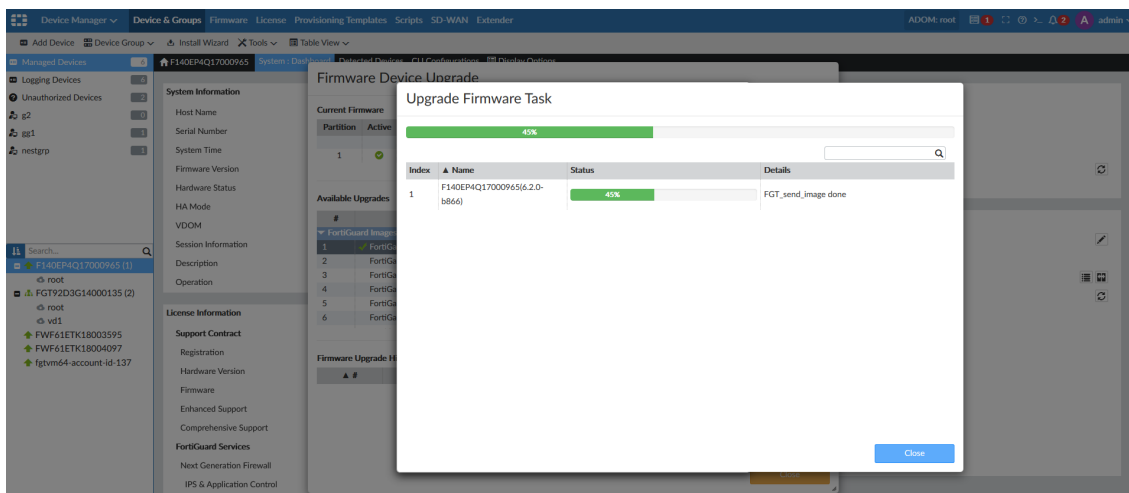
1. Go to *Device Manager > Device & Groups*, and select a device.
2. In the *System Information* widget, click the *Update* icon beside *Firmware Version*.
The *Firmware Device Upgrade* dialog box displays a list of images retrieved from FortiGuard.



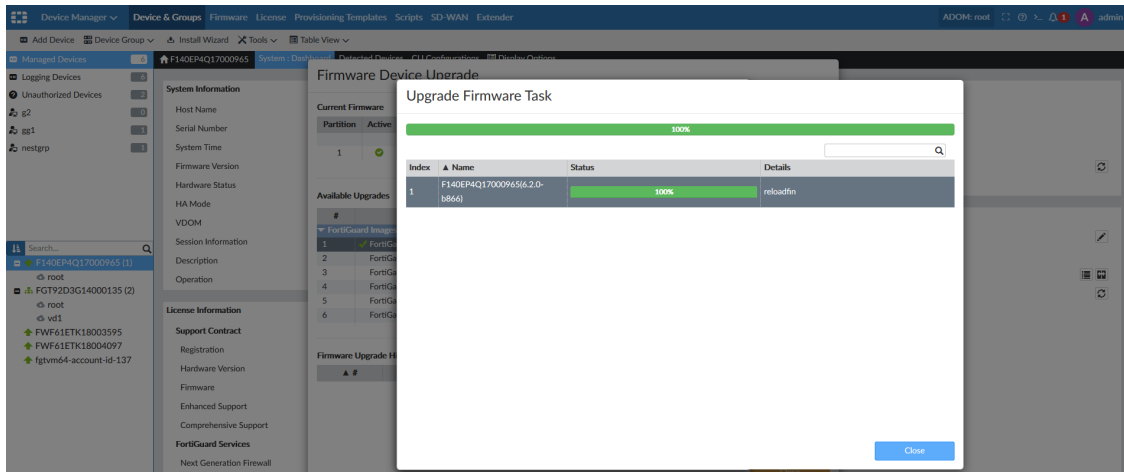
- Click **Upgrade** for the desired FortiGuard image.
The **Upgrade/Downgrade Firmware** dialog box is displayed.



- Select the **Let Device Download Firmware from FortiGuard** check box, and click **OK**.
The firmware downloaded from FortiGuard is used, and the upgrade starts.



The firmware upgrade completes.



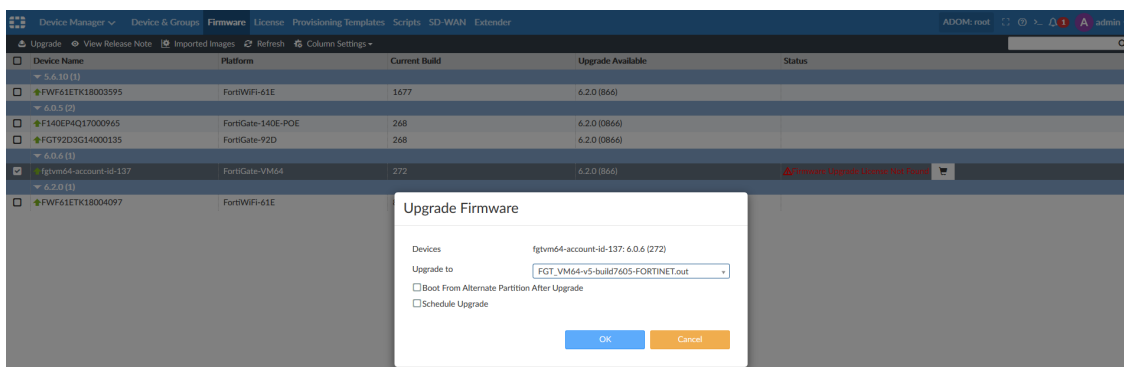
5. Click *Close*.

FortiManager performs disk check on FortiGate before upgrading firmware

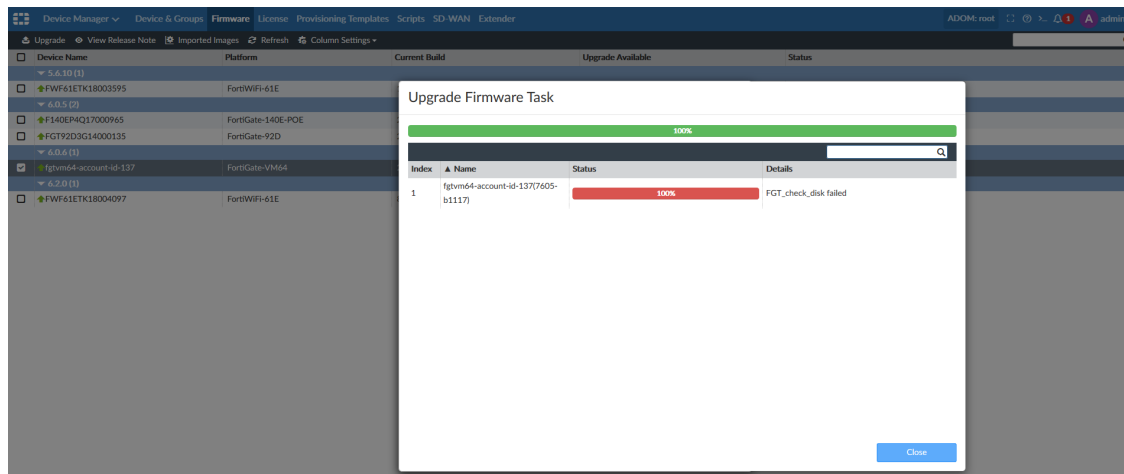
Before upgrading FortiOS, FortiManager can first check the disk file system status on FortiGate.

To upgrade FortiOS with disk check enabled:

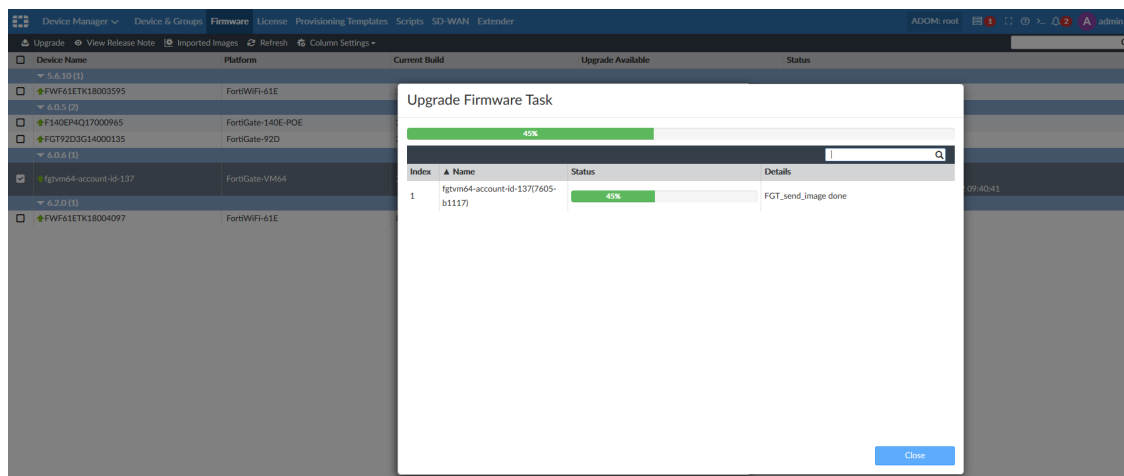
1. Go to *Device Manager > Firmware*.
2. Select a FortiGate, and click *Upgrade*.
The *Upgrade Firmware* dialog box is displayed.



3. In the *Upgrade to* box, select an image, and click *OK*.
FortiManager checks the FortiGate disk before upgrading. If the check fails, the following information is displayed, and the upgrade is not performed:



If the check passes, the upgrade proceeds:



To disable disk check:

1. Disable disk check by using the CLI:

```
config fupdate fwm-setting
(fwm-setting)# set skip-disk-check enable
```

The default setting is `disable`, which will check the FortiGate disk before upgrading FortiOS.

The following diagnose commands are also available for `diagnose fwmanager`:

- `show-dev-disk-check-status`: Shows whether a device needs a disk check.
- `show-grp-disk-check-status`: Shows whether device in a group needs a disk check.

In addition, when you log into FortiOS by using the CLI, you will be informed if you need to run a disk scan, for example:

```
$ ssh admin@193.168.70.137
```

```
WARNING: File System Check Recommended! Unsafe reboot may have caused inconsistency in disk drive.
```

It is strongly recommended that you check file system consistency before proceeding. Please run 'execute disk scan 17'

Note: The device will reboot and scan during startup. This may take up to an hour

Support FQDN address objects in firewall policies

FortiManager 6.0 ADOMs contain firewall addresses of type *Wildcard FQDN*. In FortiManager 6.2 ADOMs, the firewall address type changed from *Wildcard FQDN* to *FQDN*. However ADOM upgrade from 6.0 to 6.2 continues to support firewall address objects of type *Wildcard FQDN*.

After upgrading a 6.0 ADOM to a 6.2 ADOM, firewall addresses with type *Wildcard FQDN* change to type *FQDN*, for example:

The screenshot displays two panels: '6.0 ADOM' and '6.2 ADOM'. In the 6.0 ADOM panel, several firewall addresses are listed with the type 'Wildcard FQDN', including 'wildcard-address-qian', 'wildcard-address-1', 'update.microsoft.com', 'swscan.apple.com', and 'none'. In the 6.2 ADOM panel, these same addresses are now listed with the type 'FQDN'. A red box highlights the 'wildcard-address-qian' and 'wildcard-address-1' entries in both panels. A red arrow points from the 6.0 ADOM panel to the 6.2 ADOM panel, with the text: 'After ADOM upgraded from v6.0 to v6.2, 'wildcard-fqdn' address changed to 'fqdn' type'.

Name	Type	Details	Interface	Comments	Created Time	Last Modified
wildcard-address-qian	Wildcard FQDN	wildcard FQDN:qian.com	any		2019-10-15 17:01	admin/2019-10-15 17:01
wildcard-address-1	Wildcard FQDN	wildcard FQDN:*.qa.local	any		2019-10-15 17:01	admin/2019-10-15 17:01
update.microsoft.com	FQDN	FQDN:update.microsoft.com	any		2019-10-15 14:44	admin/2019-10-15 14:44
swscan.apple.com	FQDN	FQDN:swscan.apple.com	any		2019-10-15 14:44	admin/2019-10-15 14:44
none	IPV6 Address	IPV6 Subnet::/128	any		2019-10-15 14:44	admin/2019-10-15 14:44
none	Firewall Address	IP/Netmask:0.0.0.0/255.255.255.255	any		2019-10-15 14:44	admin/2019-10-15 14:44
google-play	FQDN	FQDN:play.google.com	any		2019-10-15 14:44	admin/2019-10-15 14:44

After upgrading a 6.0 ADOM to a 6.2 ADOM, new *_upg_wild_fqdn* firewall address are automatically created for any firewall addresses of type *FQDN* in proxy policies that existed before the upgrade, for example:

The screenshot displays two panels: '6.0 ADOM' and '6.2 ADOM'. In the 6.0 ADOM panel, several firewall addresses are listed with the type 'FQDN', including 'autoupdate.opera.com', 'fqdn-qian', 'fqdngrp', 'google-play', and 'none'. In the 6.2 ADOM panel, these same addresses are now listed with the type 'FQDN'. Additionally, new firewall addresses have been created with the type '_upg_wild_fqdn', including '_upg_wildcard-address-qian' and '_upg_wild_fqdn-qian'. A red box highlights the 'fqdn-qian' entry in the 6.0 ADOM panel and the '_upg_wild_fqdn-qian' entry in the 6.2 ADOM panel. A red arrow points from the 6.0 ADOM panel to the 6.2 ADOM panel, with the text: 'ADOM-v6.0 proxy policy used fqdn address, it created a new _upg_wild_fqdn address after ADOM upgraded to v6.2'.

Name	Type	Details	Interface	Comments	Created Time	Last Modified
FIREWALL_AUTH_PORTAL_ADDRESS	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any		2019-10-15 14:44	admin/2019-10-15 14:44
SSLVPN_TUNNEL_ADDR1	Firewall Address	IP Range:10.212.134.200-10.212.134.210	sslvpn_tun_intf		2019-10-15 14:44	admin/2019-10-15 14:44
SSLVPN_TUNNEL_IPv6_ADDR1	IPV6 Address	IPV6 Subnet:ffff:ffff::/120	any		2019-10-15 14:44	admin/2019-10-15 14:44
all	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any		2019-10-15 14:44	admin/2019-10-15 14:44
all	IPV6 Address	IPV6 Subnet::/0	any		2019-10-15 14:44	admin/2019-10-15 14:44
autoupdate.opera.com	FQDN	FQDN:autoupdate.opera.com	any		2019-10-15 14:44	admin/2019-10-15 14:44
fqdn-qian	Firewall Address	FQDN:test.com	any		2019-10-15 17:01	admin/2019-10-15 17:01
fqdngrp	Address Group	fqdn-qian	any		2019-10-15 17:01	admin/2019-10-15 17:01
google-play	Firewall Address	FQDN:play.google.com	any		2019-10-15 14:44	admin/2019-10-15 14:44
none	Firewall Address	IP/Netmask:0.0.0.0/255.255.255.255	any		2019-10-15 14:44	admin/2019-10-15 14:44
fqdngrp	Address Group	fqdn-qian	any		2019-10-15 17:01	admin/2019-10-15 17:01
fqdn-qian	Firewall Address	FQDN:test.com	any		2019-10-15 17:01	admin/2019-10-15 17:01
autoupdate.opera.com	Firewall Address	FQDN:autoupdate.opera.com	any		2019-10-15 14:44	admin/2019-10-15 14:44
all	IPV6 Address	IPV6 Subnet::/0	any		2019-10-16 13:57	admin/2019-10-16 13:57
all	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any		2019-10-16 13:57	admin/2019-10-16 13:57
_upg_wildcard-address-qian	Firewall Address	FQDN:*.qian.com	any		2019-10-16 13:57	admin/2019-10-16 13:57
_upg_wild_fqdn-qian	Firewall Address	FQDN:*.test.com	any		2019-10-16 13:57	admin/2019-10-16 13:57

When you view the proxy policy in the 6.2 ADOM after the upgrade, the proxy policy references the original firewall address object and the newly created *_upg_wild_fqdn* firewall address object, for example:

#	Proxy	Destination Int	Source	Destination	Service	Schedule	Action	Security Profile	Log
1	Explicit Web	port9	all	wildcard-address-1 wildcard-address-qian	webproxy	always	Accept	default custom-deep	Log
2	Explicit Web	port6	fqdn-qian	fqdngrp	webproxy	always	Accept	default	Log

#	Proxy	Destination Int	Source	Destination	Service	Schedule	Action	Security Profile	Log
1	Explicit Web	port9	all	wildcard-address-1 wildcard-address-qian upg_wild_wildcard-address-qian	webproxy	always	Accept	default custom-deep	Log
2	Explicit Web	port6	fqdn-qian _upg_wild_fqdn-qian	fqdngrp _upg_wild_fqdn-qian	webproxy	always	Accept	certificate-ir	Log

After upgrading to 6.2 ADOMs, you can create new firewall addresses with type *FQDN*, for example:

Create New Address

Address Name: newfqdn-wild-address

Color: [icon]

Type: FQDN

FQDN: *.fortinet.com

Interface: any

Static Route Configuration: OFF

Comments: [text area]

Add To Groups: [button: Click here to select]

Advanced Options >

Per-Device Mapping: OFF

You can also select firewall addresses with type *FQDN* in firewall policies:

Create New IPv4 Policy

Name: policy

Incoming Interface: any

Outgoing Interface: any

Source Internet Service: OFF

FSSO Groups: +

Source Address: all

Source User: +

Source User Group: +

Destination Internet Service: OFF

Destination Address: **newfqdn-wild-address**

Service: ALL

Schedule: always

Action: Deny | **Accept** | IPSEC

Log Traffic: No Log | **Log Security Events** | Log All Sessions

Generate Logs when Session Starts: [checkbox]

Capture Packets: [checkbox]

NAT: [checkbox]

Security Profiles: [checkbox]

Address List:

- login.microsoft.com
- login.microsoftonline.com
- login.windows.net
- newfqdn-wild-address**
- none
- swscan.apple.com
- update.microsoft.com
- wildcard-address-1
- wildcard-address-qian
- wildcard.dropbox.com
- wildcard.google.com
- ADDRESS GROUP (3)

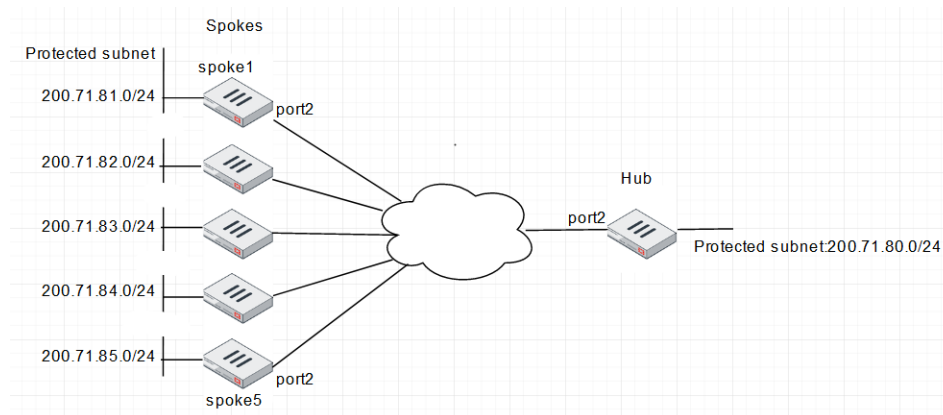
VPN Setup Wizard supports device groups

FortiManager VPN Setup Wizard supports device groups, allowing you to optimize a large number of firewalls as spokes in a VPN community.

When a device group is used in a VPN topology, FortiManager resolves the device group to individual members, and then applies the same logic to generate Phase1/Phase2 information. Keep the following restrictions in mind:

- VPN Manager only supports the use of device groups for the following hub and spoke topologies: star and dialup.
- VPN manager only supports the use of device groups for devices in the spoke role.

This document provide a sample configuration of hub and spoke (star topology) with VPN Manager and a device group.



Following is a summary of how to use device groups:

1. Create device groups. See [VPN Setup Wizard supports device groups on page 29](#).
2. Create protected subnet firewall addresses for hub and spoke devices. See [Creating protected subnet firewall addresses on page 30](#).
3. Create a VPN community. See [Creating VPN communities on page 32](#).
4. Add spoke FortiGate units to the VPN community. See [Adding spoke FortiGate units to the VPN community on page 33](#).
5. Add the hub FortiGate units to the VPN community. See [Adding the hub FortiGate unit to the VPN community on page 35](#).
The hub and spokes are created.
6. Install VPN configuration and firewall policies to hub and spoke devices. See [Installing firewall policies to hub and spoke devices on page 38](#).

This topic also covers how to:

- Remove a spoke member from a VPN community. See [Removing a spoke member from a VPN community on page 39](#).
- Add a spoke member to a VPN community. See [Adding a spoke member to a VPN community on page 41](#).

Creating device groups

To create device groups:

1. Go to *Device Manager > Device & Groups*.
2. From the *Device Group* menu, select *Create New*.
The *Create New Device Group* dialog box opens.
3. In the *Group Name* box, type a name, such as *spoke_group*.
4. Click *Add Member*, and add FortiGate units to the group.
In this example, we are adding 5 FortiGate units.

Create New Device Group

Group Name

spoke_group

Description

0/128

+ Add Member

Remove Member

Search...

Q

<input type="checkbox"/>	Device Name	Type	Platform	IP	Firmware Version
<input type="checkbox"/>	↑ vlan171_0081	Device	FortiGate-VM64	10.8.71.81	
<input type="checkbox"/>	↑ vlan171_0082	Device	FortiGate-VM64	10.8.71.82	
<input type="checkbox"/>	↑ vlan171_0083	Device	FortiGate-VM64	10.8.71.83	
<input type="checkbox"/>	⬇ vd_1 [NAT]	Device	vdom		
<input type="checkbox"/>	↑ vlan171_0084	Device	FortiGate-VM64	10.8.71.84	
<input type="checkbox"/>	⬇ vd_1 [NAT]	Device	vdom		
<input type="checkbox"/>	↑ vlan171_0085	Device	FortiGate-VM64	10.8.71.85	
<input type="checkbox"/>	⬇ FG-traffic [NAT]	Device	vdom		

OK

Cancel

5. Click *OK* to save the group.

Creating protected subnet firewall addresses

Create protected subnet firewall addresses for hub and spoke devices. VPN Manager can use the protected subnet firewall address to create static routes on FortiGate units to allow traffic destined for the remote protected network to pass through the VPN tunnel.

To create protected subnet firewall addresses:

1. Go to *Policy & Objects > Object Configurations > Addresses*.
2. From the *Create New* menu, select *Address*.
The *Create New Address* pane opens.

3. Create a protected subnet firewall address for the hub FortiGate, and click **OK**.

Create New Address

Address Name	<input type="text" value="Protected_hub_subnet"/>
Color	
Type	<input type="text" value="Subnet"/>
IP/Netmask	<input type="text" value="200.71.80.0/255.255.255.0"/>
Interface	<input type="text" value="any"/>
Static Route Configuration	<input type="button" value="OFF"/>
Comments	<div><div></div><div>0/255</div></div>
Add To Groups	<input type="button" value="Click here to select"/>

Advanced Options >

Per-Device Mapping	<input type="button" value="OFF"/>
--------------------	------------------------------------

4. From the *Create New* menu, select *Address*.
The *Create New Address* pane opens.
5. Create a protected subnet firewall address with per-device mapping for spoke FortiGate units, and click **OK**.

Create New Address

Address Name	<input type="text" value="protected_subnet_spoke"/>
Color	
Type	<input type="text" value="Subnet"/>
IP/Netmask	<input type="text" value="210.71.0.0/255.255.0.0"/>
Interface	<input type="text" value="any"/>
Static Route Configuration	<input type="button" value="OFF"/>
Comments	<div><div></div><div>0/255</div></div>
Add To Groups	<input type="button" value="Click here to select"/>

Advanced Options >

Per-Device Mapping	<input checked="" type="button" value="ON"/>
--------------------	--

+ Create New Edit Delete Column Settings ▾

<input type="checkbox"/>	▲ Name	VDOM	Details
<input type="checkbox"/>	vlan171_0081	root	IP/Netmask:200.71.81.0/255.255.255.0
<input type="checkbox"/>	vlan171_0082	root	IP/Netmask:200.71.82.0/255.255.255.0
<input type="checkbox"/>	vlan171_0083	vd_1	IP/Netmask:200.71.83.0/255.255.255.0
<input type="checkbox"/>	vlan171_0084	vd_1	IP/Netmask:200.71.84.0/255.255.255.0
<input type="checkbox"/>	vlan171_0085	root	IP/Netmask:200.71.85.0/255.255.255.0

Creating VPN communities

To create a VPN community:

1. Go to *VPN Manager > IPsec VPN*, and click *Create New*. The *VPN Topology Setup Wizard* opens.
2. In the *Name* box, type a name, such as *star*.
3. Under *Choose VPN Topology*, select *Star*, and click *Next*.

VPN Topology Setup Wizard

Choose VPN Topology

☐ Full Meshed ☒ Star ☐ Dial up

< Back Next > Cancel

4. Specify the *Authentication & Encryption Settings*, and click *Next*.

VPN Topology Setup Wizard

Authentication & Encryption Settings:

Authentication ☒ Pre-shared Key ☐ Certificates

☒ Generate (random)
☐ Specify

Encryption

IKE Security (Phase 1) Properties

IKE Version ☐ 1 ☒ 2

#	Encryption	Authentication	
1	<input type="text" value="AES128"/>	<input type="text" value="SHA1"/>	+
2	<input type="text" value="AES256"/>	<input type="text" value="SHA256"/>	+

Ipssec Security (Phase 2) Properties

< Back Next > Cancel

5. Configure VPN Phase 1 and Phase 2 settings, and click *Next*.

VPN Topology Setup Wizard

VPN Zone ☒ ON

☒ Create Default Zones

☐ Use Custom Zone

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

Exchange Mode ☐ Aggressive ☒ Main(ID Protection)

Key Life (120-172800 seconds)

Dead Peer Detection ☐ Disable ☐ On Idle ☒ On Demand

IPsec Security Phase 2 Advanced Properties

Diffie-Hellman Group(s) ☐ 1 ☐ 2 ☒ 5 ☒ 14 ☐ 15 ☐ 16
☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 27
☐ 28 ☐ 29 ☐ 30 ☐ 31 ☐ 32

< Back Next > Cancel

Adding spoke FortiGate units to the VPN community

To add spoke FortiGate units to the VPN community:

1. Go to *VPN Manager > IPsec VPN*, and click the community that you created.
The community opens in the content pane.
2. Click *Create New > Managed Gateway*.
The *VPN Gateway Setup Wizard* opens for the community.
3. Set the *Protected Network* options, and then click *Next*:
 - a. Beside *Protected Subnet*, click *Click here to select*, and select the protected subnet.

VPN Gateway Setup Wizard - star

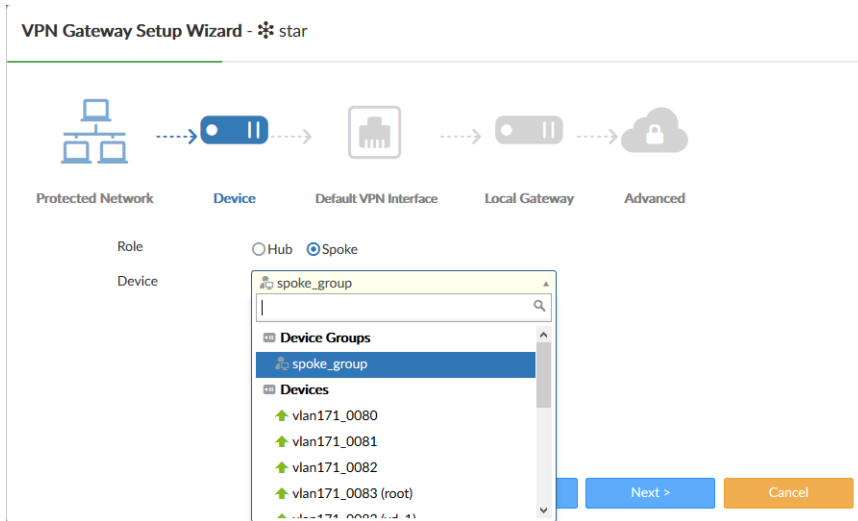
Protected Network Device Default VPN Interface Local Gateway Advanced

Protected Subnet

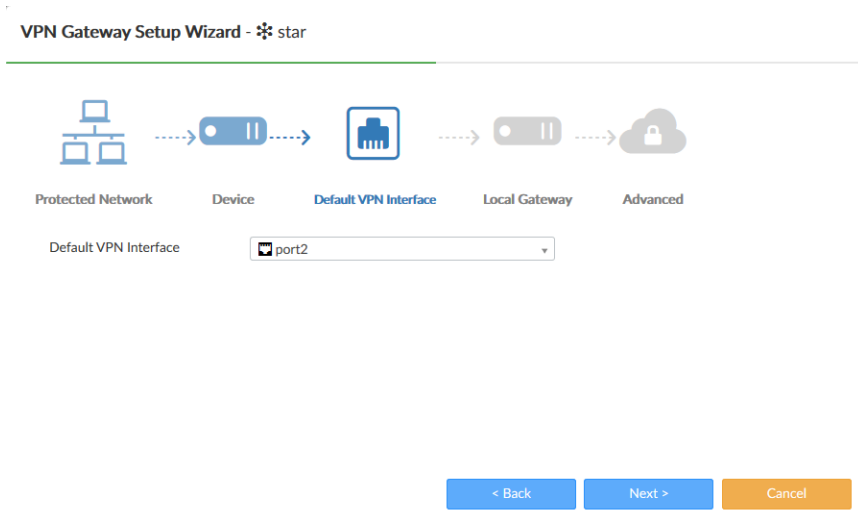
protected_subnet_spoke
IP/Netmask:210.71.0.0/255.255.0.0
1 Entry Selected

< Back Next > Cancel

4. Set the *Device* options, and then click *Next*:
 - a. Beside *Role*, select *Spoke*
 - b. Beside *Device*, select the device group you created named *spoke_group*.

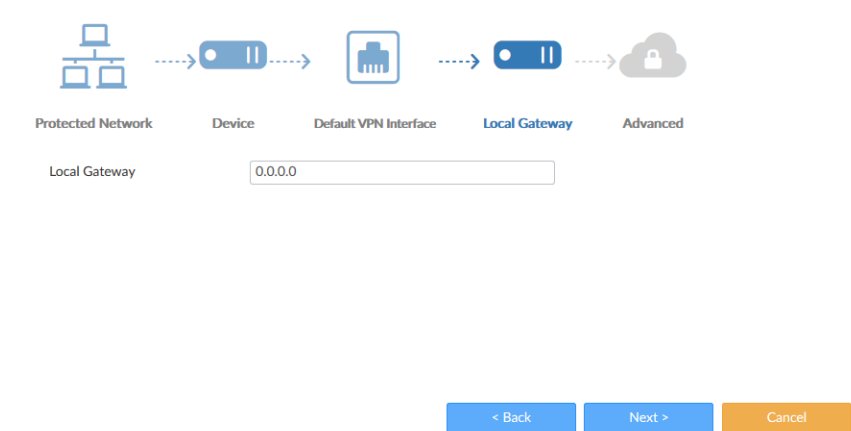


5. Set the *Default VPN Interface* options, and click *Next*.
 - a. Beside *Default VPN Interface*, select the interface for spokes, which is often the internet-facing interface.



6. Set the *Local Gateway* options, and click *Next*.
 - a. Beside *Local Gateway*, type the IP address for the gateway.

VPN Gateway Setup Wizard - ⚙️ star



The screenshot shows the 'Local Gateway' step of the VPN Gateway Setup Wizard. At the top, a progress bar indicates the sequence of steps: Protected Network, Device, Default VPN Interface, Local Gateway (current), and Advanced. Below the progress bar, the 'Local Gateway' label is followed by a text input field containing '0.0.0.0'. At the bottom of the wizard, there are three buttons: '< Back' (blue), 'Next >' (blue), and 'Cancel' (orange).

7. Set the *Advanced* options, and click *OK*.
 - a. Beside *Routing*, select *Manual (via Device Manager)* or *Automatic*.

VPN Gateway Setup Wizard - ⚙️ star

Local ID

Routing ☐ Manual (via Device Manager) ☒ Automatic

Advanced Options >

At the bottom of the wizard, there are three buttons: '< Back' (blue), 'OK' (blue), and 'Cancel' (orange).

Adding the hub FortiGate unit to the VPN community






To add a hub FortiGate unit to the VPN community:

1. Go to *VPN Manager > IPsec VPN*, and click the community that you created.
The community opens in the content pane.
2. Click *Create New > Managed Gateway*.
The *VPN Gateway Setup Wizard* opens for the community.

3. Set the *Protected Network* options, and then click *Next*:

- a. Beside *Protected Subnet*, click *Click here to select*, and select the protected subnet.

VPN Gateway Setup Wizard - ⚙️ star



Protected Subnet






Protected_subnet_hub
IP/Netmask:200.71.80.0/255.255.255.0
1 Entry Selected

< Back Next > Cancel

4. Set the *Device* options, and then click *Next*:

- a. Beside *Role*, select *Hub*
- b. Beside *Device*, select the device for the hub.

VPN Gateway Setup Wizard - ⚙️ star








Role ☒ Hub ☐ Spoke

Device

< Back Next > Cancel

5. Set the *Default VPN Interface* options, and click *Next*.
 - a. Beside *Default VPN Interface*, select the interface for the hub, which is often the internet-facing interface.

VPN Gateway Setup Wizard - ⚙️ star








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

Default VPN Interface

Hub-to-Hub Interface (Required for multiple Hubs)

6. Set the *Local Gateway* options, and click *Next*.
 - a. Beside *Local Gateway*, type the IP address for the gateway.

VPN Gateway Setup Wizard - ⚙️ star



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

Local Gateway

7. Set the *Advanced* options, and click **OK**.
 - a. Beside *Routing*, select *Manual (via Device Manager)* or *Automatic*.

VPN Gateway Setup Wizard - star

Local ID

Routing ☐ Manual (via Device Manager) ☒ Automatic

Summary Network(s)

Seq#	Network	Priority
1	<input type="text"/>	1 <input type="button" value="+"/>

Advanced Options >

< Back OK Cancel

The hub and spoke are created.

VPN Manager VPN IPsec VPN Monitor Map View SSL VPN ADOM: 60 admin

VPN Community Install Wizard

star

Star

Name: star

Number of VPN: 2

Authentication: Pre-shared Key

IKE Security (Phase 1) Properties: aes256-sha256, aes256-sha384

IPsec Security (Phase 2) Properties: aes256-sha256, aes256-sha384

Name	Role	Default VPN Interface	Protected Subnet	Automatic Routing
FGT_0080[root]	Hub	port2	Protected_subnet_hub	Automatic
spoke_group (5)	Spoke	port2	protected_subnet_spoke	Automatic
FGT_0081				
FGT_0082				
FGT_0083				
FGT_0084				
FGT_0085				

Installing firewall policies to hub and spoke devices

Create firewall policies for hub and spoke FortiGate, and then install the configurations by using the Install Wizard.

To install configurations to hub and spoke devices:

1. Go to *Policy & Object > Policy Packages*.
2. Create firewall policies for hub and spoke FortiGate.

Policy & Objects Policy Packages Object Configurations ADOM: vpn_mgmt

Policy Package Install ADOM Revisions Tools Collapse All Object Selector

Search...

+ Create New Edit Delete Section Policy Lookup Column Settings View Mode

#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profile	Log
1		vpnmgmt_star_hub2spoke	port3	lan171	Protected_hub_subnet	always	ALL		Accept	no-inspect	Log Security
2		port3	vpnmgmt_star	Protected_hub_subnet	lan171	always	ALL		Accept	no-inspect	Log Security
3		vpnmgmt_star_spoke2hub	port3	internal	lan171	always	ALL		Accept	no-inspect	Log Security
4		port3	vpnmgmt_star	lan171	internal	always	ALL		Accept	no-inspect	Log Security
Implicit (5-5 / Total: 1)											
5	Implicit Deny	any	any	all	all	always	ALL		Deny		No Log

3. From the *Install* menu, select *Install Wizard*.

4. Select *Install Policy Package & Device Settings*, and then click *Next*.

Install Wizard

☒ **Install Policy Package & Device Settings**

Install a selected policy package. Any device specific settings for devices associated with the package will also be installed.

Policy Package

star

Comment

☐ Create ADOM Revision

☐ Schedule Install

☐ **Install Device Settings (only)**

Next >

Cancel

5. Complete the wizard to install the configurations.

Removing a spoke member from a VPN community

You can remove a spoke member from a VPN community by removing the device from the device group, and then installing the configuration change to the FortiGates.

To remove a spoke member from a VPN community:

1. Remove the device from the device group:
 - a. Go to *Device Manager > Device & Groups*.
 - b. In the tree menu, right-click the group name, and select *Edit Group*.
The *Edit Device Group* dialog box opens.

- c. Select a device, for example, *vlan171_0085*, and click *Remove Member*.

Edit Device Group

Group Name: spoke_group

Description:
 0/128

+ Add Member **Remove Member** Search...

<input type="checkbox"/>	Device Name	Type	Platform	IP	Firmware Version
<input type="checkbox"/>	vlan171_0081	Device	FortiGate-VM64	10.8.71.81	
<input type="checkbox"/>	vlan171_0082	Device	FortiGate-VM64	10.8.71.82	
<input type="checkbox"/>	vlan171_0083	Device	FortiGate-VM64	10.8.71.83	
<input type="checkbox"/>	vd_1 [NAT]	Device	vdom		
<input type="checkbox"/>	vlan171_0084	Device	FortiGate-VM64	10.8.71.84	
<input type="checkbox"/>	vd_1 [NAT]	Device	vdom		
<input checked="" type="checkbox"/>	vlan171_0085	Device	FortiGate-VM64	10.8.71.85	
<input checked="" type="checkbox"/>	FG-traffic [NAT]	Device	vdom		

OK Cancel

- d. Click *OK* to save the changes.

2. Execute Policy package installation to purge VPN configuration from FortiGates.
Install preview page shows that FortiManager will purge the related configuration on the hub FortiGate.

Install Wizard - Policy Package (star)

✓ Installation Preparation Total: 7/7, Success: 7, Error: 0, Warning: 0

Index	Name	Status
1	VPN manager	Init vpn context done
2	Write summary[preview]	Write preview done
3	vlan171_0080[copy] - root	Copy to device done
4	vlan171_0081[copy] - root	Copy to device done
5	vlan171_0082[copy] - root	Copy to device done
6	vlan171_0083[copy] - vd_1	Copy to device done
7	vlan171_0084[copy] - vd_1	Copy to device done

Install Preview

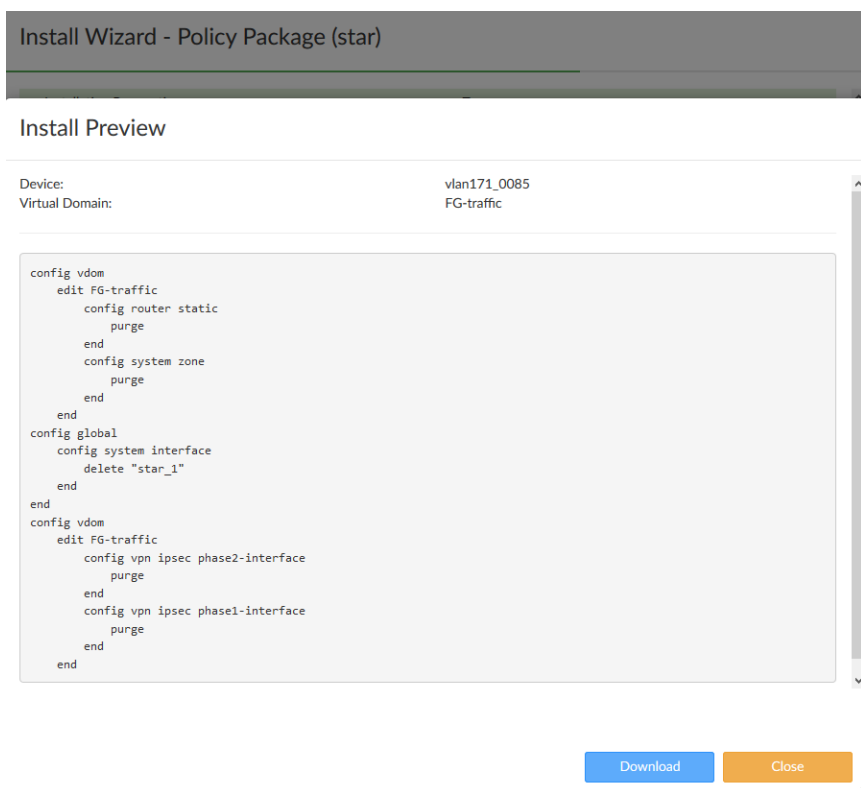
Device: vlan171_0080
Virtual Domain: root

```

config router static
  delete 1072741830
end
config system zone
  edit "vpnmgr_star_hub2spoke"
    set interface "star-1" "star-2" "star-3" "star-5"
  next
end
config system interface
  delete "star-4"
end
config vpn ipsec phase2-interface
  delete "star-4_0"
end
config vpn ipsec phase1-interface
  delete "star-4"
end

```

The *Install Preview* page shows that FortiManager will delete related configurations on the spoke FortiGate named *vlan181_0085*.

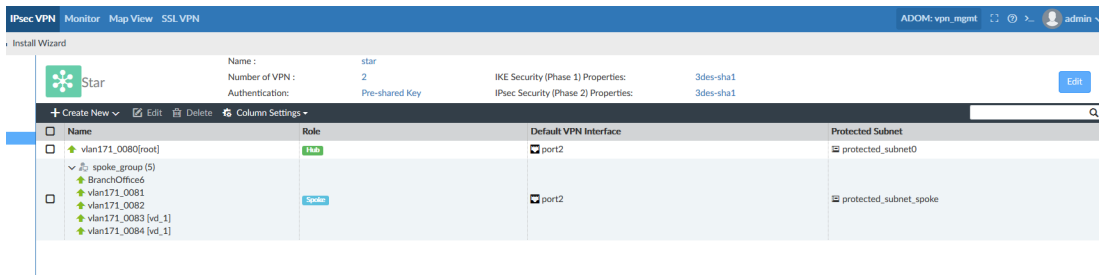


Adding a spoke member to a VPN community

You can add a spoke member to a VPN community by adding the device to the device group, and then installing the configuration change to the FortiGate.

To add a new spoke member to a VPN community:

1. Add a device to the device group:
 - a. Go to *Device Manager > Device & Groups*.
 - b. In the tree menu, right-click the group name, and select *Edit Group*.
The Edit Device Group dialog box opens.
 - c. Click *Add Member*, select the device, for example *BranchOffice6*, and click *Add*.
 - d. Click *OK* to save the changes.
2. Go to VPN manager community summary page, the new spoke member is displayed.
In the following example, the member named *BranchOffice6* is displayed.



3. Execute Policy package installation to push VPN config to HUB and newly added spoke devices.
For example, the *Install Preview* page shows that FortiManager will install IPsec VPN configuration to the new spoke member. In this example, the new spoke member is named *BranchOffice6*.

Install Preview

Device: BranchOffice6

Virtual Domain: root

```
config vpn ipsec phase1-interface
  edit "star_1"
    set interface "port2"
    set comments "[created by FMG VPN Manager]"
    set dhgrp 1 5
    set proposal 3des-sha1
    set keylife 28800
    set peertype any
    set remote-gw 100.71.80.1
    set net-device disable
    set add-gw-route enable
    set psksecret ENC Z8Zpc/bwU2j1HxCFWzO/Xkklz1iO6IOFpF2mmab0XvcAk+pnJrLz5+MLa6KZwR821VYN0GU4AL8P2BL5g5w1irFHSTRFIOE
  next
end
config system interface
  edit "star_1"
    set vdom "root"
    set type tunnel
    set snmp-index 114
    set interface "port2"
  next
end
config system zone
  edit "vpnmgm_star_spoke2hub"
    set interface "star_1"
  next
end
config vpn ipsec phase2-interface
  edit "star_1_0"
    set phase1name "star_1"
    set proposal 3des-sha1
    set auto-negotiate enable
    set comments "[created by FMG VPN Manager]"
    set dhgrp 1 5
    set keylifeseconds 1800
```

Other

This section lists other new features added to FortiManager.

List of new features:

- [Force admin password change on page 43](#)
- [Acknowledgment of expired trial license on page 44](#)

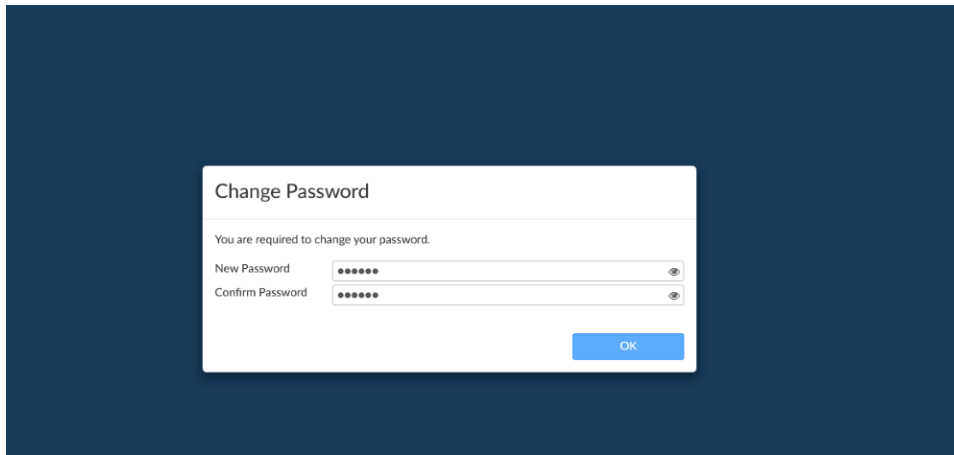
Force admin password change

The default administrator account named *admin* has an empty password by default. You can use this account to log in to a new FortiManager device or to log in to a FortiManager device after completing a factory reset.

After you log in to FortiManager for the first time by using the admin account, the system requests a password change. A password change is also required when you log in for the first time after completing a factory reset. You must change the password before you can complete logging in.

To perform a factory reset and change the admin password:

1. Reset the FortiManager device to factory settings by running the following command `execute reset all-except-ip`.
2. After the system boots up, log on by using the *admin* account with no password.
The *Change Password* dialog box is displayed, requiring you to change the password.

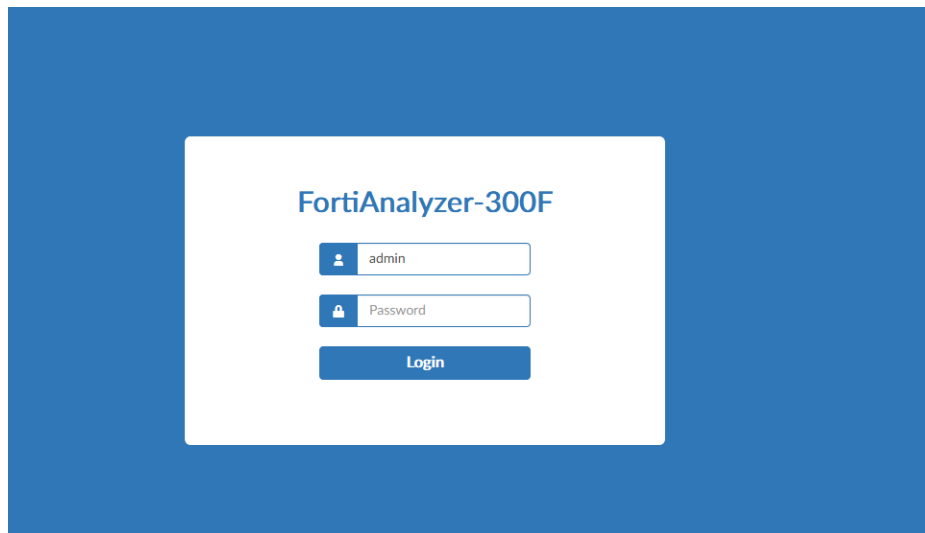


3. Specify a new password, and click *OK*.
The password is changed, and you are logged in to FortiManager.

To retain the default the admin password after upgrading FortiManager by using the GUI:

1. Before upgrading FortiManager, ensure that the *admin* account has no password.
2. Upgrade FortiManager to version 6.2.2 or later.

- Use the admin account with no password to log in to FortiManager.
You can use the GUI or CLI to log in.



Because the password for the *admin* account was empty before the upgrade, FortiManager does not require you to change the password to non-empty one.

Acknowledgment of expired trial license

FortiManager now provides an option in the GUI for an administrator to acknowledge the expired license so FortiGuard subscriptions can be reset to *Valid*.

To acknowledge expired trial licenses:

- Go to *Device Manager > License*.

Device Manager

Device & Groups

Firmware

License

Provisioning Templates

Scripts

SD-WAN

Push Update

Refresh

Export

Check License

Column Settings

Device Name

Serial Number

Firmware Version

Support Contract

FortiGuard Subscription

Service Status

Virtual Domains

❑

FG200D4614809549

5.6.6, build3444

2667

Expired

Unknown

❑

FWF60D4615017919

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q16001504

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q16001690

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q17000740

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q16001699

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q16002450

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q16002022

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q16001611

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q16001553

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q17000733

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q16001333

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q16002386

5.6.6, build3444

2667

Expired

Unknown

❑

FG201ETK18902483

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61ETK18001846

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q16001749

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q16001484

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q16001402

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q17000526

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q16001424

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q16001810

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q16002377

5.6.6, build3444

2667

Expired

Unknown

❑

FG800D3917800033

5.6.6, build3444

2667

Expired

Unknown

❑

FWF61E4Q16001254

5.6.6, build3444

2667

Expired

Unknown

IPS & Application Control

Expires on 2020-02-03

AntiVirus

Expires on 2020-02-03

Web Filtering

Expires on 2020-02-03

Email Filtering

Expires on 2020-02-03

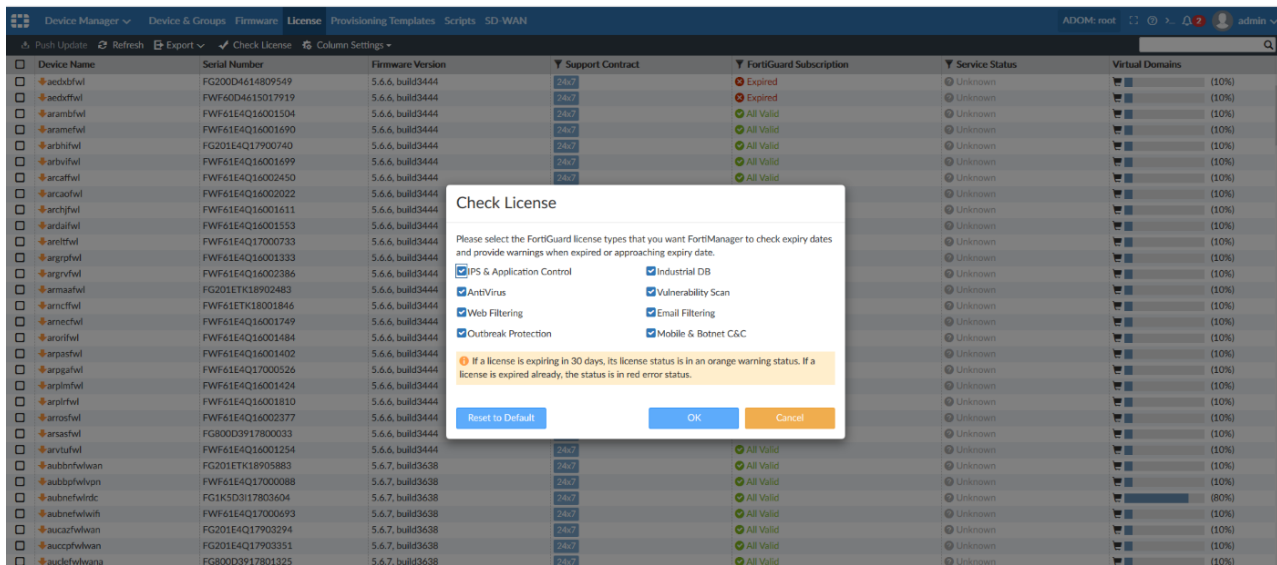
Outbreak Protection

Expires on 2020-02-03

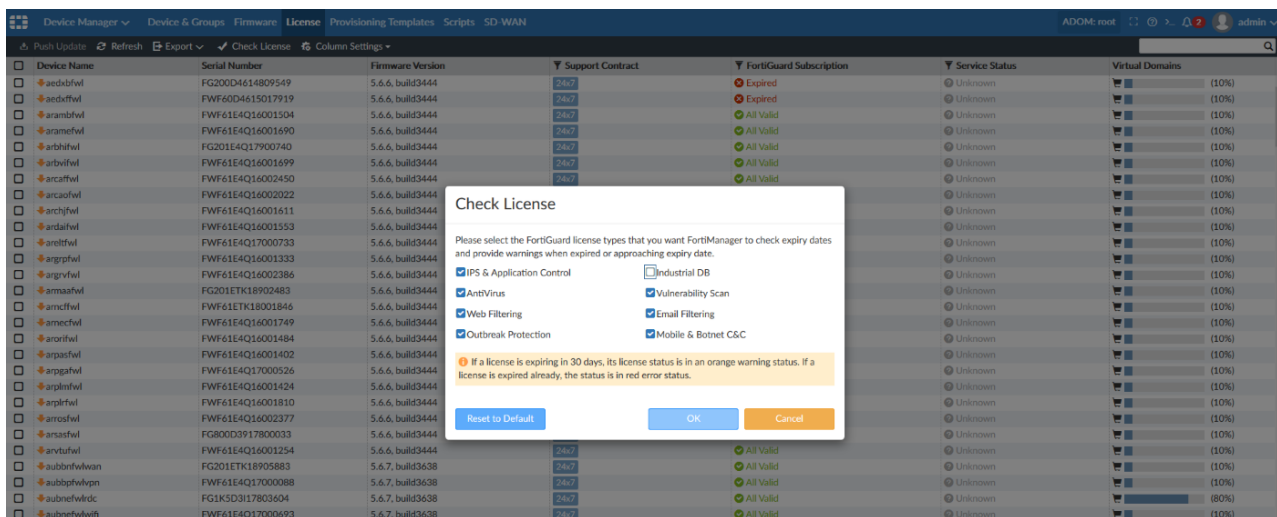
Industrial DB

Expired on 2018-04-03

2. Click *Check License*.

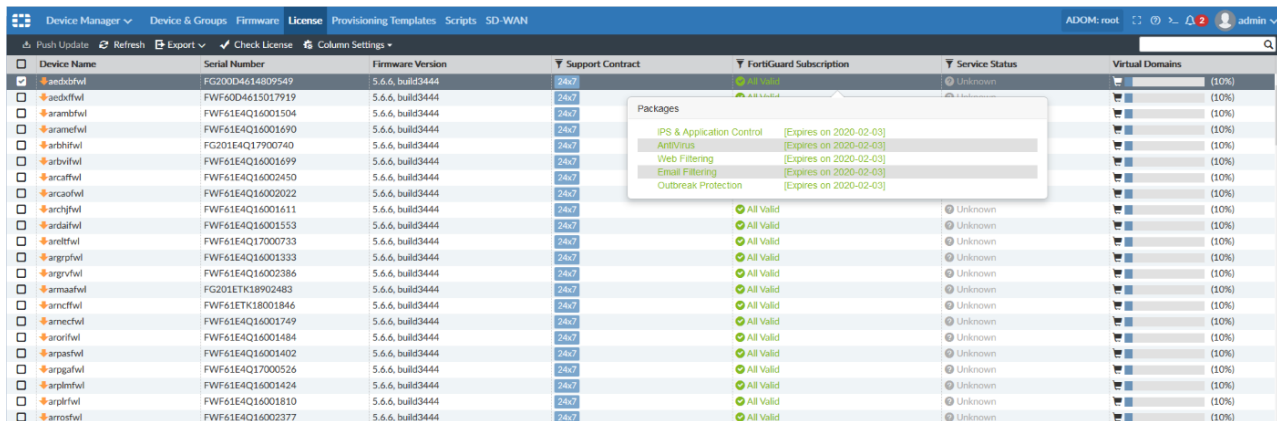


3. Clear the *Industrial DB* check box.



The FortiGuard subscription now shows the status as *Valid*.

4. Hover over the license status for more information.





FORTINET®



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.