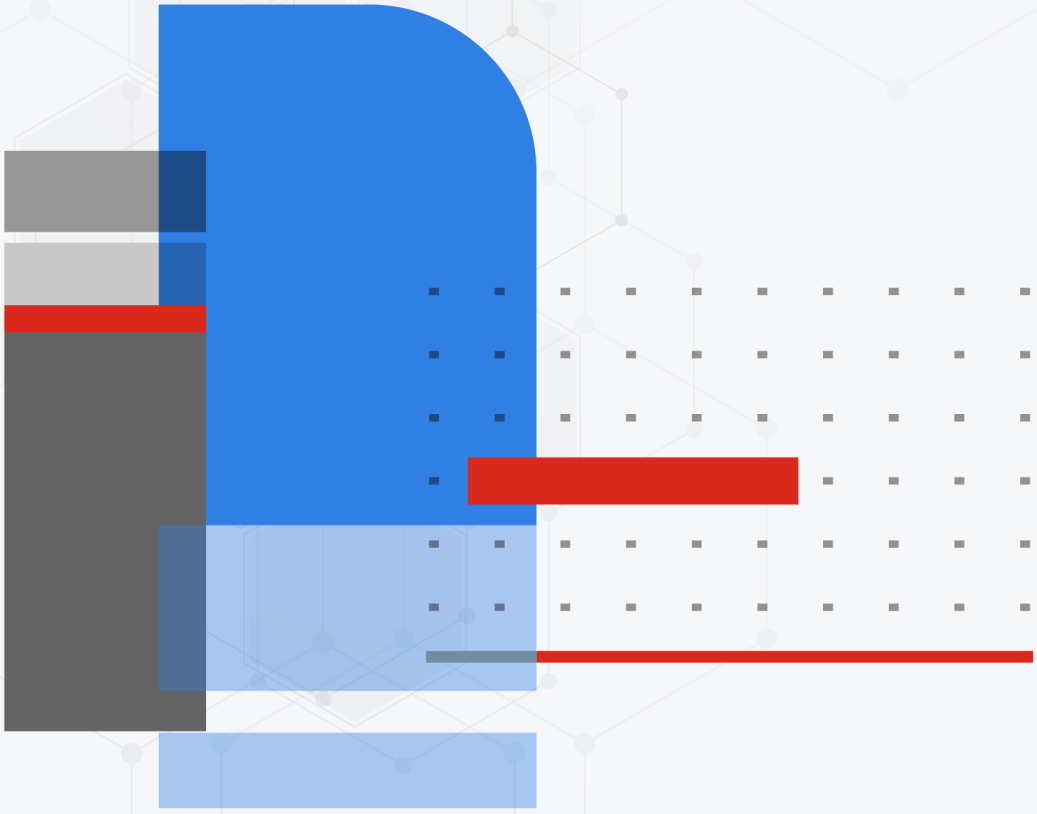
Administration Guide

FortiManager 7.4.11



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

FORTINET VIDEO LIBRARY
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/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com



May 7, 2026
FortiManager 7.4.11 Administration Guide
02-7411-890235-20260507

TABLE OF CONTENTS

Change Log **14**
Setting up FortiManager **15**
Connecting to the GUI 15
FortiManager Setup wizard 16
Activating VM licenses 22
Security considerations 24
Restricting GUI access by trusted host 24
Trusted platform module support 25
Self-encrypting drives 26
UEFI secure boot 30
Other security considerations 32
GUI overview 33
Panes 35
Color themes 36
Side menu open or closed 37
Switching between ADOMs 37
Using the right-click menu 37
Using the CLI console 38
Avatars 39
Using the Process Monitor 39
Showing and hiding passwords 40
Google Map integration 41
FortiAnalyzer Features 41
Enable or disable FortiAnalyzer features 42
Initial setup 43
Restarting and shutting down 43
FortiManager Key Concepts **44**
Communication through protocols 45
FortiGuard 46
Device Manager 46
FortiAnalyzer features 46
Configuration through Device Manager 47
Direct device database editing 47
Indirect device database editing 47
Model devices 48
Zero-touch and low-touch provisioning 48
ADOMs and devices 49
Global ADOM layer 50
ADOM and policy layer 50
Device Manager layer 51
Operations 51
Install device settings only 51
Quick install (device db) 52
Install policy package 52
Re-install policy 53

Import configuration 53
Retrieve configuration 53
Auto-update and auto-retrieve 54
Auto-backup 54
Refresh 54
Revert 54
Sequence of operations for installation to managed devices 55
Key features of the FortiManager system 59
Security Fabric 59
Configuration revision control and tracking 59
Centralized management 59
Administrative domains 60
Local FortiGuard service provisioning 60
Firmware management 60
Scripting 60
Logging and reporting 60
Fortinet device life cycle management 60
Dashboard 61
Customizing the dashboard 62
System Information widget 63
Changing the host name 64
Configuring the system time 65
Updating the system firmware 66
Backing up the system 71
Restoring the configuration 74
Migrating the configuration 75
System Resources widget 76
License Information widget 76
Registering with FortiCloud 78
Activating add-on licenses 78
Understanding license count rules 80
License expiration 80
Unit Operation widget 82
Alert Messages Console widget 82
Log Receive Monitor widget 83
Insert Rate vs Receive Rate widget 83
Log Insert Lag Time widget 84
Receive Rate vs Forwarding Rate widget 84
Disk I/O widget 85
Device widgets 85
Restart, shut down, or reset FortiManager 86
Restarting FortiManager 86
Shutting down FortiManager 87
Resetting system settings 87
Device Manager 88
ADOMs 89
Device & Groups 89

Add devices 91
Add FortiAnalyzer or FortiAnalyzer BigData 134
Add VDOM 145
Device groups 147
Table view 148
Ring view 162
Map view 165
Folder view 169
Import Configuration wizard 173
Install wizard 180
Firmware upgrade 186
Device database (DB) 194
Device DB - Dashboard 199
Device DB - configuration management 205
Device DB - Network Interface 210
Device DB - System Virtual Domain 213
Device DB - Network SD-WAN 217
Device DB - Network BGP 226
Device DB - CLI Configurations 227
Device maintenance 227
Managing FortiGate HA clusters 229
Retrieving account level entitlements for FortiGate 237
Remotely access a managed FortiGate 238
Scripts 239
Enabling scripts 240
Configuring scripts 240
CLI script group 246
Script syntax 247
Script history 251
Script samples 251
Provisioning Templates 273
Template groups 274
Fabric authorization templates 278
System templates 281
IPsec tunnel templates 286
SD-WAN templates 304
SD-WAN overlay templates 327
Static route templates 348
BGP templates 350
Certificate templates 354
Threat Weight templates 356
CLI templates 357
NSX-T service templates 371
Export and import provisioning template configurations 374
Viewing the CLI preview for provisioning templates 376
Firmware templates 378
Firmware template upgrade sequence 378
Creating firmware templates 379
Editing firmware templates 382

Deleting firmware templates 382
Assigning firmware templates to devices 382
Previewing upgrades 383
Reviewing upgrade history 383
Upgrading devices now 384
Viewing the firmware upgrade report 384
Monitors 386
SD-WAN Monitor 386
VPN Monitor 396
Asset Identity Center 398
AI Analysis 400
LTE modem monitors 401
FortiGate chassis devices 401
Viewing chassis dashboard 402
Policy & Objects 407
About policies 410
Policy theory 410
Global policy packages 411
Policy workflow 412
Provisioning new devices 412
Day-to-day management of devices 412
Feature visibility 413
Configuring feature visibility settings 413
Viewing policies and objects in a single pane 413
Managing policy packages 414
Create new policy packages 415
Create new policy package folders 416
Edit a policy package or folder 416
Clone a policy package 417
Remove a policy package or folder 417
Assign a global policy package 417
Install a policy package 419
Reinstall a policy package 419
Schedule a policy package install 421
Export a policy package 422
Policy package installation targets 422
Perform a policy consistency check 424
View logs related to a policy rule 426
Find and replace objects 426
Managing policies 427
Creating policies 429
Editing policies 501
Viewing policies 510
Using Policy Blocks 517
Creating Policy Blocks 518
Editing Policy Blocks 519
Adding policies to a Policy Block 520
Appending a Policy Block to a Policy Package 521

Installing Policy Blocks to target devices 522
Using Policy Blocks versus Global Policy Packages 525
Role-based access control for Policy Blocks 526
Migrating global policies to policy blocks 526
Managing objects and dynamic objects 532
Creating objects 533
Managing objects 536
Viewing objects 540
Normalized interfaces 544
Dynamic mapping 552
CLI configurations 556
ADOM-level metadata variables 557
FortiToken configuration 560
FSSO user groups 561
VIP mapping 564
Shaping profiles 564
Intrusion prevention (IPS) 566
Default address space objects 571
Zero Trust Network Access (ZTNA) objects 572
FortiProxy content analysis objects 575
ADOM revisions 577
AP Manager 580
Managed FortiAPs 581
Quick status bar 581
Managing APs 583
FortiAP groups 590
Device summary 591
Authorizing and deauthorizing FortiAP devices 592
Installing changes to FortiAP devices 592
Rogue APs 592
Authorizing unknown APs 594
Connected clients 595
Spectrum analysis for managed APs 596
Clients Monitor 597
Health Monitor 598
Replacing APs 599
WiFi Maps 600
Google map 601
Floor map 602
WiFi profiles and settings for central management 604
Enabling FortiAP central management 605
SSIDs 605
FortiAP profiles 616
QoS profiles 624
Bonjour profiles 626
Bluetooth profiles 629
WIDS profiles 631
L3 firewall profiles 636

ARRP profiles 639
WiFi settings 641
Assigning profiles to FortiAP devices 645
Using Fortinet recommended profiles 646
WiFi profiles and settings for per-device management 649
Enabling FortiAP per-device management 649
Creating profiles 649
VPN Manager 650
Overview 650
Enabling central VPN management 651
DDNS support 652
VPN Setup Wizard supports device groups 653
IPsec VPN 666
IPsec VPN Communities 666
IPsec VPN gateways 676
Using Map View 683
Monitoring IPsec VPN tunnels 684
SSL VPN 684
SSL VPN settings 685
SSL VPN portals 687
SSL VPN monitor 694
VPN security policies 695
Defining policy addresses 695
Defining security policies 696
Fabric View 697
Security Fabric Topology 697
Physical Topology 698
Logical Topology 699
Filter Topology Views 700
Search Topology Views 701
Security Rating 701
Viewing Security Fabric Ratings 703
Security Fabric score 704
Fabric Connectors 705
Core Network Security 705
External Connectors 707
Public and private SDN 708
Threat Feeds 744
Endpoint/Identity 745
Cloud Orchestration 781
Creating cloud connectors 782
Creating cloud deployment templates 783
Deploying cloud orchestration 785
FortiGuard 787
Using FortiManager as a local FDS 788
Firmware revision management 789

Device licenses ... 789
View licensing status ... 789
Package management ... 791
Receive status ... 791
Service status ... 792
IoT packages ... 794
Exporting packages example ... 795
Importing packages example ... 796
Manually specifying a package version to deploy ... 798
Query services ... 800
Receive status ... 800
Query status ... 801
Exporting web filter databases example ... 801
Importing web filter databases example ... 802
Providing delta updates to downstream FortiManagers in cascade mode ... 803
Enabling IoT query services ... 805
Firmware images ... 806
Download prioritization ... 808
Product download prioritization ... 808
Package download prioritization ... 809
External resources ... 810
Settings ... 812
Connecting the built-in FDS to the FDN ... 815
Operating as an FDS in a closed network ... 816
Licensing in an air-gap environment ... 819
Enabling FDN third-party SSL validation and Anycast support ... 827
Configuring devices to use the built-in FDS ... 827
FortiGuard Service Status ... 828
Matching port settings ... 828
Handling connection attempts from unauthorized devices ... 829
Configure a FortiManager without Internet connectivity to access a local FortiManager as FDS ... 829
Configuring FortiGuard services ... 830
Enabling push updates ... 831
Enabling updates through a web proxy ... 832
Overriding default IP addresses and ports ... 833
Scheduling updates ... 833
Accessing public FortiGuard web and email filter servers ... 834
Preloading FortiGuard services ... 835
Logging events related to FortiGuard services ... 835
Logging FortiGuard antivirus and IPS updates ... 836
Logging FortiGuard web or email filter events ... 836
Restoring the URL or antispam database ... 837
FortiSwitch Manager ... 838
Managed FortiSwitches ... 839
Quick status bar ... 840
Managing FortiSwitches ... 841

Authorizing and deauthorizing FortiSwitch devices 849
Upgrading firmware for managed switches 849
Using zero-touch deployment for FortiSwitch 850
Creating a FortiSwitch group 851
Installing changes to managed switches 852
Diagnostics and tools 853
Monitors 856
FortiSwitch central management 858
Enabling FortiSwitch central management 858
FortiSwitch Templates 859
FortiSwitch per-device management 877
Enabling per-device management 878
Creating VLANs 878
Creating NAC policies 879
Creating security policies 879
Creating LLDP profiles 879
Creating QoS policies 880
Creating custom commands 883
CLI Configurations 885
Configuring a port on a single FortiSwitch 886
Exporting FortiSwitch ports to another VDOM 887
Extender Manager 889
Managed extenders 889
Managing FortiExtender devices 891
Extender profiles 892
FortiExtender profiles 893
Using Fortinet recommended extender profiles 894
Data plans 896
FortiExtender SSIDs 897
System Settings 900
Logging Topology 900
Network 901
Configuring network interfaces 902
Disabling ports 904
Changing administrative access 904
Static routes 905
Packet capture 905
Aggregate links 906
VLAN interfaces 907
SNMP 908
RAID Management 918
Supported RAID levels 918
Configuring the RAID level 921
Monitoring RAID status 921
Checking RAID from command line 922
Swapping hard disks 923
Adding hard disks 924

Administrative Domains (ADOMs) 924
FortiProxy ADOMs 926
Enabling and disabling the ADOM feature 927
ADOM device modes 928
ADOM modes 928
Managing ADOMs 932
Deleting ADOMs 938
Checking ADOM health 939
ADOM versions 941
Concurrent ADOM access 946
Locking an ADOM 947
Upgrading an ADOM 948
Using mixed versions in ADOMs 950
Global Database 950
Certificates 955
Local certificates 956
CA certificates 959
Certificate revocation lists 960
Event Log 961
Event log filtering 962
Task Monitor 963
Mail Server 964
Syslog Server 966
Send local logs to syslog server 967
Meta Fields 967
Device logs 969
Configuring rolling and uploading of logs using the GUI 970
Configuring rolling and uploading of logs using the CLI 972
Miscellaneous Settings 973
Administrators 976
Trusted hosts 976
Monitoring administrators 977
Disconnecting administrators 977
Managing administrator accounts 977
Creating administrators 979
Editing administrators 984
Deleting administrators 985
Override administrator attributes from profiles 985
Creating administrators for the FortiManager API 987
Restricted administrators 989
Web Filter restricted administrator 990
Intrusion prevention restricted administrator 993
Application control restricted administrator 1006
Installing profiles as a restricted administrator 1008
Workspace mode for restricted administrators 1009
Administrator profiles 1010
Permissions 1011
Creating administrator profiles 1015

Editing administrator profiles 1016
Cloning administrator profiles 1017
Deleting administrator profiles 1017
Workspace 1018
Workspace mode 1019
Workflow mode 1026
Workflow sessions 1030
Install and unlock setting for Workspace mode 1036
Authentication 1037
Public Key Infrastructure 1037
Managing remote authentication servers 1039
LDAP servers 1040
RADIUS servers 1042
TACACS+ servers 1044
Remote authentication server groups 1045
SAML admin authentication 1046
FortiCloud SSO admin authentication 1049
Global administration settings 1051
Password policy 1054
Enhanced administrator password security 1054
Password lockout and retry attempts 1057
GUI language 1058
Idle timeout 1058
Security Fabric authorization information for FortiOS 1059
Control administrative access with a local-in policy 1059
Multi-factor authentication 1060
Multi-factor authentication with FortiAuthenticator 1060
Multi-factor authentication with FortiToken Cloud 1064
High Availability 1067
Synchronizing the FortiManager configuration and HA heartbeat 1068
If the primary or a backup unit fails 1069
FortiManager HA cluster startup steps 1069
Configuring HA options 1070
General FortiManager HA configuration steps 1073
Configuring HA using manual failover mode 1073
Configuring geo-redundant HA with VRRP failover 1075
Configuring geo-redundant HA with VRRP failover with NAT 1079
Certificate best practices for FortiManager HA with VRRP 1083
Monitoring HA status 1087
Upgrading the FortiManager firmware for an operating cluster 1088
Appendix A - Supported RFC Notes 1089
Appendix B - Policy ID support 1091
Appendix C - Re-establishing the FGFM tunnel after VM license migration 1092
FGFM connection established through FortiManager 1092
FGFM connection established through FortiGate 1093

Appendix D - FortiManager Ansible Collection documentation **1095**

Change Log

Date	Change Description
2026-05-07	Initial release.

Setting up FortiManager

This chapter describes how to connect to the GUI for FortiManager and configure FortiManager. It also provides an overview of adding devices to FortiManager as well as configuring and monitoring managed device. Some security considerations are included as well as an introduction to the GUI and instructions for restarting and shutting down FortiManager units.



After you configure IP addresses and administrator accounts for the FortiManager unit, you should log in again using the new IP address and your new administrator account.

This section contains the following topics:

- Connecting to the GUI on page 15
- Security considerations on page 24
- GUI overview on page 33
- FortiAnalyzer Features on page 41
- Initial setup on page 43
- Restarting and shutting down on page 43

Connecting to the GUI

The FortiManager unit can be configured and managed using the GUI or the CLI. This section will step you through connecting to the unit via the GUI.



If you are connecting to the GUI for a FortiManager virtual machine (VM) for the first time, you are required to activate a license. See Activating VM licenses on page 22.

To connect to the GUI:

1. Connect the FortiManager unit to a management computer using an Ethernet cable.
2. Configure the management computer to be on the same subnet as the internal interface of the FortiManager unit:
   - IP address: `192.168.1.X`
   - Netmask: `255.255.255.0`
3. On the management computer, start a supported web browser and browse to `https://192.168.1.99`.
   The login dialog box is displayed.
4. Type admin in the *Name* field, leave the *Password* field blank, and click *Login*.
   The *FortiManager Setup* wizard is displayed.

5. Click *Begin* to start the setup process. See FortiManager Setup wizard on page 16.
   The *Later* option is available for certain steps in the wizard, allowing you to postone steps. The *Register with FortiCare* step cannot be skipped and must be completed before you can access the FortiManager appliance or VM.
6. If ADOMs are enabled, the *Select an ADOM* pane is displayed. Click an ADOM to select it.
   The FortiManager home page is displayed.
7. Click a tile to go to that pane. For example, click the *Device Manager* tile to go to the *Device Manager* pane.
   See also GUI overview on page 33.



If the network interfaces have been configured differently during installation, the URL and/or permitted administrative access protocols (such as HTTPS) may no longer be in their default state.

For information on enabling administrative access protocols and configuring IP addresses, see Configuring network interfaces on page 902.



If the URL is correct and you still cannot access the GUI, you may also need to configure static routes. For details, see Static routes on page 905.



When the system is busy during a database upgrade or rebuild, you will receive a message in the GUI log-in pane. The message will include the estimated completion time.

After logging in for the first time, you should create an administrator account for yourself and assign the *Super_User* profile to it. Then you should log into the FortiManager unit by using the new administrator account. See Managing administrator accounts on page 977 for information.

FortiManager Setup wizard

When you log in to FortiManager, the FortiManager Setup wizard is displayed to help you set up FortiManager by performing the following actions:

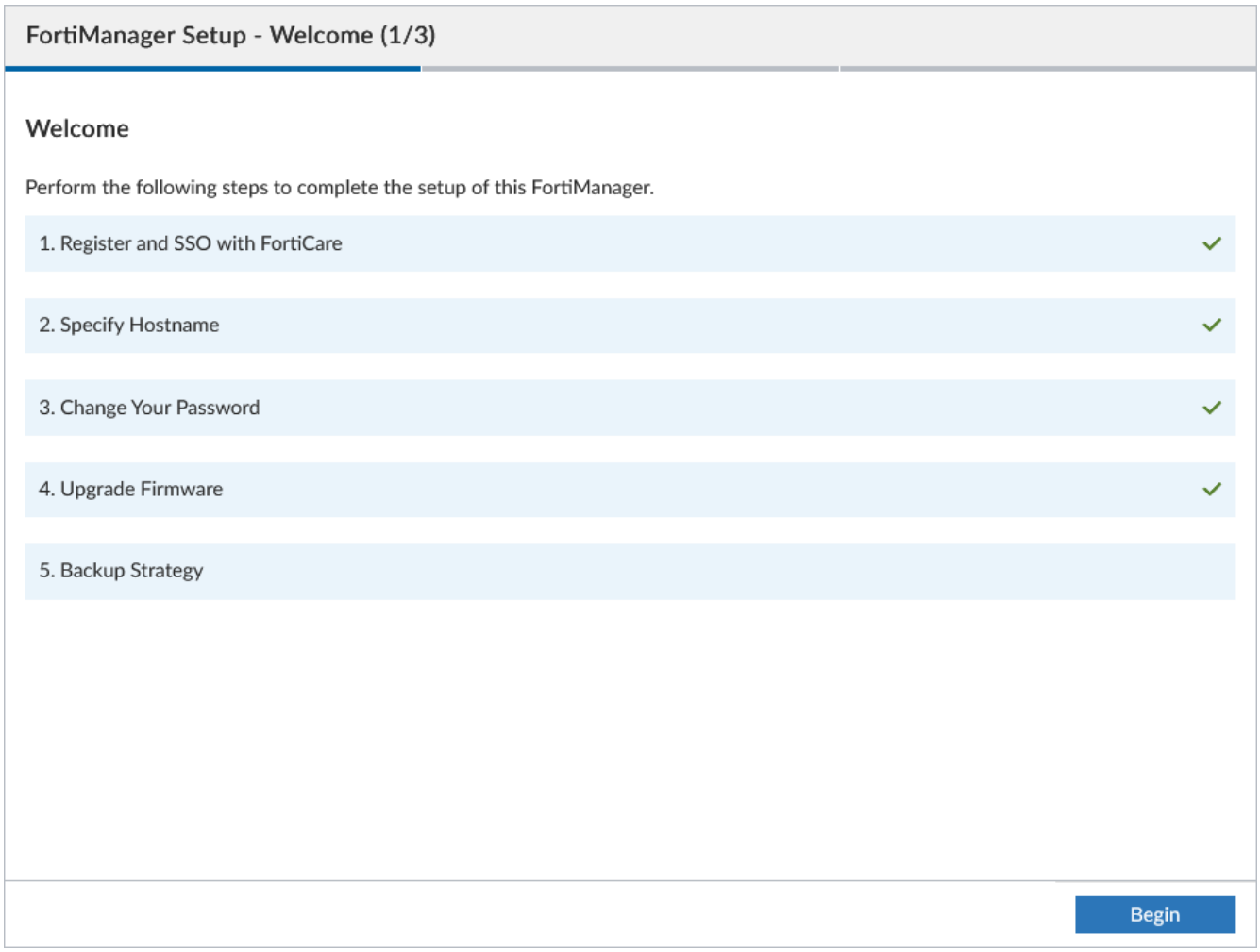
- Registering with FortiCare and enabling FortiCare single sign-on
- Specifying the hostname
- Changing your password
- Upgrading firmware (when applicable)

You can choose whether to complete the wizard now or later.



The FortiManager Setup wizard requires that you complete the *Register with FortiCare* step before you can access the FortiManager appliance or VM.

When actions are complete, a green checkmark displays beside them in the wizard, and the wizard no longer displays after you log in to FortiManager.

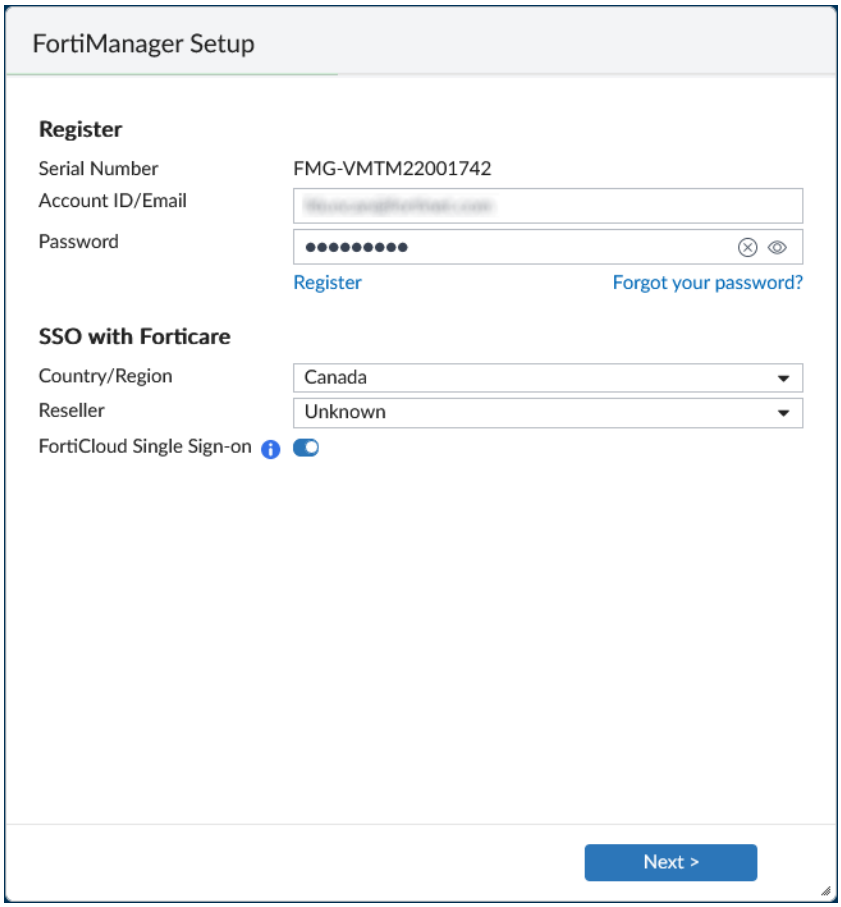


This topic describes how to use the *FortiManager Setup* wizard.

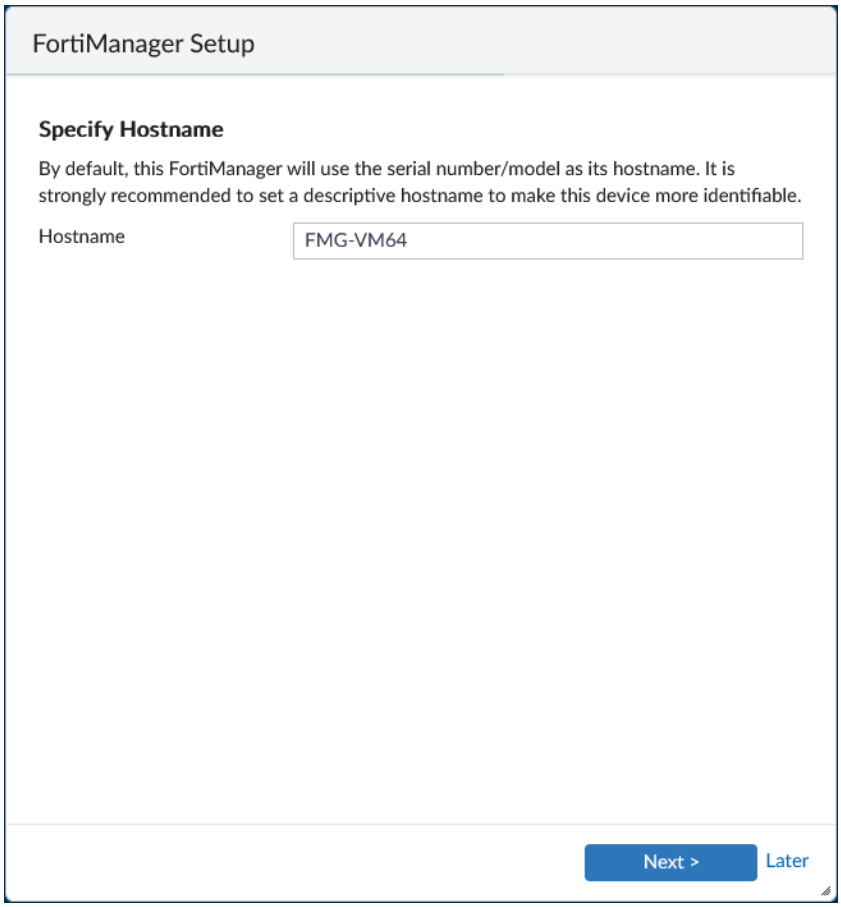
To use the FortiManager setup wizard:

1. Log in to FortiManager.
   The *FortiManager Setup* dialog box is displayed.
2. Click *Begin* to start the setup process now.
   Alternately, click *Later* to postpone the setup tasks. Some tasks cannot be postponed.
3. When prompted, register with FortiCare and enable FortiCare single sign-on. You must complete the *Register with FortiCare* step before you can access the FortiManager appliance or VM.

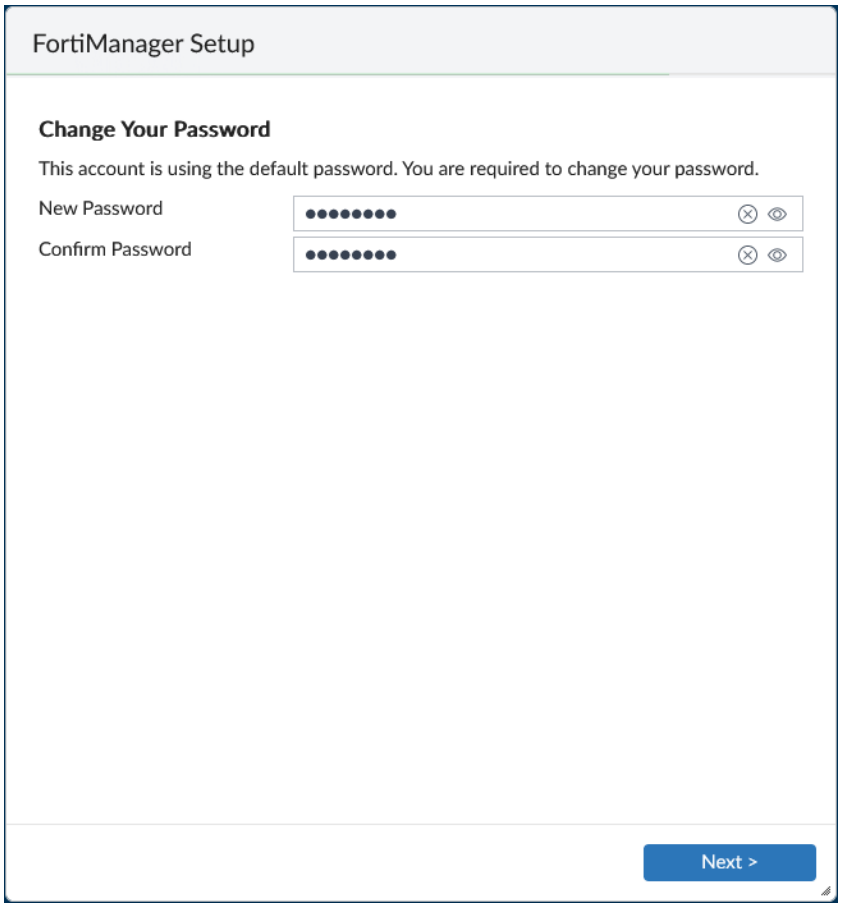
When using FortiManager in an air-gapped environment, you must manually import your *Entitlement File*. See Licensing in an air-gap environment on page 819.



4. When prompted, specify the hostname.

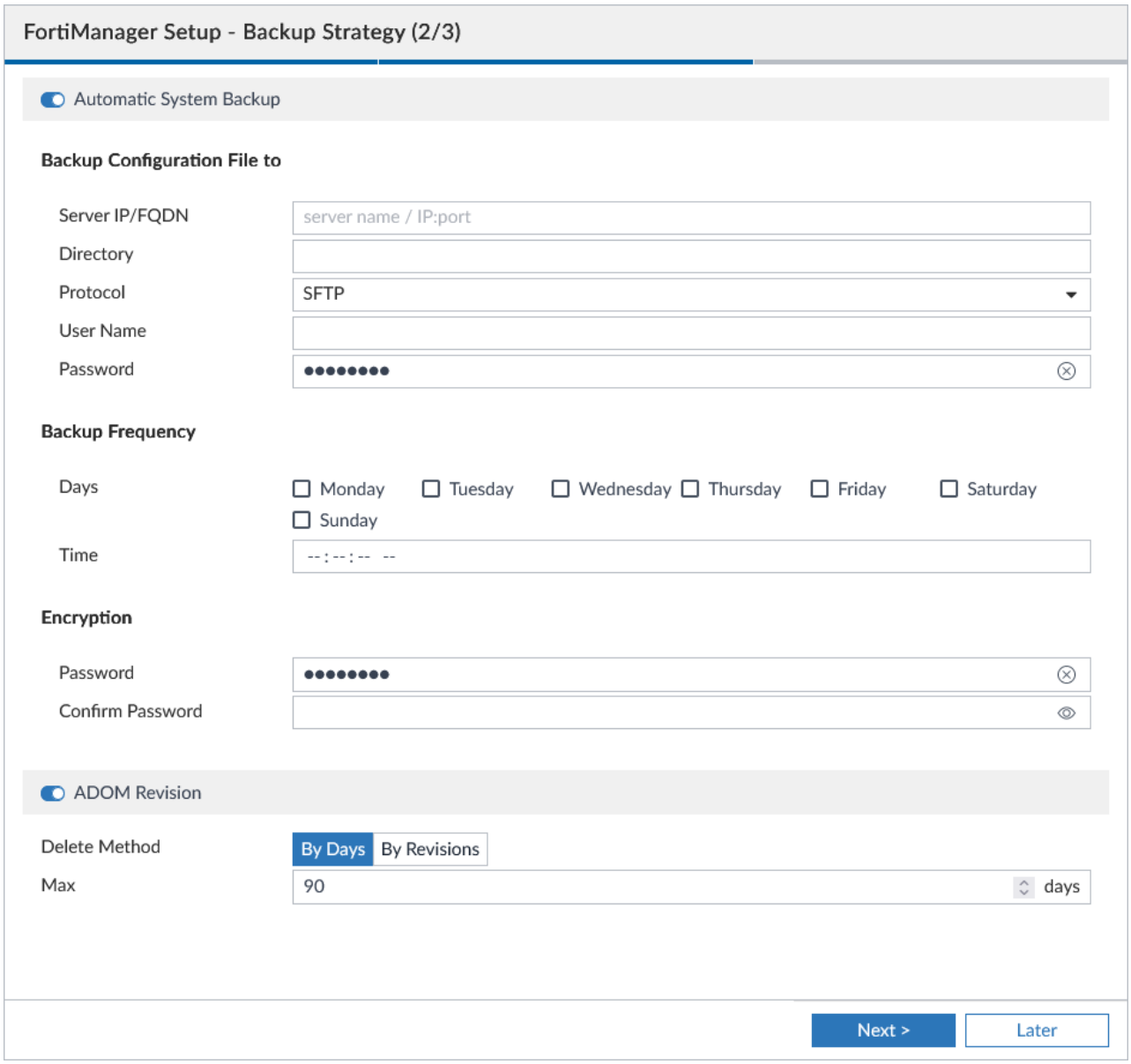


5. In the *Hostname* box, type a hostname.
6. Click *Next*.
7. When prompted, change your password.



a. In the *New Password* box, type the new password.
b. In the *Confirm Password* box, type the new password again.
c. Click *Next*.

8. When a new firmware version is available for your device on FortiGuard, the *Upgrade Firmware* option in the wizard indicates that a new version is available, and you can click *Next* to upgrade to the new firmware, or *Later* to upgrade later.
9. Configuration of a backup strategy is recommended as part of the initial configuration of your FortiManager. When prompted, you can optionally configure your backup settings.



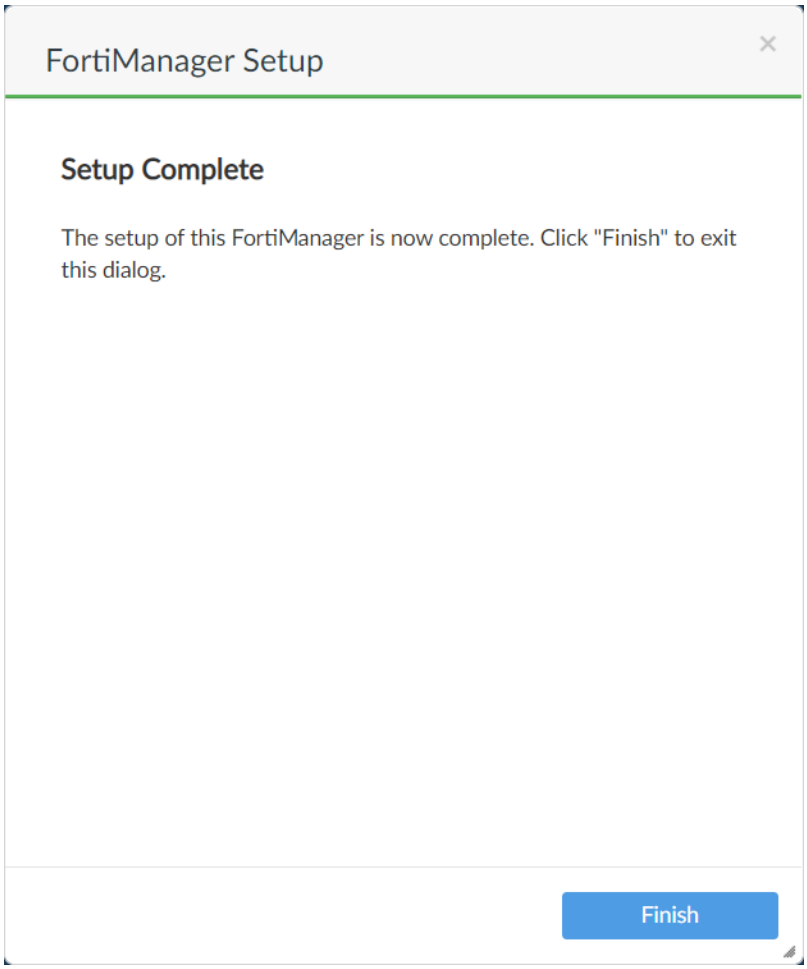
a. *Automatic System Backup* is enabled by default. Configure the following to specify your backup settings, or disable automatic backups.

- In *Backup Configuration File to*, configure where the backup file will be sent.
- In *Backup Frequency*, select when the day(s) and time for the backup to be performed.
- In *Encryption*, set an encryption password.

b. Optionally, enable *ADOM Revision* and configure the following:

- In *Delete Method*, select *By Days* or *By Revisions*.
- In *Max*, specify the maximum number of days or revisions to keep. The default value for *By Days* is `90` and *By Revisions* is `120`.

10. Complete the setup by clicking *Finish*.



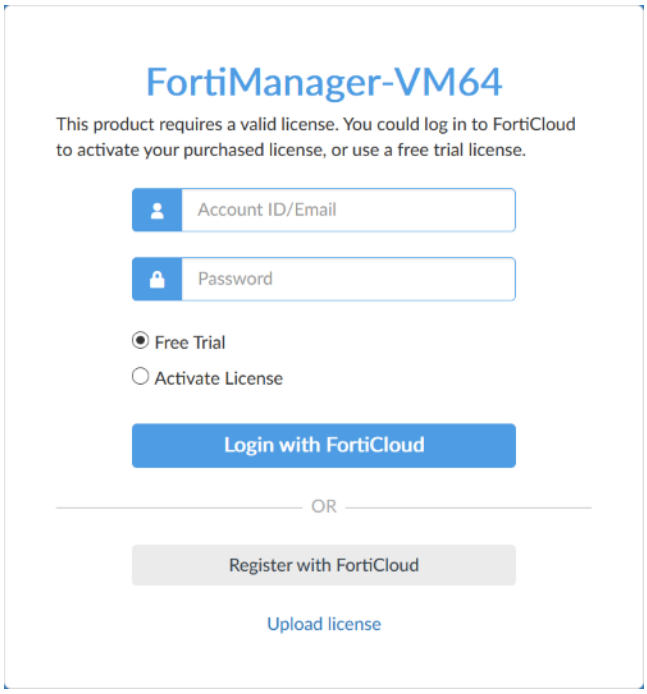
You are logged in to FortiManager.

Activating VM licenses

If you are logging in to a FortiManager VM for the first time by using the GUI, you are required to activate a purchased license or activate a trial license for the VM.

To activate a license for FortiManager VM:

1. On the management computer, start a supported web browser and browse to `https://<ip address>` for the FortiManager VM.
   The login dialog displays.



2. Take one of the following actions:

Action	Description
Free Trial	If a valid license is not associated with your FortiCloud account, you can start a free trial license. 1. In the *Account ID/Email* field, enter the account ID or email for your FortiCloud account. 2. In the *Password* field, enter the password for your FortiCloud account. 3. Select *Free Trial*, and then click *Login with FortiCloud*. FortiManager connects to FortiCloud to get the trial license. The system will restart to apply the trial license. 4. Read and accept the license agreement. For more information, see the *FortiManager VM Trial License Guide*.
Activate License	If you have a license certificate, you can activate the license using the registration code. 1. In the *Account ID/Email* field, enter the account ID or email for your FortiCloud account. 2. In the *Password* field, enter the password for your FortiCloud account. 3. Select *Activate License*, and then click *Login with FortiCloud*. FortiManager connects to FortiCloud, and the license agreement is displayed. 4. In the *Registration Code* field, enter the registration code included in your license certificate. 5. In the *IP Address* field, enter the static IP address used for the FortiManager VM. 6. Read and accept the license agreement.

Action	Description
	For more information, see the FortiCloud Services Asset Management Admin Guide in the Fortinet Document Library.
Register with FortiCloud	If you do not have a FortiCloud account, you can create one. 1. Click *Register with FortiCloud*. 2. Follow steps to create a new FortiCloud account. For more information, see the FortiCloud Account User Guide in the Fortinet Document Library. 3. Once created, you can proceed to activate a license or a free trial for the FortiManager VM.
Upload License	If you have the license file (.lic), you can upload the license. 1. Click *Upload License*. 2. Click *Browse* to upload the license file, or drag it onto the field. 3. Click *Upload*. After the license file is uploaded, the system will restart to verify it. This may take a few moments.  To download the license file, go to the Fortinet Technical Support site (https://support.fortinet.com/), and use your FortiCloud credentials to log in. Go to *Asset* > *Manage/View Products*, then click the product serial number. For more information, see the FortiCloud Services Asset Management Admin Guide in the Fortinet Document Library. If you are using this method to license the device in an air-gap environment, see Licensing in an air-gap environment on page 819

Security considerations

You can take steps to prevent unauthorized access and restrict access to the GUI. This section includes the following information:

- Restricting GUI access by trusted host on page 24
- Trusted platform module support on page 25
- Self-encrypting drives on page 26
- UEFI secure boot on page 30
- Other security considerations on page 32

Restricting GUI access by trusted host

To prevent unauthorized access to the GUI you can configure administrator accounts with trusted hosts. With trusted hosts configured, the administrator user can only log into the GUI when working on a computer with the

trusted host as defined in the administrator account. You can configure up to ten trusted hosts per administrator account. See Administrators on page 976 for more details.

Trusted platform module support

On supported FortiManager hardware devices, the Trusted Platform Module (TPM) is used to protect system against malicious attacks.

The dedicated module hardens the FortiManager by storing your `master-encryption-password` which is created when the private data encryption feature is enabled. For more information about which models feature TPM support, see the FortiManager Data Sheet.

By default, the TPM is disabled. To enable it, you must enable `private-data-encryption` and set the 32 hexadecimal digit `master-encryption-password`.

When private data encryption is enabled, the `master-encryption-password` is used to generate a primary key which encrypts and protects the individual passwords stored on the FortiManager (for example, FortiManager Admin passwords, HA passwords, SNMP passwords, and others). These individual passwords are not stored within the TPM themselves.

The primary key is never displayed in the FortiManager backup file or the system CLI, thereby obscuring the information and leaving the encrypted information in the TPM.



The TPM module does **not** encrypt the FortiManager disk drive or protect sensitive data contained in managed FortiGate configurations that are stored in FortiManager databases.

Configuration backups and migrations

The primary key binds the encrypted backup file to a specific FortiManager unit and never leaves the TPM. When backing up the configuration, the TPM uses the key to encrypt the master-encryption-password in the FortiManager backup file. When restoring a configuration that includes a TPM protected master-encryption-password:

- If TPM is enabled but has a different master-encryption-password than the FortiManager backup file, then the configuration cannot be restored.
- If TPM is enabled and the master-encryption-password is the same in the FortiManager backup file, then the configuration can be restored.

For information on backing up and restoring the configuration, see Backing up the system on page 71 and Restoring the configuration on page 74.

The master-encryption-password is also required when migrating the configuration, regardless if TPM is available on the other FortiManager model. For more information, see

Migrating the configuration on page 75.

To check if your FortiManager device has a TPM:

Enter the following command in the FortiManager CLI:

```
diagnose hardware info
```

The output in the CLI includes `### TPM info`, which displays if the TPM is detected (enabled), not detected (disabled), or not available.

To enable TPM and input the master-encryption-password:

Enter the following command in the FortiManager CLI:

```
config system global
   set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
********************************
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
********************************
Your private data encryption key is accepted.
```

Self-encrypting drives

Self-encrypting drives (SED) are supported for the following models:

- FortiManager-410G
- FortiManager-1000G
- FortiManager-3100G

The following type of key is supported for SED in FortiManager:

- **Encryption key**: This key can only be changed/created by the user. Exercise caution when changing the encryption key because all of the data previously written to the drive will now be read and decrypted using the new key; therefore, it will become unrecoverable if the user forgets the new key during restoration. However, this is an effective technique for rendering data on the disk unusable and unreadable. It is referred to as an auto-lock feature, which is useful if a drive has to be repurposed (used in a different application where the data is neither required nor wanted) or scrapped.

The SED features are only available using the CLI, not the GUI.

Auto-lock feature

To protect the disk's contents, assign the SED encryption key after RAID has been setup. The disk's contents are protected if plugged into a system unless the encryption key is known and the system supports a similar RAID controller.

To use the auto-lock feature:

1. After RAID setup, enter the following command in the FortiManager CLI:
   ```
   diagnose system disk sed {sed-key}
   ```
   The key requires 8-32 characters, and it must include upper case, lower case, number, and special character (excluding '\).



If a foreign SED disk is installed, this disk will be unavailable due to auto-lock feature.

Cryptographic erase

To quickly and securely dispose of disks, you can format the drives from the CLI and then use the auto-lock feature.

To complete a cryptographic erase:

1. In the FortiManager CLI, enter the following command:
   ```
   execute format disk {raid-level}
   ```
2. In the FortiManager CLI, apply the auto-lock by entering the following command:
   ```
   diagnose system disk sed {sed-key}
   ```

To change the SED key:

1. When the SED key has been set, it can be changed by entering the following command in the FortiManager CLI:
   ```
   diagnose system disk sed {new-sed-key} {old-sed-key}
   ```

Examples

SED feature disabled

```
diagnose system raid status
Storcli RAID:
RAID Level: Raid-50
RAID Status: OK
RAID Size: 52156GB
File System: ext4 51337GB
SED Encryption: Disabled
Groups: 2

Disk  1:           OK     3724GB    Group-1
Disk  2:           OK     3724GB    Group-1
Disk  3:           OK     3724GB    Group-1
```

If there are non-SED disks, they are displayed in the output. For example:

```
diagnose system raid status
Storcli RAID:
RAID Level: Raid-50
RAID Status: OK
RAID Size: 52156GB
File System: ext4 51337GB
SED Encryption: Disabled
```

```
Groups: 2

Disk  1:           OK     3724GB    Group-1
Disk  2:           OK     3724GB    Group-1   non-SED
Disk  3:           OK     3724GB    Group-1
```

SED feature enabled

1. Use the following command to provide the SED key:
   `diagnose system raid sed {sed-key}`

Variable	Description
sed-key	SED encryption key. 8-32 chars, must include upper case, lower case, number and special chars (exclude '\).

2. Use the following command to verify SED encryption status:

```
diagnose system raid status
Storcli RAID:
RAID Level: Raid-50
RAID Status: OK
RAID Size: 22353GB
File System: ext4 22001GB
SED Encryption: Enabled
Groups: 2

Disk  1:           OK     3724GB    Group-1
Disk  2:           OK     3724GB    Group-1
Disk  3:           OK     3724GB    Group-1
Disk  4:           OK     3724GB    Group-1
Disk  5:           OK     3724GB    Group-2
```

Changing the SED key

1. In this example, the SED key is initially set to `Qq1!Qq1!` using the following command:
   `diagnose system raid sed {sed-key}`
   For example:

```
diagnose system raid sed Qq1!Qq1!
OK

diagnose system raid status
Storcli RAID:
RAID Level: Raid-50
RAID Status: OK
RAID Size: 21.83T
File System: ext4 21.49T
SED Encryption: Enabled
```

2. The SED key is later changed to `Ee3#Ee3#` using the following command:
   `diagnose system raid sed {new-sed-key} {old-sed-key}`

For example:

```
diagnose system raid sed Ee3#Ee3# Qq1!Qq1!
OK

diagnose system raid status
Storcli RAID:
RAID Level: Raid-50
RAID Status: OK
RAID Size: 21.83T
File System: ext4 21.49T
SED Encryption: Enabled
```

Working with SED-based systems

To replace an SED disk:

You can replace disks that supports SED feature, regardless of brand, however it's optimal to use the same specification of hard drive in the existing array. The new disk will be automatically rebuilt by the system and it will have the same SED key used by the existing system. This will be transparent for the user.

To reformat after an SED-enabled RAID failure:

If an SED-enabled RAID failure occurs, formatting the drives will effectively clear the SED key. Thus, the user can assign an SED key. For example, see below.

```
FMG-410G # diagnose system raid status
Storcli RAID:
RAID Level: Raid-50
RAID Status: Failed
RAID Size: 22353GB
File System: ext4 22001GB
SED Encryption: Enabled
Groups: 2

Disk  1:           OK     3724GB    Group-1
Disk  2:           OK     3724GB    Group-1
Disk  3:           OK     3724GB    Group-1
Disk  4:           OK     3724GB    Group-1
Disk  5:           OK     3724GB    Group-2
Disk  6:           OK     3724GB    Group-2
Disk  7:       Unused     3724GB
Disk  8:       Unused     3724GB    Group-2

FMG-410G # execute format disk 50
This operation will format hard disk to ext4 filesystem.
Do you want to continue? (y/n)y

Resetting ...

login as: admin
```

```
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server

FMG-410G # diagnose system raid status
Storcli RAID:
RAID Level: Raid-50
RAID Status: OK
RAID Size: 22353GB
File System: ext4 22001GB
SED Encryption: Disabled
Groups: 2

Disk  1:           OK     3724GB    Group-1
Disk  2:           OK     3724GB    Group-1
Disk  3:           OK     3724GB    Group-1
Disk  4:           OK     3724GB    Group-1
Disk  5:           OK     3724GB    Group-2
Disk  6:           OK     3724GB    Group-2
Disk  7:           OK     3724GB    Group-2
Disk  8:           OK     3724GB    Group-2
```

To move SED-enabled disks to a new physical chassis:

In situations where SED-enabled disks need to be moved (re-homed) to a new physical chassis, the process will require additional steps. See below.

1. On the target unit, install the same build as the source unit. Install SED capable drives and setup the RAID similar to that of the source unit, and then enable SED using the same key as that of the source unit.
2. Shutdown both units and remove the drives from their respective chassis.
3. Move the source drives and install them to the target chassis.

UEFI secure boot

The BIOS-level signature and integrity checking enforces each FortiManager GA firmware image, AV engine file, and IPS engine file to be dually-signed by the Fortinet CA and a third-party CA. The BIOS verifies that each file matches their secure hash as indicated by their certificates. Users are warned when there is a failed integrity check, and the system may be prevented from booting depending on the severity and the BIOS security level.

Signature checking occurs when the FortiManager firmware, AV, and IPS engine files are uploaded. This allows the FortiManager to warn users of potential risks involved with uploading an unauthenticated file.

The outcome of the signature and integrity check depends on the security level configured in BIOS and the certificate authority that signed the file.

The following table summarizes the use cases and the potential outcome based on the security level.

Use case	Certificate signed by		Outcome based on security level		
	Fortinet CA	Third-party CA	Level 2	Level 1	Level 0
GA-Certified (GA firmware, Beta firmware, Top3 final builds)	Yes	Yes	Accept	Accept	Accept
Non-GA certified (Special builds: Top3 and NPI quick builds)	Yes	No	Warning	Accept	Accept
Interim and Dev builds, or unknown build	No	Yes or No	Reject	Warning	Accept

The FortiManager secure boot feature supports the following security levels:

- Level 2: in order to operate normally, FortiManager requires all file signatures to match their secure checksums as indicated on both Fortinet and third-party CA signed certificates.
  - If a file has a Fortinet CA signed certificate but no third-party signed certificates, then FortiManager can still run but displays a warning in the GUI and CLI.
  - If a file has no valid certificate signed by the Fortinet CA, then FortiManager is not allowed to run.
- Level 1: in order to operate normally, FortiManager only requires all file signatures to match their secure checksums as indicated on the Fortinet CA signed certificate.
  - If a file has no valid certificate signed by the Fortinet CA, then FortiManager can still run but displays a warning in the GUI and CLI.
- Level 0 (not recommended): FortiManager does not perform code verification.

On FortiManager without supported BIOS security levels, the device acts like security level 1. For example, on a FortiManager-VM that does not have BIOS, the security level is defaulted to level 1.

Models that support BIOS security levels:

The following FortiManager models support setting the security level in the BIOS as of the release of FortiManager 7.4.11.

- FMG-410G
- FMG-1000G
- FMG-3100G

To verify the security level:

```
# get system status
Version: vx.x.x-buildxxxx xxxxxx (GA)
Secure Boot: Enabled
Security Level: 2
Image Signature: Image is GA Certified
```

To change the security level:

```
Version 2.20.1271. Copyright (C) 2023 American Megatrends, Inc.
BIOS Date: 06/30/2023 Ver: C1820J0B
Press <DEL> or <ESC> to enter setup.
FortiBootLoader

Loading Device Drivers

FortiAnalyzer-410G (21:52-07.17.2023)
Ver:00030003

Serial number:FMG*************
Total RAM: 32768MB
Boot up, boot device capacity: 15272MB.
Press any key to display configuration menu...   <<============= Press any key when this message
is displayed
......
[C]:  Configure TFTP parameters.
[R]:  Review TFTP parameters.
[T]:  Initiate TFTP firmware transfer.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[I]:  System configuration and information.      <<============= Choose System configuration and
information
[Q]:  Quit menu and continue to boot.
[H]:  Display this list of options.

Enter C,R,T,F,B,I,Q,or H:
[T]:  Set menu timeout.
[U]:  Set security level.
[Q]:  Quit menu and continue to boot.
[H]:  Display this list of options.

Enter T,U,Q,or H:
[0]:  Level 0
[1]:  Level 1
[2]:  Level 2
Enter security level setting [1]:2
```



Serial console access to the device is required in order to change the security level settings.

Other security considerations

Other security consideration for restricting access to the FortiManager GUI include the following:

- Configure administrator accounts using a complex passphrase for local accounts
- Configure administrator accounts using RADIUS, LDAP, TACACS+, or PKI

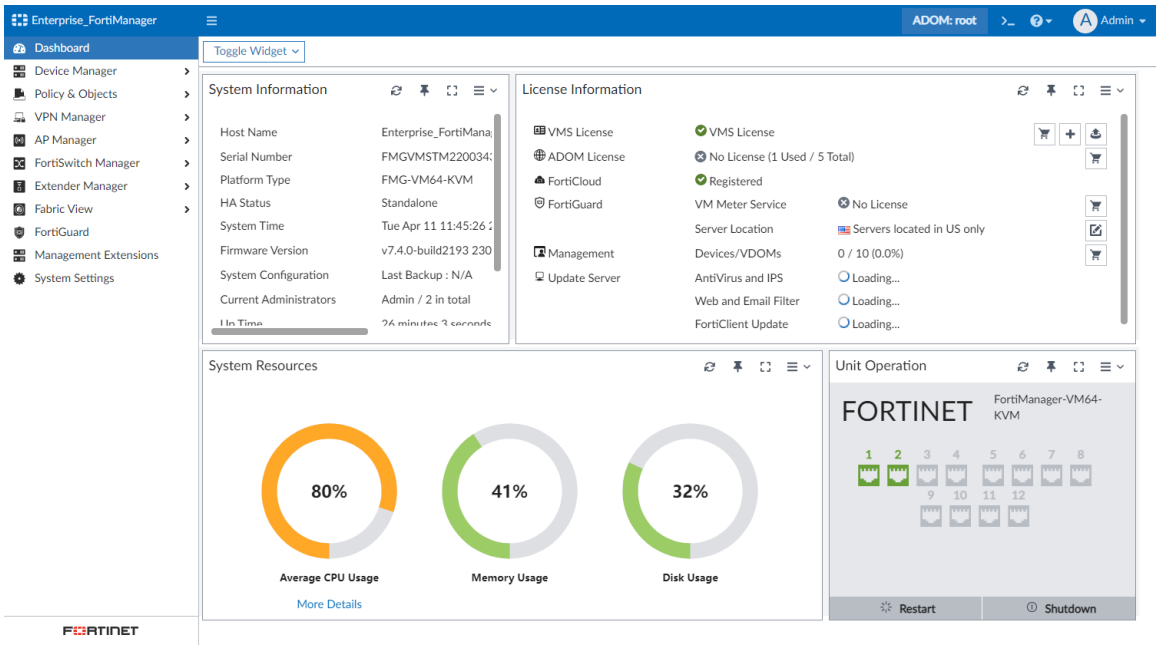
- Configure the administrator profile to only allow read/write permission as required and restrict access using read-only or no permission to settings which are not applicable to that administrator
- Configure the administrator account to only allow access to specific ADOMs as required
- Configure the administrator account to only allow access to specific policy packages as required.

When setting up FortiManager for the first time or after a factory reset, the password cannot be left blank. You are required to set a password when the *admin* user tries to log in to FortiManager from GUI or CLI for the first time. This is applicable to a hardware device as well as a VM. This is to ensure that administrators do not forget to set a password when setting up FortiManager for the first time.

After the initial setup, you can set a blank password from *System Settings* > *Administrators*.

GUI overview

When you log into the FortiManager GUI, the *Dashboard* pane is displayed. The *Dashboard* contains widgets that provide performance and status information. For more information about the *Dashboard*, see Dashboard on page 61



Use the navigation menu on the left to open another pane. The available panes vary depending on the privileges of the current user.

Device Manager	Add and manage devices and VDOMs. Create and assign scripts and provisioning templates. You can also access the SD-WAN monitor and VPN monitor. See Device Manager on page 88.

Policy & Objects	Configure policy packages and objects. See Policy & Objects on page 407.
VPN Manager	Configure and manage VPN connections. You can create VPN topologies and managed/external gateways. See VPN Manager on page 650.
AP Manager	Configure and manage FortiAP access points. For more information, see AP Manager on page 580.
FortiSwitch Manager	Configure and manage FortiSwitch devices. See FortiSwitch Manager on page 838.
Extender Manager	Configure and manage FortiExtenders. See Extender Manager on page 889.
Log View	View logs for managed devices. You can display, download, import, and delete logs on this page. You can also define custom views and create log groups. This pane is only available when FortiAnalyzer features are enabled.
Fabric View	Configure fabric connectors and view Security Fabric Ratings. See Fabric View on page 697.
Incidents & Events	Configure and view events for logging devices. This pane is only available when FortiAnalyzer features are enabled.
Reports	Generate reports. You can also configure report templates, schedules, and output profiles, and manage charts and datasets. This pane is only available when FortiAnalyzer features are enabled.
FortiGuard	Manage communication between devices and the FortiManager using the FortiGuard protocol. See FortiGuard on page 787.
System Settings	Configure system settings such as network interfaces, administrators, system time, server settings, and others. You can also perform maintenance and firmware operations. See System Settings on page 900.

The banner at the top of the screen is available in every pane.

The following options are available in the banner:

Menu	Click to toggle the visibility of the navigation menu on the left.
HA status	If HA is enabled, the status is shown.
ADOM	If ADOMs are enabled, the required ADOM can be selected from the dropdown list. If enabled, ADOMs can also be locked or unlocked. The ADOMs available from the ADOM menu will vary depending on the privileges of the current user.
CLI Console	Open the CLI console to configure the FortiManager unit using CLI commands directly from the GUI, without making a separate SSH, or local console connection to access the CLI. For more information, see Using the CLI console on page 38. **Note:** The *CLI Console* requires that your web browser support JavaScript.

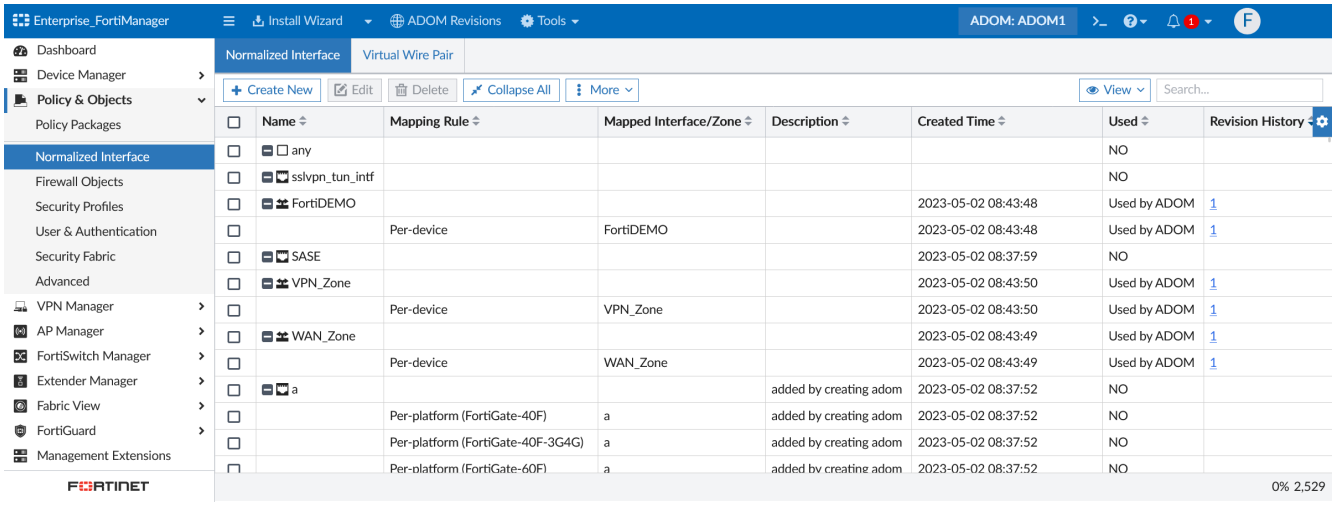
Online Help	Click to open the FortiManager online help dropdown which contains the following options: **Relevant Documentation**: Opens related online help topics on the Fortinet Document Library. This option is context-sensitive, so it will open to the relevant documentation for the pane you are in. **Video Tutorials**: Opens the Fortinet Video Library. **Release Notes**: Opens the FortiManager's Release Notes for the current version. **FortiAnswers**: Opens the Fortinet Community. **FortiCare Debug Report**: Runs the `execute tac report` CLI command and downloads a local copy of the report.
Notifications	Click to display a list of notifications. Select a notification from the list to take action on the issue.
admin	From this dropdown, you can: • view the current firmware build of your FortiManager device. • upgrade the firmware. • open the *Process Monitor*. • change your password. • update your profile information, including the avatar and theme. • log out of the GUI.

Panes

In general, each pane four primary parts: the banner, toolbar, tree menu, and content pane.

Banner	Along the top of the page. The banner includes the device name (next to the Fortinet logo) and options to open/close side menu, switch ADOMs (when enabled), open the CLI console, view notifications, view help content, and access the admin menu. In some panes, further options will be included in the banner.
Tree menu	On the left side of the screen. In some panes, further navigation will be available as tabs along the top of the content pane. This additional horizontal menu can be toggled to a vertical menu, if preferred. Use this navigation menu to open panes in the GUI.

Content pane	Contains widgets, lists, configuration options, or other information, depending on the pane, menu, or options that are selected. Most management tasks are handled in the content pane.
Toolbar	Directly above the content pane. The toolbar includes options for managing content in the content pane, such as *Create New* and *Delete*.



Color themes

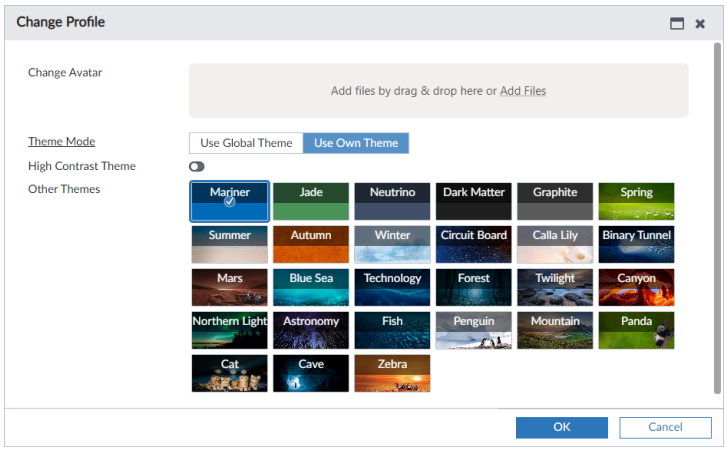
You can choose a color theme for the FortiManager GUI. For example, you can choose a color or image such as jade, summer, or autumn.

By default, all users are assigned the global color theme. To change the global color theme, see Global administration settings on page 1051.

To change your color theme:

1. In the banner, open the dropdown for your account and click *Change Profile*.
   The *Change Profile* dialog displays.
2. In the *Theme Mode* field, select *Use Own Theme*.

3. Enable the *High Contrast Theme* or select a color them from the list.



Side menu open or closed

After you choose a tile, such as *Device Manager*, you can close the side menu and view only the content pane. Alternately you can view both the side menu and the content pane.

In the banner, click the *Open/close side menu* button to change between the views.

Switching between ADOMs

When ADOMs are enabled, you can move between ADOMs by selecting an ADOM from the *ADOM* button in the banner. You are also prompted to select an ADOM when you log in.



ADOM access is controlled by administrator accounts and the profile assigned to the administrator account. Depending on your account privileges, you might not have access to all ADOMs. See Managing administrator accounts on page 977 for more information.

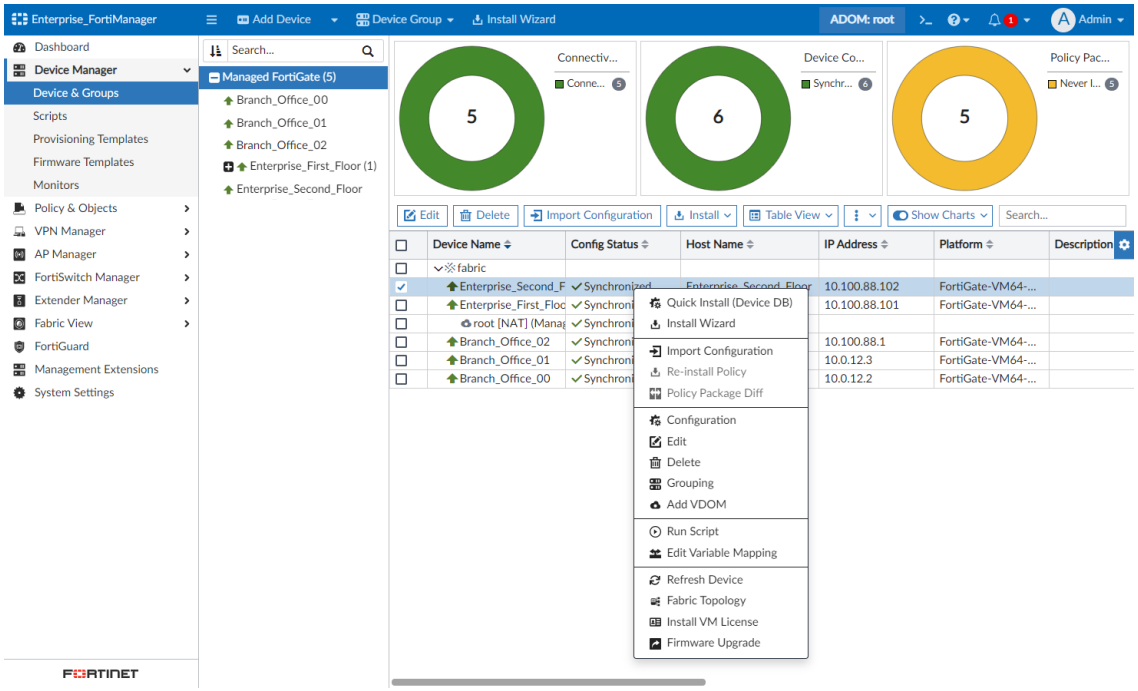
To switch ADOMs:

1. In the banner, click the *ADOM* button.
   The *Select an ADOM* diaolog displays.
2. Click the ADOM to switch to.
   The ADOM you are in displays on the *ADOM* button in the banner.

Using the right-click menu

Options are sometimes available using the right-click menu. Right-click an item in the content pane to display the menu of available options. This menu often includes actions available in the toolbar, as well as some unique actions depending on the pane and its content.

In the following example on the *Device Manager* pane, you can right-click a device in the content pane, and select many options, such as *Quick Install (Device DB)*, *Install Wizard*, *Edit*, *Run Script*, and more.



Using the CLI console

The CLI console is a terminal window that enables you to configure the FortiManager unit using CLI commands directly from the GUI, without making a separate SSH, or local console connection to access the CLI.

When using the CLI console, you are logged in with the same administrator account that you used to access the GUI. You can enter commands by typing them, or you can copy and paste commands into or out of the console.

For more information about using the CLI, see the *FortiManager CLI Reference* on the Fortinet Documents Library.



The *CLI Console* requires that your web browser support JavaScript.

To open the CLI console in the GUI, click the CLI Console icon (>_) in the banner.

You can perform the following actions from the top of the CLI Console:

Option	Description
Clear Console	Clear previous text in the console.
Copy History to Clipboard	Copy all text in the console.

Option	Description
Record CLI Commands	Begin recording the next commands entered in the console; click again to finish recording. The commands and outputs from the recording are copied to the clipboard.
Download History	Download all text in the console as a text file.
Reconnect Console	Reconnect to the console, clearing the previous text in the console and returning to the initial prompt.
Run CLI Script	Drag and drop or select a script file to run in the CLI.
Detach	Open the console in a new tab.
CLI of Current Page (if available)	Go to the commands for the current page of the GUI, if they are available.
Minimize	Minimize the console in the GUI.
Full screen	Expand the console to full screen within the GUI.
Close	Close the console.

Avatars

When FortiClient sends logs to FortiManager with FortiAnalyzer features enabled, an avatar for each user can be displayed in the *Source* column in the *FortiView* and *Log View* panes. FortiManager can display an avatar when FortiClient is managed by FortiGate or FortiClient EMS with logging to FortiManager enabled.

- When FortiClient Telemetry connects to FortiGate, FortiClient sends logs (including avatars) to FortiGate, and the logs display in FortiManager under the FortiGate device as a sub-type of security.
  The avatar is synchronized from FortiGate to FortiManager by using the FortiOS REST API.
- When FortiClient Telemetry connects to FortiClient EMS, FortiClient sends logs (including avatars) directly to FortiManager, and logs display in a FortiClient ADOM.

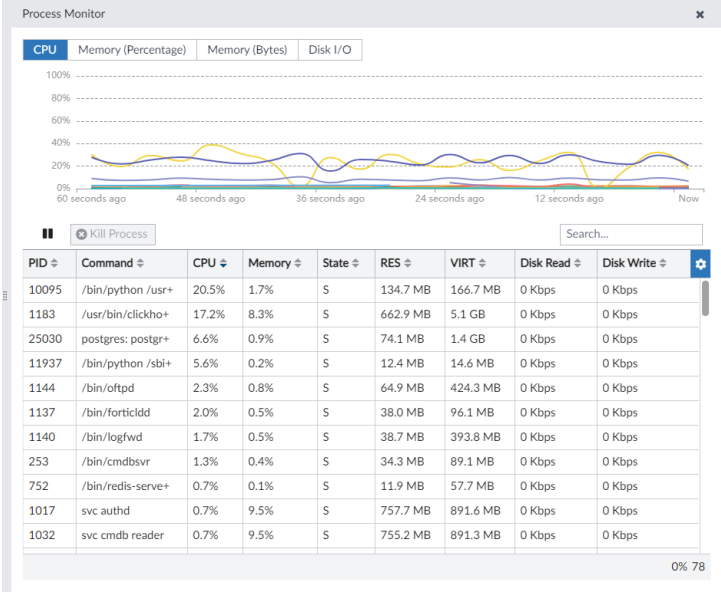
If FortiManager cannot find the defined picture, a generic, gray avatar is displayed.



You can also optionally define an avatar for FortiManager administrators. See Creating administrators on page 979.

Using the Process Monitor

The *Process Monitor* displays running processes with their CPU and memory usage as well as their disk I/O levels. Administrators can sort, filter, and terminate processes within the *Process Monitor* pane.



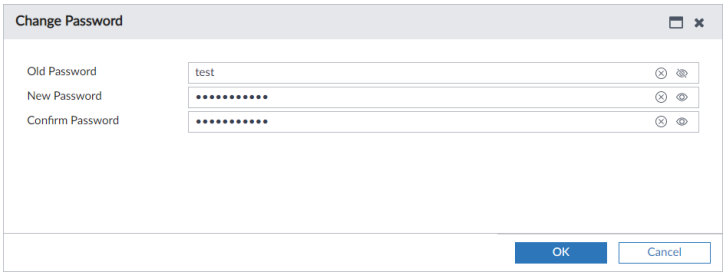
To use the Process Monitor:

1. In the banner, click *[admin_name] > Process Monitor*.
   A line chart and a table view are available in the *Process Monitor* pane. Both the chart and the table refresh automatically unless paused.
2. To change the line chart according to your needs, click *CPU*, *Memory (Percentage)*, *Memory (Bytes)*, or *Disk I/O*.
   The table view will automatically sort by the selection as well.
3. To pause the chart and table from refreshing, click the pause button.
   You can click the play button to resume the automatic refresh.
4. Use the search field to search for any field in the table view.
5. To terminate a process, select it in the table view and click *Kill Process*.

Showing and hiding passwords

In some fields, you can show and hide information by clicking the toggle icon.

For example, see the image of the *Change Password* dialog below. In this example, the *Old Password* is toggled to show the password. The other fields are toggled to hide the password.



Google Map integration

FortiManager integrates with Google Maps to provide map data for features including but not limited to the following:

- AP Manager's WiFi maps
- VPN Manager's IPsec VPN map view
- SD-WAN Monitors
- Device location in the Device Manager map view

Google Maps integration requires the following access. If this access is not available, map data will not be visible on FortiManager.

- FortiManager must have access to `https://mapserver.fortinet.com` to register and retrieve the Google Map license.
- The administrator PC must have an internet connection and be able to access to the following sites in order for the browser to be able to download and display the Google Maps and overlay:
  - `https://maps.google.com`
  - `https://maps.googleapis.com`
  - `https://fonts.googleapis.com`
  - `https://mapserver.fortinet.com`

FortiAnalyzer Features

FortiAnalyzer features can be used to view and analyze logs from devices with logging enabled that are managed by the FortiManager.

When FortiAnalyzer features are enabled by using the *System Settings* module, logs are stored on FortiManager and FortiAnalyzer features are configured on the FortiManager device. See Enable or disable FortiAnalyzer features on page 42.

When a FortiAnalyzer is added to the FortiManager, logs are stored on FortiAnalyzer and log storage settings are configured on the FortiAnalyzer device. Managed devices with logging enabled send logs to the FortiAnalyzer. The FortiManager remotely accesses logs on the FortiAnalyzer unit and displays the information. See Add FortiAnalyzer or FortiAnalyzer BigData on page 134.

When FortiAnalyzer features are enabled on FortiManager, the following modules are available:

FortiView	Enables *FortiView* and additional *Monitors*, including monitoring network traffic, WiFi security, and system performance. See the *FortiAnalyzer Administration Guide*.
Log View	View log messages from managed devices with logging enabled. You can view the traffic log, event log, or security log information. See the *FortiAnalyzer Administration Guide*.

Incidents & Events	View events from logs that you want to monitor. You can specify what log messages to display as events by configuring event handlers. See the *FortiAnalyzer Administration Guide*.
Reports	Generate reports of data from logs. See the *FortiAnalyzer Administration Guide*.

When FortiAnalyzer features are enabled, the following options are available on the *System Settings* module:

Dashboard widgets	The following widgets can be added to the dashboard: *Log Receive Monitor*, *Insert Rate vs Receive Rate*, *Log Insert Lag Time*, *Receive Rate vs Forwarding Rate*, and *Disk I/O*. The *License Information* widget will include a *Logging* section. See Dashboard on page 61.
Logging Topology	View the logging topology. See Logging Topology on page 900.
Storage Info	View and configure log storage policies. See the *FortiAnalyzer Administration Guide*. This pane is only available when ADOMs are enabled.
Device Log Settings	Configure device log file size, log rolling, and scheduled uploads to a server. As well, configure the automatic deletion of device log files, quarantined files, reports, and content archive files after a set period of time. See Device logs on page 969.

Various other settings and information will be included on the FortiManager when FortiAnalyzer features are enabled.

Enable or disable FortiAnalyzer features

If FortiAnalyzer features are enabled, you cannot add FortiAnalyzer to FortiManager. Nor can you enable FortiManager HA.

When FortiAnalyzer is added to FortiManager, FortiAnalyzer features are automatically enabled to support the managed FortiAnalyzer unit, and cannot be disabled.



Log forwarding, log fetching, and log aggregation are not supported on FortiManager, including when FortiAnalyzer features are enabled.

See Add FortiAnalyzer or FortiAnalyzer BigData on page 134 for more information.

To enable or disable the FortiAnalyzer features from the GUI:

1. Go to *Dashboard*.
2. In the *System Information* widget, click the *FortiAnalyzer Features* toggle switch.
   The FortiManager will reboot to apply the change.

To enable or disable the FortiAnalyzer features from the CLI:

1. Log in to the FortiManager CLI.
2. Enter the following commands:

```
config system global
   set faz-status {enable | disable}
end
```

Initial setup

This topic provides an overview of the tasks that you need to do to get your FortiManager up and running.

To set up FortiManager:

1. Connect to the GUI. See Connecting to the GUI on page 15.
2. Configure the RAID level, if the FortiManager unit supports RAID. See RAID Management on page 918.
3. Configure network settings. See Configuring network interfaces on page 902.
4. (Optional) Configure administrative domains. See Managing ADOMs on page 932.
5. Configure administrator accounts. See Managing administrator accounts on page 977.

Restarting and shutting down

Always use the operation options in the GUI or the CLI commands to reboot and shut down the FortiManager system to avoid potential configuration problems.

See Restart, shut down, or reset FortiManager on page 86 in System Settings on page 900.

FortiManager Key Concepts

FortiManager is an integrated platform for the centralized management of products in a Fortinet security infrastructure. FortiManager provides centralized policy-based provisioning and configuration management for FortiGate, FortiWiFi, FortiAP, and other devices. For a complete list of supported devices, see the *FortiManager 7.4.11 Release Notes*.

FortiManager recognizes Security Fabric groups of devices and lets you display the Security Fabric topology as well as view Security Fabric Ratings.

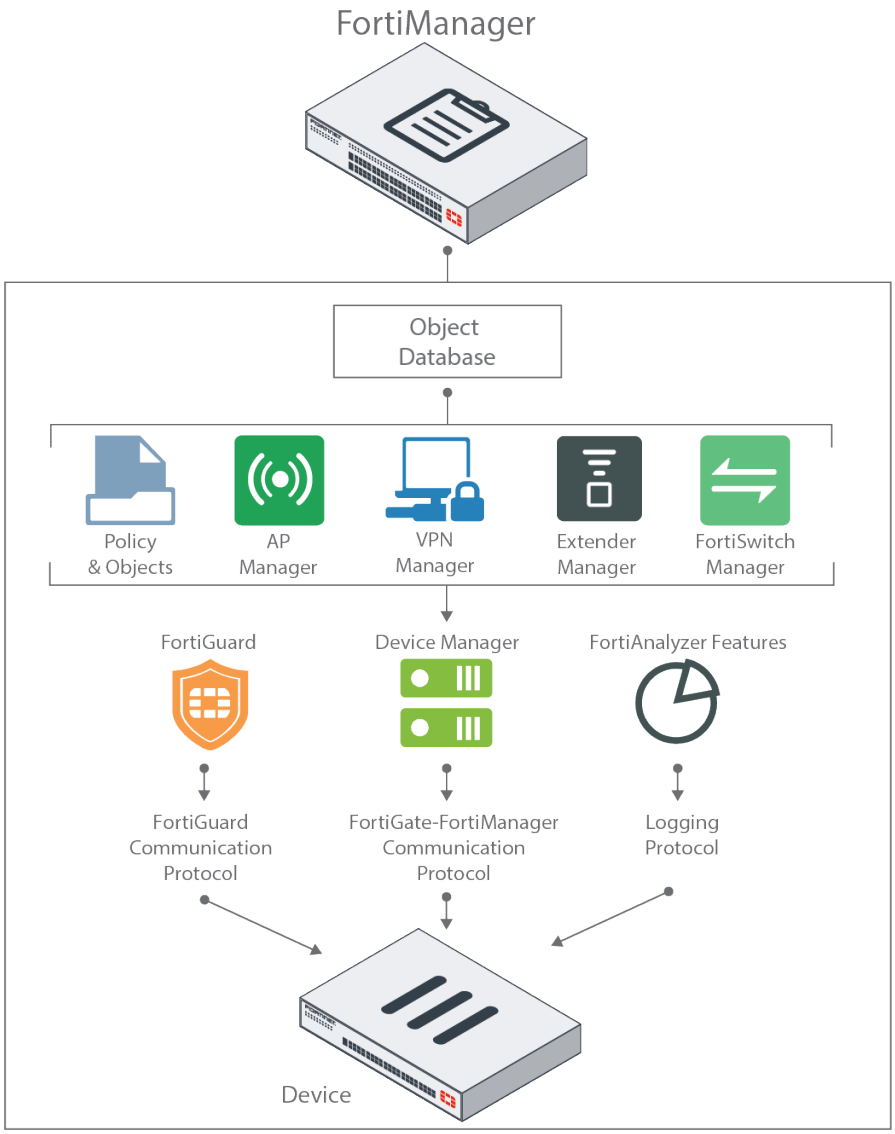
To reduce network delays and to minimize external Internet usage, a FortiManager installation can also act as an on-site FortiGuard Distribution Server (FDS) for your managed devices and FortiClient agents to download updates to their virus and attack signatures, and to use the built-in web filtering and email filter services.

You can also optionally enable the FortiAnalyzer features, which enables you to analyze logs for managed devices and generate reports.

FortiManager scales to manage 10000 or more devices and virtual domains (VDOMs) from a single FortiManager interface. It is primarily designed for medium to large enterprises and managed security service providers.

Using a FortiManager device as part of an organization's Fortinet security infrastructure can help minimize both initial deployment costs and ongoing operating expenses. It allows fast device provisioning, detailed revision tracking, and thorough auditing.

Inside FortiManager, an object database is shared by several modules, such as *Policies & Objects*, *AP Manager*, *VPN Manager*, *Extender Manager*, and *FortiSwitch Manager*, to provide policy configuration information to FortiGates. Other modules, such as *FortiGuard*, *Device Manager*, and FortiAnalyzer features, use protocols to communicate directly from FortiManager to FortiGates. This chapter describes how these components in FortiManager work together to manage FortiGates.



This section contains the following topics:

- Communication through protocols on page 45
- Configuration through Device Manager on page 47
- ADOMs and devices on page 49
- Operations on page 51
- Key features of the FortiManager system on page 59

Communication through protocols

FortiManager contains several modules that are used to configure managed devices. Some modules use their own protocol to communicate directly with managed devices, and other modules provide information to the

Device Manager module for installation to managed devices.

The following modules use protocols to directly communicate with managed devices and provide configuration information:

- FortiGuard
- FortiAnalyzer features
- Device Manager

For information about modules that provide information to *Device Manager*, see Configuration through Device Manager on page 47.

FortiGuard

FortiManager can act as a local FortiGuard server to provide FortiGuard services, such as AV engines and signatures, IPS engines and signatures, web filtering lookups, and firmware upgrades to your FortiGates.

FortiManager provides the resources by communicating with the FortiGuard Distribution Network (FDN) on a regular basis to keep the local services up to date, and providing the information to managed devices through the *FortiGuard* module. The *FortiGuard* module communicates with devices by using the FortiGuard protocol.

The *FortiGuard* module is often used to keep FortiGates up to date when FortiGates are not permitted to access the Internet.

For more information, see FortiGuard on page 787.

Device Manager

The *Device Manager* module contains all devices that are managed by FortiManager. You can create new device groups, provision and add devices, and install policy packages and device settings. The *Device Manager* module communicates with managed devices by using the FortiGate-FortiManager (FGFM) protocol. See Device Manager on page 88.

FortiAnalyzer features

When FortiAnalyzer features are enabled, the following additional modules become available in FortiManager:

- FortiView
- Log View
- Incidents & Events
- Reports

FortiAnalyzer features include tools for viewing and analyzing log messages, and the feature communicates with managed devices by using the logging protocol.

For details on each of these modules, see the FortiAnalyzer Administration Guide.

Configuration through Device Manager

The *Device Manager* module contains a database for each managed device. Each database contains the entire configuration of the managed device.

The database is created when the device is added to FortiManager, an FGFM connection is established between the device and FortiManager, and FortiManager retrieves the configuration from the managed device.

You can edit the database by using the following methods:

- Directly in *Device Manager*
- Indirectly by using the central management modules to provide changes to *Device Manager*

This section contains the following topics:

- Direct device database editing on page 47
- Indirect device database editing on page 47
- Model devices on page 48
- Zero-touch and low-touch provisioning on page 48

Direct device database editing

In *Device Manager*, you can directly edit the device database. However the changes apply only to the device.

Some device settings can only be changed by directly editing the device database. For example, you can only change the hostname or the IP address for an interface by editing the device database in *Device Manager*.

After you change the settings, you must install the changes to the device. When you install the changes, the configuration in the FortiManager device database is compared to the configuration on the managed device, and the difference is installed to or removed from the device.



Policy package changes overwrite device database changes.

Indirect device database editing

When you use the following central management modules to configure managed devices, the changes affect *Device Manager*, and you are indirectly editing the device database:

- *Policy & Objects*
- *AP Manager*
- *VPN Manager*
- *FortiSwitch Manager*
- *Extender Manager*

In the central management modules, you can make changes and apply the changes to one or more managed devices. For example, you can use *AP Manager* to create settings, and then apply the settings to every FortiGate that manages an AP.

Each of the central management modules utilizes the Object Database to access shared objects, such as Address Objects, Security Profiles, and Services.

Any configuration done by using one of the central management modules generates settings that are then "pushed" to the device database on the next policy package install. This push overwrites the existing configuration in the device's database for that setting.

After the device database has been updated by the policy package push, an install of the device database takes place in the same way as if you edited directly.

Model devices

Model devices are used to store configuration for a device that is not yet online and not yet connected to the network.

Once the device is online, connected to the network, and connected to FortiManager, the following process begins:

- FortiManager adds the unregistered FortiGate device.
- The FortiGate device is authorized for management by FortiManager.
- FortiManager checks the version of the Internet Service database on the FortiGate.

  If the Internet Service database is lower on the FortiGate, FortiManager requests FortiGate to update its objects.
- After the Internet Service database version is updated on the FortiGate device, FortiManager installs the configuration to the FortiGate.

  If the Internet Service database version is not updated after three minutes, FortiManager still installs the configuration to the FortiGate.

See also Adding offline model devices on page 104.

Zero-touch and low-touch provisioning

FortiManager supports zero-touch provisioning (ZTP) and low-touch provisioning (LTP) of FortiGate devices using model devices.

A model device is configured for a FortiGate device before it is added to FortiManager. The FortiManager administrator can apply device configurations and policies to the model device. When the real FortiGate comes online and is connected to FortiManager, the auto-link process begins, and the device settings and policies are installed on the real device. Once auto-linking is complete, the real device is configured and connected to FortiManager for central management, replacing the model device.

How the FortiGate devices discover and connect to the FortiManager determines if it is zero-touch or low-touch provisioning.

- **Zero-touch provisioning**: Preconfiguration of FortiGate is **not** required. FortiGate boots up, obtains connectivity to the WAN or Internet, and connects to the FortiManager for auto-linking and central

management. Example methods for ZTP include:

- *FortiCloud/FortiDeploy*: FortiGate boots up and obtains its internet connectivity from a DHCP server, automatically connects to FortiCloud, and obtains the location of the FortiManager from FortiCloud.
- *DHCP Option 240/241*: FortiGate boots up and obtains its WAN connectivity from a DHCP server, and the same DHCP server provides the location of FortiManager using DHCP Option 240/241.
- *USB boot method*: FortiGate obtains its initial configuration from a USB stick.

- **Low-touch provisioning**: Some preconfiguration on FortiGate is required before it can discover the FortiManager. For example, configuring network settings on FortiGate and providing the location of FortiManager.



For ZTP methods where DHCP is used to establish the FortiGate's network connection, generally, FortiGate models that have ports labeled as 'WAN' have the interface IP addressing mode set to DHCP client. This provides the ability to connect with WAN upon boot from factory-default configuration. There are models with exceptions where a non-WAN interface has IP addressing mode set to DHCP client by default.

The DHCP Option 240/241 will only work with FortiGates that are in factory default. If any setting is modified, the FortiGate will no longer accept the DHCP Option 240/241. Therefore, the DHCP Option 240/241 method of ZTP only works with models which have interfaces in DHCP client mode by default.

See the following related topics for more information:

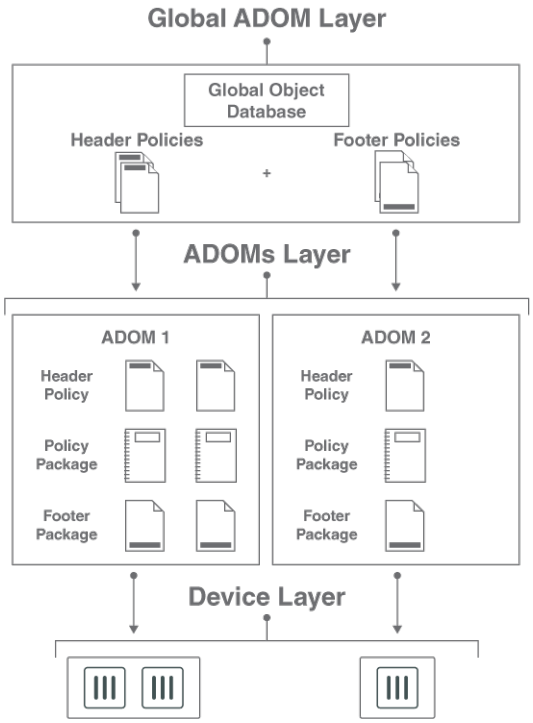
- Model devices on page 48
- Adding offline model devices on page 104
- Sequence of operations for installation to managed devices on page 55

ADOMs and devices

Policy packages can include header policies and footer policies. You can create header and footer policies by using the global ADOM. The global ADOM allows you to create header and footer policies once, and then assign the header and footer policies to multiple policy packages in one or more ADOMs.

For example, a header policy might block all network traffic to a specific country, and a footer policy might start antivirus software. Although you have unique policy packages in each ADOM, you might want to assign the same header and footer policies to all policy packages in all ADOMs.

Following is a visual summary of the process and a description of what occurs in the global ADOM layer, ADOM layer, and device manager layer.



This section contains the following topics:

- Global ADOM layer on page 50
- ADOM and policy layer on page 50
- Device Manager layer on page 51

Global ADOM layer

The global ADOM layer contains the following key pieces:

- The global object database
- All header and footer policies

Header and footer policies are used to envelop policies within each individual ADOM. These are typically invisible to users and devices in the ADOM layer. An example of where this would be used is in a carrier environment, where the carrier would allow customer traffic to pass through their network but would not allow the customer to have access to the carrier's network assets.

ADOM and policy layer

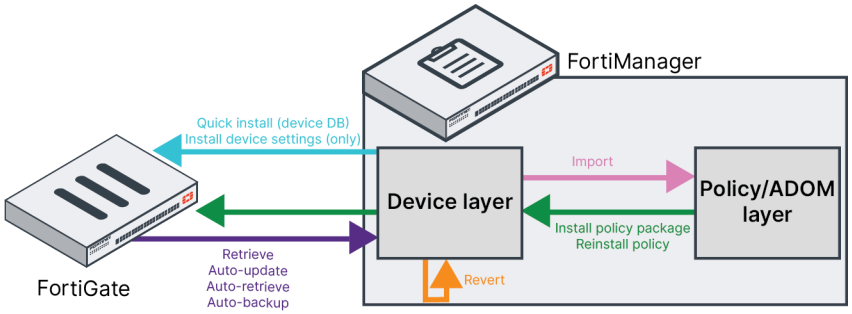
The ADOM layer is where FortiManager manages individual devices, VDOMs, or groups of devices. It is inside this layer where policy packages and folders are created, managed, and installed on managed devices. Multiple policy packages and folders can be created here. The ADOM layer contains one common object database per ADOM, which contains information such as addresses, services, antivirus and attack definitions, and web filtering and email filter.

Device Manager layer

The *Device Manager* layer records information on devices that are centrally managed by FortiManager, such as the name and type of device, the specific device model, its IP address, the current firmware installed on the unit, the device's revision history, and its real-time status.

Operations

This section describes how the different FortiManager operations use the device layer and the ADOM and policy layer to configure FortiGates.



This section describes the following FortiManager operations:

- Install policy package on page 52
- Install device settings only on page 51
- Quick install (device db) on page 52
- Re-install policy on page 53
- Import configuration on page 53
- Retrieve configuration on page 53
- Auto-update and auto-retrieve on page 54
- Auto-backup on page 54
- Refresh on page 54
- Revert on page 54
- Sequence of operations for installation to managed devices on page 55

Install device settings only

The *Install Wizard* includes access to the *Install Device Settings (only)* operation. The *Install Device Settings (only)* operation pushes the device configuration from FortiManager device layer to a FortiGate device.



Before you initiate the installation, you can access an installation preview. If you do not want to install the changes, you can cancel the operation without modifying anything.

FortiManager compares the configuration information that it has with the current configuration on the FortiGate. It then pushes the necessary configuration changes to the FortiGate to ensure that the FortiGate is synchronized with FortiManager.

The install operation can include only device settings or device settings and policy packages. When policy packages are included, the policies defined in the policy package are inserted into the device database, where they overwrite any related settings existing in the device database.

For more information, see Install device settings only on page 183.

Quick install (device db)

The *Quick Install (Device DB)* operation pushes device configuration from the FortiManager device layer to a FortiGate device. This operation does not have an installation preview, and you cannot cancel this operation.

The quick install operation is useful for zero-touch provisioning or when you are familiar with the changes you are applying.

Install policy package

If you do not have a policy package assigned to your FortiGate(s), the best way to install a policy package for the first time is by using the *Install Wizard* and the *Install Policy Package & Device Settings* operation. This operation takes ADOM and policy layer information (from the *Policies & Objects* module) and installs the settings to the device layer, and the difference from the device layer is installed to the FortiGate(s).

You can access an installation preview for this operation. If you do not want to install the changes, you can cancel the operation without modifying anything.

See Installing policy packages and device settings on page 180.

FGFM recovery

When FortiManager installs policy packages to a FortiGate, the FortiGate will restart the FGFM tunnel after each installation and attempt to reconnect to FortiManager.

When the `rollback-allow-reboot` command is enabled on FortiManager and the reconnection fails, the FortiGate will reboot to recover the previous configuration from its config file and attempt to reestablish the connection with FortiManager. You can enable or disable the reboot recovery using the following FortiManager CLI command. This option is disabled by default.

```
config system dm
  set rollback-allow-reboot {enable |disable}
end
```

For more information, see FGFM Recovery Logic in the Communications Protocol Guide.

Re-install policy

If you have already a policy package assigned to your FortiGate(s), you can use the *Re-install Policy* operation. This operation takes ADOM and policy layer information (from the *Policies & Objects* module) and installs it to the device layer and to FortiGate(s). You can access an installation preview for this operation. If you do not want to install the changes, you can cancel the operation without modifying anything.

For more information, see Reinstall a policy package on page 419.

Import configuration

The *Import Configuration* operation copies policies and policy-related objects from the device layer into the ADOM and policy later, creating a policy package that reflects the current configuration of the FortiGate device. The import operation does not modify the FortiGate configuration.

The imported objects go into the shared object database.

If you are importing an object that already exists in the object database (same object type and name), you have the following choices:

1. Update the definition for the object in the database.
   When you update the definition for an object in the database, it affects all FortiGates that reference the object. All FortiGates that reference the object go out of sync, and the updated object is considered a pending change. This action is equivalent to manually updating an object.
2. Keep the definition for the object that is already in the database.
   When you keep the definition for an object in the database, all FortiGates that reference the object remain synchronized. The next time that you install to the FortiGate, the definition for the object from the FortiManager database is pushed to the device.



After you import policies and objects from FortiGate to FortiManager, you might see some objects deleted the first time that you install a policy package to the FortiGate. The objects are on FortiGate because the objects are unused. FortiManager does not need to keep unused objects. You can always install the objects back to the FortiGate by adding them to a policy rule.

For more information, see Importing policies and objects on page 173.

Retrieve configuration

The retrieve operation retrieves the FortiGate configuration and stores it in the device database on FortiManager.

The policy package is not updated when you retrieve a FortiGate configuration.



If you make a change locally on the FortiGate, and then retrieve the FortiGate configuration, the change is stored in the database. However, if a policy also includes the same setting, the setting from the policy overwrites the setting on the FortiGate the next time that the policy package is installed.

For more information, see Viewing configuration revision history on page 206.

Auto-update and auto-retrieve

The auto-retrieve operation is only invoked if the FortiGate fails to initiate an auto-update operation. When FortiManager detects a change on the FortiGate, it automatically retrieves the full configuration.

The auto-update operation is enabled by default. To disable auto-update and allow the administrator to accept or refuse updates, use the following CLI commands:

```
config system admin setting
   set auto-update disable
end
```

When a change is made on the FortiGate, but the change is not initiated by a FortiManager install operation, the FortiGate automatically sends the configuration changes to FortiManager. If the change from FortiGate is a device level setting, the policy layer status in FortiManager remains unchanged. If the change from FortiGate is a policy level setting, the policy layer status in FortiManager might change to *Conflict status*. It is highly recommended to always modify settings on FortiManager and not on FortiGate.

Auto-backup

The auto-backup operation is similar to auto-update, but only available when the FortiManager is in backup mode. The FortiGate device will wait until the FortiGate admin user has logged out before performing the backup.

For more information, see ADOM modes on page 928.

Refresh

FortiManager queries FortiGate to update that FortiGate's current synchronization status. For more information, see Refreshing a device on page 158.

Revert

The revert operation loads a saved configuration revision into the device database. The revert operation does not affect the policy package or other modules. As a result, you may need to update the policy package to ensure that the policy package is aligned with the device database.

After the revert operation completes, complete the following actions to install the changes to the FortiGate:

1. Import the configuration from the managed FortiGate to synchronize the policy package stored in the ADOM database.
2. Re-install the policy package from FortiManager.

For more information, see Viewing configuration revision history on page 206.

Sequence of operations for installation to managed devices

When FortiManager installs changes to managed devices, for example installing Policy Packages and CLI templates to a FortiGate, it follows a sequence where the configuration is first copied to the device's *Device Database* on FortiManager before actual installation to the target device.

This section includes the following:

- FortiManager databases used during installation on page 55
- Sequence for installing changes to managed devices on page 56
- Execution sequence for real devices on page 56
- Execution sequence for model devices on page 57
- Installation example on page 58

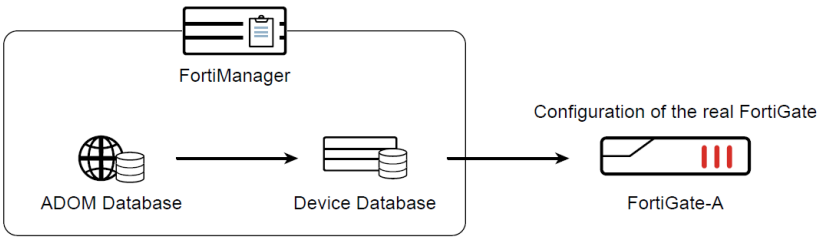
FortiManager databases used during installation

The FortiManager has two databases that are used in the process of installing configuration changes to target devices.

- **ADOM Database**: The FortiManager's ADOM Database includes all ADOM objects including policy objects, provisioning templates, AP Profiles, FortiSwitch templates, and FortiExtender templates.
- **Device (FortiGate) Database**: The FortiManager's Device (FortiGate) Database has complete configuration files for each FortiGate that is managed by the FortiManager.

The diagram below demonstrates the relationship between the *ADOM Database*, *Device Database* and *target device* (real FortiGate) when installing changes.

FortiManager Installation Sequence



Step 1

ADOM objects copied to Device Database

ADOMs objects are copied from the ADOM database to the target device's Device Database.

Step 2

Diff is pushed to the device

FortiManager generates a diff between FortiGate-A's Device Database and the actual configuration on the real device. The diff is installed on the real FortiGate-A device.

Sequence for installing changes to managed devices

The process of installing the changes to the target FortiGate is as follows:

1. FortiManager copies the ADOM objects (including policy objects, Provisioning Templates, etc.) related to the configuration change from the *ADOM Database* to the *Device Database* for the target FortiGate.
   - As an example, each command line in a CLI template is applied to the configuration file stored in the *Device Database* for the target FortiGate.
   - At this point, the configuration file in the *Device Database* is an updated and completely new version.
   - See Execution sequence for real devices on page 56 and Execution sequence for model devices on page 57 for the exact sequence of operations.
2. FortiManager retrieves the current configuration file from the real FortiGate device and compares it to the newly updated configuration file in the *Device Database* to determine the difference (diff) between the old and new configuration. FortiManager installs the changes identified in the diff to the target device.



The diff between the old and new configuration is installed to the target FortiGate, but *not* the original content.
Because of this behavior, some object details (for example, some command lines in a CLI template) are not directly pushed to the target FortiGate. Instead, FortiManager is responsible to make sure that the changes identified in the diff are correctly updated on the real FortiGate.

Execution sequence for real devices

The templates, packages, and profiles are applied to the *Device Database* from the *ADOM Database* in the following order:

1. System template.
2. Threat weight template.
3. IPsec tunnel template.
4. Static route template.
5. BGP template.
6. NSX-T service template.
7. SD-WAN template.
8. AP Profile
9. FortiSwitch template.
10. FortiExtender template.
11. Policy Package.
12. CLI template.

When installing the changes to a real FortiGate:

- FortiManager compares the *Device Database* of the target FortiGate with the configuration retrieved from the real FortiGate device.
- FortiManager generates a diff of the configuration.
- FortiManager installs the difference on the real FortiGate.

Execution sequence for model devices

Pre-Run CLI/Jinja templates run once on a model device to preconfigure them with required settings, for example to add interfaces to a FortiGate-VM. Pre-run CLI/Jinja templates are exclusively available to model devices, and can only be assigned to model devices.

Similar to other Provisioning Templates, the pre-run CLI/Jinja template is only applied to the *Device Database* on the FortiManager side, not to the target FortiGate.

When a pre-run CLI template has been assigned to a model device, it will be automatically applied to the model device's *Device Database* once the *Add Device* wizard completes. Once applied, the pre-run CLI template is unassigned from the model device.

The templates, packages, and profiles are applied to the *Device Database* from the *ADOM Database* in the following order:

1. Pre-run CLI template (Only available on model devices. Pre-run CLI/Jinja templates are applied to the *Device Database* once the *Add Device* wizard completes).
2. System template.
3. Threat weight template.
4. IPsec tunnel template.
5. Static route template.
6. BGP template.
7. NSX-T service template.
8. SD-WAN template.
9. AP Profile
10. FortiSwitch template.
11. FortiExtender template.
12. Policy Package.
13. CLI template.

With zero touch provisioning, you only need to assign Provisioning Templates and Policy Packages to model devices and are not required to perform any of the installation actions (see the note below for best practices and exceptions). Once the real device comes online, FortiManager copies everything to the *Device Database* (excluding the pre-run CLI template which is automatically applied when the model device is added to FortiManager) and then installs it on the real device as part of the auto-link process.



- When a model device has a Policy Package assigned, it is recommended as a best practice that you perform the Policy Package installation before bringing the real device online so that you can catch potential configuration errors before auto-link occurs.
- When a model device is part of a device group, and the device group itself is the installation target of a Policy Package, the policy will *not* be installed automatically during the auto-link process. You *must* perform a Policy Package install before bringing the real device online.

Installation example

The following example demonstrates that during installation to a real FortiGate device, FortiManager does not push the content of a CLI template to the FortiGate line-by-line. Instead FortiManager identifies the difference between the *Device Database* and the FortiGate's current configuration, and is responsible for installing the necessary changes.

1. On the FortiManager, a CLI template is assigned to a FortiGate-60E.
   The CLI template contains the following commands:
   ```
   config firewall policy
      delete 1
   end
   config firewall policy
      edit "1"
         set action accept
         set srcintf "internal1"
         set dstintf "internal1"
         set srcaddr "all"
         set dstaddr "all"
         set schedule "always"
         set service "ALL"
         set logtraffic all
      next
   end
   ```
2. The real FortiGate-60E is currently configured with *Policy ID 1* as shown below:
   ```
   config firewall policy
      edit 1
         set uuid bddc84d8-a64f-51ed-405b-90156f074f85
         set srcintf "any"
         set dstintf "any"
         set action accept
         set srcaddr "all"
         set dstaddr "all"
         set schedule "always"
         set service "ALL"
         set logtraffic all
      next
   end
   ```
3. To install the updated Policy Package to the FortiGate-60E, FortiManager first copies all of the CLI template's content from the FortiManager's *ADOM Database* to the *Device Database* for the FortiGate-60E.
   ```
   config firewall policy
      delete 1
   end
   config firewall policy
      edit "1"
         set action accept
         set srcintf "internal1"
         set dstintf "internal1"
         set srcaddr "all"
         set dstaddr "all"
         set schedule "always"
         set service "ALL"
         set logtraffic all
      next
   ```

```
end
```

4. After the copy process is finished, the FortiGate-60E's device configuration status on FortiManager is shown as *Modified*.
5. FortiManager compares the modified FortiGate-60E's *Device Database* with the real FortiGate-60E's configuration, and generates a diff of the configuration. The changes identified in the diff are pushed to the real FortiGate-60E.
   In this example, the installation log below shows that only *Policy ID 1's UUID*, *source interface*, and *destination interface* settings are installed on the real FortiGate-60E as those are the differences identified.

```
Starting log (Run on device)
Start installing
   FGT60ETK19025756 $ config firewall policy
   FGT60ETK19025756 (policy) $ edit 1
   FGT60ETK19025756 (1) $ set uuid 2fa87c82-a765-51ed-e337-052557345417
   FGT60ETK19025756 (1) $ set srcintf "internal1"
   FGT60ETK19025756 (1) $ set dstintf "internal1"
   FGT60ETK19025756 (1) $ next
   FGT60ETK19025756 (policy) $ end
---> generating verification report
<--- done generating verification report
install finished
```

Key features of the FortiManager system

Security Fabric

FortiManager can recognize a Security Fabric group of devices and display all units in the group on the *Device Manager* pane, and you can manage the units in the Security Fabric group as if they were a single device. See Adding a Security Fabric group on page 122.You can also display the security fabric topology (see Displaying Security Fabric topology on page 157) and view Security Fabric Ratings (see Fabric View on page 697).

Configuration revision control and tracking

Your FortiManager unit records and maintains the history of all configuration changes made over time. Revisions can be scheduled for deployment or rolled back to a previous configuration when needed.

Centralized management

FortiManager can centrally manage the configurations of multiple devices from a single console. Configurations can then be built in a central repository and deployed to multiple devices when required.

Administrative domains

FortiManager can segregate management of large deployments by grouping devices into geographic or functional ADOMs. See Administrative Domains (ADOMs) on page 924.

Local FortiGuard service provisioning

A FortiGate device can use the FortiManager unit for antivirus, intrusion prevention, web filtering, and email filtering to optimize performance of rating lookups, and definition and signature downloads. See FortiGuard on page 787.

Firmware management

FortiManager can centrally manage firmware images and schedule managed devices for upgrade using firmware templates.

Scripting

FortiManager supports CLI or Tcl based scripts to simplify configuration deployments. See Scripts on page 239.

Logging and reporting

FortiManager can also be used to log traffic from managed devices and generate Structured Query Language (SQL) based reports. FortiManager also integrates FortiAnalyzer logging and reporting features.

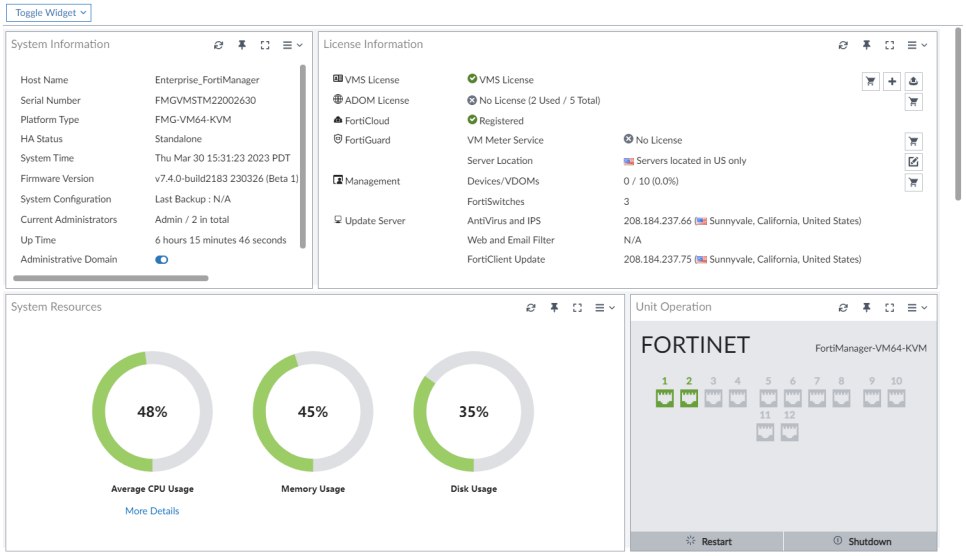
Fortinet device life cycle management

The management tasks for devices in a Fortinet security infrastructure follow a typical life cycle:

- *Deployment*: An administrator completes configuration of the Fortinet devices in their network after initial installation.
- *Monitoring*: The administrator monitors the status and health of devices in the security infrastructure, including resource monitoring and network usage. External threats to your network infrastructure can be monitored and alerts generated to advise.
- *Maintenance*: The administrator performs configuration updates as needed to keep devices up-to-date.
- *Upgrading*: Virus definitions, attack and data loss prevention signatures, web and email filtering services, and device firmware images are all kept current to provide continuous protection for devices in the security infrastructure.

Dashboard

Dashboard contains widgets that provide performance and status information and enable you to configure basic system settings.



The following widgets are available:

Widget	Description
System Information	Displays basic information about the FortiManager system, such as up time and firmware version. You can also enable or disable Administrative Domains and FortiAnalyzer features. For more information, see System Information widget on page 63. From this widget you can manually update the FortiManager firmware to a different release. For more information, see Updating the system firmware on page 66. The widget fields will vary based on how the FortiManager is configured, for example, if ADOMs are enabled.
System Resources	Displays the real-time and historical usage status of the CPU, memory and hard disk. For more information, see System Resources widget on page 76.
License Information	Displays whether the unit license is registered to FortiCloud. Displays the devices being managed by the FortiManager unit and the maximum numbers of devices allowed. For more information, see License Information widget on page 76. From this widget you can add a license or manually upload a license for VM systems.

Widget	Description
Unit Operation	Displays status and connection information for the ports of the FortiManager unit. It also enables you to shutdown and restart the FortiManager unit or reformat a hard disk. For more information, see Unit Operation widget on page 82.
Alert Message Console	Displays log-based alert messages for both the FortiManager unit and connected devices. For more information, see Alert Messages Console widget on page 82.
Log Receive Monitor	Displays a real-time monitor of logs received. You can view data per device or per log type. For more information, see Log Receive Monitor widget on page 83. The *Log Receive Monitor* widget is available when *FortiAnalyzer Features* is enabled.
Insert Rate vs Receive Rate	Displays the log insert and receive rates. For more information, see Insert Rate vs Receive Rate widget on page 83. The *Insert Rate vs Receive Rate* widget is available when *FortiAnalyzer Features* is enabled.
Log Insert Lag Time	Displays how many seconds the database is behind in processing the logs. For more information, see Log Insert Lag Time widget on page 84. The *Log Insert Lag Time* widget is available when *FortiAnalyzer Features* is enabled.
Receive Rate vs Forwarding Rate	Displays the *Receive Rate*, which is the rate at which FortiManager is receiving logs. When log forwarding is configured, the widget also displays the log forwarding rate for each configured server. For more information, see Receive Rate vs Forwarding Rate widget on page 84. The *Receive Rate vs Forwarding Rate* widget is available when *FortiAnalyzer Features* is enabled.
Disk I/O	Displays the disk utilization, transaction rate, or throughput as a percentage over time. For more information, see Disk I/O widget on page 85. The *Disk I/O*widget is available when *FortiAnalyzer Features* is enabled.
Device widgets	For example, widgets such as *Connectivity*, *Device Config Status*, and *Firmware Status*. These widgets display summary information for authorized devices. For more inforamtion, see Device widgets on page 85.

Customizing the dashboard

The FortiManager system dashboard can be customized. You can select which widgets to display, where they are located on the page, and whether they are minimized or maximized. It can also be viewed in full screen by selecting the full screen button on the far right side of the toolbar.

Action	Steps
Move a widget	Move the widget by clicking and dragging its title bar, then dropping it in its new location
Add a widget	Select *Toggle Widgets* from the toolbar, then select the name widget you need to add.
Delete a widget	Click the *Close* icon in the widget's title bar.
Customize a widget	For widgets with an edit icon, you can customize the widget by clicking the Edit icon and configuring the settings.
Reset the dashboard	Select *Toggle Widgets* > *Reset to Default* from the toolbar. The dashboards will be reset to the default view.

System Information widget

The information displayed in the *System Information* widget is dependent on the FortiManager model and device settings. The following information is available on this widget:

Host Name	The identifying name assigned to this FortiManager unit. Click the edit host name button to change the host name. For more information, see Changing the host name on page 64.
Serial Number	The serial number of the FortiManager unit. The serial number is unique to the FortiManager unit and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
Platform Type	Displays the FortiManager platform type, for example *FMGVM64* (virtual machine).
HA Status	Displays if FortiManager unit is in High Availability mode and whether it is the Primary or Secondary unit in the HA cluster. For more information see High Availability on page 1067.
System Time	The current time on the FortiManager internal clock. Click the edit system time button to change system time settings. For more information, see Configuring the system time on page 65.
Firmware Version	The version number and build number of the firmware installed on the FortiManager unit. You can access the latest firmware version available on FortiGuard from FortiManager. Alternately you can manually download the latest firmware from the Customer Service & Support website at https://support.fortinet.com. Click the update button, then select the firmware image to load from the local hard disk or network volume. For more information, see Updating the system firmware on page 66.

System Configuration	The date of the last system configuration backup. The following actions are available: • Click the backup button to backup the system configuration to a file; see Backing up the system on page 71. • Click the restore to restore the configuration from a backup file; see Restoring the configuration on page 74. You can also migrate the configuration to a different FortiManager model by using the CLI. See Migrating the configuration on page 75.
Current Administrators	The number of administrators currently logged in. Click the current session list button to view the session details for all currently logged in administrators.
Up Time	The duration of time the FortiManager unit has been running since it was last started or restarted.
Administrative Domain	Displays whether ADOMs are enabled. Toggle the switch to change the Administrative Domain state. See Enabling and disabling the ADOM feature on page 927.
FortiAnalyzer Features	Displays whether FortiAnalyzer features are enabled. Toggle the switch to change the FortiAnalyzer features state. *FortiAnalyzer Features* are not available on the FortiManager 100C or when FortiManager HA is enabled. See FortiAnalyzer Features on page 41 for information.

Changing the host name

The host name of the FortiManager unit is used in several places.

- It appears in the *System Information* widget on the dashboard.
- It is used in the command prompt of the CLI.
- It is used as the SNMP system name.

The *System Information* widget and the `get system status` CLI command will display the full host name. However, if the host name is longer than 16 characters, the CLI and other places display the host name in a truncated form ending with a tilde (~) to indicate that additional characters exist, but are not displayed. For example, if the host name is FortiManager1234567890, the CLI prompt would be `FortiManager123456~#`.

To change the host name:

1. Go to *Dashboard*.
2. In the *System Information* widget, click the edit host name button next to the *Host Name* field.
3. In the *Host Name* box, type a new host name.
   The host name may be up to 35 characters in length. It may include US-ASCII letters, numbers, hyphens, and underscores. Spaces and special characters are not allowed.
4. Click the checkmark to change the host name.

Configuring the system time

You can either manually set the FortiManager system time or configure the FortiManager unit to automatically keep its system time correct by synchronizing with a Network Time Protocol (NTP) server.



For many features to work, including scheduling, logging, and SSL-dependent features, the FortiManager system time must be accurate.

To configure the date and time:

1. Go to *Dashboard*.
2. In the *System Information* widget, click the edit system time button next to the *System Time* field.
3. Configure the following settings to either manually configure the system time, or to automatically synchronize the FortiManager unit's clock with an NTP server:

System Time	The date and time according to the FortiManager unit's clock at the time that this pane was loaded or when you last clicked the *Refresh* button.
Time Zone	Select the time zone in which the FortiManager unit is located and whether or not the system automatically adjusts for daylight savings time. Time zone settings can also be for each ADOM. See Creating ADOMs on page 934.
Update Time By	Select *Set time* to manually set the time, or *Synchronize with NTP Server* to automatically synchronize the time.
Set Time	Manually set the data and time.
Select Date	Set the date from the calendar or by manually entering it in the format: YYYY/MM/DD.
Select Time	Select the time.
Synchronize with NTP Server	Automatically synchronize the date and time.
Server	Enter the IP address or domain name of an NTP server. Click the plus icon to add more servers. To find an NTP server that you can use, go to http://www.ntp.org.
Min	Minimum poll interval in seconds as power of 2 (e.g. 6 means 64 seconds, default = 6).
Max	Maximum poll interval in seconds as power of 2 (e.g. 6 means 64 seconds, default = 10).

4. Click the checkmark to apply your changes.

Updating the system firmware

To take advantage of the latest features and fixes, you can update FortiManager firmware. From the *Dashboard* menu in FortiManager, you can access firmware images on FortiGuard and update FortiManager. Alternately you can manually download the firmware image from the Customer Service & Support site, and then upload the image to FortiManager.

For information about upgrading your FortiManager device, see the *FortiManager Upgrade Guide*, or contact Fortinet Customer Service & Support.

Back up the system



Back up the configuration and database before changing the firmware of FortiManager. Changing the firmware to an older or incompatible version may reset the configuration and database to the default values for that firmware version, resulting in data loss. For information on backing up the configuration, see Backing up the system on page 71.

Register FortiManager



Before you can download firmware updates for FortiManager, you must first register your FortiManager unit with Customer Service & Support. For details, go to https://support.fortinet.com/ or contact Customer Service & Support.

Valid firmware contracts are required to upgrade major/minor versions



If the FortiManager support contract which includes the *Firmware & General Updates* entitlement has expired, you will be unable to upgrade the firmware to a higher major version, such as from FortiManager 7.0 to 8.0, or to a higher minor version, such as from FortiManager 7.4 to 7.6. However, you can upgrade the firmware of a FortiManager with an expired contract to a higher patch build, such as from FortiManager 7.4.0 to 7.4.1, to allow for security updates.

Network vulnerability management engine



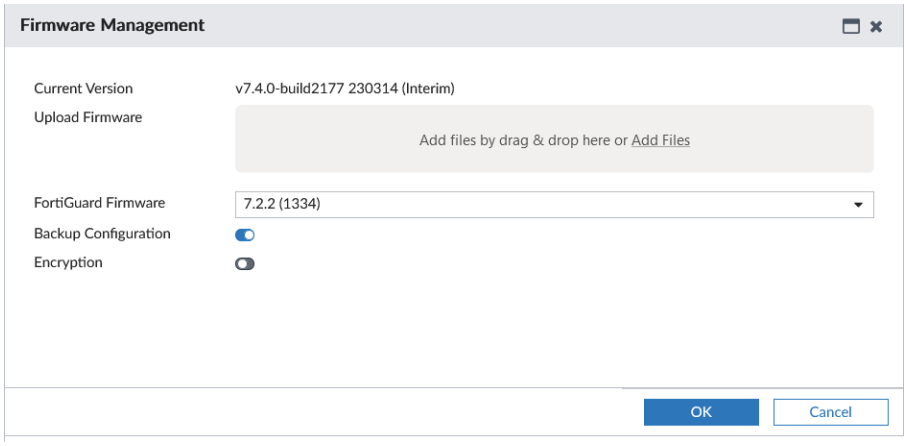
Installing firmware replaces the current network vulnerability management engine with the version included with the firmware release that you are installing. After you install the new firmware, make sure that your vulnerability definitions are up-to-date. For more information, see FortiGuard on page 787.

After updating FortiManager firmware, you should update the following items in the following order:

1. Update firmware for managed FortiGates.
2. Upgrade the ADOM version.
3. Upgrade the global ADOM version.

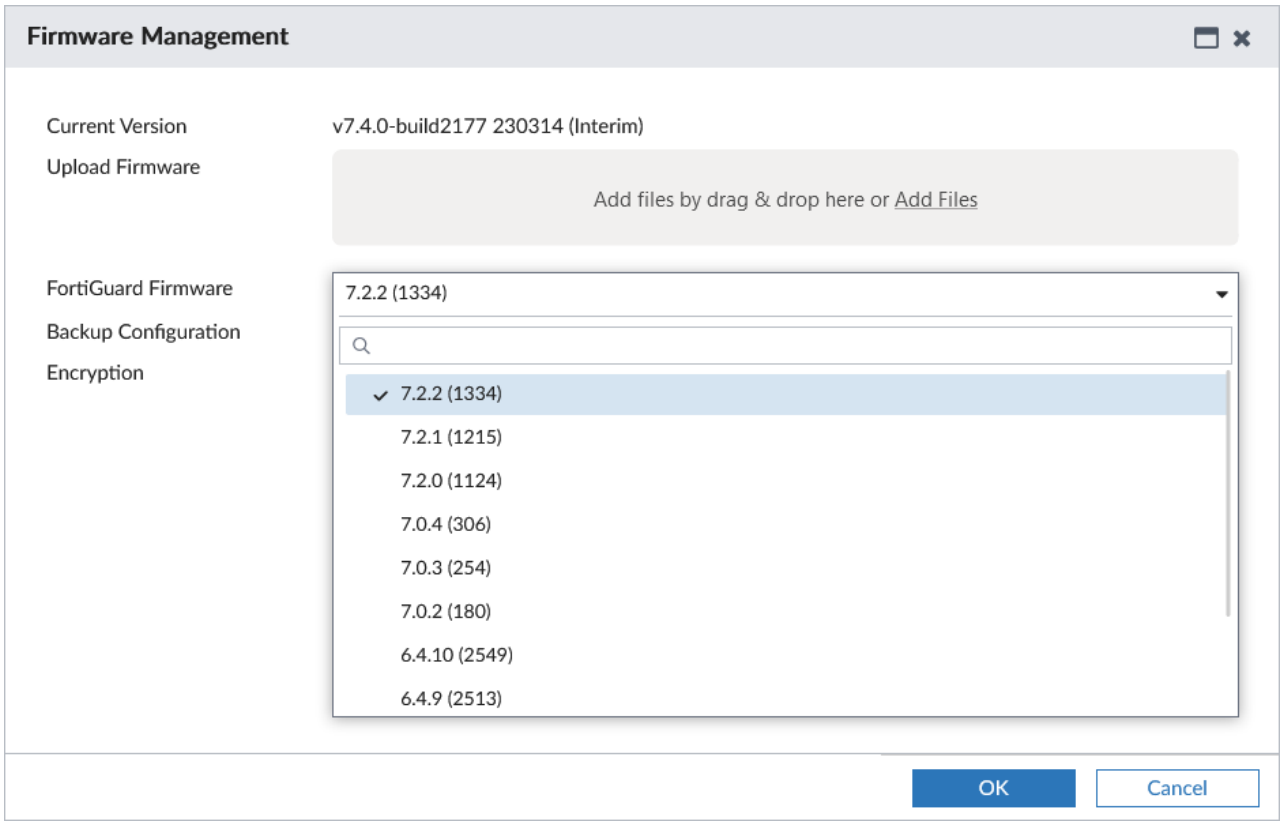
To update FortiManager firmware using FortiGuard:

1. Go to *Dashboard*.
2. In the *System Information* widget, beside *Firmware Version*, click *Upgrade Firmware*.
   The *Firmware Management* dialog box opens.

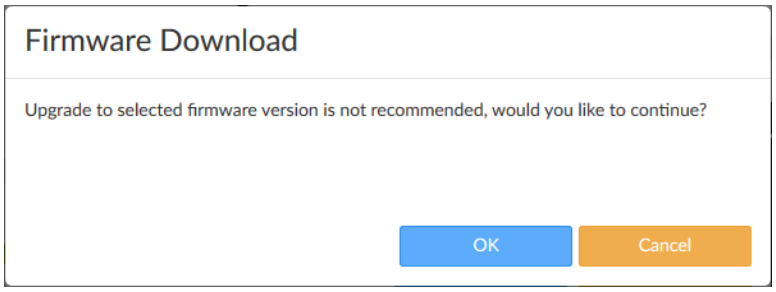


3. Before upgrading your firmware, you can choose to enable or disable *Backup Configuration*. When this setting is enabled, you will automatically download a backup copy of your FortiManager configuration when performing a firmware upgrade.

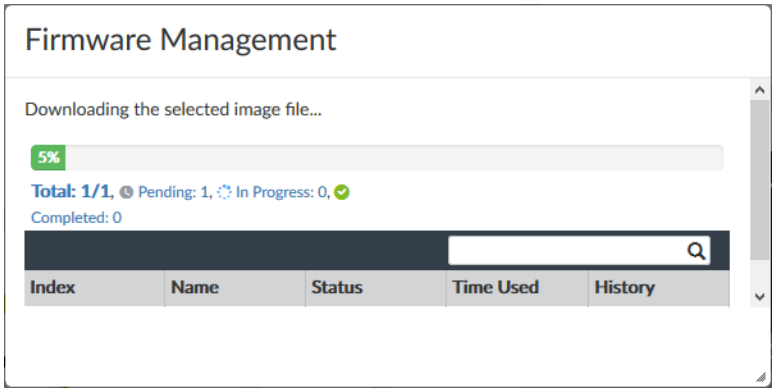
   Type and confirm the password you want to use for encryption. The password can be a maximum of 63 characters.
4. From the *FortiGuard Firmware* box, select the version of FortiManager for the upgrade, and click *OK*.
   The *FortiGuard Firmware* box displays the FortiManager firmware images available for upgrade:
   - When FortiManager has a valid contract, all available firmware versions are displayed for upgrading or downgrading.
   - When FortiManager has no valid contract, or the contract is expired, only display the available patch upgrades.
   - A green checkmark displays beside the recommended image for FortiManager upgrade.



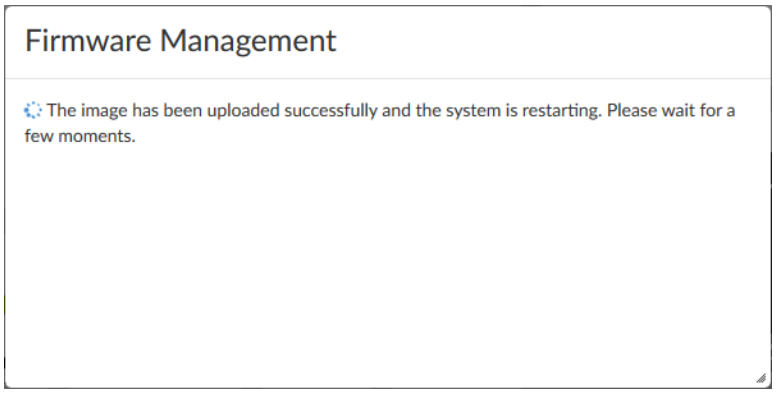
- If you select an image without a green checkmark, a confirmation dialog box is displayed. Click *OK* to continue.



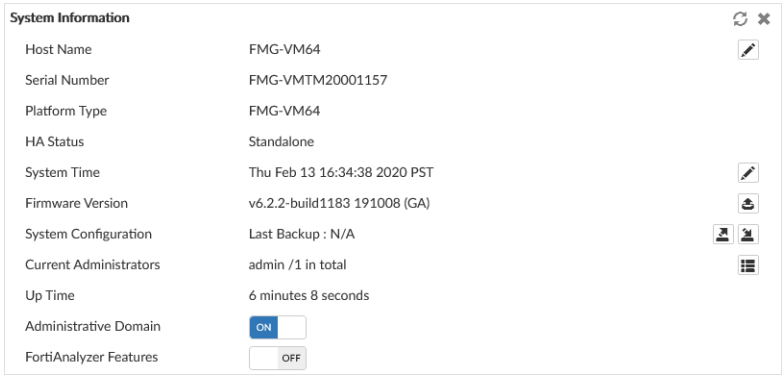
- FortiManager downloads the firmware image from FortiGuard.



- FortiManager uses the downloaded image to update its firmware, and then restarts.



- After FortiManager restarts, the upgrade is complete.



To manually update FortiManager firmware:

1. Download the firmware (the `.out` file) from the Customer Service & Support website, https://support.fortinet.com/.
2. Go to *Dashboard*.
3. In the *System Information* widget, in the *Firmware Version* field, click *Upgrade Firmware*. The *Firmware Upload* dialog box opens.
4. Before upgrading your firmware, you can choose to enable or disable *Backup Configuration*. When this setting is enabled, you will automatically download a backup copy of your FortiManager configuration when performing a firmware upgrade.

   Type and confirm the password you want to use for encryption. The password can be a maximum of 63 characters.
5. Drag and drop the file onto the dialog box, or click *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support portal and then click *Open*.
6. Click *OK*.
   Your device will upload the firmware image and you will receive a confirmation message when the upgrade was successful.
   Attempting to upgrade major/minor versions without a valid *Firmware & General Updates* entitlement will result in an error message, and the upgrade will not proceed.

Optionally, you can upgrade firmware stored on an FTP or TFTP server using the following CLI command:

```
execute restore image {ftp | tftp} <file path to server> <IP of server>
      <username on server> <password>
```

For more information, see the FortiManager CLI Reference.

7. Refresh the browser and log back into the device.
8. Go to *Device Manager* module and make sure that all formerly added devices are still listed.
9. Open the other functional modules and make sure they work properly.

You can also update FortiManager firmware images by using the *FortiGuard* module. For more information, see Firmware images on page 806.

Firmware maturity levels

FortiManager 7.4.4 and later firmware images use tags to indicate the following maturity levels:

- The *Feature* tag indicates that the firmware release includes new features. It can also include bug fixes and vulnerability patches where applicable.
- The *Mature* tag indicates that the firmware release includes no new, major features. Mature firmware will contain bug fixes and vulnerability patches where applicable.

Administrators can use the tags to identify the maturity level of the current firmware in the GUI or CLI.

Administrators can view the maturity level of each firmware image that is available for upgrade on the Firmware Management dialog box. When upgrading from mature firmware to feature firmware, a warning message is displayed.

To view maturity levels for firmware in the GUI:

1. Go to *Dashboard*.
2. In the *System Information* widget, beside *Firmware Version*, click *Upgrade Firmware*.
   The *Firmware Management* dialog box opens.
3. From the *FortiGuard Firmware box*, select the version of FortiManager for the upgrade.
   The Firmware Version displays the version with build number and either (Mature) or (Feature).

To view maturity levels for firmware in the CLI:

In this example, the *Version* field includes `.F` to indicate that the maturity level is feature:

```
# get system status
   Platform Type : FMG-3000G
   Platform Full Name : FortiManager-3000G
   Version : vx.x.x0-buildxxxx 240620 (GA.F)
```

In this example, the *Version* field includes `.M` to indicate that the maturity level is mature:

```
# get system status
   Platform Type : FMG-3000G
   Platform Full Name : FortiManager-3000G
   Version : vx.x.x-buildxxxx 240620 (GA.M)
```

Backing up the system

Fortinet recommends that you back up your FortiManager configuration to your management computer on a regular basis to ensure that, should the system fail, you can quickly get the system back to its original state with minimal affect to the network. You should also back up your configuration after making any changes to the FortiManager configuration or settings that affect connected devices.

You can perform backups manually or at scheduled intervals. You can use *ADOM Revisions* in *Policy & Objects* to maintain a revision of your FortiManager configurations in an ADOM. See ADOM revisions on page 577.

Fortinet recommends backing up all configuration settings from your FortiManager unit before upgrading the FortiManager firmware. See Updating the system firmware on page 66.

An MD5 checksum is automatically generated in the event log when backing up the configuration. You can verify a backup by comparing the checksum in the log entry with that of the backup file. The filename is also included in the event log for reference.



FortiManager uses AES-GCM encryption for backup configurations.

Perform a system backup

To back up the FortiManager configuration:

1. Go to *Dashboard*.
2. In the *System Information* widget, click the backup button next to *System Configuration*. The *Backup System* dialog box opens.
3. Select the *Backup Now* tab.
4. Enter and confirm the password you want to use for encryption. The password can be a maximum of 63 characters.



The character " \" is used in the FortiManager CLI as an escape character.

If your encryption password contains the \ character, you must either escape it (by adding an additional \) or use single quotes around the password when referring to it in the CLI. For example:

- `execute backup all-settings ftp 10.0.0.1 backup/backup1.dat admin admin1234 ~jFeS.Z/i\\ilA~gnAaq=8c1n`gCabc`
- `execute backup all-settings ftp 10.0.0.1 backup/backup1.dat admin admin1234 '~jFeS.Z/i\ilA~gnAaq=8c1n`gCabc'`

5. Select *OK* and save the backup file on your management computer.

Scheduling automatic backups

You can configure FortiManager to automatically backup your configuration on a set schedule.

To schedule automatic backup in the GUI:

1. Go to *Dashboard*.
2. In the *System Information* widget, click the backup button next to *System Configuration*. The *Backup System* dialog box opens.
3. Select the *Schedule Backup* tab.
4. Enable the *Enable Schedule Backup* option, and configure the options including the backup location, backup frequency, and an encryption password.
5. Click *OK*.

To schedule automatic backup in the CLI:

1. In the FortiManager CLI, enter the following command:
   ```
   config system backup all-settings
   ```
2. Configure the backup settings:
   ```
   set status {enable | disable}
   set server {<ipv4_address>|<fqdn_str>}
   set user <username>
   set directory <string>
   set week_days {monday tuesday wednesday thursday friday saturday sunday}
   set time <hh:mm:ss>
   set protocol {ftp | scp | sftp}
   set passwd <passwd>
   set crptpasswd <passwd>
   end
   ```

For example, the following configuration uses the FTP protocol to backup the configuration to server `172.20.120.11` in the `/usr/local/backup` directory every Monday at 1:00pm.

```
config system backup all-settings
   set status enable
   set server 172.20.120.11
   set user admin
   set directory /usr/local/backup
   set week_days monday
   set time 13:00:00
   set protocol ftp
end
```

For more information, see the FortiManager CLI Reference Guide on the Fortinet Documents Library.

View backup history

After performing backups, you can view the backup history to see all backups performed on the FortiManager.

To see backup history:

1. Go to *Dashboard*.
2. In the *System Information* widget, click the backup button next to *System Configuration*. The *Backup System* dialog box opens.
3. Select the *Backup History* tab.
   The backup history displays the *Date & Time*, *Admin*, *Size* and *Status* of each backup.

MD5 checksum

To find the MD5 checksum generated with the backup:

1. In the GUI, go to *System Settings* > *Event Log*.
2. In the *Changes* column for the event log, note the MD5 checksum.

Perform backups using SCP

You can use secure copy protocol (SCP) with a SSH certificate to back up the FortiManager system configuration.

The following is an example of SSH certificate generation to be used with SCP for configuration backup. This example uses RSA but can also be applied to ED25519 keys.

To configure a SSH certificate for backup using SCP:

1. Create a SSH CA user key pair.
   ```
   ssh-keygen -t rsa -b 4096 -f ~/.ssh/ssh_user_ca
   ```
2. Create a SSH CA host key pair.
   ```
   ssh-keygen -t rsa -b 4096 -f ~/.ssh/ssh_host_ca
   ```
3. Copy the CA host `ssh_host_ca*` to `/etc/ssh/`.
4. Sign the user's public key using the host CA key.
   ```
   ssh-keygen -s ~/.ssh/ssh_host_ca -I qa -n qa -V +52w ~/.ssh/ssh_user_ca.pub

   ssh-keygen -Lf ~/.ssh/ssh_user_ca-cert.pub
   /root/.ssh/ssh_user_ca-cert.pub:
      Type: ssh-rsa-cert-v01@openssh.com host certificate
      Public key: RSA-CERT SHA256:/Ue4vx5n2oUp+XhwLuAkadsfa0YTt7dpuZgbZ8TBNuw
      Signing CA: RSA SHA256:/Ue4vx5n2oUp+XhwLuAkIkvadfadTt7dpuZgbZ8TBNuw (using rsa-sha2-512)
      Key ID: "qa"
      Serial: 0
      Valid: from 2023-09-25T14:24:00 to 2024-09-23T14:25:08
      Principals: qa
      Critical Options: (none)
      Extensions: (none)
   ```

   In the example command `ssh-keygen -s ~/.ssh/ssh_host_ca -I qa -n qa -V +52w ~/.ssh/ssh_user_ca.pub`, the `-n qa` option specifies the username (*qa*) that will be allowed to authenticate using the signed certificate. This should match the username used to log in to the FortiManager device when transferring backups via SCP.

5. Edit the SSH server config file at `/etc/ssh/sshd_config` and make the *TrustedUserCAKeys* directive to point to the user CA public key.
   ```
   TrustedUserCAKeys /etc/ssh/ssh_host_ca.pub
   ```
6. Restart the sshd process to make the configuration change take effect..
   ```
   systemctl restart sshd
   ```
7. On FortiManager, configure the SSH certificate.
   ```
   config sys certificate ssh
   ```

```
edit ssh_cert_1
   set certificate "ssh_user_ca-cert.pub"
   set private "ssh_user_ca"
end
```

8. Configure backup of all settings using SCP .

```
execute backup all-settings scp <server IP> <path and file name> <username> <ssh-cert>
```

For more information on configuration of backup settings in the FortiManager CLI, see the FortiManager CLI Reference.

Restoring the configuration

You can use the following procedure to restore your FortiManager configuration from a backup file on your management computer.

If your FortiManager unit is in HA mode, switch to Standalone mode.



The restore operation will temporarily disable the communication channel between FortiManager and all managed devices. This is a safety measure, in case any devices are being managed by another FortiManager. To re-enable the communication, please go to *System Settings* > *Advanced* > *Advanced Settings* and disable *Offline Mode*.

To restore the FortiManager configuration:

1. Go to *Dashboard*.
2. In the *System Information* widget, click the restore button next to *System Configuration*. The *Restore System* dialog box opens.
3. Configure the following settings then select *OK*.

Choose Backup File	Select *Browse* to find the configuration backup file you want to restore, or drag and drop the file onto the dialog box.
Password	Type the encryption password.
Overwrite current IP, routing and HA settings	Select the checkbox to overwrite the current IP, routing, and HA settings.
Restore in Offline Mode	Informational checkbox. Hover over the help icon for more information.
Migrate from a different platform	Enable this option to migrate the uploaded database from a different version or platform. See Migrating the configuration on page 75. • When this option is disabled, the default operation of FortiManager is to restore the database based on the uploaded file. • When the option is enabled, the FortiManager migrates the database of the uploaded file.

Migrating the configuration

You can back up the configuration of one FortiManager and then use the GUI or CLI to migrate the settings to another FortiManager on the same or different platform or version.

If you encrypted the FortiManager configuration file when you created it, you need the password to decrypt the configuration file when you migrate the file to another FortiManager model.



When migrating the database from another platform, all configurations except the system settings are migrated. These system settings must be manually copied from the original FortiManager model to the other FortiManager model.

To migrate the FortiManager configuration using the GUI:

1. In one FortiManager model, go to *Dashboard*.
2. Back up the system. See Backing up the system on page 71.
3. In the other FortiManager model, go to *Dashboard*.
4. If the configuration file is for multiple ADOMs, enable *Administrative Domains* in the *System Information* widget before migrating.
5. Click on the *Restore* option next to *System Configuration*.
   The *Restore System* dialog appears.
6. Enable the option to *Migrate from a different platform*.
7. Upload the backup file from the migrating platform, and click *OK*.
8. After migrating, update the system settings, as needed.
9. Re-establish the FGFM tunnels. See Appendix C - Re-establishing the FGFM tunnel after VM license migration on page 1092.

To migrate the FortiManager configuration using the CLI:

1. In one FortiManager model, go to *Dashboard*.
2. Back up the system. See Backing up the system on page 71.
3. In the other FortiManager model, go to *Dashboard*.
4. If the configuration file is for multiple ADOMs, enable *Administrative Domains* in the *System Information* widget before migrating.
5. Open the CLI Console, and enter the following command:
```
execute migrate all-settings <ftp | scp | sftp> <server> <filepath> <user> <password>
      <cryptpasswd>
```
6. After migrating, update the system settings, as needed.
7. Re-establish the FGFM tunnels. See Appendix C - Re-establishing the FGFM tunnel after VM license migration on page 1092.



If the original FortiManager has databases from FortiGuard (antivirus, antispam, webfilter, etc.), they will not be included in the configuration file. After migrating, export the packages from the original FortiManager and import them to the other FortiManager. For example, see Exporting web filter databases example on page 801 and Importing web filter databases example on page 802.

System Resources widget

The *System Resources* widget displays the usage status of the CPUs, memory, and hard disk. You can view system resource information in real-time or historical format, as well as average or individual CPU usage.

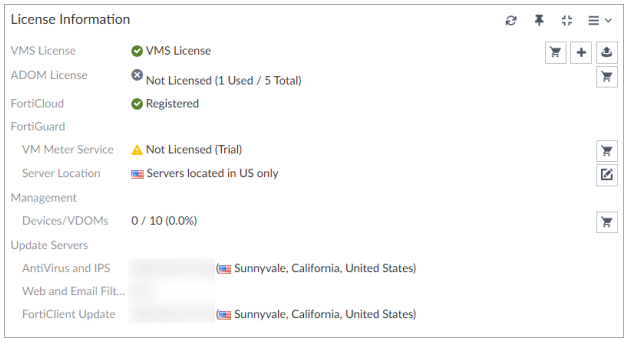
On VMs, warning messages are displayed if the amount of memory or the number of CPUs assigned are too low, or if the allocated hard drive space is less than the licensed amount. These warnings are also shown in the notification list (see GUI overview on page 33). Clicking on a warning opens the *FortiManager VM Install Guide*.

To toggle between real-time and historical data, click *Edit* in the widget toolbar, select *Historical* or *Real-time*, edit the other settings as required, then click *OK*.

To view individual CPU usage, from the Real-Time display, click on the CPU chart. To go back to the standard view, click the chart again.

License Information widget

The *License Information* widget displays the number of devices connected to the FortiManager.



VMS License	VM license information and status. Click the *Add License* button to log in to FortiCloud and activate an add-on license. See Activating add-on licenses on page 78. Click the *Upload License* button to upload a new VM license file. This field is only visible for FortiManager VM. The *Duplicate* status appears when users try to upload a license that is already in use. Additionally, the following message will be displayed in the Notifications: *Duplicate License has been found! Your VM license will expire in XX hours (Grace time: 24 hours)* Users will have 24 hours to upload a valid license before the duplicate license is blocked.

ADOM License		ADOM license information and status. For Hardware models, the default number of ADOMs can be found in the Release Notes on docs.fortinet.com.
FortiCloud		License registration status with FortiCloud. Displays *Not Registered* or *Registered*. When *FortiCloud* displays *Not Registered*, a *Register Now* link is available. You can click the *Register Now* link to register the device or VM license with FortiCloud. See Registering with FortiCloud on page 78.
FortiGuard		
	VM Meter Service	The license status. Click the purchase button to go to the Fortinet Customer Service & Support website, where you can purchase a license.
	Secure DNS Server	The SDNS server license status. Click the upload image button to upload a license key.
	Server Location	The locations of the FortiGuard servers, either global or US only. Click the edit icon to adjust the location. Changing the server location will cause the FortiManager to reboot.
Management		
	Device/VDOMs	The total number of devices and VDOMs connected to the FortiManager and the total number of device and VDOM licenses.
	FortiGates/Logging Devices	The number of connected FortiGates and other logging devices.
	FortiAPs	The number of connected FortiAPs.
	FortiSwitches	The number of connected FortiSwitches.
Logging		This section is only shown when *FortiAnalyzer Features* is enabled. For more information, see FortiAnalyzer Features on page 41.
	Device/VDOMs	The total number of devices and VDOMs connected to the FortiManager and the total number of device and VDOM licenses.
	GB/Day	The gigabytes per day of logs allowed and used for this FortiManager. Click the show details button to view the GB per day of logs used for the previous 6 days. FortiManager displays a warning after exceeding the quota for more than 7 days, and it is recommended that you review your daily logging or upgrade your license to accommodate the extra logs. The GB/Day log volume can be viewed per ADOM through the CLI using: `diagnose fortilogd logvol-adom <name>`.
Update Server		
	AntiVirus and IPS	The IP address and physical location of the Antivirus and IPS update server.

Web and Email Filter	The IP address and physical location of the web and email filter update server.
FortiClient Update	The IP address and physical location of the FortiClient update server.

Registering with FortiCloud

Register your device with FortiCloud to receive customer services, such as firmware updates and customer support.



To view a list of registered devices, go to the Fortinet Technical Support site (https://support.fortinet.com/), and use your FortiCloud credentials to log in. Go to *Asset* > *Manage/View Products*.

See also Activating VM licenses on page 22.

To register a FortiManager device:

1. Go to *Dashboard*.
2. In the *License Information* widget, click *Register Now* for FortiCloud.
   The registration dialog opens.
3. Enter the device details.
4. Click *OK*. FortiManager connects to FortiCloud and registers the device.
   A confirmation message appears at the top of the content pane, and the *Status* field changes to *Registered*.

Activating add-on licenses

If you have purchased an add-on license and have a FortiCloud account, you can use the *License Information* widget to activate an add-on license. You will need the contract registration code to activate the license.

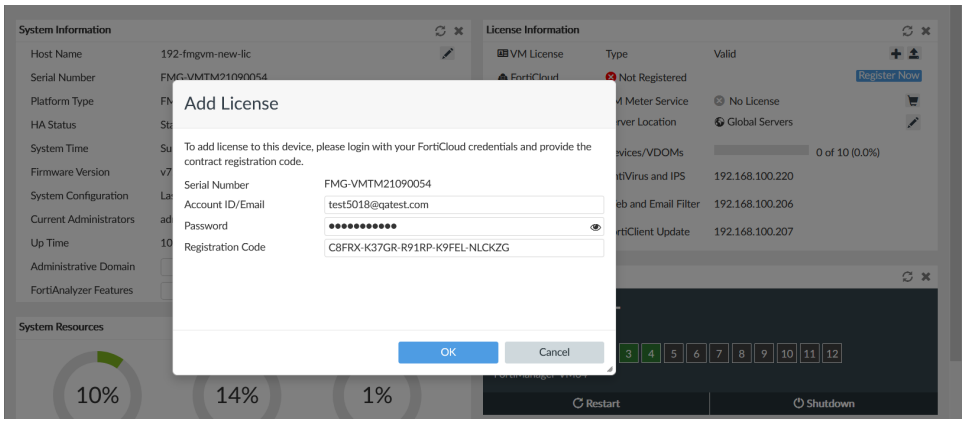
After you enter the contract registration code for the license, FortiManager communicates with FortiCloud to activate the license.

To purchase a new license:

1. Go to the FortiCloud.
2. Log in by using your FortiCloud account credentials.
3. Purchase a license.
   You will receive an email from Fortinet with a PDF attachment that includes a contract registration code.

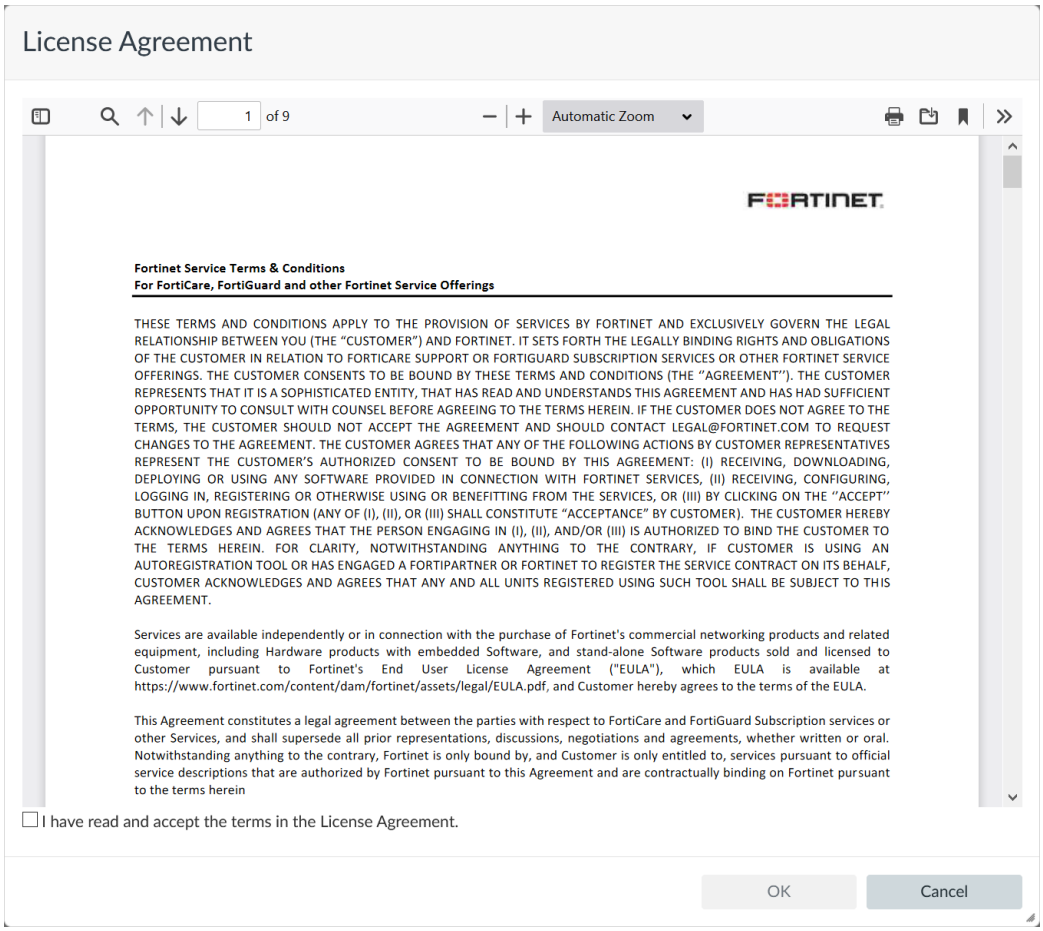
To add a license:

1. Go to *Dashboard*.
2. In the *License Information* widget, beside the *VM License* option, click the *Add License* button.
   The *Add License* dialog box is displayed.



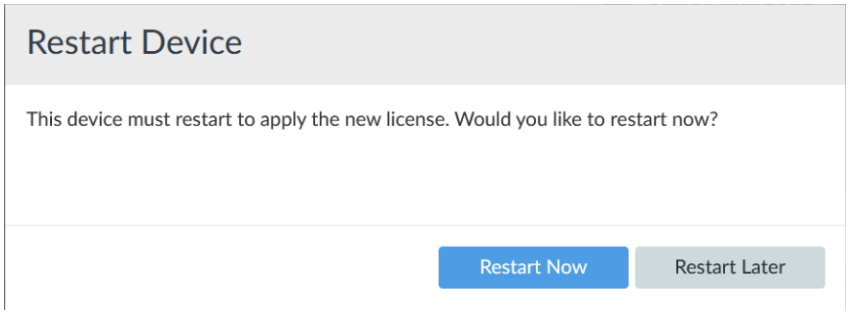
3. Complete the following options, and click *OK*:
   a. In the *Account ID/Email* box, type the email for your FortiCloud account.
   b. In the *Password* box, type the password for your FortiCloud account.
   c. In the *Registration Code* box, enter the contract registration code for the add-on license.

   The *License Agreement* is displayed.



4. Accept the license agreement:
   a. Read the license agreement.
   b. Select the *I have read and accept the terms in the License Agreement* checkbox.
   c. Click *OK*.

The *Restart Device* dialog box is displayed.



5. Click *Restart Now* to apply the license.
   FortiManager restarts, and the license is applied.
6. Go to *Dashboard > License Information* widget.
   The *VM License* option displays *Valid <license name>*.

Understanding license count rules

License count rules for FortiManager-VM, Cloud (Fortinet, Azure, or AWS), and Hardware:

- VDOM disabled: 1 FortiGate = 1 license.
- VDOM enabled: 1 VDOM = 1 license.

Excluded VDOMs

- The Global VDOM is not included in the license count.
- *Admin* type VDOMs are not included in the license count. Only *Traffic* type VDOMs are counted.

- VDOM enabled but no VDOMs: root = 1 license.
- FortiGate in HA mode: No license count for secondary FortiGate.
- Unregistered device in root ADOM: 1 unregistered device = 1 license. Hidden devices are not counted.
- FortiGate with FMGC entitlement: FortiManager-VMs *do not* include FortiGate devices with FMGC entitlements in the license count. FortiManager hardware devices (for example, FortiManager 3900E) *do* include FortiGate devices with FMGC entitlements in the license counts.
- FortiAnalyzer managed by FortiManager: FortiAnalyzer is added to the device count. In addition, FortiManager and FortiAnalyzer synchronize the ADOM device list with each other, and synchronized devices are included in the license count on each of FortiManager and FortiAnalyzer

FortiAP, FortiSwitch, and FortiExtender are not included in the license count. For more information see the Fortinet Product Matrix.

License expiration

This topic explains what occurs when a license used on FortiManager has expired.

You can see the current status of FortiManager licenses in the license information widget. See License Information widget on page 76.

License type		Expiration impact
FortiManager VM		
	Trial License (Evaluation)	Expiration impact not applicable. The trial license is free, limited, and non-expiring. It is available with a FortiCare account. Only one free trial per product, per account, can be active at a time. For more information, see the FortiManager VM Trial License Guide.
	VMS (Subscription)	FortiManager can no longer manage devices or provide update services.
	VM (Perpetual)	Expiration impact not applicable. The perpetual license does not expire.
FortiCare Support		FortiCare services included with *FortiCare Elite* or *FortiCare Premium* are suspended, including *Firmware & General Updates*, *Enhanced Support* coverage, and object updates from FortiGuard.
	Firmware & General Updates `FMWR`	Firmware upgrades are suspended.
	Enhanced Support `ENHN`	Access to FortiCare support services are suspended. FortiCare support is included as part of either your FortiCare Premium or FortiCare Elite subscription.

The table below displays the name of the licenses as found in FortiCare and the FortiManager GUI and CLI.

FortiCare	License Information widget	CLI*
VM License	VMS License	VMLS VM license
ADOM Subscription**	ADOM License**	Not visible
Enhanced Support	Not visible	ENHN Enhanced Support
Firmware & General Updates	Not visible	FMWR Firmware & General Updates
Telephone Support	Not visible	COMP Telephone Support
Hardware Coverage	Not visible	Not visible

*The licenses can be viewed in the FortiManager CLI using the following commands:

- `diagnose fmupdate dbcontract`

** Only displayed for the subscription VM license type. This option is not visible for perpetual licenses.

License expiration dates are different when viewed from the FortiManager (GUI or CLI) or from FortiCloud. This occurs for the following reasons:

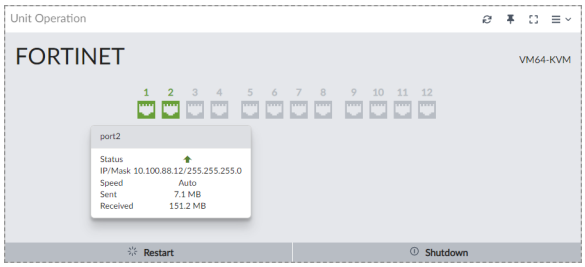
- FortiCloud displays the actual contract expiration date.
- The FortiManager GUI/CLI displays the expiration date including a 3 day grace period. The grace period is designed to prevent service disruption.

To avoid any risk of service disruption, always plan to renew licenses before the actual expiration date shown in FortiCloud. This ensures continuous entitlement coverage and uninterrupted functionality across all licensed services.

Unit Operation widget

The *Unit Operation* widget graphically displays the status of each port. The port name indicates its status by its color. Green indicates the port is connected. Grey indicates there is no connection.

Hover the cursor over the ports to view a pop-up that displays the full name of the interface, the IP address and netmask, the link status, the speed of the interface, and the amounts of sent and received data.

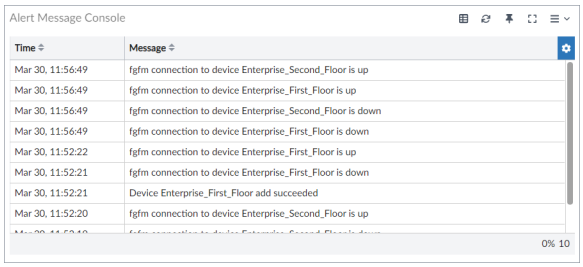


Alert Messages Console widget

The *Alert Message Console* widget displays log-based alert messages for both the FortiManager unit itself and connected devices.

Alert messages help you track system events on your FortiManager unit such as firmware changes, and network events such as detected attacks. Each message shows the date and time the event occurred.

Alert messages can also be delivered by email, syslog, or SNMP.



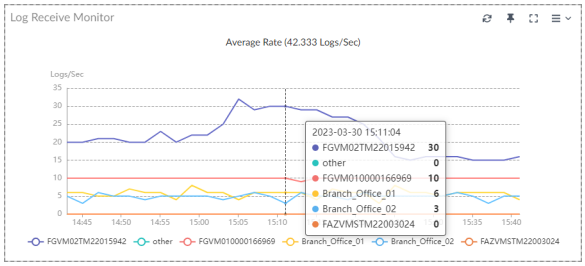
Click *Edit* from the widget toolbar to view the *Alert Message Console Settings*, where you can adjust the number of entries that are visible in the widget, and the refresh interval.

To view a complete list of alert messages, click *Show More* from the widget toolbar. The widget will show the complete list of alerts. To clear the list, click *Delete All Messages*. Click *Show Less* to return to the previous view.

Log Receive Monitor widget

The *Log Receive Monitor* widget displays the rate at which the FortiManager unit receives logs over time. Log data can be displayed by either log type or device.

Hover the cursor over a point on the graph to see the exact number of logs that were received at a specific time. Click the name of a device or log type to add or remove it from the graph. Click *Edit* in the widget toolbar to modify the widget's settings.





This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see FortiAnalyzer Features on page 41.

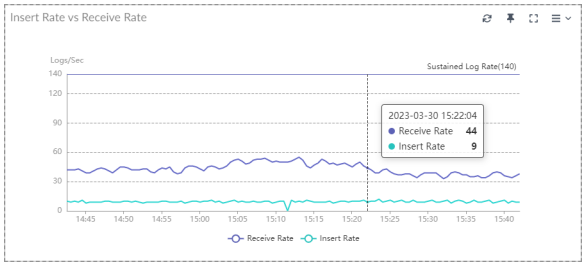
Insert Rate vs Receive Rate widget

The *Insert Rate vs Receive Rate* widget displays the log insert and log receive rates over time.

- Log receive rate: how many logs are being received.
- Log insert rate: how many logs are being actively inserted into the database.

If the log insert rate is higher than the log receive rate, then the database is rebuilding. The lag is the number of logs waiting to be inserted.

Hover the cursor over a point on the graph to see the exact number of logs that were received and inserted at a specific time. Click *Receive Rate* or *Insert Rate* to remove those data from the graph. Click the edit icon in the widget toolbar to adjust the time interval shown on the graph and the refresh interval.

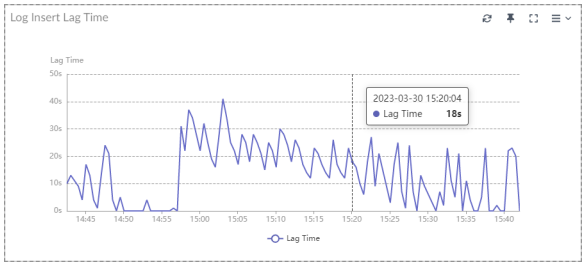


This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see FortiAnalyzer Features on page 41.

Log Insert Lag Time widget

The *Log Insert Lag Time* widget displays how many seconds the database is behind in processing the logs.

Click the edit icon in the widget toolbar to adjust the time interval shown on the graph and the refresh interval (0 to disable) of the widget.

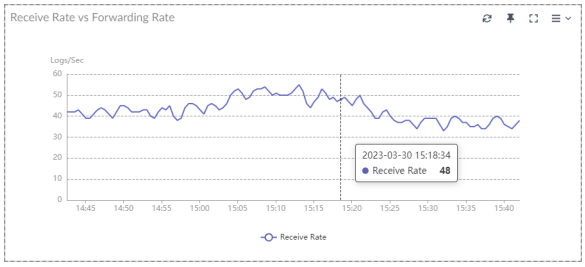


This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see FortiAnalyzer Features on page 41.

Receive Rate vs Forwarding Rate widget

The *Receive Rate vs Forwarding Rate* widget displays the rate at which the FortiManager is receiving logs. When log forwarding is configured, the widget also displays the log forwarding rate for each configured server.

Click the edit icon in the widget toolbar to adjust the time period shown on the graph and the refresh interval, if any, of the widget.

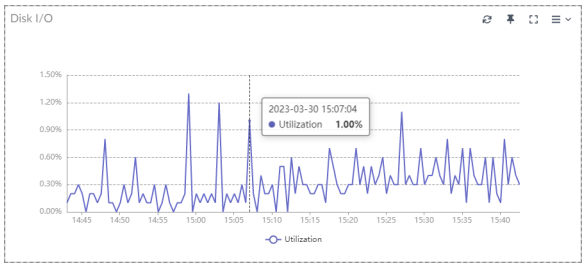


This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see FortiAnalyzer Features on page 41.

Disk I/O widget

The *Disk I/O* widget shows the disk utilization (%), transaction rate (requests/s), or throughput (KB/s), versus time.

Click the edit icon in the widget toolbar to select which chart is displayed, the time period shown on the graph, and the refresh interval (if any) of the chart.



This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see FortiAnalyzer Features on page 41.

Device widgets

The following widgets in the *Dashboard* provide a summary of the devices that are added and authorized in the FortiManager. These widgets link to other panes in the GUI, which provide more detailed information.

Click one of the following widgets to open *Device Manager* > *Device & Groups*. For more information, see Device & Groups on page 89.

- *Connectivity*
- *Device Config Status*
- *Policy Package Status*
- *Firmware Status*
- *FortiGuard License Status*

Click the following widget to open *Device Manager > Monitors > Asset Identity Center*. For more information, see Asset Identity Center on page 398.

- *Hardware Vendor*

Click the following widget to open *AP Manager > Managed FortiAPs*. For more information, see Managed FortiAPs on page 581.

- *FortiAP Status*

Click the following widget to open *FortiSwitch Manager > Managed FortiSwitches*. For more information, see Managed FortiSwitches on page 839.

- *FortiSwitch Status*

Click the following widget to open *Extender Manager > Managed Extenders*. For more information, see Managed extenders on page 889.

- *FortiExtender Status*

Restart, shut down, or reset FortiManager

Always use the operation options in the GUI or the CLI commands to reboot and shut down the FortiManager system to avoid potential configuration problems.

Restarting FortiManager

To restart the FortiManager unit from the GUI:

1. Go to *Dashboard*.
2. In the *Unit Operation* widget, click the *Restart* button.
3. Enter a message for the event log, then click *OK* to restart the system.

To restart the FortiManager unit from the CLI:

1. From the CLI, or in the *CLI Console* menu, enter the following command:
```
execute reboot
The system will be rebooted.
Do you want to continue? (y/n)
```
2. Enter *y* to continue. The FortiManager system will restart.

Shutting down FortiManager

To shutdown the FortiManager unit from the GUI:

1. Go to *Dashboard*.
2. In the *Unit Operation* widget, click the *Shutdown* button.
3. Enter a message for the event log, then click *OK* to shutdown the system.

To shutdown the FortiManager unit from the CLI:

1. From the CLI, or in the *CLI Console* menu, enter the following command:
```
execute shutdown
The system will be halted.
Do you want to continue? (y/n)
```
2. Enter y to continue. The FortiManager system will shutdown.

Resetting system settings

FortiManager settings can be reset to factory defaults using the CLI.

To reset settings to factory defaults:

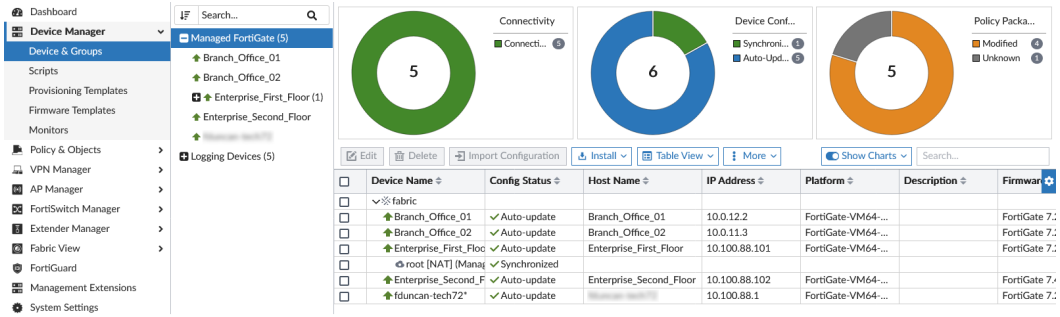
1. From the CLI, or in the *CLI Console* menu, enter the following command:
```
execute reset {adom-settings | all-except ip | all-settings | all-shutdown}
```

Variable	Description
`adom-settings <adom> <version> <mr> <ostype>`	Reset an ADOM's settings. • `<adom>`: The ADOM name. • `<version>`: The ADOM version. • `<mr>`: The major release number. • `<ostype>`: Supported OS type.
`all-except-ip`	Reset all settings except the current IP address and route information.
`all-settings`	Reset to factory default settings.
`all-shutdown`	Reset all settings and shutdown.

2. Enter y to continue. The device will reset settings based on the type of reset performed.
For example, `execute reset all-settings` will reset all FortiManager to factory defaults.

Device Manager

Use the *Device Manager* pane to add and authorize devices for management by FortiManager. You can also use the *Device Manager* pane to create device configuration changes and install device and policy package configuration changes to managed devices. You can also monitor managed devices from the *Device Manger* pane.



The *Device Manager* pane includes the following items in the tree menu:

Device & Groups	Add, configure, and view managed and logging devices. Use the toolbar to add devices, devices groups, and launch the install wizard. See Add devices on page 91. The *Device & Groups* tab also contains a quick status bar for a selected device group. See Using the quick status bar on page 149.
Scripts	Create new or import scripts. Scripts is disabled by default. You can enable this advanced configuration option in *System Systems > Settings*. Select *Show Script* to enable on this option in the *Device Manager* pane. See Scripts on page 239.
Provisioning Templates	Configure provisioning templates. For information on system, Threat Weight, FortiClient, and certificate templates, see Provisioning Templates on page 273.
Firmware Templates	Configure templates for upgrading firmware on FortiGates and all access devices, such as FortiAP, FortiSwitch, and FortiExtender. See Firmware templates on page 378.
Monitors	Monitor traffic for all SD-WAN networks. See SD-WAN Monitor on page 386. Monitor traffic for all VPN communities. See VPN Monitor on page 396.
Chassis devices	Add, configure, and monitor chassis devices. See FortiGate chassis devices on page 401.

When you select a tree menu item, the toolbar and the content pane change to reflect your selection.

Additional configuration options and short-cuts are available using the right-click content menu. Right-click different parts of the navigation panes on the GUI page to access these context menus.



If workspace or workflow is enabled, the ADOM must be locked before changes can be made. See Locking an ADOM on page 947.

ADOMs

You can organize connected devices into ADOMs to better manage the devices. ADOMs can be organized by:

- Firmware version: group all 7.0 devices into one ADOM, and all 7.2 devices into another.
- Geographic regions: group all devices for a specific geographic region into an ADOM, and devices for a separate region into another ADOM.
- Administrator users: group devices into separate ADOMs based for specific administrators responsible for the group of devices.
- Customers: group all devices for one customer into an ADOM, and devices for another customer into another ADOM.
  FortiAnalyzer, FortiCache, FortiClient, FortiDDos, FortiMail, FortiManager, FortiSandbox, FortiWeb, Chassis, and FortiCarrier devices are automatically placed in their own ADOMs.

Each administrator profile can be customized to provide read-only, read/write, or restrict access to various ADOM settings. When creating new administrator accounts, you can restrict which ADOMs the administrator can access, for enhanced control of your administrator users. For more information on ADOM configuration and settings, see Administrative Domains (ADOMs) on page 924.



For information on adding devices to an ADOM by using the *Add Device* wizard, see Adding online devices using Discover mode on page 92.

Device & Groups

On the *Device Manager* pane, use the *Device & Group* tree menu to access options for adding devices to FortiManager and authorizing them for management. After the device is managed, you can use the *Device & Group* pane to monitor managed devices, install and manage configurations, as well as access the device database for each managed device.

The *Device & Group* pane includes the following options in the banner:

Add Device	Click *Add Device* to display the *Add Device* wizard. With the wizard, you can add an online device, add an offline device, add an HA cluster, and import offline devices from a CSV file. Zero-touch provisioning is supported. See Add devices on page 91.

	Click the dropdown menu next to *Add Device* in the toolbar to see additional options including *Add FortiAnalyzer* and *Device Blueprint*. See Add FortiAnalyzer or FortiAnalyzer BigData on page 134 or Using device blueprints for model devices on page 114. You can also add VDOMs to FortiGates. See Add VDOM on page 145.
Device Group	Click *Device Group* to create groups that you can use to organize managed devices. See Device groups on page 147.
Install Wizard	Click *Install Wizard* to display the *Install* wizard. With the wizard, you can install policy packages and device settings to managed devices. Alternately, you can install only device settings. See Install wizard on page 180.

The default view for the *Device Manager > Device & Groups* pane is *Table View*. See Table view on page 148.

Under the banner in *Table View* is a quick status bar for all managed devices. See Using the quick status bar on page 149.

In *Table View*, a tree menu of device groups and devices displays on the left side of the pane. Managed devices are organized into groups. Select a group, such as *Managed FortiGates*, to hide and display the FortiGates in the group. The devices in a group are displayed in the left tree menu and in the content pane:

- In the left tree menu, click a device to display the device database. See Displaying the device database on page 194.
- In the content pane, click a device to use options in the toolbar on *Table View*.

The toolbar for *Table View* contains the following options:

Edit	In the content pane, select a device, and click *Edit* to edit device information. See Editing device information on page 153.
Delete	In the content pane, select a device, and click *Delete* to remove the device from FortiManager management.
Import Configuration	In the content pane, select a device, and click *Import Configuration* to start the *Import Device* wizard. See Import Configuration wizard on page 173.
Install	In the content pane, select a device, and from the *Install menu* menu, select one of the following options: • *Install Wizard* • *Quick Install (Device DB)* • *Re-install Policy*
Table View	Click the *Table View* menu to choose the view format for managed devices. Choose from the following options: • *Table View* • *Map View* • *Ring View* • *Folder View*
More	In the content pane, select a device, and from the *More* menu, select one of the following options: • *Refresh Device* • *Configuration*

	• *Add VDOM* • *Firmware Upgrade* • *Grouping* • *Run Script* • *Swap Device* • *Enable Auto-link* • *Disable Auto-link*
Full Screen/Exit Full Screen	Click to toggle full screen mode for the device table.
Show Charts	Click the toggle to enable/disable charts in the Devices & Groups pane. Select the dropdown to choose which charts are displayed.
Column Settings	From the *Column Settings* menu, select what columns to display for *Table View*.

You can right-click on a selected managed device to see options in the context menu. The right-click context menu includes the following additional options.

Remote Access	Remotely access the selected FortiGate device.
Policy Package Diff	View a diff on the policy package for the selected device.
Edit Variable Mapping	Edit the variable mappings for the selected device.
Fabric Topology	View the topology for Fabric devices.
Install VM License	Select to open the Install VM License wizard which includes options to install a BYOL VM license, or install a license from a FortiFlex connector. See Installing VM licenses on managed devices on page 159.

Add devices

In FortiManager, you must add devices to *Device Manager* and authorize the devices for management before you can manage them.

On the managed device, you must also enable *Central Management* to allow FortiManager to manage the device.

You can use the *Add Device* wizard to add the following devices:

- Online or offline devices
- Online or offline FortiGate HA clusters
- Security Fabric group

Another method is to import detected devices to FortiManager for management.

You can also configure a device to request management by FortiManager. These devices appear on the *Device Manager* pane in the unauthorized device list. For example, you can configure a FortiGate to be managed by FortiManager, and the FortiGate device is displayed in the unauthorized device list in FortiManager.

Adding a VM device



By default, FortiManager will not recognize the serial numbers of the following VM devices:

- FortiGate-VM
- FortiCarrier-VM
- FortiProxy-VM
- FortiFirewall-VM
- FortiAnalyzer-VM

When adding a VM device to FortiManager, you must first enable the recognition of VM serial numbers. See Adding VM devices on page 118.

Adding online devices using Discover mode

The following steps describe how to add an online device by using the *Add Device* wizard and *Discover* mode.



For FortiGates, you can use the new authorization method described in this topic with FortiOS 7.0.0 and later. If FortiGate is running FortiOS 6.4.x and earlier, the wizard automatically switches to the legacy login. See also Adding online devices using Discover mode and legacy login on page 104.

For FortiAnalyzer, you cannot use the *Add Device* wizard to add FortiAnalyzer to FortiManager. You must use the *Add FortiAnalyzer* wizard instead. See Add FortiAnalyzer or FortiAnalyzer BigData on page 134.

Use the *Discover* option for devices that are currently online and discoverable on your network. When the wizard completes, the device is added to FortiManager and authorized.

Adding an online device does not result in an immediate connection to the device. Device connection happens only when you successfully synchronize the device.

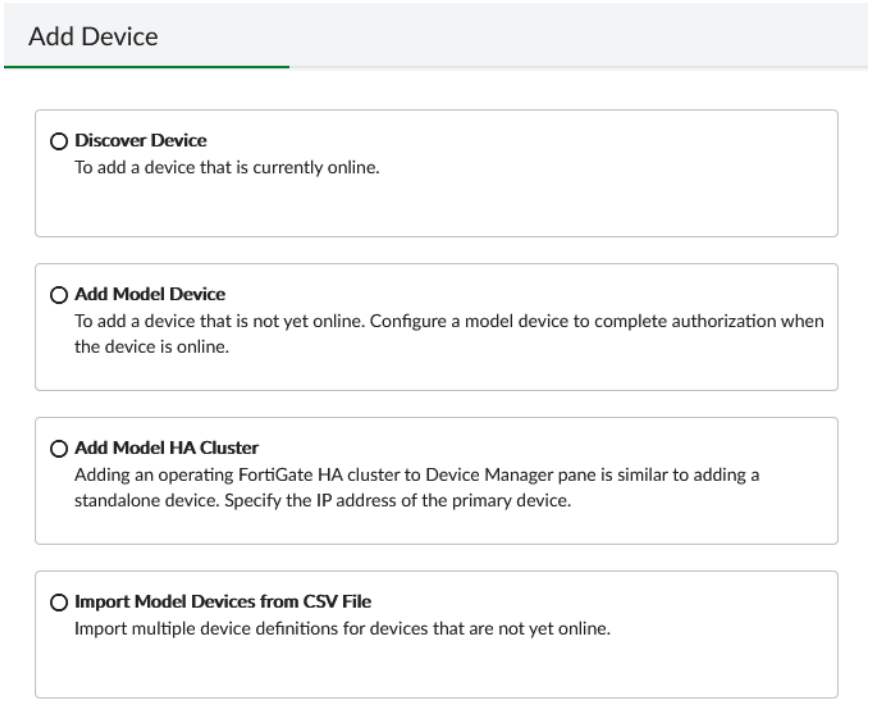


FortiManager cannot communicate with FortiGate when offline mode is enabled. Enabling offline mode prevents FortiManager from discovering devices.

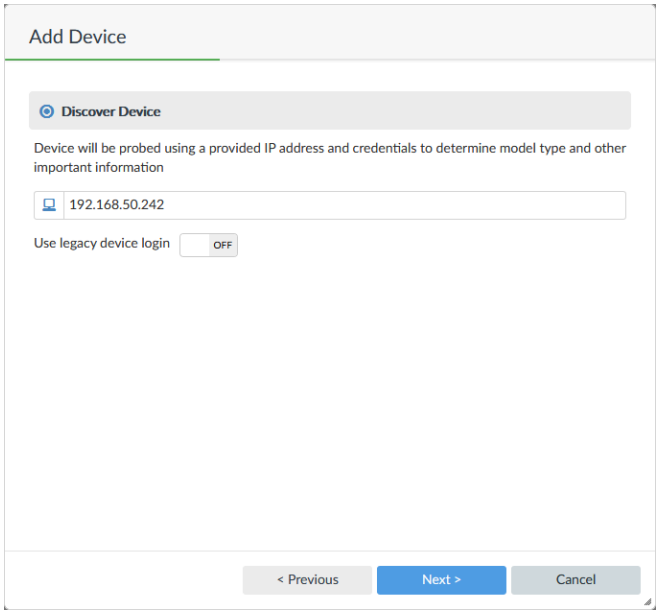
To add a device using Discover mode:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager* > *Device & Groups*.

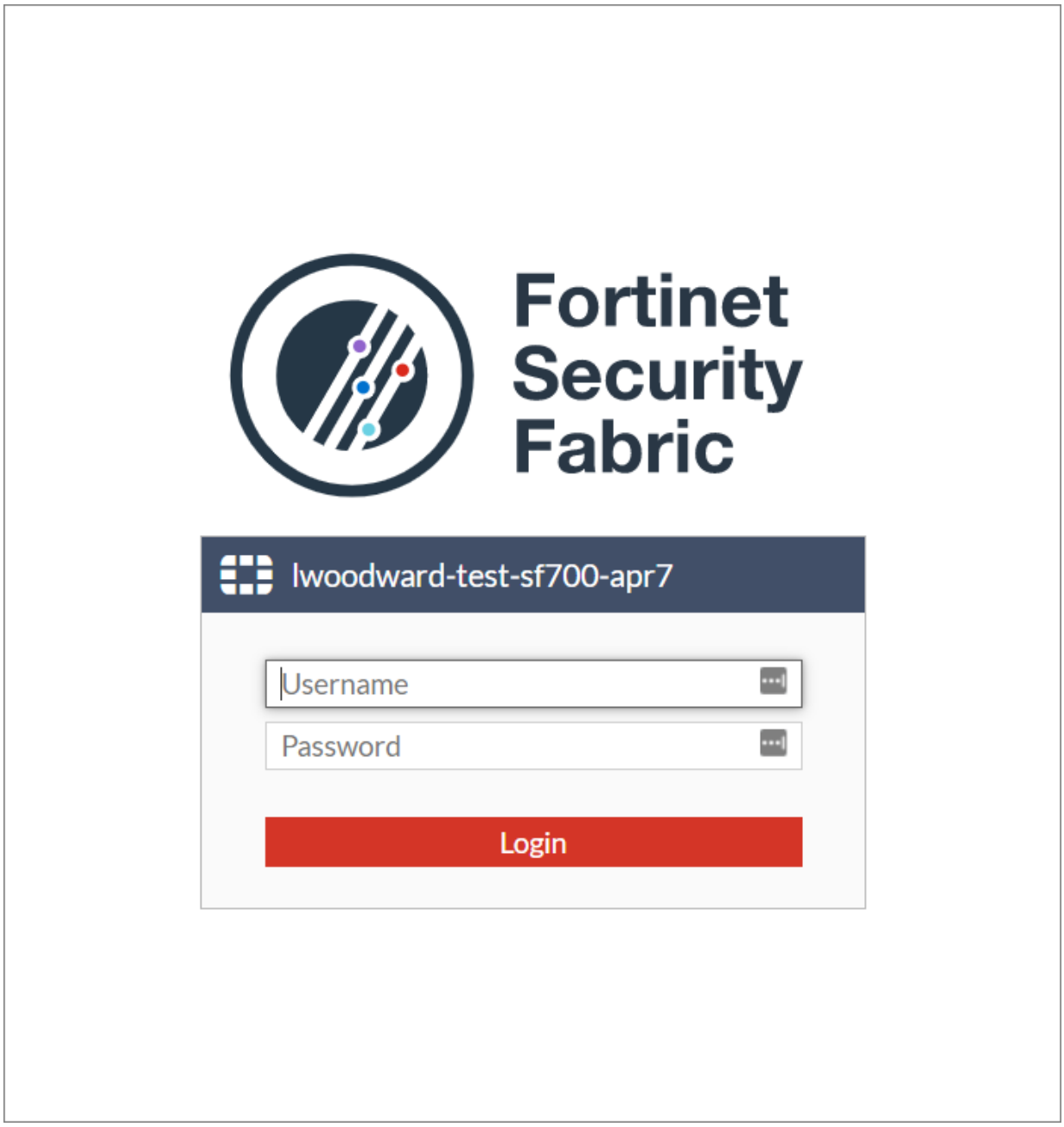
3. Click *Add Device*. The wizard opens.



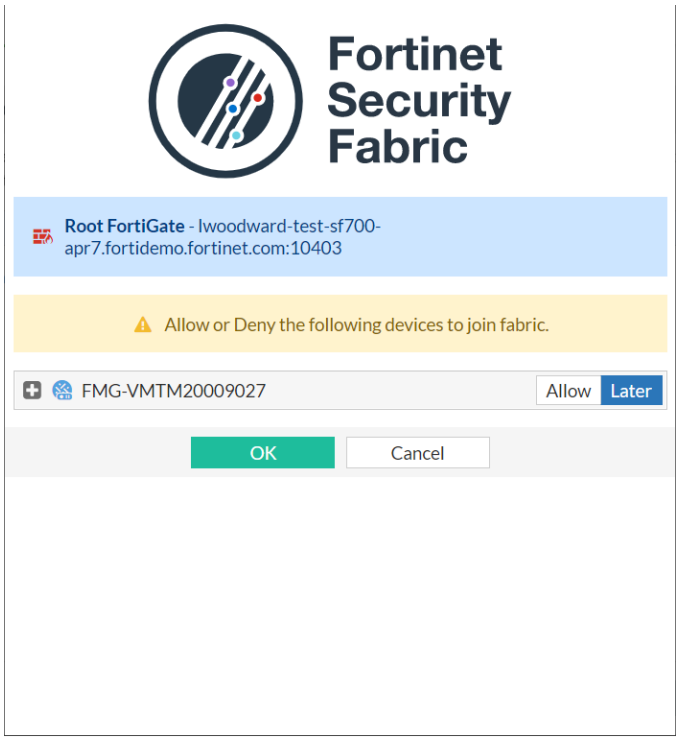
4. Discover and authorize the device for management by FortiManager:
   a. Select *Discover Device*.
   b. In the box, type the management port IP address for the device, and click *Next*.
   If you are adding a FortiGate running FortiOS 6.4.x or earlier, the wizard automatically switches to legacy device login where you also type the username and password for the device in the wizard.



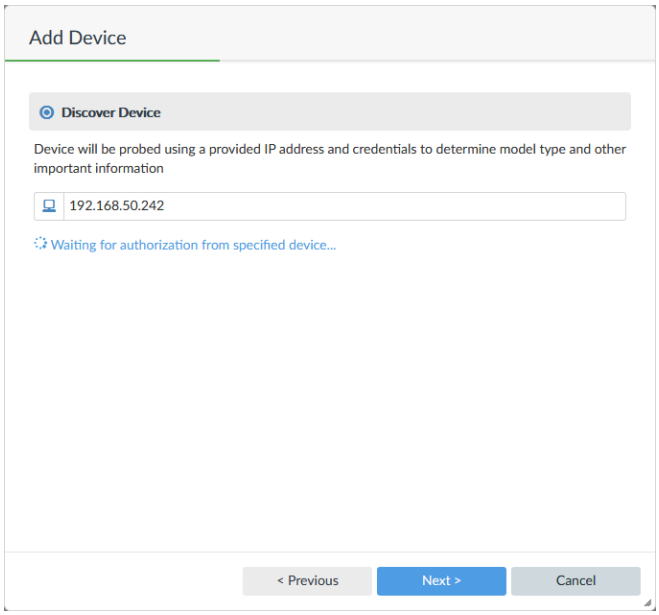
   A login window for the device is displayed. If the login window is not displayed, see Security Fabric authorization on page 101.



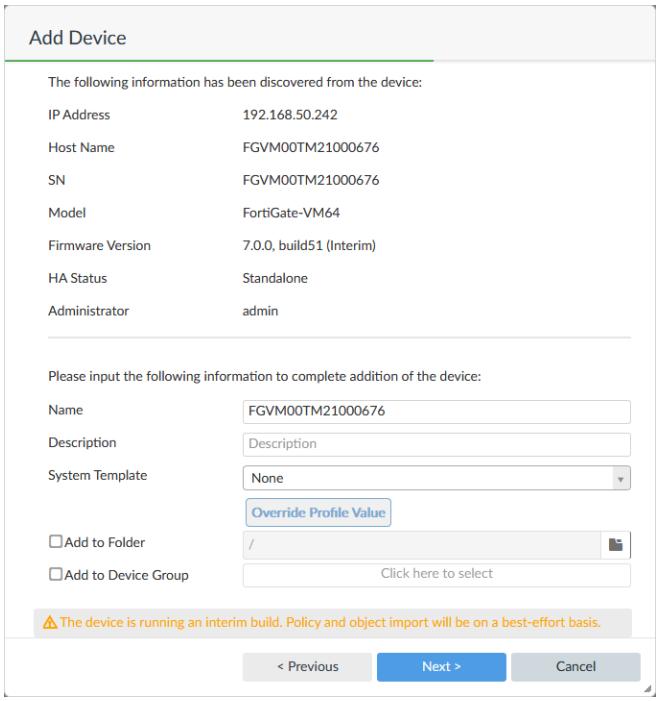
c. Type the username and password for the device, and click *Login*.
An authorization request window for the device is displayed.



d. Click *Allow*, and then *OK* to authorize management by FortiManager. Authorization proceeds, and the device discovery process is initiated.



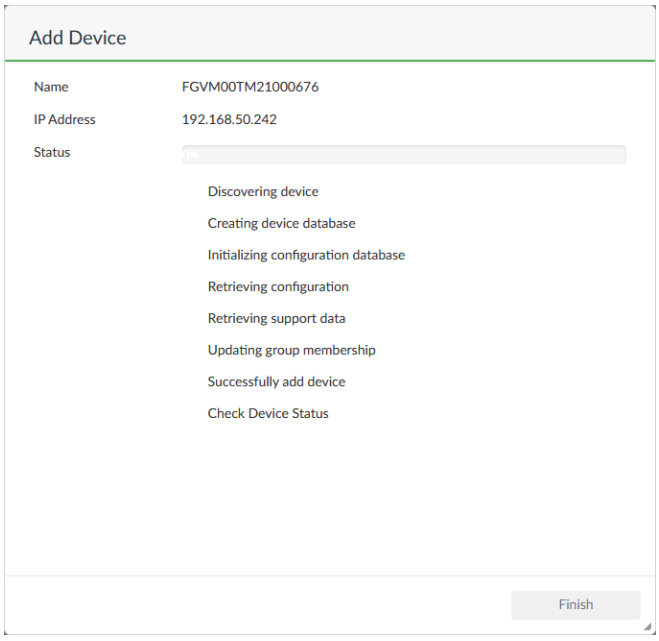
After the device discovery process completes, the following page of information is displayed.


Add Device
The following information has been discovered from the device:
IP Address
192.168.50.242
Host Name
FGVM00TM21000676
SN
FGVM00TM21000676
Model
FortiGate-VM64
Firmware Version
7.0.0, build51 (Interim)
HA Status
Standalone
Administrator
admin
Please input the following information to complete addition of the device:
Name
FGVM00TM21000676
Description
Description
System Template
None
Override Profile Value
Add to Folder
/
Add to Device Group
Click here to select
The device is running an interim build. Policy and object import will be on a best-effort basis.
< Previous
Next >
Cancel

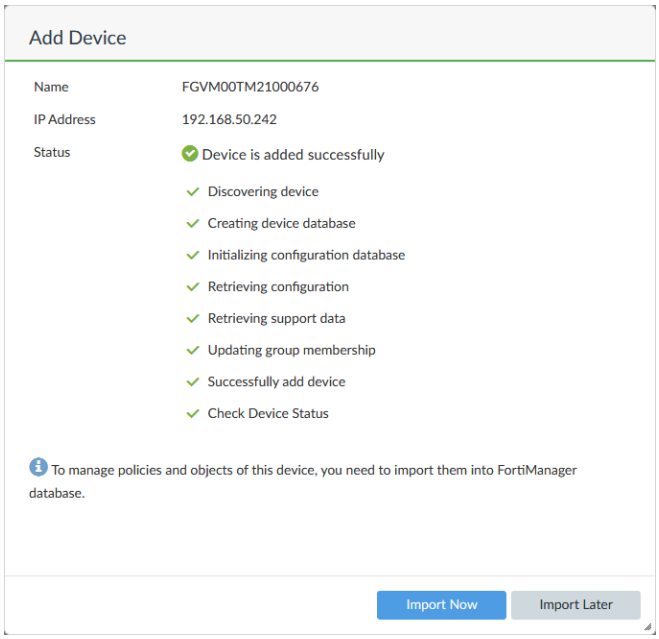
5. Configure the following settings, and click *Next*:

Name	Type a unique name for the device. The device name cannot contain spaces or special characters.
Description	Type a description of the device (optional).
System Template	System templates can be used to centrally manage certain device-level options from a central location. If required, assign a system template using the dropdown menu. Alternatively, you can configure all settings per-device inside *Device Manager*. For more information, see Provisioning Templates on page 273.
Override Profile Value	After selecting a system template, click to override values in the template.
Add to Folder	Select to add the device to any predefined folders.
Add to Device Group	Select to add the device to any predefined groups.
Copy Device Dashboard	Select a device to copy custom device dashboards from (optional). For more information about dashboards in the device database, see Device DB - Dashboard on page 199.

More information about the device is checked.

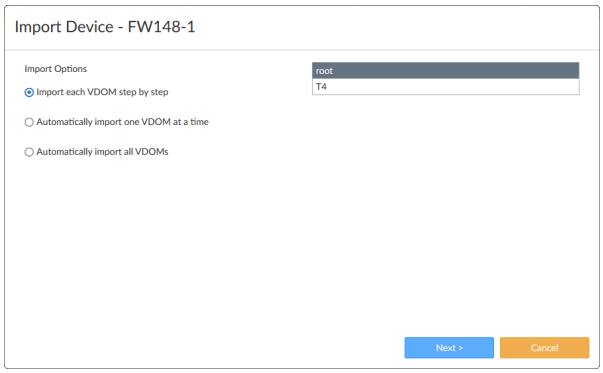


After the wizard completes the checks, you are asked to choose whether to import policies and objects for the device now or later.



6. Click *Import Later* to finish adding the device and close the wizard.
   If you click *Import Now*, the wizard continues. The next step in the wizard depends on whether you are importing a FortiGate VDOM.

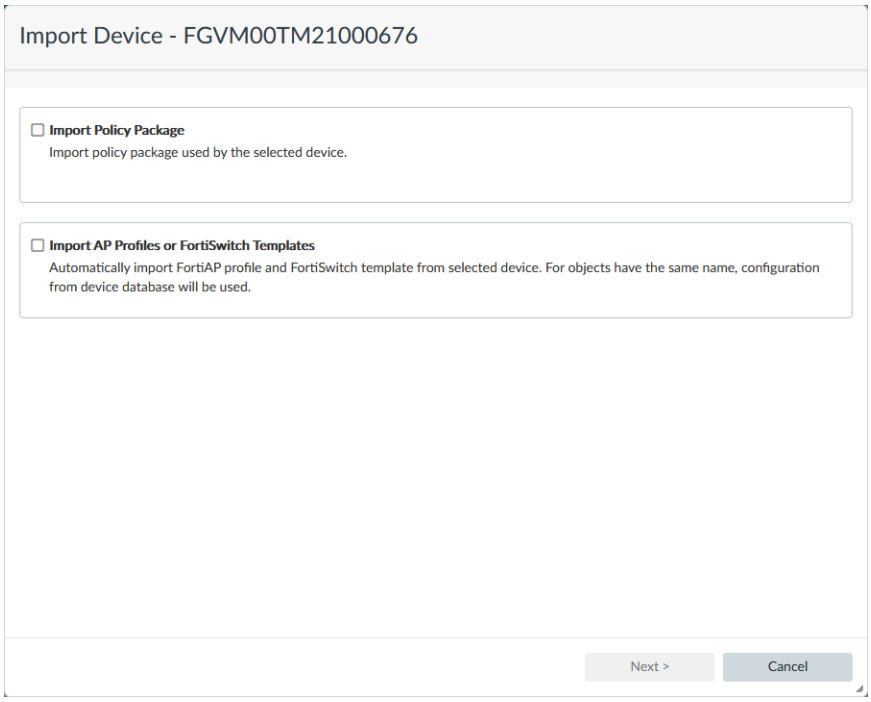
   If you are importing a FortiGate VDOM, the following page is displayed with import options for the VDOM. Select an option, and click *Next*.



If you select *Automatically import one VDOM at a time* or *Automatically Import all VDOMs*, conflict detection for objects will not be performed. If there are conflicting objects between FortiGate and FortiManager, the objects on FortiManager will be overwritten by the objects on FortiGate.

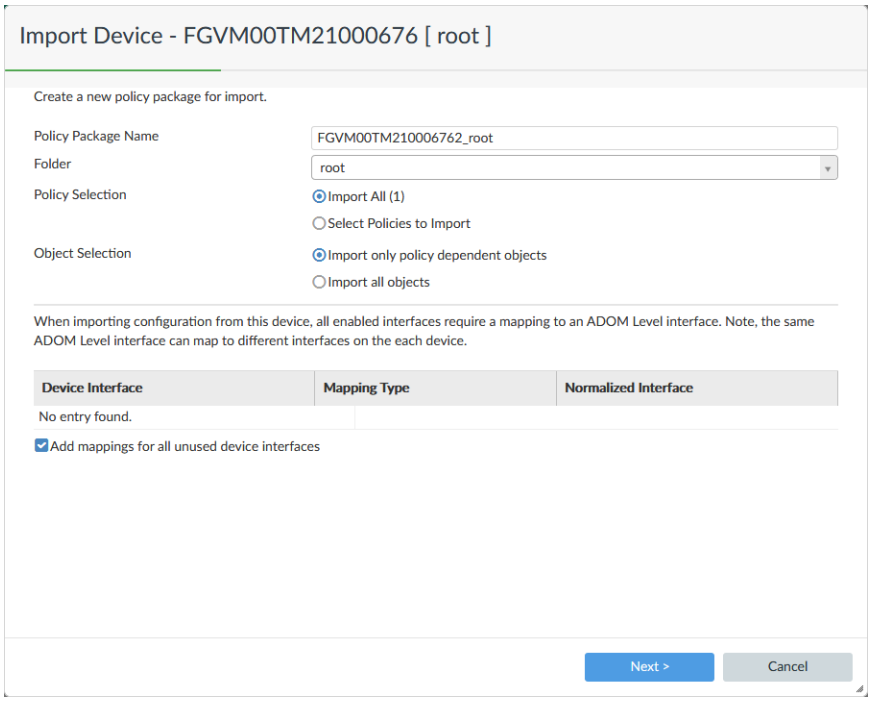
For more information, see What to do when an object conflict occurs in the FortiManager Best Practices guide.

If you are not importing a FortiGate VDOM, the following page is displayed.



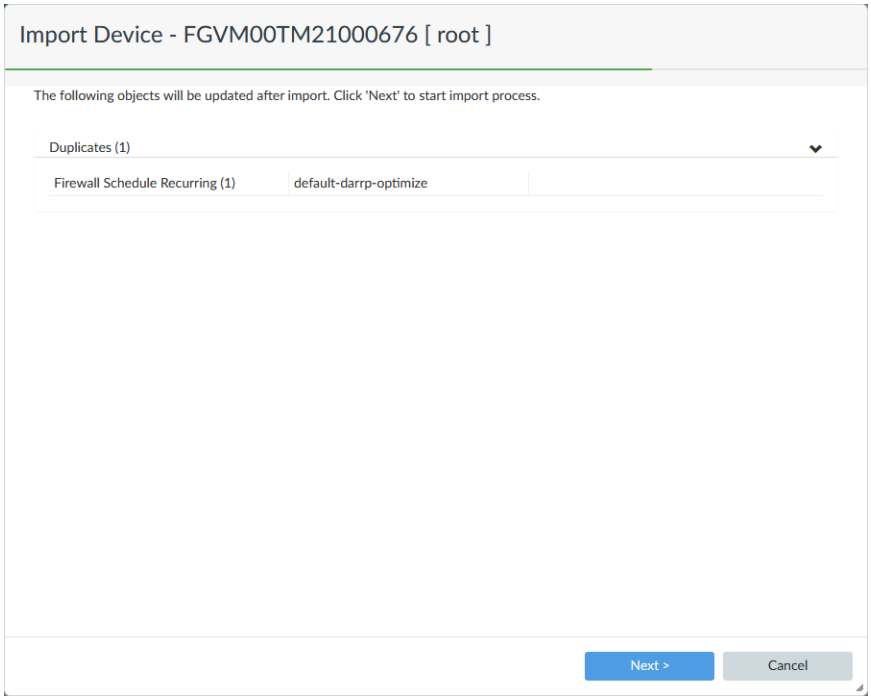
7. Set the following options, and click *Next*:
   a. Select *Import Policy Package*.
   b. If you have FortiAP and/or FortiSwitch units connected to the device, select *Import AP Profiles or FortiSwitch Templates*.

   The *Import Device* page is displayed.

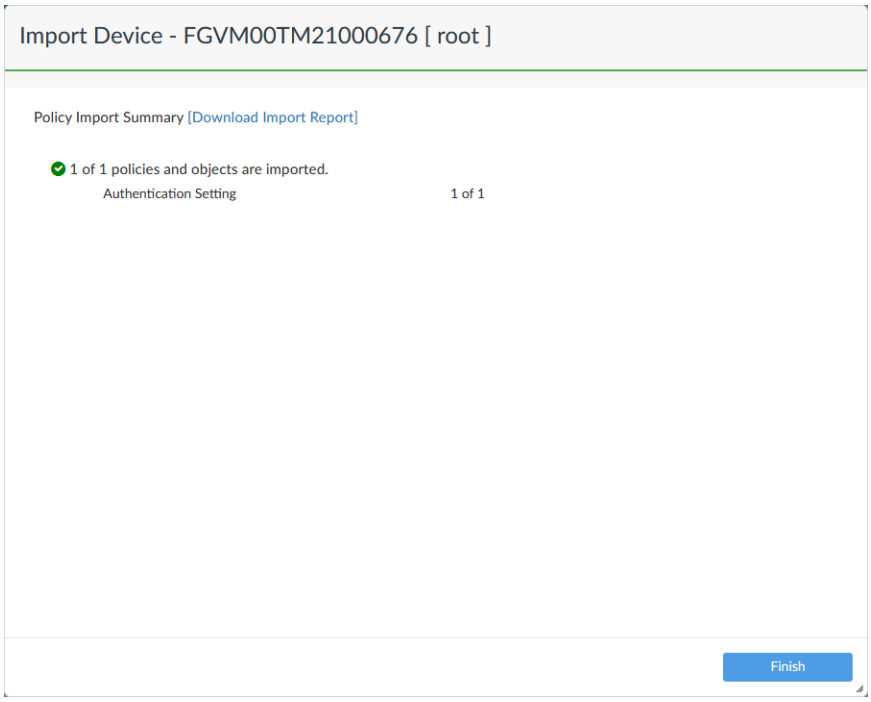


8. Set the following options, then click *Next*:
   a. In the *Policy Selection* section, select *Import All* or *Select Policies and Profile Groups to Import*.
   b. In the *Object Selection* section, select *Import only policy dependent objects* or *Import all objects*.
   c. Check the device interface mappings.
   d. Select or clear the *Add mappings for all unused device interfaces* checkbox.

   The list of objects that will be updated is displayed.



9. Click *Next*.
   A detailed summary of the import is shown. Click *Download Import Report* to download a report of the import. The report is only available on this page.



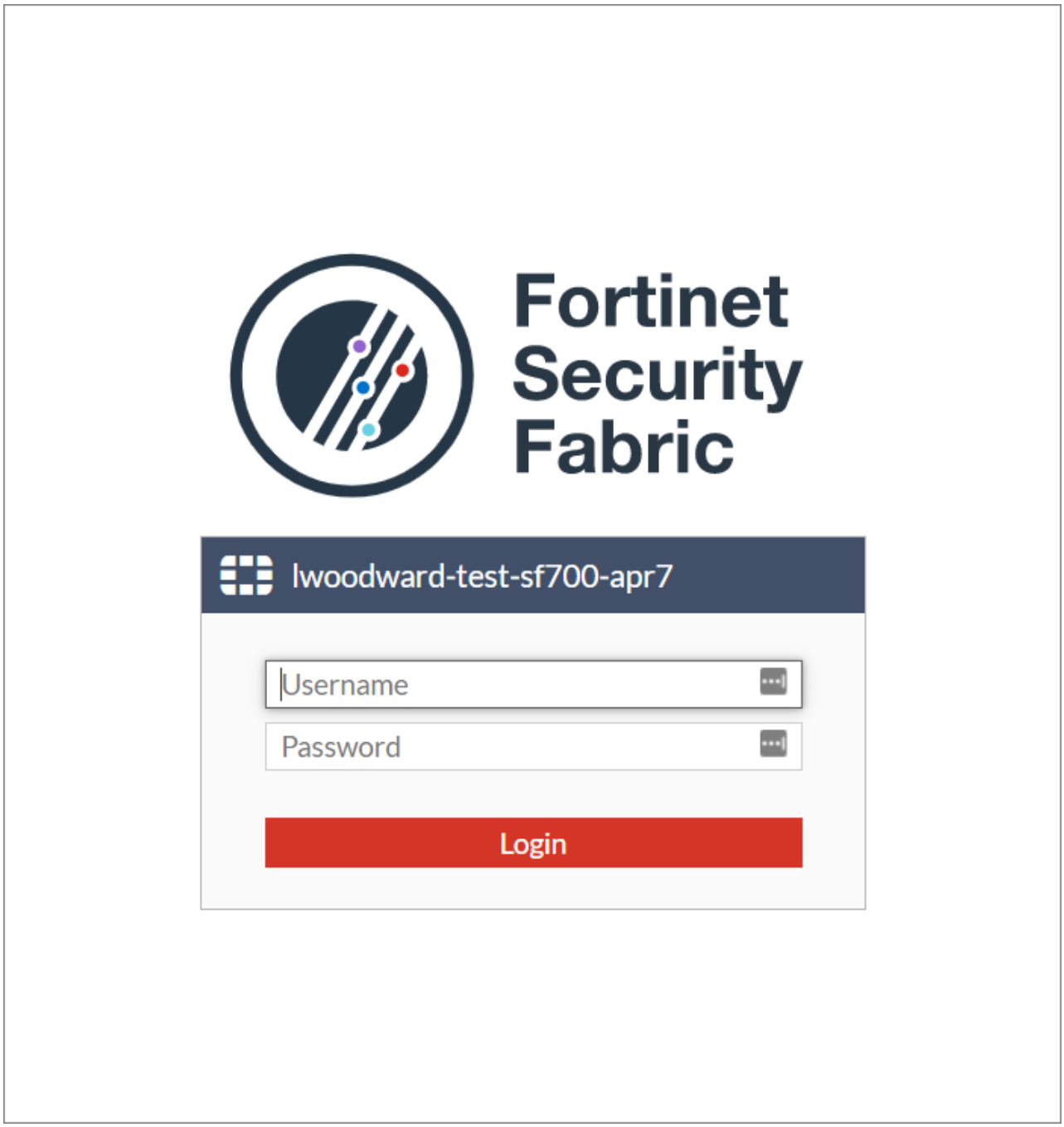
10. Click *Finish* to finish adding the device and close the wizard.

Security Fabric authorization

With FortiManager and FortiOS 7.0.0 and later, the *Add Device* wizard and *Discover* mode can use the OAUTH protocol for the authorization step. This topic describes how the authorization step works when the OATH protocol is used. You are not required to use the new authorization method, you can choose to use the legacy login method instead, which does not use the OAUTH protocol.

You can add an online device to FortiManager by using the *Add Device* wizard and *Discover* mode. You type in the IP address of the management port for the FortiGate, and press *Next*. At this stage of the wizard, the following actions occur:

1. FortiManager connects to the online FortiGate.
2. A browser popup window is displayed to let you log in to FortiGate as part of the authorization process:



When FortiManager connects to FortiGate, it retrieves the following settings from FortiOS that define the accessible FQDN or IP address and port for FortiOS:

```
config system global
   set management-ip
   set management-port
```

In FortiOS, you can also view the management IP and management port in the GUI. Go to *Security Fabric > Fabric Connectors > Security Fabric Setup*.

FortiManager provides the settings to the browser popup window for connection to FortiGate.

If no FortiOS settings are defined, both FortiManager and the browser popup window use the IP address of the management port and the default HTTPS port for connection to FortiGate.

If FortiManager cannot access the management IP and/or default HTTPS port for the FortiGate the wizard fails, and you must specify an accessible management IP on FortiGate before starting the *Add Wizard* again.

In some cases FortiManager can access FortiGate, but the browser popup window cannot. For example, if FortiGate uses NAT, FortiManager can access the internal IP address for FortiGate and establish connection. However the browser popup window cannot access the internal IP address for the FortiGate, and the authentication connection fails. You can workaround this problem by specifying an accessible management IP address and port on FortiOS.

As an alternate to specifying the accessible management IP and port for FortiOS, you can use the legacy login for the *Add Device* wizard with *Discover* mode. If you are adding a FortiGate running FortiOS 6.4.x and earlier, you must use the legacy login. See Adding online devices using Discover mode and legacy login on page 104.

Topologies that do and do not require management IP address and/or port

This section includes examples of topologies that don't and do require you to specify an accessible management IP address for FortiOS to enable browser authorization communication:

- Same subnet on page 103
- NAT on page 103
- Non-default port on page 103

Same subnet

You are not required to set specify an accessible management IP address for FortiOS when:

- FortiGate is directly connected to FortiManager.
- FortiGate and FortiManager use the same subnet.
- FortiOS is using the default management HTTPS port.

In this scenario, you can use the *Add Device* wizard with the IP address of the management port for the FortiGate, and the browser can access the IP address. Authorization communication proceeds.

NAT

When using NAT, the following scenarios require you to specify an accessible management IP address for FortiOS:

- FortiGate is behind NAT with VIP.
- FortiManager and FortiGate are behind NAT in the same network.

In these cases, specify the FortiOS virtual public IP (VIP) as the accessible management IP address. After configuration, FortiManager can retrieve the information to enable authentication communication.

Non-default port

The default management HTTPS port for FortiGate is 443. If you are using a custom port, you must specify the custom port used by FortiGate.

For example, when FortiGate uses HTTPS port 8443 instead of 443, you must use the following command on FortiOS to configure the non-default port:

```
config system global
   set management-port 8443
```

After configuration, FortiManager can retrieve the information to enable authentication communication.

Adding online devices using Discover mode and legacy login

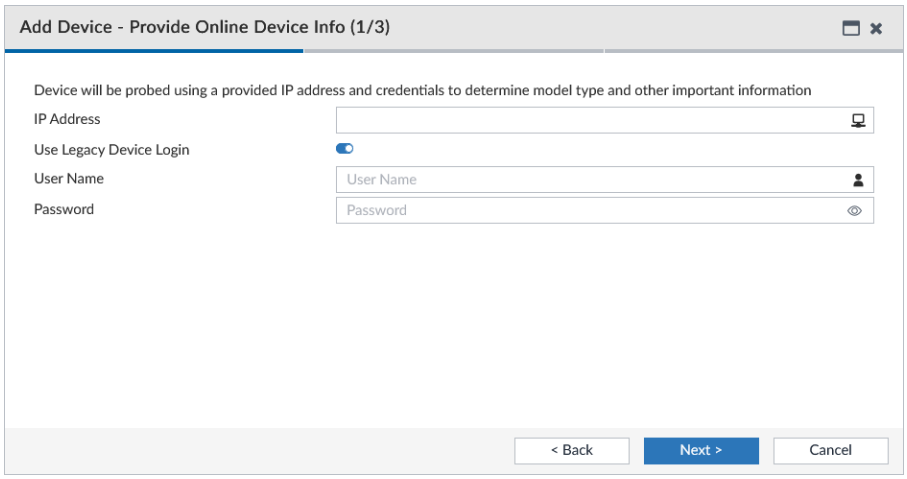
For FortiGates running FortiOS 6.4.x and earlier, the *Add device* wizard automatically switches to legacy login.

For FortiGates running FortiOS 7.0.0 and later, you can use the legacy login method instead of using the new authorization method. The legacy login method is useful for certain topologies where the browser popup window used by the new authorization method cannot connect to online FortiGate devices.

See also Security Fabric authorization on page 101.

To use the legacy login:

1. On *Device Manager*, click *Add Device*.
   The *Add Device* wizard is displayed.
2. Select *Discover Device*, and then toggle *Use legacy login* to *ON*.



3. Set the following options, and click *Next*.

IP Address	Type the IP address of the management port for the device.
User Name	Type the username for the device.
Password	Type the password for the device.

   FortiManager connects to FortiGate and authorization proceeds.
4. Complete the wizard. For details, see Adding online devices using Discover mode on page 92.

Adding offline model devices

The following steps describe how to add a new, offline device by using the *Add Device* wizard and *Add Model Device* mode for zero-touch provisioning (ZTP).



To confirm that a device model or firmware version is supported by the FortiManager's current firmware version, run the following CLI command:

```
diagnose dvm supported-platforms list
```

The *Add Model Device* mode is intended for new FortiGate deployments, where no pre-existing configuration on the FortiGate must be preserved. The configuration associated with the model device overwrites the configuration of the FortiGate as part of the ZTP process, after FortiManager authorizes the FortiGate and checks the version of the Internet Service database on the FortiGate. See also Model devices on page 48.

You can configure a model device to automatically complete authorization with FortiManager.



When configuring a model device to automatically complete authorization with FortiManager, add the model device to FortiManager by using a pre-shared key. When the device connects to FortiManager, run the `execute central-mgmt register-device` command from the FortiGate console. The device is automatically authorized, and the configuration of the matched model device is applied.

For FortiOS 5.4.1 or earlier, you must run the `execute central-mgmt register-device` command.

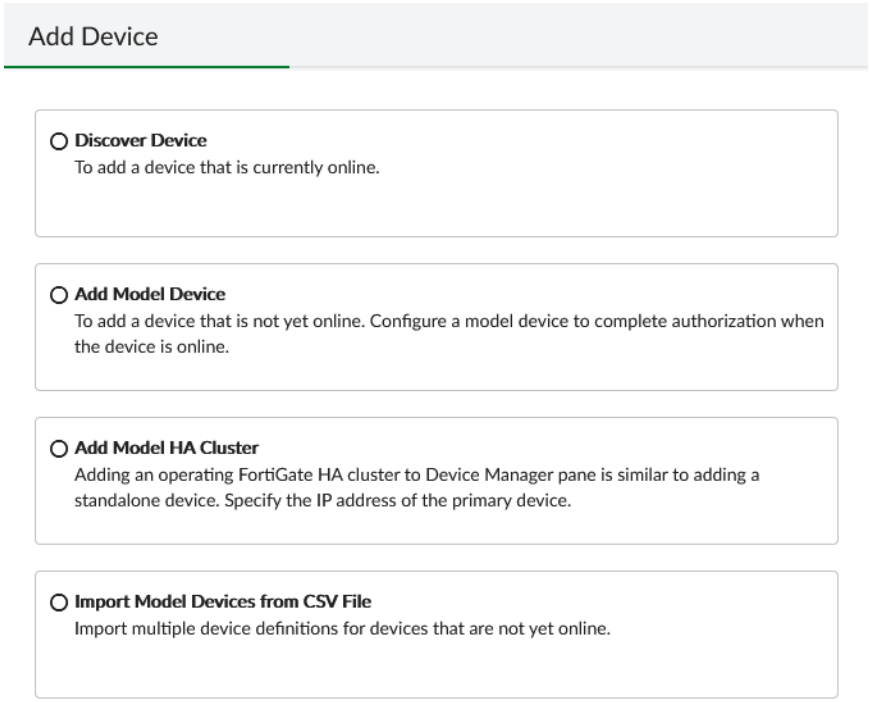


When adding devices to product-specific ADOMs, you can only add that product type to the ADOM. When adding a non-FortiGate device to the root ADOM, the device will automatically be added to the product-specific ADOM.

To add a model device:

1. If ADOMs are enabled, select the ADOM to which you want to add the device.
2. Go to *Device Manager* > *Device & Groups*.

3. Click *Add Device*. The *Add Device* wizard displays.



4. Click *Add Model Device* and enter the following information:

Add Model Device	Device will be added using the chosen model type and other explicitly entered information.
Name	Type a descriptive name for the device. This name is displayed in the *Device Name* column. Each device must have a unique name; otherwise, the wizard will fail.
Link Device By	The method by which the model device will be linked to the real device. Model devices can be linked by *Serial Number* or *Pre-Shared Key*. The serial number should be used if it is known. A pre-shared key can be used if the serial number is not known when you add the model device to FortiManager. If using a pre-shared key, the following CLI command needs to be issued from the FortiGate device when it is installed in the field: `execute central-mgmt register-device <fmg-serial-number> <preshared-key>`
Serial Number or Pre-Shared Key	Type the device serial number or pre-shared key. This field is mandatory. If using a pre-shared key, each device must have a unique pre-shared key. You can change the pre-shared key after adding the model device. See Editing device information on page 153.

	Adding a VM device  By default, FortiManager will not recognize the serial numbers of the following VM devices: • FortiGate-VM • FortiCarrier-VM • FortiProxy-VM • FortiFirewall-VM • FortiAnalyzer-VM When adding a VM device to FortiManager, you must first enable the recognition of VM serial numbers. See Adding VM devices on page 118.
Use Device Blueprint	Toggle ON to enable the use of device blueprints. When a device blueprint is selected, the following configurations are imported from the blueprint and cannot be specified in the *Add Device* wizard: Enforce Firmware Version, Add to Device Group, Add to Folder, Pre-run CLI Templates, Assign Policy Package, Provisioning Template. See Using device blueprints for model devices on page 114.
Device Model	Select the device model from the list. If linking by serial number, the serial number must be entered before selecting a device model.
Port Provisioning	Select the number of ports (1-10) to be provisioned for the FortiGate VM during initialization. This feature uses the `provision_instances_on_vm` script in *Device Manager > Provisioning Templates > CLI Templates* to configure the selected number of ports on the device. The script is performed while adding the offline model into the Device Manager. This option is only available for FortiGate-VM device models.
Automatically Link to Real Device	Toggle ON to allow the model device to automatically link to the real device. When enabled, the *Auto-link Status* of the model device will be displayed as *Enabled* in FortiManager's Device Manager. When disabled, the *Auto-link Status* of the model device will be displayed as *Disabled* in FortiManager's Device Manager. You can edit model devices added to FortiManager to enable or disable the *Automatically Link to Real Device* setting.
Split Switch Ports	Select to enable splitting virtual switch ports. This feature uses the `split_hardware_switch_ports_40_80_100` or `split_hardware_switch_ports_60_90` scripts in *Device Manager > Provisioning Templates > CLI Templates* to configure splitting virtual switch ports on the selected device. The script is performed while adding the offline model into the Device Manager. This option is only available on select hardware device models including FGT 40F/60F/80E/90E/100E/100F.

Enforce Firmware Version	Select the check box to enforce the firmware version. The *Firmware Version* shows the firmware that will be upgraded or downgraded on the device.
Enforce Device Configuration	Enable to enforce the device configuration. The *Enforce Device Configuration* option allows auto-link to push changes on FortiGate management interface during ZTP/LTP. When enabled, this option will provision the configuration to the real device, as is. Misconfiguration of the FortiGate management interface may cause the device to not be able to connect to the FortiManager.
Add to Device Group	Select the check box to choose a device group.
Add to Folder	Select the check box to choose a folder.
Pre-run CLI Templates	Select the check box to choose pre-run CLI templates. Pre-run CLI templates are run before provisioning templates.
Assign Policy Package	Select the check box and select a policy package from the drop-down to assign a particular policy package to the device.
Provisioning Template	Click to display the *Assign Provisioning Templates* dialog box. You can select one or more individual provisioning templates, or you can select a template group.
Override Profile Value	Click *Override Profile Value* to display the interface template and override settings. Overrides must be enabled in the interface template before you can override settings.
Metadata Variables	Edit the metadata variables for the new model device. See ADOM-level metadata variables on page 557.
Copy Device Dashboard	Select a device to copy custom device dashboards from (optional). For more information about dashboards in the device database, see Device DB - Dashboard on page 199.

5. Click *Next*. The device is created in the FortiManager database.
6. Click *Finish* to exit the wizard.
   A device added using the *Add Model Device* option has similar dashboard options as a device added using the *Discover* option. As the device is not yet online, some options are not available.



When adding a model device that has been configured with an admin password, you must import the device's existing configuration or set the password in FortiManager before pushing new configuration changes to it for the first time.

If the password is not imported or configured in FortiManager, when auto-push occurs, the installation will fail because the admin password in FortiGate devices cannot be unset without knowing the existing password.

A configuration file must be associated with the model device to enable FortiManager to automatically install the configuration to the matching device when the device connects to FortiManager and is authorized. FortiManager does not retrieve a configuration file from a real device that matches a model device.

Use the *Import Revision* function to associate a configuration file with the model device. See Viewing configuration revision history on page 206.

When FortiManager performs database updates

Following the device auto-link process, FortiManager determines if the following databases must be updated when the configuration is pushed to the managed device. Each database is checked individually for updates.

- Internet service database
- IPS database
- Application Signature database

This check is performed based on the following criteria:

- If there is no Internet Service/IPS/Application Signature database used in the Policy Package, there will be no database update performed.
- If the internet Internet Service/IPS/Application Signature database used in the Policy Package is the same version or an older version than the version on the FortiGate, there will be no database update performed.
- If the internet Internet Service/IPS/Application Signature database used in the Policy Package is newer than the database version on the FortiGate, a database update is performed.

Example: Adding an offline device by pre-shared key

This section describes how to add a FortiGate model by using the pre-shared key for FortiGate for zero-touch provisioning (ZTP). You must perform some steps using FortiManager and some steps using FortiOS.

To add a model device by pre-shared key:

1. If ADOMs are enabled, select the ADOM to which you want to add the device.
2. Go to *Device Manager* > *Device & Groups*.
3. Click *Add Device*. The *Add Device* wizard displays.
4. Click *Add Model Device* and type a name for the model device.
5. Beside *Link Device By*, select *Pre-shared Key*, and type the pre-shared key from FortiGate.
6. Set the remaining options, and click *Next*. The device is created in the FortiManager database.
7. Click *Finish* to exit the wizard.
   After the device model is added to FortiManager, you can use FortiManager to configure the model device.
8. In FortiOS, configure the FortiManager IP address or FQDN in device central management by using the following command:

```
config system central-management
   set type fortimanager
   set fmg {<ip address> | <FQDN>}
   set serial-number <FMG serial number>
end
```

9. In FortiOS, use the following command to link the model device to the real device, and to install configurations to the real device:
   ```
   exe central-mgmt register-device <fmg-serial-number> <pre-shared key>
   ```
   After the command is executed, FortiManager automatically links the model device to the real device, and installs configurations to the device.

Example: Adding an offline device by serial number

This section describes how to add a FortiGate model device to FortiManager by using the serial number for the FortiGate for zero-touch provisioning (ZTP). You must perform some steps using FortiManager and some steps using FortiOS.

To add a model device by serial number:

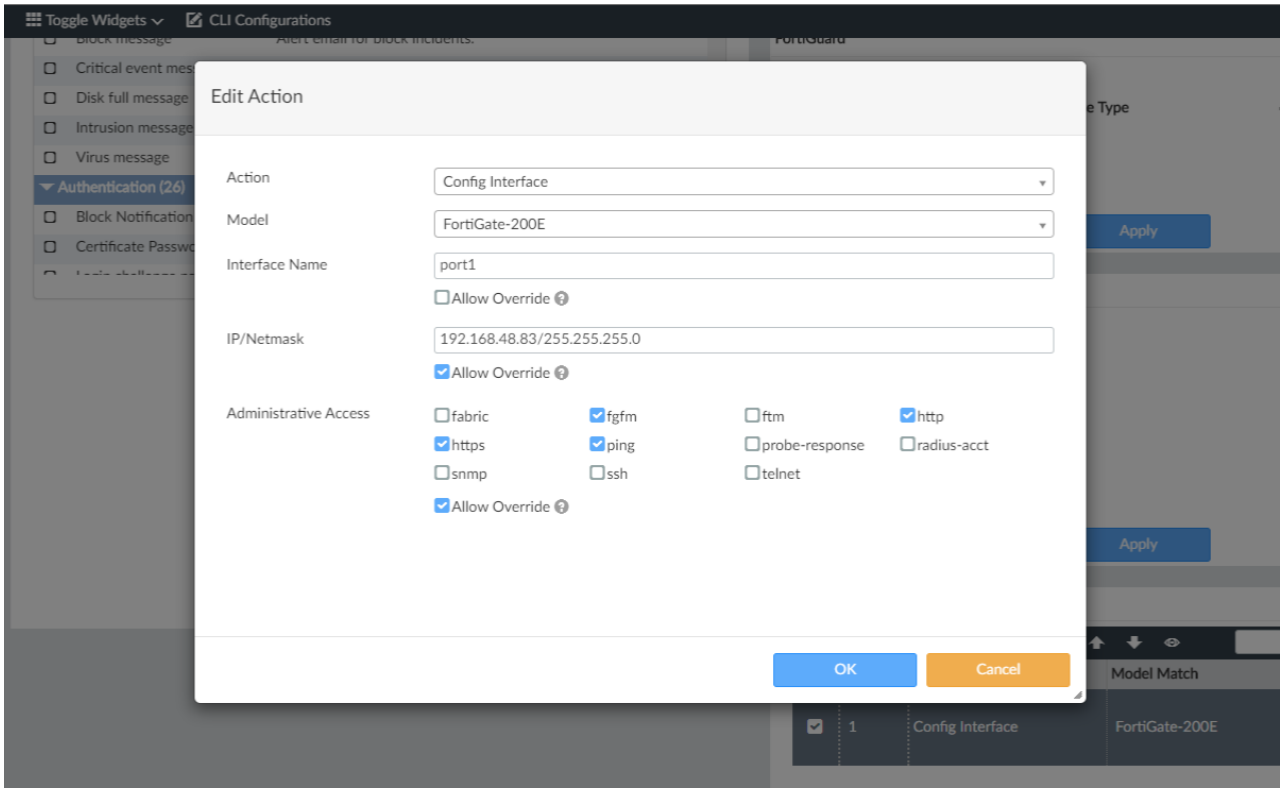
1. If ADOMs are enabled, select the ADOM to which you want to add the device.
2. Go to *Device Manager > Device & Groups*.
3. Click *Add Device*. The *Add Device* wizard displays.
4. Click *Add Model Device* and type a name for the model device.
5. Beside *Link Device By*, select *Serial Number* and type the serial number for the FortiGate unit.
6. Set the remaining options, and click *Next*. The device is created in the FortiManager database.
7. Click *Finish* to exit the wizard.
   After the device model is added to FortiManager, you can use FortiManager to configure the model device.
8. In FortiOS GUI, configure the FortiManager IP address.
   a. Go to *Security Fabric > Fabric Connectors*.
   b. Under *Other Fortinet Products*, double-click the FortiManager tile to open it for editing.
   c. In the *IP address* box, type the FortiManager IP address, and click *OK*.
   FortiManager automatically links the model device to the real device, and installs configurations to the device.

Example: Adding an offline device by using device template

This section describes how to add a FortiGate model device to FortiManager by using a device template. You can either use a site template or a provisioning template to add a model device. You must perform some steps using FortiManager and some steps using FortiOS.

To add a model device using a provisioning template:

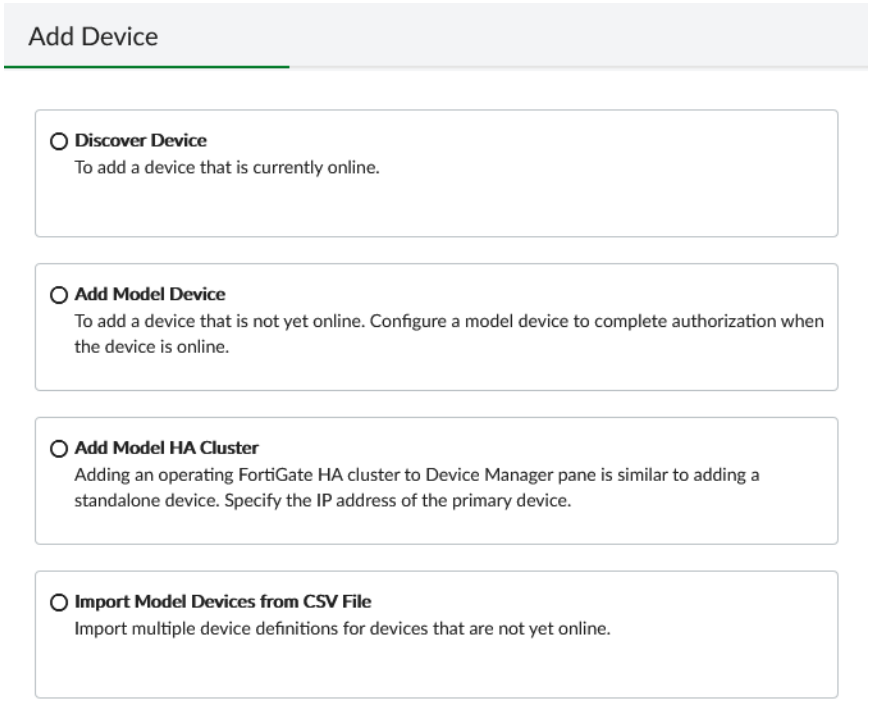
1. Go to *Device Manager* > *Provisioning Templates* > *System Templates*, and create a new system template.



The *Allow Override* option allows overriding profile values when using a provisioning template to add a model device. Use the option while creating a template to override any profile values later when you add a model device using a provisioning template. If the option is left unchecked, you cannot override profile values when adding a model device using a provisioning template.

2. Go to *Device Manager* > *Device & Groups* > *Add Device*. The *Add Device* dialog appears.

3. Click *Add Model Device*.

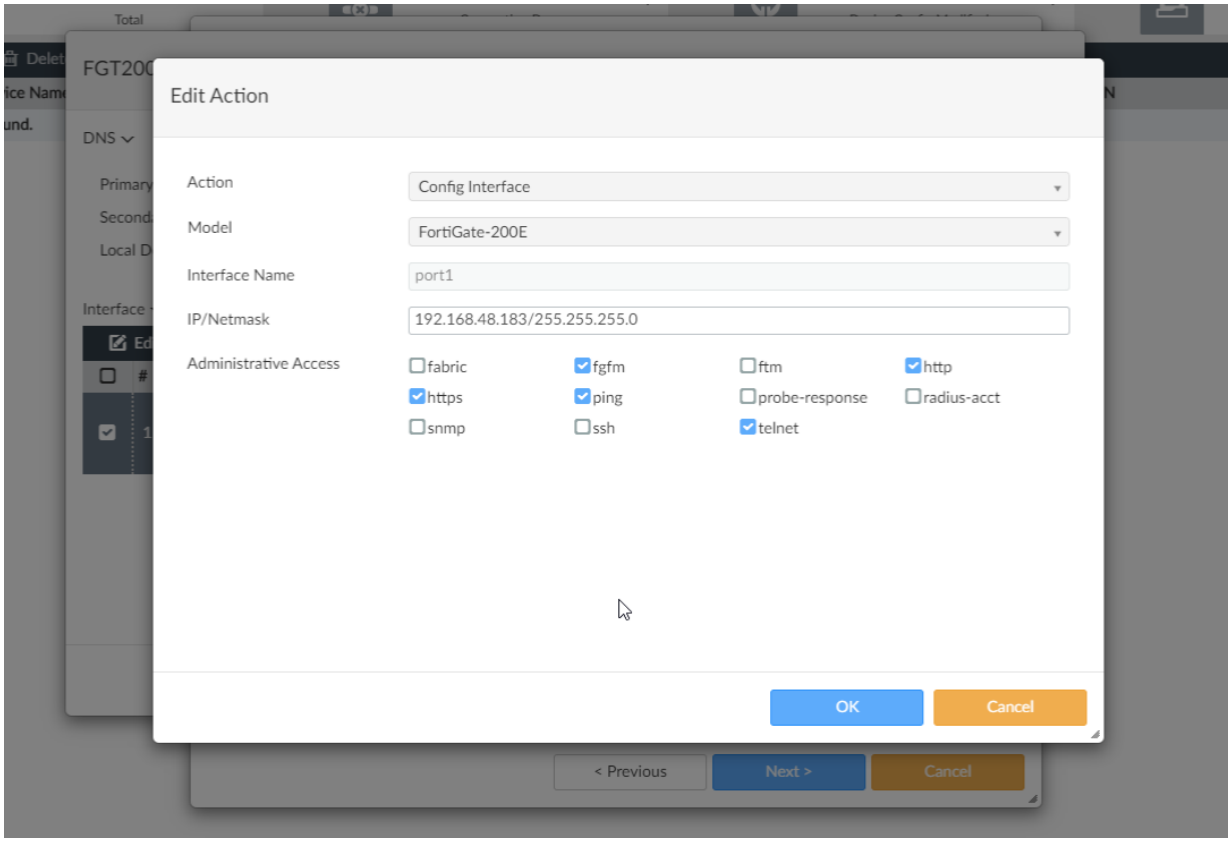


4. Configure the settings as follows:

Name	Enter a name for the model device.
Link Device By	Select *Serial Number*.
Serial Number	Add the serial number of the FortiGate device to be added.
Device Model	Select the device model from the drop-down list.
Provisioning Template	Click to display the *Assign Provisioning Templates* dialog box, and then select the system template you created in Step 1.

To continue without overriding the profile values, proceed with the next steps. To override profile values in the system template:

a. Click *Override Profile Value*. The template widget override dialog appears.
b. Select the interface and click *Edit*. The *Edit Action* dialog appears.



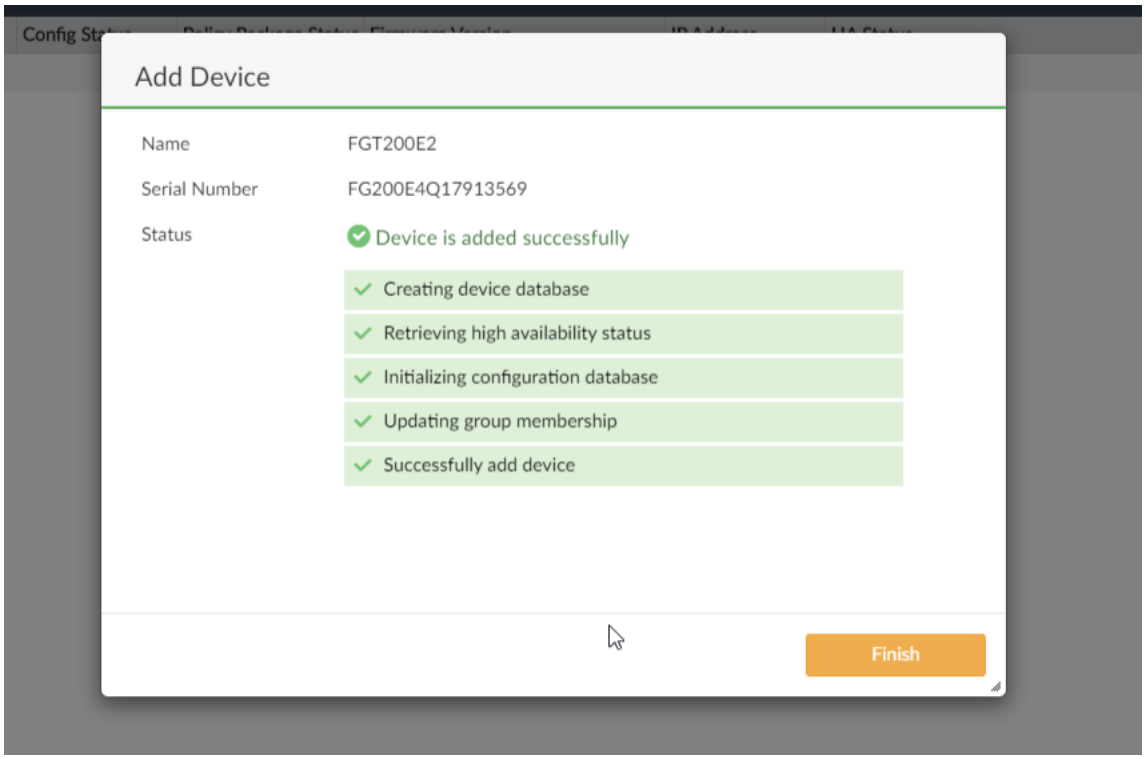
c. Make the required changes and click *OK*.



You can only change the fields that were configured with the *Allow Override* option while creating the template. If the option was left unchecked, you cannot override profile values when adding a model device using a provisioning template.

d. The profile values have successfully been overridden. Click *OK*.

5. Click *Next*. The device is successfully added.



6. On the added FortiGate device, add the FortiManager IP address.
7. Confirm the FortiGate on the FortiManager to synchronize both the devices. The provisioning template, along with profile overrides if any, is pushed to the FortiGate device.



Using device blueprints for model devices

Device blueprints can be used when adding model devices to simplify configuration of certain device settings, including device groups, configuring pre-run templates, policy packages, provisioning templates, and more.

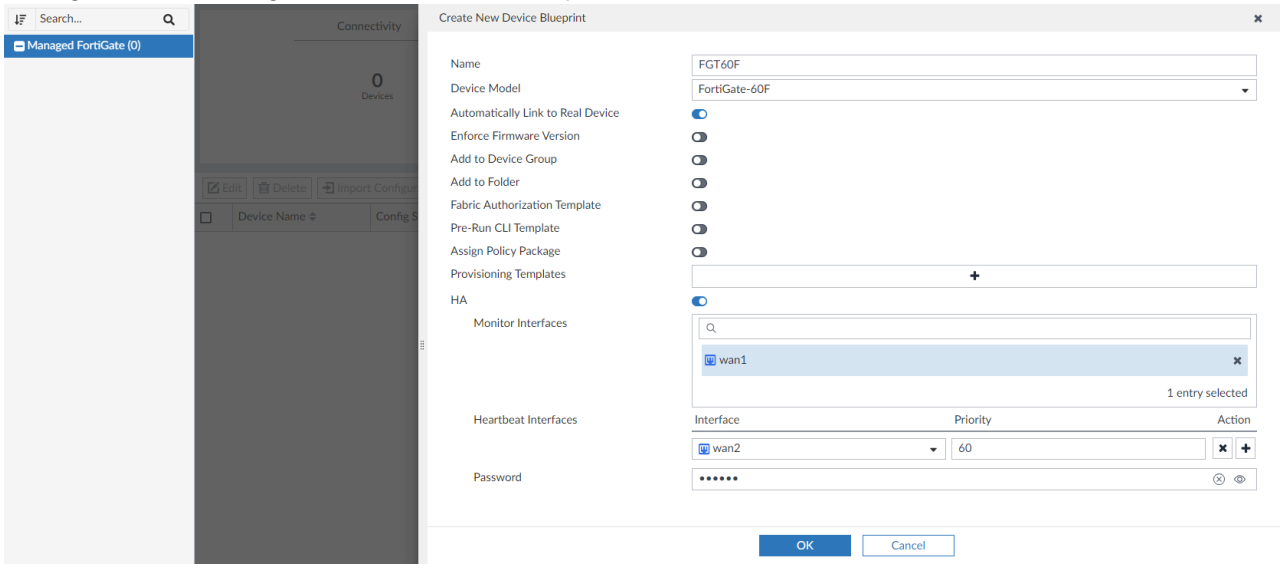
Once a device blueprint has been created, it can be selected when adding a model device or when importing multiple model devices from a CSV file. See Adding offline model devices on page 104.

Devices that are assigned the blueprint are automatically configured with the settings specified by the blueprint when they are added to FortiManager.

As an exmaple, device blueprints can be used to simplify the onboarding of branch devices in an SD-WAN configuration when using SD-WAN Overlay Templates by configuring the default device group to which the devices are added. See SD-WAN overlay templates on page 327.

To create a new device blueprint:

1. Go to *Device Manager* > *Device & Groups*.
2. From the *Add Device* dropdown, select *Device Blueprint*.
   Previously configured blueprints are displayed in the table below and can be edited or deleted.
3. Click *Create New* to add a new blueprint.
4. Configure the following information for the blueprint:



Name	Enter a name for the device blueprint.
Device Model	Select the model type that the device blueprint will be applied to.
Automatically Link to Real Device	Enable to allow the model device to automatically link to the real device. See Adding offline model devices on page 104.
Enforce Firmware Version	Enable to choose an enforced firmware version.
Enforce Device Configuration	Enable to enforce the device configuration. The *Enforce Device Configuration* option allows auto-link to push changes on FortiGate management interface during ZTP/LTP. When enabled, this option will provision the configuration to the real device, as is. Misconfiguration of the FortiGate management interface may cause the device to not be able to connect to the FortiManager.
Add to Device Group	Enable to add one or more device groups. All devices assigned this device blueprint are added to the selected device group(s).
Add to Folder	Enable to add the devices to the specified folder in the *Device Manager*.
Fabric Authorization Template	Enable to add a Fabric Authorization Template to the device blueprint, and then select or create a template from the dropdown menu. See Fabric authorization templates on page 278.

Pre-Run CLI Template	Enable to add a Pre-run CLI Template to the device blueprint, and then select or create a template from the dropdown menu. See Adding CLI templates on page 358.
Assign Policy Package	Enable to add a Policy Package to the device blueprint, and then select the Policy Package from the dropdown menu. Devices added with this device blueprint will be automatically assigned the selected Policy Package. See Managing policies on page 427.
Provisioning Template	Select provisioning templates. You can assign system, IPsec, SD-WAN, static route, BGP, CLI, and IPS templates, or select a template group. See Provisioning Templates on page 273.
HA	Enable to define an HA cluster.
Monitor Interfaces	Select the device interfaces to monitor.
Heartbeat Interfaces	Select the heartbeat interfaces and set their priority.
Password	Enter the cluster password.

5. Click *OK* to save the blueprint.
   The blueprint can now be selected when adding a model device or importing devices from a CSV file. See Add devices on page 91.

To edit or delete a device blueprint:

1. Go to *Device Manager* > *Device & Groups*.
2. From the *Add Device* dropdown, select *Device Blueprint*.
3. Select an existing device blueprint from the table. The following actions are available:
   a. **Edit**: You can edit an existing device blueprint. Changes made to existing blueprints only affect new devices added to FortiManager after the changes have been made; devices previously configured with the blueprint are not affected.
   b. **Delete**: Delete an existing device blueprint.

To generate a CSV file for a device blueprint:

1. Go to *Device Manager* > *Device & Groups*.
2. From the *Add Device* dropdown, select *Device Blueprint*.
3. Select a blueprint and click *Generate CSV*.

Import model devices from a CSV file

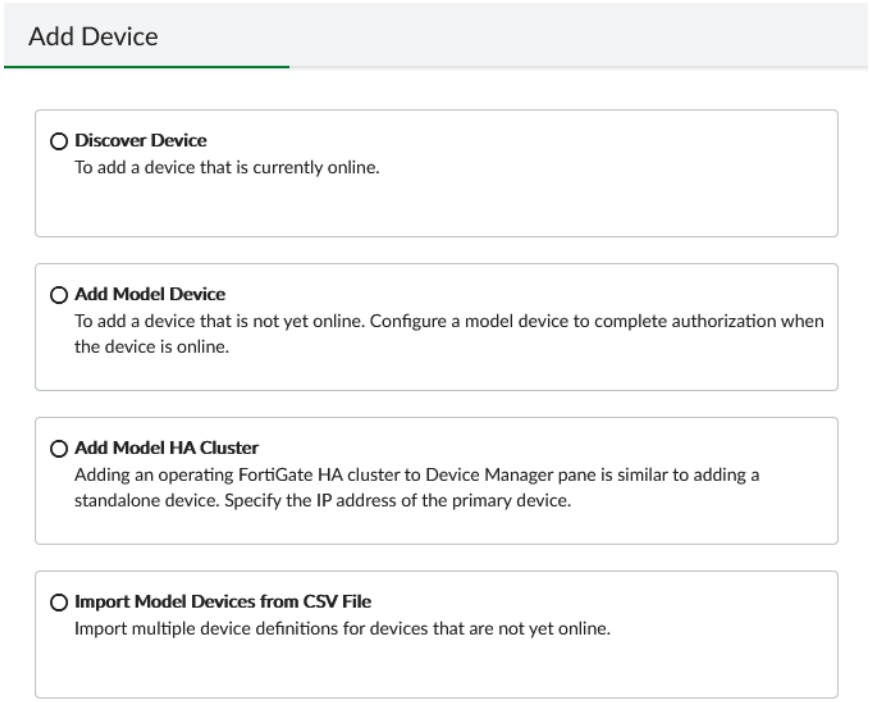
Model devices can be imported using a CSV file. This can be used to import large numbers of model devices into FortiManager.

When importing model devices from a CSV file, a device blueprint is used to configure the initial settings. See Using device blueprints for model devices on page 114.

ADOM-level metadata variables for each device can be specified in the CSV file.

To import model devices from a CSV File:

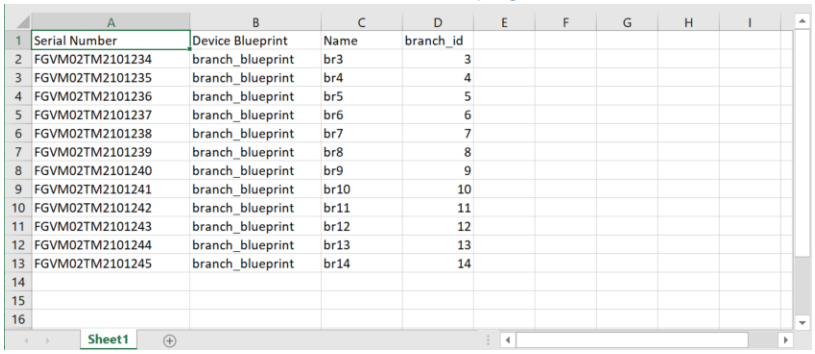
1. If ADOMs are enabled, select the ADOM to which you want to add the device.
2. Go to *Device Manager > Device & Groups*.
3. Click *Add Device*.
   The *Add Device* dialog is displayed.



4. Click *Import Model Devices from CSV File*.
5. Configure your local CSV file for the devices that you want to import. The CSV file must contain the following columns: `Serial Number`, `Device Blueprint`, and `Name`, with the respective data listed in the cells below. The headers in the CSV file are case-sensitive.

   If you are creating an HA cluster, also include the following columns: `Cluster Id`, `Cluster Name`, `Priority`, and `HA Mode`.

   Additional columns can be added for each metadata variable that you want to specify. In the following image, the `branch_id` metadata variable has been added to specify this variable for each imported device. See ADOM-level metadata variables on page 557.



	A	B	C	D	E	F	G	H	I
1	Serial Number	Device Blueprint	Name	branch_id					
2	FGVM02TM2101234	branch_blueprint	br3	3					
3	FGVM02TM2101235	branch_blueprint	br4	4					
4	FGVM02TM2101236	branch_blueprint	br5	5					
5	FGVM02TM2101237	branch_blueprint	br6	6					
6	FGVM02TM2101238	branch_blueprint	br7	7					
7	FGVM02TM2101239	branch_blueprint	br8	8					
8	FGVM02TM2101240	branch_blueprint	br9	9					
9	FGVM02TM2101241	branch_blueprint	br10	10					
10	FGVM02TM2101242	branch_blueprint	br11	11					
11	FGVM02TM2101243	branch_blueprint	br12	12					
12	FGVM02TM2101244	branch_blueprint	br13	13					
13	FGVM02TM2101245	branch_blueprint	br14	14					
14									
15									
16									

Sheet1

6. Drag and drop the CSV file into the *Upload* area, or select the CSV file location on your computer.
   The model devices' serial numbers, names, blueprints, and optional metadata variables are displayed in the table.
7. (Optional) From the *Copy Device Dashboard* dropdown, select a device to copy custom device dashboards from.
   For more information about dashboards in the device database, see Device DB - Dashboard on page 199.
8. Review the device list, and click *Next* to begin importing the devices. Click *Finish* when the import process is complete.

Adding VM devices

By default, VM serial numbers are not recognized when adding devices to FortiManager. This applies to:

- FortiGate-VM
- FortiCarrier-VM
- FortiProxy-VM
- FortiFirewall-VM
- FortiAnalyzer-VM

This measure increases security of the FortiManager system by ensuring that VM devices can only be added to FortiManager when recognition of VM serial numbers has been enabled by an administrator.

If you attempt to add a VM device (for example, a model FortiGate-VM) to FortiManager while the `fgfm-allow-vm` command is disabled, an error will appear indicating that VM devices are not allowed or that the device is an unsupported model.

When upgrading from an earlier version of FortiManager that does not enforce this behavior, VM devices already managed by FortiManager will continue to be supported without interruption, but you must enable the `fgfm-allow-vm` command before you can add any additional VM devices.

To add a FortiGate-VM to FortiManager:

1. In the FortiManager CLI, enable recognition of FortiGate-VM serial numbers:
   ```
   config sys global
      set fgfm-allow-vm enable
   end
   ```
2. Proceed with adding the FortiGate-VM device through one of the supported methods. See Add devices on page 91.

Adding a model FortiGate HA cluster

You can add an offline FortiGate HA cluster by using the *Add Model Device* method. The process of adding an offline FortiGate HA cluster is similar to adding a model device using FortiGate serial numbers. See Example: Adding an offline device by serial number on page 110.

You can add the two FortiGate devices as model devices to be part of the HA cluster.

You can also add an operating FortiGate HA cluster. Adding an operating FortiGate HA cluster to the *Device Manager* pane is similar to adding a standalone device. Specify the IP address of the primary device. FortiManager handles a cluster as a single managed device.

You can define a device blueprint for an HA cluster and use it to add the model HA cluster. See Using device blueprints for model devices on page 114.



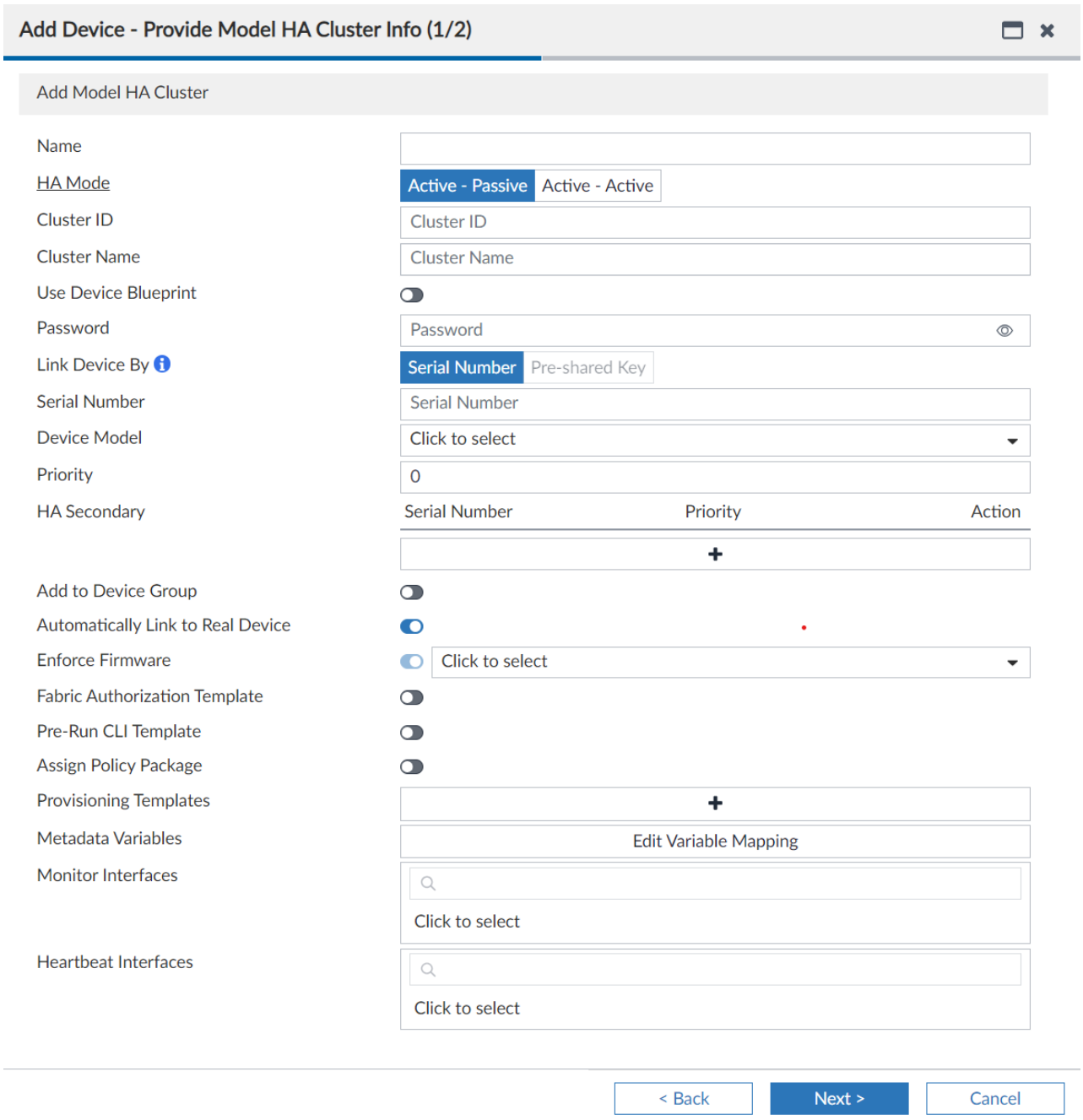
If you are using an HA cluster, you can promote a secondary device to a primary device. Go to *Device Manager > Device & Groups > Managed FortiGate > [HA_Cluster_Name]*. The *System:Dashboard* pane shows the cluster members under *Cluster Members*. Click *Promote* to promote a secondary device to a primary device.



FortiGate devices in an HA cluster should not use `ha-mgmt-interface` or `standalone-mgmt-vdom` to establish the FGFM connection.

To add a model FortiGate HA cluster:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > Device & Groups*.
3. Click *Add Device*. The wizard opens.
4. Select *Add Model HA Cluster*.
5. Populate the mandatory fields *Name*, *HA Mode*, *Cluster ID*, *Cluster Name*, and *Serial Number*.
6. Optionally, enable *Enforce Device Configuration*.
   The *Enforce Device Configuration* option allows auto-link to push changes on FortiGate management interface during ZTP/LTP. When enabled, this option will provision the configuration to the real device, as is. Misconfiguration of the FortiGate management interface may cause the device to not be able to connect to the FortiManager.
7. To use a device blueprint, enable *Use Device Blueprint*, then select the *Device Blueprint*.
8. Configure the remaining settings as needed, and click *OK*.
   Optionally, you can disable *Automatically Link to Real Device*. When auto-linking is enabled, auto-link will start after all cluster members are connected. You can edit model devices added to FortiManager to enable or disable the *Automatically Link to Real Device* setting. See Adding offline model devices on page 104.



The FortiGate device with a higher node priority will be considered as the primary device of the HA cluster.

Both the FortiGate devices to be added to the HA cluster must be on the same firmware version. If not, the devices will be enforced with the same version as selected in the *Enforce Firmware Version* field in the *Add Device* dialog.

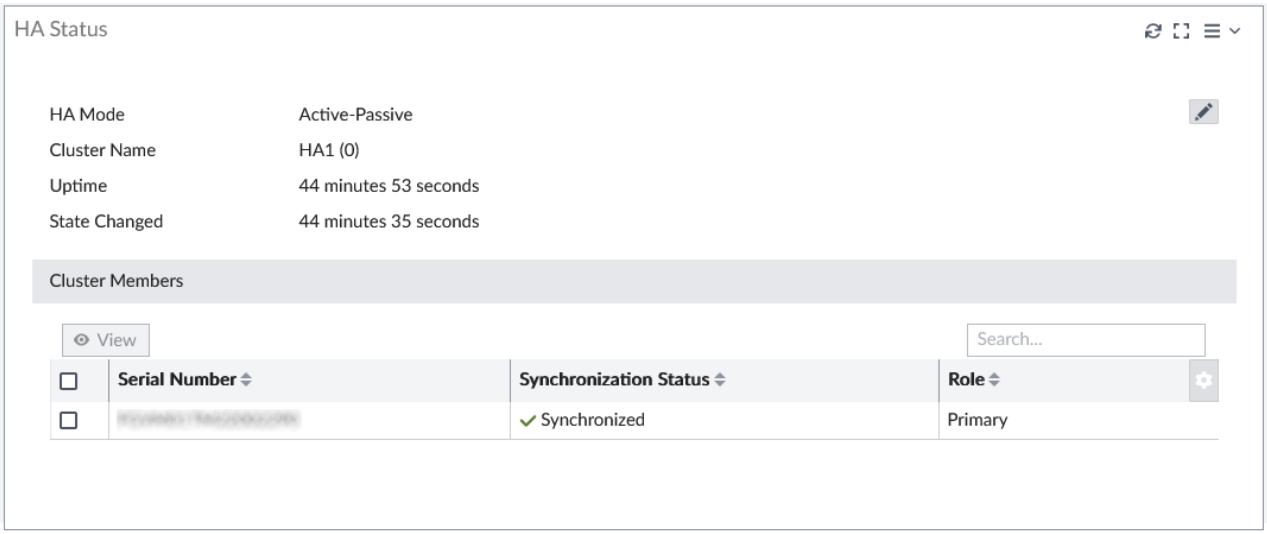
FortiManager adds both the FortiGate devices as model devices and creates an HA cluster. Based on device node priorities, both the devices will come online and show up in FortiManager one after the other. You can view the status of the HA cluster and information about each of the nodes of the HA cluster in *Device Manager*.

Viewing the status of the HA cluster

You can view the synchronization status of cluster members in *Device Manager* > *Device & Groups*, the device database, or while editing cluster member devices.

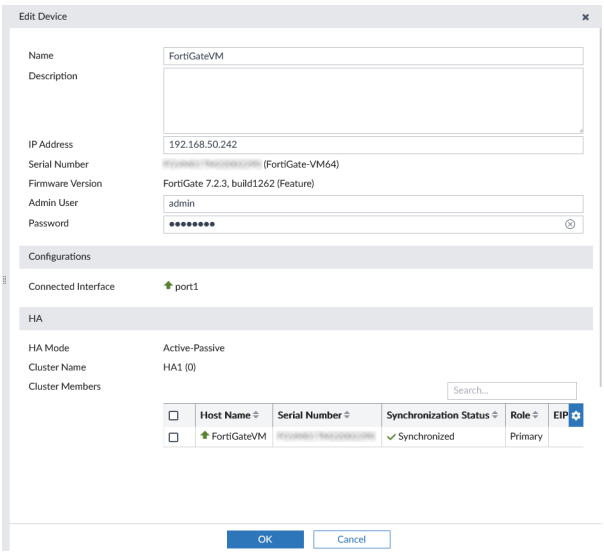
These views display information about the HA cluster, including the *Synchronization Status* and *Role* of HA members. The *Synchronization Status* is displayed as one of the following:

- *Synchronized*: The FortiGate HA cluster member is in sync.
- *Out of Sync*: The FortiGate HA cluster member is out of sync.
- *Unknown*: The FortiGate HA cluster members is offline.



Editing HA cluster information

You can edit the HA cluster information. Use the *Edit Device* screen to modify the HA cluster information by modifying the fields *IP Address*, *Admin User*, *Password*, and *Cluster Members*. .



Adding a Security Fabric group

Before you can add a Security Fabric group to FortiManager, you must create the Security Fabric group in FortiOS.

You must add to FortiManager the root FortiGate for the Security Fabric group. All the devices in the Security Fabric group are automatically added in *Unauthorized Devices* after you add the root FortiGate.

See also Displaying Security Fabric topology on page 157.

To add a Security Fabric group:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager* > *Device & Groups*.
3. Add the root FortiGate unit for the Security Fabric group. See Adding online devices using Discover mode on page 92.
   Alternatively, you can enable Central Management in the root FortiGate unit and specify the IP address of the FortiManager. See Authorizing devices on page 128.
   All devices part of the Security Fabric group are automatically added in *Unauthorized Devices*.
4. Select all devices in *Unauthorized Devices* and click *Add*.
5. Specify the credentials for each device in the *Add Device* dialog and click *OK*.

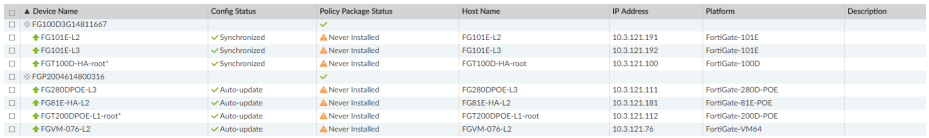
The entire Security Fabric group with all the devices are added to FortiManager. FortiGate devices are listed under *Managed Devices*.



If the FortiManager is behind NAT, adding the root FortiGate will not add all the members of the Security Fabric Group automatically. If the FortiManager is behind NAT, the only way is to add each member of the Security Fabric group manually.

Refresh the Security Fabric root after all the members of the group are added to FortiManager. FortiManager retrieves information about the Security Fabric group via the root FortiGate unit. All units are displayed in a Security Fabric group. The *Security Fabric* icon identifies the group, and the group name is the serial number for

the root FortiGate in the group. Within the group, a * at the end of the device name identifies the root FortiGate in the group.



Device Name	Config Status	Policy Package Status	Host Name	IP Address	Platform	Description
FG100D3G14811667						
FG101E-L2	Synchronized	Never Installed	FG101E-L2	10.3.121.191	FortiGate-101E	
FG101E-L3	Synchronized	Never Installed	FG101E-L3	10.3.121.192	FortiGate-101E	
FGT100D-HA-root*	Synchronized	Never Installed	FGT100D-HA-root	10.3.121.100	FortiGate-100D	
FGP200K4614800316						
FG280DPOE-L3	Auto-update	Never Installed	FG280DPOE-L3	10.3.121.111	FortiGate-280D-POE	
FG81E-HA-L2	Auto-update	Never Installed	FG81E-HA-L2	10.3.121.181	FortiGate-81E-POE	
FGT200DPOE-L1-root*	Auto-update	Never Installed	FGT200DPOE-L1-root	10.3.121.112	FortiGate-200D-POE	
FGVM-076-L2	Auto-update	Never Installed	FGVM-076-L2	10.3.121.76	FortiGate-VM64	

Adding FortiSOAR devices

You can configure FortiSOAR devices to use the FortiGuard module in FortiManager for license checks by configuring FortiManager as the override FortiGuard server.

When FortiSOAR is configured to use FortiManager as the override FortiGuard server, the unit is displayed in FortiManager on the *Device Manager* pane in the unauthorized devices list. You can authorize the FortiSOAR device to a fabric ADOM, and FortiSOAR can communicate with the FortiGuard module for license updates.

To add FortiSOAR devices:

1. On each FortiSOAR device, add the FortiManager IP and configured port as the FortiGuard override server. The devices are displayed as unauthorized devices in FortiManager.
2. In the root ADOM, go to *Device Manager* > *Device & Groups*, and click the *Unauthorized Devices* tree menu. The content pane displays the unauthorized FortiSOAR devices.
3. If necessary, select the *Display Hidden Devices* check box to display hidden unauthorized devices.
4. Select the unauthorized device or devices, then click *Authorize*. The *Authorize Device* dialog box opens.
5. In the *Add the following device(s) to ADOM* list, select a fabric ADOM, and click *OK*. The device or devices are added to the fabric ADOM and authorized to communicate with FortiGuard.

If FortiSOAR is operating with FortiManager in a closed network without internet access, which is sometimes called an air-gapped network, you must request a license file from Fortinet support, and upload the file to *FortiGuard*. See Requesting account entitlement files on page 823 and Uploading account entitlement files on page 826.

Adding FortiSASE

FortiSASE can be added to FortiManager for central management. Only one FortiSASE can be onboarded per FortiManager.

When FortiManager is used for central management of FortiManager, a FortiSASE Connector is created to enable communication between FortiManager and FortiSASE. Administrators can use the connector to configure which FortiManager objects are synchronized to the FortiSASE. Currently, central management supports only one-way synchronization of configurations from FortiManager to FortiSASE. Therefore, administrators should avoid deleting objects from FortiManager to prevent any conflicts.

Only select FortiSASE configuration settings are supported for central management using FortiManager.

For full configuration steps, supported objects, and information about what FortiManager versions are supported for central management of FortiSASE, see the FortiSASE documentation on the Fortinet Documentation Library.

FortiSASE can only be added to FortiGate and Fabric ADOMs. Other ADOMs where the connector appears including *FortiProxy*, *FortiFirewallCarrier*, *FortiFirewall*, *FortiCarrier*, and the *Global Database ADOMs* are not supported.

Additionally, FortiSASE cannot be added to ADOMs operating in *Backup* mode. Attempting to do so will present the user with the error message "An unexpected error has occurred".

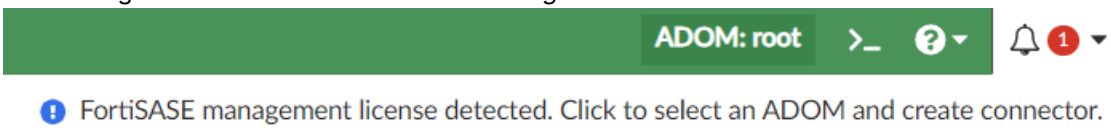
Prerequisites

In order to add FortiSASE to FortiManager, the following prerequisite steps must be completed:

- The FortiCloud account must include a valid FortiSASE entitlement.
- The FortiManager must be included in the same FortiCloud account as the FortiSASE entitlement.

To add FortiSASE to FortiManager:

1. When FortiSASE is on the same FortiCloud account as FortiManager, you will receive a notification in the FortiManager toolbar that the *FortiSASE management license is detected*. Click on the notification to begin.



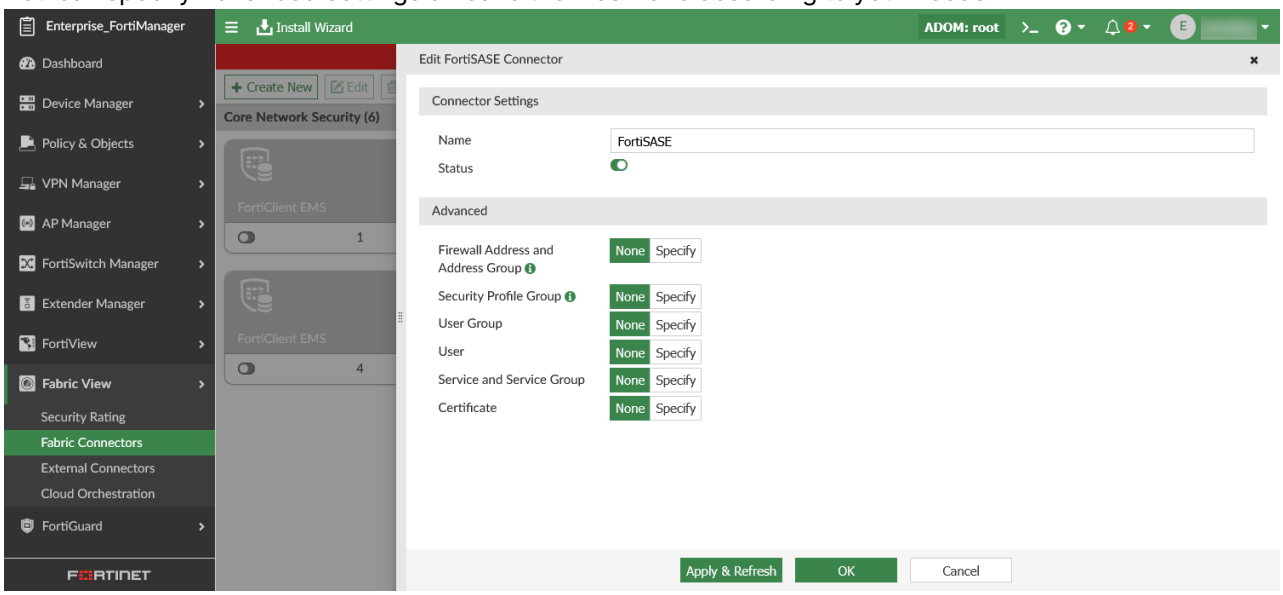
2. Select the ADOM where the FortiSASE device will be added.

FortiSASE cannot be added to version 7.0 ADOMs or the Global Database ADOM.

Once added, FortiSASE devices cannot be moved to other ADOMs.

3. In the *Edit FortiSASE Connector* dialog, enable the connector.

You can specify *Advanced* settings or leave them as *None* according to your needs.



Connector Settings		Configure the FortiSASE connector settings.
	Name	Enter a name for the connector.
	Status	Toggle the status of the connector *ON*.
Advanced		You can define the supported FortiManager objects to be synchronized to FortiSASE. For each object type, you can click *Specify* and *Click to select* to see a list of existing FortiManager objects. Click *+v* or *+* to create new objects from the dialog.
	Firewall Address and Address Group	Select or create Firewall Address and Firewall Address Groups.
	Security Profile Group	Select or create Security Profile Group and Security Profiles (selected types are supported only)
	User Group	Select or create User Groups.
	User	Select or create Users.
	Service and Service Group	Select or create Service and Service Groups.
	Certificate	Select or import Certificates.

4. Click *OK* to save the connector. You will see the *Connect to FortiSASE* dialog and *Add FortiSASE service* step marked as *Completed* when the onboarding is successful.
5. Go to *Fabric View* > *Fabric Connector* and you can see that the FortiSASE Connector is enabled. When hovering your mouse over the connector, you can observe the status of the connector and the list of synchronized objects.
6. In the FortiManager Device Manager, you can see the Managed FortiSASE device has been added after the FortiSASE Connector has been enabled.

7. Use the *Install Wizard* to *Install Device Settings (only)* to push the object configurations to FortiSASE. See Install device settings only on page 183.

To edit the FortiSASE connector:

1. Go to *Fabric View* > *Fabric Connectors*.
2. Double-click the *FortiSASE Connector* tile, or right-click and choose *Edit*.
3. In the *Edit FortiSASE Connector* dialog, configure the settings as required.
4. Click *OK*.
5. Use the *Install Wizard* to *Install Device Settings (only)* to push any object configuration changes to FortiSASE. See Install device settings only on page 183.

Installing policy packages to FortiSASE

Once the FortiSASE connector is enabled, you can view the *Policy Package Status* column for the FortiSASE controller in *Device Manager*.

FortiManager automatically retrieves built-in FortiSASE interfaces/zones through the connector. These interfaces/zones and their mappings can be viewed in *Policy & Objects* > *Normalized Interface*:

- *SASE_ingress_zone*
- *SASE_public_zone*
- *SASE_secure_private_access_zone*

The FortiSASE connector does not require any special configuration to install policy packages to FortiSASE. The objects used in policies are implicitly synced to FortiSASE during the policy package installation.

Firewall policies and proxy policies can be installed from FortiManager to FortiSASE. They are partially supported. See the tables below for requirements when installing to FortiSASE.

Firewall Policy requirements	
Action	Must be set to *ACCEPT* or *DENY* only.
Type	Must be set to *Standard*.
Incoming/Outgoing Interfaces	Limited to the following normalized interfaces/zones: • *SASE_ingress_zone* • *SASE_public_zone* • *SASE_secure_private_access_zone*
Supported traffic directions	• Internet access > SASE_ingress_zone > SASE_public_zone • Private access to hubs > SASE_ingress_zone > SASE_secure_private_access_zone • Private access from hubs > SASE_secure_private_access_zone > SASE_ingress_zone
Inspection Mode	Must be set to *Proxy-based*.
Security Profile	Status must be enabled, and *Profile Type* set to *Use Security Profile Group*.

For more information about creating firewall policies, see Create a new firewall policy on page 435.

Proxy Policy requirements	
Explicit Proxy Type	Must be set to *Explicit Web*.
Outgoing Interface	Must be either *SASE_public_zone* or *SASE_secure_private_access_zone*.
Action	Must be set to *ACCEPT* or *DENY* only.
Service	Must be explicitly defined.

For more information about creating proxy policies, see Create a new proxy policy on page 471.

The Proxy configuration and Secure Private Access Network configuration must both be enabled in order to install policies using the *SASE_secure_private_access_zone* in FortiSASE.

Adding FortiGate CNF device

FortiManager supports management of FortiGate CNF instances.

When creating a new FortiGate CNF instance in the FortiGate CNF console, you must enable *FortiManager Mode* in order to manage the instance in FortiManager. This setting cannot be changed after the instance is created.

You can only see the FortiGate connection information if the instance was created with *FortiManager Mode* enabled.

To add a FortiGate CNF instance to FortiManager:

1. In the FortiGate CNF console, in the *Display Primary FortiGate Information* field in the *Edit CNF* form, find the FortiGate connection details.
2. In FortiManager, go to *Device & Groups* > *Add Device*.
3. Click *Discover Device*.
4. Enter the *IP Address* of the FortiGate CNF instance.
5. Enable *Use Legacy Device Login* and enter the *User Name* and *Password*, then click *Next*.
6. Update or enter any required details and click *Next*.
7. Click *Finish*. The FortiGate CNF instance is added to FortiManager. There may be a short delay before the device is available.
8. Import the *FG-traffic* policy package from the FortiManager instance into FortiManager. Use this policy package to install policies to the FortiGate CNF instance.

When adding a FortiGate CNF instance, you will only see details of the primary FortiOS node. Other nodes are not displayed in the Members list on FortiManager.

For more information, see the FortiGate CNF Administration Guide.

Authorizing devices

You can enable central management by using the operating system for supported units. For example, in FortiOS, you can enable central management for the FortiGate unit by adding the IP address of the FortiManager unit. When central management is enabled, the device is displayed on the FortiManager GUI in the root ADOM on the *Device Manager* pane in the *Unauthorized Devices* list.

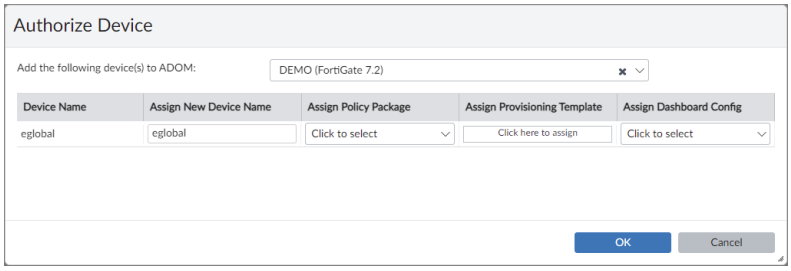
In FortiManager, you must authorize devices before you can use FortiManager to manage them. FortiManager cannot manage unauthorized devices.

When ADOMs are enabled, you can assign the device to an ADOM. When authorizing multiple devices at one time, they are all added to the same ADOM.

By default, FortiManager expects you to use the default admin account with no password. If the default admin account is no longer usable, or you have changed the password, the device authorization process fails. If the device authorization fails, delete the device from FortiManager, and add the device again by using the *Add Device* wizard, where you can specify the admin login and password.

To authorize devices:

1. In the root ADOM, go to *Device Manager > Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. Click the *Unauthorized Devices* tree menu. The content pane displays the unauthorized devices.
4. If necessary, select the *Display Hidden Devices* check box to display hidden unauthorized devices.
5. Select the unauthorized device or devices, then click *Authorize*. The *Authorize Device* dialog box opens.



6. If ADOMs are enabled, select the ADOM in the *Add the following device(s) to ADOM* list. If ADOMs are disabled, select *root*. The default value is *None*.

   If you try to authorize devices having different firmware versions than the selected ADOM version, the system shows a *Version Mismatch Warning* confirmation dialog.

   If you authorize the devices in spite of the warning, the configuration syntax may not be fully supported in the selected ADOM.

7. (Optional) In the *Assign New Device Name* list, type a different name for the device.
8. (Optional) In the *Assign Policy Package* list, select a policy package.
9. (Optional) In the *Assign Provisioning Template* list, select a profile.
10. (Optional) In the *Assign Dashboard Config* list, select a device to copy custom device dashboards from. For more information about dashboards in the device database, see Device DB - Dashboard on page 199.

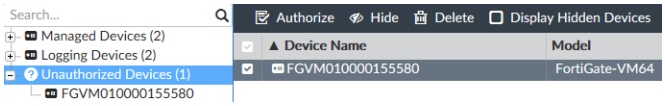
11. Click *OK* to authorize the device or devices.
    The device or devices are authorized, and FortiManager can start managing the device or devices.

Hiding unauthorized devices

You can hide unauthorized devices from view, and choose when to view hidden devices. You can authorize or delete hidden devices.

To hide and display unauthorized devices:

1. In the root ADOM, go to *Device Manager* > *Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. Click the *Unauthorized Devices* tree menu. The content pane displays the unauthorized devices.



4. Select the unauthorized device or devices, then click *Hide*.
   The unauthorized devices are hidden from view.
   You can view hidden devices by selecting the *Display Hidden Devices* check box.

Setting unauthorized device options

Type the following command lines to enable or disable unauthorized devices to be authorized with FortiManager.

```
config system admin setting
   set unreg_dev_opt {add_allow_service | add_no_service | ignore}
end
```

unreg_dev_opt	Set the action to take when an unauthorized device connects to FortiManager.
add_allow_service	Add unregistered devices and allow service requests.
add_no_service	Add unregistered devices but deny service requests.
ignore	Ignores unregistered devices.

Importing and exporting device lists

Using the *Import Device List* and *Export Device List* option, you can import or export a large number of devices, ADOMs, device VDOMs, and device groups. The device list is a compressed text file in JSON format.

You can also use the *Export to CSV* option to export a device list to CSV format. However, you cannot use the CSV format to import a device list to FortiManager. You can only import a device list that was exported to JSON format.

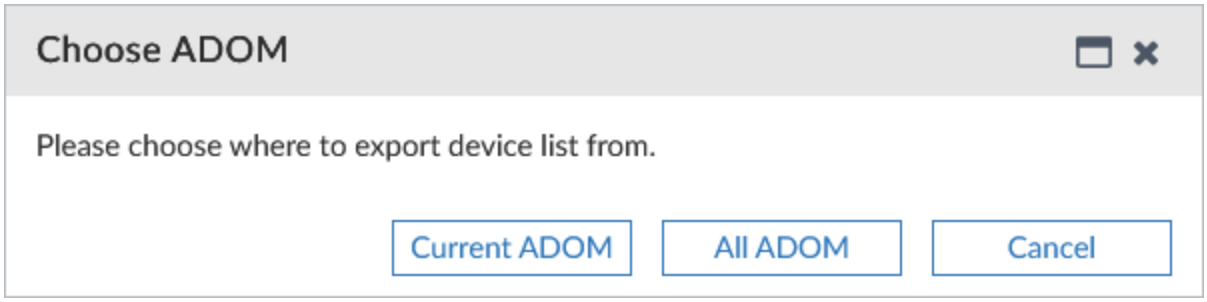


Advanced configuration settings such as dynamic interface bindings are not part of import/export device lists. Use the backup/restore function to backup the FortiManager configuration.

Proper logging must be implemented when importing a list. If any add or discovery operations fail, there must be appropriate event logs generated to help you trace what occurred.

To export a device list to compressed JSON format:

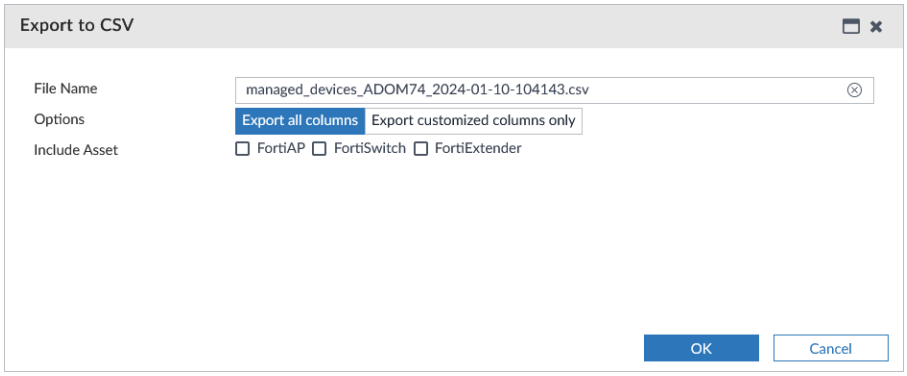
1. Enable the GUI options:
   a. Go to *System Settings* > *Settings*.
   b. Expand the *Display Options on GUI* section, and select *Show Device List Import/Export buttons*.
   c. Click *Apply*.
2. Go to *Device Manager* > *Device & Groups*.
3. In the toolbar, select *Table View* from the dropdown menu.
4. Select a device group, such as *Managed FortiGate*.
5. From the *More* menu, select *Export Device List*.
   The *Choose ADOM* dialog box is displayed.



6. Click *Current ADOM* to export the device list from the current ADOM, or click *All ADOM* to export the device list from all ADOMs.
   A device list in JSON format is exported in a compressed file (`device_list.dat`).

To export a device list to CSV format:

1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. Select a device group, such as *Managed Devices*.
4. From the *More* menu, select *Export to CSV*.
   The *Export to CSV* dialog box is displayed.



5. (Optional) Change the file name.
6. Select whether to export all columns or only customized columns.
7. Select whether to include FortiAP, FortiSwitch, and FortiExtender information.
8. Click *Download*.

To import a device list:

1. Go to *Device Manager* > *Device & Groups*.
2. Select a device group, such as *Managed Devices*.
3. In the toolbar, select *Table View* from the dropdown menu.
4. From the *More* menu, select *Import Device List*.
5. Click *Browse* and locate the compressed device list file (`device_list.dat`) that you exported from FortiManager, or drag and drop the file onto the dialog box.
6. Click *OK*.

Configuring the management address

Configure the management address setting on a FortiManager that is behind a NAT device so the FortiGate can initiate a connection to the FortiManager. By configuring the management address setting in the CLI, FortiManager knows the public IP and can configure it on the FortiGate.

When a FortiGate is discovered by a FortiManager that is behind a NAT device, the FortiManager does not automatically set the IP Address on the FortiGate. This prevents the FortiGate from pointing to the FortiManager's private IP address and initiating the FortiGate-FortiManager (FGFM) tunnel to the FortiManager.

You can use the CLI to configure the management address when the NAT device in front of the FortiManager has a static 1:1 NAT rule.

To configure the management address:

In the FortiManager CLI, enter the following command to define either the management IP address or FQDN.

```
config system admin setting
   set mgmt-addr <string>
   set mgmt-fqdn <string>
```

Configuring multiple management addresses

Multiple IP addresses or FQDNs can be configured for FortiManager. When multiple addresses are listed, the FortiGate will attempt to establish the FGFM tunnel using the first IP/FQDN listed, and if it is unreachable will try each subsequent IP/FQDN until the tunnel is established. Only one address is ever used to establish the FGFM tunnel at a time.

In FortiManager-HA, when listing multiple management addresses, the first address defines the Primary device and the second address is the Secondary device.

To configure multiple management addresses:

1. In the FortiManager CLI, enter the following commands.
   ```
   config system admin setting
   ```

```
set mgmt-fqdn <FQDN/IP 1> <FQDN/IP 2> ...
```

The `set mgmt-fqdn` command can be used with FQDNs and IP addresses.

2. FortiManager automatically pushes the configuration to FortiGate, and on the FortiGate you can see both management addresses listed:

```
config system central-management
   set type fortimanager
   set fmg <FQDN/IP 1> <FQDN/IP 2> ...
end
```

Alternatively, you can configure these settings directly on FortiGate devices.

Verifying devices with private data encryption enabled

FortiManager supports the private data encryption settings on FortiOS. FortiGates with the `private-data-encryption` setting enabled can be managed by FortiManager.

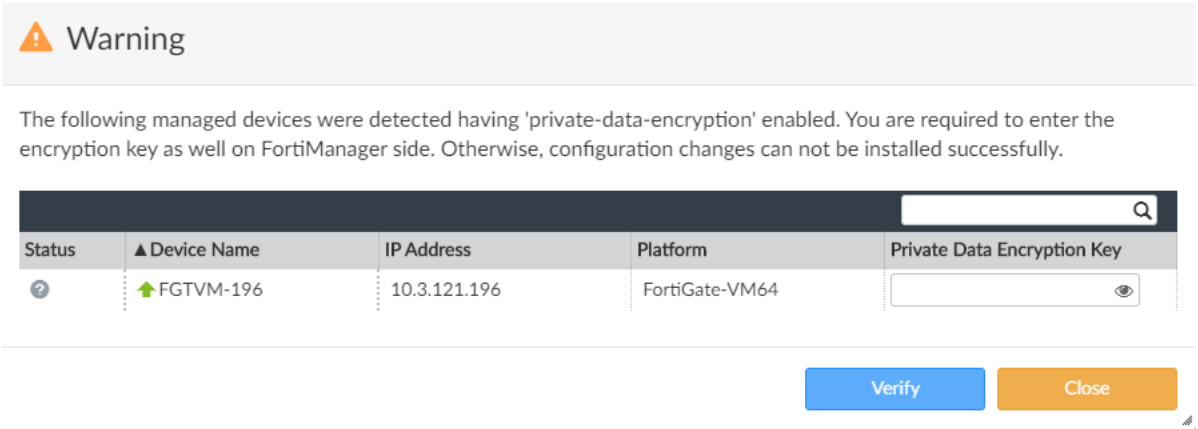
When a FortiGate with the `private-data-encryption` setting enabled is added to FortiManager, FortiManager requires the FortiGate encryption key to be entered in FortiManager to successfully install device configuration settings and manage the added FortiGate. To know more about adding devices to FortiManager, see Add devices on page 91.

FortiManager does not support enabling or disabling the `private-data-encryption` setting on FortiOS. It must be done on the managed FortiGate. To learn more about it, see the FortiOS Administration Guide on the Docs Library.

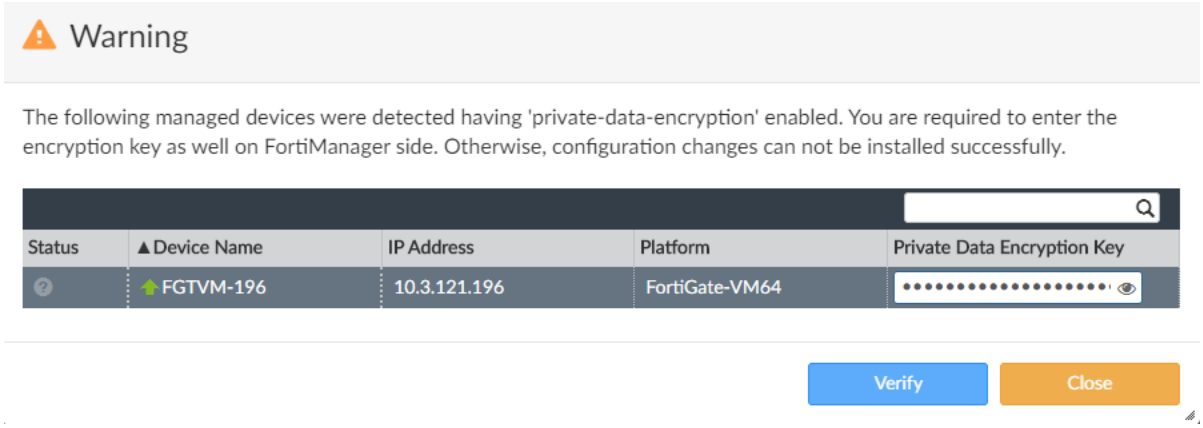
If the `private-data-encryption` setting is enabled on an already managed FortiGate, you must manually retrieve device configuration settings again on the FortiManager.

To verify an added FortiGate with its encryption key on FortiManager:

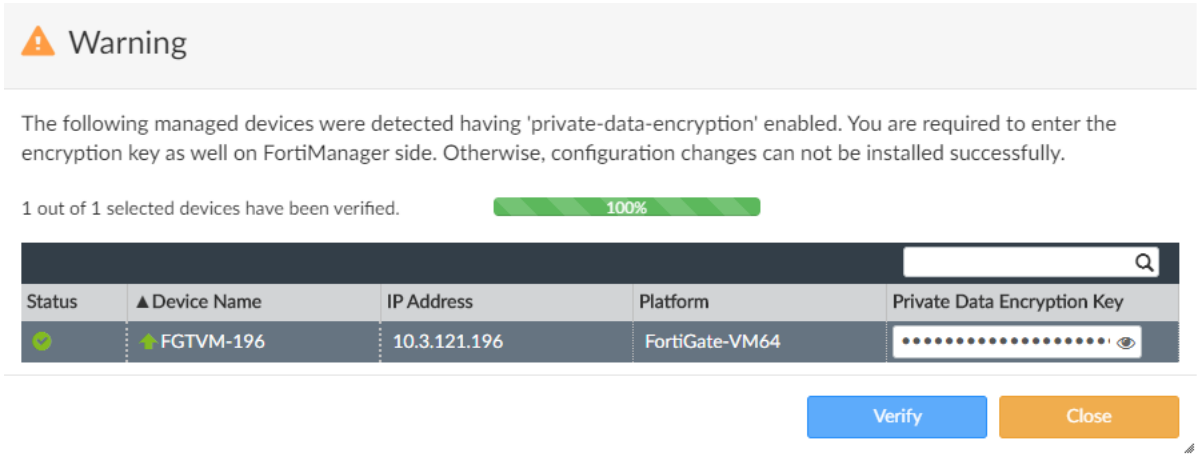
1. Go to *Device Manager* > *Device & Groups*. The *Device Manager* prompts with a *Warning* dialog that requires the FortiGate encryption key to be entered:



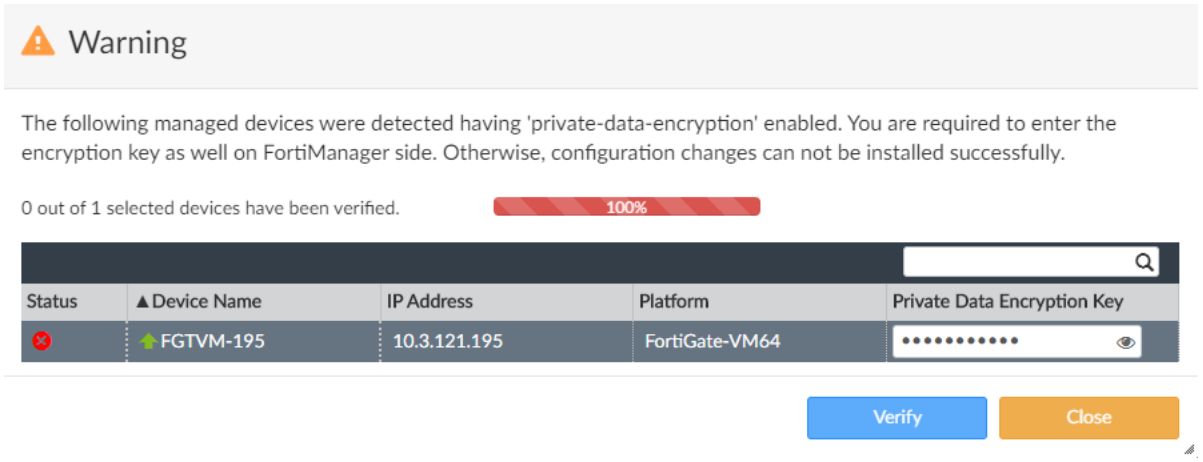
2. Enter the correct encryption key into the *Private Data Encryption Key* field for each of the listed FortiGates. The *Warning* dialog lists all the FortiGates for which the respective encryption keys are required.



3. Click *Verify*. If the encryption key matches, the device is verified.

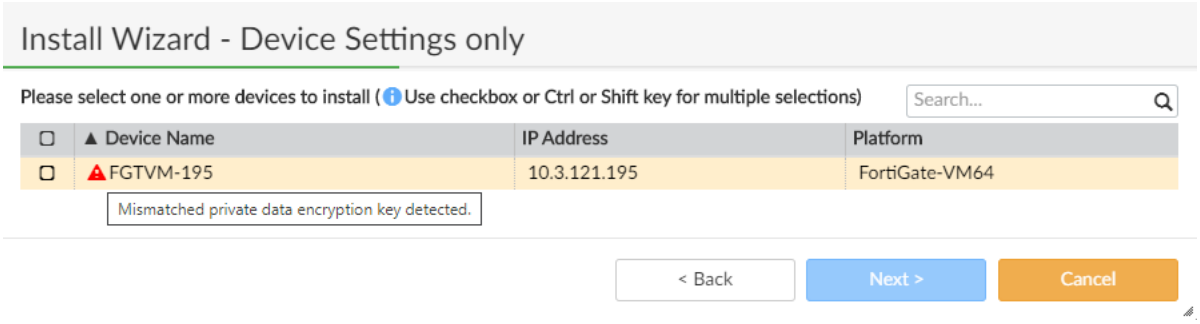


If the encryption key does not match, the verification fails, and you may try again with the correct key.



Once the added FortiGates are verified, you may start managing the added devices.

Every time you try to install configuration settings to the managed FortiGates, FortiManager checks if the FortiGate encryption is correct. If the encryption key is incorrect, the added device is disabled for installation.



You may verify devices again from the *Device Manager* by entering the correct encryption keys for the disabled FortiGates.

Add FortiAnalyzer or FortiAnalyzer BigData

Adding a FortiAnalyzer or FortiAnalyzer BigData device to FortiManager gives FortiManager visibility into the logs on the FortiAnalyzer, providing a Single Pane of Glass on FortiManager. It also enables FortiAnalyzer Features, including:

- *FortiView*
- *Log View*
- *Incidents & Events*
- *Reports*

For information about FortiAnalyzer Features, see FortiAnalyzer Features on page 41. See also Viewing policy rules on page 142 and View logs related to a policy rule on page 426.

To add a FortiAnalyzer or FortiAnalyzer BigData to FortiManager, they both must be running the same OS version, at least 5.6 or later.

FortiAnalyzer BigData-VM and FortiAnalyzer BigData 4500F device are supported.

If FortiAnalyzer Features are enabled, you cannot add a FortiAnalyzer or FortiAnalyzer BigData to FortiManager. See FortiAnalyzer Features on page 41.

In addition, you cannot add a FortiAnalyzer or FortiAnalyzer BigData to FortiManager when ADOMs are enabled with ADOM mode set to *Advanced*.

As of 7.4.1, there are two methods to add a FortiAnalyzer to FortiManager.

- Adding FortiAnalyzer devices using the wizard on page 135
- Adding FortiAnalyzer devices using a fabric connection on page 141

ADOMs disabled

When you add a FortiAnalyzer device to FortiManager with ADOMs disabled, all devices with logging enabled can send logs to the FortiAnalyzer device. You can add only one FortiAnalyzer device to FortiManager, and the FortiAnalyzer device limit must be equal to or greater than the number of devices managed by FortiManager.

When you add additional devices with logging enabled to FortiManager, the managed devices can send logs to the FortiAnalyzer device. The new devices display in the *Device Manager* pane on FortiAnalyzer unit when FortiManager synchronizes with the FortiAnalyzer unit.

ADOMs enabled

When you add a FortiAnalyzer device to FortiManager with ADOMs enabled, all devices with logging enabled in the ADOM can send logs to the FortiAnalyzer device. Following are the guidelines for adding a FortiAnalyzer device to FortiManager when ADOMs are enabled:

- FortiAnalyzer devices can be added to each ADOM, and the FortiAnalyzer device limit must be equal to or greater than the number of devices in the ADOM.
- The same FortiAnalyzer device can be added to more than one ADOM.
- The same ADOM name and settings must exist on the FortiAnalyzer device and FortiManager. The wizard synchronizes these settings for you if there is a mismatch.
- The logging devices in the FortiAnalyzer ADOM and FortiManager ADOM must be the same. The wizard synchronizes these settings for you.
- When one FortiAnalyzer is added to more than one ADOM, FortiAnalyzer features and visibility in the ADOM are limited to the logging devices included in the ADOM.

When you add additional devices with logging enabled to an ADOM in FortiManager, the managed devices can send logs to the FortiAnalyzer device in the ADOM. The new devices display in the *Device Manager* pane on the FortiAnalyzer unit when FortiManager synchronizes with the FortiAnalyzer unit.

Provisioning templates for log settings

After you add a FortiAnalyzer device to FortiManager, you can use FortiManager to enable logging for all FortiGates in the root ADOM (when ADOMs are disabled) or the ADOM (when ADOMs are enabled) by using the log settings in a system template. See System templates on page 281.

Log storage and configuration

Logs are stored on the FortiAnalyzer device, not the FortiManager device. You configure log storage settings on the FortiAnalyzer device; you cannot change log storage settings using FortiManager.

Configuration and data for FortiAnalyzer features

When FortiManager manages a FortiAnalyzer unit, all configuration and data is kept on the FortiAnalyzer unit to support the following FortiAnalyzer features: *FortiView*, *Log View*, *Incidents & Events*, and *Reports*. FortiManager remotely accesses the FortiAnalyzer unit to retrieve requested information for FortiAnalyzer features. For example, if you use the *Reports* pane in FortiManager to create a report, the report is created on the FortiAnalyzer unit and remotely accessed by FortiManager.

Adding FortiAnalyzer devices using the wizard

If the FortiAnalyzer or FortiAnalyzer BigData device is receiving logs from devices that are not managed by FortiManager, the wizard requires you to add the devices to FortiManager by typing the IP address and login credentials for each device. Ensure that you have the IP addresses and login credentials for each device before you start the wizard.

The *Add FortiAnalyzer* option is hidden when you cannot add a FortiAnalyzer unit to the FortiManager unit. For example, the *Add FortiAnalyzer* option is hidden if you have already added a FortiAnalyzer unit to the FortiManager unit (when ADOMs are disabled) or to the ADOM (when ADOMs are enabled). You also cannot add a FortiAnalyzer unit when you have enabled FortiAnalyzer features for the FortiManager unit.

FortiManager does not recognize VM devices by default. In order to add a FortiAnalyzer-VM to FortiManager, you must first enable recognition of VM devices. See Adding VM devices on page 118.

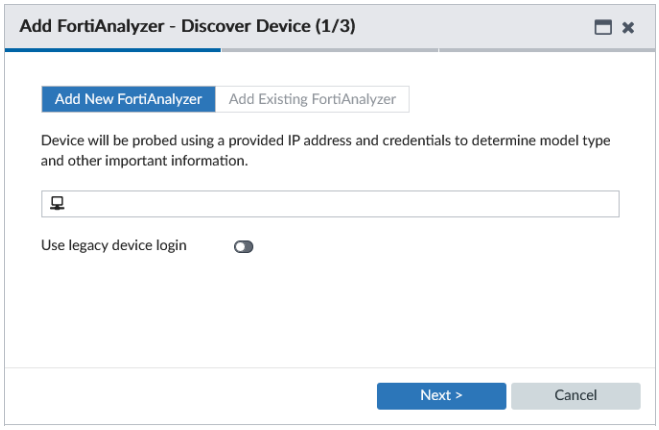
The FortiManager and FortiAnalyzer versions must be the same on both devices.

After completing the wizard, ensure that you enable logging on the devices, so the managed FortiAnalyzer can receive logs from the devices. You can enable logging by using the log settings in a system template. See System templates on page 281.

Add a new FortiAnalyzer or FortiAnalyzer BigData using the wizard

To add a FortiAnalyzer device using the wizard:

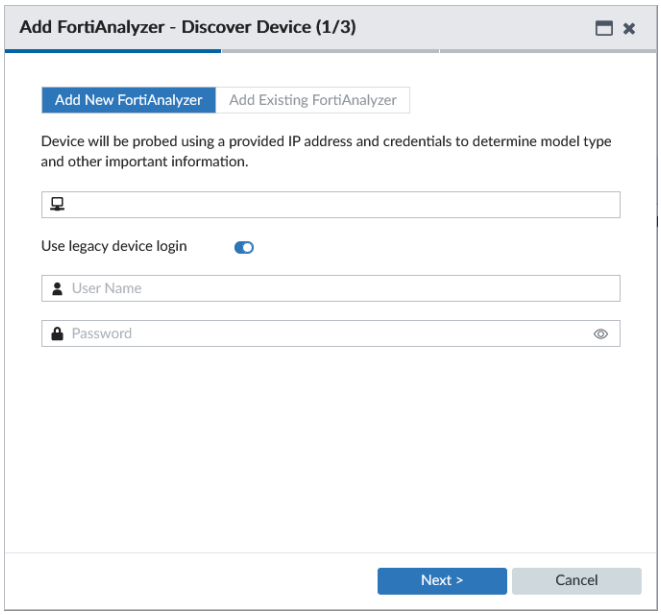
1. Confirm that the FortiAnalyzer device supports the number of devices managed by FortiManager.
   - If ADOMs are disabled, ensure that the FortiAnalyzer device limit is equal to or greater than the number of devices managed by FortiManager.
   - If ADOMs are enabled, ensure that the FortiAnalyzer device limit is equal to or greater than the number of devices in the ADOM.
2. If ADOMs are enabled, select the ADOM to which you want to add the device.
3. Go to *Device Manager* > *Device & Groups*.
4. Click the *Add Device* dropdown and select *Add FortiAnalyzer*. The wizard opens.
   The *Add FortiAnalyzer* option is hidden if you've already added a FortiAnalyzer device.



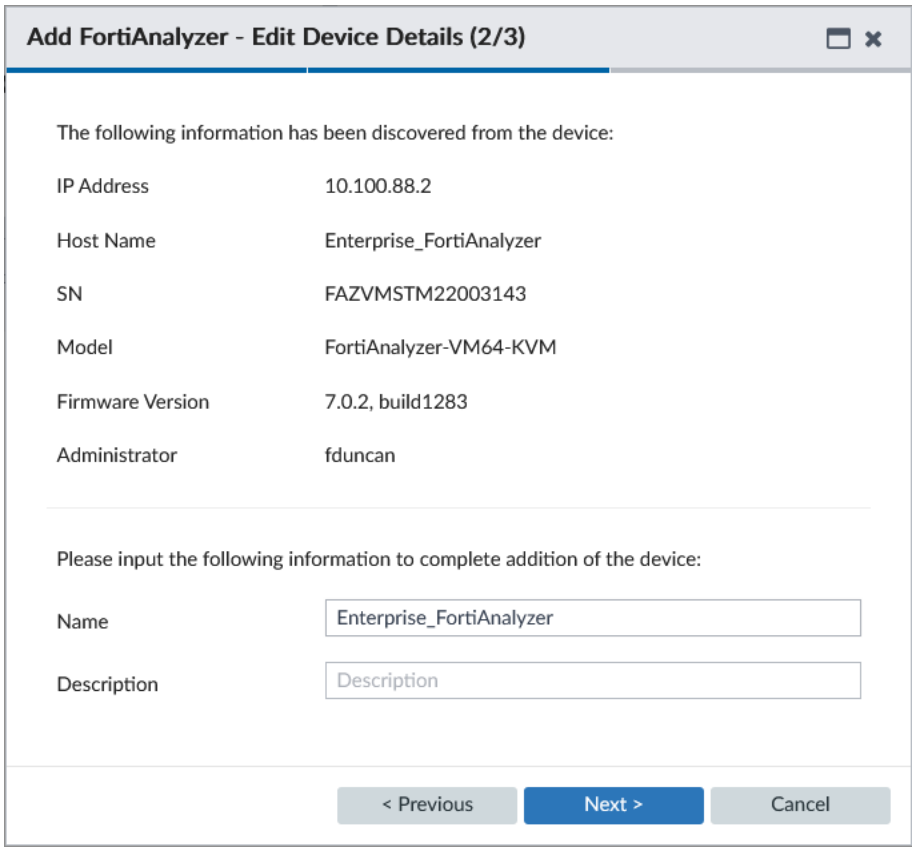
5. Use the *Add New FortiAnalyzer* tab to add new FortiAnalyzer devices to FortiManager.
   When adding a FortiAnalyzer device that is already being managed on another ADOM in FortiManager,

select the *Add Existing FortiAnalyzer* option. See Add an existing FortiAnalyzer using the wizard on page 140.

6. Toggle *Use legacy device login* to *ON*.
   The *User Name* and *Password* boxes are displayed.



7. Type the IP address, user name, and password for the device, then click *Next*.
   FortiManager probes the IP address on your network to discover FortiAnalyzer device details, including:
   - IP address
   - Host name
   - Serial number
   - Device model
   - Firmware version (build)
   - High Availability status
   - Administrator user name



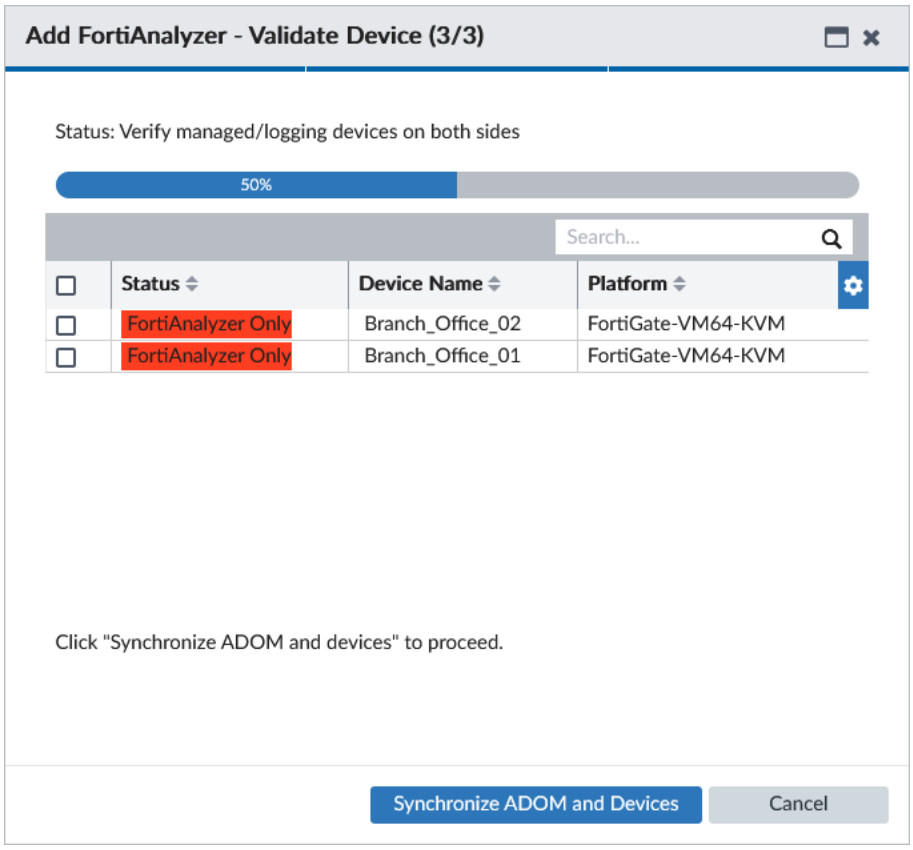
8. Configure the following settings if desired, and click *Next*:

Name	Type a unique name for the device. The device name cannot contain spaces or special characters (optional).
Description	Type a description of the device (optional).

The wizard performs the following tasks:

- Compares the ADOM name and configuration as well as devices between FortiAnalyzer and FortiManager
- Verifies the devices in the *Device Manager* pane for FortiAnalyzer with the devices in the *Device Manager* pane for FortiManager

If any discrepancies are found, information is displayed in the *Status* column, and you can resolve the discrepancies by clicking the *Synchronize ADOM and Devices* button.



The following table describes the different statuses:

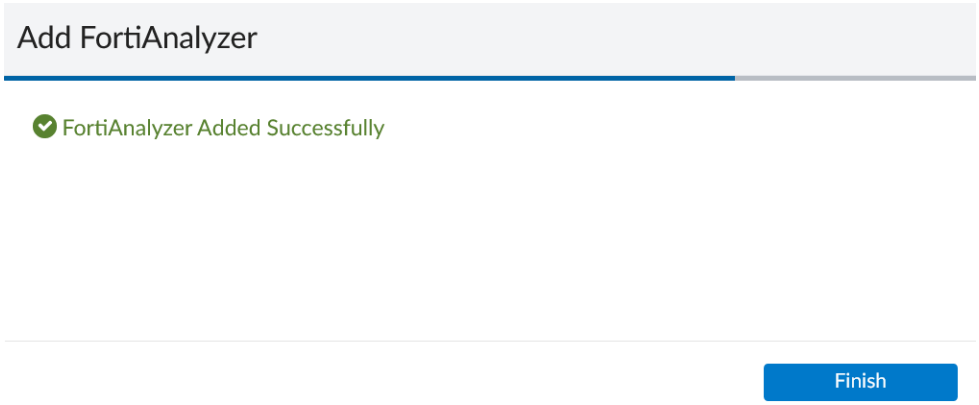
Status	Description
FMG Only	The device was located in FortiManager, but not FortiAnalyzer. If you proceed with the wizard, the device will be added to FortiAnalyzer too.
FAZ Only	The device was located in FortiAnalyzer, but not FortiManager. If you proceed with the wizard, the device will be added to FortiManager too. The login and password for the device is required to complete the wizard.
Sync	The device was located in both FortiAnalyzer and FortiManager without any differences, and the wizard will synchronize the device between FortiManager and FortiAnalyzer.
Mismatched	The device was located in both FortiAnalyzer and FortiManager with some differences, and the wizard will synchronize the device settings between FortiManager and FortiAnalyzer to remove the differences.

If the FortiManager ADOM does not exist on the FortiAnalyzer device, a warning is displayed. You can add the ADOM and devices to FortiAnalyzer by clicking the *Synchronize ADOM and Devices* button.

9. Click *Synchronize ADOM and Devices* to continue.
   a. If you are synchronizing devices from FortiAnalyzer to FortiManager, type the IP address and login for each device, and click *OK* to synchronize the devices.
   b. After the devices successfully synchronize, click *OK* to continue.

The devices, ADOM name, and ADOM version are synchronized between FortiAnalyzer and FortiManager.

10. Click *Finish* to close the wizard.

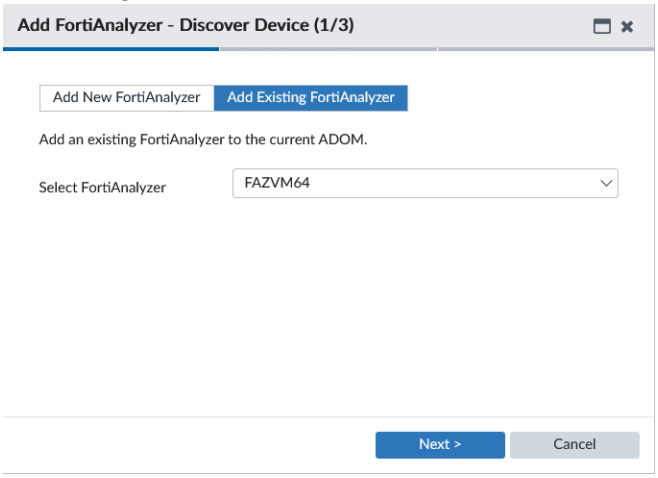


The FortiAnalyzer device is displayed on the *Device Manager* pane as a *Managed FortiAnalyzer*, and FortiAnalyzer features are enabled.

Add an existing FortiAnalyzer using the wizard

To add an existing FortiAnalyzer device to a new ADOM:

1. Confirm that the FortiAnalyzer device supports the number of devices managed by FortiManager.
2. Select the ADOM to which you want to add the device.
3. Go to *Device Manager* > *Device & Groups*.
4. Click the *Add Device* dropdown and select *Add FortiAnalyzer*. The wizard opens.
5. Click the *Add Existing FortiAnalyzer* tab, and select the existing FortiAnalyzer from the dropdown. FortiManager retrieves the device details from the local database.



6. Click *Synchronize ADOM and Devices* to continue.
   The devices, ADOM name, and ADOM version are synchronized between FortiAnalyzer and FortiManager.
7. Click *Finish* to close the wizard.

Adding FortiAnalyzer devices using a fabric connection

FortiManager does not recognize VM devices by default. In order to add a FortiAnalyzer-VM to FortiManager, you must first enable recognition of VM devices. See Adding VM devices on page 118.

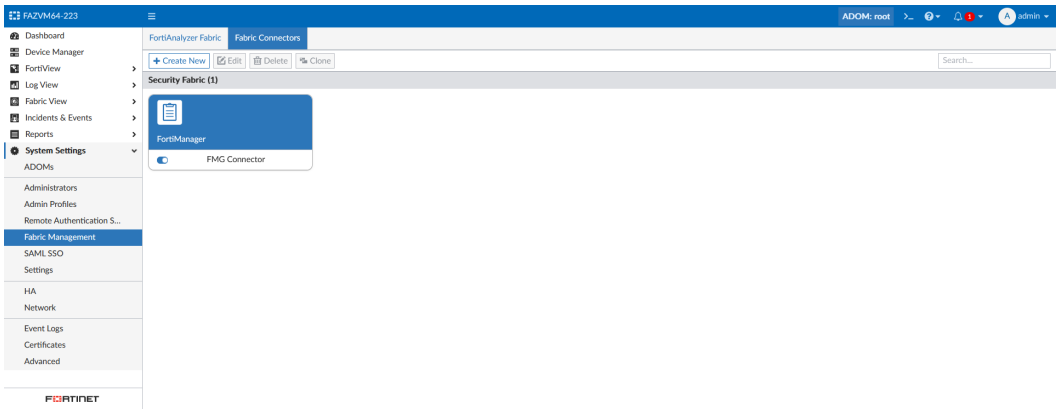
To add a remote FortiAnalyzer using a fabric connection:

The following configuration is required in the FortiManager CLI before adding a FortiAnalyzer using a fabric connection:

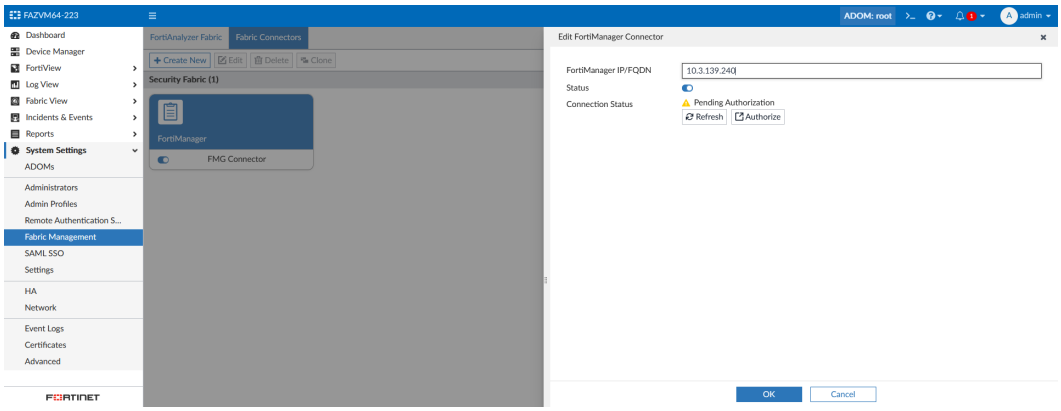
```
config system csf
   set status enable
   set accept-auth-by-cert enable
   set downstream-access enable
end
```

In both the FortiAnalyzer and FortiManager CLI, under `config system interface`, the port's `allowaccess` setting must include `fabric`.

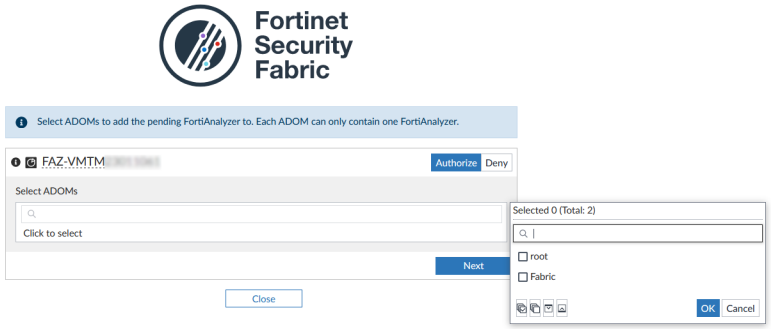
1. In the FortiAnalyzer, go to *System Settings* > *Fabric Management* > *Fabric Connectors*.



2. Select the FortiManager connector and click *Edit*.
   Alternatively, you can double-click the connector, or right-click the connector and select *Edit*.
3. In the *FortiManager IP/FQDN* field, enter the IP of the FortiManager.
4. Toggle the *Status* to *Enabled*.
5. Click *OK* and wait for the connection.
6. Once the connection status is *Pending Authorization*, click *Authorize*.

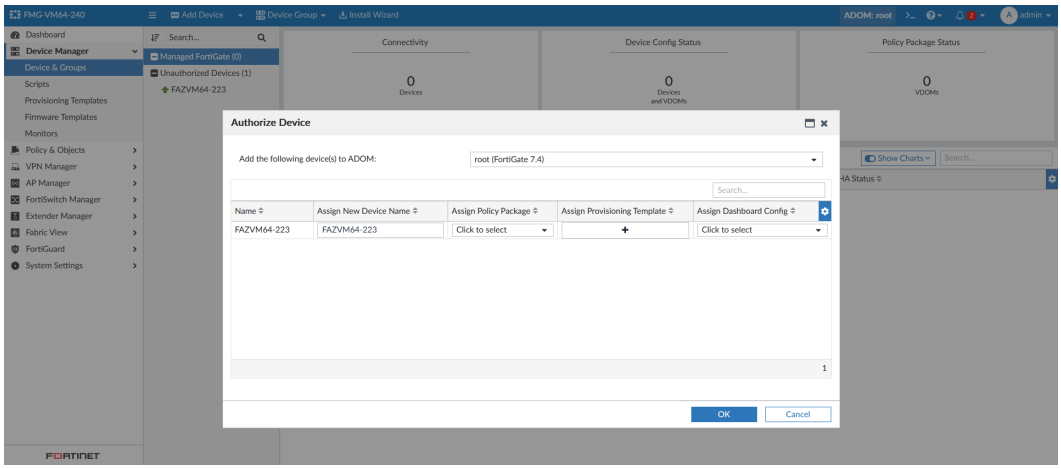


7. In the authorization page, select the ADOM to add the FortiAnalyzer to and click *Next*.



8. After authorizing, the FortiAnalyzer is added to FortiManager under *Device Manager* > *Device & Groups* > *Managed FortiAnalyzer*.

   Alternatively, you can authorize the FortiAnalyzer from the FortiManager GUI.



Viewing policy rules

When a FortiAnalyzer is managed by a FortiManager, you can view the logs that the FortiAnalyzer unit receives. In the *Log View* module, you can also view the policy rules by clicking a policy ID number.

See Add FortiAnalyzer or FortiAnalyzer BigData on page 134.

To view policy rules:

1. Go to *Log View* > *Traffic*.
2. Click the number in the *Policy ID* column.
   The *View Policy* window is displayed, showing the policy rules.
3. Click *Return* to close the window.

Support for FortiAnalyzer HA

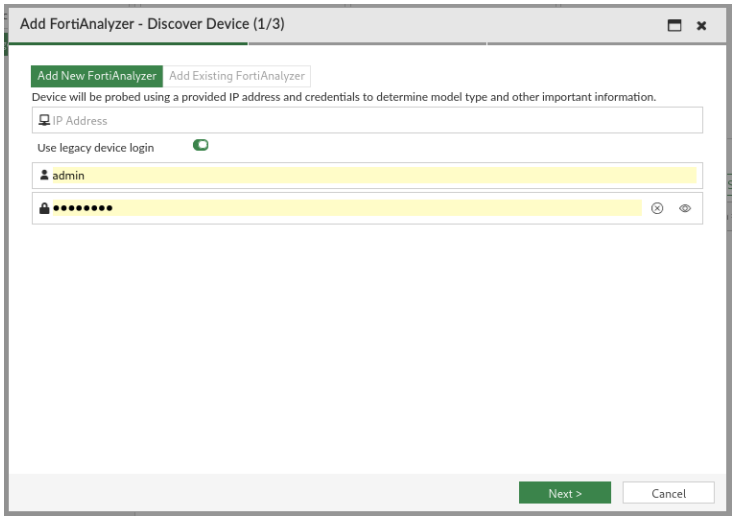
You can manage FortiAnalyzer HA using FortiManager.

FortiManager retrieves the cluster member list and updates the information whenever it changes, including when there is a FortiAnalyzer HA failover event or a change in cluster members.

Adding a FortiManager HA cluster provides FortiManager with the same visibility into FortiAnalyzer logs, single pane of glass experience, and FortiAnalyzer features that adding a standalone FortiAnalyzer does, but with the additional benefit of redundancy in cases where the FortiManager loses connectivity with the Primary FortiAnalyzer.

To add a FortiAnalyzer HA cluster to FortiManager:

1. Go to *Device Manager* > *Device & Groups*.
2. Click the down arrow next to *Add Devices*. Select *Add FortiAnalyzer*.
   The *Add FortiAnalyzer - Discover Device* dialog opens.



3. On the *Add New FortiAnalyzer* tab, enter the *IP Address* for the FortiAnalyzer HA cluster, and click *Next*.
   The IP address can be the cluster's VIP address or the IP address of the Primary FortiAnalyzer if a VIP address is not used in the configuration, for example in an active-active geo-redundant HA cluster.

In 7.4.7 and later, the FortiManager IP address and serial number is configured for central-management on both the Primary and Secondary FortiAnalyzer when it is added to FortiManager.

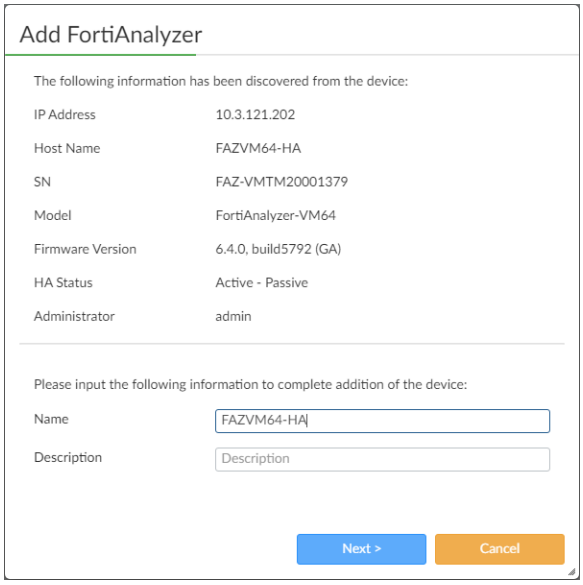
In 7.4.6 and earlier, you must manually specify the FortiManager IP address and serial number in the `central-management` settings on the Primary FortiAnalyzer in order for FortiAnalyzer to be able to reconnect back after failover event.

For example:

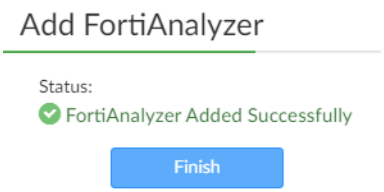
```
config system central-management
   set fmg <VIP or IP address>
   set serial-number <serial number>
end
```

The FortiAnalyzer HA cluster is discovered with its HA status information.

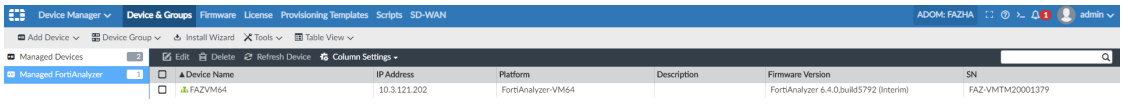
4. Click *Next* to continue.



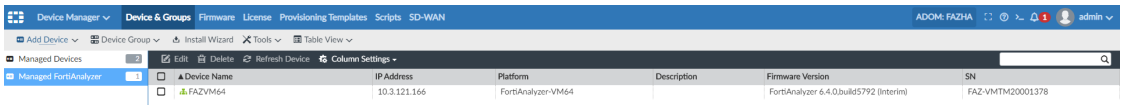
5. FortiAnalyzer HA is added successfully. Click *Finish*.



6. In the tree menu, select *Managed FortiAnalyzer*. The device status icon is shown as the HA cluster and the SN is shown as the primary SN.



FortiManager DVM gets an update after the failover on FortiAnalyzer in 300 seconds. Here, the previous primary "FAZ-VMTM20001379" becomes the secondary and the new primary is "FAZ-VMTM20001378".



You can get the HA status update immediately, select the FortiAnalyzer device and either click *Refresh Device* from the toolbar, or right-click and select *Refresh*.

To check the DVM device list in the CLI:

1. View the DVM device list once FortiAnalyzer HA is added to FortiManager:
   ```
   diagnose dvm device list
   ```
   It will have correct HA cluster information, including member list and role.
2. View the DVM device list after the failover on FortiAnalyzer:
   ```
   diagnose dvm device list
   ```
   It will have the updated HA cluster information. The previous primary changes to secondary and vice versa.

Add VDOM

You can add a VDOM to a FortiGate by using the content pane or by using the device database. This topic describes how to use the content pane. For information on using the device database, see Device DB - System Virtual Domain on page 213.

Two types of VDOM modes available: Split-Task VDOM and Multi VDOM.

The number of VDOMs you can add is dependent on the device model. For more information, see the *Maximum Values Table* in the Fortinet Document Library.

This section contains the following topics:

- Adding a split-task VDOM on page 145
- Adding a multi VDOM on page 146

Kubernetes Service must be enabled on the server side for AWS, Azure, OCI and, GCP for Kubernetes to function for the particular cloud platform. Once the service is enabled, Kubernetes can be configured for the particular cloud platform in FortiManager.

Adding a split-task VDOM

The Split-Task VDOM mode creates two VDOMs automatically: *FG-traffic* and *root*. Additional VDOMs cannot be added.

FG-traffic is a regular VDOM and can contain policies, UTM profiles and it will handle the traffic like the no-VDOM mode. The *root* VDOM is only for management and it cannot have policies or profiles.

To add a Split-Task VDOM to a FortiGate device:

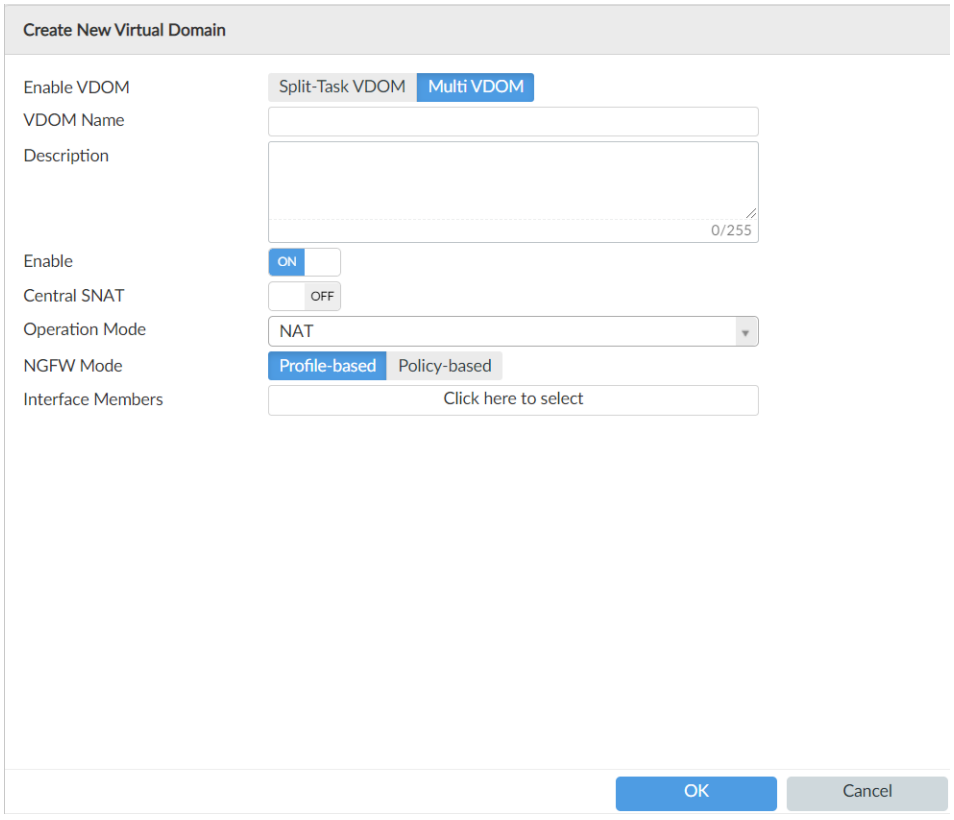
1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. In the tree menu, click the group. The devices in the group are displayed in the content pane.
4. In the content pane, right-click a device and select *Add VDOM*.
5. Select *Split-Task VDOM*, and click *OK*.

Adding a multi VDOM

The Multi VDOM mode allows you to create multiple VDOMs as per your license.

To add a Multi VDOM to a FortiGate device:

1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. In the tree menu, click the group. The devices in the group are displayed in the content pane.
4. In the content pane, right-click a device and select *Add VDOM*.
5. Click *Multi VDOM*
6. The *Create New Virtual Domain* window opens.



7. Configure the following options, and click *OK*.

VDOM Name	Type a name for the new virtual domain.
Description	Optionally, enter a description of the VDOM.
Enable	Select to enable the VDOM.
Central SNAT	Toggle *ON* to enable, and toggle *OFF* to disable.
Operation Mode	Select either *NAT* or *Transparent*.
NGFW Mode	Select either *Profile-based* or *Policy-based*.
Interface Members	Click to select each port one by one.
Management IP Address 1 / 2	Type the management IP addresses and network masks for the VDOM. This setting is only available when *Operation Mode* is *Transparent*.
Gateway	Type the gateway IP address. This setting is only available when *Operation Mode* is *Transparent*.



Kubernetes Service must be enabled on the server side for AWS, Azure, OCI and, GCP for Kubernetes to function for the particular cloud platform. Once the service is enabled, Kubernetes can be configured for the particular cloud platform in FortiManager.

Device groups

When viewing a device group entry from the *Managed FortiGate* table on *Device Manager > Device & Groups*, the device group entry is displayed in an expanded hierarchical view and the device listings within the group entry are displayed by default.

You can collapse or expand the device group entry in the table. From the toolbar above the table, you can create, edit, and delete device groups.



The maximum number of device groups that can be created is the same as the maximum number of devices/VDOMs supported for your VM license or model. See the FortiManager data sheet on https://www.fortinet.com/ for information about the maximum number of supported devices/VDOMs for your VM license or device.

Default device groups

When you add devices to FortiManager, devices are displayed in default groups based on the type of device. For example, all FortiGate devices are displayed in the *Managed FortiGate* group. You can create custom device groups.

Adding custom device groups

You can create a custom device group and add devices to it.

To add custom device groups:

1. Go to *Device Manager* > *Device & Groups*.
2. From the *Device Group* menu, select *Create New Group*.
3. Enter a name for the group.
   A group name can contain only numbers (0-9), letters (a-z, A-Z), and limited special characters (- and _).
4. Optionally, enter a description of the group.
5. Add devices to the group as needed. Devices can also be added and removed after the group has been created.
6. Click *OK* to create the group.



FortiManager allows nested device groups. For example, you can create *Device Group A* and add it under *Device Group B*.

Managing device groups

You can manage device groups from the *Device Manager* > *Device & Groups* pane. From the *Device Group* menu, select one of the following options:

Option	Description
Create New	Create a new device group.
Edit Group	Edit the selected device group. You cannot edit default device groups.
Delete Group	Delete the selected device group.



You must delete all devices from the group before you can delete the group. You must delete all device groups from an ADOM before you can delete an ADOM.

Table view

On the *Device Manager* > *Device & Groups* pane, you can choose *Table View* from the toolbar to monitor devices. The *Table View* displays a list of managed devices in a view that resembles a table.

The table view includes a quick status bar, and you can customize the columns.

This section also includes the following topics:

- Using the quick status bar on page 149
- Viewing managed devices on page 150
- Viewing configuration status on page 151
- Viewing policy package status on page 152
- Editing device information
- Setting values for required meta fields on page 155
- Customizing columns on page 156
- Displaying Security Fabric topology on page 157
- Refreshing a device
- Using device group tree menus on page 158
- Installing VM licenses on managed devices on page 159

Using the quick status bar

You can quickly view the status of devices on the *Device Manager* pane by using the quick status bar, which contains the following donut charts:

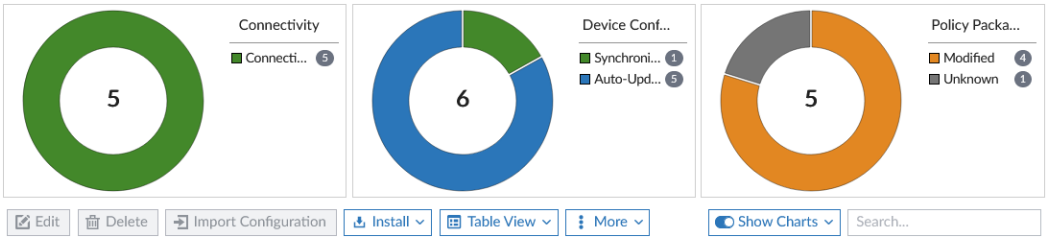
- *Connectivity*
- *Device Config Status*
- *Policy Package Status*
- *FortiAP Status*
- *FortiSwitch Status*
- *Firmware Status*
- *FortiGuard License*

By default, the *Show Charts* toggle is enabled to display the quick status bar. You can select which charts appear in the quick status bar by selecting them in the *Show Charts* dropdown. Alternatively, you can hide the quick status bar and all its charts by disabling the *Show Charts* toggle.

Mouse over the charts to see more information in a tooltip. Click a section of a chart to filter the charts and the table by that information. You can apply multiple filters across the charts. Once filtered, a filter icon appears next to the chart title; click the filter icon to remove the filter.

To view the quick status bar:

1. Go to *Device Manager* > *Device & Groups*, and select a device group of authorized devices.
   The quick status bar is displayed above the table view. If it is not visible, enable the *Show Charts* toggle.



Viewing managed devices

On the *Device Manager* pane in *Table View*, you can view all managed devices and access detailed status information.

You can customize what columns are displayed in *Table View*. See Customizing columns on page 156.

To view managed devices:

1. Go to *Device Manager > Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. In the tree menu, click the device group name, for example, *Managed Devices*. The devices in the group are displayed in the content pane.
   The following columns are displayed. You can filter columns that have a Filter icon.

Device Name	The name of the device and its connectivity status.
Auto-link Status	Displays the auto-link status of model devices as either *Enabled* or *Disabled*. You can change the auto-link status by editing the device or by clicking on the status in the column and selecting *Disable Auto-link* or *Enable Auto-link*.
Config Status	Displays the status of the configuration for the managed device. For details, see Viewing configuration status on page 151.
Host Name	The host name for the device (available for managed devices).
IP Address	The IP address of the device.
Platform	The platform of the device (available for managed devices).
Description	Description of the device.
HA Status	The HA status of the device.
Serial Number	The serial number of the device.
Controller Counter	The number of each device type controlled by this device, such as FortiAPs and FortiSwitches.
Management Mode	Management mode of the device.
Firmware Version	Displays the version of the firmware currently installed on the managed device. If a vulnerability has been identified for the FortiGate firmware, a notification will display below the firmware version. Click the notification to review the details, including the *IR*, *Title*, *Severity*, and *CVE* for the vulnerability. Alternatively, click the notification in the banner to open the *Vulnerable Devices* pane where you can create a firmware template to upgrade the affected devices. See Creating firmware templates on page 379.
Upgrade Status	Displays whether a firmware upgrade is available for the managed device.

Firmware Template	Displays the name of the assigned firmware template. The firmware template specifies what firmware version should be installed on the device. A status icon indicates whether the device is running the firmware version specified in the firmware template.
Policy Package Status	Displays the status of the policy package for the managed device. For details, see Viewing policy package status on page 152. Click on the policy package name to go to view and manage the package. See Managing policy packages on page 414.
Provisioning Templates	Displays one of the following: • The name of each assigned provisioning template. • The name of the assigned template group. Hover the mouse over the assigned template or group to display and access an edit option.
FortiGuard License	Status of the FortiGuard license for the device.
Company/Organization	The company or organization information.
Contact Email	Displays the email of a contact for the managed device.
Contact Phone Number	Displays the phone number of a contact for the managed device.
Address	Displays the geographical location of the managed device by address.

Viewing configuration status

On the *Device Manager* pane, you can view the configuration status for managed devices.

For a description of other columns on the *Device Manager* pane, see Viewing managed devices on page 150.

To view configuration status:

1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. In the tree menu, click the device group name, for example, *Managed Devices*. The devices in the group are displayed in the content pane.
   The following table identifies the different config statuses.

Config Status	Icon	Description
Synchronized	Green check ✓	Configurations are synchronized between FortiManager and the managed device.
Modified	Yellow triangle ⚠	Configurations are modified on FortiManager and not synchronized between FortiManager and the managed device.

Config Status	Icon	Description
Auto-update	Green check	Configurations modified on the managed device are auto synced to FortiManager.
Modified (recent auto-updated)	Yellow triangle	Configurations are modified on FortiManager and configurations modified on the managed device are auto synced to FortiManager.
Out of Sync	Red X	Configurations are modified on the managed device and not synced to FortiManager.
Conflict	Red X	When one of the following happens: • Install failed • Configurations are modified on both FortiManager and the managed device, and not auto synced to FortiManager.
Unknown	Gray question mark	When one of the following happens: • Connection goes down • No revision is generated, like added model device

Resolving a configuration in conflict

A config status in *Conflict* can be resolved by retrieving the configuration from the managed device or by re-installing FortiManager's stored configuration:

1. *Using the configuration from the Managed Device*
   a. Go to *Device Manager*, and select the managed device from the *Managed FortiGate* tree menu to enter the device database.
   b. On the *Dashboard > Summary* page, select the revision history icon in the *Configuration and Installation* widget.
   c. Select the revision from the managed device, and click *Retrieve Config*. The FortiManager will retrieve the selected revision from the managed device. See Device DB - configuration management on page 205.
   d. Once the configuration has been retrieved, re-import the policy to synchronize the policy package status between the managed device and FortiManager. See Import Configuration wizard on page 173.
2. *Using the configuration from FortiManager*:
   a. Go to *Device Manager*, and select the managed device from the devices table.
   b. Select *Install > Install Wizard > Install Device Settings (Only)*. See Install device settings only on page 183.
   The device settings stored in FortiManager are installed on the managed device.

Viewing policy package status

On the *Device Manager* pane, you can view the policy package status for managed devices.

For a description of other columns on the *Device Manager* pane, see Viewing managed devices on page 150.

To view policy package status:

1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. In the tree menu, click the device group name, for example, *Managed Devices*. The devices in the group are displayed in the content pane.
   The following table identifies the different available policy package statuses.

Policy Package Status	Icon	Description
Imported	Green check ✓	Policies and objects are imported into FortiManager.
Installed	Green check ✓	Policies and objects have been installed from FortiManager to the managed device.
Modified	Yellow triangle ⚠	Policies or objects are modified on FortiManager.
Out of Sync	Red X ✗	Policies or objects are modified on the managed device.
Unknown with policy package name	Gray question mark ?	Configurations of the managed device are retrieved on FortiManager after being imported/installed. For example, when you retrieve a policy package after upgrading FortiOS, the policy package status changes to *Unknown*.
Never Installed	Yellow triangle ⚠	The assigned policy package is not the result of an import for this device, and the package has not been installed since it has been assigned to this device.

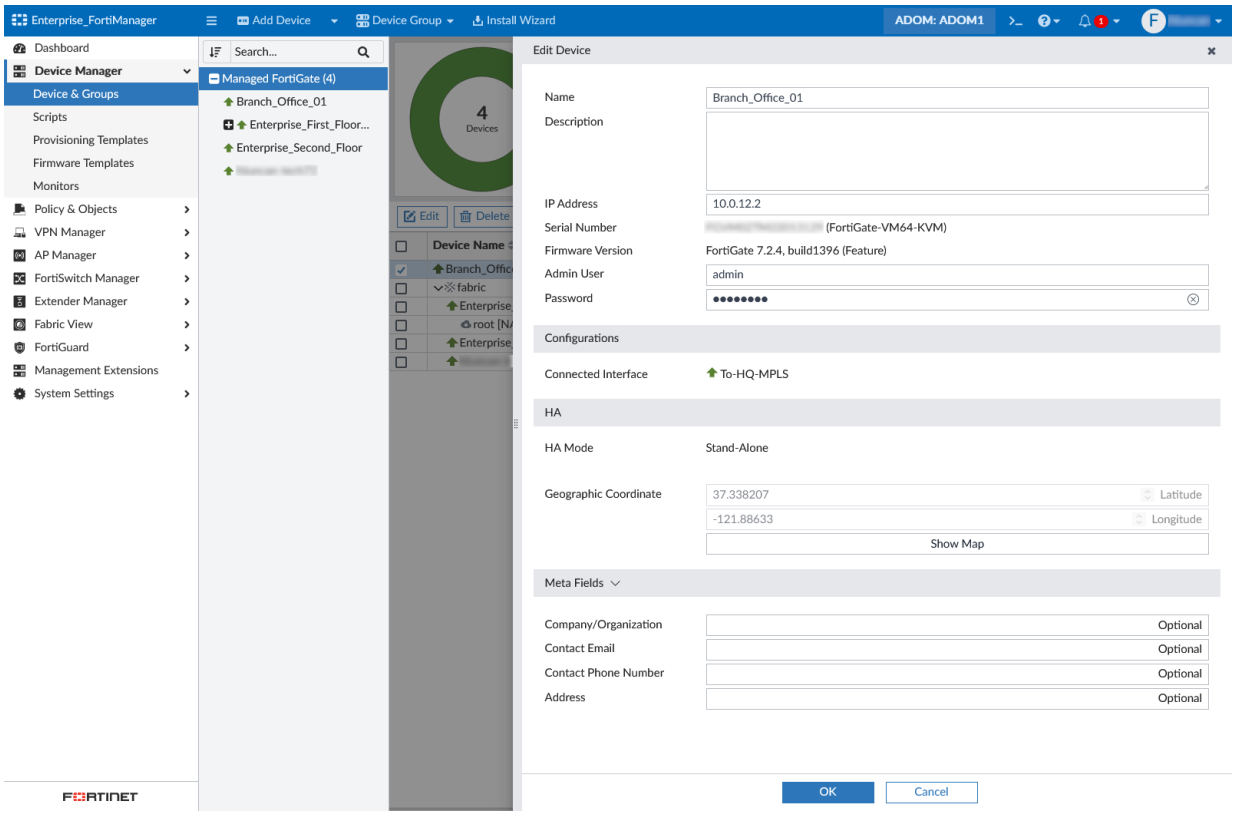
Editing device information

Use the *Edit Device* page to edit information about a device. The information and options available on the *Edit Device* page depend on the device type, firmware version, and which features are enabled. Some settings are only displayed when FortiAnalyzer features are enabled.

To edit information for a device or model device:

1. Go to *Device Manager* > *Device & Groups*.
2. In the tree menu, select the device group.

3. In the content pane, select the device or model device and click *Edit*, or right-click on the device and select *Edit*.
   The *Edit Device* pane displays.



4. Edit the device settings and click *OK*.

Name	Change the name of the device.
Description	Type a description of the device.
IP Address	Change the IP address.
Pre-Shared Key	Enter the model device's pre-shared key. Select *Show Pre-shared Key* to see the key. This option is only available when editing a model device that was added with a pre-shared key.
Automatically link to real device	Select to automatically authorize the device to be managed by FortiManager when the device is online. This option is only available when editing a model device.
Serial Number	Displays the serial number of the device. For model devices added with a pre-shared key, this will show the device model.
Firmware Version	Displays the firmware version of the device.
Admin User	Change the administrator user name for the device.

	If the FortiManager serial number is not specified for central management on FortiGate, the admin user/password specified here is used by FortiManager to login to the FortiGate. This also includes FortiManager geo-HA failover where the FortiGate may only have the primary FortiManager IP configured.
Password	Change the administrator user password for the device.
Connected Interface	Displays the name of the connected interface, if the connection is up.
HA Mode	Displays whether the FortiGate unit is operating in stand-alone or high availability mode.
Geographic Coordinate	Displays the latitude and longitude of the device. Click *Show Map* to view and edit the device location. The default location is `0,0`. This field is used to display the location of the device on maps throughout the GUI. See also Google Map integration on page 41.
Meta Fields	Displays default and custom meta fields for the device. Optional meta fields can be left blank, but required meta fields must be defined. See also Setting values for required meta fields on page 155.
Company/Organization	Optionally, enter the company or organization information.
Contact Email	Optionally, enter the contact email.
Contact Phone Number	Optionally, enter the contact phone number.
Address	Optionally, enter the address where the device is located.

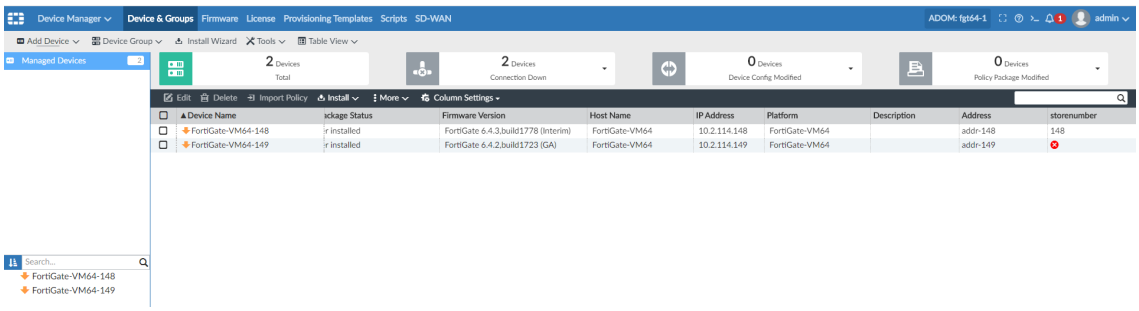
Setting values for required meta fields

When a required meta field is defined for a device object, a column automatically displays on the *Device Manager* pane. The column displays the value for each device. When the required meta field lacks a value, an exclamation mark displays, indicating that you must set the value.

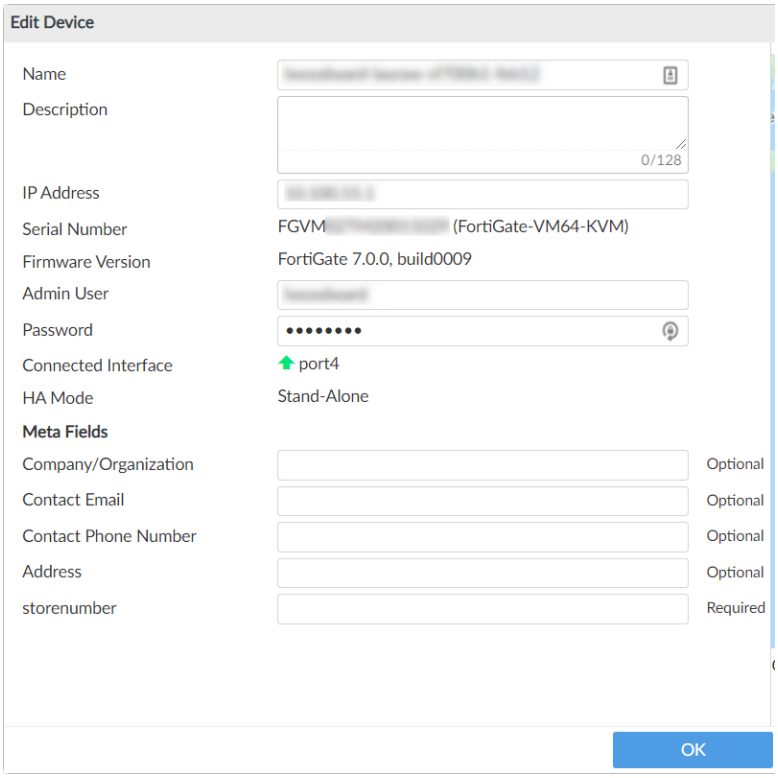
See also Meta Fields on page 967.

To set values for required meta fields:

1. Go to *Device Manager > Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. View the columns.
   A column displays for required meta fields.
   In the following example, a column for each of the following required meta fields is displayed: *Address* and *storenumber*. A value of *148* is defined for one device, but no value is defined for the other device.



4. Right-click the device that lacks a value, and select *Edit*.
   The *Edit Device* pane is displayed.



5. Under *Meta Fields*, complete the options labeled as *Required*, and click *OK*.
   The value displays on the *Device Manager* pane.

Customizing columns

You can choose what columns display on the content pane for the *Device Manager* > *Device & Groups* pane.

Column settings are not available for all device types. The default columns also vary by device type.

You can filter columns that have a *Filter* icon. Column filters are not available for all columns.



The columns available in the *Column Settings* menu depends on features enabled in FortiManager. When the FortiAnalyzer feature set is disabled, all related settings are hidden in the GUI.

To customize columns:

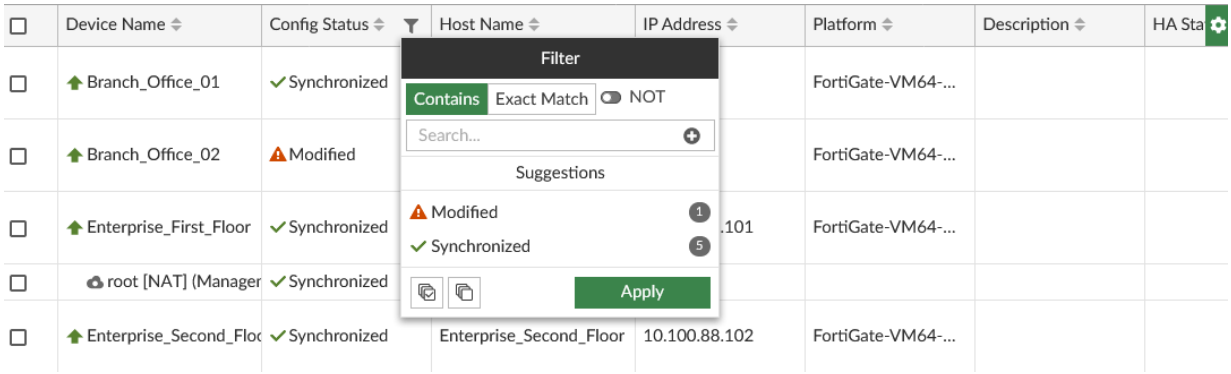
1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. Click the *Configure Table* icon, and select the columns you want to display.

Apply filters to the Device Manager table

The FortiManager Device Manager includes filters that can be applied to columns in the device table. Multiple filters can be applied simultaneously.

To apply filters to the Device Manager table:

1. Go to *Device Manager*.
2. Click on the filter icon next to a column header. The *Filter* dialog option is displayed for the selected column.
   - Filter options include *Contains*, *Exact Match*, and *Not* which can be applied to a keyword search.
   - Filter suggestions are populated with identified values for the selected column below the search bar.



3. After the filter has been configured, click *Apply*. The filter icon color changes to indicate that a filter is applied to that column.

You can remove the filter on a column by clicking the filter icon and then clicking *Remove*.

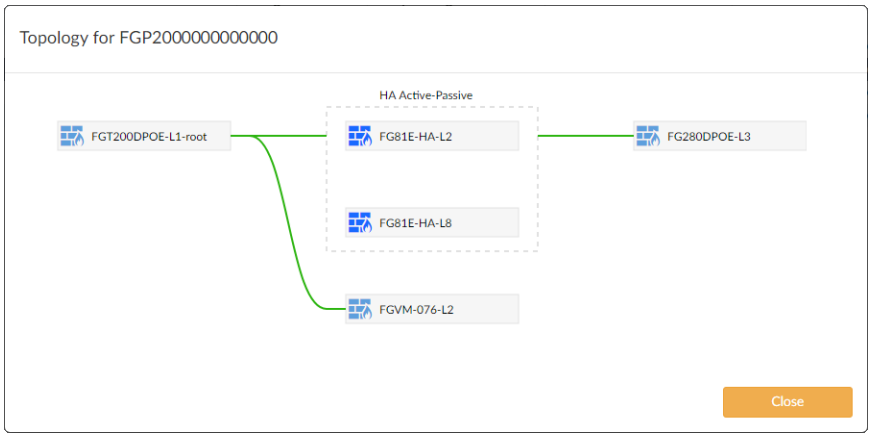
Displaying Security Fabric topology

For Security Fabric devices, you can display the Security Fabric topology.

To display the Security Fabric topology:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager* > *Device & Groups*
3. In the toolbar, select *Table View* from the dropdown menu, and click the *Devices Total* tab in the quick status bar.
4. Right-click a Security Fabric device and select *Fabric Topology*.
   A pop-up window displays the Security Fabric topology for that device.

If you selected *Fabric Topology* by right-clicking a device within the Security Fabric group, the device is highlighted in the topology. If you selected *Fabric Topology* by right-clicking the name of the Security Fabric group, no device is highlighted in the topology.



Refreshing a device

Refreshing a device refreshes the connection between the selected devices and the FortiManager system. This operation updates the device status and the FortiGate HA cluster member information.

To refresh a device:

1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. In the tree menu, click the device group name, for example, *Managed Devices*. The devices in the group are displayed in the content pane.
4. In the content pane, select a device.
5. Select *More* > *Refresh Device*. The *Update Device* dialog box opens to show the refresh progress.

Using device group tree menus

In *Table View* when *Display Device/Group tree view in Device Manager* is enabled, the left tree menu displays devices under device groups, and you can right-click devices and access menu options.

By default, device group tree menu is enabled, and devices are displayed in the following groups in the tree menu:

- *Managed FortiGate*
- *Logging Devices*, if FortiAnalyzer Features are enabled
- *Unauthorized Devices*, if any unauthorized devices are present in the root ADOM

If you have created custom device groups, the custom groups and the devices they contain are displayed in the left tree menu too. See Device groups on page 147.

The following table identifies what menu options you can access when you right-click a device in the left tree menu:

Device Group	Right-Click Menu Options
Managed Devices and custom groups	• Quick Install (Device DB) • Import Policy • Re-install Policy • Policy Package Diff • Edit • Delete • Grouping • Add VDOM • Run Script • Firmware Upgrade
Logging Devices	• Edit • Delete
Unauthorized Devices	• Authorize • Hide • Delete

To use device groups:

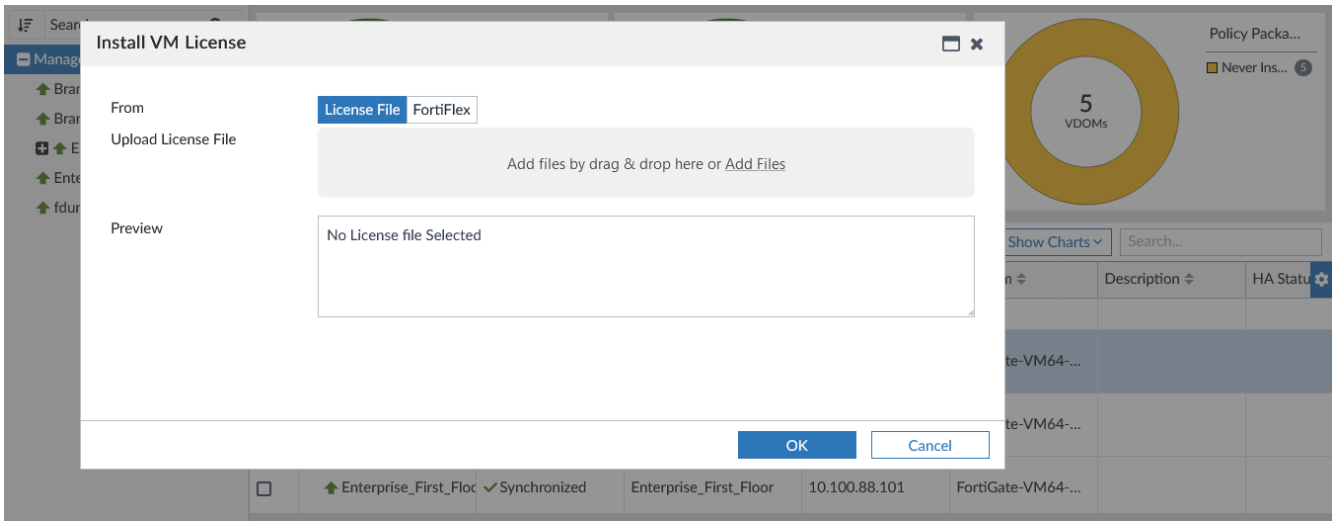
1. Enable device groups:
   a. Go to *System Settings > Advanced > Advanced Settings*.
   b. Beside *Display Device/Group tree view in Device Manager*, select *Enable*, and click *Apply*.
2. Go to *Device Manager > Device & Groups*.
3. In the toolbar, select *Table View* from the dropdown menu.
   In the left tree menu, devices are displayed under device groups.
4. In the left tree menu, right-click a device to access menu options.

Installing VM licenses on managed devices

You can install VM licenses on managed FortiGate and FortiWeb VMs using the FortiManager *Device Manager*, enabling management and replacement of license files without having to directly access the VM.

FortiManager retrieves the license information from a provided license file or FortiFlex configuration, and then provides the license to the managed device. Because the managed device gets the license information directly from FortiManager, this feature can be used to install licenses on VMs that are operating in an air-gapped

environment.



The device manager supports VM license installation with two options:

- Installing licenses using a BYOL license file on page 160
- Installing licenses using the FortiFlex connector on page 160

Installing licenses using a BYOL license file

To install a FortiGate BYOL VM license file:

1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, make sure *Table View* is selected.
3. Select a managed device from the table, and right-click on it to view the context menu.
4. Select *Install VM License*. The *Install VM License* wizard opens.
   Select *License File*, and drag-and-drop your license file into the *Upload License File* field.
5. You can preview the license file selected, and click *OK*.

Installing licenses using the FortiFlex connector

When you are installing VM licenses using a FortiFlex connector, you must first configure the FortiFlex connector as well as created a *Configuration* and *Flex Entitlement* for the device on FortiFlex. See Creating FortiFlex connectors on page 779 and the FortiFlex documentation.

To install a FortiGate license using the FortiFlex connector:

1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, make sure *Table View* is selected.
3. Select a managed device from the table, and right-click on it to view the context menu.
4. Select *Install VM License*.The *Install VM License* wizard opens.

5. Select *FortiFlex Connector*, and select the previously configured FortiFlex connector in the dropdown menu.
6. Select a *FortiFlex Configuration*. Available configurations are pulled automatically from FortiFlex using the selected connector.
7. Click *OK*.

After a license has been installed onto the device using FortiManager, the device will reboot to complete the installation.



When a custom certificate is used by the FortiGate admin for central management, FortiManager requires that the certificate must contain the FortiGate serial number either in the CN or SAN. Without the serial number, the tunnel connection will fail, and FortiManager will be unable to provide a license to the FortiGate using the FortiFlex connector.

In order to use the FortiFlex connector to install a new license to a FortiGate using a custom certificate without a valid serial number, this check can be disabled using the CLI.

```
config system global
   set fgfm-peercert-withoutsn enable
end
```

To install a FortiWeb license using the FortiFlex connector:

1. Configure the FortiManager update service on port 443.
   For example:
   ```
   config system interface
      edit <port>
         set ip <ip & netmask>
         set serviceaccess fgtupdates webfilter-antispam
         set update-service-ip <ip & netmask>
      next
   end
   ```
2. Go to *Device Manager > Device & Groups*.
3. In the toolbar, make sure *Table View* is selected.
4. Select a managed device from the table, and right-click on it to view the context menu.
5. Select *Install VM License*.The *Install VM License* wizard opens.
6. Select *FortiFlex Connector*, and select the previously configured FortiFlex connector in the dropdown menu.
7. Select a *FortiFlex Configuration*. Available configurations are pulled automatically from FortiFlex using the selected connector.
8. Click *OK*.

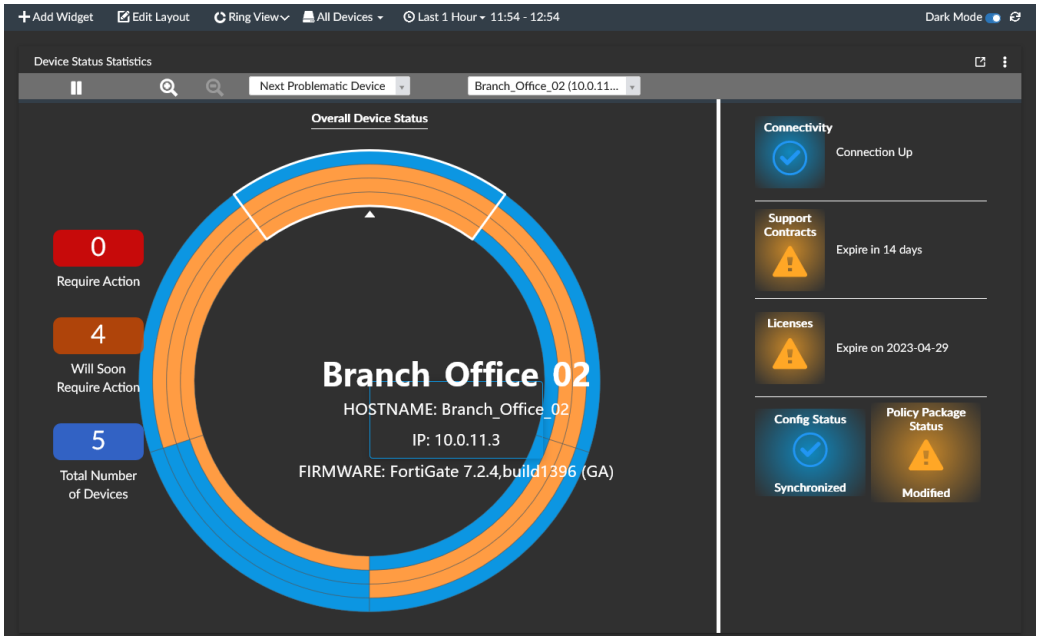
After a license has been installed onto the device using FortiManager, the device will reboot to complete the installation.

Ring view

To prevent timeout, ensure *Idle Timeout* is greater than the widget's *Refresh Interval*. See Idle timeout on page 1058 and Settings icon on page 164.

On the *Device Manager > Device & Groups* pane, you can choose *Ring View* from the toolbar to monitor devices.

The *Ring View* dashboard communicates the configuration status between FortiManager and managed devices.



The center of the *Ring View* dashboard includes a circular chart that automatically rotates to communicate configuration status about managed devices. You can control what information displays by using the following controls at the top of the widget:

Playing and Paused	Click to start and pause the automatic rotation of the circle chart.
Zoom in and out	Use the *Zoom in* and *Zoom out* tools to enlarge and shrink areas of the circle chart. When zoomed in, use the scroll bar to move across the circle chart.
Rotate Options	Specify whether the chart automatically displays information about *Next Problematic Device* or *One by One*.
Search Devices	Select a device and display its information.
Settings icon	Change the settings of the widget. Widgets have settings applicable to that widget, such as how many of the top items to display, *Time Period*, *Refresh Interval*, and *Chart Type*.
Remove widget icon	Delete the widget from a predefined or custom dashboard.

The *Ring View* dashboard includes the following information:

Overall Device Status	A summary of the status of all devices. The following colors are used to communicate status: • Red indicates action is required now. • Orange indicates action is required soon. • Blue indicates no action is required. Each device is represented by a segment in the circle. Click each segment to display the following information about the selected device in the middle of the circle: • Host name • IP address • Firmware version Information about the following statuses of the selected device is also displayed on the right: • Connectivity status • Support Contracts • Licenses • Configuration Status and Policy Package Status The colored rings in the circle correspond to the status information on the right. The outer ring in the circle corresponds with the *Connectivity* status. The second most outer ring corresponds to the *Supports Contracts* status, and so on.
Require Action	The number of devices that require configuration changes. The number is displayed in a red box.
Will Soon Require Action	The number of devices that will require configuration changes in the near future. The number is displayed in an orange box.
Total Number of Devices	The total number of devices displayed on the dashboard. The number is displayed in a blue box.
Connectivity	Displays the connectivity status for the selected device. Click the *Connectivity* link to display the selected device on the *Device Manager > Device & Groups* pane.
Support Contracts	Displays the expiration date of the support contracts for the selected device. Click the *Support Contracts* link to display the selected device on the *Device Manager > License* pane.
Licenses	Displays the expiration date of the licenses for the selected device. Click the *Licenses* link to display the selected device on the *Device Manager > License* pane.
Configuration Status	Displays the configuration status for the selected device. Click the *Configuration Status* link to display the selected device on the *Device Manager > Device & Groups* pane.
Policy Package Status	Displays the policy package status for the selected device. Click the *Policy Package Status* link to display the selected device on the *Device Manager > Device & Groups* pane.

Using the monitors dashboard

FortiView monitors contain widgets that provide network and security information. Use the controls in the dashboard toolbar to work with a dashboard.

Add Widget	Add widgets from the list available.
Edit Layout	Remove, resize, or move widgets on a predefined dashboard.
Devices	Select the devices to include in the widget data.
Time Period	Select a time period from the dropdown menu, or set a custom time period.
Dark Mode	Enable/disable dark mode. Dark mode shows a black background for the widgets in the dashboard.
Refresh	Refresh the data in the widgets.
Hide Side-menu or Show Side-menu	Using the main toolbar, you can hide or show the tree menu on the left. In a typical SOC environment, the side menu is hidden and dashboards are displayed in full screen mode.

Use the controls in the widget title bar to work with widgets.

Settings icon	Change the settings of the widget.

Customizing the monitors dashboard

You can add any widget to a custom or predefined dashboard. You can also move, resize, or remove widgets. You cannot rename or delete a predefined dashboard. To reset a predefined dashboard to its default settings, open the dashboard and click *Edit Layout* > *Reset Layout*.

To create a dashboard:

1. In *FortiView*, click the menu icon for *Custom Views*.
   Mouse-over *Custom Views* to display the menu icon.
2. From the shortcut menu, click *Create New*.
3. Specify the *Name* and whether you want to create a blank dashboard or use a template.
   If you select *From Template*, specify which predefined dashboard you want to use as a template.
4. Click *OK*. The new dashboard appears in the tree menu.
5. Select widgets to include on the dashboard, and click *Save Changes*.

To add a widget:

1. Select the predefined or custom dashboard where you want to add a widget.
2. Click *Add Widget* to see a list of available widgets. Select the widget(s) you would like to add.
3. When you have finished adding widgets, click *Save Changes* to close the *Add Widget* pane.

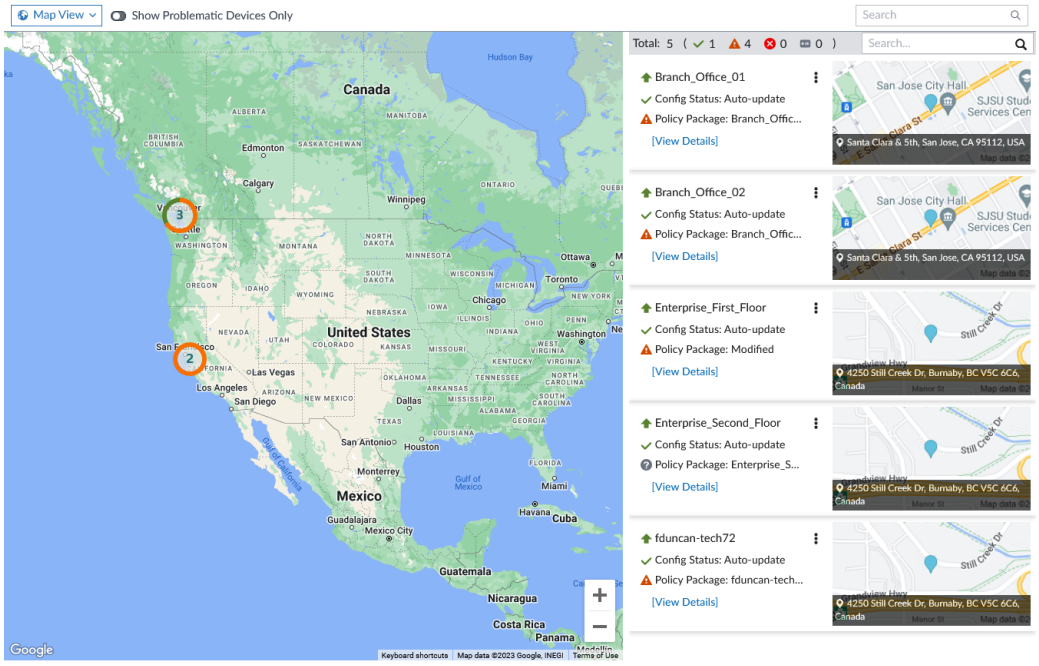
Map view

On the *Device Manager > Device & Groups* pane, you can choose *Map View* from the toolbar to monitor devices.

The *Map View* displays the location of managed devices on Google Maps. With *Map View* you view and configure the location of FortiGate devices on the map. You can also manage devices directly from *Map View*.

To monitor devices from Map View:

1. Go to *Device Manager > Device & Groups*.
2. In the toolbar, select *Map View* from the dropdown menu.
3. Map view shows device location on Google Maps, and a combined status in Green, Orange, and Red colors.
   - Green - Shows devices are healthy. The policy package configuration and device configuration are in sync.
   - Orange - Shows a warning status. The device configuration status or policy package configuration status is *Out of Sync*. Or, there is no policy imported or no policy package installed.
   - Red - Shows an error status. Copy has failed, installation has failed or device connection is down.



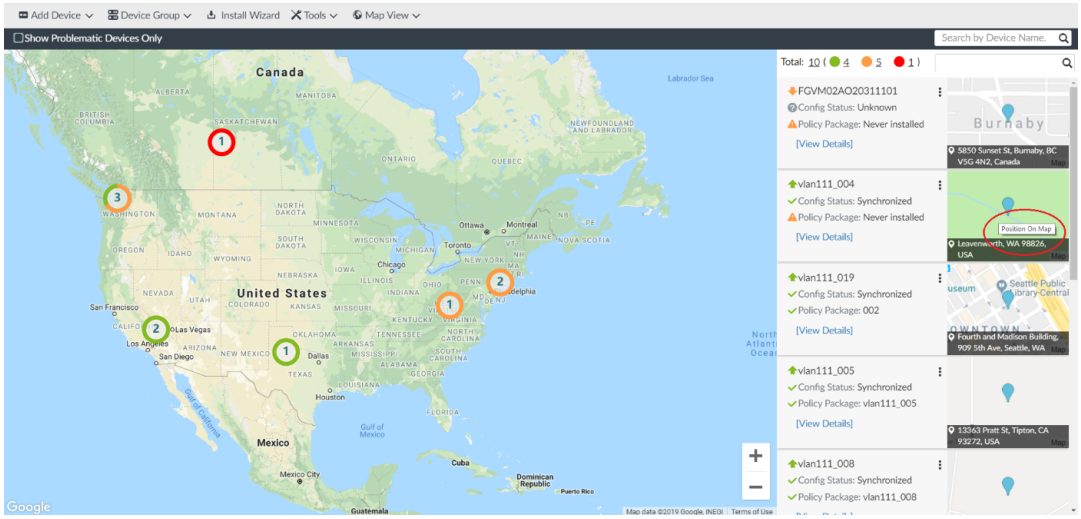
Positioning devices on the map

On *Map View*, you can position devices on the map to assign an address to each device. You can also filter the view to display only devices with unknown locations to help you position those devices on the map.

To position devices on the map:

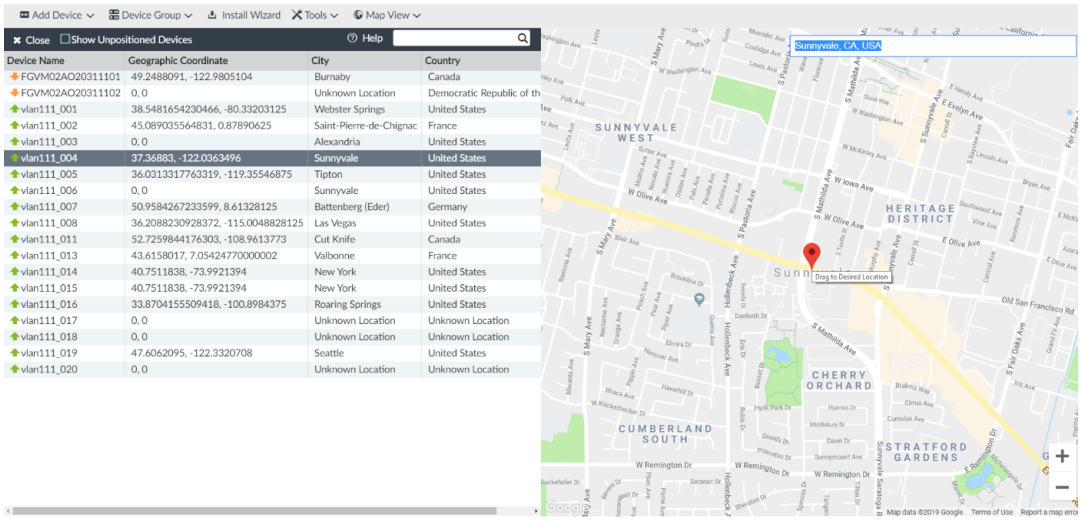
1. Go to *Device Manager > Device & Groups*.
2. In the toolbar, select *Map View* from the dropdown menu.

3. On the right pane, click a device on a small map.



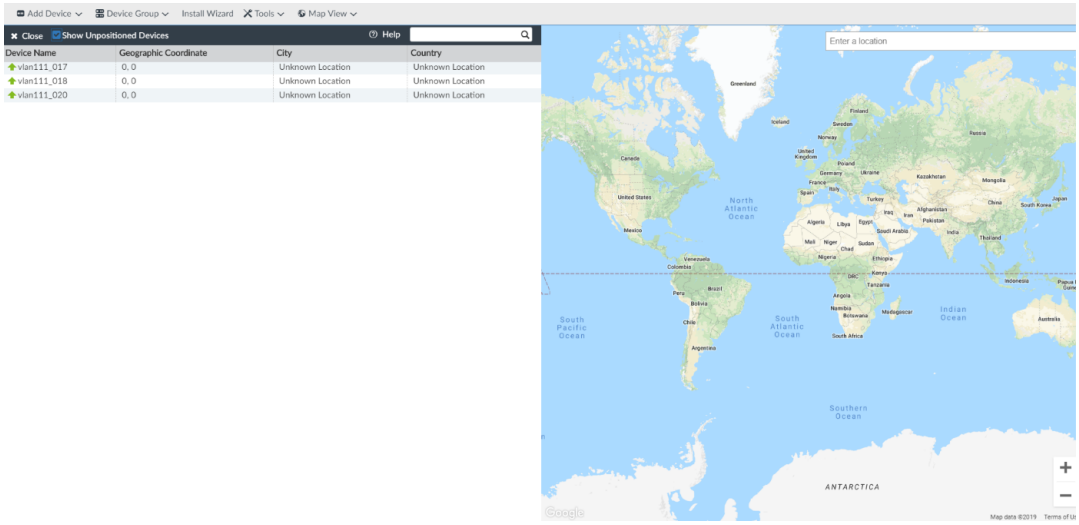
The small map opens and displays an *Enter a location* box for the selected device.

4. In the *Enter a location* box, type the city name, and press *Enter*.
The device is positioned in the city on the map.



5. On the map, drag the device to the desired location in the city.

6. Select the *Show Unpositioned Devices* to display only devices with an unknown location and position them.



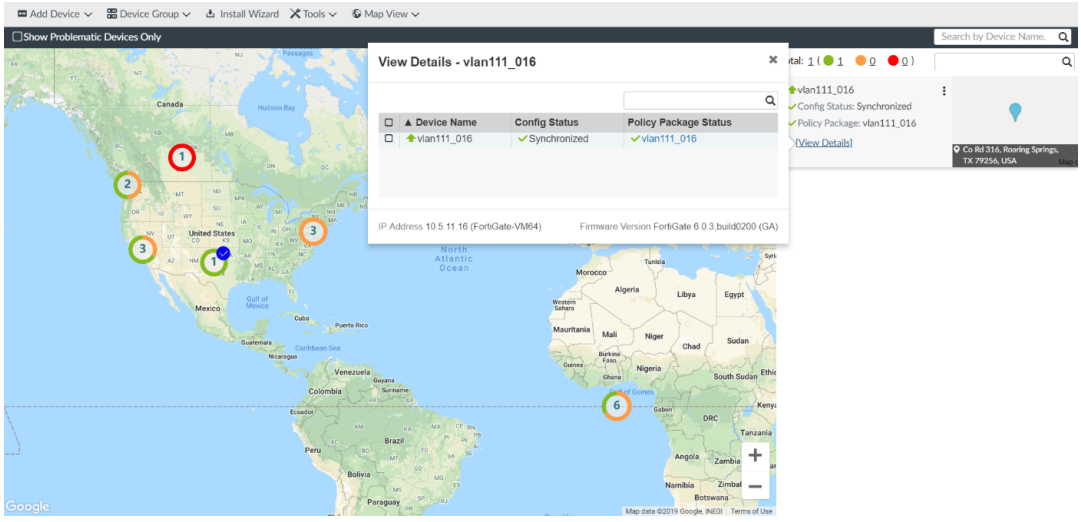
7. Click *Close*.

Viewing device details

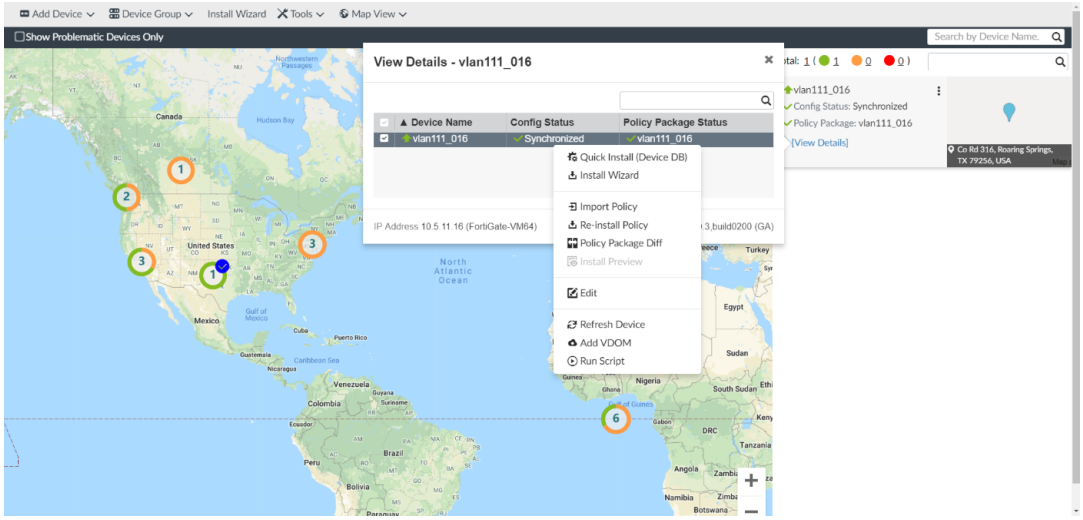
On *Map View*, you can view device configuration status and policy package status. You can also right-click a device to display a menu and run various operations.

To view device details:

1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, select *Map View* from the dropdown menu.
3. For the device, click *View Details*.



4. Right-click the device to display a menu of options and run various operations such as *Quick Install*, *Install Wizard*, *Import Policy*, *Re-install Policy*, *Policy Package Diff*, *Edit*, *Refresh Device*, *Add VDOM*, and *Run Script*.

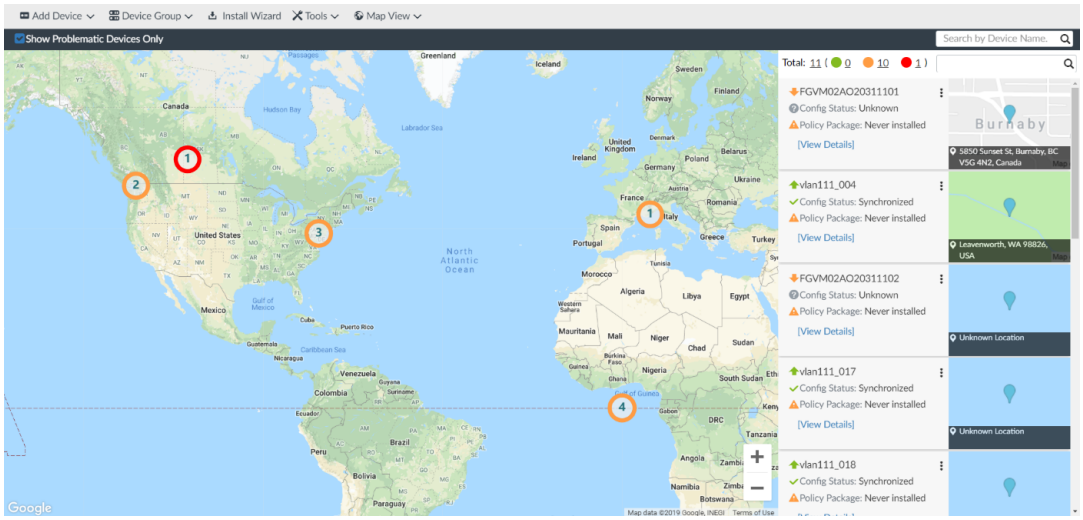


Viewing problematic devices

On *Map View*, you can filter the display to view only devices with problematic statuses.

To view problematic devices:

1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, select *Map View* from the dropdown menu.
3. Select the *Show Problematic Devices Only* checkbox.
   Only problematic devices are displayed on the map, and the right pane identifies problematic devices with *Orange* or *Red* status.



Folder view

On the *Device Manager > Device & Groups* pane, you can choose *Folder View* from the toolbar to monitor devices. The *Folder View* lets you organize devices within a tree menu. In *Folder View* , you can create, nest, and move folders in the tree menu. You can also move devices between folders.

In *Folder View*, you can also view in one pane each managed FortiGate and all access devices connected to the FortiGate, such as FortiAPs, FortiSwitches, and FortiExtenders. You can view the firmware version installed on each device, and you can assign a firmware template to the FortiGate that also includes firmware for access devices, such as FortiAPs, FortiSwitches, and FortiExtenders.

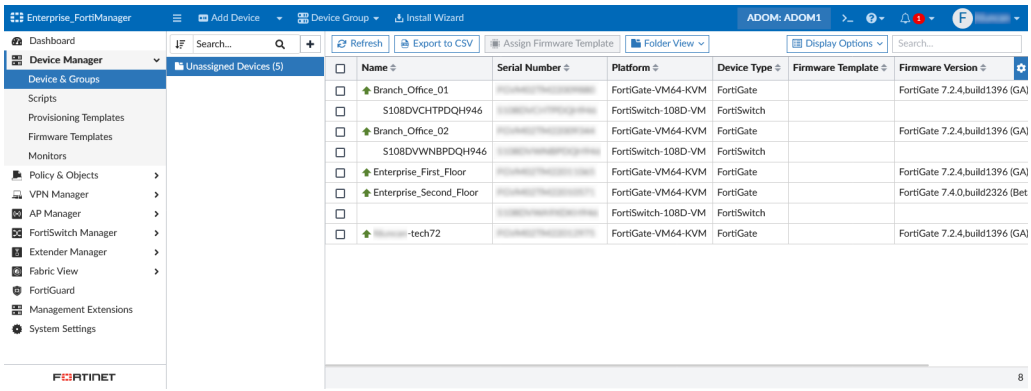
See also Firmware templates on page 378.

Folder View is not available when the ADOM device mode is set to *Advanced*. See ADOM device modes on page 928.

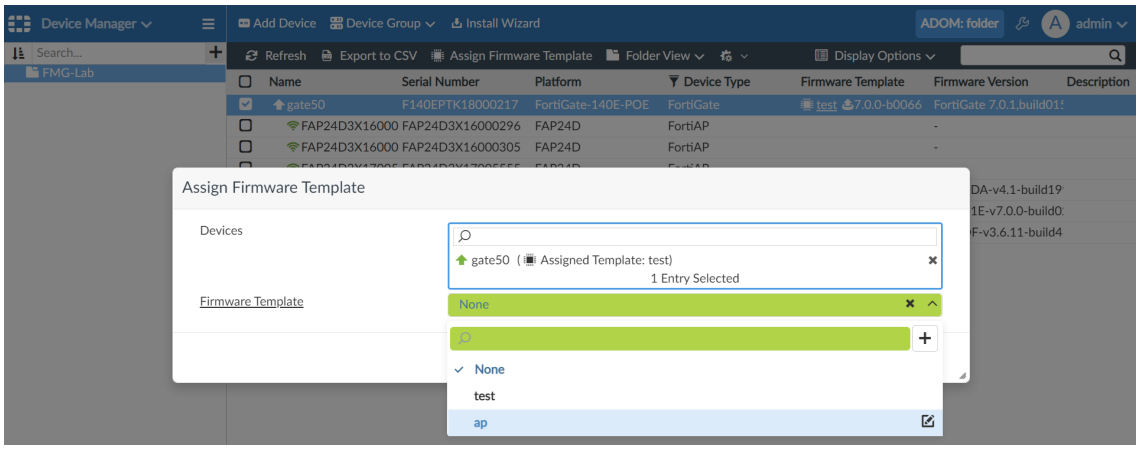
To access Folder View:

1. Go to *Device Manager > Device & Groups*.
2. In the toolbar, select *Folder View* from the dropdown menu

   By default, all the devices are placed under *Unassigned Devices* in the tree menu.



3. From the *Display Options* menu, choose from the following options:
   - *Fabric View*: Indents attached devices, such as FortiSwitch and FortiAP devices, under the FortiGate to which they are attached in a Security Fabric.
   - *Flat View*: Displays the list of devices in alphabetical order by name.
   - *Device Type View*: Displays the list of devices by device type, such as FortiGate, FortiAP, and FortiSwitch.
4. (Optional) Assign a firmware template.
   a. Right-click a FortiGate, and select *Assign Firmware Template*.
   The *Assign Firmware Template* dialog box is displayed.



b. In the *Devices* list, select one or more devices.

c. In the *Firmware Template* list, select a firmware template, and click *OK*.
A firmware template can include firmware for FortiGate as well as access devices, such as FortiAP, FortiSwitch, and FortiExtender.

The firmware template is assigned to the selected devices.

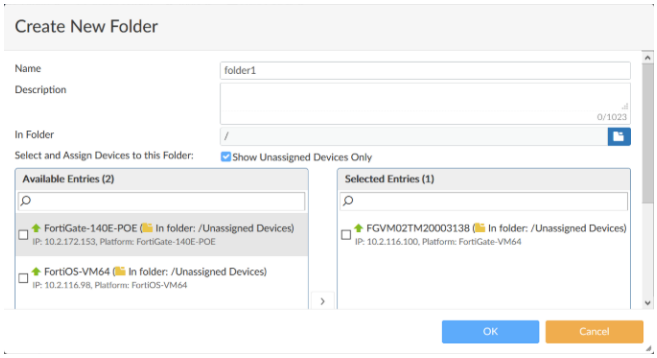
Creating folders

To create folders:

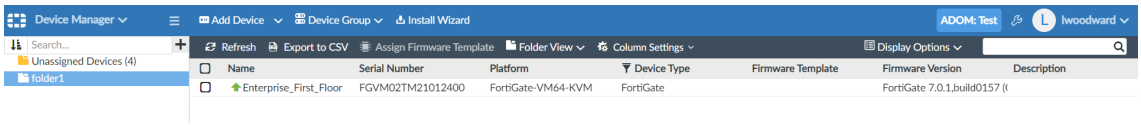
1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, select *Folder View* from the dropdown menu.
Folder view is displayed.
3. Beside the *Search* bar, click *+*.

   Alternately, right-click *Unassigned Devices*, and select *Create New Folder*.

   The *Create New Folder* dialog box opens.



4. In the *Name* box, type a name for the folder, for example, `folder1`, and click *OK*.
The new folder is created and visible in the tree menu. Also, the FortiGates in the folder are now displayed in the content pane.



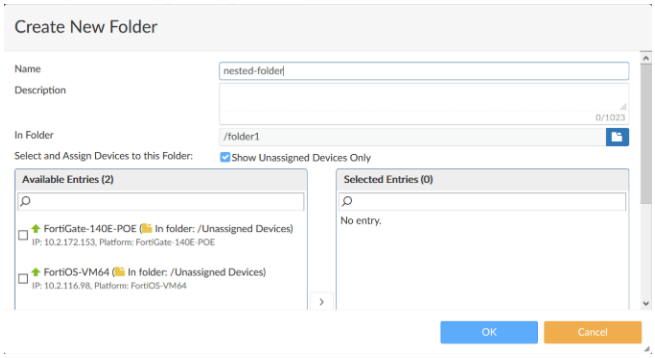
You can add FortiGates directly to a folder by selecting devices from the *Available Entries* list in the *Create New Folder* dialog.

Nesting folders

The new *Folder View* supports nested folders.

To create nested folders:

1. In the tree menu, right-click the folder you intend to nest, and select *Create New Folder*.
   For instance, right-click the previously created named *folder1*, and select *Create New Folder*.
   The *Create New Folder* dialog opens.
   In Folder shows that the new folder will be created within *folder1*.



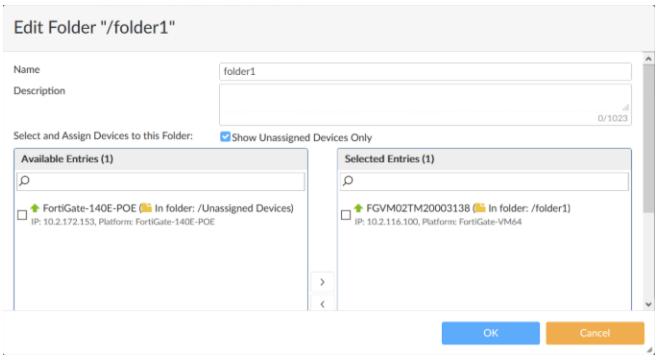
2. In the *Create New Folder* dialog, type a name for the folder, for example, `nested-folder`, and click *OK*.
   The *nested-folder* is created and displayed in the tree menu under the previously created *folder1*. Also, the folder and the FortiGates in the parent folder are displayed in the content pane.



Moving devices between folders

To move devices between folders:

1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, select *Folder View* from the dropdown menu.
3. In the tree menu, right-click the folder where the FortiGate is to be moved, and select *Edit*.
   The *Edit Folder* dialog opens.



4. In the *Edit Folder* dialog, select the FortiGate to be moved from the *Available Entries* list, and click *OK*.

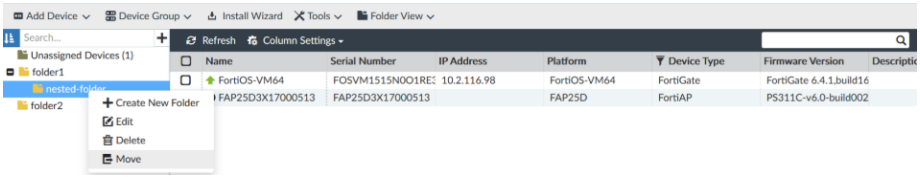
Alternatively, from the *Device & Groups* pane, select a FortiGate, drag and drop it on the folder to which you want to move it.

At any given time, a FortiGate can only be added to one folder.

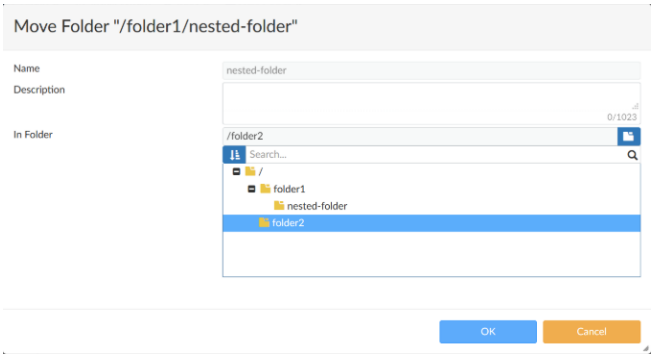
Moving folders

To move a folder:

1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, select *Folder View* from the dropdown menu.
3. In the tree menu, right-click the folder you want to move, here nested-folder, and select *Move*. The *Move Folder* dialog opens.

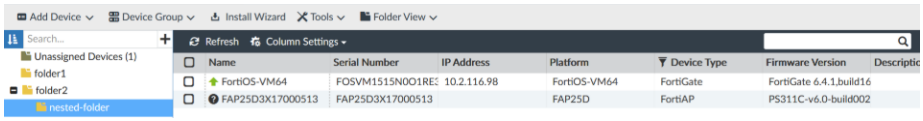


4. In the *Move Folder* dialog, under *In Folder*, select the destination folder, here folder2.



Click *OK*.

The nested-folder moves to folder2 including folders and devices in it.



Import Configuration wizard

You can use the *Import Configuration* wizard to import policies, objects, AP profiles, and FortiSwitch templates from managed devices to FortiManager.

This section contains the following topics:

- Importing policies and objects on page 173
- Importing AP profiles and FortiSwitch templates on page 179

Importing policies and objects

The import policy wizard helps you import policy packages and objects from managed FortiGates as well as specify per-device or per-platform mappings for FortiGate interfaces. Default or per-device mapping must exist or the installation will fail.

Resolving conflicts during import

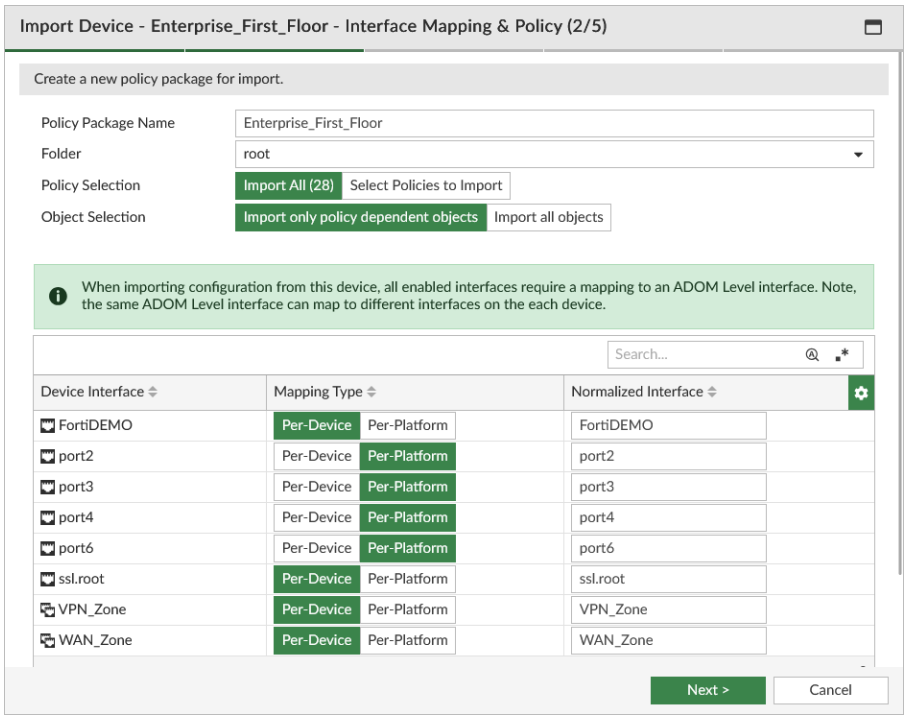
During the import process, any conflicts between the objects being imported from the FortiGate and the objects already stored on FortiManager will be identified, and the administrator can choose which object to retain during the import process.

After initially importing policies from the device, make all changes related to policies and objects in *Policy & Objects* on the FortiManager. Making changes directly on the FortiGate device will require reimporting policies to resynchronize the policies and objects.

See ADOM versions on page 941 to determine which ADOM versions can import configurations from which device firmware versions.

To import policy packages and objects:

1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. In the tree menu, click the device group name. The devices in the group are displayed in the content pane.
4. Right-click a device, and select *Import Configuration*.
   The *Import Device* dialog box is displayed.
5. Select *Import Policy Package*, and click *Next*.
   The next screen is displayed.



6. Specify what policies and objects to import:

Policy Package Name	(Optional) Type a name for the policy package.
Folder	(Optional) Select a folder on the dropdown menu. The default storage folder is *root*.
Policy Selection	Select *Import All* to import all policies. Select *Select Policies to Import* to select which policies and policy groups to import.
Object Selection	Select *Import only policy dependent objects* to import only policy dependent objects for the device. Select *Import all objects* to import all objects for the selected device.

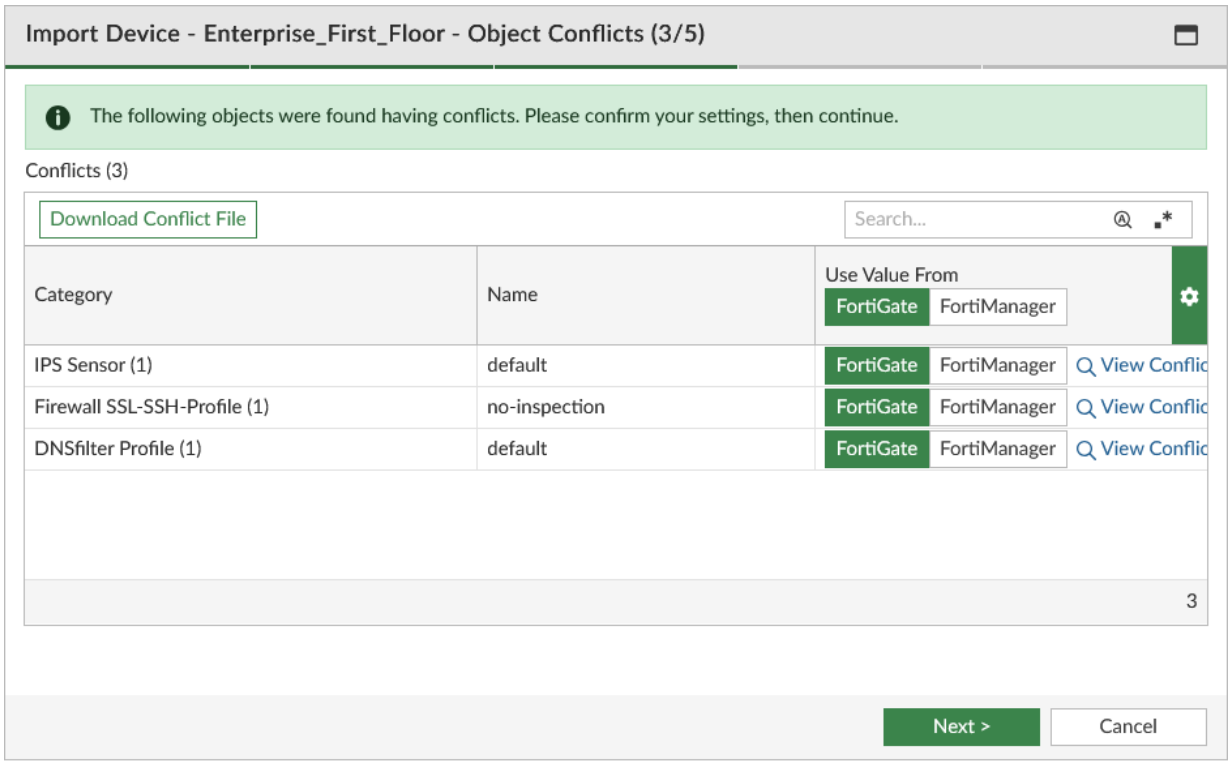
7. Specify mapping types for enabled FortiGate interfaces:
   When importing policies and objects from a device, all enabled interfaces require a mapping.

Device Interface	Displays the enabled interfaces for the device for which you are importing policies.
Mapping Type	For each enabled device interface, select one of the of the following options: *Per-Device* or *Per-Platform*.
Normalized Interface	Displays the name of the normalized interface to which the device interface is mapped.
Add mapping for all unused device interfaces	Select to automatically create interface maps for unused device interfaces.

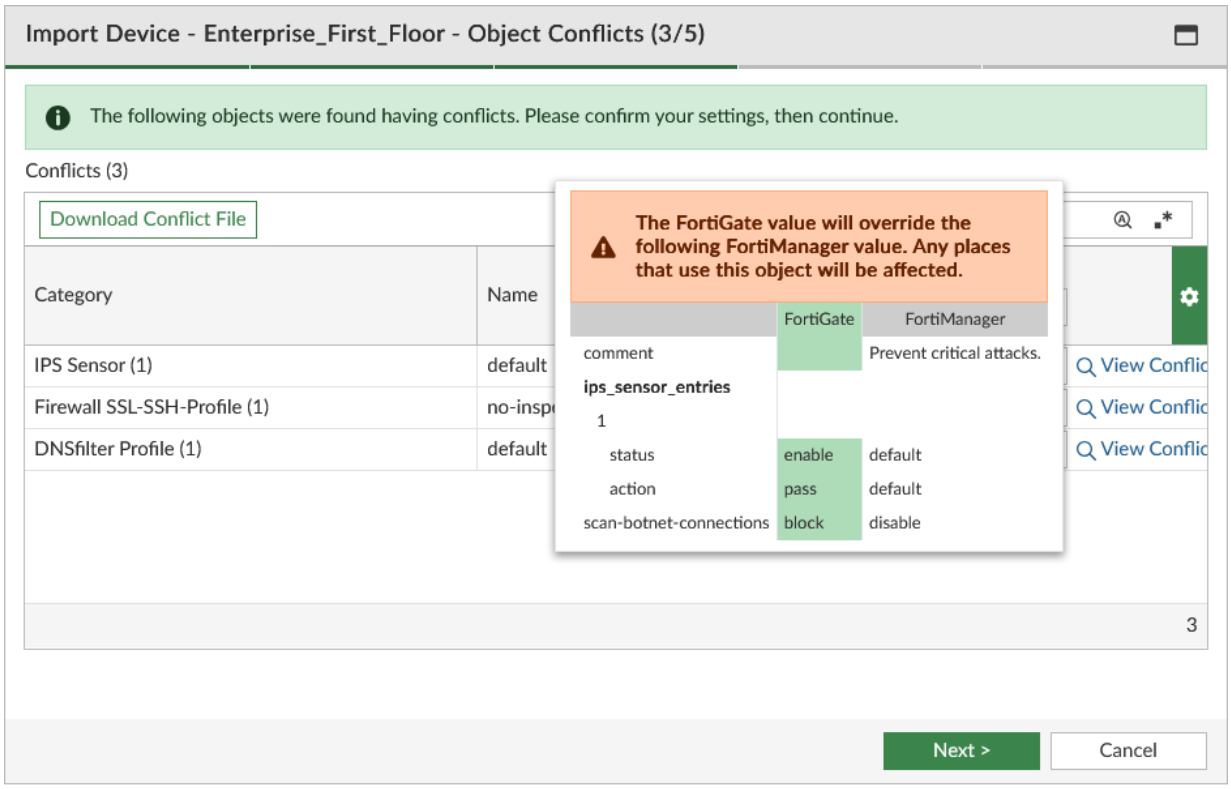
8. When finished mapping device interfaces, click *Next*.
   The next page displays any object conflicts between the device and FortiManager.

9. If object conflicts are detected, you can choose whether to use the value from FortiGate or FortiManager.
   - The object page searches for dependencies, and reports any conflicts it detects. If conflicts are detected, you must decide whether to use the FortiGate value or the FortiManager value:

Use the value from..	Result
FortiGate	The value from the FortiGate will be imported and will overwrite the existing object on FortiManager. Any places on FortiManager that use the object will be affected.
FortiManager	The value from the FortiManager will be retained and the FortiGate value will be discarded.

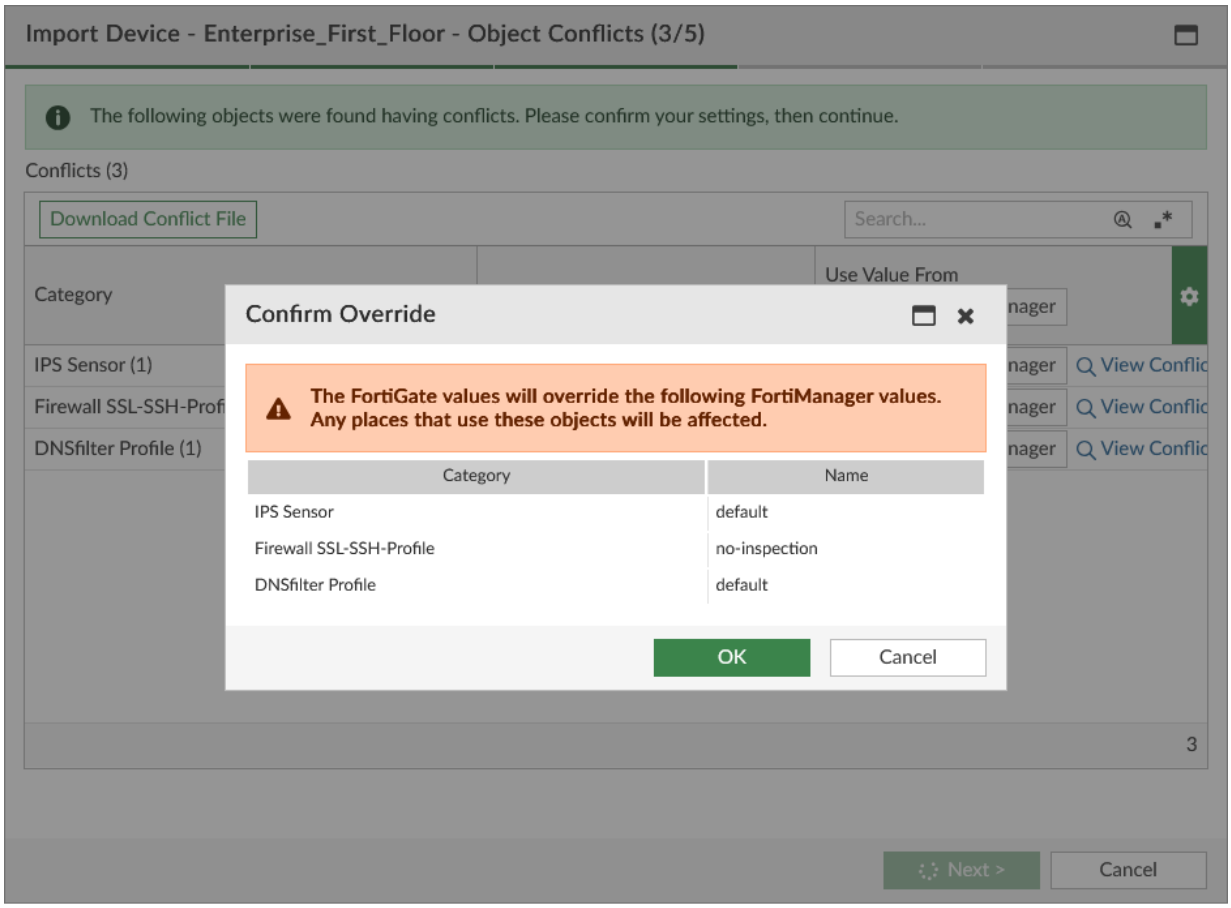


   - You can select *View Conflict* to view the details of each conflict. The values that will be kept are highlighted.

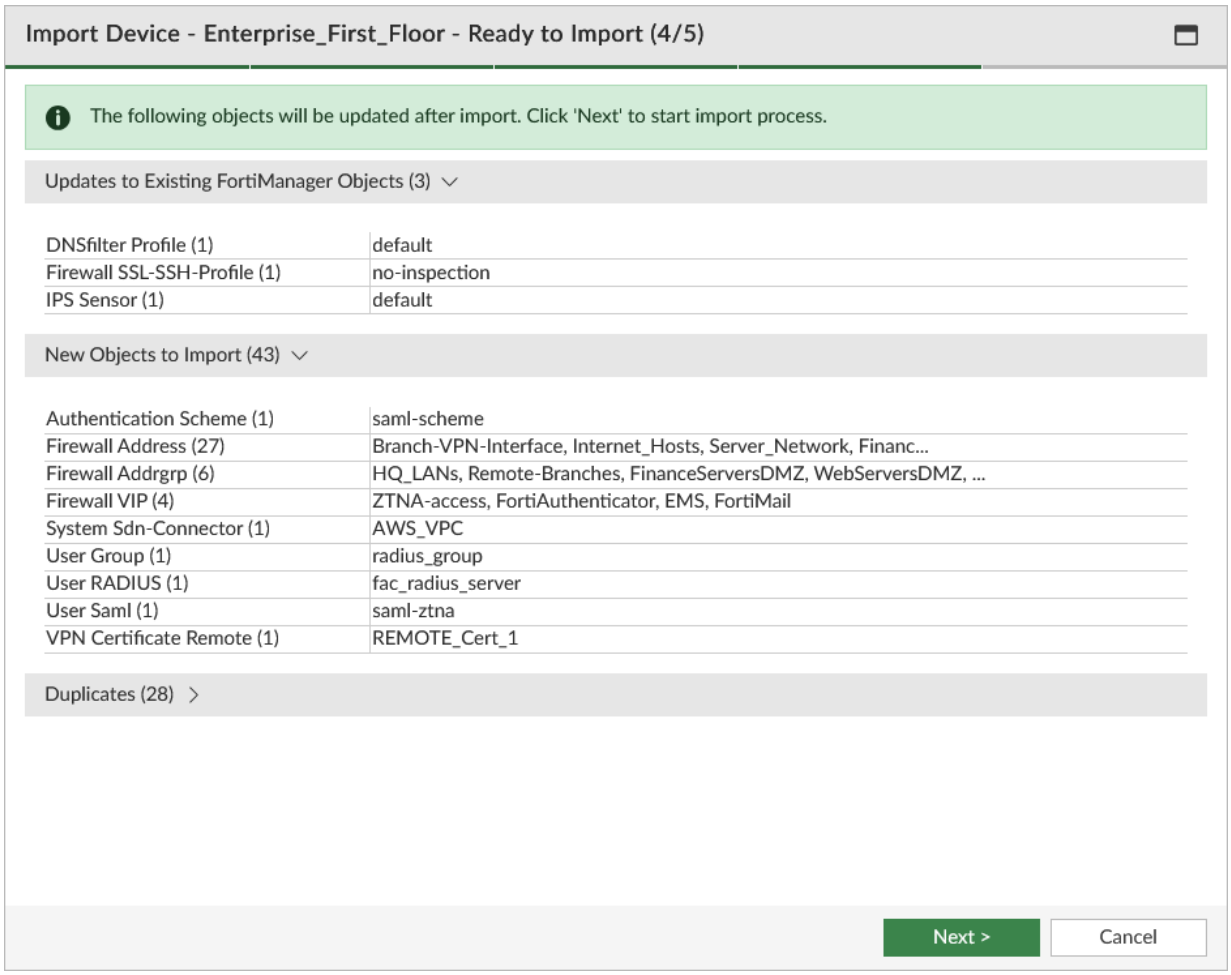


- Duplicate objects are not imported to FortiManager.
- You can click *Download Conflict File* to save a file of the conflicts to your hard drive.

10. When finished managing object conflicts, click *Next*.
    - If FortiGate values were chosen to resolve a conflict, a *Confirm Override* warning appears to remind the administrator that the FortiGate values will override the FortiManager values, and any places that use the objects will be affected. Click *OK* to continue.



- A summary is provided that lists *Dynamic Mappings*, *Updates to Existing FortiManager Objects*, *New Objects to Import*, and *Duplicate objects*.



11. Click *Next* to start the import process.
    - When the import process completes, a summary page is displayed.
    - You can click *Download Import Report*, and save the report file to your hard drive.
    - Objects are imported into the common database, and the policies are imported into the selected package.

    The import process removes all policies that have FortiManager generated policy IDs, such as 1073741825, that were previously learned by the FortiManager device. The FortiGate unit may inherit a policy ID from the global header policy, global footer policy, policy block, or VPN console.

12. Click *Finish* to close the wizard.

Importing the FortiClient EMS configuration from FortiGate is not supported. See Creating FortiClient EMS connectors on page 705.

Importing AP profiles and FortiSwitch templates

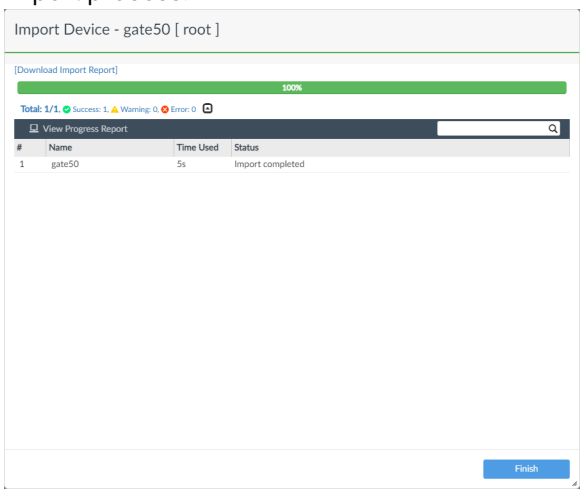
You can import AP profiles and FortiSwitch templates using the Import configuration wizard. In order to import AP profile and FortiSwitch templates, central management must be enabled for the chosen ADOM.

To import AP profiles and FortiSwitch templates:

1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. In the tree menu, click the device group name. The devices in the group are displayed in the content pane.
4. Right-click a device, and select *Import Configuration*.
   The *Import Device* dialog box is displayed.
5. Select *Import AP Profiles or FortiSwitch Templates*, and click *Next*.
   The next screen is displayed.
6. Select the access point and FortiSwitch profiles you want to import.
   In the AP profile list and FortiSwitch template list, you can keep or change the default names.



7. Click *Next* to begin the import process.
   On the next page, the import progress bar is displayed along with any errors or warnings resulting from the import process.



8. After the import has successfully completed, imported AP profiles and FortiSwitch templates are visible in *AP Manager > WiFi Profiles > AP Profile* and *FortiSwitch Manager > FortiSwitch Templates* respectively.

Install wizard

- To use the *Install Wizard* to install policy packages and device settings to one or more FortiGate devices, see Installing policy packages and device settings on page 180.
- To use the *Install Wizard* to install device settings only, see Install device settings only on page 183.
- To reinstall a policy package without using the *Install Wizard*, see Reinstall a policy package on page 419.



If auto-push is enabled, policy packages and device settings will be installed to offline devices when they come back online. See Creating ADOMs on page 934 for information on enabling this feature.



FortiManager 7.4.1 and later supports partial installs the JSON API.

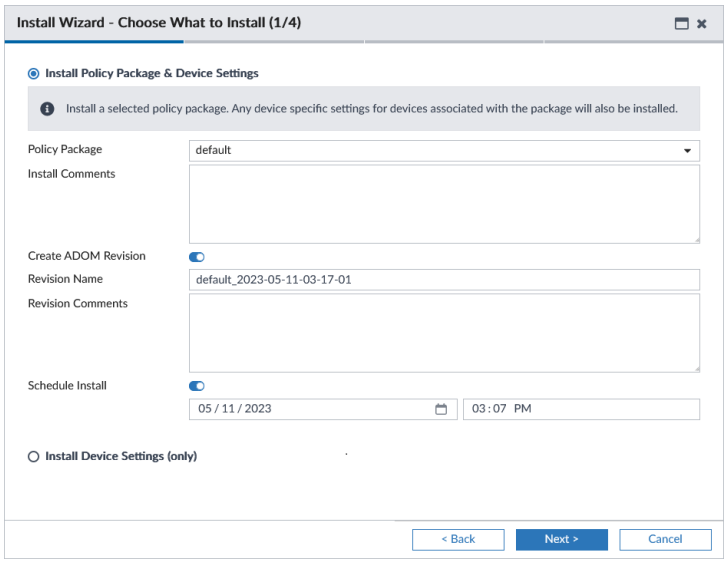
Installing policy packages and device settings

You can use the *Install Wizard* to install policy packages and device settings to one or more FortiGate devices, including any device-specific settings for the devices associated with that package.

To use the Install Wizard to install policy packages and device settings:

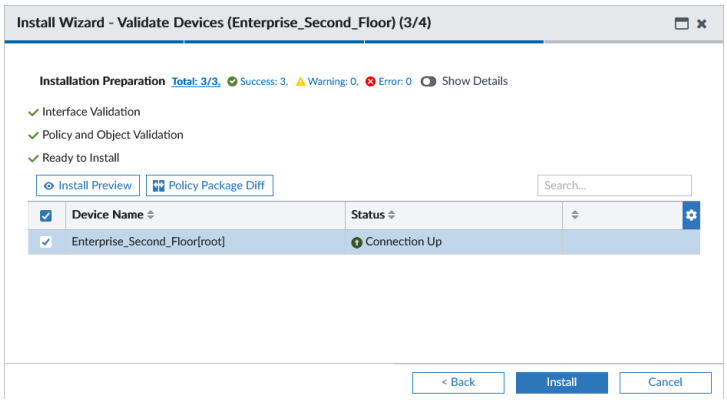
1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > Device & Groups*.
3. In the toolbar, select *Install Wizard* or *Install > Install Wizard*.

4. Select *Install Policy Package & Device Settings* and specify the policy package and other parameters. Click *Next*.



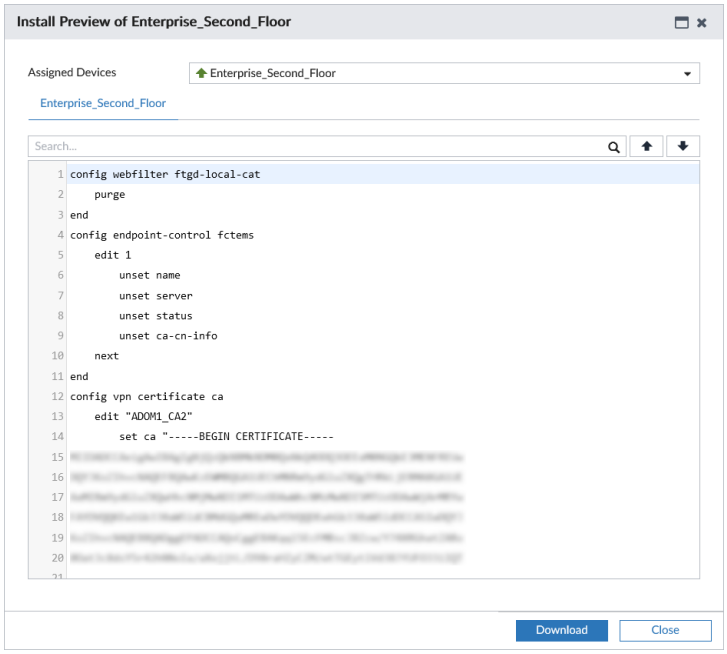
Policy Package	Select the policy package from the dropdown list.
Comment	Type an optional comment.
Create ADOM Revision	Select the checkbox to create an ADOM revision.
Revision Name	Type the revision name.
Revision Comments	Type an optional comment.
Schedule Install	Select the checkbox to schedule the installation.
Date	Click the date field and select the date for the installation in the calendar pop-up.
Time	Select the hour and minute from the dropdown lists.

5. On the next page, select one or more devices or groups to install, and click *Next*.
The select devices are validated. Validation includes validating the policy and object, the interface, and installation preparation. Devices with validation errors are skipped for installation. The validation results are displayed.
If enabled, a policy consistency check will be performed and the results will be available (see Perform a policy consistency check on page 424).



If there are errors in validation, click the link in the error message to see the progress report with the error lines highlighted.

6. (Optional) Click the *Install Preview* button to view a preview of the installation. You can view multiple devices at the same time.
   - Click *Download* to download a text file of the installation preview details.
   - Select a device from the *Assigned Devices* dropdown menu to preview the installation on the chosen device.



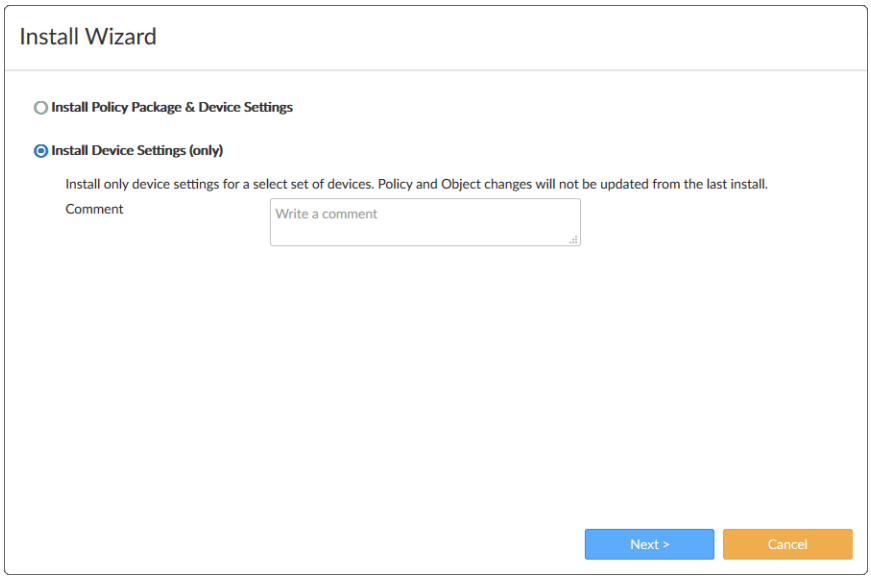
7. (Optional) Click the *Policy Package Diff* button to view the differences between the current policy and the policy in the device. See also Viewing a policy package diff on page 184.
8. When validation is complete, click *Install* or *Schedule Install* (if you selected *Schedule Install*). FortiManager displays the status of the installation and then lists the devices onto which the settings were installed and any errors or warning that occurred during the installation process.
9. Click *Finish* to close the wizard.

Install device settings only

You can use the *Install Wizard* to install device settings only to one or more FortiGate devices. The *Install Wizard* includes a preview feature.

To use the Install Wizard to install device settings only:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. In the toolbar, select *Install Wizard* or *Install* > *Install Wizard*.
3. Select *Install Device Settings (only)* and if you want, type a comment. Click *Next*.



4. In the *Device Settings* page, select one or more devices to install, and click *Next*.
5. (Optional) Preview the changes:
   a. Click *Install Preview*.
      The *Install Preview* window is displayed. You have the option to download a text file of the settings.
   b. Click *Close* to return to the installation wizard.
6. Click *Install*.
   FortiManager displays the status of the installation and then lists the devices onto which the settings were installed and any errors or warning that occurred during the installation process.
   You can click the *View History* and *View Log* buttons for more information.
7. Click *Finish* to close the wizard.

Out-of-Sync device

FortiManager is able to detect when the settings were changed on the FortiGate and synchronize back to the related policy and object settings. This allows you to know when the policy package is out-of-sync with what is installed on the FortiGate.

When a change is made to the FortiGate, FortiManager displays an out-of-sync dialog box.

Select the *View Diff* icon to view the changes between the FortiGate and FortiManager.

You can select to accept, revert the modification, or decide later.

When accepting remote changes, all local configurations will be replaced by remote configurations. When reverting, the FortiGate will be reset to the latest revision.

You can view details of the retrieve device configuration action in the Task Monitor. See Task Monitor on page 963.

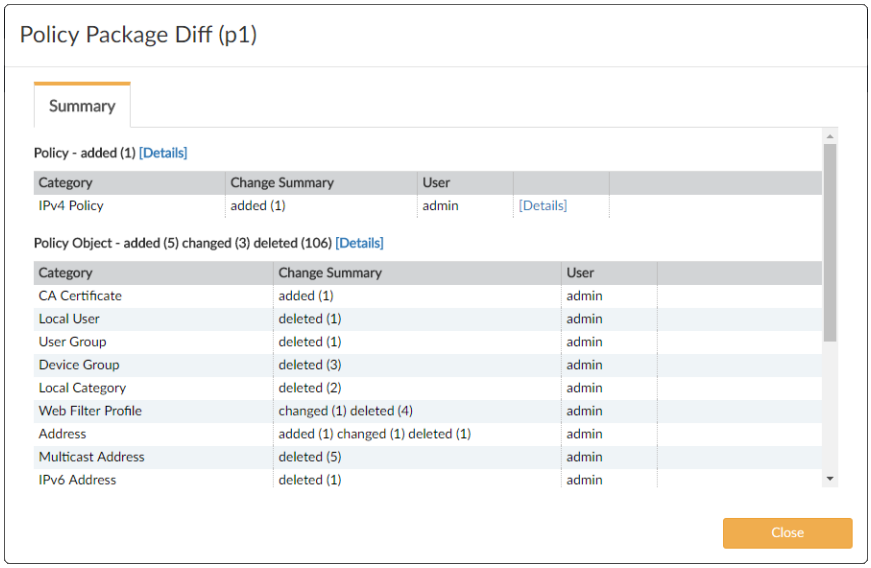
Viewing a policy package diff

You can view the difference between the policy package associated with (or last installed on) the device and the policies and policy objects in the device.

The connection to the managed device must be up to view the policy package diff.

To view a policy package diff in *Device Manager*:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager> Device & Groups*.
3. In the toolbar, select *Table View* from the dropdown menu.
4. In the tree menu, click the device group name. The devices in the group are displayed in the content pane.
5. Right-click a device and select *Policy Package Diff*.
   The *Policy Package Diff* window is displayed after data is gathered.



6. Beside *Policy*, click the *Details* link to display details about the policy changes.
7. In the *Category* row, click the *Details* link to display details about the specific policy changes.
8. Beside *Policy Object*, click the *Details* link to display details about the policy object changes.
9. Click *Cancel* to close the window.

Firewall policy reordering on first installation

On the first discovery of a FortiGate unit, the FortiManager system will retrieve the unit's configuration and load it into the Device Manager. After you make configuration changes and install them, you may see that the FortiManager system reorders some of the firewall policies in the FortiGate unit's configuration file.

This behavior is normal for the following reasons:

- The FortiManager system maintains the order of policies in the actual order you see them and manipulate them in the GUI, whereas the FortiGate unit maintains the policies in a different order (such as order of creation).
- When loading the policy set, the FortiManager system re-organizes the policies according to the logical order as they are shown in the user interface. In other words, FortiManager will group all policies that are organized within interface pairs (internal -> external, port1 -> port3, etc.).

The FortiManager system does not move policies within interface pairs. It will only move the configuration elements so that policies with the same source/destination interface pairs are grouped together.

This behavior would only be seen:

- On the first installation.
- When the unit is first discovered by the FortiManager system. If using the FortiManager system to manage the FortiGate unit from the start, you will not observe the policy reordering behavior.

Installing the device database

Configuring a FortiGate unit using the device database in FortiManager is very similar to configuring FortiGate units using the FortiOS GUI. You can also save the configuration changes to the configuration repository and install them to other FortiGate units at the same time.

This document does not provide detailed procedures for configuring FortiGate units. See the FortiGate documentation for complete information. The most up-to-date FortiGate documentation is also available in the Fortinet Document Library.

To install the device database:

1. Go to *Device Manager > Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. In the tree menu, select a device group.
4. In the content pane, select a device.
5. From the *Install* menu, select *Quick Install (Device DB)*.
6. When the installation configuration is complete, click *Finish*.
   The configuration changes are saved to the FortiManager device database instead of the FortiManager repository represented by the *Revision History* window.



To view the history of the configuration installation, click the *View History* button in the *History* column to open the *Install History* dialog box. This can be particularly useful if the installation fails.

You can rename and reapply firewall objects after they are created and applied to a firewall policy. When you do so, the FortiManager system will: delete all dependencies, delete the object, recreate a new object with the same value, and recreate the policy to reapply the new object.

Firmware upgrade

On the *Device Manager > Device & Groups* pane, you can view the firmware installed on managed devices, and you can upgrade firmware for managed devices.

This section contains the following topics:

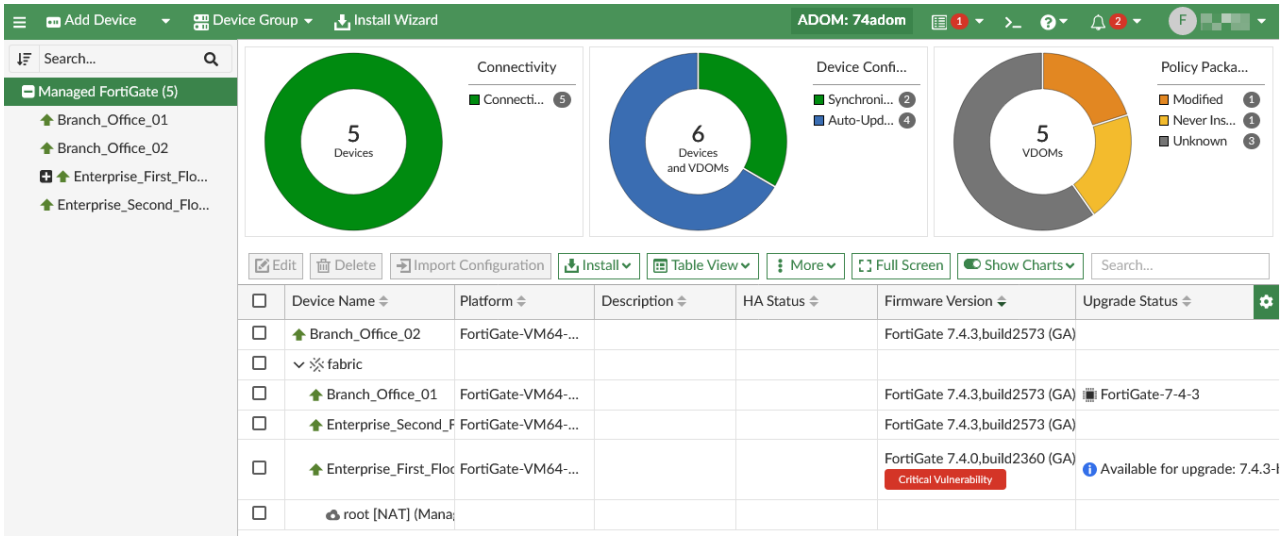
- Viewing installed firmware versions on page 186
- Upgrading firmware on page 187
- Upgrading multiple firmware versions on FortiGate on page 190
- Upgrading firmware using images from FortiGuard on page 192

Viewing installed firmware versions

You can view the installed firmware version for all managed devices in a group.

To view installed firmware versions:

1. Go to *Device Manager > Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. In the tree menu, select the device group name, for example, *Managed FortiGate*.
   Devices in the group are displayed in the content pane.
4. View information in the *Firmware Version* column.



Upgrading firmware

From the *Device Manager* pane, you can update firmware for managed devices.

Upgrades can be scheduled to occur at a later date using firmware templates. See Firmware templates on page 378.

When workspace is enabled, you must lock a device (or ADOM) to allow firmware upgrade.

The FortiGate device requires a valid firmware upgrade license. Otherwise a *Firmware Upgrade License Not Found* error is displayed.



When *Boot to Alternate Partition After Upgrade* is selected, the inactive partition will be upgraded.

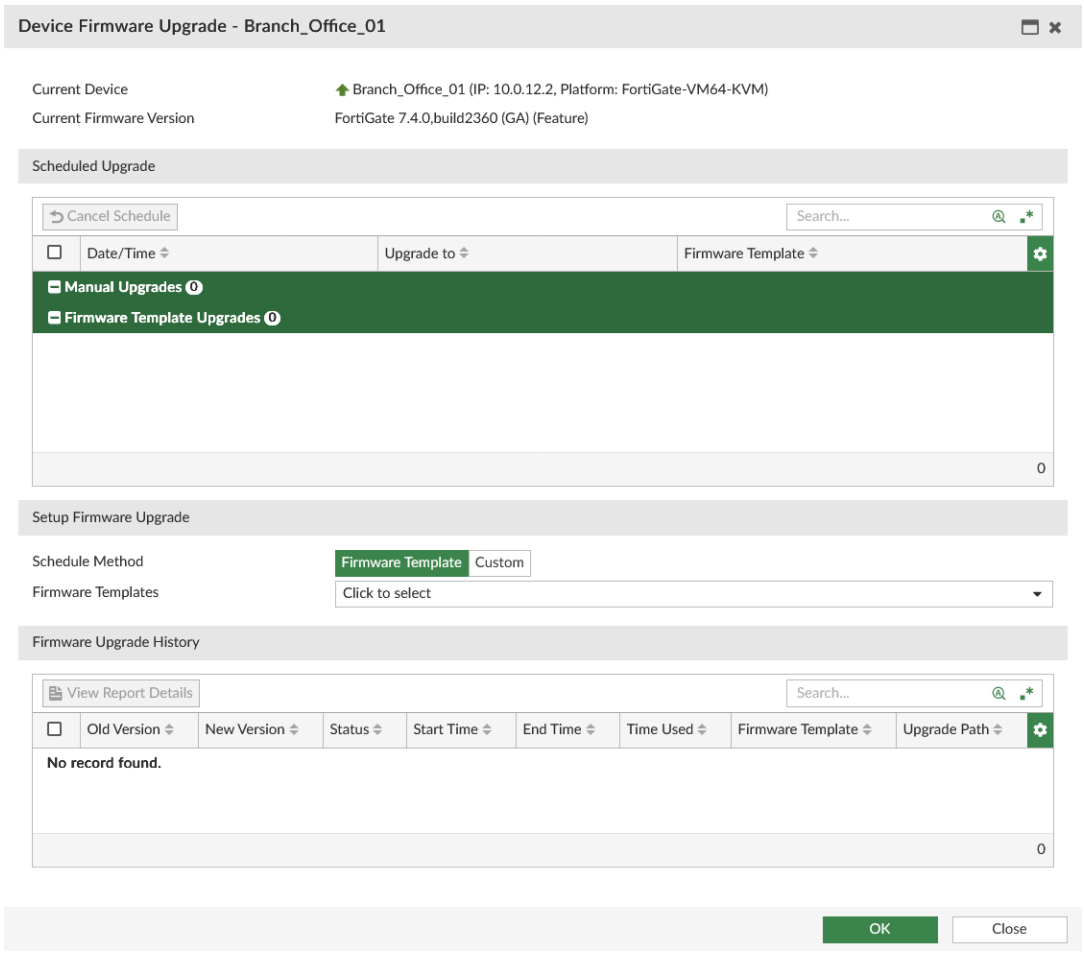


FortiGate devices must have a valid Firmware & General Updates (FMWR) contract in order for firmware updates to be performed through FortiManager. This applies to firmware images from FortiGuard and images that are manually uploaded to FortiManager.

When a FortiGate device is added to the FortiManager, a 24 hour grace period is provided in which firmware updates can be applied without a license to allow time for the FMWR contract information to synchronize from FortiCare. FortiManager expects the managed device to be on the same FortiCloud account, or have the device serial number added in FortiGuard's auth list.

To upgrade firmware for managed devices:

1. Go to *Device Manager > Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. In the tree menu, select the device group name, for example, *Managed FortiGate*.
   Devices in the group are displayed in the content pane.
4. Select one or more devices, and select *Firmware Upgrade* from the *More* menu.
   The *Device Firmware Upgrade* dialog box opens.



5. Configure the following settings, then click *OK*:

Schedule Upgrade		View scheduled upgrades. This option is only displayed when selecting one device. You can selected an entry in the table and click *Cancel Schedule* to cancel the scheduled upgrade.
Setup Firmware Upgrade		Configure the firmware upgrade method using a firmware template or a custom firmware upgrade configuration.
	Firmware Templates	Click the *Firmware Templates* dropdown to select an existing firmware template, or click the *Create New* icon to create a new firmware template for use. See Creating firmware templates on page 379 The upgrade will start based on the schedule configured in the template or when the upgrade is manually started. See Upgrading devices now on page 384.
	Custom	Select a firmware version to upgrade to in the *Upgrade To* field. Once a firmware version is selected, the following additional options are displayed: **Boot from** — Applies only to FortiGates.

	Alternate Partition After Upgrade	Select to upgrade the inactive partition. Clear to skip the inactive partition during upgrade. Selecting this option causes the device to reboot twice during the upgrade process: first to upgrade the inactive partition, and second to boot back into the active partition.
	Let Device Download Firmware from FortiGuard	Select to have the device download the firmware from FortiGuard for the upgrade. Clear to have the device download the firmware from FortiManager.
	Upgrade Path	Select one of the following options: • *Skip All Intermediate Steps in Upgrade Path If Possible*: Select to skip some builds in an upgrade path. • *Follow The Recommended Upgrade Path*: Select to install all builds in an upgrade path.  The *Follow The Recommended Upgrade Path* feature is not supported when FortiManager is operating in a closed network. Each image in the path must instead be imported to FortiManager and manually pushed to the managed devices in the correct order. You can view the recommended upgrade path at support.fortinet.com.
	Only upgrade FortiGate Clusters with all members up	When enabled, if any HA secondary node is down, the firmware upgrade will be skipped for the HA cluster.
	Schedule Upgrade	Configure a schedule for the firmware upgrade in hours or by specifying a date/time.
Firmware Upgrade History	View the firmware upgrade history for the selected device. This option is only displayed when selecting one device	

FortiManager checks the FortiGate disk before upgrading. If the check fails, a message indicates the failure, and the upgrade is not performed.

If the check passes, the upgrade proceeds.

FortiOS devices cannot be upgraded to a version that is higher than the FortiManager that is managing them. This rule is applicable only for major and minor versions. For example, FortiManager 6.2.0 cannot upgrade FortiOS devices to 6.3.0 or 7.0.0. When trying to upgrade FortiOS devices to a version higher than FortiManager, the upgrade process cannot be completed and a warning is shown.

When upgrading FortiGate devices to a firmware version that is not part of the upgrade path (shown by the green check mark), the warning *The firmware version is not on firmware upgrade path of selected devices. Upgrading the image may cause the current syntax to break.* is shown. Click *Upgrade to Recommended X.X.X* which shows the recommended version, or *Continue* to upgrade to the selected version. A warning is also shown when upgrading FortiGate devices to a custom firmware.

The disk on the FortiGate is checked automatically before upgrade. To enable skip disk check run the `set skip-disk-check` from the command line.

To disable disk check:

1. Disable disk check by using the CLI:
```
config fmupdate fwm-setting
(fwm-setting)# set check-fgt-disk disable
```

The default setting is `enable`, 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
```

Upgrading multiple firmware versions on FortiGate

When using FortiManager to upgrade firmware on FortiGate, FortiManager can choose the shortest upgrade path based on the FortiGate upgrade matrix. In a multi-step firmware upgrade, each upgrade is a subtask. You can also enable the option to skip all intermediate steps in an upgrade path when available. See Upgrading firmware on page 187.

You can use the FortiManager GUI to review the shortest upgrade path. You can also use the CLI to view and check the shortest upgrade path for a managed device by using the `diagnose fwmanager` command.

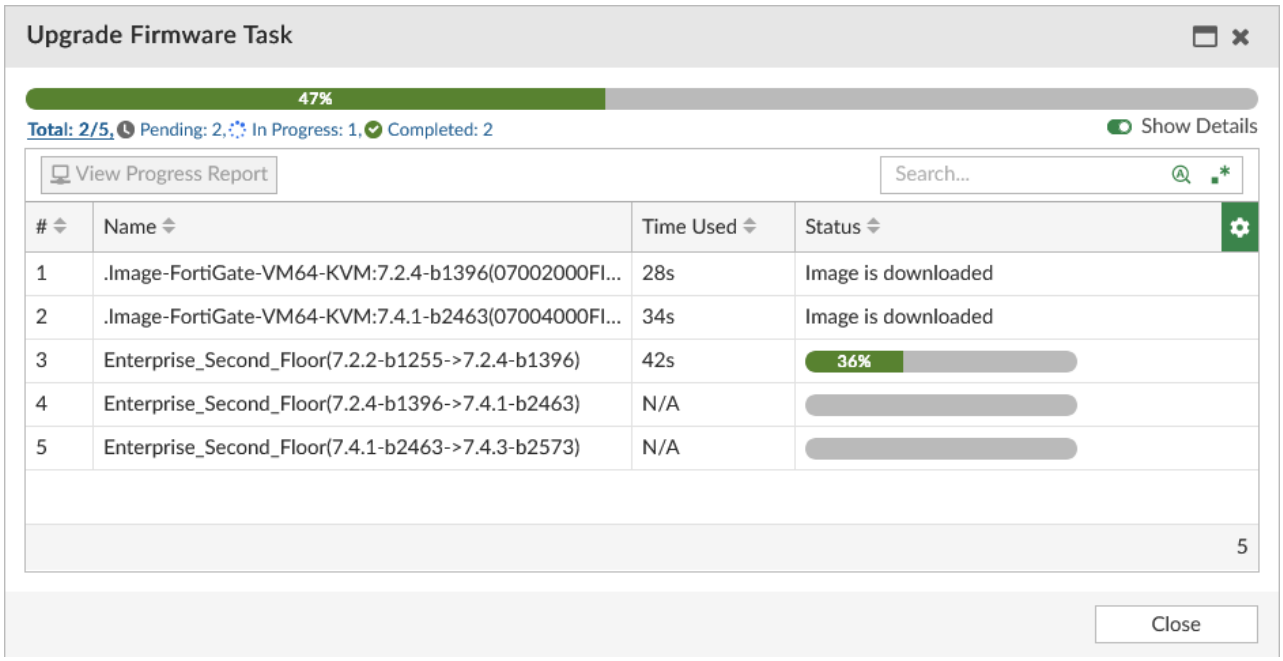
In this example, the device (ID 210) is on version 7.2.4 and the administrator wants to upgrade it to version 7.4.3. Using the `diagnose fwmanager` command, they are able to see the upgrade path in the CLI:

```
diagnose fwmanager show-dev-upgrade-path 210 7.4.3
   Enterprise_Second_Floor(210): ->7.2.4-b1396-F ->7.4.1-b2463-F ->7.4.3-b2573-F
```

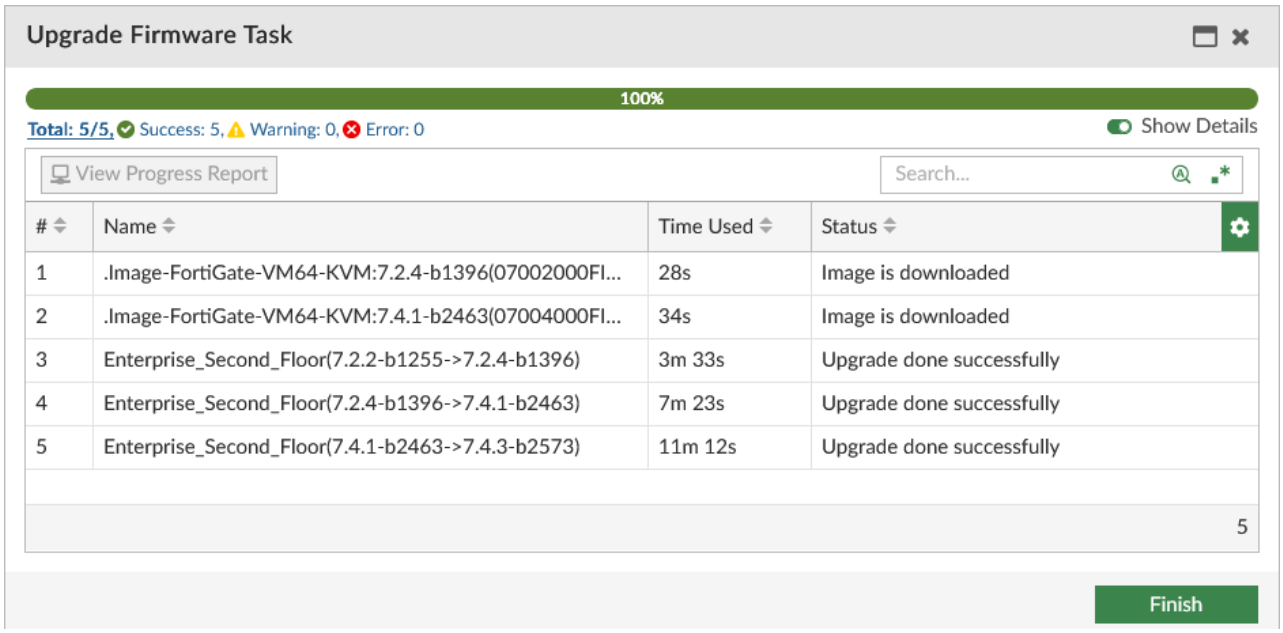
It is recommended to also check that the upgrade path for FortiGate reported by FortiManager matches the upgrade path reported on the FortiCloud FortiCare portal for FortiGate devices.

To upgrade multiple firmware versions using the GUI:

1. Configure the firmware upgrade for the device in the Device Manager. See Upgrading firmware on page 187 and Firmware templates on page 378.
2. When the upgrade begins, each firmware upgrade in the path is listed as a subtask.



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



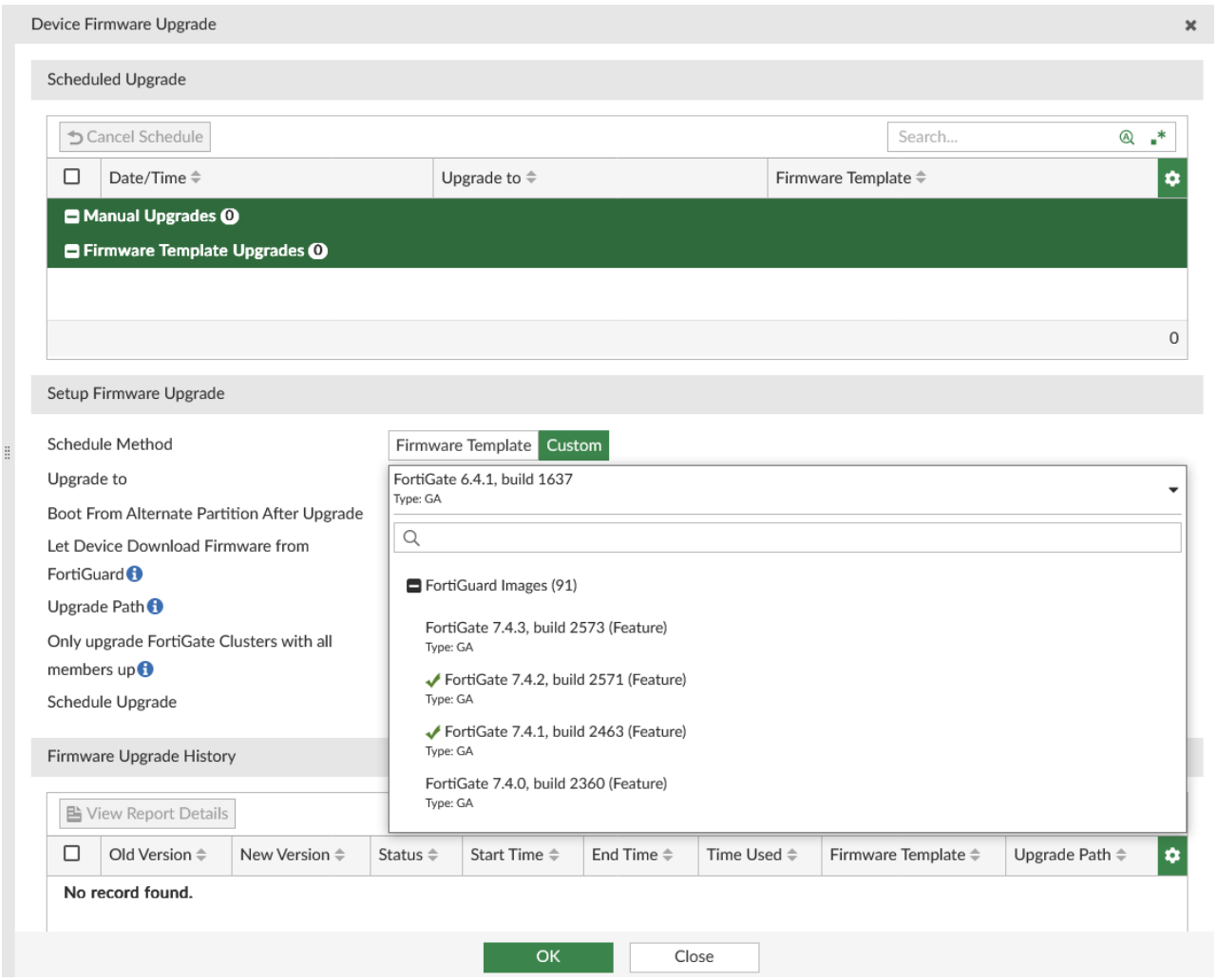
3. When the upgrade completes, click *Close*.

Upgrading firmware using images from FortiGuard

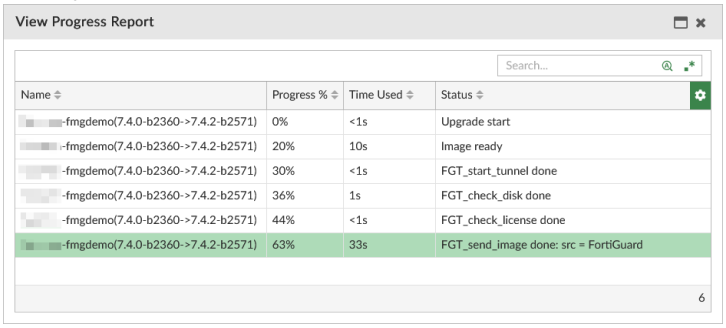
FortiManager retrieves firmware for managed devices from FortiGuard, and you can choose to use the images to upgrade firmware on managed devices.

To upgrade firmware using images retrieved from FortiGuard:

1. Configure the firmware upgrade for the device in the Device Manager. See Upgrading firmware on page 187 and Firmware templates on page 378.
2. When selecting a version to upgrade to, the *Device Firmware Upgrade* dialog box displays a list of available firmware releases from FortiGuard.



3. Under *Upgrade Options*, enable *Let Device Download Firmware from FortiGuard*.
4. Click *OK*. When the upgrade process begins, the upgrading device will download the firmware image directly from FortiGuard.



5. Click *Close*.

Device database (DB)

FortiManager maintains a device database for each managed device, and you can access the device database for each device.

The device database is used to view and monitor information about individual devices. You can also use the device database to configure individual devices.

This section contains the following topics:

- Displaying the device database on page 194
- Choosing feature visibility for devices on page 195
- Using the CLI console for managed devices on page 197
- Viewing and managing LTE modems on page 198

Displaying the device database

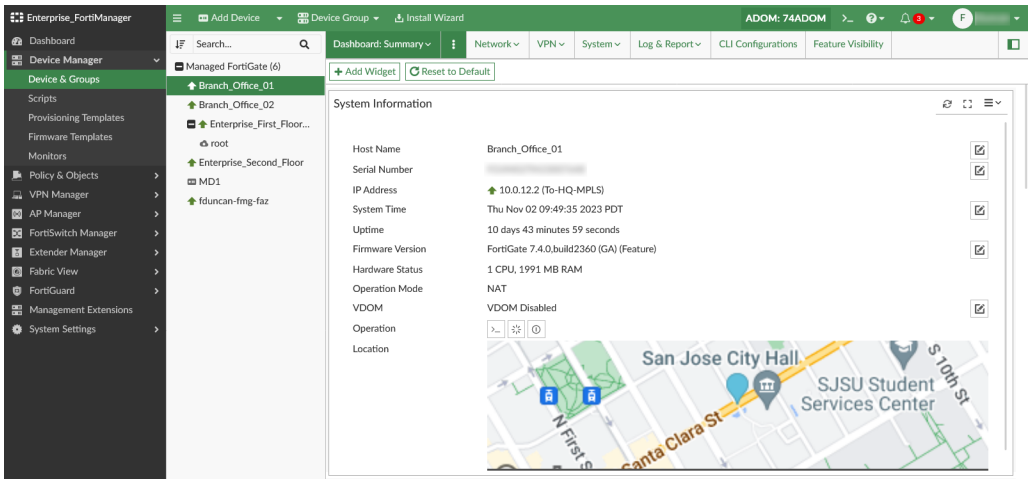


When the FortiAnalyzer feature set is enabled, the *All FortiGates* device group is replaced with *Managed Devices* and *Logging Devices*. Managed devices include FortiGate devices, which are managed by FortiManager, but do not send logs. Logging device include FortiGate devices, which are not managed, but do send logs to FortiManager.

To display the device database:

1. Go to *Device Manager* > *Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. In the tree menu, select the device group.
   The list of devices in the group are displayed.
4. Take one of the following actions:
   - In the left tree menu, click a device.
   - In the content pane, double-click a device.
   - In the content pane, select a device, and select *Configuration* from the *More* menu.

   The device database is displayed. By default the *Dashboard* > *Summary* pane is displayed.



Use the menu to access the following menus:

Dashboard	By default, the device database includes the following dashboards: • *Summary* • *Security Monitors* • *Network Monitors* You can also create and copy custom dashboards.
Network	View network panes including Interfaces, *DNS*, *IPAM*, *SD-WAN*, and *Static Routes*.
VPN	View VPN panes including *IPsec Phase 1* and *IPsec Phase 2*.
System	View system panes including *Administrators*, *Admin Profiles*, *Settings*, *SNMP*, and *Replacement Messages*.
Log & Report	View log and report panes including *Log Settings*.
CLI Configurations	View CLI configurations.
Feature Visibility	By default, some of the menu items are hidden. Click *Feature Visibility* to choose what menu items to hide and display. See Choosing feature visibility for devices on page 195.

For information on configuring FortiGate settings, see the *FortiOS Administration Guide*.

Choosing feature visibility for devices

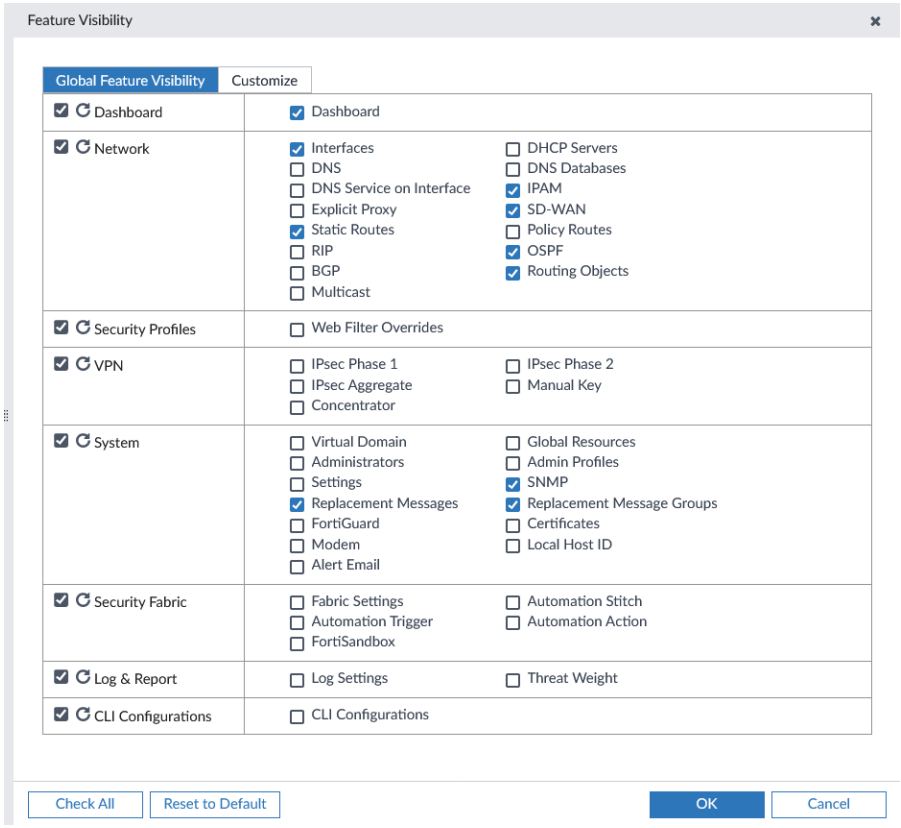
You can choose what settings to hide and display in the device database, allowing you to hide settings that you don't use and display settings that you do use.

By setting the global feature visibility options, you are specifying what options to hide and display for all device databases, and you can customize individual device databases as needed.

When ADOMs are enabled, the global feature visibility applies to all devices in the ADOM, letting you specify different global feature visibility for each ADOM.

To specify global feature visibility for all devices in an ADOM:

1. Go to the device database. See Displaying the device database on page 194.
   The *Dashboard* for the device database is displayed.
2. In the left pane, click *Feature Visibility*.
   The *Feature Visibility* dialog box is displayed.



3. Select *Global Feature Visibility*, and then select the checkboxes for the items you want to display, and clear the checkboxes for the items you want to hide.
   The selections apply to all devices. When ADOMs are enabled, the selections apply to all devices in the ADOM.



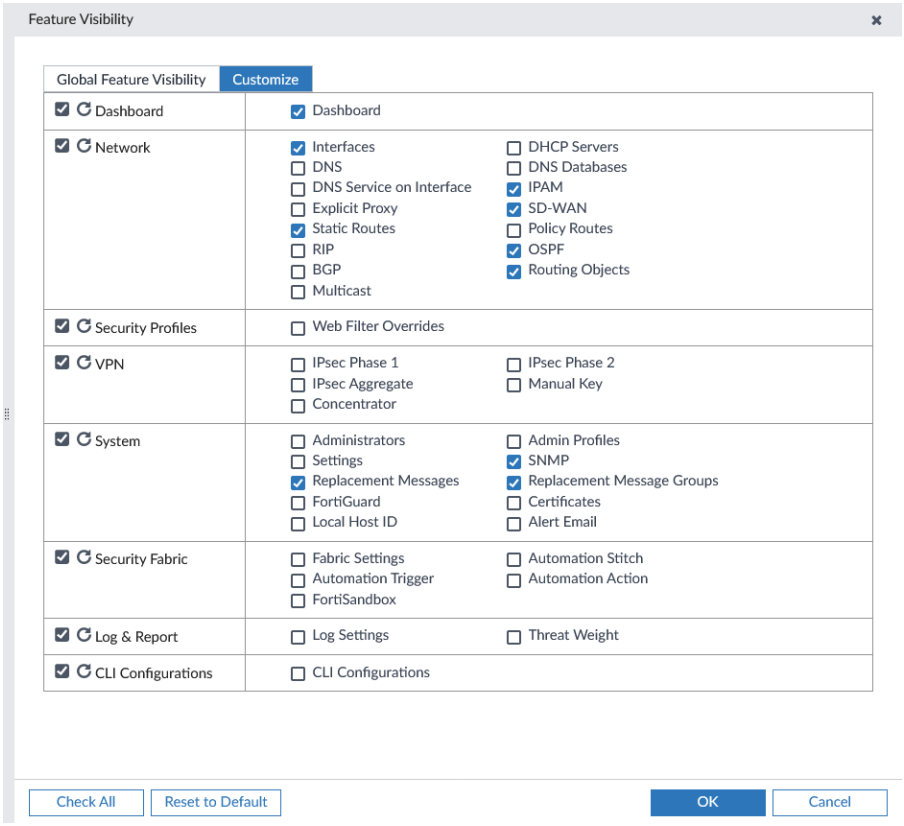
The available options depend on the ADOM version.

   Select *Check All* at the bottom of the window to select all content panels. Select *Reset to Default* at the bottom of the window to reset all of the selected panels to the default settings.
4. Click *OK*.

To customize feature visibility for a device:

1. Go to the device database. See Displaying the device database on page 194.
   The *Dashboard* for the device database is displayed.

2. In the left pane, click *Feature Visibility*.
   The *Feature Visibility* dialog box is displayed.
3. Select *Customize*, and then select the checkboxes for the items you want to display on the toolbar, and clear the checkboxes for the items you want to hide from the toolbar.
   The selections apply only to the device.





The available options depend on the device model and settings configured for that model.

4. Click *OK*.

Using the CLI console for managed devices

You can access the CLI console of managed devices.

To use the CLI console:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Dashboard* > *Summary*.
3. On the *System Information* widget, in the *Operation* line, click *Connect to CLI via SSH*.
   The *Connect CLI via SSH* dialog box is displayed.
4. In the *Admin Name* box, type your admin login, and click *OK*.

The CLI console for the device is displayed.

5. At the prompt, type your password, and press *Enter*.
   You are connected.
   You can cut (*CTRL+C*) and paste (*CTRL+V*) text from the CLI console. You can also use *CTRL+U* to remove the line you are currently typing before pressing *ENTER*.
6. Click *Close* to exit.

Viewing and managing LTE modems

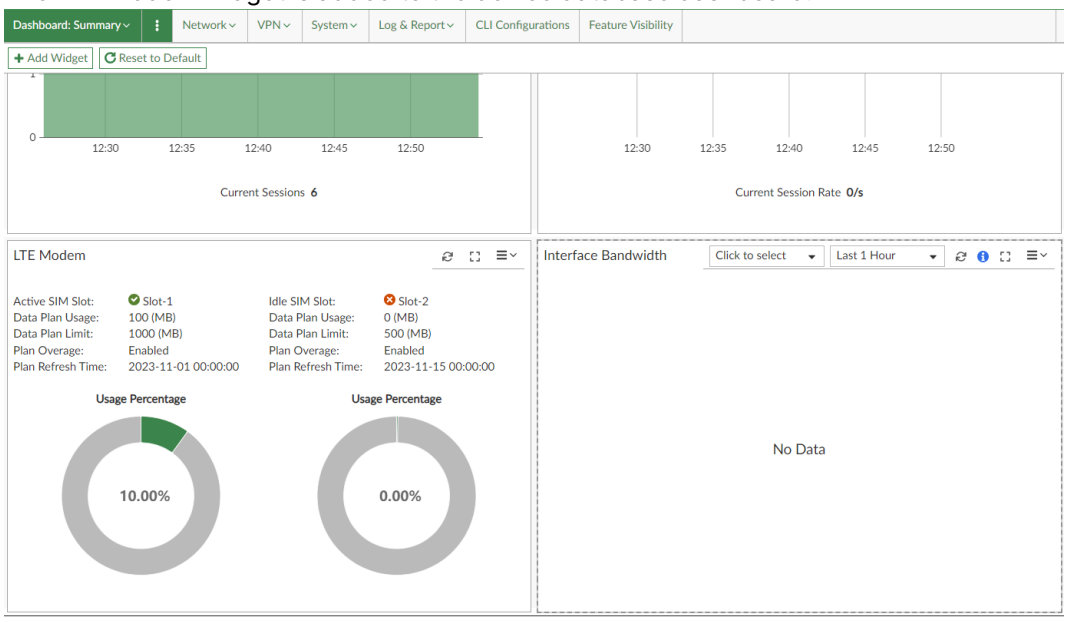
Using the device database, you can view the LTE monitor and configure LTE modem CLI configurations for managed FortiGate 3G4G devices.

Using the LTE Modem widget

The *LTE Modem* widget can be viewed by adding the LTE Modem widget to a device database dashboard. The *LTE Modem* widget includes data about SIM slots, data plan usage, data plan limits, plan overage status, and the plan refresh time.

To view the LTE monitor in the device dashboard:

1. Go to *Device Manager* > *Devices & Groups*.
2. Double click on the 3G4G FortiGate from the device table.
3. On a *Dashboard* page (For example *Dashboard: Summary*), click *Add Widget*.
4. Click the add icon next to *LTE Modem*.
5. The LTE Modem widget is added to the device database dashboard.

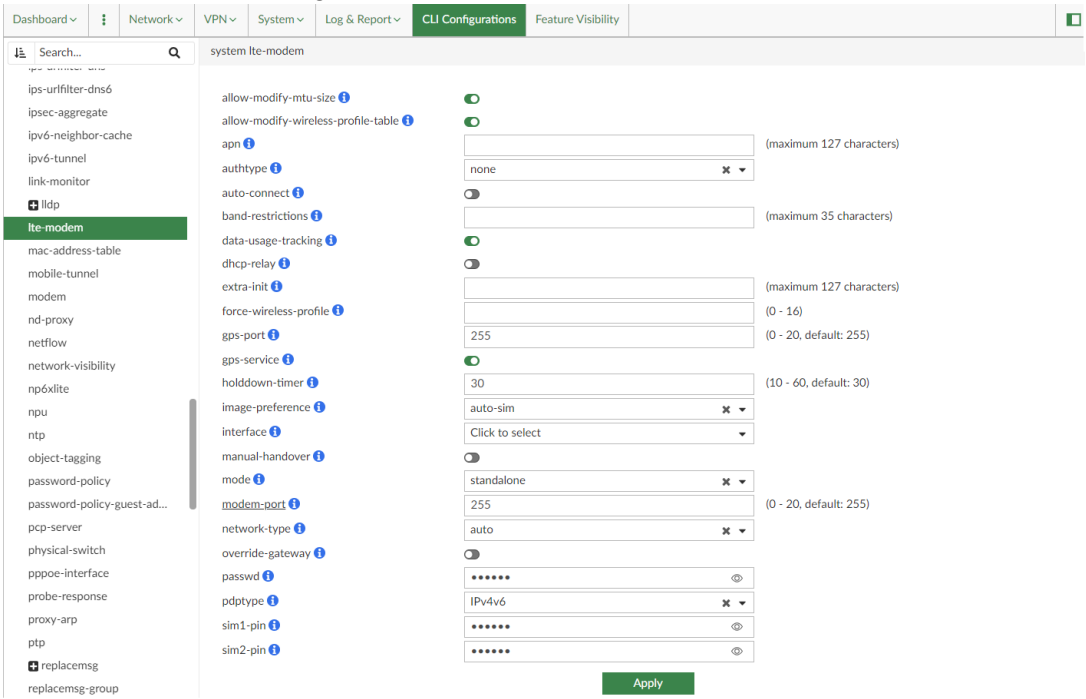


Configuring the LTE modem

Detailed configurations to the LTE modem can be performed using the *lte-modem* CLI configuration window in the device database.

To manage LTE modem configurations:

1. Go to *Device Manager* > *Devices & Groups*.
2. Double click on the 3G4G FortiGate from the device table.
3. Go to CLI Configurations.
   The *lte-modem* page is available in the CLI configurations window, and it can be used to show and make detailed LTE modem configurations.



FortiManager also includes an LTE Modem monitor when managing FortiGate 3G4G devices. See LTE modem monitors on page 401

Device DB - Dashboard

Each dashboard contains widgets that you can use to monitor information about the device.

You can add widgets to dashboards, create custom dashboards, and copy dashboards to other devices as needed.

- Adding widgets to dashboards on page 200
- Creating custom system dashboards on page 200
- Copying custom system dashboards on page 201

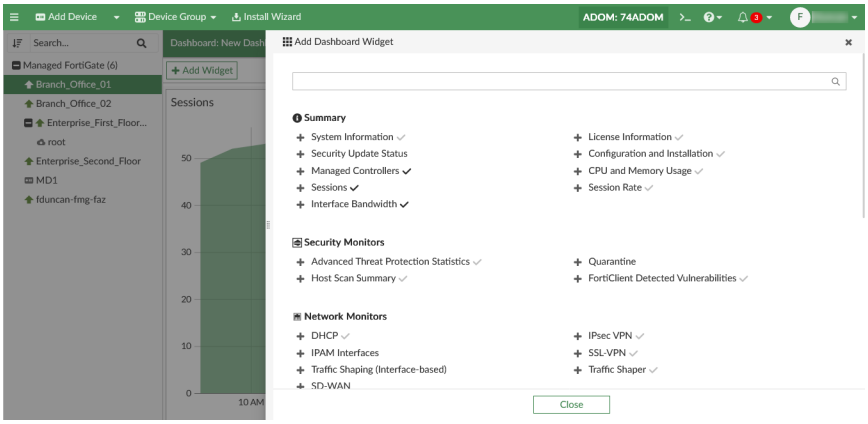
The *Dashboard* menu provides access to the following default dashboards:

- Summary dashboard on page 202
- Security Monitors dashboard
- Network Monitors dashboard

Adding widgets to dashboards

To add a widget to a dashboard:

1. Go to the device database. See Displaying the device database on page 194.
2. Select a dashboard from the Dashboard dropdown menu.
3. Click *Add Widget*.
   The *Add Dashboard Widget* pane displays.
4. Click the add icon ✚ next to the widgets you want to add to the dashboard, and click *Close*.



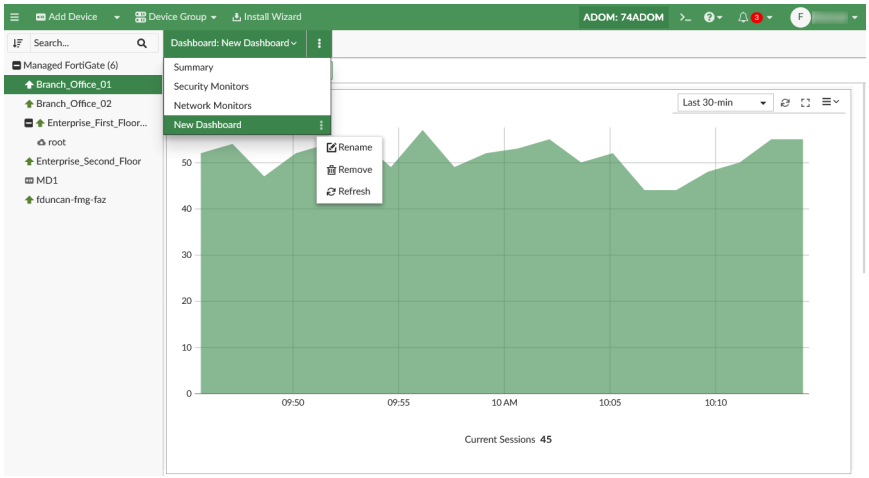
Creating custom system dashboards

In the device database, the *Dashboard* menu contains several dashboards, and each dashboard contains several widgets. You can create custom dashboards and change the dashboard layout.

To create custom dashboards:

1. Go to the device database. See Displaying the device database on page 194.
2. From the settings icon ⋮, select *Create New* .
   The *Create New Dashboard* pane is displayed.
3. In the *Dashboard Name* field, type a name, and click *OK*.
   The dashboard is created.
4. Click *Add Widget* to select widget(s) for the dashboard, and click *Close*.
   The widgets are added to the dashboard.
5. (Optional) Click the settings icon next to the dashboard name to *Rename*, *Remove*, or *Refresh* the dashboard.

You cannot remove the *Summary*, *Resource Usage*, and *Network Monitors* dashboards.



You cannot remove the default dashboards.

Copying custom system dashboards

In the device database, you can copy custom dashboards to and from other devices/VDOMs. After copying a dashboard to or from another device/VDOM, it can be customized further on each device individually.

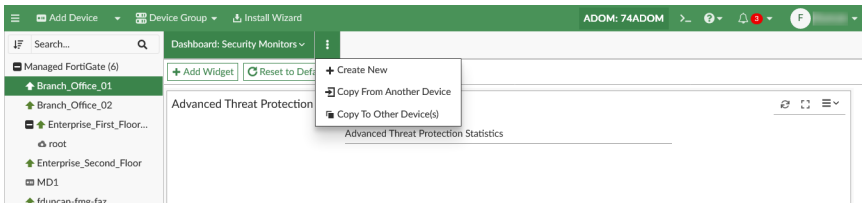
When copying dashboards to and from other devices/VDOMs, the target device's/VDOM's current dashboard configurations will be overwritten.

You cannot copy a dashboard to or from devices on different ADOMs.

You can also copy custom dashboards from devices when adding a new device using discover mode, model devices, CSV file, or when authorizing a device. For example, see Adding online devices using Discover mode on page 92.

To copy custom dashboards from another device:

1. Go to the device database to copy the custom dashboard to. See Displaying the device database on page 194.
2. From the settings icon for the *Dashboard* menu, select *Copy From Another Device*.



The *Copy From Device* pane is displayed.

3. From the *From Device* dropdown, select a device to copy dashboards from, and click *OK*.
   A message asks you to confirm the action.
4. Click *OK*.
   The dashboards are added to the device/VDOM with the same name and widgets as configured on the device/VDOM they were copied from.

To copy custom dashboards to other devices:

1. Go to the device database to copy the custom dashboard from. See Displaying the device database on page 194.
2. From the settings icon for the *Dashboard* menu, select *Copy To Other Device(s)*.
   The *Copy To Device* pane is displayed.
3. From the *To Device* dropdown, select the devices to copy the dashboards to, and click *OK*.
   A message asks you to confirm the action.
4. Click *OK*.
   The custom dashboard is now available on the select device(s)/VDOM(s). The dashboards have the same name and widgets as configured on the device/VDOM they were copied from.

If copying dashboards to and from VDOMs, the GUI will display VDOM instead of Device in the options and dialogs. For example, you will see *Copy From Another VDOM* instead of *Copy From Another Device*.

Summary dashboard

The *Summary* dashboard widgets provide quick access to device information. The following widgets are available:

- System Information
- License Information
- Configuration and Installation
- Summary dashboard (available when the ADOM is in backup mode)

The following table provide a description of these dashboard widgets. Note that not all of the listed options will be available on every device.

System Information	
Host Name	The host name of the device.

System Information	
Serial Number	The device serial number.
IP Address	The IP address of the device.
Platform Type	The platform type for the device.
HA Status	FortiGate HA configuration on FortiManager is read-only. Standalone indicates non-HA mode. Active-Passive, Active-Active indicates the device is operating in a cluster.
System Time	The device system time and date information.
Uptime	Displays the duration the device has been up.
Firmware Version	The device firmware version and build number.
Hardware Status	The number of CPUs and the amount of RAM for the device.
Operation Mode	Displays whether the device is in *NAT* or *Central NAT* operation mode.
VDOM	The status of VDOMs on the device.
Operation	Select one of the following: • *Connect to CLI via SSH* to connect to the CLI console of the device • *Reboot* to reboot the device • *Shutdown* to shut down the device
License Information	
FortiCare Support	The support contract information and the expiry date. The support contract includes the following: Registration, Hardware, Firmware, and Support Level e.g. Enhanced Support, Comprehensive Support.  FortiManager does not retrieve *FortiCare Support* information when the device was added using *Add Model Device*, even when the device is registered to the same FortiCloud account.
FortiGuard Services	The contract version, issue date and service status. FortiGuard Services includes the following: Antivirus, Intrusion protection, Web filtering, Email Filtering, Outbreak Protection, and Industrial Security Service.
VDOM	The number of virtual domains that the device supports.
Configuration and Installation	
Enforce Firmware Version	The firmware version enforced on the device. The firmware version is enforced when FortiGate is connected to the network. Click the *Edit* icon to select the firmware version. You can also select the firmware version in the *Add Device* screen when adding a model device. For more information, see Adding offline model devices on page 104.

Configuration and Installation	
System Template	The system template installed on the device. The system template is installed when FortiGate is connected to the network. Click the *Edit* icon to select the system template. You can also select the system template in the *Add Device* screen when adding a model device. For more information, see Adding offline model devices on page 104.
Policy Package	The policy package installed on the device. The policy package is installed when FortiGate is connected to the network. Click the *Edit* icon to select the policy package. You can also select the policy package in the *Add Device* screen when adding a model device. For more information, see Adding offline model devices on page 104.
Database Configuration	Select *View* to display the configuration file of the FortiGate unit.
Total Revisions	Displays the total number of configuration revisions and the revision history. Select *Revision History* to view device history. Select the revision history icon to open the *Revision Diff* menu. You can view the diff from a previous revision or a specific revision and select the output.
Config Status	The synchronization status with the FortiManager: • *Synchronized*: The latest revision is confirmed as running on the device. • *Out_of_sync*: The configuration file on the device is not synchronized with the FortiManager system. • *Unknown*: The FortiManager system is unable to detect which revision (in revision history) is currently running on the device. Select *Refresh* to update the Installation Status.
Warning	Displays any warnings related to configuration and installation status: • *None*: No warning. • *Unknown configuration version running on FortiGate: FortiGate configuration has been changed!*: The FortiManager system cannot detect which revision (in *Revision History*) is currently running on the device. • *Unable to detect the FortiGate version*: Connectivity error! • *Aborted*: The FortiManager system cannot access the device.
Installation Tracking	
Device Settings Status	• *Modified*: Some configuration on the device has changed since the latest revision in the FortiManager database. Select *Save Now* to install and save the configuration. • *UnModified*: All configuration displayed on the device is saved as the latest revision in the FortiManager database.
Installation Preview	Select the icon to display a set of commands that will be used in an actual device configuration installation in a new window.
Last Installation	The FortiManager system sent a configuration to the device at the indicated date and time.

Configuration and Installation		
	Scheduled Installation	A new configuration will be installed on the device at the indicated date and time.
Script Status		Select Configure to view script execution history.
	Last Script Run	Displays the date when the last script was run against the managed device.
	Scheduled Script	Displays the date when the next script is scheduled to run against the managed device.



The information presented in the System Information, License Information, and Configuration and Installation Status widgets will vary depending on the managed device model.

Device DB - configuration management

FortiManager maintains a configuration repository to manage device configuration revisions. After modifying device configurations, you can save them to the FortiManager repository and install the modified configurations to individual devices or device groups. You can also retrieve the current configuration of a device or revert a device's configuration to a previous revision.

This section contains the following topics:

- Checking device configuration status on page 205
- Viewing configuration revision history
- Viewing configuration settings on FortiGate on page 208
- Adding a tag to configuration versions on page 208
- Downloading a configuration file on page 208
- Importing a configuration file on page 209
- Comparing different configuration files on page 209
- Reverting to another configuration file on page 210

Checking device configuration status

In the *Device Manager* pane, when you select a device, you can view that device's basic information under the *device dashboard*. You can also check if the current configuration file of the device stored in the FortiManager repository is in sync with the one running on the device.

If you make any configuration changes to a device directly, rather than using the FortiManager system, the configuration on the device and the configuration saved in the FortiManager repository will be out of sync. In this case, you can re synchronize with the device by retrieving the configuration from the device and saving it to the FortiManager repository.

You can use the following procedures when checking device configuration status on a FortiGate, FortiCarrier, or FortiSwitch.

To check the status of a configuration installation on a FortiGate unit:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Dashboard* > *Summary*.
3. Locate the *Configuration and Installation* widget.
   The *Configuration and Installation Status* widget shows the following information:

Configuration		
	Config Status	Displays the synchronization status of the configuration with FortiManager. • *Synchronized*: The latest revision is confirmed as running on the device. • *Out_of_sync*: The configuration file on the device is not synchronized with the FortiManager system. • *Unknown*: The FortiManager system is unable to detect which revision (in revision history) is currently running on the device. • *Auto-update*: The configuration was changed directly on the FortiGate, and the changes were automatically retrieved to the FortiManager's device database. See: Auto-update and auto-retrieve on page 54. Click *Refresh* to update the synchronization status.
	Provisioning Template	Displays the name of the selected provisioning templates. Click + to add or edit selected provisioning templates.
Revision		
	Total Revisions	Displays the total number of configuration revisions and the revision history. Click *Revision History* to view device history. For details, see Viewing configuration revision history on page 206. Click *Revision Diff* to compare revisions. For details, see Comparing different configuration files on page 209.
	Last Installation	Displays the last installation's date, time, revision number, and the person who did the installation.
	Device Configuration DB	Click *View Full Config* to display the database configuration file of the FortiGate unit. Click *View Diff* to display the *Device Revision Diff* dialog box.

Viewing configuration revision history

The revision history repository stores all configuration revisions for a device. You can view the version history, view configuration settings and changes, import files from a local computer, compare different revisions, revert to a previous revision, and download configuration files to a local computer.

To view the revision history of a FortiGate unit:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Dashboard* > *Summary*.
3. In the *Configuration and Installation* widget, click the *Revision History* icon.
   In the *Configuration Revision History* dialog box is displayed. The toolbar contains the following buttons:

View Config	View the configuration for the selected revision.
View Install Log	View the installation log for the selected revision.
Revision Diff	Show only the changes or differences between two versions of a configuration file. For details, see Comparing different configuration files on page 209.
Retrieve Config	View the current configuration running on the device. If there are differences between the configuration file on the device and the configuration file in the repository, a new revision is created and assigned a new ID number.
More	From the More menu, you can select one of the following: • Download Factory Default • Revert • Delete • Rename • Import Revision • Download Revision

You can also right-click a revision to access the same options.

The following columns of information are displayed:

ID	The revision number. Double-click an ID to view the configuration file. You can also click *Download* to save the configuration file.
Date & Time	The time and date when the configuration file was created.
Name	A name assigned by the user to make it easier to identify specific configuration versions. You can rename configuration versions.
Created by	The name of the administrator account used to create the configuration file.
Installation	Display the status of the installation. *N/A* indicates that the revision was not sent to the device. The typical situation is that the changes were part of a later revision that was sent out to the device. For example, you make some changes and commit the changes. Now you have a revision called ID1. Then you make more changes and commit the changes again. Then you have a revision called ID2, which also includes the changes you made in revision ID1. If you install revision ID2, then the status of revision ID1 becomes N/A.
Comments	Display the comment added to this configuration file when you rename the revision.

Viewing configuration settings on FortiGate

The revision history repository stores all configuration revisions for a device. You can view the version history, view configuration settings and changes, import files from a local computer, compare different revisions, revert to a previous revision, and download configuration files to a local computer.

To view the configuration settings on a FortiGate unit:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Dashboard* > *Summary*.
3. Locate the *Configuration and Installation* widget.
4. In the *Total Revisions* row, click the *Revision History* button.
   The *Configuration Revision History* dialog box is displayed.
5. Select the revision, and click *View Config*. The *View Configuration* pane is displayed.
6. To download the configuration settings, click *Download*.
7. Click *Return* when you finish viewing.

Adding a tag to configuration versions

To add a tag (name) to a configuration version on a FortiGate unit:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Dashboard* > *Summary*.
3. Locate the *Configuration and Installation* widget.
4. In the *Total Revisions* row, click the *Revision History* button.
   The *Configuration Revision History* dialog box is displayed.
5. Right-click the revision, and select *Rename*.
6. Type a name in the *Tag (Name)* field.
7. Optionally, type information in the *Comments* field.
8. Click *OK*.

Downloading a configuration file

You can download a configuration file and a factory default configuration file.

To download a configuration file:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Dashboard* > *Summary*.
3. Locate the *Configuration and Installation* widget.
4. In the *Total Revisions* row, click the *Revision History* button.
   The *Configuration Revision History* dialog box is displayed.
5. Select the revision you want to download.

6. Click *View Config* > *Download*.
   The *Download Revision* dialog box is displayed.
7. Select *Regular Download* or *Encrypted Download*. If you select *Encrypted Download*, type a password.
8. Click *OK*.

To download a factory default configuration file:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Dashboard* > *Summary*.
3. Locate the *Configuration and Installation* widget.
4. In the *Total Revisions* row, click the *Revision History* button.
   The *Configuration Revision History* dialog box is displayed.
5. From the More menu, select *Download Factory Default*.

Importing a configuration file

You can import a configuration file into the FortiManager repository.



You can import a configuration file that is downloaded from the FortiManager repository or from the FortiGate directly. Encrypted configuration files downloaded from FortiGate are not supported.

To import a configuration file from a local computer:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Dashboard* > *Summary*.
3. Locate the *Configuration and Installation* widget.
4. In the *Total Revisions* row, click the *Revision History* button.
   The *Configuration Revision History* dialog box is displayed.
5. Right-click a revision and select *Import Revision*.
6. Click *Browse* and locate the revision file, or drag and drop the file onto the dialog box.
7. If the file is encrypted, select *File is Encrypted*, and type the password.
8. Click *OK*.

Comparing different configuration files

You can compare the changes or differences between two versions of a configuration file by using the *Diff* function.

The *Diff* function behaves differently under certain circumstances.

For example, when a device is first added to the FortiManager system, the FortiManager system gets the configuration file directly from the FortiGate unit and stores it as is. This configuration file is version/ID 1.

If you make changes to the device configuration in *Device Manager* and select *Commit*, the new configuration file is saved as version/ID 2. If you use the *Diff* icon to view the changes/differences between version/ID 1 and version/ID 2, you will be shown more changes than you have made.

This happens because the items in the file version/ID 1 are ordered as they are on the FortiGate unit. Configurations of version/ID 2 are sequenced differently when they are edited and committed in *Device Manager*. Therefore, when you compare version/ID 1 and version/ID 2, the *Diff* function sees every item in the configuration file as changed.

If you take version/ID 2, change an item and commit it, the tag is changed to version/ID 3. If you use *Diff* with version/ID 2 and version/ID 3, only the changes that you made are shown. This is because version/ID 2 and version/ID 3 have both been sequenced in the same way in *Device Manager*.

To compare different configuration files:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Dashboard* > *Summary*.
3. Locate the *Configuration and Installation* widget.
4. In the *Total Revisions* row, click the *Revision History* button.
   The *Configuration Revision History* dialog box is displayed.
5. Select a revision, and click *Revision Diff* in the toolbar.
6. In the Compare Database <name> Against section, select another version for the diff.
7. In the *Diff Output* section, select *Show Full File Diff*, *Show Diff Only*, or *Capture Diff to a Script*.
   Show Full File Diff shows the full configuration file and highlights all configuration differences.
   Show Diff Only shows only configuration differences.
   Capture Diff to a Script downloads the diff to a script.
8. Click *Apply*.
   If you selected show diff, the configuration differences are displayed in colored highlights. If you selected capture to a script, the script is saved in your downloads folder.

Reverting to another configuration file

To revert to another configuration file:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Dashboard* > *Summary*.
3. Locate the *Configuration and Installation* widget.
4. In the *Total Revisions* row, click the *Revision History* button.
   The *Configuration Revision History* dialog box is displayed.
5. Right-click the revision to which you want to revert, and click *Revert*.
   The system immediately reverts to the selected revision.

Device DB - Network Interface

You can view interface information about individual devices in the *Device Manager* tab.

This section also includes information on the following topics:

- Device zones on page 211
- Interface packet capture on page 212

To view interfaces for a device:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Network* > *Interfaces*. The *Interface* pane is displayed.
   While viewing the interfaces table, you can toggle full screen mode by clicking *Full Screen/Exit Full Screen*.

To create aggregate interfaces for devices:

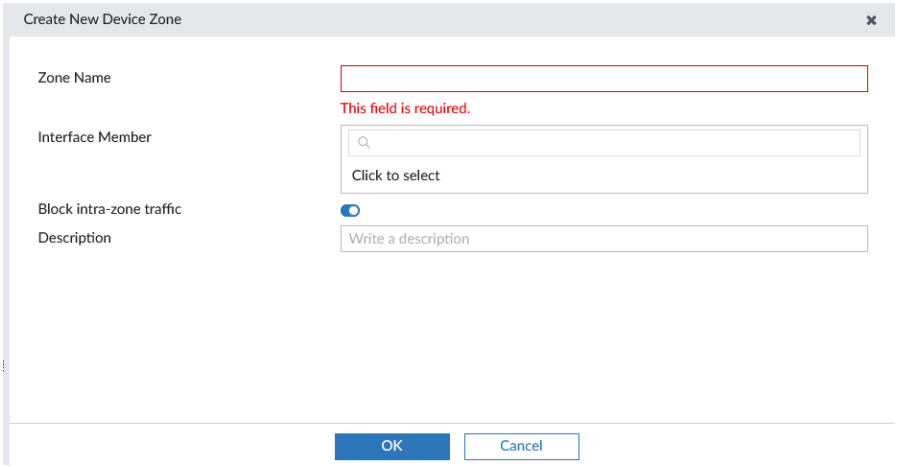
1. Go to the device database.
2. In the device database, go to *Network* > *Interface*.
3. Select *Create New* > *Interface*.
4. In the *Type* dropdown menu, select *Aggregate*.
5. Configure the aggregate interface details, and click *OK*.
6. (Optional) You can leave the *Physical Interface Member* field empty.
7. After the interface is created, you can deploy the interface to FortiGate.

Device zones

When creating a device zone, map the zone to a physical interface. You must also map the zone to a normalized interface to use the zone in a policy. See also Normalized interfaces on page 544.

To create a device zone:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Network* > *Interface*. The *Interface* pane is displayed.
3. Click *Create New* > *Device Zone*.
   The *New Device Zone* pane opens.



4. Complete the options, and click *OK*.
   The interface members are physical interfaces.
5. Create a normalized interface for the zone. See Creating normalized interfaces on page 548.

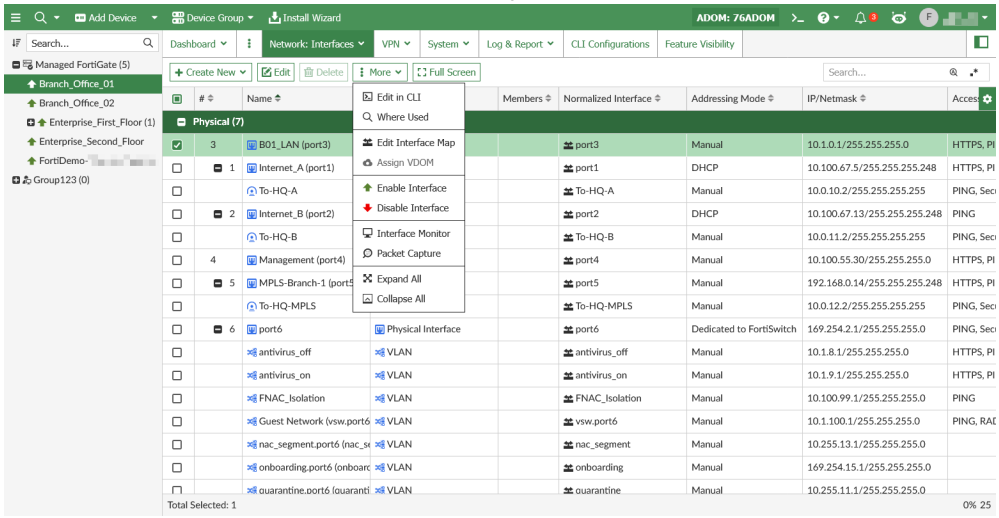
Interface packet capture

You can perform packet capture on a managed FortiGate's interface through the device database.

For additional information on performing packet capture on FortiGate interfaces, see Using the packet capture tool in the FortiGate/FortiOS Administration Guide.

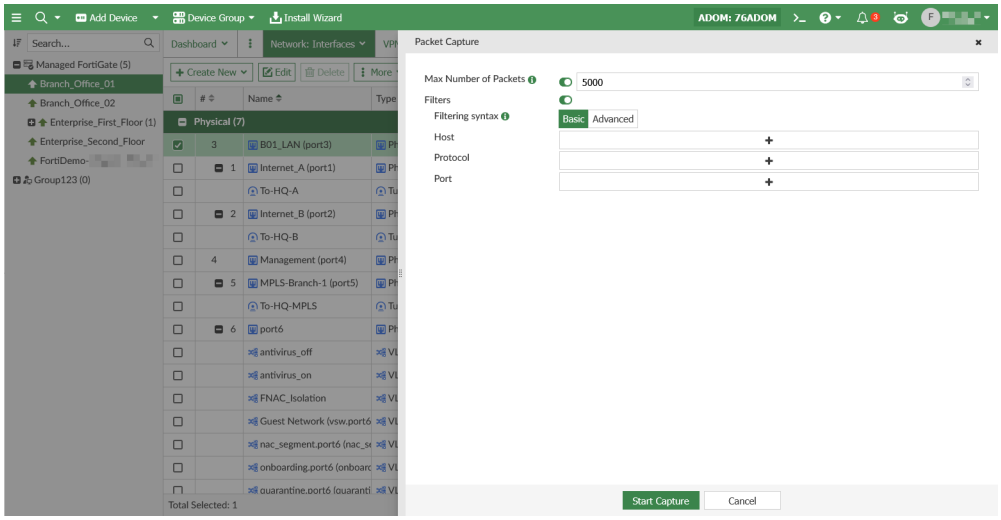
To perform a packet capture on managed FortiGate interfaces:

1. In *Device Manager*, select a FortiGate and go to *Network> Interfaces*.
2. Select an interface, click *More > Packet Capture*.



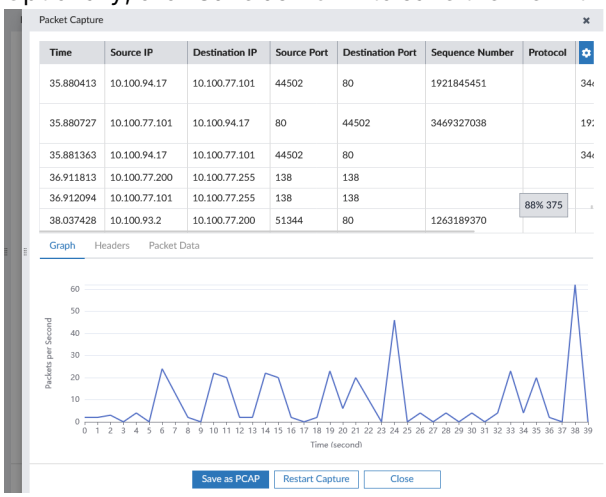
3. You can configure the *Max Number of Packets* and/or *Filters*, and click *OK* to start the packet capture.

   If *Max Number of Packets* is not specified, the packet capture will stop after the default maximum supported packets is reached to preserve memory. You can view the default maximum for the interface by hovering your mouse over the info icon. This maximum depends on the device model.



4. Select *Graph*, *Headers*, or *Packet Data* to view details of the packet.

5. Optionally, click *Save as PCAP* to save the file in the .pcap format.



Device DB - System Virtual Domain

Virtual domains (VDOMs) enable you to partition and use your FortiGate unit as if it were multiple units. This section contains the following topics:

- Enabling virtual domains on page 213
- Viewing virtual domains on page 214
- Creating virtual domains on page 215
- Configuring inter-VDOM routing on page 215
- Deleting a virtual domain on page 216
- Editing resource limits on page 216

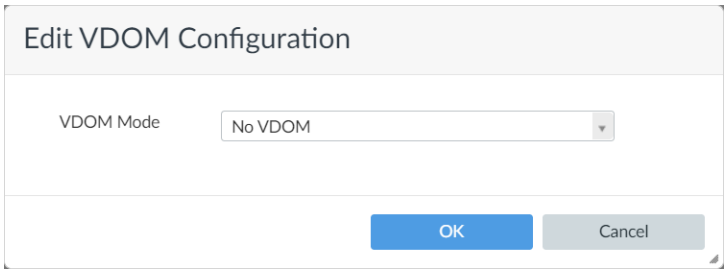
For more information about VDOMs, see the FortiOS Administration Guide available in the Fortinet Document Library.

Enabling virtual domains

Before you can create virtual domains, you must enable virtual domains on the device.

To enable virtual domains:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Dashboard > Summary*.
3. In the *System Information* widget, click the *Edit VDOM* icon beside *VDOM*.
   The *Edit VDOM Configuration* dialog box is displayed.



4. In the *VDOM Mode* box, select *Multi VDOM* or *Split VDOM*, and click *OK*.
5. Create virtual domains. See Creating virtual domains on page 215.

Viewing virtual domains

Before you can access the Virtual Domain pane in the device database, you must enable VDOMs for the device.

To view virtual domains:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *System* > *Virtual Domain*. The *Virtual Domain* pane is displayed.

The *Virtual Domain* menu may be hidden. See Choosing feature visibility for devices on page 195.

The following toolbar displays at the top of the page:

Create New	Select to create a new virtual domain.
Edit	Select a VDOM, and click *Edit* to edit the settings.
Delete	Select a VDOM, and click Delete to remove it. This function applies to all virtual domains except the root.
Resource Limits	Select a VDOM, and click *Resource Limits* to configure the resource limit profile.
Set Management	Select a VDOM, and click *Set Management* to define the VDOM as the root VDOM also known as the management VDOM.

Under the toolbar, the following columns of information are displayed:

Name	The name of the virtual domain and if it is the management VDOM.
NGFW Mode	Displays the Next Generation Firewall setting for the VDOM of *Profile-based* or *Policy-based*.
Operation Mode	Displays the operation mode for the VDOM.
Status	Displays the status of the VDOM.
Interfaces	Displays the interfaces for the VDOM.

Creating virtual domains

You must enable virtual domains on the device before you can create virtual domains. See Enabling virtual domains on page 213.

To create virtual domains:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *System* > *Virtual Domain*.



The *Virtual Domain* tab may be hidden. See Choosing feature visibility for devices on page 195.

3. Click *Create New* to create a new VDOM.
   After the first VDOM is created you can create additional VDOMs by right-clicking on the existing VDOM and selecting *Add VDOM* from the right-click menu.
4. Complete the options, and click *OK* to create the new VDOM.

Configuring inter-VDOM routing

By default, for two virtual domains to communicate it must be through externally connected physical interfaces. Inter-VDOM routing creates a link with two ends that act as virtual interfaces, internally connecting the two virtual domains.

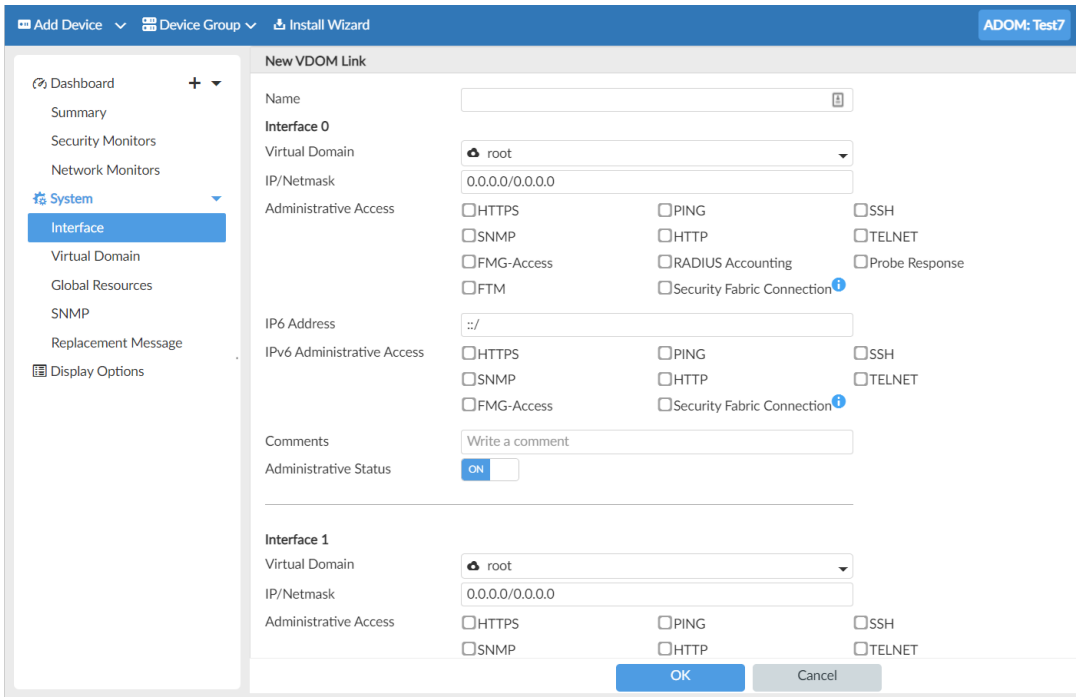
Before configuring inter-VDOM routing:

- You must have at least two virtual domains configured.
- The virtual domains must all be in NAT mode.
- Each virtual domain to be linked must have at least one interface or subinterface assigned to it.

To create a VDOM link:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *System* > *Interface*.

3. Click *Create New* > *VDOM Link*. The *New VDOM Link* pane opens.



4. Complete the options, and click *OK* to save your settings.

Deleting a virtual domain

Prior to deleting a VDOM, all policies must be removed from the VDOM. To do this, apply and install a blank, or empty, policy package to the VDOM (see Create new policy packages on page 415). All objects related to the VDOM must also be removed, such as routes, VPNs, and admin accounts.

To delete a VDOM:

1. Go to the device database. See Displaying the device database on page 194.
2. Go to *System* > *Virtual Domain*.
3. Right-click the VDOM, and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the VDOM.

Editing resource limits

To edit resource limits:

1. Go to the device database. See Displaying the device database on page 194.
2. Go to *System* > *Virtual Domain*.
3. Select the VDOM, and click *Resource Limits* in the toolbar.
4. Edit the settings, and click *OK* to save the changes.

Device DB - Network SD-WAN

In the device database, you can use the *SD-WAN* pane to configure SD-WAN for a device. When you use the device database to configure SD-WAN, you are using SD-WAN per-device management. For information about SD-WAN central management, see SD-WAN templates on page 304.

In the device database, the *SD-WAN* pane lets you:

- Create SD-WAN zones and interface members
- Create IPsec VPN tunnels by using a wizard
- Create performance SLA
- Create SD-WAN rules
- (Optional) Add BGP Neighbors
- Enable packet duplication

Using SD-WAN per-device management consists of the following steps:

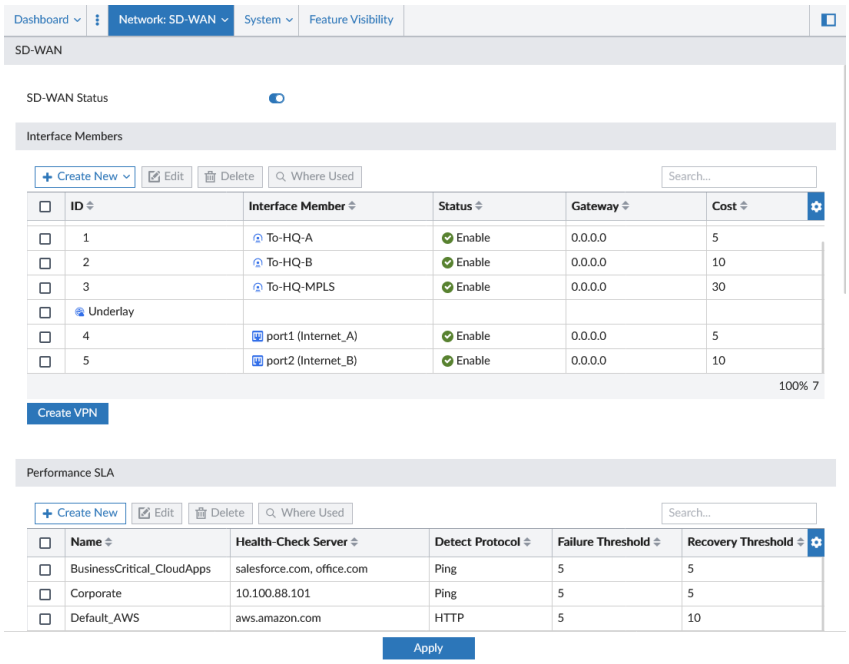
1. (Optional) Specify BGP Neighbors that you can select in SD-WAN configurations. See BGP Neighbors on page 225.
2. Configure SD-WAN settings for each device. See SD-WAN per-device management on page 217.
3. Install device settings using the *Install Wizard*. See Install device settings only on page 183.
4. Monitor SD-WAN networks. See SD-WAN Monitor on page 386.

SD-WAN per-device management

In the device database, use the *SD-WAN* pane to configure SD-WAN directly on each device.

To configure SD-WAN directly on a device:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Network* > *SD-WAN*.
   The *SD-WAN* pane opens.



3. Configure the following options, and click *Apply*:

SD-WAN Status	Select *On* or *Off*.
Interface Members	Zones and interface members can be added, edited, and removed. See SD-WAN zones and interface members on page 218.
Create VPN	See IPsec VPN Wizard on page 220.
Performance SLA	See Performance SLA on page 222.
SD-WAN Rules	See SD-WAN rules on page 222.
Neighbor	See BGP Neighbors on page 225.
Duplication	See Duplication on page 225.
Advanced Options	Expand *Advanced Options* to view and set the options. Hover the mouse over each advanced option to view a description of the option.

The SD-WAN settings are saved.

4. Install the device settings to the device.

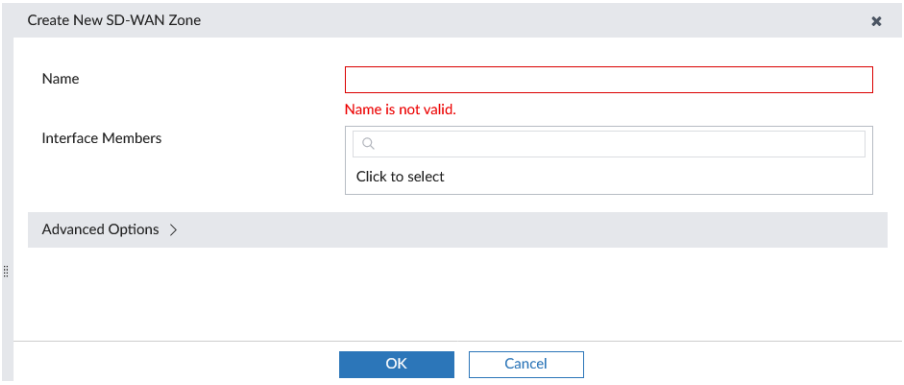
SD-WAN zones and interface members

For each device, you can create SD-WAN zones and interface members. You can select SD-WAN zones as source and destination interfaces in firewall policies. You cannot select interface members of SD-WAN zones in firewall policies.

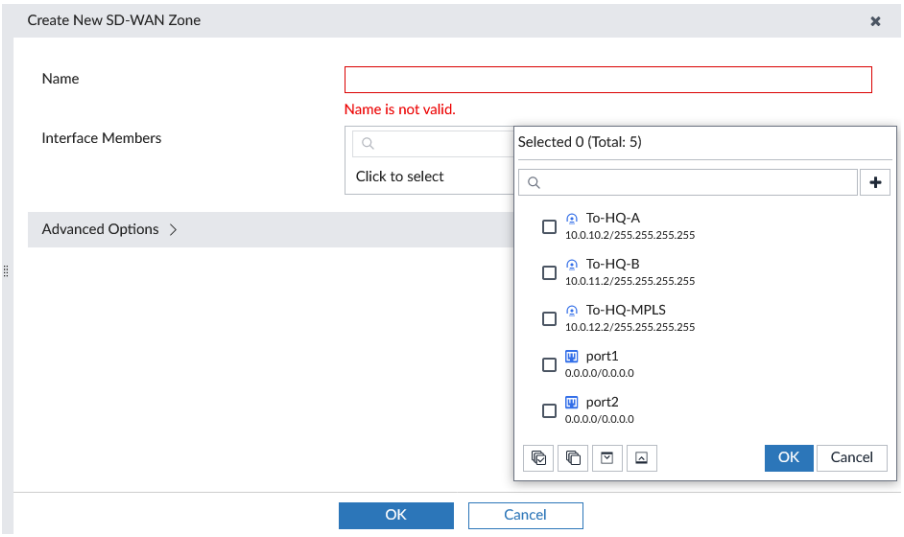
The default SD-WAN zone is named `virtual-wan-link`.

To create an SD-WAN zone:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Network* > *SD-WAN*.
   The *SD-WAN* pane opens.
3. In the *Interface Members* section, click *Create New* > *SD-WAN Zone*.
   The *Create New SD-WAN Zone* dialog box is displayed.



4. In the *Name* box, type a name for the zone.
5. Click the *Interface Members* box.
   The list of interfaces is displayed.

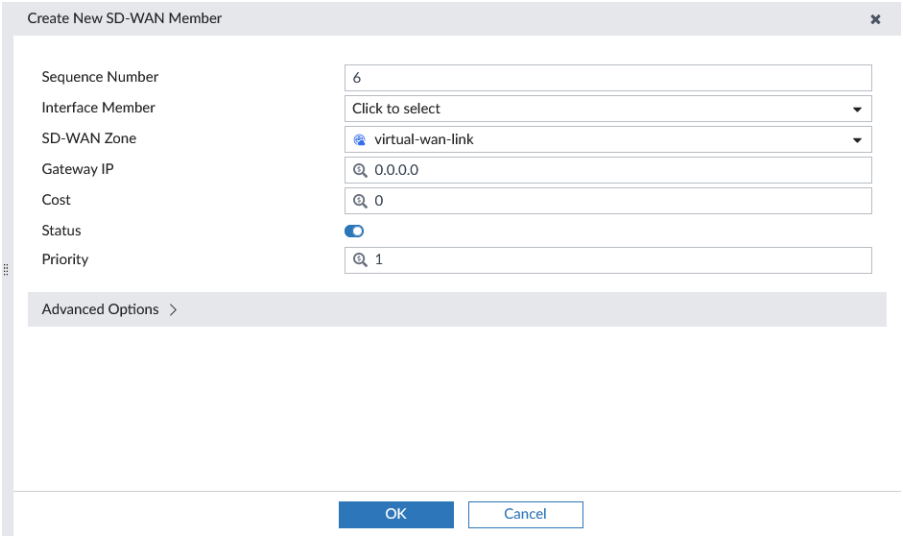


6. Select the interfaces to be members of the zone, and click *OK*.
7. (Optional) Expand the *Advanced Options*, and set them.
   Hover the mouse over each advanced option to view a description of the option.
8. Click *OK* to finish creating the zone.
9. Click *Apply* to save the SD-WAN settings.

To create an SD-WAN interface member:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Network* > *SD-WAN*.
   The *SD-WAN* pane opens.

3. In the *Interface Members* section, click *Create New > SD-WAN Member*.
   The *Create New SD-WAN Interface Member* dialog box is displayed.



4. Set the options, and click *OK*.
   The interface is added to the zone.
5. Click *Apply* to save the SD-WAN settings.

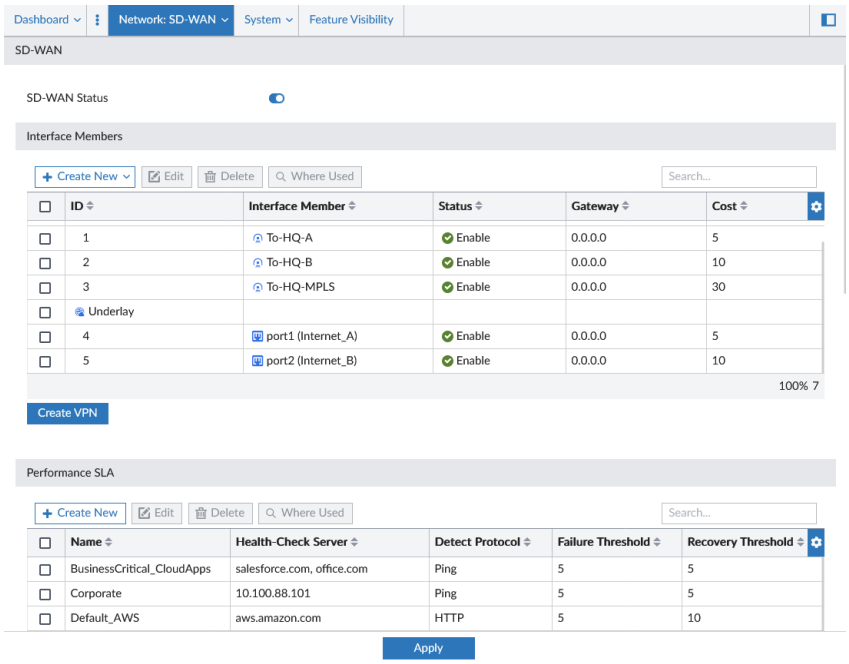
IPsec VPN Wizard

For each device, the SD-WAN pane includes access to an IPsec VPN Wizard. You can use the wizard to create IPsec VPN tunnels and automatically generate interface members for the tunnel.

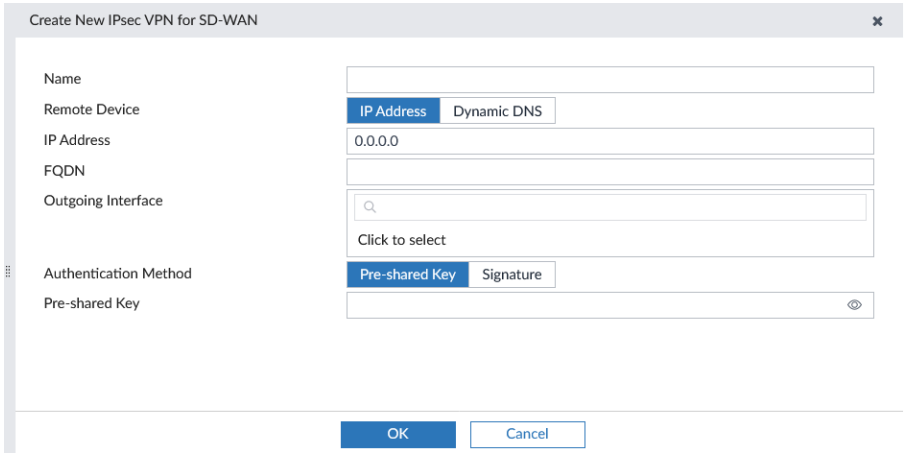
To configure the IPsec VPN in SD-WAN:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Network > SD-WAN*.
   The *SD-WAN* pane opens.

3. In the *Interface Members* section, click *Create VPN*.



The *Create IPsec VPN for SD-WAN* dialog box is displayed.



4. Configure the following settings, and click *OK* to generate IPsec VPNs:

Name	Specify a name for the VPN.
Remote Device	Select *IP Address* or *Dynamic DNS*.
IP Address	Specify the IP address if *IP Address* is selected for *Remote Device*.
FQDN	Specify the FQDN if *Dynamic DNS* is selected for *Remote Device*.
Outgoing Interface	Select the outgoing interface.
Authentication Method	Select *Pre-shared key* or *Signature*.
Certificate Name	Select the certificate (if *Signature* was selected as the *Authentication Method*)

Peer Certificate CA	Select the Peer Certificate CA (if *Signature* was selected as the *Authentication Method*)
Pre-shared Key	Select the pre-shared key (if *Pre-shared key* was selected as the *Authentication Method*)

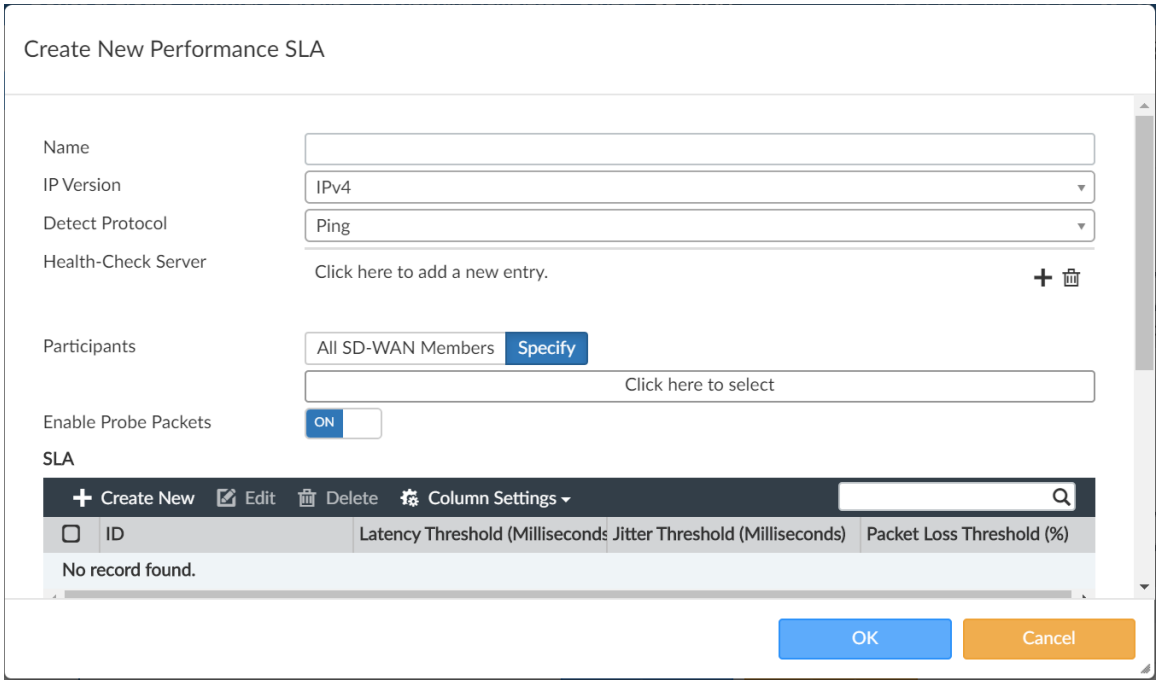
The auto-generated VPN interface is automatically added to the list of SD-WAN interface members.

5. Edit the VPN in *Interface Members* to configure *Gateway IP*, *Estimated Upstream Bandwidth (Kbps)*, and *Estimated Downstream Bandwidth (Kbps)*.
6. Click *Apply* to save the SD-WAN settings.

Performance SLA

To create a new performance SLA:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Network* > *SD-WAN*.
   The *SD-WAN* pane opens.
3. In the *Performance SLA* section, click *Create New*.
   The *Create Performance SLA* dialog-box opens



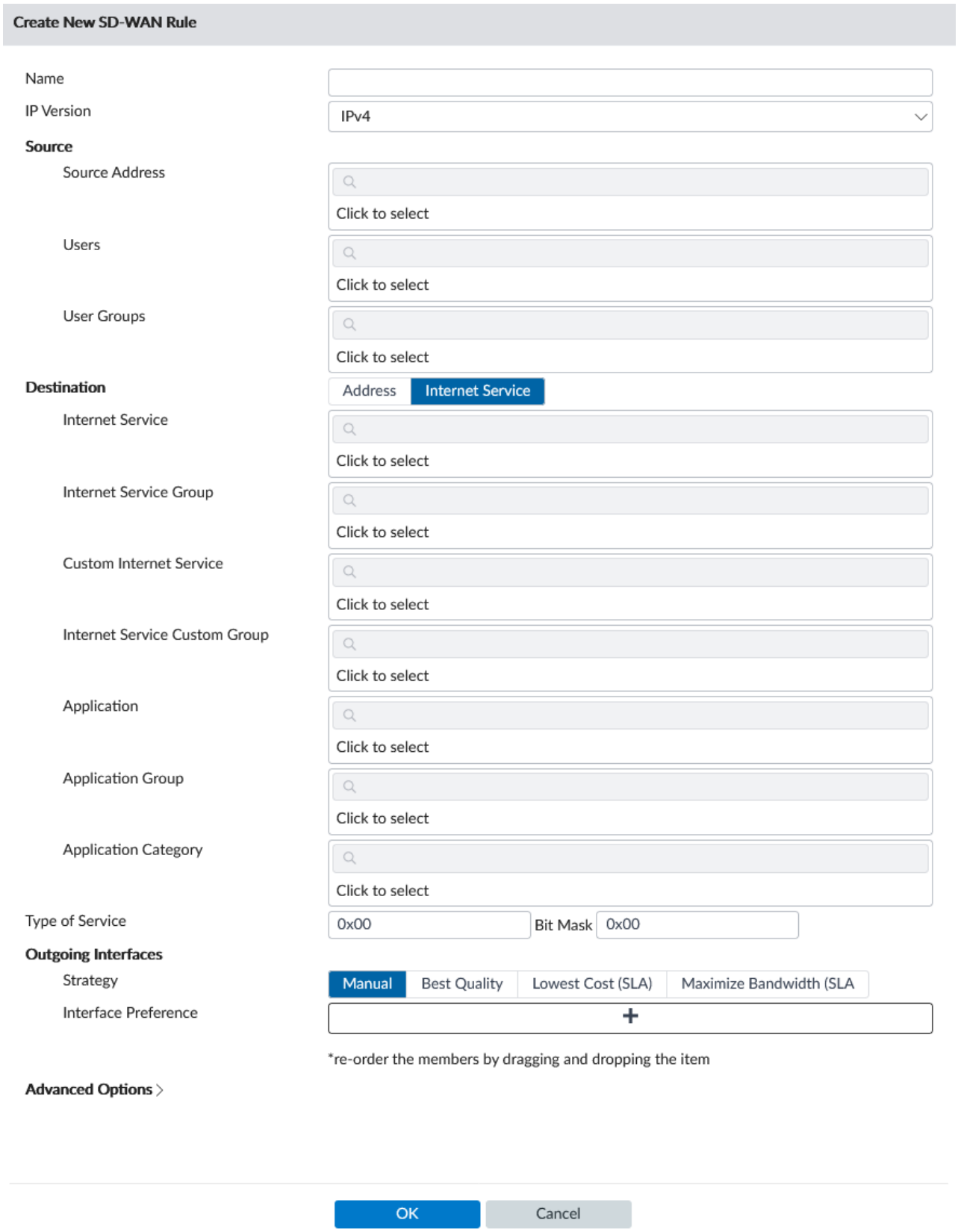
4. Configure the options, and click *OK* to create the performance SLA.
5. Click *Apply* to save the SD-WAN settings.

SD-WAN rules

Configure SD-WAN rules for WAN links by specifying the required network parameters.

To create a new SD-WAN rule:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Network* > *SD-WAN*.
   The *SD-WAN* pane opens.
3. In the *SD-WAN Rules* section, click *Create New*.
   The *Create New SD-WAN Rule* dialog-box opens.


Create New SD-WAN Rule
Name
IP Version
IPv4
Source
Source Address
Click to select
Users
Click to select
User Groups
Click to select
Destination
Address
Internet Service
Internet Service
Click to select
Internet Service Group
Click to select
Custom Internet Service
Click to select
Internet Service Custom Group
Click to select
Application
Click to select
Application Group
Click to select
Application Category
Click to select
Type of Service
0x00
Bit Mask
0x00
Outgoing Interfaces
Strategy
Manual
Best Quality
Lowest Cost (SLA)
Maximize Bandwidth (SLA
Interface Preference
*re-order the members by dragging and dropping the item
Advanced Options
OK
Cancel

4. Configure the options, and click *OK* to create the new SD-WAN rule.



Starting in FortiManager 7.2.0, you can configure application categories as a destination. The application category field uses the default internet service database (ISDB) categories received from FortiGuard. For more information about the options, see SD-WAN rules on page 312.

5. Click *Apply* to save the SD-WAN settings.

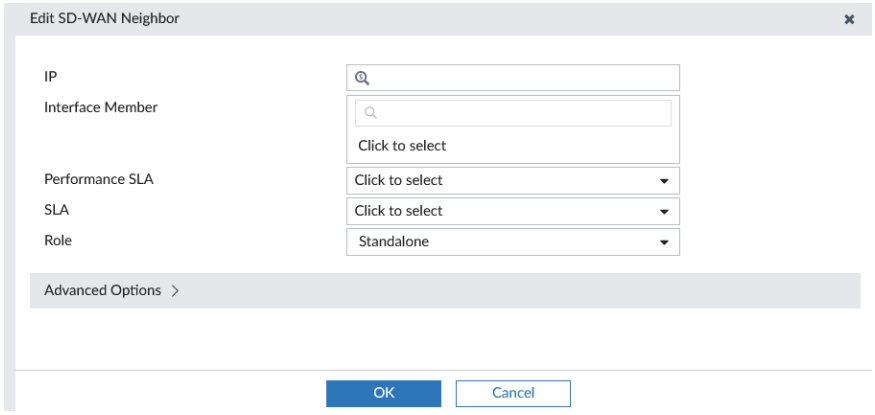
BGP Neighbors

When configuring SD-WAN per-device, you can add Border Gateway Protocol (BGP) neighbors.

You must create BGP neighbors for FortiGate devices before you can add them to the SD-WAN network. See Device DB - Network BGP on page 226.

To add BGP neighbors:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Network* > *SD-WAN*.
   The *SD-WAN* pane opens.
3. In the *Neighbor* section, click *Create New*.
   The *Create New Neighbor* dialog box is displayed.



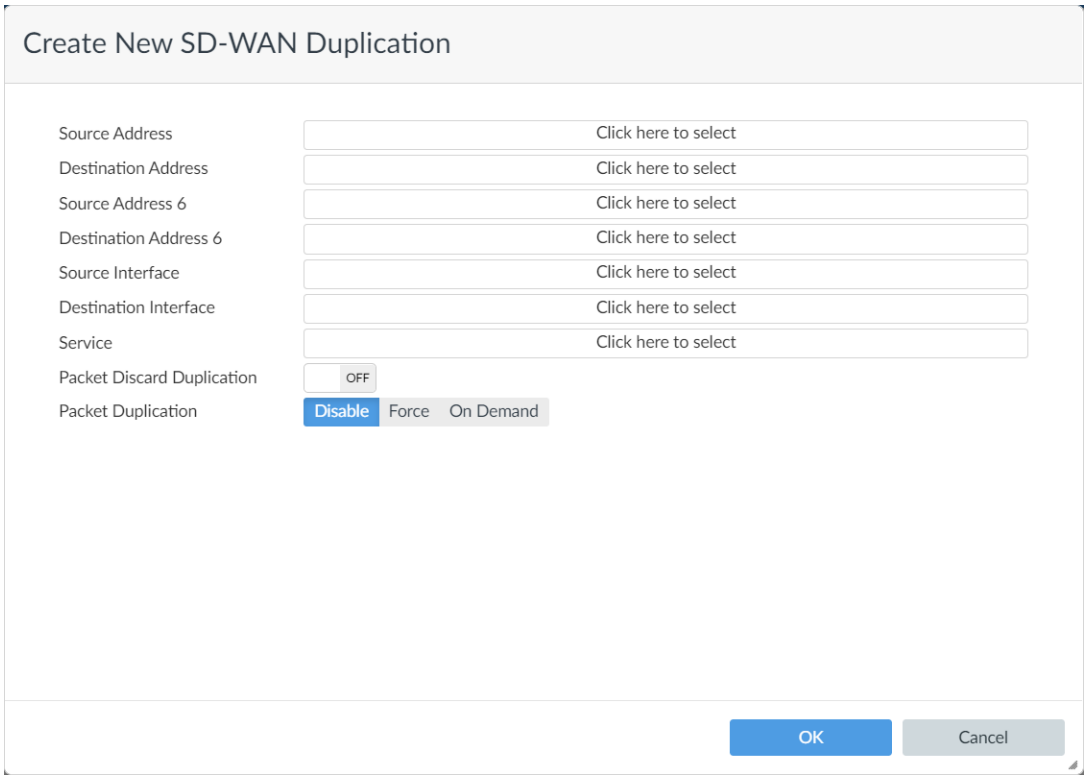
4. Set the options, and click *OK*.
   The neighbor is created.
5. Click *Apply*.
   The SD-WAN settings are saved.

Duplication

You can configure packet duplication for the SD-WAN network.

To configure packet duplication:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Network* > *SD-WAN*.
3. On the *SD-WAN* pane for the device, go to the *Duplication* section, and click *Create New*. The *Create New SD-WAN Duplication* pane opens.



4. Configure the options, and click *OK*.
5. Click *Apply* to save the SD-WAN settings.

Device DB - Network BGP

You can create Border Gateway Protocol (BGP) neighbors for FortiGates.

If BGP is hidden, see Choosing feature visibility for devices on page 195.

To create BGP neighbors:

1. Go to the device database. See Displaying the device database on page 194.
2. In the device database, go to *Network* > *BGP*. The *BGP* pane is displayed.

Device DB - CLI Configurations

In the device database, you can access the *CLI Configurations* menu to configure device settings that are normally configured via the CLI on the device. You can also use it to access settings that are not available in the FortiManager GUI.

To access the CLI Configurations menu:

1. Go to the device database. See Displaying the device database on page 194.
2. Display *CLI Configurations* in the menu:
   a. Click *Display Options*.
   The *Display Options* dialog box is displayed.
   b. Select *Customize*.
   c. Select the *CLI Configurations* checkbox, and click *OK*.
   The *CLI Configurations* menu is displayed.
3. Click *CLI Configurations*.



The options available in the menu will vary from device to device, depending on what feature set the device supports. The options will also vary depending on the device firmware version.

Device maintenance

This section includes the following procedures:

- Deleting a device on page 227
- Replacing a managed device on page 228

Deleting a device

Devices can be deleted in Device Manager. Deleting a device does not delete other management elements associated with it:

- If the device is a member of a group, the group will remain without the device in it (Device groups on page 147).
- If a template is assigned to the device, the template will remain with no device assignment (Provisioning Templates on page 273).
- If the device is an installation target for a policy package, the package will remain with that device removed from the installation targets (Policy package installation targets on page 422).
- If there is a policy in a policy package that only installs on the device that is deleted, the policy will remain but will not be installed on any devices (see Installing policies to specific devices on page 503).
- If there are VDOMs in other ADOMs, they will be deleted with the device (ADOM device modes on page 928).

To delete a device:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager* > *Device & Groups*.
3. In the toolbar, select *Table View* from the dropdown menu.
4. In the content pane, select a device and then click *Delete* in the toolbar, or right click on a device and select *Delete*.
5. Click *OK* in the confirmation dialog box to delete the device.

Replacing a managed device

The serial number is verified before each management connection. If you replace a device, you must manually change the serial number in the FortiManager system. You can only replace a device using another serial number of the same model.



You can only reinstall a device that has a *Retrieve* button under the *Revision History* tab.

Changing the serial number from the GUI

To swap a FortiGate device (standalone or HA cluster member):

1. Go to *Device & Groups* > *Managed FortiGate*.
2. Select a managed FortiGate device from the table, and click *More* > *Swap Device*.
   The Swap Device menu is displayed.

   When selecting a FortiGate cluster, all cluster members are displayed in the *Swap Device* menu.

3. Enter the FortiGate's *New Serial Number*, and specify the *Admin Name* and *Admin Password*, and click *OK*.
   The serial number must be of the same model as the device being replaced.
4. On the FortiGate *Central Management Settings* page, enter the FortiManager IP and click *OK*.
5. On FortiManager, the device serial number and configuration is pushed to the new device.



When replacing a managed FortiGate cluster member's license on FortiOS, the device is added as a new cluster member on FortiManager. The cluster member with the old license is still listed in the *Device Manager* on FortiManager.

Once you have confirmed that the cluster member with the updated license has been added to FortiManager, you can manually delete the downed cluster member with the old license from the device dashboard's HA widget.

View all managed devices from the CLI

To view all devices that are managed by your FortiManager, use the following command:

```
diagnose dvm device list
```

The output lists the number of managed devices, device type, OID, device serial number, VDOMs, HA status, IP address, device name, and the ADOM to which the device belongs.

Changing the serial number from the CLI

If the device serial number was entered incorrectly using the *Add Model Device* wizard, you can replace the serial number from the CLI only. Use the command:

```
execute device replace sn <device name> <serial number>
```

This command is also useful when performing an RMA replacement.

Managing FortiGate HA clusters

This topic includes the following information for managing devices using HA.

- Configuring model HA cluster members on page 229
- How FortiGate VDOM exceptions interact with FortiManager on page 230
- Firmware upgrades are prevented for FortiGate HA clusters in MVC mode on page 232
- FortiManager supports FortiGate auto-scale clusters on page 234



For information on adding offline model FortiGate HA clusters, see Adding a model FortiGate HA cluster on page 118.



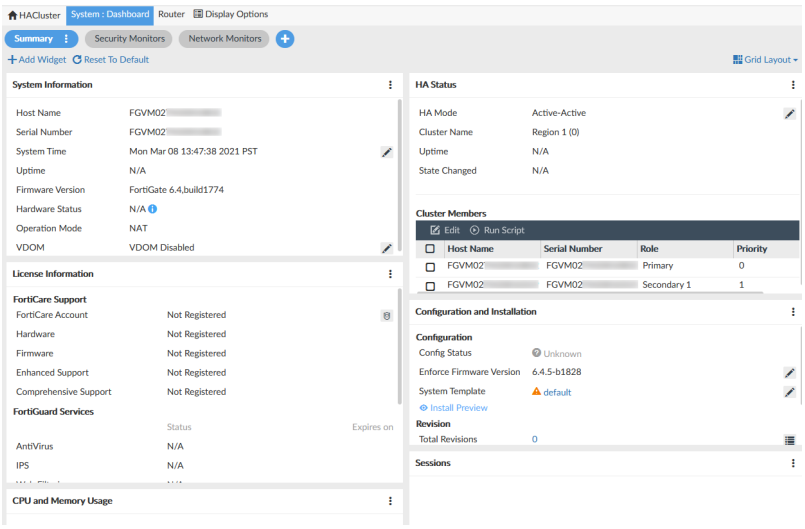
When FortiManager is managing a FortiGate HA cluster configured on Azure or AWS, you cannot use FortiManager to push device-level changes to the FortiGates, such as changes for the following commands: `system ha`, `system interface`, `system sdn-connector nic`, and `system sdn-connector route-table`. As a workaround, you can make the change on each FortiGate.

Configuring model HA cluster members

The *HA Status* widget in the in the system dashboard allows you to configure model HA cluster members. After the model HA device is created, its HA configuration can be modified.

To configure a model HA cluster member:

1. Go to *Device Manager* > *Device & Groups* > *Managed FortiGate*.
2. In the content pane, select the HA Cluster, and click *Edit*. The *System:Dashboard* is displayed.



3. In the *HA Status* widget, under *Cluster Members*, select a cluster device, and click *Edit*. The *Edit HA Member <cluster_name>* dialog is displayed.
4. Configure the cluster settings.

Host Name	Sets the hostname and password for each member in the cluster.
Priority (0-512)	Sets the priority for the cluster member. The cluster member with a higher number will be considered as the primary device of the HA cluster.
Management Interface Reservation	Enables a dedicated interface for individual cluster member management.
Session Pickup	Exposes the session-pick option from the GUI.
Session Pickup Connectionless	Exposes the connectionless sessions from the primary FortiGate.
Heartbeat Interface	Sets the heartbeat *Interface* and *Priority*.
Monitor Interface	Sets the monitor interface.

5. *Click OK.*

You cannot use FortiManager to configure high availability (HA) on real FortiGate devices. FortiManager learns about HA settings from managed FortiGate devices, but does not manage that part of the FortiGate configuration.

As a result the *HA* pane in the device database is read-only in *Device Manager*.

How FortiGate VDOM exceptions interact with FortiManager

In a typical FortiGate HA configuration, when a setting on the Primary FortiGate changes, those changes are automatically synchronized to the Secondary device.

In order to manually prevent certain settings from synchronizing between the Primary and Secondary devices in the HA cluster, administrators can configure VDOM exceptions. When a FortiGate's configuration is updated

during failover, settings specified as VDOM exceptions are not changed. FortiManager administrators can still make changes to VDOM exception objects directly through the device database on FortiManager.

FortiManager treats VDOM exceptions as read-only in the ADOM database. When FortiManager adds the HA cluster, VDOM exception objects will only be added to firewall policies if the FortiGate has the object created locally, otherwise the object is not created.

VDOM exceptions can be required when FortiGate HA cluster members are not in the same physical location, subnets, or availability zones in a cloud environment. For example, you need to prevent management interfaces that have unique VIPs from being synchronized between cluster devices.

See the FortiGate Administration Guide for a list of settings and resources that can be exempted from synchronization in an HA cluster.

Example: VDOM exception for VIP objects

In the following example, an administrator wants to centrally manage a FortiGate Active-Passive HA cluster (FortiGate-A and FortiGate-B) with unique VIP objects hosted on AWS using FortiManager.

VDOM exception example:

1. FortiGate-A and FortiGate-B are each configured with unique VIP objects.
2. The administrator configures a VDOM exception for the VIP objects on FortiGate-A.
   For example, the administrator sets the following command:
   ```
   config vdom exception
      edit 1
         set object firewall.vip
   ```
   The VDOM exception only needs to be configured on the device that will be Primary in the cluster. The Secondary device will automatically synchronize the VDOM exception settings when the HA cluster is formed.
3. The administrator forms an HA cluster where FortiGate-A is the Primary and FortiGate-B is the Secondary.
   - VIP objects configured on the FortiGate devices are not synchronized between the Primary and Secondary because of the VDOM exception.
   - See the FortiGate/FortiOS Administrator Guide for more information on forming HA clusters.
4. The FortiGate cluster is added to FortiManager for central management.
   - FortiManager retrieves the configuration of the FortiGate cluster, and the cluster is displayed as *Synchronized*.
   - The VDOM exception objects (VIP objects in this example) are not synchronized between the cluster devices. FortiManager imports the configuration from the current Primary (FortiGate-A).
   - See Adding a model FortiGate HA cluster on page 118 for more information on adding an FortiGate HA cluster to FortiManager.
5. After failover occurs, FortiGate-B becomes the new Primary, and FortiManager retrieves its configuration with auto-update.
   - FortiGate-B's VIP objects are not synchronized to the FortiManager databases and remain as local objects on the FortiGate.
   - In order to push any configuration changes to the new Primary (FortiGate-B), the administrator must first manually import its configuration. The VIP object from FortiGate-B will be updated in the device database, and the ADOM database will contain the VIP objects from FortiGate-A and FortiGate-B.

Additional Resources

- FortiOS AWS Administration Guide
- FortiOS Azure/Azure Stack Administration Guide
- FortiGate Administration Guide
- FortiGate CLI Reference

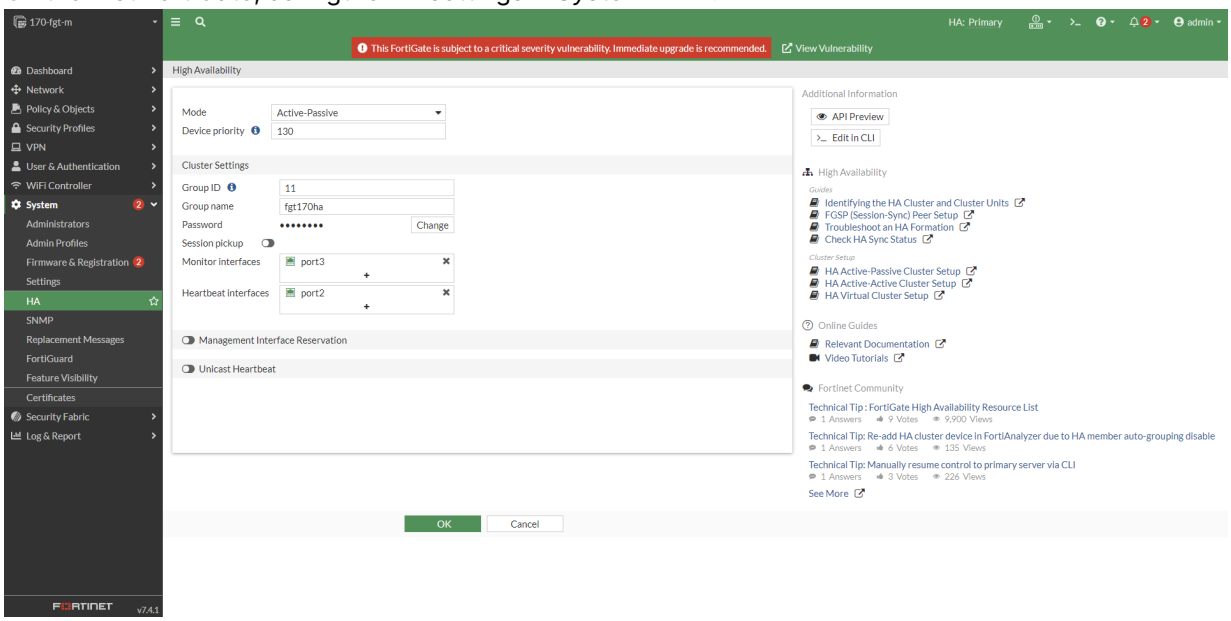
Firmware upgrades are prevented for FortiGate HA clusters in MVC mode

FortiManager detects FortiGate HA clusters operating in multi-version cluster (MVC) mode, provides a warning, and prevents the cluster firmware from being upgraded.

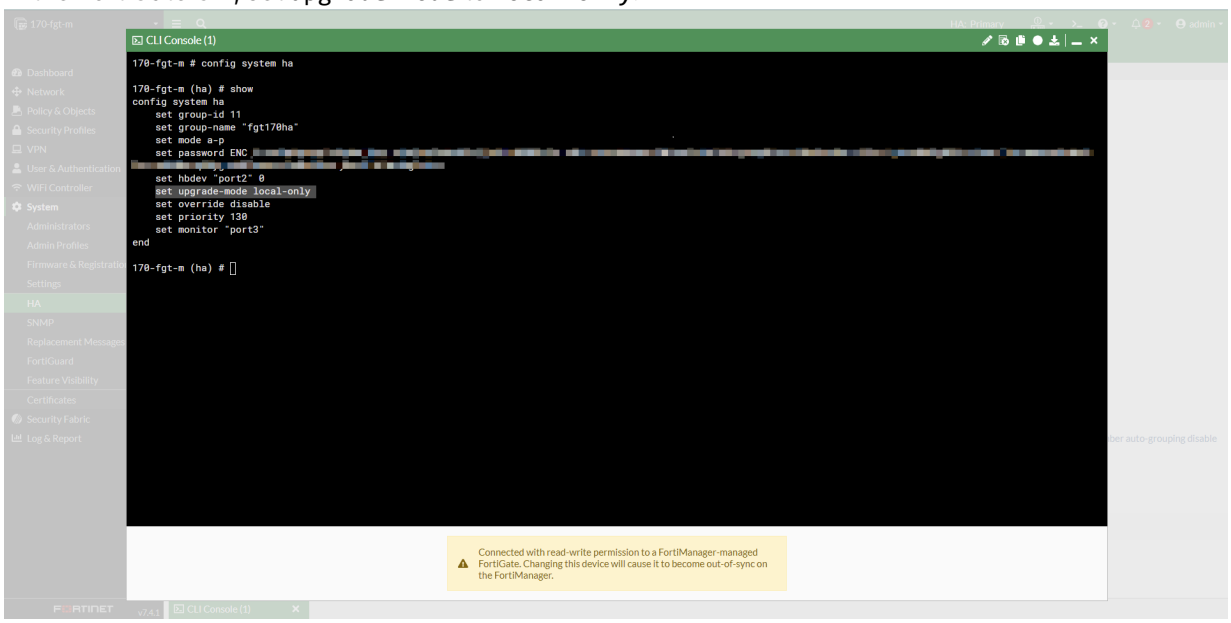
For more information on MVC mode, see the FortiGate Administration Guide.

Example

1. Configure the FortiGate HA cluster with MVC mode:
   a. On the first FortiGate, configure HA settings in *System* > *HA*.



b. In the FortiGate CLI, set `upgrade-mode` to `local-only`.

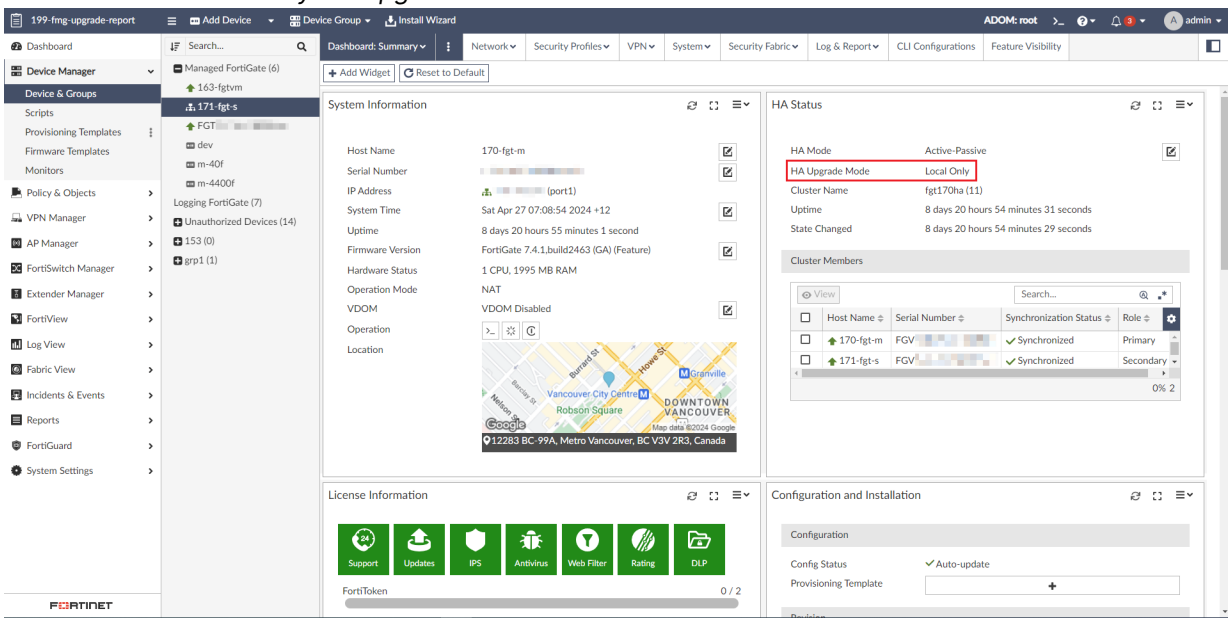


c. Repeat the steps above on the second FortiGate.

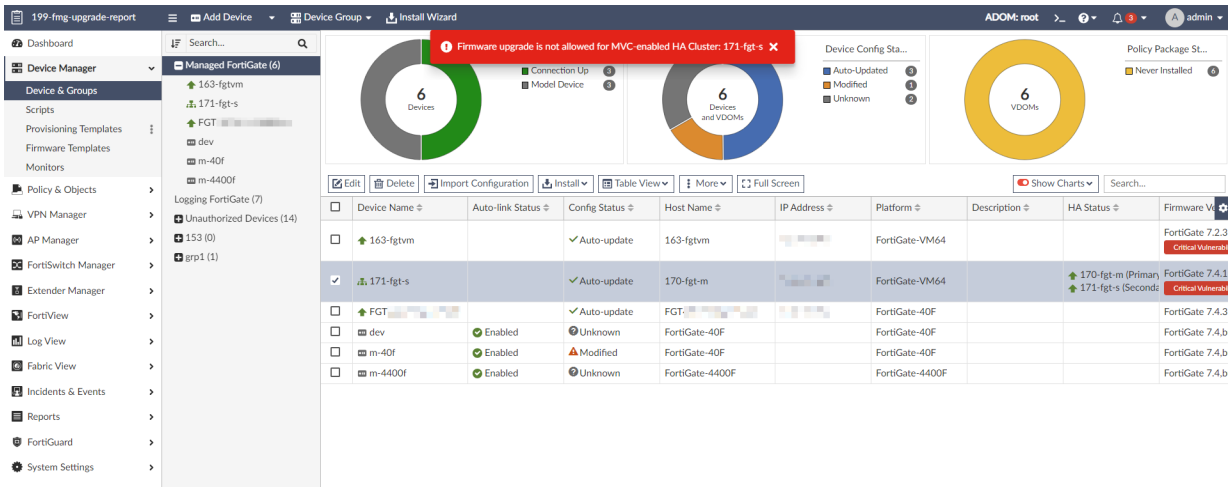
d. Go to *System* > *HA* and verify that the HA is formed and synchronized.

2. Attempt to upgrade the FortiGate cluster from FortiManager.

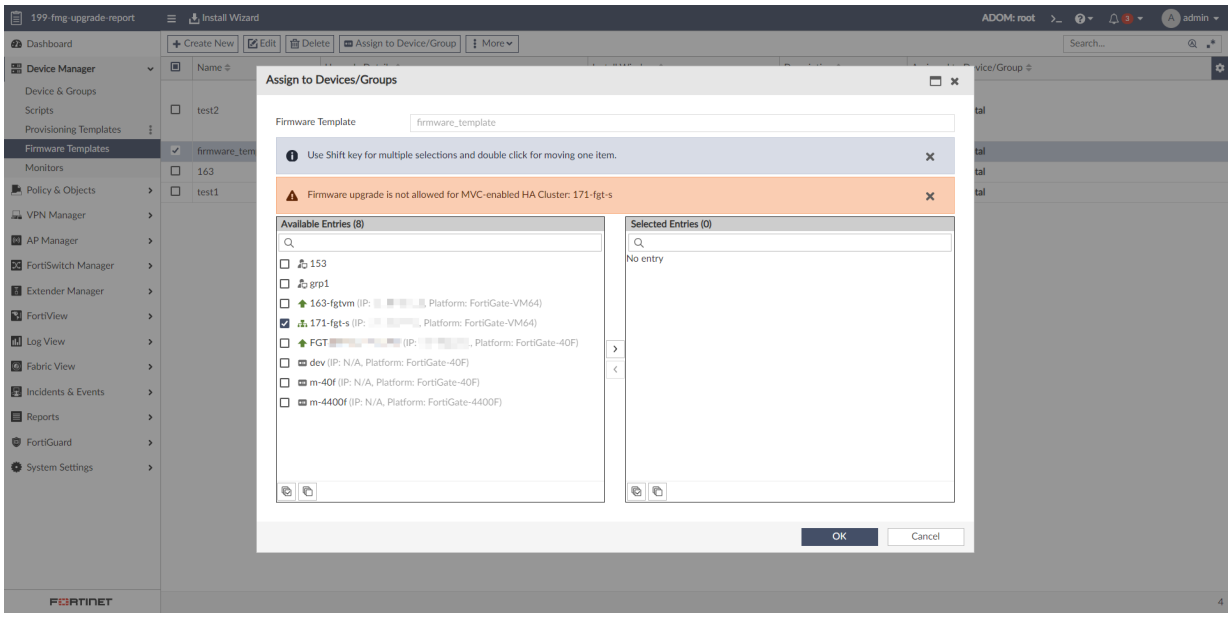
a. Go to *Device Manager* > *Device & Groups* > *Managed FortiGate* > *Dashboard: Summary*, and verify that the cluster is in *Local Only HA Upgrade Mode*.



b. Go to *Device Manager* > *Device & Groups* > *Managed FortiGate*, select the device and click *More* > *Firmware Upgrade* and try to perform a direct upgrade of the firmware. A warning message is displayed denying the firmware upgrade of the MVC enabled HA cluster.



c. Go to *Device Manager* > *Firmware Templates*, and try to assign the device to a firmware template. A warning message is displayed stating that firmware upgrades for MVC-enabled HA clusters is not allowed.



FortiManager supports FortiGate auto-scale clusters

FortiManager supports the public cloud functionality to scale-in or scale-out the number of FortiGate-VMs on-demand using auto-scaling. When an auto-scale event is triggered, the public cloud platform will launch a new FortiGate-VM and it will appear automatically on FortiManager as an authorized device in the *Device Manager*. When a scale-in event occurs, the device will automatically removed from FortiManager.

FortiManager cannot be used to manage the upgrade of Virtual Machine Scale Set (VMSS) FortiGates in Azure.

Example of how FortiManager manages auto-scale clusters

As an example, an administrator creates an auto-scale cluster on the public cloud with two FortiGate-VMs which includes a rule to trigger a scale-out event when the CPU or network utilization exceeds 70% capacity. The scale-out event increases the number of FortiGate-VMs in the cluster to three so that the additional traffic can be managed.

In the event of a scale-out, the newly added FortiGate device syncs with the Primary FortiGate in the cluster and fetches the FortiManager configuration. Once the deployment and sync is complete on the new FortiGate, the device is authorized and added to the existing cluster on the FortiManager.

A separate rule specifies that when the CPU or network utilization is less than 10%, a scale-in event occurs to reduce the number of FortiGate-VMs back to two. When the scale-in event occurs, the third FortiGate device is automatically removed from FortiManager.

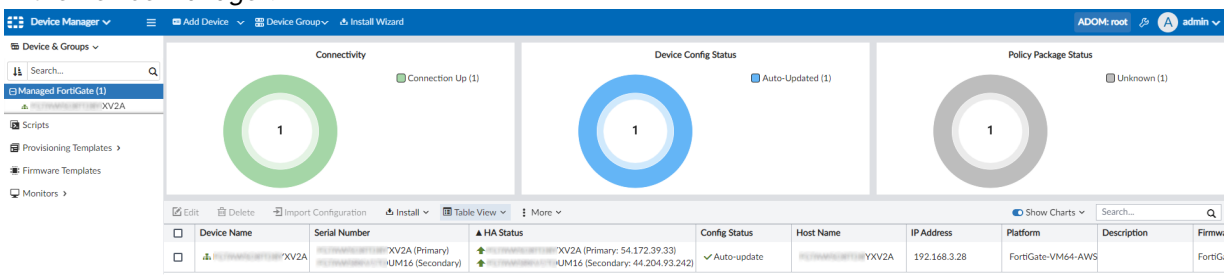
These changes are reflected on the FortiManager without any manual intervention required.



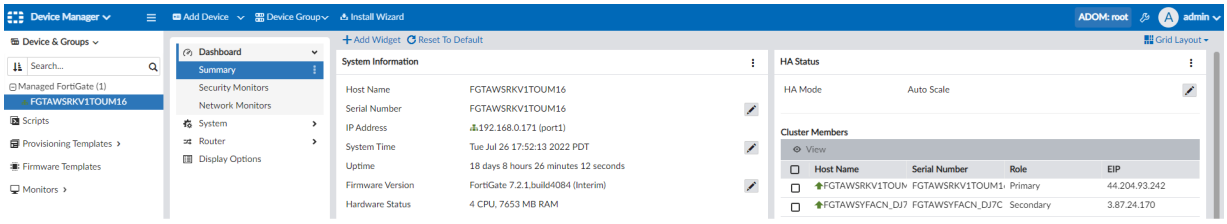
The amount of time required for FortiManager to add or remove FortiGate devices to or from the cluster depends upon the time it takes to deploy or terminate the FortiGate-VM on the cloud, and for the FortiGate clusters to resync.

To manage FortiGate auto-scale clusters on FortiManager:

1. Add the auto-scale cluster to FortiManager:
   - Add the FortiGate auto-scale cluster to FortiManager for the first time using the IP address of the Primary FortiGate. Once the configuration between the cluster members are in sync, the remaining devices are added to the FortiManager automatically.
   - Alternatively, you can configure the FortiManager Fabric Connector on the Primary FortiGate to add the cluster to FortiManager.
   - You can check the *Serial Number*, *Hostname*, *HA Status* and elastic IP of the FortiGate cluster devices in the *Device Manager*.

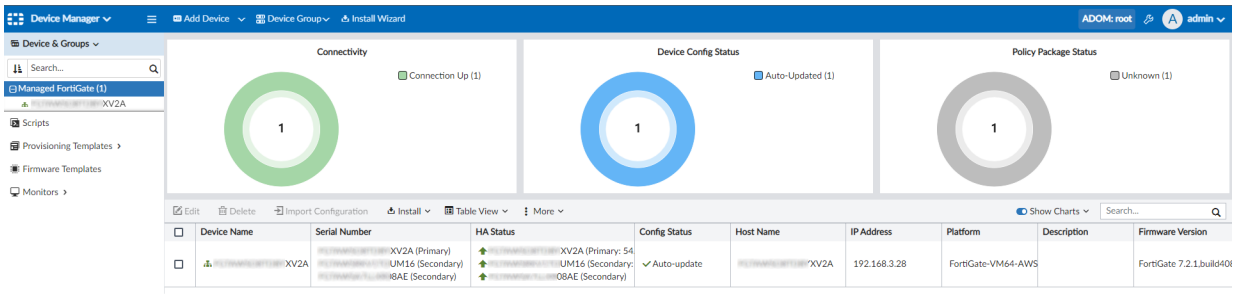


   - Administrators can check the HA mode (i.e. auto-scale) along with cluster members, roles, and the elastic IP in the device database.

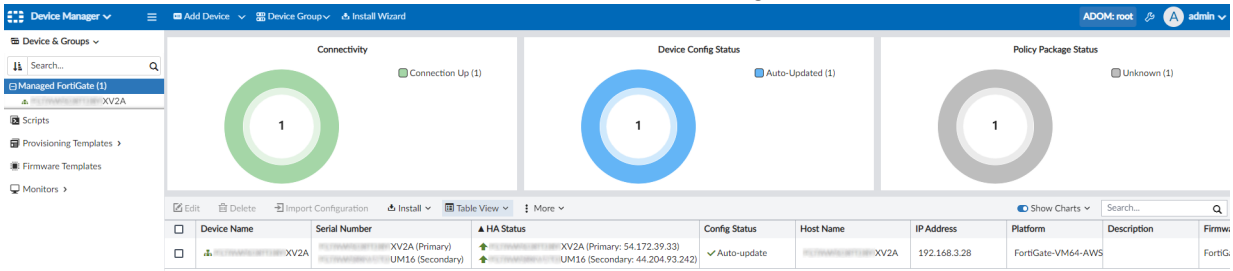


2. When a scale-out event occurs where the number of FortiGate devices in the cluster increases, once the newly added FortiGate becomes a part of the cluster and syncs its configuration with the cluster's Primary

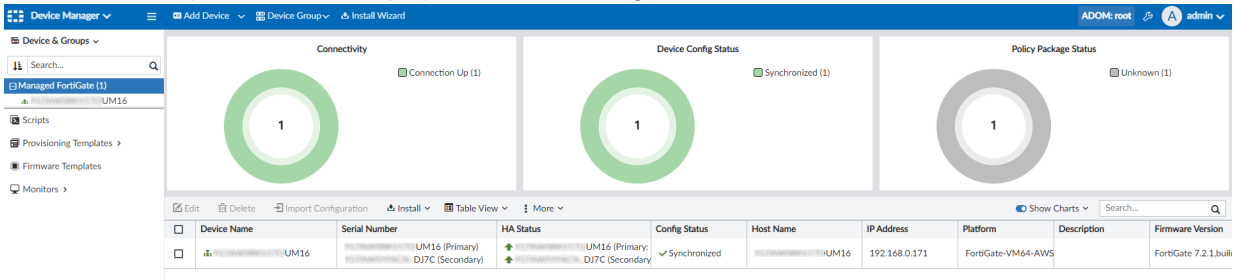
device, it is added to FortiManager.
On FortiManager, the device is automatically authorized and added to the existing cluster without manual intervention.



3. When a scale-in event occurs where the number of FortiGate devices in the cluster decreases, once the FortiGate is removed from the cluster on the cloud and the FGFM expires on the FortiManager, the FortiGate device will be removed from the cluster on FortiManager.



4. During any scale-in event, if the Primary FortiGate is removed from the cluster on the cloud, then FortiManager will be able to detect the change and will reflect the state of the new Primary and Secondary devices in the Device Manager.
In the example image below the Primary FortiGate failed and there was an auto-scale event to replace it. The new Primary FortiGate is displayed on FortiManager.



FortiManager supports FortiGate clusters with vSN

FortiManager supports FortiGate HA cluster contracts with virtual serial numbers (vSN). FortiManager can get the vSN contract from FDS server and provide update services to the cluster.

The FortiManager `diagnose dvm device list` command supports showing the FortiGate cluster vSN.

To view the vSN for a FortiGate cluster in the FortiManager CLI:

1. Enter the `diagnose dvm device list` command in the FortiManager CLI:

```
diagnose dvm device list
```

```
fmgfaz-managed  1932   FG40FITK******85 a-p     10.59.67.114    FortiGate-40F-3G4G  7-4
     6.00741 (regular)  7.0 MR2 (4911)  N/A
   |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: autoupdated; conn: up
HA cluster member: FG40FITK******85 (primary); conn: up; conf: in sync; logical-sn:
     FG40FIHA******07
HA cluster member: FG40FITK******86 (secondary 1); conn: up; conf: in sync
   |- vdom:[3]root flags:1 adom:7-4 pkg:[imported]FortiGate-40F-3G4G
```

Retrieving account level entitlements for FortiGate

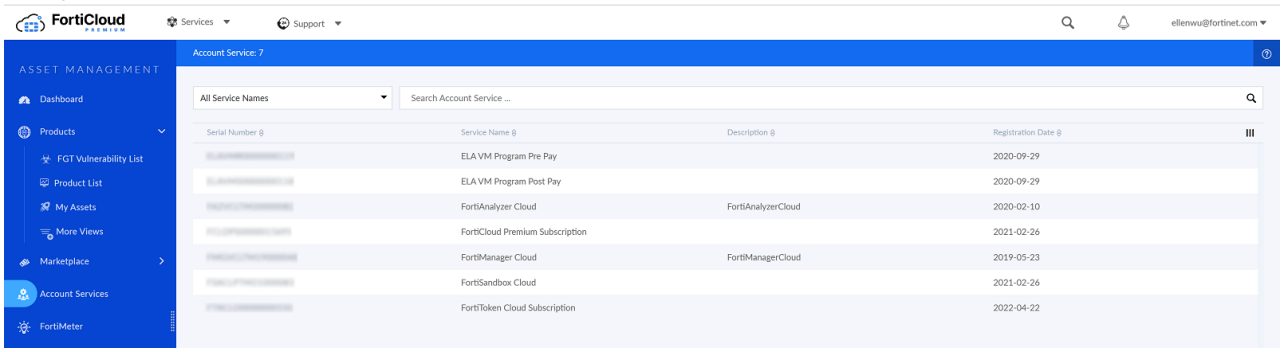
Managed FortiGate devices can retrieve their account level entitlements from FortiCloud directly through the FortiManager. This allows features controlled by account level entitlements, for example FortiSandbox Cloud sandboxing, to be enabled without requiring the FortiGate to connect to the internet. This feature requires that FortiManager has an internet connection.

Example - FortiSandbox Cloud entitlements

For example, when FortiGate has an entitlement for FortiSandbox Cloud, the FortiGate can retrieve that entitlement information directly from FortiManager and then allow the FortiSandbox Cloud settings to be enabled in the Sandbox Fabric Connector.

To retrieve FortiGate's FortiSandbox Cloud entitlement through FortiManager:

1. Verify that the FortiGate has an entitlement for FortiSandbox Cloud on FortiCloud.

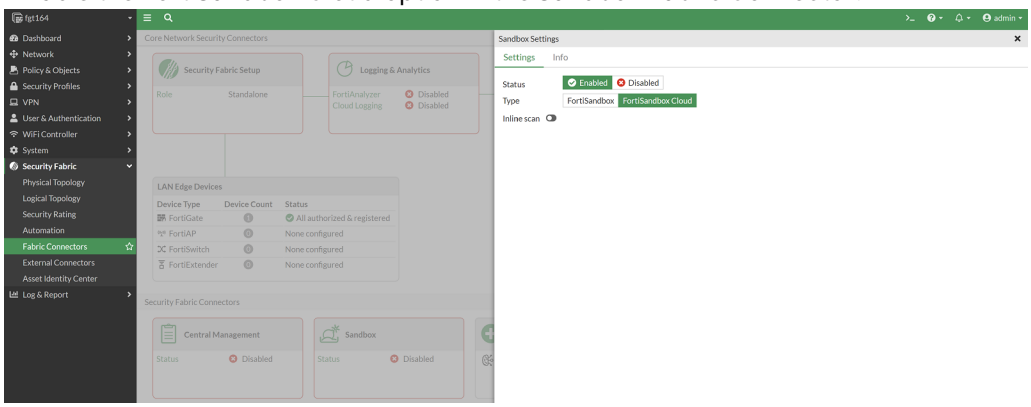


2. Configure the FortiGate to use FortiManager for update services.

```
config system central-management
   config server-list
      edit 1
         set server-type update rating
         set server-address {ipv4-address}
      next
   end
   set include-default-servers disable
end
```

The FortiGate retrieves the account level contract from FortiManager.

3. Enable the *FortiSandbox Cloud* option in the *Sandbox Fabric Connector*.



Remotely access a managed FortiGate

You can remotely connect to managed FortiGate devices through the FortiManager Device Manager.

To remotely access to the FOS GUI:

1. Go to *System Settings* > *Admin Profiles* and enable the *Remote GUI Access* option for an Admin Profile. *Remote GUI Access* is enabled for the *Super_User* profile by default. The setting is disabled for newly created profiles but can be manually enabled.
2. Log in as a user with Remote GUI Access permission.
3. Go to *Device Manager* > *Device & Groups*, right-click on a managed FortiGate, and the *Remote Access* option appears in the context menu.
4. Click *Remote Access*. You are redirected to the FortiGate's login page using the following URL: `<FMG IP>:<8082>`.
5. Enter your FortiGate login credentials to access the FortiGate.

To change the port used for remote access:

1. Go to *System Settings* > *Settings*.
2. Change the port number in the *Access Remote GUI via Port* setting. The default port used is `8082`.
3. Click *Apply*.



When configuring the port used for remote access, FortiManager reserved ports cannot be used. See the FortiManager Ports document for more information.

Scripts

FortiManager scripts enable you to create, execute, and view the results of scripts executed on FortiGate devices, policy packages, the ADOM database, global policy packages, or the device database. Scripts can also be filtered based on different device information, such as OS type and platform.

At least one FortiGate device must be configured in the FortiManager system before you can use scripts.



Additional configuration options and short-cuts are available using the right-click menu. Right-click the mouse on different navigation panes in the GUI page to access these options.



Any scripts that are run on the global database must use complete commands. For example, if the full command is `config system global`, do not use `conf sys glob`.

Scripts can be written in one of two formats:

- A sequence of FortiGate CLI commands, as you would type them at the command line. A comment line starts with the number sign (#). A comment line will not be executed.
- Tcl scripting commands to provide more functionality to your scripts including global variables and decision structures.

When writing your scripts, it is generally easier to write them in a context-sensitive editor, and then cut and paste them into the script editor on your FortiManager system. This can help avoid syntax errors and can reduce the amount of troubleshooting required for your scripts.

CLI scripts can be grouped together, allowing multiple scripts to be run on a target at the same time. See CLI script group on page 246 for information.

Go to *Device Manager* > *Scripts* to view the *Script* and *Script Group* entries.

For information about scripting commands, see the *FortiGate CLI reference*.



Before using scripts, ensure the `console-output` function has been set to `standard` in the FortiGate CLI. Otherwise, scripts and other output longer than a screen in length will not execute or display correctly.



When pushing a script from the FortiManager to the FortiGate with *workspace* enabled, you must save the changes in the *Policy & Objects* tab.



By design, the following FortiOS settings under `system central-management` cannot be modified using FortiManager database scripts or CLI templates: `fmg`, `fmg-source-ip`, `fmg-source-ip6`, `serial-number`, `type`, and `vdom`.

Attempting to commit changes to these fields will result in the following error: *not allowed to change*.

If you need to apply changes to these fields using FortiManager, a *CLI Script* can be used and run against the *Remote FortiGate Directly (via CLI)*.



After running a script with configuration changes directly on a FortiGate, you can import the configuration from the FortiGate to FortiManager in order to bring the script's changes into the FortiManager database.

Enabling scripts

You must enable scripts to make the *Scripts* option visible in the GUI.

To enable scripts:

1. Go to *System Settings* > *Settings*.
2. In the *Display Options on GUI* section, select *Show Scripts*. For more information, see Global administration settings on page 1051.
3. Select *Apply* to apply your changes.

Configuring scripts

To configure, import, export, or run scripts, go to *Device Manager* > *Scripts*, or *Policy & Objects* > *Object Configuration* > *Advanced* > *Scripts* if you are in the Global Database ADOM. The script list for your current ADOM displays.

The following information is displayed:

Name	The user-defined script name.
Type	The script type.
Target	The script target.
Comments	User defined comment for the script.
Last Modified	The date and time the script was last modified.

The following options are available in the toolbar, in the *More* menu, or in the right-click menu.

Run Script / Run	Run the selected script. See Run a script on page 241.
Schedule Script	Schedule when the selected script will run. See Schedule a script on page 245.

Create New / New	Create a new script. See Add a script on page 242.
Edit	Edit the selected script. See Edit a script on page 243.
Delete	Delete the selected script. See Delete a script on page 244.
Clone	Clone the selected script. See Clone a script on page 243.
Import CLI Script / Import	Import a script from your management computer. See Import a script on page 244.
Export	Export the selected script as a `.txt` file to your management computer. See Export a script on page 244.
Select All	Select all the scripts. This option is only available for Global Database scripts.
Search	Enter a search term in the search field to search the scripts.

Run a script

You can select to enable automatic script execution or create a recurring schedule for the script (see Schedule a script on page 245).

To run a script:

1. Go to *Device Manager* > *Scripts*.
2. Select a script then click *Run Script* in the toolbar, or right-click on a script and select *Run Script*.



Scripts can also be re-run from the script execution history by selecting the run button. See Script history on page 251 for information.

The *Run Script* dialog box will open. This dialog box will vary depending on the script target. You will either be able to select a device or devices, or a policy package.

3. Select a device group, devices, or a policy package.
4. Click *Run Now* to run the script.
The progress of the operation will be shown, providing information on its success or failure.



Scripts can also be run directly on a device using the right-click menu in *Device Manager* > *Device & Groups*.

To run a script on the Global Database ADOM:

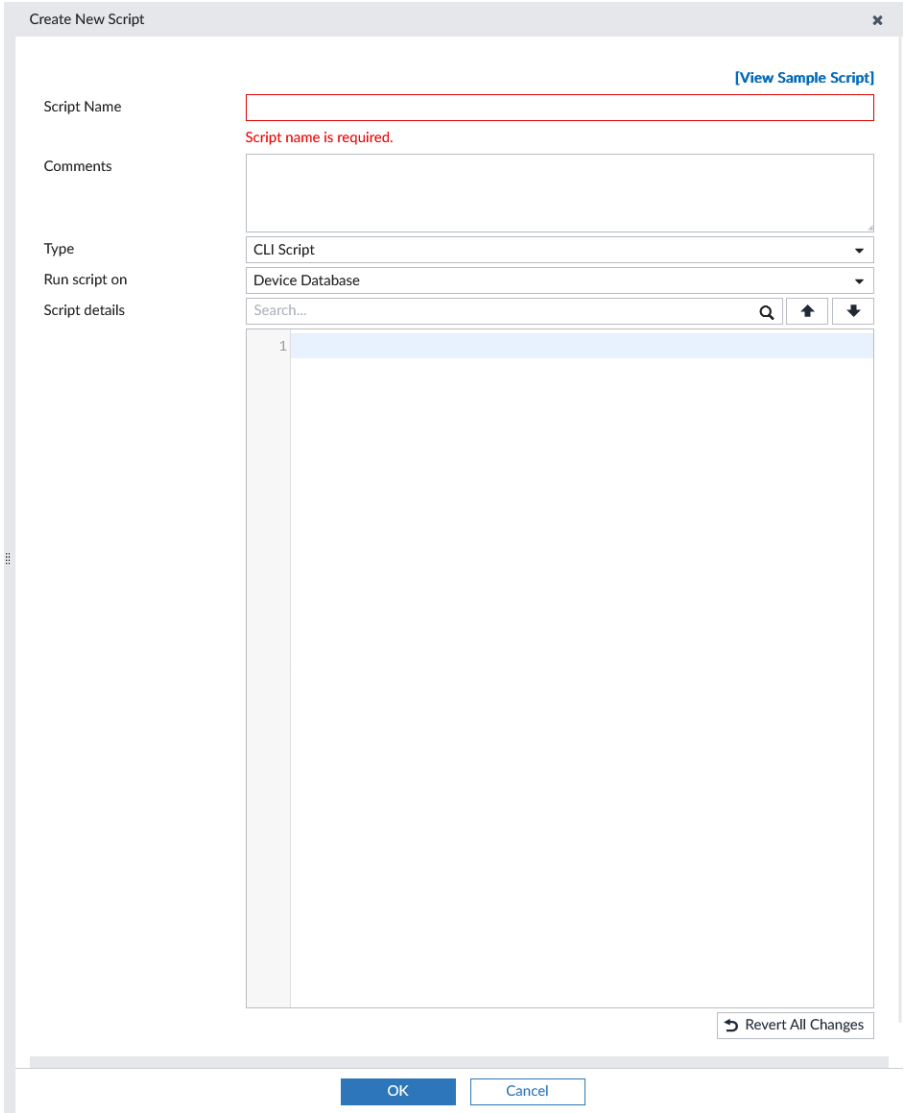
1. Ensure you are in the global database ADOM.
2. Go to *Policy & Objects* > *Scripts*. If it is not visible, enable it in the *Feature Visibility* (Feature visibility on page 413).
3. Select a script then click *Run Script* in the toolbar, or right-click on a script and select *Run Script*. The *Run Script* dialog box will open.
4. Select the policy package from the dropdown list.

5. Click *Run Script* to run the script.
   The progress of the operation will be shown, providing information on its success or failure.

Add a script

To add a script to an ADOM:

1. Go to *Device Manager* > *Scripts*, or *Policy & Objects* > *Scripts* for the Global Database ADOM.
2. Click *Create New* > *Script*, or right-click anywhere in the script list and select *New* from the menu. The *Create Script* dialog box.



3. Enter the required information, then select *OK* to create the new script.

Script Name	Type a unique name for the script.
View Sample Script	This option points to the FortiManager online help.

Comments	Optionally, type a comment for the script.
Type	Specify the type of script. This option is not available for Global Database ADOM scripts.
Run Script on	Select the script target. This settings will affect the options presented when you go to run a script. The options include: • *Device Database* • *Policy Package or ADOM Database* • *Remote FortiGate Directly (via CLI)* For Global Database ADOM scripts, this option is set to *Policy Package or ADOM Database* and cannot be changed.
Script Detail	Type the script itself, either manually using a keyboard, or by copying and pasting from another editor.
Advanced Device Filters	Select to adjust the advanced filters for the script. The options include: • *Platform* (select from the dropdown list) • *Build* • *Device* (select from the dropdown list) • *Host name* • *SN* These options are not available for Global Database ADOM scripts, or if *Run script on* is set to *Policy Package or ADOM Database*.

Edit a script

All of the same options are available when editing a script as when creating a new script, except the name of the script cannot be changed.

To edit a script, either double click on the name of the script, or right-click on the script name and select *Edit* from the menu. The *Edit Script* dialog box will open, allowing you to edit the script and its settings.

Clone a script

Cloning a script is useful when multiple scripts that are very similar.

To clone a script:

1. Go to *Device Manager* > *Scripts*, or *Policy & Objects* > *Object Configuration* > *Advanced* > *Scripts* if you are in the Global Database ADOM.
2. Right-click a script, and select *Clone*.
   The *Clone Script* pane opens, showing the exact same information as the original, except *copy_* is prepended to the script name.
3. Edit the script and its settings as needed then click *OK* to create the clone.

Delete a script

Scripts can be deleted from the script list as needed.

To delete a script or scripts:

1. Go to *Device Manager* > *Scripts*, or *Policy & Objects* > *Object Configuration* > *Advanced* > *Scripts* if you are in the Global Database ADOM.
2. Select the script to be deleted, or selected multiple scripts by holding down the Ctrl or Shift keys.
3. Right-click anywhere in the script list window, and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the script or scripts.

Export a script

CLI and Tcl scripts can be exported to text files on your local computer.



While FortiManager supports exporting both CLI and Tcl scripts, only CLI scripts can be re-imported using the FortiManager GUI. To import Tcl scripts, you must do so using the CLI. See Importing Tcl scripts on page 245.

To export a script:

1. Go to *Device Manager* > *Scripts*, or *Policy & Objects* > *Object Configuration* > *Advanced* > *Scripts* if you are in the Global Database ADOM.
2. Right-click a script, and select *Export Script*.
3. If prompted by your web browser, select a location to where save the file, or open the file without saving, then click *OK*.

Import a script

CLI scripts can be imported as text files from your local computer using the FortiManager GUI. See Importing CLI scripts on page 244

Tcl scripts can be imported using the FortiManager CLI using FTP or SCP. See Importing Tcl scripts on page 245

Importing CLI scripts

To import a CLI script:

1. Go to *Device Manager* > *Scripts*.
2. Select *Import CLI Script* from the toolbar. The *Import CLI Script* window opens.
3. Drag and drop the script file onto the dialog box, or click *Add Files* and locate the file to be imported on your local computer.

4. Click *Import* to import the script.
   If the script cannot be read, due to an incorrect file type or other issue, an error message will be displayed and the import process will be canceled.

To import a CLI script in the Global Database ADOM:

1. Go to *Policy & Objects* > *Object Configuration* > *Advanced* > *Scripts*.
2. Select *Import* from the toolbar. The *Import Script* dialog box opens.
3. Enter a name for the script and, optionally, comments, in the requisite fields.
4. Click *Browse...* and locate the file to be imported on your local computer.
5. Click *Import* to import the script.
   If the script cannot be read, due to an incorrect file type or other issue, an error message will be displayed and the import process will be canceled.

Importing Tcl scripts

Tcl scripts can only be imported using the FortiManager CLI. Importing a Tcl script as a text file using the *Import CLI Script* function in the FortiManager GUI will import the script as CLI and it will not function correctly.

To import a Tcl script using the FortiManager CLI, enter the following command to import the script by FTP/SCP:

```
execute fmscript import {scp | ftp} <server> <finename> <username> <password> <scriptname> <TCL>
      <target> <comment> <adom_name> <os_type> <os_version> <platform> <devicename> <buildno>
      <hostname> <serial number>
```

Schedule a script

Scripts and script groups can be scheduled to run at a specific time or on a recurring schedule. This option must be enabled in the CLI before it is available in the GUI.



Schedules cannot be used on scripts with the target *Policy Package or ADOM Database*.

To enable script scheduling:

1. From the toolbar, open the `CLI Console`, or connect to the FortiManager with terminal emulation software.
2. Enter the following CLI command:

```
config system admin setting
   set show_schedule_script enable
end
```

To schedule a script or script group:

1. Go to *Device Manager* > *Scripts*, or *Policy & Objects* > *Object Configuration* > *Advanced* > *Scripts* if you are in the Global Database ADOM.
2. Right-click on the script or group and select *Schedule Script*, or select a script or group then click *Schedule Script* or *More* > *Schedule Script* in the toolbar. The *Schedule Script* window opens.

3. Configure the following options, then click *OK* to create the schedule:

Devices	Select the devices that the script will be run on. If required, use the search field to find the devices in the list.
Enable Automatic execute after each device install	Select to enable automatic execution of the script or script group after each device install. If this is selected, no schedule can be created. This option is only available is the target is *Remote FortiGate Directly (via CLI)*.
Enable Schedule	Select to schedule when the script or groups runs. This option is only available is the target is *Remote FortiGate Directly (via CLI)*.
Recurring	Select how frequently the script or script group will run: • *One Time*- Set the date and time that script or group will run. • *Daily* - Set the time that the script or group will run everyday. • *Weekly* - Set the day of the week and the time of day that the script or group will run. • *Monthly* - Set the day of the month and the time of day that the script or group will run.

CLI script group

CLI scripts can be put into groups so that multiple scripts can be run on a target at the same time.

To manage script groups, go to to *Device Manager* > *Scripts* . *Script* and *Script Group* entries are displayed in the content pane.

The following information is displayed:

Name	The user-defined script group name.
Type	The script type, for example *CLI Script*.
Target	The script group target.
Comments	User defined comment for the group.
Members	The scripts that are included in the script group.
Last Modified	The date and time the group was last modified.

The following options are available in the toolbar, or right-click menu.

Create New	Create a new script group.
Edit	Edit the selected group.
Delete	Delete the selected group or groups.
Run Script	Run the selected script group.

	If the target is *Device Database* or *Remote FortiGate Directly (via CLI)*, select the device or devices to run the scripts in the group on, then click *Run Now*. If the target is *Policy Package or ADOM Database*, select the policy package from the drop-down list, then click *Run Now*.
Search	Enter a search term in the search field to search the script groups.

To create a new CLI script group:

1. Go to *Device Manager > Scripts* .
2. Click *Create New > Script Group* in the toolbar. The *Create New CLI Script Group(s)* pane opens.
3. Configure the following settings, then click *OK* to create the CLI script group.:

Script Group Name	Enter a name for the script group.
Comments	Optionally, type a comment for the script group.
Type	CLI Script. This field is read-only.
Run Script on	Select the script target. This settings will affect the options presented when you go to run a script. The options include: • *Device Database* • *Policy Package or ADOM Database* • *Remote FortiGate Directly (via CLI)*
Members	Use the directional arrows to move available scripts to member scripts.

Script syntax

Most script syntax is the same as that used by FortiOS. For information see the *FortiOS CLI Reference*, available in the Fortinet Document Library.

Some special syntax is required by the FortiManager to run CLI scripts on devices.

Syntax applicable for address and address6

```
config firewall address
   edit xxxx

      ...regular FOS command here...

   config dynamic_mapping
      edit "<dev_name>"-"<vdom_name>"
         set subnet x.x.x.x x.x.x.x
      next
   end
```

Syntax applicable for ippool and ippool6

```
config firewall ippool
   edit xxxx
```

```
      ...regular FOS command here...

   config dynamic_mapping
      edit "<dev_name>"-"<vdom_name>"
         set startip x.x.x.x
         set endip x.x.x.x
      next
   end
```

Syntax applicable for vip, vip6, vip46, and vip64

```
config firewall vip
   edit xxxx

      ...regular FOS command here...

   config dynamic_mapping
      edit "<dev_name>"-"<vdom_name>"
         set extintf "any"
         set extip x.x.x.x-x.x.x.x
         set mappedip x.x.x.x-x.x.x.x
         set arp-reply enable|disable
      next
   end
```

Syntax applicable for dynamic zone

```
config dynamic interface
   edit xxxx
      set single-intf disable
      set default-mapping enable|disable
      set defmap-intf xxxx
      config dynamic_mapping
         edit "<dev_name>"-"<vdom_name>"
            set local-intf xxxx
            set intrazone-deny enable|disable
         next
      end
   next
end
```

Syntax applicable for dynamic interface

```
config dynamic interface
   edit xxxx
      set single-intf enable
      set default-mapping enable|disable
      set defmap-intf xxxx
      config dynamic_mapping
         edit "<dev_name>"-"<vdom_name>"
            set local-intf xxxx
            set intrazone-deny enable|disable
         next
      end
   next
end
```

Syntax applicable for dynamic multicast interface

```
config dynamic multicast interface
   edit xxx
      set description xxx
      config dynamic_mapping
         edit "fgtname"-"vdom"
            set local-intf xxx
         next
      end
   next
end
```

Syntax applicable for local certificate (dynamic mapping)

```
config dynamic certificate local
   edit xxxx
      config dynamic_mapping
         edit "<dev_name>"-"global"
            set local-cert xxxx
         next
      end
```

Syntax applicable for vpn tunnel

```
config dynamic vpntunnel
   edit xxxx
      config dynamic_mapping
         edit "<dev_name>"-"<vdom_name>"
            set local-ipsec "<tunnel_name>"
         next
      end
```

Syntax applicable for vpn console table

```
config vpnmgr vpntable
   edit xxxx
      set topology star|meshed|dial
      set psk-auto-generate enable|disable
      set psksecret xxxx
      set ike1proposal 3des-sha1 3des-md5 ...
      set ike1dhgroup XXXX
      set ike1keylifesec 28800
      set ike1mode aggressive|main
      set ike1dpd enable|disable
      set ike1nattraversal enable|disable
      set ike1natkeepalive 10
      set ike2proposal 3des-sha1 3des-md5
      set ike2dhgroup 5
      set ike2keylifetype seconds|kbyte|both
      set ike2keylifesec 1800
      set ike2keylifekbs 5120
      set ike2keepalive enable|disable
      set replay enable|disable
      set pfs enable|disable
      set ike2autonego enable|disable
```

```
      set fcc-enforcement enable|disable
      set localid-type auto|fqdn|user-fqdn|keyid|addressasn1dn
      set authmethod psk|signature
      set inter-vdom enable|disable
      set certificate XXXX
   next
end
```

Syntax applicable for vpn console node

```
config vpnmgr node
   edit "1"
      set vpntable "<table_name>"
      set role hub|spoke
      set iface xxxx
      set hub_iface xxxx
      set automatic_routing enable|disable
      set extgw_p2_per_net enable|disable
      set banner xxxx
      set route-overlap use-old|use-new|allow
      set dns-mode manual|auto
      set domain xxxx
      set local-gw x.x.x.x
      set unity-support enable|disable
      set xauthtype disable|client|pap|chap|auto
      set authusr xxxx
      set authpasswd xxxx
      set authusrgrp xxxx
      set public-ip x.x.x.x
      config protected_subnet
         edit 1
            set addr xxxx xxxx ...
         next
      end
```

Syntax applicable for setting installation target on policy package

```
config firewall policy
   edit x

      ...regular policy command here...

      set _scope "<dev_name>"-"<vdom_name>"
   next
end
```

Syntax applicable for global policy

```
config global header policy

   ...regular policy command here...

end

config global footer policy
```

```
    ...regular policy command here...
end
```

Script history

The execution history of scripts run on specific devices can be viewed from a device's dashboard. The script log can be viewed in the Task Monitor. The script execution history table also allows for viewing the script history, and re-running the script.

To view the script execution history:

1. Go to *Device Manager* > *Device & Groups*.
2. In the tree menu, select the device group, for example, *Managed Devices*. The list of devices display in the content pane and in the bottom tree menu.
3. In the bottom tree menu, select the device whose script history you want to view. The *System: Dashboard* for the device displays in the content pane.
4. In the *Configuration and Installation Status* widget, select *View History* in the *Script Status* field to open the *Script Execution History* pane.
5. To view the script history for a specific script, select the *Browse* icon in the far right column of the table to open the *Script History* dialog box.
6. To re-run a script, select the Run script now icon in the far right column of the table. The script is re-run.
   See Run a script on page 241.
7. Select *Return* to return to the device dashboard.

To view a script log:

1. Go to *System Settings* > *Task Monitor*.
2. Locate the script execution task whose log you need to view, and expand the task.
3. Select the *History* icon to open the script log window.
   For more information, see Task Monitor on page 963.

Script samples

This section helps familiarize you with FortiManager scripts, provides some script samples, and provides some troubleshooting tips.

The scripts presented in this section are in an easy to read format that includes:

- the purpose or title of the script
- the script itself
- the output from the script (blank lines are removed from some output)
- any variations that may be useful
- which versions of FortiOS this script will execute on



Do not include `\r` in your scripts as this will cause the script to not process properly.

Script samples includes:

- CLI scripts
- Tcl scripts

CLI scripts

CLI scripts include only FortiOS CLI commands as they are entered at the command line prompt on a FortiGate device. CLI scripts do not include Tool Command Language (Tcl) commands, and the first line of the script is not "#!" as it is for Tcl scripts.

CLI scripts are useful for specific tasks such as configuring a routing table, adding new firewall policies, or getting system information. These example tasks easily apply to any or all FortiGate devices connected to the FortiManager system.

However, the more complex a CLI script becomes the less it can be used with all FortiGate devices - it quickly becomes tied to one particular device or configuration. One example of this is any script that includes the specific IP address of a FortiGate device's interfaces cannot be executed on a different FortiGate device.

Samples of CLI scripts have been included to help get you started writing your own scripts for your network administration tasks. See CLI script examples on page 252.

Error messages will help you determine the causes of any CLI scripting problems, and fix them. See Error Messages on page 256.

The troubleshooting tips section provides some suggestions on how to quickly locate and fix problems in your CLI scripts. See Troubleshooting Tips on page 257.

CLI script examples

There are two types of CLI scripts. The first type is getting information from your FortiGate device. The second type is changing information on your FortiGate device.

- Scripts for getting information on page 252
- Scripts for device configuration on page 255

Scripts for getting information

Getting information remotely is a main function of FortiManager, and CLI scripts allow you to access any information on your FortiGate devices. Getting information typically involves only one line of script as the following scripts show.

View information for port1

Script	`show system interface port1`

Output	`config system interface`
	`edit "port1"`
	`set vdom "root"`
	`set ip 172.20.120.148 255.255.255.0`
	`set allowaccess ping https ssh`
	`set type physical`
	`next`
	`end`

Variations	Remove the interface name to see a list that includes all the interfaces on the FortiGate device including virtual interfaces such as VLANs.
Notes	This script does not work when run on a policy package.

	If the preceding script is to be run on the *FortiGate Directly (via CLI)* or run on the device database for a FortiGate that has VDOMs enabled, the script will have be modified to the following:
	`config global`
	`show system interface port1`
	`end`

	Since running on device database does not yield any useful information, the script should be run on the FortiGate directly (via CLI).
	Example log of script run against the device database:
	`------- Executing time: 2013-10-15 13:27:32 ------`
	`Starting log (Run on database)`
	`config global`
	`end`
	`Running script on DB success`
	`------- The end of log ----------`
	Example log of script run on *FortiGate Directly (via CLI)*:
	`------- Executing time: 2013-10-15 13:52:02 ------`
	`Starting log (Run on device)`
	`FortiGate-VM64 $ config global`
	`FortiGate-VM64 (global) $ show system interface port1`
	`config system interface`
	`edit "port1"`
	`set vdom "root"`
	`set ip 10.2.66.181 255.255.0.0`
	`set allowaccess ping https ssh snmp http fgfm auto-ipsec radius-acct probe-response capwap`
	`set type physical`
	`set snmp-index 1`
	`next`
	`end`
	`FortiGate-VM64 (global) $ end`
	`------- The end of log ----------`

View entries in the static routing table

Script	`show route static`

Output	`config router static`
	`edit 1`
	`set device "port1"`

```
      set gateway 172.20.120.2
   next
   edit 2
      set device "port2"
      set distance 7
      set dst 172.20.120.0 255.255.255.0
      set gateway 172.20.120.2
   next
end
```

Notes

If VDOMs are enabled for the FortiGate, the script must be re-written as follows and run on the *FortiGate Directly (via CLI)*:

```
config vdom
   edit root
      show route static
   next
end
```

Example log of script run on *FortiGate Directly (via CLI)*:

```
------- Executing time: 2013-10-15 14:24:10 ------
Starting log (Run on device)
FortiGate-VM64 $ config vdom
FortiGate-VM64 (vdom) $ edit root
current vf=root:0
FortiGate-VM64 (root) $ show route static
config router static
   edit 1
      set device "port1"
      set gateway 10.2.0.250
   next
end
FortiGate-VM64 (root) $ next
FortiGate-VM64 (vdom) $ end
------- The end of log ----------
```

View information about all configured FDN servers on the device

Script

```
config global
   diag debug rating
end
```

Output

View the log of script running on device: FortiGate-VM64

```
------- Executing time: 2013-10-15 14:32:15 ------
Starting log (Run on device)
FortiGate-VM64 $ config global
FortiGate-VM64 (global) $ diagnose debug rating
Locale : english
License : Contract
Expiration : Thu Jan 3 17:00:00 2030
-=- Server List (Tue Oct 15 14:32:49 2013) -=-
IP Weight RTT Flags TZ Packets Curr Lost Total Lost
192.168.100.206 35 2 DIF -8 4068 72 305
192.168.100.188 36 2 F -8 4052 72 308
FortiGate-VM64 (global) $ end
------- The end of log ----------
```

Variations	Output for this script will vary based on the state of the FortiGate device. The preceding output is for a FortiGate device that has never been authorized.
	For an authorized FortiGate device without a valid license, the output would be similar to:
	`Locale : english`
	`License : Unknown`
	`Expiration : N/A`
	`Hostname : guard.fortinet.net`
	
	`-=- Server List (Tue Oct 3 09:34:46 2006) -=-`
	
	`IP Weight Round-time TZ Packets Curr Lost Total Lost`
	`** None **`

Scripts for device configuration

Setting FortiGate device information with CLI scripts gives you access to more settings and allows for more granular control than you may have in the *Device Manager*. CLI commands also allow access to more advanced options that are not available in the FortiGate GUI. Scripts that set information require more lines.



Any scripts that you will be running on the global database must include the full CLI commands and not use short forms for the commands. Short form commands will not run on the global database.

Create a new admin profile allowing *read-only* access to policy related areas

Script	`config global`
	`  config system accprofile`
	`  edit "policy_admin"`
	`  set fwgrp read`
	`  set loggrp read`
	`  set sysgrp read`
	`  next`
	`  end`
	`end`

Output	View the log of script running on device: FortiGate-VM64:
	`------- Executing time: 2013-10-16 13:39:35 ------`
	`Starting log (Run on device)`
	`FortiGate-VM64 $ config global`
	`FortiGate-VM64 (global) $ config system accprofile`
	`FortiGate-VM64 (accprofile) $ edit "prof_admin"`
	`FortiGate-VM64 (prof_admin) $ set fwgrp read`
	`FortiGate-VM64 (prof_admin) $ set loggrp read`
	`FortiGate-VM64 (prof_admin) $ set sysgrp read`
	`FortiGate-VM64 (prof_admin) $ next`
	`FortiGate-VM64 (accprofile) $ end`
	`FortiGate-VM64 (global) $ end`
	`------- The end of log ----------`

Variations	This profile is read-only to allow a policy administrator to monitor this device's configuration and traffic.

	Variations may include enabling other areas as read-only or write permissions based on that account type's needs.

Configure a firewall policy in the global database

You can run a CLI script in the FortiManager Global Database in addition to running it on a FortiGate unit directly. Compare the following sample scripts:

Running a CLI script on a FortiGate unit	`config vdom`
	`edit "root"`
	`config firewall policy`
	`edit 10`
	`set srcintf "port5"`
	`set dstintf "port6"`
	`set srcaddr "all"`
	`set dstaddr "all"`
	`set status disable`
	`set schedule "always"`
	`set service "ALL"`
	`set logtraffic disable`
	`next`
	`end`

Running a CLI script on the Global Database	`config global footer policy`
	`edit 10`
	`set srcintf "any"`
	`set dstintf "any"`
	`set srcaddr "gall"`
	`set dstaddr "gall"`
	`set status disable`
	`set schedule "galways"`
	`set service "gALL"`
	`set logtraffic disable`
	`next`
	`end`

Variations	The command `config global footer policy` can be replaced with `config global header policy` to create a header policy in the Global Database.

Error Messages

Most error messages you will see are regular FortiGate CLI error messages. If you are familiar with the CLI you will likely recognize them.

Other error messages indicate your script encountered problems while executing, such as:

- `command parse error`: It was not possible to parse this line of your script into a valid FortiGate CLI command. Common causes for this are misspelled keywords or an incorrect command format.
- `unknown action`: Generally this message indicates the previous line of the script was not executed, especially if the previous line accesses an object such as "config router static".
- `Device XXX failed-1`: This usually means there is a problem with the end of the script. XXX is the name of the FortiGate unit the script is to be executed on. If a script has no end statement or that line has an error in

it you may see this error message. You may also see this message if the FortiGate unit has not been synchronized by deploying its current configuration.

Troubleshooting Tips

Here are some troubleshooting tips to help locate and fix problems you may experience with your scripts.

- Check the script output. Generally the error messages displayed here will help you locate and fix the problem.
- See the *FortiGate CLI Reference* for more information on all CLI commands.
- There is a limit to the number of scripts allowed on the FortiManager unit. Try removing an old script before trying to save your current one.
- As mentioned at the start of this chapter, ensure the `console more` command is disabled on the FortiGate devices where scripts execute. Otherwise a condition may occur where both the FortiGate device and the FortiManager system are waiting for each other to respond until they timeout.
- There should be no punctuation at the start or end of the lines.
- Only whitespace is allowed on the same line as the command. This is useful in lining up `end` and `next` commands for quick and easy debugging of the script.
- Keep your scripts short. They are easier to troubleshoot and it gives you more flexibility. You can easily execute a number of scripts after each other.
- Use full command names. For example instead of “set host test” use “set hostname test”. This is required for any scripts that are to be run on the global database.
- Use the number sign (#) to comment out a line you suspect contains an error.

Tcl scripts

Tcl is a dynamic scripting language that extends the functionality of CLI scripting. In FortiManager Tcl scripts, the first line of the script is “#!” as it is for standard Tcl scripts.



TCL Scripts do not run through the FGFM tunnel like CLI Scripts do. TCL Scripts use SSH to tunnel through FGFM and they require SSH authentication to do so. If FortiManager does not use the correct administrative credentials in Device Manager, the TCL script will fail. CLI scripts use the FGFM tunnel and the FGFM tunnel is authenticated using the FortiManager and FortiGate serial numbers.



Do not include the exit command that normally ends Tcl scripts; it will prevent the script from running.

This guide assumes you are familiar with the Tcl language and regular expressions, and instead focuses on how to use CLI commands in your Tcl scripts. Where you require more information about Tcl commands than this guide contains, please refer to resources such as the Tcl newsgroup, Tcl reference books, and the official Tcl website at https://www.tcl.tk.

Tcl scripts can do more than just get and set information. The benefits of Tcl come from:

- variables to store information,
- loops to repeats commands that are slightly different each time
- decisions to compare information from the device

The sample scripts in this section will contain procedures that you can combine to use your scripts. The samples will each focus on one of four areas:

- Tcl variables
- Tcl loops
- Tcl decisions
- Tcl file IO

To enable Tcl scripting, use the following CLI commands:

```
config system admin setting
   set show_tcl_script enable
end
```

Limitations of FortiManager Tcl

- FortiManager Tcl executes in a controlled environment. You do not have to know the location of the Tcl interpreter or environment variables to execute your scripts. This also means some of the commands normally found in Tcl are not used in FortiManager Tcl.
- Depending on the CLI commands you use in your Tcl scripts, you may not be able to run some scripts on some versions of FortiOS as CLI commands change periodically.
- Metadata variables are not supported in Tcl scripts.



Before testing a new script on a FortiGate device, you should backup that device's configuration and data to ensure it is not lost if the script does not work as expected.

Tcl variables

Variables allow you to store information from the FortiGate device, and use it later in the script. Arrays allow you to easily manage information by storing multiple pieces of data under a variable name. The next script uses an array to store the FortiGate system information.

Example: Save system status information in an array

Script

```
#!
proc get_sys_status aname {
   upvar $aname a
puts [exec "#This is an example Tcl script to get the system status of the FortiGate\n" "# " 15 ]
   set input [exec "get system status\n" "# " 15 ]
# puts $input
```

Script

```
   set linelist [split $input \n]
# puts $linelist
foreach line $linelist {
   if {![regexp {([^:]+):(.*)} $line dummy key value]} continue
      switch -regexp -- $key {
      Version {
      regexp {FortiGate-([^ ]+) ([^,]+),build([\d]+),.*} $value dummy a(platform) a(version) a
            (build)
   }
Serial-Number {
   set a(serial-number) [string trim $value]
}
   Hostname {
      set a(hostname) [string trim $value]
      } }
   }
}
get_sys_status status
puts "This machine is a $status(platform) platform."
puts "It is running version $status(version) of FortiOS."
puts "The firmware is build# $status(build)."
puts "S/N: $status(serial-number)"
puts "This machine is called $status(hostname)"
```

Output

```
Starting log (Run on device)
#This is an example Tcl script to get the system status of the FortiGate
Branch_Office_02 #This machine is a VM64-KVM platform.
It is running version v7.4.0 of FortiOS.
The firmware is build# ****
S/N: FGVM02TM2*******
This machine is called Branch_Office_02


----------------End of Log-------------------------
```

Variations:

Once the information is in the variable array, you can use it as part of commands you send to the FortiGate device or to make decisions based on the information. For example:

```
if {$status(version) == 7.4.7} {
# follow the version 7.4.7 commands
} elseif {$status(version) == 7.4.6} {
# follow the version 7.4.6 commands
}
```

This script introduces the concept of executing CLI commands within Tcl scripts using the following method:

```
set input [exec "get system status\n" "# "]
```

This command executes the CLI command "`get system status`" and passes the result into the variable called `input`. Without the "\n" at the end of the CLI command, the CLI command will not execute to provide output.

In analyzing this script:

- line 1 is the required #! to indicate this is a Tcl script
- lines 2-3 open the procedure declaration
- lines 4-5 puts the output from the CLI command into a Tcl variable as a string, and breaks it up at each return character into an array of smaller strings
- line 6 starts a loop to go through the array of strings
- line 7 loops if the array element is punctuation or continues if its text
- line 8 takes the output of line 7's regular expression command and based on a match, performs one of the actions listed in lines 9 through 17
- lines 9-11 if regular expression matches 'Version' then parse the text and store values for the platform, version, and build number in the named array elements
- line 12-14 if regular expression matches 'Serial-Number' then store the value in an array element named that after trimming the string down to text only
- lines 15-17 is similar to line 12 except the regular expression is matched against 'Hostname'
- line 17-19 close the switch decision statement, the for each loop, and the procedure
- line 20 calls the procedure with an array name of status
- lines 21-25 output the information stored in the status array

Tcl loops

Even though the last script used a loop, that script's main purpose was storing information in the array. The next script uses a loop to create a preset number of users on the FortiGate device, in this case 10 users. The output is only shown for the first two users due to space considerations.

Example: Create 10 users from usr0001 to usr0010

Script

```
#!
proc do_cmd {cmd} {
puts [exec "$cmd\n" "# " 15]
}
   set num_users 10
do_cmd "config vdom"
do_cmd "edit root"
do_cmd "config user local"
for {set i 1} {$i <= $num_users} {incr i} {
   set name [format "usr%04d" $i]
   puts "Adding user: $name"
   do_cmd "edit $name"
   do_cmd "set status enable"
   do_cmd "set type password"
   do_cmd "next"
}
do_cmd "end"
```

Script

```
do_cmd "end"

do_cmd "config vdom"
do_cmd "edit root"
do_cmd "show user local"
do_cmd "end"
```

Output

```
View the log of script running on device:FortiGate-VM64

------- Executing time: 2013-10-16 15:27:18 ------
Starting log (Run on device)
config vdom
FortiGate-VM64 (vdom) #
edit root
current vf=root:0
FortiGate-VM64 (root) #
config user local
FortiGate-VM64 (local) #
Adding user: usr0001
edit usr0001
new entry 'usr0001' added
FortiGate-VM64 (usr0001) #
set status enable
FortiGate-VM64 (usr0001) #
set type password
FortiGate-VM64 (usr0001) #
next
FortiGate-VM64 (local) #
Adding user: usr0002
edit usr0002
new entry 'usr0002' added
FortiGate-VM64 (usr0002) #
set status enable
FortiGate-VM64 (usr0002) #
set type password
FortiGate-VM64 (usr0002) #
next
```

Variations:

There are a number of uses for this kind of looping script. One example is to create firewall policies for each interface that deny all non-HTTPS and non-SSH traffic by default. Another example is a scheduled script to loop through the static routing table to check that each entry is still reachable, and if not remove it from the table.

This script loops 10 times creating a new user each time whose name is based on the loop counter. The format command is used to force a four digit number.

In analyzing this script:

- line 1 is the required #! to indicate this is a Tcl script
- lines 2-4 open CLI command wrapper procedure
- line 5 declares the number of users to create

- line 6 gets the FortiGate ready for entering local users
- line 7 opens the for loop that will loop ten times
- line 8 sets the user name based on the incremented loop counter variable
- line 9 is just a comment to the administrator which user is being created
- lines 10-13 create and configure the user, leaving the CLI ready for the next user to be added
- line 14 ends the for loop
- line 15 ends the adding of users in the CLI
- line 16 executes a CLI command to prove the users were added properly

Tcl decisions

Tcl has a number of decision structures that allow you to execute different CLI commands based on what information you discover.

This script is more complex than the previous scripts as it uses two procedures that read FortiGate information, make a decision based on that information, and then executes one of the CLI sub-scripts based on that information.

Example: Add information to existing firewall policies

Script

```
#!
# need to define procedure do_cmd
# the second parameter of exec should be "# "
# If split one command to multiple lines use "\" to continue
proc do_cmd {cmd} {
puts [exec "$cmd\n" "# "]
}
foreach line [split [exec "show firewall policy\n" "# "] \n] {
if {[regexp {edit[ ]+([0-9]+)} $line match policyid]} {
continue
} elseif {[regexp {set[ ]+(\w+)[ ]+(.*)\r} $line match key value]} {
lappend fw_policy($policyid) "$key $value"
}
}
do_cmd "config firewall policy"
foreach policyid [array names fw_policy] {
if {[lsearch $fw_policy($policyid){diffservcode_forward 000011}] == -1} {
do_cmd "edit $policyid"
do_cmd "set diffserv-forward enable"
do_cmd "set diffservcode-forward 000011"
do_cmd "next"
}
}
do_cmd "end"
```

Variations:

This type of script is useful for updating long lists of records. For example if the FortiOS version adds new keywords to user accounts, you can create a script similar to this one to get the list of user accounts and for each one edit it, add the new information, and move on to the next.

This script uses two decision statements. Both are involved in text matching. The first decision is checking each line of input for the policy ID and if its not there it skips the line. If it is there, all the policy information is saved to an array for future use. The second decision searches the array of policy information to see which polices are missing.

In analyzing this script:

- line 1 is the required #! to indicate this is a Tcl script
- line 2-8 is a loop that reads each policy's information and appends only the policy ID number to an array variable called fw_policy
- line 9 opens the CLI to the firewall policy section to prepare for the loop
- line 10 starts the for each loop that increments through all the firewall policy names stored in fw_policy
- line 11 checks each policy for an existing differvcode_forward 000011 entry - if its not found lines 12-15 are executed, otherwise they are skipped
- line 12 opens the policy determined by the loop counter
- line 13-14 enable diffserv_forward, and set it to 000011
- line 15 saves this entry and prepares for the next one
- line 16 closes the if statement
- line 17 closes the for each loop
- line 18 saves all the updated firewall policy entries

Additional Tcl Scripts

Example: Get and display state information about the FortiGate device

Script

```
#!
#Run on FortiOS v7.4.0
#This script will display FortiGate's CPU states,
#Memory states, and Up time
puts [exec "# This is an example Tcl script to get the system performance of the FortiGate\n" "# "
      15 ]
   set input [exec "get system status\n" "# " 15]
regexp {Version: *([^ ]+) ([^,]+),build([0-9]+),[0-9]+} $input dummy status(Platform) status
      (Version) status(Build)
if {$status(Version) eq "v7.4.0"} {
   puts -nonewline [exec "config global\n" "# " 30]
   puts -nonewline [exec "get system performance status\n" "# " 30]
   puts -nonewline [exec "end\n" "# " 30]
} else {
   puts -nonewline [exec "get system performance\n" "#" 30]
}
```

Output

```
-------Executing time: Mon May 12 10:30:22 2025----------
Starting log (Run on device)

# This is an example Tcl script to get the system performance of the FortiGate
FortiGate-VM64 #
config global
FortiGate-VM64 (global) # get system performance status

CPU states: 2% user 2% system 0% nice 96% idle 0% iowait 0% irq 0% softirq
CPU0 states: 2% user 0% system 0% nice 98% idle 0% iowait 0% irq 0% softirq
CPU1 states: 2% user 3% system 0% nice 95% idle 0% iowait 0% irq 0% softirq
Memory: 4041496k total, 2029456k used (50.2%), 1481528k free (36.7%), 530512k freeable (13.1%)
Average network usage: 305 / 293 kbps in 1 minute, 319 / 308 kbps in 10 minutes, 574 / 563 kbps in
      30 minutes
Maximal network usage: 641 / 713 kbps in 1 minute, 1339 / 1378 kbps in 10 minutes, 48415 / 48414
      kbps in 30 minutes
Average sessions: 940 sessions in 1 minute, 995 sessions in 10 minutes, 992 sessions in 30 minutes
Maximal sessions: 973 sessions in 1 minute, 1113 sessions in 10 minutes, 1114 sessions in 30
      minutes
Average session setup rate: 12 sessions per second in last 1 minute, 11 sessions per second in
      last 10 minutes, 10 sessions per second in last 30 minutes
Maximal session setup rate: 36 sessions per second in last 1 minute, 40 sessions per second in
      last 10 minutes, 43 sessions per second in last 30 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in
      last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in
      last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 25 total in 1 minute
Uptime: 0 days, 2 hours, 50 minutes

FortiGate-VM64 (global) # end
FortiGate-VM64 #
------- The end of log ----------
```

Example: Configure common global settings

Script

```
#!
#Run on FortiOS v7.4.0
#This script will configure common global, user group and ntp settings
#if you do not want to set a parameter, comment the
#corresponding set command
#if you want to reset a parameter to it's default
#value, set it an empty string
puts [exec "# This is an example Tcl script to configure global, user group and ntp setting of
      FortiGate\n" "# " 15 ]
# global
set sys_global(admintimeout) ""
# user group
set sys_user_group(authtimeout) 20
# ntp
```

Script

```
set sys_ntp(source-ip) "0.0.0.0"
set sys_ntp(ntpsync) "enable"
#procedure to execute FortiGate command
proc fgt_cmd cmd {
puts -nonewline [exec "$cmd\n" "# " 30]
}
#config system global---begin
fgt_cmd "config global"
fgt_cmd "config system global"
foreach key [array names sys_global] {
if {$sys_global($key) ne ""} {
fgt_cmd "set $key $sys_global($key)"
} else {
fgt_cmd "unset $key"
}
}
fgt_cmd "end"
fgt_cmd "end"
#config system global---end
#config system user group---begin
fgt_cmd "config vdom"
fgt_cmd "edit root"
fgt_cmd "config user group"
fgt_cmd "edit groupname"
foreach key [array names sys_user_group] {
if {$sys_user_group($key) ne ""} {
fgt_cmd "set $key $sys_user_group($key)"
} else {
fgt_cmd "unset $key"
}
}
fgt_cmd "end"
fgt_cmd "end"
#config system user group---end
#config system ntp---begin
fgt_cmd "config global"
fgt_cmd "config system ntp"
foreach key [array names sys_ntp] {
if {$sys_ntp($key) ne ""} {
fgt_cmd "set $key $sys_ntp($key)"
} else {
fgt_cmd "unset $key"
}
}
fgt_cmd "end"
fgt_cmd "end"
#config system ntp---end
```

Output

```
-------Executing time: Mon May 12 10:35:41 2025-----------
Starting log (Run on device)

# This is an example Tcl script to configure global, user group and ntp setting of FortiGate
```

Output

```
FortiGate-VM64 #
config global
FortiGate-VM64 (global) # config system global
FortiGate-VM64 (global) # unset admintimeout
FortiGate-VM64 (global) # end
FortiGate-VM64 (global) # end
FortiGate-VM64 # config vdom
FortiGate-VM64 (vdom) # edit root
current vf=root:0
FortiGate-VM64 (root) # config user group
FortiGate-VM64 (group) # edit groupname
new entry 'groupname' added
FortiGate-VM64 (groupname) # set authtimeout 20
FortiGate-VM64 (groupname) # end
FortiGate-VM64 (root) # end
FortiGate-VM64 # config global
FortiGate-VM64 (global) # config system ntp
FortiGate-VM64 (ntp) # set ntpsync enable
FortiGate-VM64 (ntp) # set source-ip 0.0.0.0
FortiGate-VM64 (ntp) # end
FortiGate-VM64 (global) # end
FortiGate-VM64 #
----------------End of Log-------------------------
```

Example: Configure syslogd settings and filters

Script

```
#!
#Run on FortiOS v7.4.7
#This script will configure log syslogd setting and
#filter
#key-value pairs for 'config log syslogd setting', no
#value means default value.
set setting_list {{status enable} {facility alert} {port} {server 1.1.1.2}}
#key-value pairs for 'config log syslogd filter', no
#value means default value.
puts [exec "# This is an example Tcl script to configure log syslogd setting and filter setting of
FortiGate\n" "# " 15 ]
set filter_list {{forward-traffic enable} {local-traffic enable} {severity} {ztna-traffic enable}
{anomaly disable} {forti-switch enable}}
#set the number of syslogd server, "", "2" or "3"
set syslogd_no "2"
#procedure to execute FortiGate CLI command
proc fgt_cmd cmd {
puts -nonewline [exec "$cmd\n" "# "]
}
```

Script

```
#procedure to set a series of key-value pairs
proc set_kv kv_list {
foreach kv $kv_list {
set len [llength $kv]
if {$len == 0} {
continue
} elseif {$len == 1} {
fgt_cmd "unset [lindex $kv 0]"
} else {
fgt_cmd "set [lindex $kv 0] [lindex $kv 1]"
} } }
#configure log syslogd setting---begin
#fgt_cmd "config global"
fgt_cmd "config log syslogd$syslogd_no setting"
set_kv $setting_list
fgt_cmd "end"
#configure log syslogd setting---end
#configure log syslogd filter---begin
fgt_cmd "config log syslogd$syslogd_no filter"
set_kv $filter_list
fgt_cmd "end"
#configure log syslogd filter---end
```

Output

```
Starting log (Run on device)
# This is an example Tcl script to configure log syslogd sett ing and filter setting of FortiGate

Branch_Office_01 #
config log syslogd2 setting
Branch_Office_01 (setting) # set status enable
Branch_Office_01 (setting) # set facility alert
Branch_Office_01 (setting) # unset port
Branch_Office_01 (setting) # set server 1.1.1.2
Branch_Office_01 (setting) # end
Branch_Office_01 # config log syslogd2 filter
Branch_Office_01 (filter) # set forward-traffic enable
Branch_Office_01 (filter) # set local-traffic enable
Branch_Office_01 (filter) # unset severity
Branch_Office_01 (filter) # set ztna-traffic enable
Branch_Office_01 (filter) # set anomaly disable
Branch_Office_01 (filter) # set forti-switch enable
Branch_Office_01 (filter) # end
Branch_Office_01 #

----------------End of Log-------------------------
```

Example: Configure the FortiGate device to communicate with a FortiAnalyzer unit

Script

```
#!
#This script will configure the FortiGate device to
#communicate with a FortiAnalyzer unit
#Enter the following key-value pairs for 'config
#system fortianalyzer'
   set status enable
   set enc-algorithm high
#localid will be set as the hostname automatically
#later
puts [exec "# This is an example Tcl script to configure the FortiGate to communicate with a
      FortiAnalyzer\n" "# " 15 ]
   set server 1.1.1.1
#for fortianalyzer, fortianalyzer2 or
#fortianalyzer3, enter the corresponding value "",
#"2", "3"
   set faz_no ""
#keys used for 'config system fortianalyzer', if you
#do not want to change the value of a key, do not put
#it in the list
   set key_list {status enc-algorithm server }
##procedure to get system status from a FortiGate
proc get_sys_status aname {
upvar $aname a
set input [split [exec "get system status\n" "# "] \n]
foreach line $input {
if {![regexp {([^:]+):(.*)} $line dummy key value]} continue
   set a([string trim $key]) [string trim $value]
}
}
#procedure to execute FortiGate command
proc fgt_cmd cmd {
puts -nonewline [exec "$cmd\n" "# "]
}
#set the localid as the FortiGate's hostname
#config system fortianalyzer---begin
fgt_cmd "config global"
fgt_cmd "config log fortianalyzer$faz_no setting"
foreach key $key_list {
if [info exists $key] {
   fgt_cmd "set $key [set $key]"
} else {
   fgt_cmd "unset $key"
}
}
fgt_cmd "end"
fgt_cmd "end"
#config system fortianalyzer---end
```

Output

```
Starting log (Run on device)
```

Output

```
FortiGate-VM64 # config global
FortiGate-VM64 (global) # config log fortianalyzer setting
FortiGate-VM64 (setting) # set status enable
FortiGate-VM64 (setting) # set enc-algorithm high
FortiGate-VM64 (setting) # set localid FortiGate-VM64
FortiGate-VM64 (setting) # set server 1.1.1.1
FortiGate-VM64 (setting) # end
FortiGate-VM64 (global) # end
FortiGate-VM64 #
------- The end of log ---------
```

Example: Create custom IPS signatures and add them to a custom group

Script

```
#!
#Run on FortiOS v7.00
#This script will create custom ips signatures and
#change the settings for the custom ips signatures

puts [exec "# This is an example Tcl script to create custom ips signatures and change the
      settings for the custom ips signatures on a FortiGate\n" "# " 15 ]
#Enter custom ips signatures, signature names are the
#names of array elements
   set custom_sig(c1) {"F-SBID(--protocol icmp;--icmp_type 10; )"}
   set custom_sig(c2) {"F-SBID(--protocol icmp;--icmp_type 0; )"}
#Enter custom ips settings
   set custom_rule(c1) {{status enable} {action block} {log enable} {log-packet} {severity high}}
   set custom_rule(c2) {{status enable} {action pass} {log} {log-packet disable} {severity low}}
#procedure to execute FortiGate command
proc fgt_cmd cmd {
puts -nonewline [exec "$cmd\n" "# "]
}
#procedure to set a series of key-value pairs
proc set_kv kv_list {
foreach kv $kv_list {
set len [llength $kv]
if {$len == 0} {
   continue
} elseif {$len == 1} {
   fgt_cmd "unset [lindex $kv 0]"
} else {
   fgt_cmd "set [lindex $kv 0] [lindex $kv 1]"
}
} }
#config ips custom---begin
fgt_cmd "config vdom"
fgt_cmd "edit root"
fgt_cmd "config ips custom"
foreach sig_name [array names custom_sig] {
fgt_cmd "edit $sig_name"
fgt_cmd "set signature $custom_sig($sig_name)"
fgt_cmd "next"
```

Script

```
}
fgt_cmd "end"
#config ips custom settings---begin
foreach rule_name [array names custom_rule] {
fgt_cmd "config ips custom"
fgt_cmd "edit $rule_name"
set_kv $custom_rule($rule_name)
fgt_cmd "end"
}
fgt_cmd "end"
#config ips custom settings---end
```

Output

```
Starting log (Run on device)
FortiGate-VM64 # config vdom
FortiGate-VM64 (vdom) # edit root
current vf=root:0
FortiGate-VM64 (root) # config ips custom
FortiGate-VM64 (custom) # edit c1
set signature "F-SBID(--protocol icmp;--icmp_type 10; )"
FortiGate-VM64 (c1) # set signature "F-SBID(--protocol icmp;--icmp_type 10; )"
FortiGate-VM64 (c1) # next
FortiGate-VM64 (custom) # edit c2
FortiGate-VM64 (c2) # set signature "F-SBID(--protocol icmp;--icmp_type 0; )"
FortiGate-VM64 (c2) # next
FortiGate-VM64 (custom) # end
FortiGate-VM64 (root) # config ips custom
FortiGate-VM64 (custom) # edit c1
FortiGate-VM64 (c1) # set status enable
FortiGate-VM64 (c1) # set action block
FortiGate-VM64 (c1) # set log enable
FortiGate-VM64 (c1) # unset log-packet
FortiGate-VM64 (c1) # set severity high
FortiGate-VM64 (c1) # end
FortiGate-VM64 (root) # config ips custom
FortiGate-VM64 (custom) # edit c2
FortiGate-VM64 (c2) # set status enable
FortiGate-VM64 (c2) # set action pass
FortiGate-VM64 (c2) # unset log
FortiGate-VM64 (c2) # set log-packet disable
FortiGate-VM64 (c2) # set severity low
FortiGate-VM64 (c2) # end
FortiGate-VM64 (root) # end
FortiGate-VM64 #
------- The end of log ----------
```

Variations:

None.

Tcl file IO

You can write to and read from files using Tcl scripts. For security reasons there is only one directory on the FortiManager where scripts can access files. For this reason, there is no reason to include the directory in the file name you are accessing. For example “/var/temp/myfile” or “~/myfile” will cause an error, but “myfile” or “/myfile” is OK.

The Tcl commands that are supported for file IO are: `file`, `open`, `gets`, `read`, `tell`, `seek`, `eof`, `flush`, `close`, `fcopy`, `fconfigure`, and `fileevent`.

The Tcl file command only supports `delete` subcommand, and does not support the `-force` option.

There is 10MB of diskspace allocated for Tcl scripts. An error will be reported if this size is exceeded.

These files will be reset when the following CLI commands are run: `exec format`, `exec reset partition`, or `exec reset all`. The files will not be reset when the firmware is updated unless otherwise specified.

To write to a file:

Script

```
#!
set somefile [open “tcl_test” w]
puts $somefile "Hello, world!"
close $somefile
```

To read from a file:

Script

```
#!
set otherfile [open “tcl_test” r]
while {[gets $otherfile line] >= 0} {
puts [string length $line]
}
close $otherfile
```

Output

```
Hello, world!
```

These two short scripts write a file called `tcl_test` and then read it back.

Line 3 in both scripts opens the file either for reading (r) or writing (w) and assigns it to a filehandle (somefile or otherfile). Later in the script when you see these filehandles, its input or output passing to the open file.

When reading from the file, lines 4 and 5 loop through the file line by line until it reaches the end of the file. Each line that is read is put to the screen.

Both scripts close the file before they exit.

Troubleshooting Tips

This section includes suggestions to help you find and fix problems you may be having with your scripts.

- Make sure the commands you are trying to execute are valid for the version of FortiOS running on your target FortiGate device.
- Do not use FortiManager metadata variables in Tcl scripts.
- You should always use braces when evaluating code that may contain user input, to avoid possible security breaches. To illustrate the danger, consider this interactive session:

```
% set userinput {[puts DANGER!]}
```

```
[puts DANGER!]
% expr $userinput == 1
DANGER!
0
% expr {$userinput == 1}
0
```

In the first example, the code contained in the user-supplied input is evaluated, whereas in the second the braces prevent this potential danger. As a general rule, always surround expressions with braces, whether using expr directly or some other command that takes an expression.

- A number that includes a leading zero or zeros, such as 0500 or 0011, is interpreted as an octal number, not a decimal number. So 0500 is actually 320 in decimal, and 0011 is 9 in decimal.
- There is a limit to the number of scripts allowed on the FortiManager unit. Try removing an old script before trying to save your current one.
- Using the Tcl command “catch” you can add custom error messages in your script to alert you to problems during the script execution. When catch encounters an error it will return 1, but if there is no error it will return 0. For example:

```
if { [catch {open $someFile w} fid] } {
   puts stderr "Could not open $someFile for writing\n$fid"
   exit 1 ;# error opening the file!
   } else {
# put the rest of your script here
   }
```

Use Tcl script to access FortiManager’s device database or ADOM database

You can use Tcl script to access FortiManager’s device database or ADOM database (local database). The option to run a TCL script on remote FortiGate directly (via CLI) should be still used. However, for any portion of a script that needs to be run on a local database, FortiManager uses a syntax within the TCL script `exec_ondb` to define it.

Example 1:

Run the Tcl script on an ADOM database for a specify policy package. For example, creating new a policy or object:

Syntax	`puts [exec_ondb "/adom/<adom_name>/pkg/<pkg_fullpath>" "embedded cli commands" "# "]`
Usage	`puts [exec_ondb "/adom/52/pkg/default" " config firewall address edit port5_address next end " "# "]`

Example 2:

Run the Tcl script on the current ADOM database for a specify policy package. For example, creating a new policy and object:

Syntax	puts [exec_ondb "/adom/./pkg/<pkg_fullpath>" "embedded cli commands" "# "] or puts [exec_ondb "/pkg/<pkg_fullpath>" "embeded cli commands" "# "]
Usage	puts [exec_ondb "/adom/./pkg/default" " config firewall address edit port5_address next end " "# "]

Example 3:

Run Tcl script on a specific device in an ADOM:

Syntax	puts [exec_ondb "/adom/<adom_name>/device/<dev_name>" "embedded cli commands" "# "]
Usage	puts [exec_ondb "/adom/v52/device/FGT60CA" " config global config system global set admintimeout 440 end end " "# "]

Example 4:

Run Tcl script on current devices in an ADOM:

Syntax	puts [exec_ondb "/adom/<adom_name>/device/." "embedded cli commands" "# "]
Usage	puts [exec_ondb "/adom/v52/device/." " config global config system global set admintimeout 440 end end " "# "]

exec_ondb cannot be run on the Global ADOM.

Provisioning Templates

Go to *Device Manager* > *Provisioning Templates* to access configuration options for the following templates:

- Template groups on page 274
- Fabric authorization templates on page 278

- System templates
- IPsec tunnel templates on page 286
- SD-WAN templates on page 304
- SD-WAN overlay templates on page 327
- Static route templates on page 348
- BGP templates on page 350
- Certificate templates
- Threat Weight templates
- CLI templates on page 357
- NSX-T service templates on page 371

Template groups

The *Device Manager > Provisioning Templates > Template Group* pane allows you to create a template group, and add templates to the group. Then you can assign the template group to one or more devices or VDOMs or to a device group rather than assigning individual templates to devices or VDOMs.

You can assign one provisioning template from each of the following template types to a template group. Multiple AP profiles can be selected.

- System template
- Threat weight template
- IPsec tunnel template
- Static route template
- BGP template
- NSX-T service template
- SD-WAN template
- AP Profile
- FortiSwitch template
- FortiExtender template
- CLI template
- CLI template group

When a template group is assigned to a device or device group, FortiManager ensures the templates in the group are installed to devices in the correct order. For example, if a template group contains both an IPsec template and an interface template, FortiManager ensures that the IPsec template is installed to devices before the interface template to allow the interface template to configure IP addresses on the interfaces created by the IPsec template.

When uninstalling template groups, FortiManager ensures the templates are uninstalled in the correct order too.

Following is an overview of how to use template groups:

1. Create a template group. See Creating template groups on page 275.
2. Assign the template group to one or more devices or to one or more device groups. See Assigning template groups on page 276.
3. Edit template groups as needed. See Editing template groups on page 277.

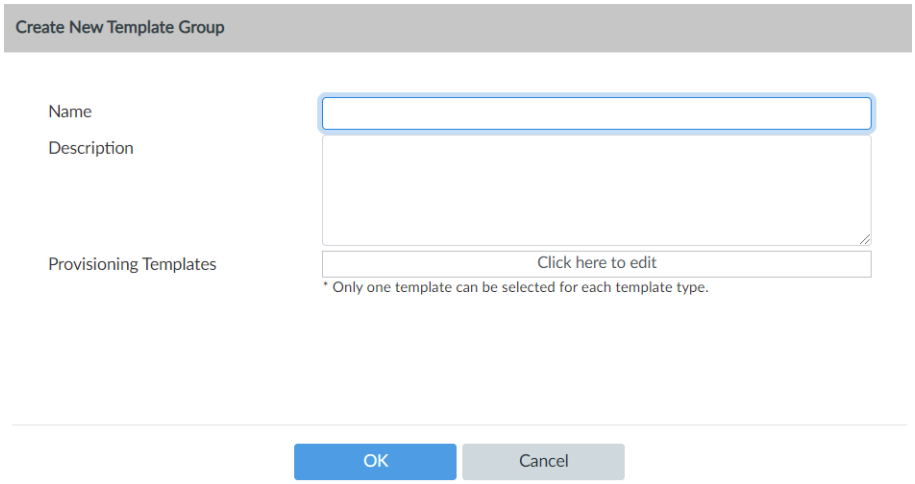
You can also delete template groups. See Deleting template groups on page 278.

Creating template groups

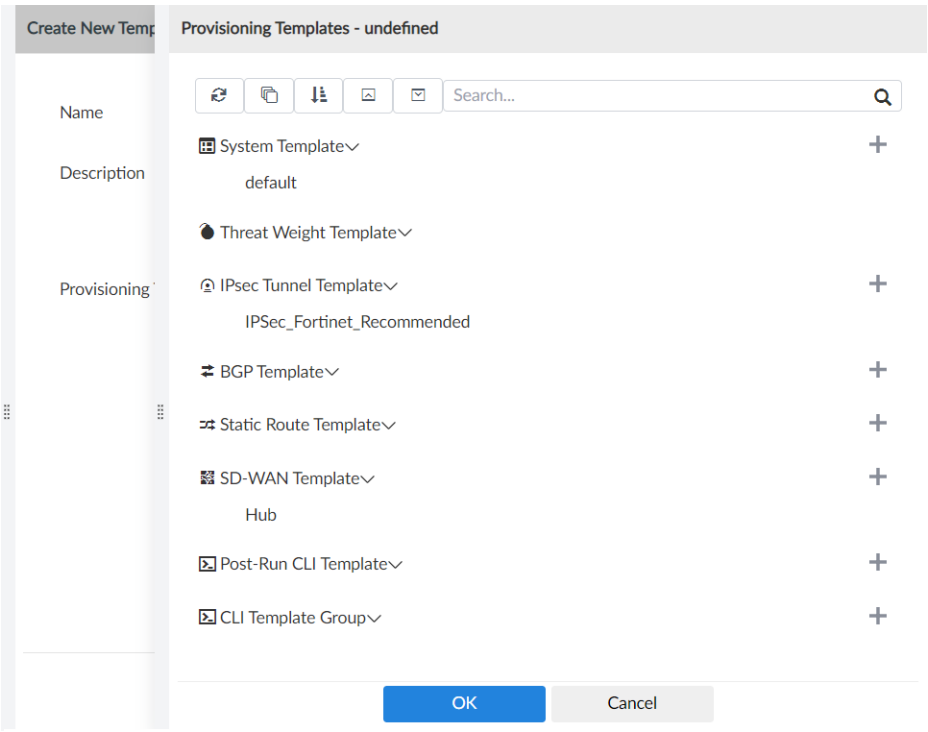
You can create a template group, and add provisioning templates to it.

To create a template group:

1. Go to *Device Manager* > *Provisioning Templates* > *Template Group*.
2. In the toolbar, click *Create New*.
   Alternately, you can select a template group, and click *Clone* to create a new template group.
   The *Create New Template Group* pane is displayed.



3. In the *Name* box, type a name for the template group.
4. (Optional) In the *Description* box, type a description of the template group.
5. Beside *Provisioning Templates*, click the box to display a list of provisioning templates available for selection.
   The *Provisioning Templates - <name>* pane is displayed.
   At the top of the screen is a row of buttons that you can use to locate provisioning templates. Hover over each button for a tooltip.
   In the *Search* box, type the name of the provisioning template, and press *Enter* to locate it.
   You can also create a new provisioning template by clicking the *+* button.



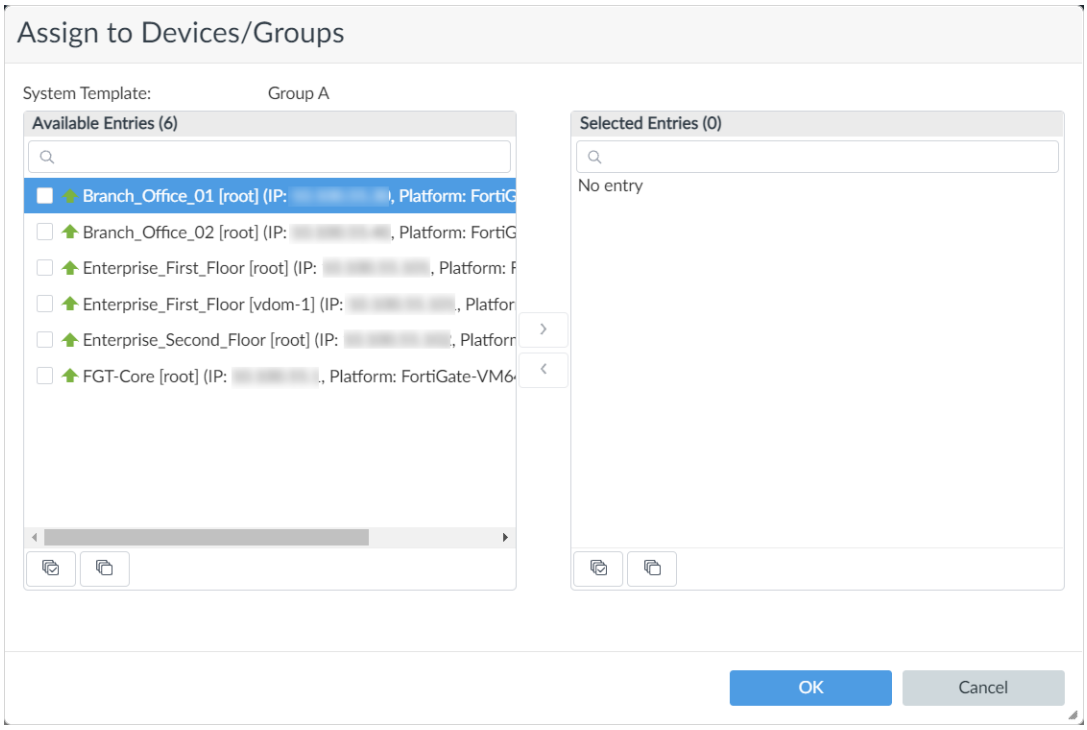
6. Select one or more templates, and click *OK*.
   You can only select one template for each template type.
   The templates are selected.
7. Click *OK*.
   The template group is created.

Assigning template groups

You can assign a template group to one or more devices or to a device group.

To assign template group:

1. Go to *Device Manager* > *Provisioning Templates* > *Template Group*.
2. In the content pane, select a template group, and click *Assigned to Device*.
   The *Assign to Devices/Groups* dialog box is displayed.



3. In the *Available Entries* list, select one or more devices or device groups, and click > to move them to the *Selected Entries* list, and then click *OK*.
   The devices and device groups assigned to the template group are shown in the *Assign to Device/Device Group* column.
4. Go to *Device Manager* > *Device & Groups*, and view the list of devices in *Table View*.
   The *Provisioning Templates* column displays the name of the assigned template group.

Editing template groups

After you create a template group, you can edit it to add or remove templates. You can also edit templates.

To edit template groups:

1. Go to *Device Manager* > *Provisioning Templates* > *Template Group*.
2. In the content pane, select a template group, and click *Edit*.
   The *Edit Template Group - <group name>* dialog box is displayed.
3. Beside *Provisioning Templates*, click the *Click here to edit* link.
   The *Provisioning Templates - <group name>* pane is displayed.
4. Change the templates in the group by using any of the following methods:
   - Expand a template type, and select a template to display or hide a checkmark. Templates with a checkmark are added to the template group, and templates without a checkmark are removed from the template group.
   - Beside a template type, click the + button to create a new template.
   - Expand a template type, select a template, and click the Edit button to edit the template.

5. Click *OK*.
   The *Provisioning Templates - <group name>* pane closes, and the list of selected provisioning templates is displayed.
6. Click *OK*.
   The template group changes are saved.

Deleting template groups

You can delete template groups.

To delete template groups:

1. Go to *Device Manager > Provisioning Templates > Template Group*.
2. In the content pane, select a template group, and click *Delete*.
   The *Confirm Deletion* dialog box is displayed.
3. Click *OK*.
   The template group is deleted.

Fabric authorization templates

Fabric authorization templates can be used to allow FortiManager to automatically authorize FortiAP, FortiSwitch, and FortiExtender devices.

Fabric authorization templates can be created by going to *Device Manager > Provisioning Templates > Fabric Authorization Template*.

The following options are available:

Create New	Create a new template.
Edit	Edit a template. Right-click a template, and select *Edit*.
Delete	Delete a template. Right-click a template, and select *Delete*.
Generate	Generate the Fabric devices using the template.

Fabric authorization template workflow

Fabric authorization template workflow for online devices

1. Create the Fabric authorization template.
2. Generate the template and select the required target FortiGate device(s). See Generating Fabric authorization templates on page 281.
   - FortiManager will create or update the list of Fabric devices (FortiAP, FortiSwitch, and FortiExtender) on the device database according to the template configuration.
   - The device's *Config Status* will be set to *Modified*. The newly created entries can be modified/deleted at this stage as required.

3. Perform an install on the target FortiGate devices so the Fabric devices are pushed to the targets.
   - When the real Fabric devices come online matching the specified prefix, it will replace the device in the Device Manager. The list is followed from top to bottom until all devices have been replaced by real devices, at which point additional devices will not be automatically authorized.
   - Fabric devices configured by FortiManager are displayed in the *Device Manager*. You can go to FortiAP Manager , FortiSwitch Manager, and FortiExtender Manager to view and assign profiles to the devices.

Fabric authorization template workflow for model devices

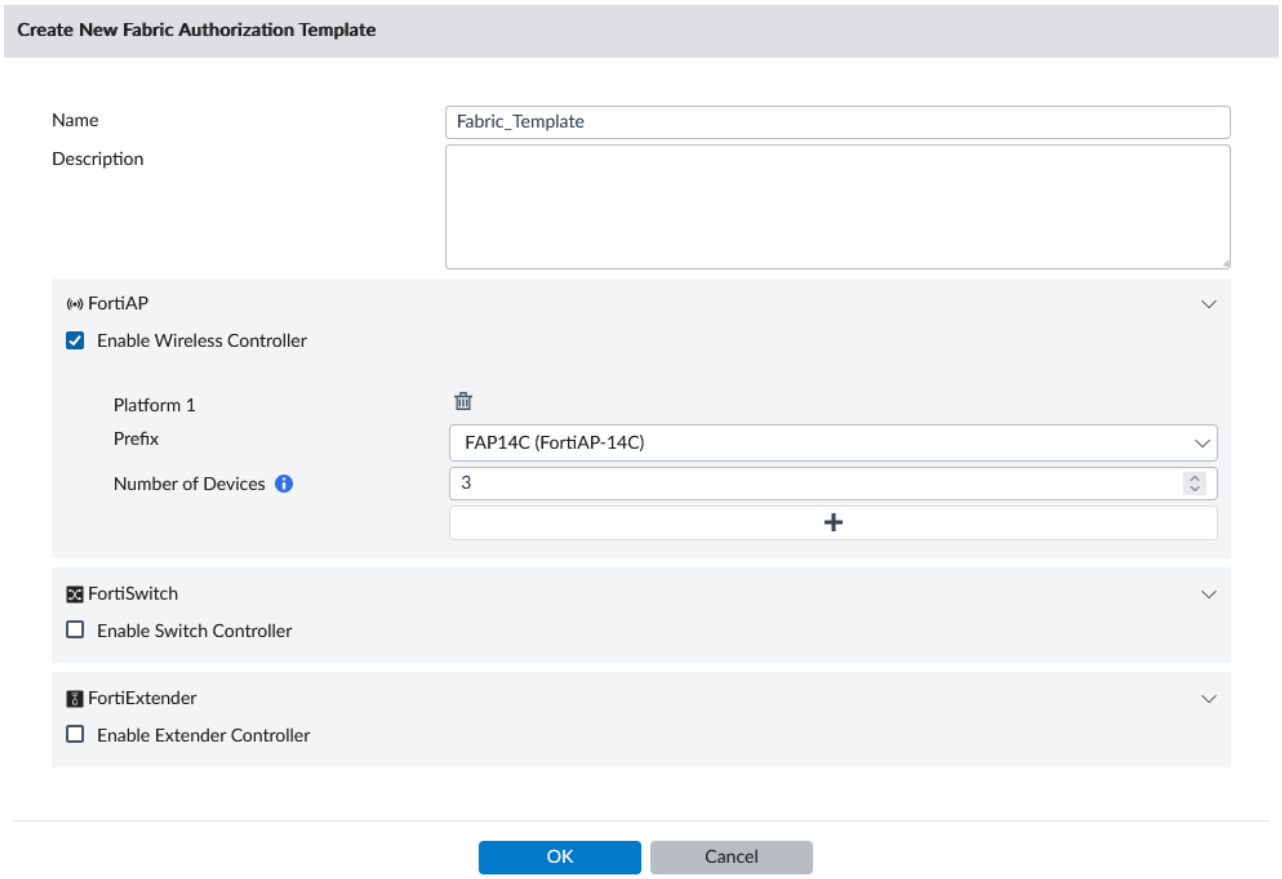
1. Create the Fabric authorization template.
2. Add the template to a device blueprint. See Using device blueprints for model devices on page 114.
3. Add model devices individually or by importing them from a CSV file, and select the device blueprint which includes the Fabric authorization template.
4. After the device is added to FortiManager, the FortiAP, FortiExtender and FortiSwitch devices will be automatically configured for the FortiGate(s) as defined in the Fabric authorization template.
   - When the real Fabric devices come online matching the specified prefix, it will replace the device in the Device Manager. The list is followed from top to bottom until all devices have been replaced by real devices, at which point additional devices will not be automatically authorized.

Creating and applying the Fabric authorization template

To create a new Fabric authorization template:

1. Go to *Device Manager* > *Provisioning Templates* > *Fabric Authorization Template*.

2. Click *Create New*. The *Create New Fabric Authorization Template* pane opens.



3. Enter the following information, then click *OK* to create the certificate template:

Name		Enter a name for the Fabric authorization template.
Description		Optionally, provide a description for the template.
FortiAP		
	Enable Wireless Controller	Toggle to enable wireless controllers. Additional settings are available once this option is selected.
	Platform 1	By default, only one wireless controller platform is listed. You can click the add button at the bottom of the page to add another platform to the template. Click the trash icon to delete the platform.
	Prefix	Select the serial number prefix for the selected devices from the dropdown menu.
	Number of Devices	Select the number of devices to pre-authorize.
FortiSwitch		
	Enable Switch Controller	Toggle to enable switch controllers. Additional settings are available once this option is selected.

	Platform	By default, only one switch platform is listed. You can click the add button at the bottom of the page to add another platform to the template. Click the trash icon to delete the platform.
	Prefix	Select the serial number prefix for the selected devices from the dropdown menu.
	Number of Devices	Select the number of devices to pre-authorize.
	FortiLink Interface	Type the interface for FortiLink.
FortiExtender		
	Enable Extender Controller	Toggle to enable extender controllers. Additional settings are available once this option is selected.
	Platform 1	By default, only one extender platform is listed. You can click the add button at the bottom of the page to add another platform to the template. Click the trash icon to delete the platform.
	Prefix	Select the serial number prefix for the selected devices from the dropdown menu.
	Number of Devices	Select the number of devices to pre-authorize.
	Extension Type	Select the extension type as either *WAN Extension* or *LAN Extension*.

Generating Fabric authorization templates

To generate a Fabric authorization template:

1. Go to *Device Manager* > *Provisioning Templates* > *Fabric Authorization Template*.
2. Select a previously created Fabric authorization template, and click *Generate* in the toolbar or right-click menu.
3. Select the target FortiGate devices on which to generate the configuration.
   The *Generate authorization template* wizard runs and applies the authorization template to the selected device.
4. Click *Finish*.

System templates

The *Device Manager* > *Provisioning Templates* > *System Templates* pane allows you to create and manage device profiles. A system template is a subset of a model device configuration. Each device or device group can be linked with a system template. When linked, the selected settings come from the template and not from the *Device Manager* database.

By default, there is one generic default profile defined. System templates are managed in a similar manner to policy packages. You can use the context menus to create new device profiles. You can configure the settings in each section or import settings from a specific device.

Fields that support metadata variables are identified with the following magnifying glass icon . See ADOM-level metadata variables on page 557..

Go to *Device Manager* > *Provisioning Templates* > *System Templates* to configure system templates.

Some settings may not be available in all ADOM versions.

To import settings from a device, click *More* > *Import* and select the device.

Enable a section to expose the settings. The following sections and settings are available:

Widget	Description
DNS	DNS includes the following settings: • Primary DNS Server • Secondary DNS Server • Local Domain Name • Interface Selected Method • Advanced Options
NTP Server	NTP Server includes the following settings: • Synchronize with NTP Server • Sync Interval • Interface • Server mode • Source IP • Advanced Options You can select to use the FortiGuard server or specify one or more other servers.
Alert Email	Alert Email includes the following settings: • SMTP Server • Authentication
Admin Settings	Admin Settings includes the following settings: • HTTP Port • HTTPS Port • SSH Port • SSH v1 compatibility • Idle Timeout • Enable SCP • Host Name • Time Zone • Geographic Coordinate
SNMP	SNMP v1/v2 and SNMP v3 settings. In the toolbar, you can select to create, edit, or delete the record.

Widget	Description
	To create a new SNMP, click *Create New* and specify the community name, hosts, queries, traps, and SNMP events.
Replacement Messages	You can customize replacement messages. Click *Import* to select a device and the objects to import.
FortiGuard	Enable *Enable FortiGuard Security Updates* to retrieve updates from FortiGuard servers or from this FortiManager. You can define multiple servers and specify *Update*, *Rating*, or *Updates and Rating*. You can also select *Include Worldwide FortiGuard Servers*.
Log Settings	Select *Send Logs to FortiAnalyzer Cloud*, *Send Logs to FortiAnalyzer/FortiManager*, and/or *Send Logs to Syslog*. If selected, enter the requisite information for the option.
Interface	Zone and interface settings. In the toolbar, you can select to create, edit, or delete the record. By default the *Interface* widget is hidden. From the *Toggle Widgets* menu, select *Interface* to display the *Interface* widget. To create a new interface, click *Create New* and specify an action and identify what models will receive the action.

You can create, edit, or delete templates. Select *System Templates* in the tree to display the *Create New*, *Edit*, *Delete*, and *Import* options in the content pane. You can also select the devices or device groups to be associated with the template by selecting *Assign to Devices/Groups*.

Assigning system templates to devices and device groups

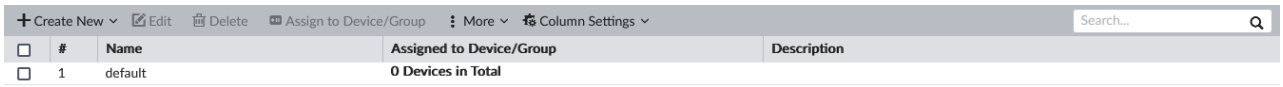
You must assign an interface template to devices when *Required* is enabled for device object meta fields.

A value must be defined for each device for the required meta fields before you can assign an interface template to the device.

See also Meta Fields on page 967.

To assign system templates to devices or device groups:

1. Go to *Device Manager* > *Provisioning Templates* > *System Templates*.
2. In the table, select a template.



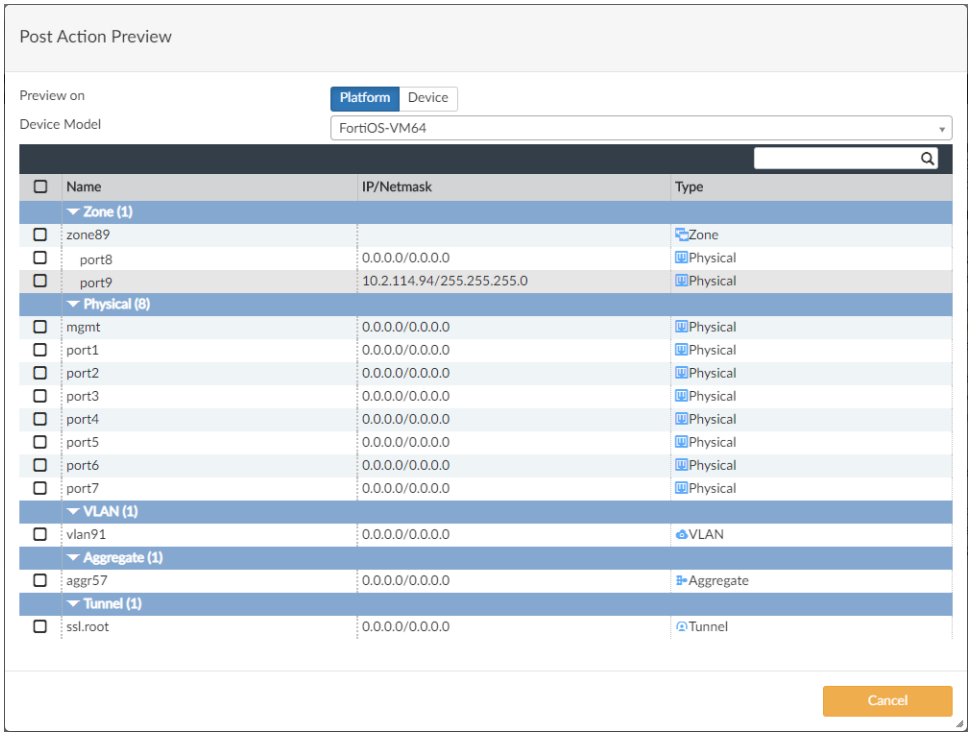
3. Click *Assign to Devices/Groups*.
   The *Assign to Device/Groups* dialog box is displayed.
4. In the *Available Entries* list, select one or more devices or device groups, and click > to move them to the *Selected Entries* list, and then click *OK*.
   The devices and device groups assigned to the template are shown in the *Device/Group Name* column.

Previewing interface actions

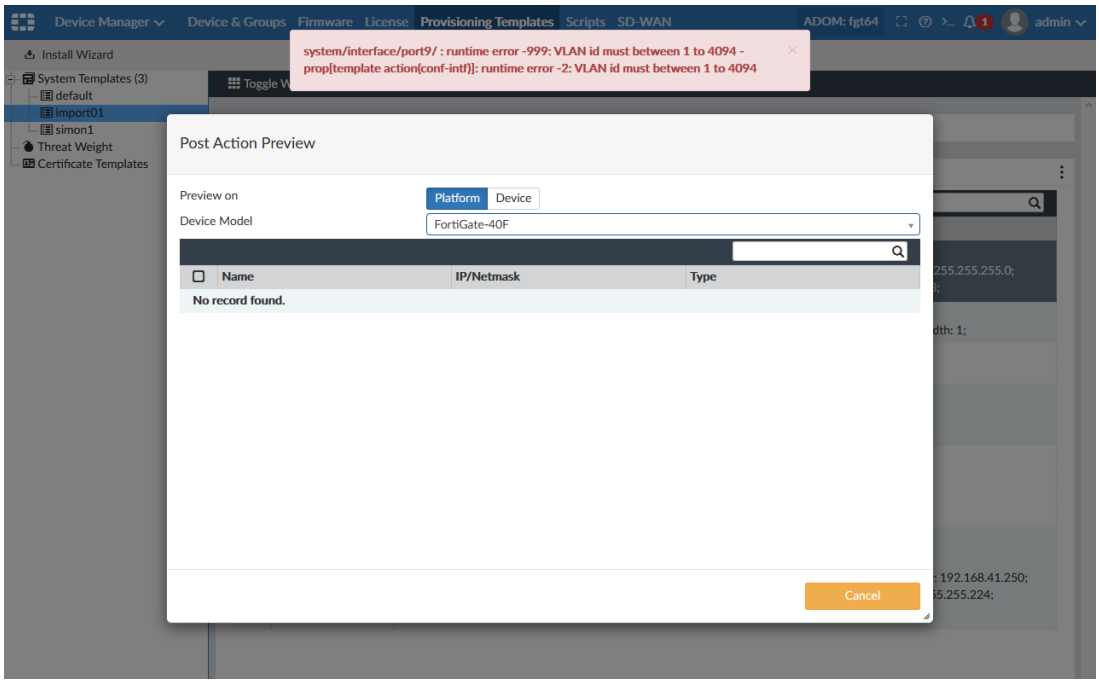
After you create an interface action, you can preview the interface action per model or device.

To preview interface actions:

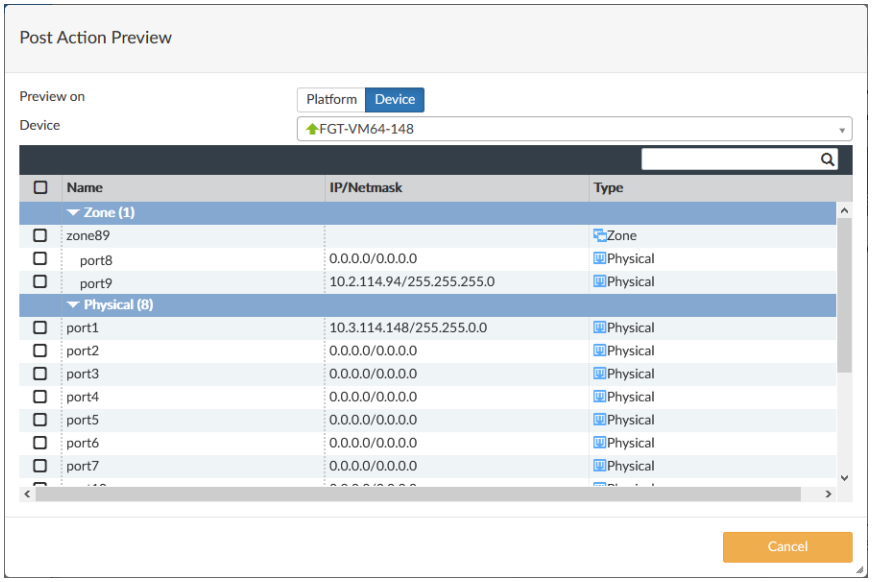
1. Go to *Device Manager* > *Provisioning Templates* > *System Templates*.
2. In the tree menu, select a template with an interface.
   The template details are displayed in the content pane.
3. In the *Interface* widget, select an interface, and click *Post Action View*.
   The *Post Action Preview* dialog box is displayed.
4. Beside *Preview on*, click *Platform* or *Device*, and then select the platform or device from the list.
   In the following example, the selected platform has the same type of port.



In the following example, the selected platform does not have the same type of port, and an error is displayed.



In the following example, the selected device has the same type of port.



5. Click *Cancel* to close the dialog box.

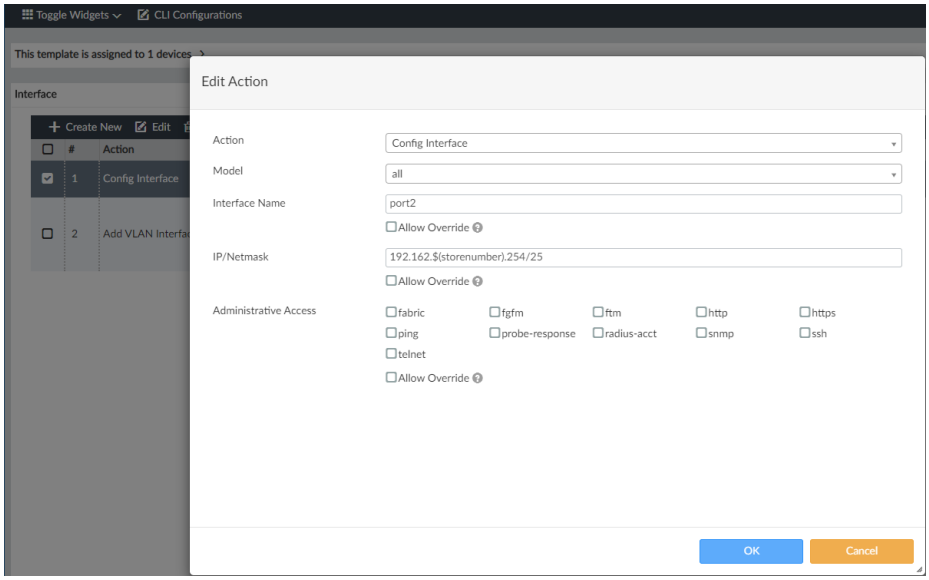
Using meta field variables

You can use metadata variables in interface templates.

For information about creating a meta field, see ADOM-level metadata variables on page 557.

To use meta variables in interface templates:

1. Go to *Device Manager* > *Provisioning Templates* > *System Templates*.
2. Edit the *default* template.
3. Display the *Interface* widget by clicking *Toggle Widgets* and enabling *Interface*.
4. In the *Interface* widget, create a new *Config Interface* action that uses the variable.
   a. In the *Interface* widget, click *Create New*.
   b. In the *Action* list, select *Config Interface*.
   c. In the *Model* list, select *all*.
   d. In the *Interface Name* list, type `port2`.
   e. In the *IP/Netmask* box, type the variable with the IP/netmask, such as `192.162.$(storenumber).254/25`, and click *OK*.
   Note that `$(storenumber)` is the metadata variable.



The action is created.

IPsec tunnel templates

IPsec templates are used to standardize IPsec tunnel configurations for consistency and scalability. Templates may be applied to one or more individual devices, or device groups. ADOM-level metadata variables are used to facilitate the templates being assigned to multiple FortiGates, and the tunnel interfaces may be mapped to normalized interfaces to be used in firewall policies and SD-WAN configuration.

This topic includes the following sections:

- Recommended IPsec templates on page 287.
- Creating new IPsec VPN templates on page 289
- Assigning IPsec VPN templates on page 291.
- Installing IPsec VPN configuration on page 291.
- Verifying IPsec template configuration status on page 292.
- Verifying IPsec VPN tunnel status on page 292.

- Un-assigning IPsec templates on page 292.
- IPsec tunnel template example on page 293.

Recommended IPsec templates

FortiManager includes recommended IPsec templates that come preconfigured with FortiManager best practices recommendations for use within your environment. These templates can be used to simplify deployment of SD-WAN interconnected sites or to create IPsec VPN for FortiGate devices.

Once a new IPsec template has been created from a recommended template, it can be edited, deleted, and/or cloned.

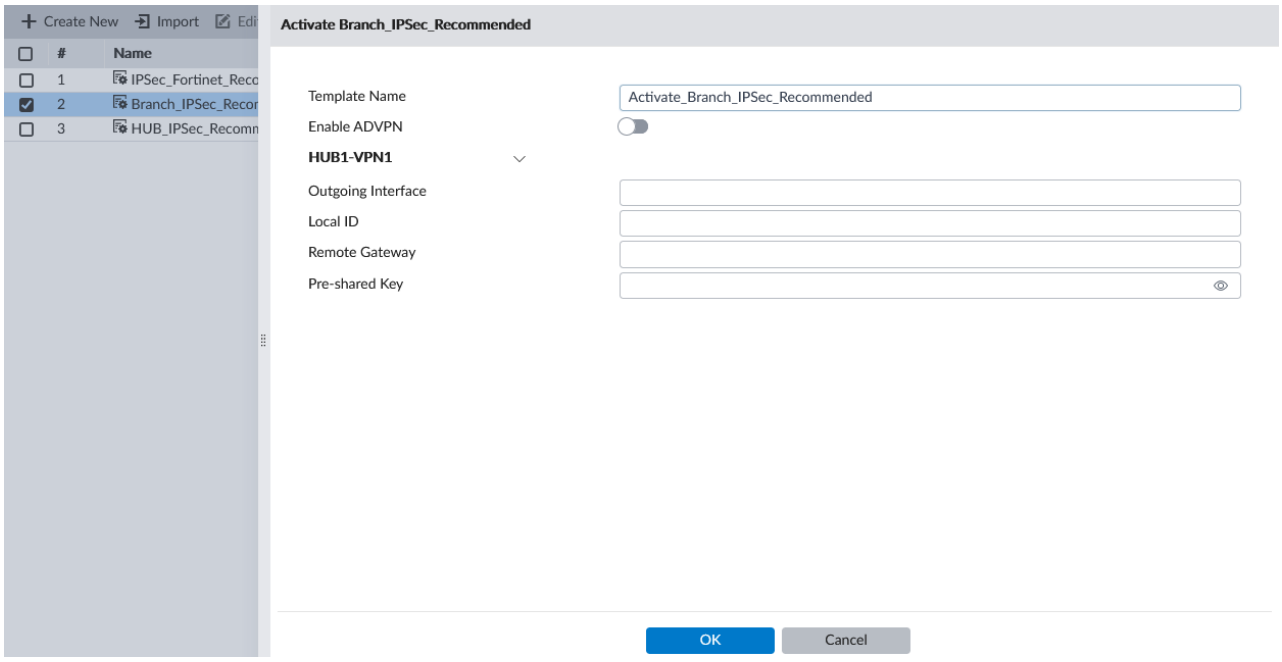
ADOM-level metadata variables can be used when configuring a recommended template's required fields to ensure that fields like *Local ID* are unique when the template is assigned to multiple devices. See ADOM-level metadata variables on page 557.

The following IPsec recommended templates are available.

Template Name	Description
HUB_IPSec_Recommended	This template was created for use with the SD-WAN provisioning template. The wizard prompts for input expected for HUB IPsec tunnels used by the SD-WAN template. The template assumes dialup clients by selecting *Dynamic* for *Remote Devices*.
Branch_IPSec_Recommended	Fortinet's recommended template for IPSec branch device configurations. The wizard prompts for the remote gateway (HUB) and requests a local ID to facilitate multiple tunnels for use in SD-WAN.
IPSec_Fortinet_ Recommended	Fortinet's recommended template for IPSec configurations. Unlike the HUB and Branch templates above, this template does not make assumptions about the function of the assigned device/group.

To use a default IPsec template in your environment:

1. Go to *Device Manager* > *Provisioning Templates* > *IPsec Tunnel Templates*.
2. Select a recommended template, and click *Activate* in the toolbar.
3. Enter configuration details specific to your environment.



4. Click *OK* to save your changes.
   A new template is created in the template list based on the recommended template you selected and the configuration details provided.
5. (Optional) Edit the template to view or change the automatically configured settings.



Any field with a magnifying glass indicates that a metadata variable may be used. See ADOM-level metadata variables on page 557.

6. (Optional) Once a template has been created, it can be added to a template group. SeeTemplate groups on page 274
7. Assign the new template (or template group) to one or more managed devices or device groups.
8. Install the changes.

To create a HUB_IPSec_Recommended template:

1. Activate the *HUB_IPSec_Recommended* template.
2. Enter the following requested information.

Template Name	Enter a name for the template.
Enable ADVPN	Optionally, toggle this setting to enable Auto Discovery VPN (ADVPN).
Outgoing Interface	Enter the outgoing interface. This is the physical port that the branch devices will connect to.
IPv4 Start IP	Enter the first usable IP address in the range.
IPv4 End IP	Enter the last usable IP address in the range.
IPv4 Netmask	Enter the IPv4 netmask.

Pre-shared Key	Enter the pre-shared key.

3. Click *OK* to create the template.

To create a Branch_IPSec_Recommended template:

1. Activate the *Branch_IPSec_Recommended* template.
2. Enter the following requested information.

Template Name	Enter a name for the template.
Enable ADVPN	Optionally, enable or disable Auto Discovery VPN (ADVPN).
Outgoing Interface	Enter the outgoing interface. This is the physical port that the branch devices will use to connect to the HUB.
Local ID	Enter a Local ID. This is used by the HUB to identify the connecting device.
Remote Gateway	Enter the IP address of the HUB interface that the Branch will connect to.
Pre-shared Key	Enter the pre-shared key.

3. Click *OK* to create the template.

To create an IPSec_Fortinet_Recommended template:

1. Activate the *IPSec_Recommended* template.
2. Enter the following requested information.

Template Name	Enter a name for the template.
Outgoing Interface	Enter the outgoing interface. This is the physical port that the branch devices will connect to.
Remote Gateway	Enter the IP address of the destination device's interface that the assigned FortiGates will connect to.
Pre-shared Key	Enter the pre-shared key.

3. Click *OK* to create the template.

Creating new IPsec VPN templates

If you prefer to input all the settings required for a VPN tunnel, you may create a new IPsec VPN template as follows.

To create an IPsec VPN template:

1. Go to *Device Manager > Provisioning Templates > IPsec Tunnel Templates*.
2. Click *Create New* from the toolbar. The *Create New IPsec Tunnel Template* dialog appears.
3. Enter a *Name* for the template, optionally add a description, then click *OK*.
4. Click *Create New* to create a new IPsec tunnel.



Any field with a magnifying glass indicates that an ADOM-level metadata variable may be used. See ADOM-level metadata variables on page 557.

Setting	Value/Description
Tunnel Name	Enter the name of the IPsec tunnel.
Routing	*Automatic*: Static routes to remote subnet will be created. See Remote Subnet on page 290. *Manual*: Routes will not automatically created.
Remote Device	*IP Address*: Select when you know the IP address of the VPN tunnel destination. *Dynamic DNS*: Select when you will provide a FQDN for the VPN tunnel destination. *Dynamic*: Select when the remote device will be dial-up clients where their IP address may vary or cannot be determined at the time of configuration.
Remote Gateway (IP Address)	Enter the IP address of the VPN tunnel destination. Only available when *IP Address* is selected.
Remote Gateway (FQDN)	Enter the FQDN of the VPN tunnel destination. Only available when *Dynamic DNS* is selected.
IPv4 Start IP	Enter the first usable IP address assigned to connecting dial-up devices.
IPv4 End IP	Enter the last usable IP address assigned to connecting dial-up devices.
IPv4 Netmask	Define the netmask for the IP addresses assigned to connecting dial-up devices.
Outgoing Interface	Define the interface used to establish the VPN tunnel.
Local ID	If there are several dialup IPsec VPN tunnels configured on the same interface, specify a Local ID for the dial-up client's peer ID to match.
Network Overlay	Toggle on to provide a network ID. Distinct network overlay IDs are required to establish multiple IPsec VPN tunnels between the same two FortiGate IP addresses.
Remote Subnet	Enter one or more remote subnets, with netmask. This field is available when *Automatic* routing is selected. This subnet is used to generate a static route.
Proposal	Define the cipher suites offered when negotiating the VPN tunnel settings.
FEC Health Check	If FEC is to be used, this health check server allows the FortiGate to assess the link quality and adaptively increase redundancy levels as the link quality or throughput changes.
Authentication Method	*Pre-shared Key*: Alphanumeric key used for device authentication. *Signature*: Select a certificate to be used for authentication, including the Peer Certificate CA.

Setting	Value/Description
Tunnel Interface Setup	Configure the IP or remote IP for the tunnel to use in the IPsec template.
Phase 2 Interface	Click *Create New* to define the parameters for the phase 2 interface.
Advanced Options	Expand to access and set a number of advanced options.

5. Click *OK* to save the settings. The IPsec template is created and ready to be assigned to devices.

Assigning IPsec VPN templates

Before they can be installed, IPsec templates must be assigned to devices.

To assign an IPsec VPN template to a device or device group:

1. Go to *Device Manager > Provisioning Templates > IPsec Tunnel Templates*.
2. Click on the template name from the tree menu at the left.
3. Click *Assign to Device/Group* from the toolbar.
4. Select the appropriate devices from the list of devices in the *Available Entries* section, and move them to the *Selected Entries* section.
   Available device groups will also be displayed in the *Available Entries* list.
5. Click *OK*. The IPsec template is assigned to the selected devices.

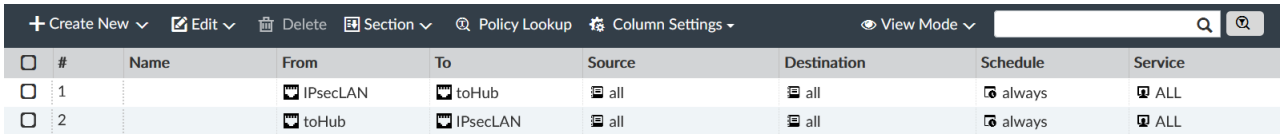
Installing IPsec VPN configuration

After the IPsec template is assigned to devices, it still must be installed to push the configuration to the devices.

If a template is assigned but not installed, a *Caution* icon displays before the template name in the *IPsec Template* column. You must install the IPsec VPN configuration and firewall policies to the devices for the IPsec template to push through all the settings.

To install IPsec VPN configuration and firewall policies to a device:

1. Go to *Policy & Objects > Policy Packages > Firewall Policy*.
2. Click *Create New* from the toolbar. The *Create New Firewall Policy* pane appears.
3. Create two firewall policies for traffic between the normalized interface and *HQ* site.

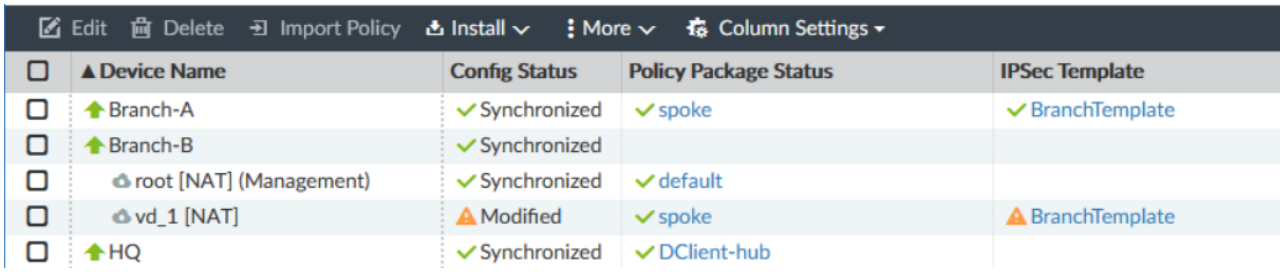


4. Click *Install > Install Wizard* from the toolbar. The *Install Wizard* dialog appears.
5. Continue with the policy installation on the appropriate devices.
6. Click *Finish*. The firewall policies are installed and the IPsec VPN configurations are pushed to the devices.

Verifying IPsec template configuration status

To verify IPsec template configuration status:

1. Go to *Device Manager* > *Device & Groups* > *Managed Devices*.
2. Click *Column Settings* from the toolbar and select *IPsec Template*. The *IPsec Template* column appears in the table.



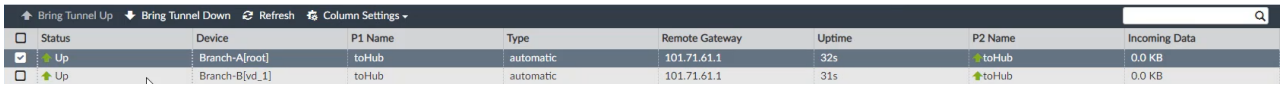
A green checkmark next to the template name in the *IPsec Template* column indicates that the template is synchronized.

A yellow triangle caution icon indicates that the template is modified.

Verifying IPsec VPN tunnel status

To verify IPsec VPN tunnel status:

1. Go to *VPN Manager* > *Monitor*.
2. Check the tunnel status from the *Status* column. The tunnels may be *Down*.
3. Select the tunnels with a *Down* status and click *Bring Tunnel Up* from the toolbar.
4. Click *OK* to confirm in the *Bring Tunnel Up* dialog.
5. Click *Refresh* from the toolbar to verify that the tunnels now have an *Up* status.



Un-assigning IPsec templates

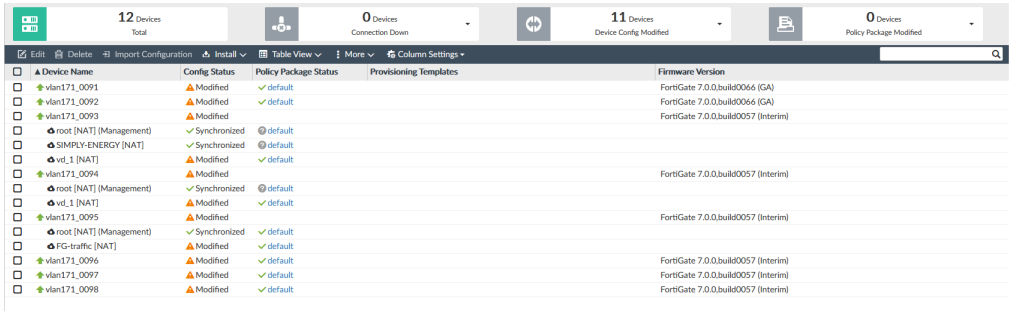
When you un-assign an IPsec template from a device, FortiManager modifies the configuration for the affected devices. When you install the modified configuration to devices, FortiManager automatically uninstalls the configuration (phase1 and phase2 interfaces) generated by the IPsec template from the devices.



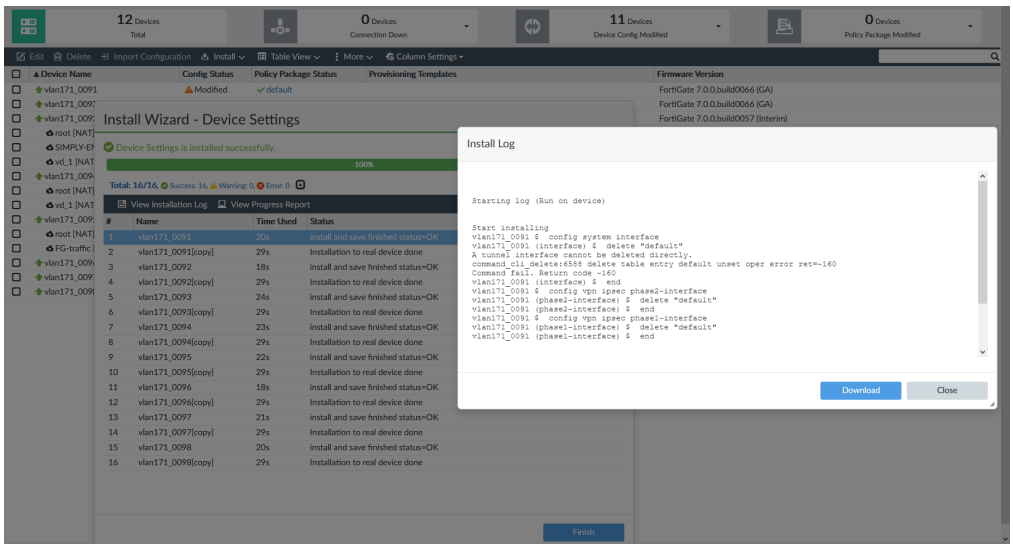
FortiManager does not remove dependencies, such as routing, policies, and normalized interfaces. You must manually remove those dependencies. For example, if the VPN tunnel is being used in a policy, you must edit the policy to manually remove the VPN tunnel interface from the source or destination interface.

To un-assign IPsec templates:

1. Go to *Device Manager* > *Provisioning Templates* > *IPsec Tunnel Templates*.
2. Select the template, and click *Assign to Device*.
   The *Assign to Device* dialog box is displayed.
3. In the *Selected Entries* list, select the device and click < to move the device to the *Available Entries* list.
4. Click *OK*.
   The IPsec template is un-assigned from the device, and the configuration status changes to *Modified*.
5. Go to *Device Manager* > *Device & Groups*, and select *Table View* to view the configuration status.
   In the following example, the IPsec template was removed from several devices, and the *Config Status* displays *Modified*:



6. Install the modified device configuration to remove the IPsec template configuration from the device.
   You can view the changes in the *Install Log*. For example, the *Install Log* for the device named *vlan171_0091* shows that FortiManager removed phase1 and phase2 interface settings.

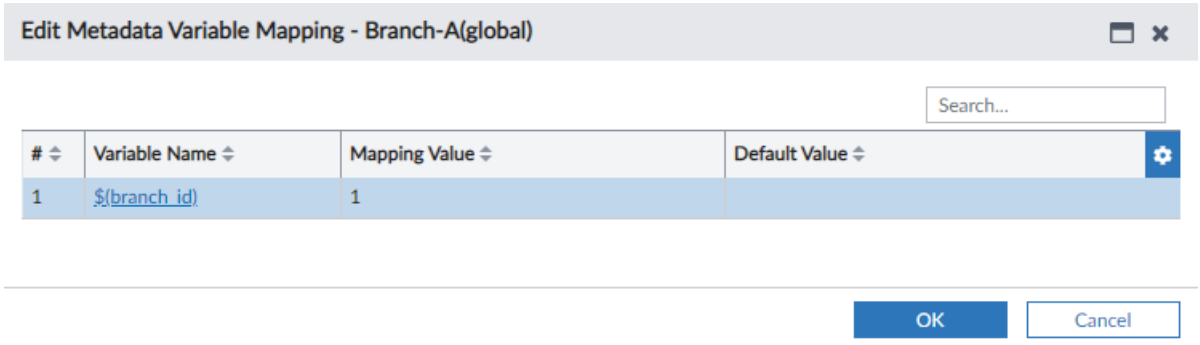


IPsec tunnel template example

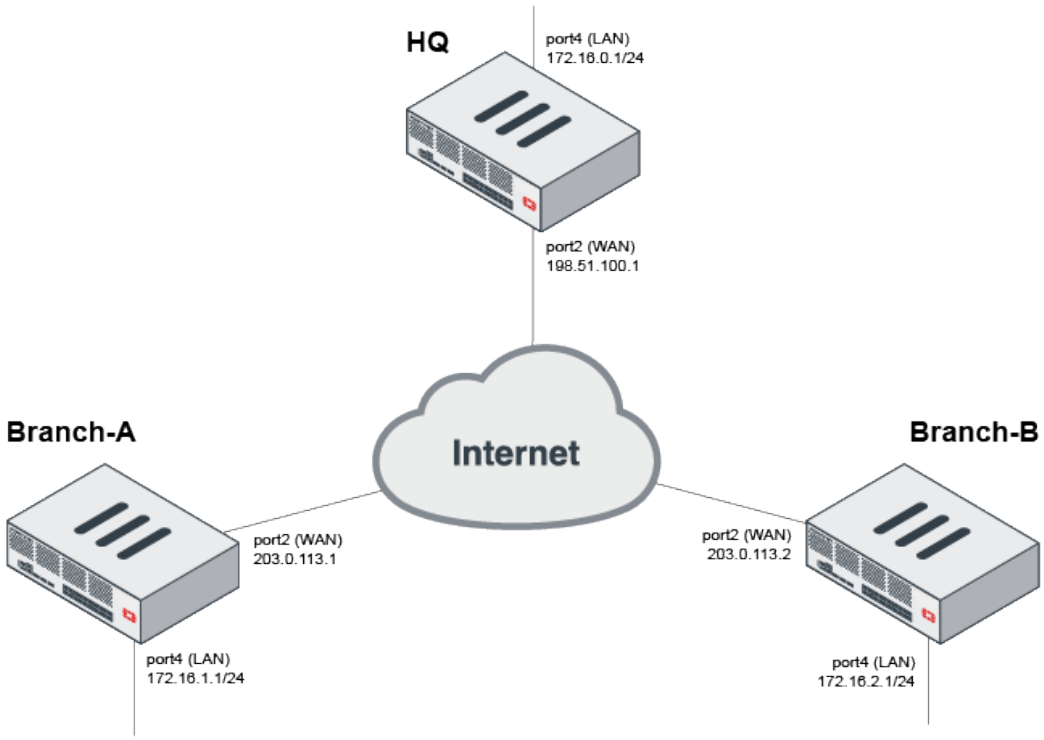
The following example demonstrates the IPsec template features with the following assumptions:

- All three FortiGates are added in FortiManager without prior configuration.
  - The branch FortiGates are added to a *Branches* device group. See Adding custom device groups on page 148.

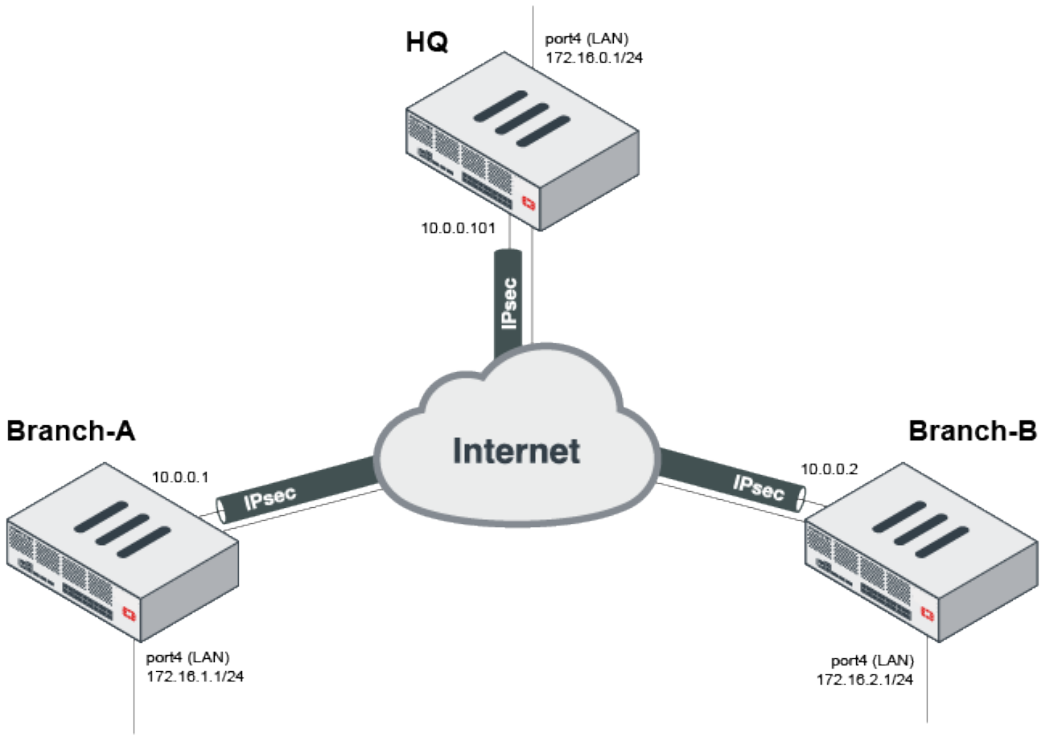
    - The hub *HQ* device is added to a *HUB* device group.
- Each FortiGate uses *port2* as the WAN and *port4* as LAN.
    - These names are added as aliases.
- The WAN interface is configured as the default gateway (0.0.0.0/0) with a static route (you may use DHCP to receive the default route).
- Only the necessary policies for the VPN connections are specified.
    - *Branch* FortiGates use the *Branches* policy package.
    - *HQ* FortiGate uses the *HUB* policy package.
- Static routes are used to direct traffic over the VPN tunnels.
- Auto Discovery VPN (ADVPN) is not configured.
    - ADVPN may be enabled in the *HUB_IPsec_Recommended* or *BRANCH_IPsec_Recommended* recommended templates during activation, or it may be enabled in advanced settings after activation in any IPsec template.
    - See ADVPN in the FortiGate Administration Guide for more details.
- Policies only allow traffic from the branches to the hub.
    - You may wish to create policies in each *Branch* and *HUB* policy package to allow traffic from the hub to the branches.
- A metadata variable `branch_id` is used in the configuration. See ADOM-level metadata variables on page 557.
    - The branch_id allows you to dynamically configure each branch's LAN subnet as follows:
        - `192.168.branch_id.0` = 192.168.**1**.0, 192.168.**2**.0, and so on.
- Set branch_id value for each branch
    - *Branch-A*: `1`.
    - *Branch-B*: `2`.



- The below topology outlines the connected networks for each FortiGate.



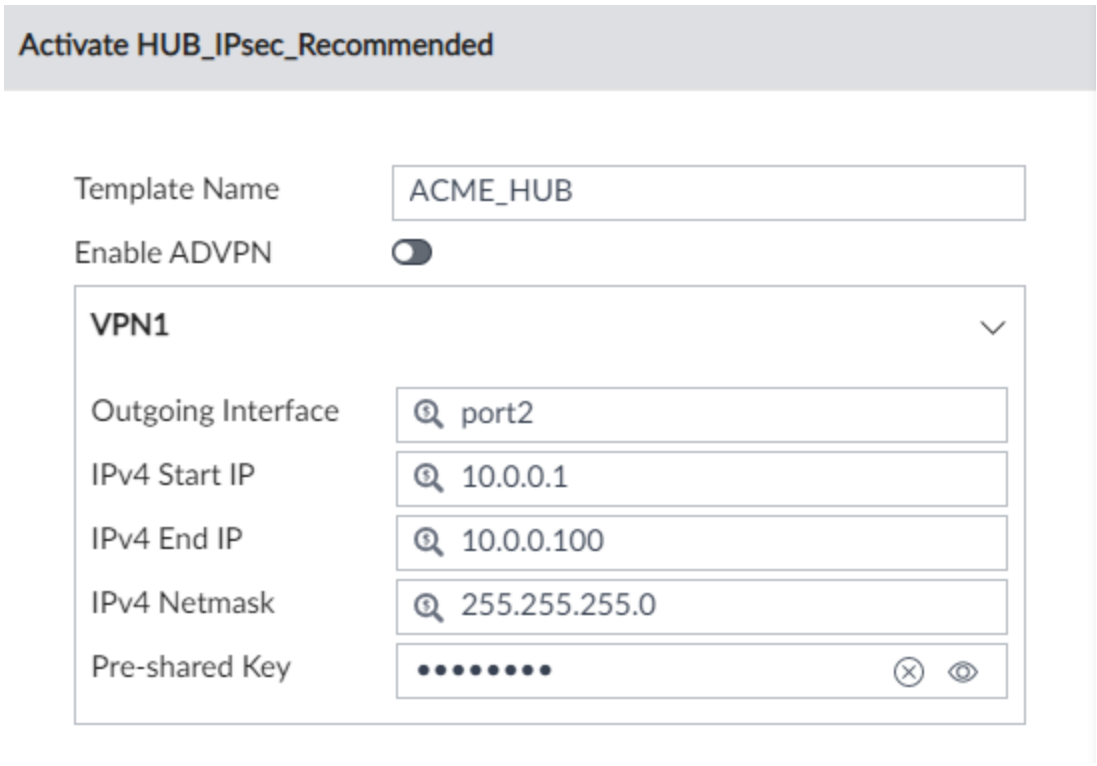
Once configured, the overlay will look like the following topology.



Defining the hub template

1. Go to *Device Manager* > *Provisioning Templates* > *IPsec Tunnel Templates*.
2. Right click *HUB_IPsec_Recommended* and select *Activate*.
3. Provide a template name and fill out the *VPN1* section as follows:

Field	Value
Outgoing Interface	`port2`
IPv4 Start IP	`10.0.0.1`
IPv4 End IP	`10.0.0.100`
IPv4 Netmask	`255.255.255.0`
Pre-shared Key	Enter a pre-shared key.



IPv4 Start IP and *IPv4 End IP* specify the range of IP addresses that connecting branches will use for their IPsec tunnel IP. These IP addresses can be adjusted to fit your needs. The current scheme only scales to 100 branches.

4. Click *OK* to save.
5. Edit the newly created template, then edit the *VPN1* tunnel.
   a. Change *Routing* from *Manual* to *Automatic*
      i. Under *Remote Subnet*, enter `172.16.0.0/255.255.0.0`.
   b. Set the *Tunnel Interface Setup* to:
      - *IP*: `10.0.0.101/32`.
      - *Remote IP*: `10.0.0.254/24`.

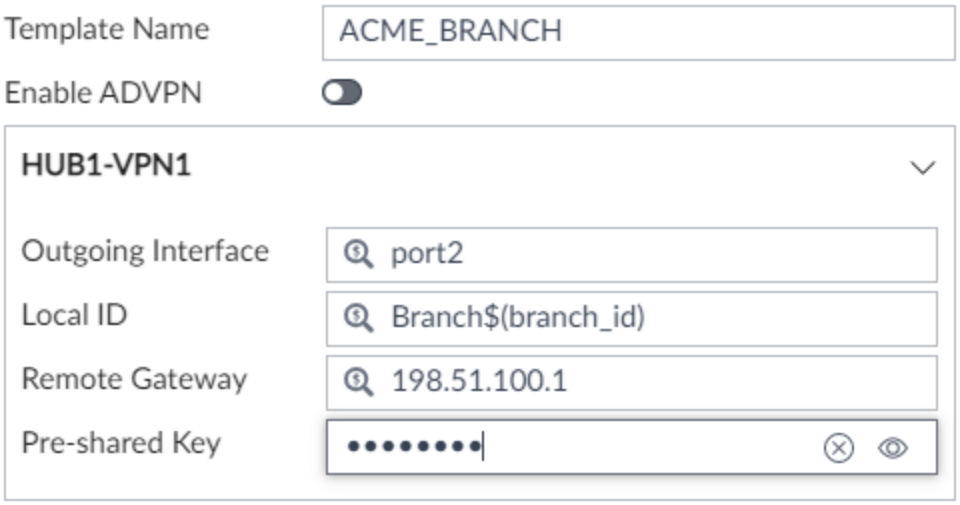
      These settings configure the *HQ* FortiGate's IPsec interface. The same can be done for the branch FortiGates. However, this example uses mode-config to assign addresses using the IPv4 range shown in the image above.
6. Click *OK* to save.

Defining the branch template

1. Go to *Device Manager > Provisioning Templates > IPsec Tunnel Templates*.
2. Right click *BRANCH_IPsec_Recommended* and click *Activate*.
3. Provide a template name and fill out the *HUB1-VPN1* section as follows:

Field	Value
Outgoing Interface	`port2`
Local ID	`Branch$(branch_id)`
Remote Gateway	Enter the hub WAN IP address.
Pre-shared Key	Enter a pre-shared key.

Activate BRANCH_IPsec_Recommended

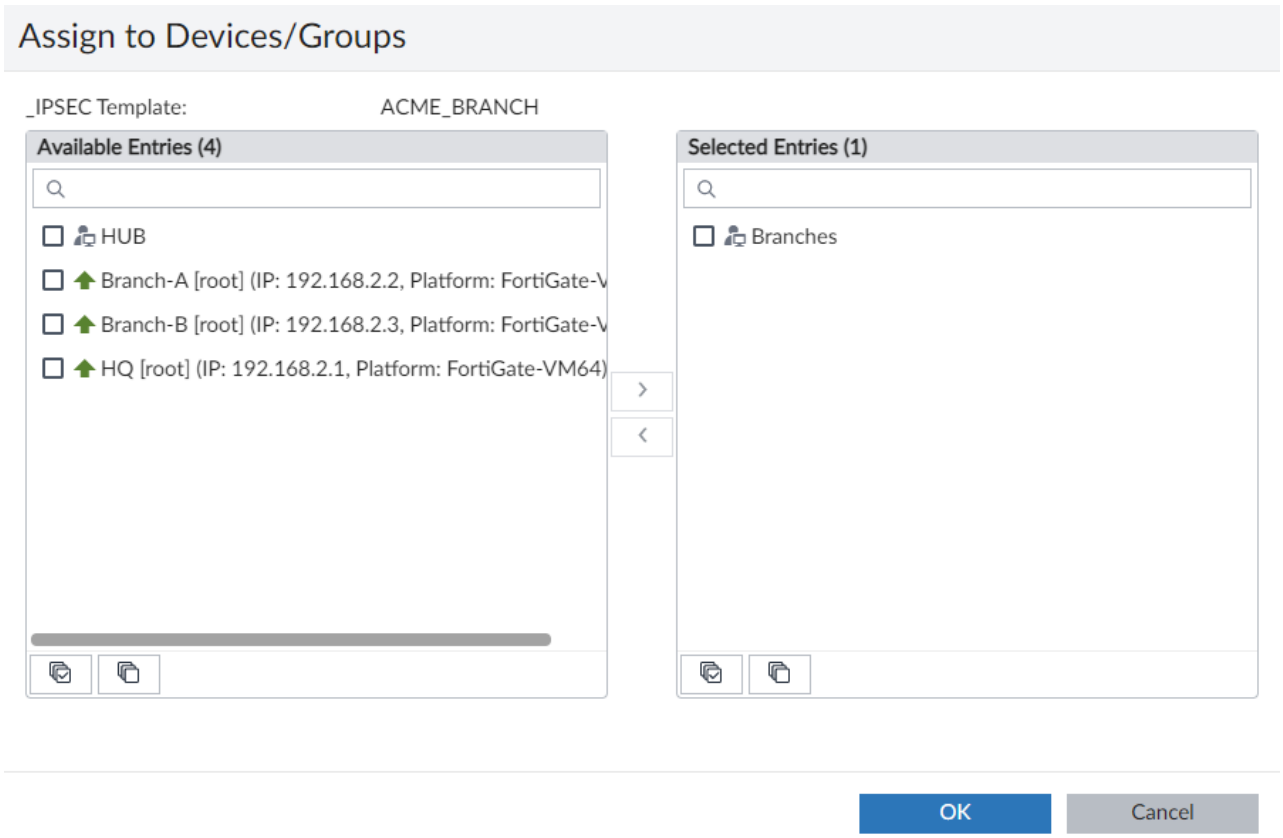


4. Click *OK* to save.
5. Edit the newly created template, then edit the *HUB1-VPN1* tunnel.
6. Change *Routing* from *Manual* to *Automatic*
7. Under *Remote Subnet*, enter `172.16.0.0/255.255.255.0`.
8. Click *OK* to save.

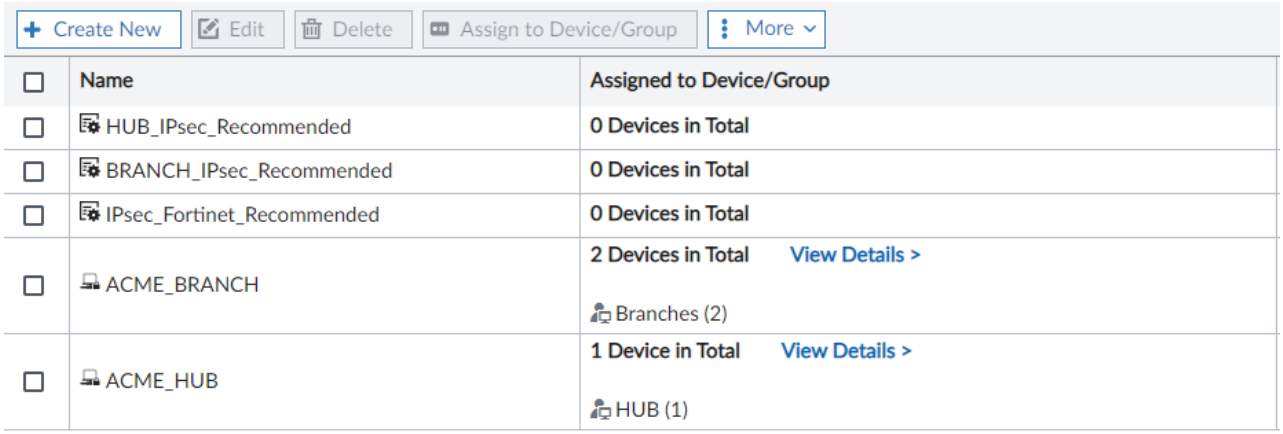
Assigning templates to devices and groups

To assign templates to devices:

1. In *Device Manager* > *Provisioning Tempates* > *IPsec Tunnel Templates*, Right click `ACME_BRANCH` and click *Assign to Devices/Groups*.
2. Select `Branches` and move it to *Selected Entries*, then click *OK*.



3. Repeat the same procedure to assign the HUB device group to ACME_HUB.



Creating and installing the policy package and IPsec template

In order to establish an IPsec tunnel between the FortiGate devices, define policies to permit the traffic. When you install the policy package, the device settings (including provisioning templates) are installed at the same time.

To create and install the policy package and IPsec template:

1. Map VPN interfaces to objects.
2. Map LAN interfaces to LAN object.
3. Map WAN interface to WAN object.
4. Define the LAN address objects.
5. Create the branch policy.
6. Create the HUB policy.
7. Install the policy packages.

To map VPN interfaces to objects:

1. In *Policy & Objects > Normalized Interface*, click *Create New*.
2. Enter a name for the normalized interface.
3. Under *Per-Device Mapping*, map the hub FortiGate as follows:
   a. Click *Create New*.
   b. In *Mapped Device*, select the hub FortiGate.
   c. In *Mapped Interface Name*, select *VPN1*.
   d. Click *OK* to save.
4. Under *Per-Device Mapping*, map the two branch FortiGates as follows:
   a. Click *Create New*.
   b. In *Mapped Device*, select the first branch FortiGate.
   c. In *Mapped Interface Name*, select *HUB1-VPN1*.
   d. Click *OK* to save.
   e. Repeat for the other branch FortiGate.
5. Enter a *Change Note* and click *OK* to save.

To map the LAN interfaces to a LAN object:

1. In *Policy & Objects > Normalized Interface*, click *Create New*.
2. Under Per-Device Mapping, click *Create New*.
3. Name it `LAN`.
   a. In *Matched Device*, select the first branch FortiGate.
   b. In *Mapped Interface Name*, enter `port4`.
   c. Click *OK* to save.
4. Repeat for the other branch and the hub FortiGate.
5. Enter a *Change Note* and click *OK* to save.

To map the WAN interface to a WAN object:

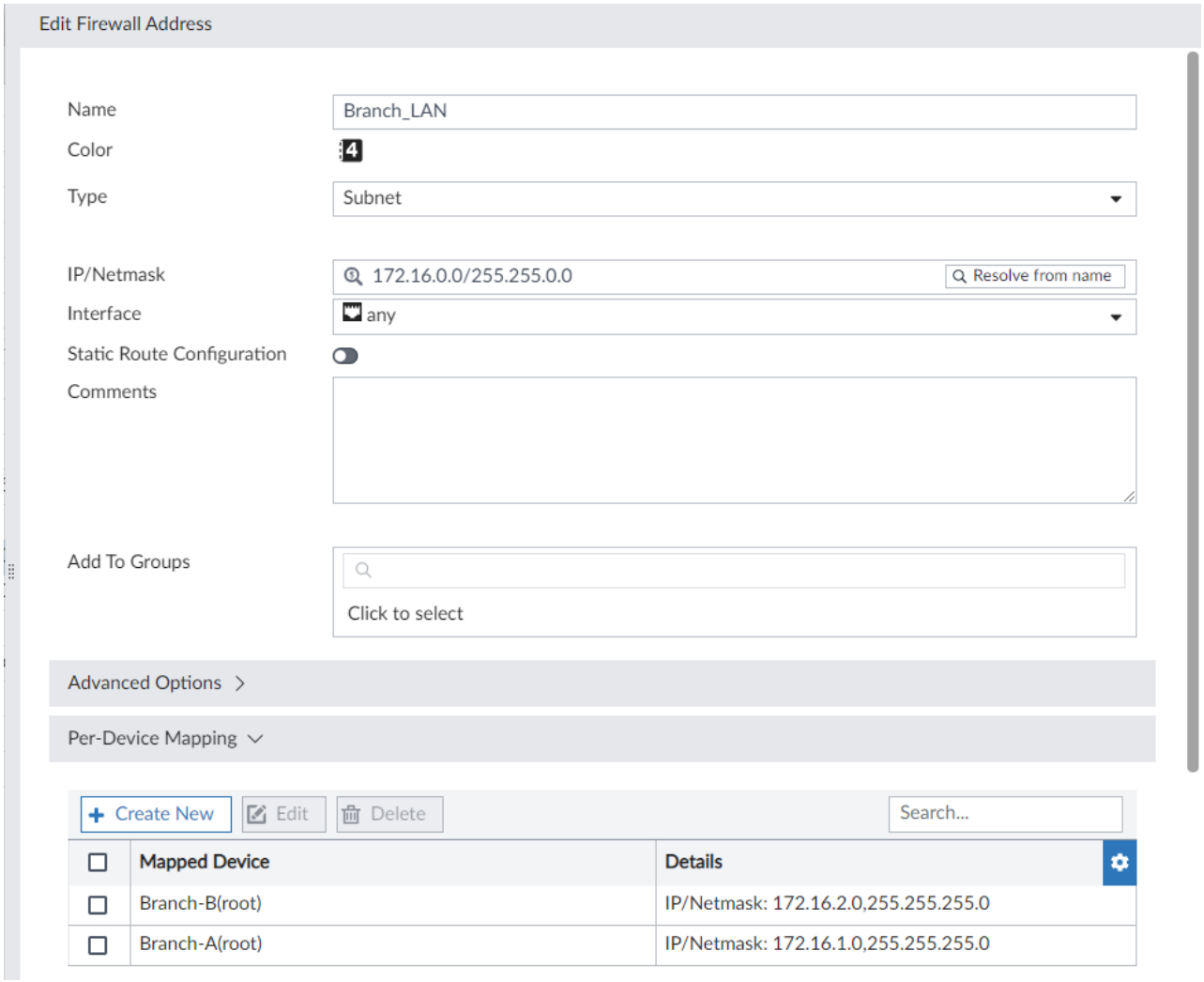
1. In *Policy & Objects > Normalized Interface*, click *Create New*.
2. Under *Per-Platform Mapping*, click *Create New*.
3. Name it `WAN`.
   a. In *Matched Platform*, select your platform (if consistent) or select all.
   b. In *Mapped Interface Name*, enter `port2`.

c. Click *OK* to save.

4. Enter a *Change Note* and click *OK* to save.

To define the LAN address objects:

1. In *Policy & Objects* > *Addresses*, go to *Create New* > *Address*.
2. Repeat this procedure for each of the following address objects:
   - Branch_LAN
     - *Name*: `Branch_LAN`
     - *IP/Netmask*: `172.16.0.0/16`
     - *Per-Device Mapping*:
       - Branch-A: `172.16.1.0/24`
       - Branch-B: 172.16.2.0/24
   - *HQ_LAN*
     - *Name*: HQ_LAN
     - *IP/Netmask*: 172.16.0.0/24
   - Enter a *Change Note* and click *OK* to save.

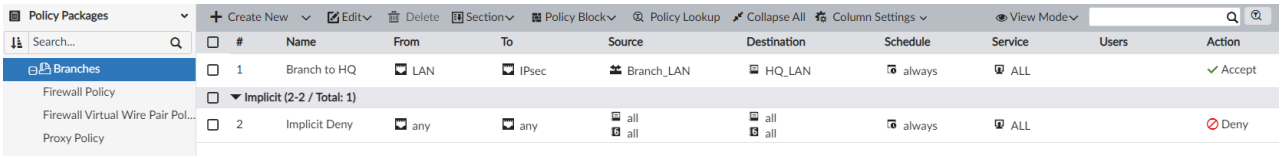


To create the branch policy:

1. In *Policy Packages*, select the *Branches* policy package and click *Create New*.
2. Set the following values:

Field	Value
Name	Branch to HQ
Incoming Interface	LAN
Outgoing Interface	IPsec
IPv4 Source Address	Branch_LAN
IPv4 Destination Address	HQ_LAN
Action	Accept

3. Click *OK* to save.

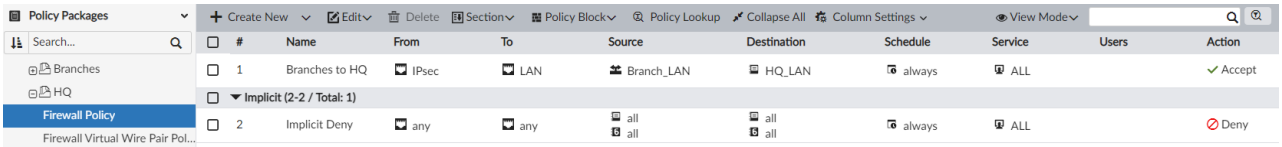


To create the HUB policy:

1. In *Policy Packages*, select the *HUB* policy package and click *Create New*.
2. Set the following values:

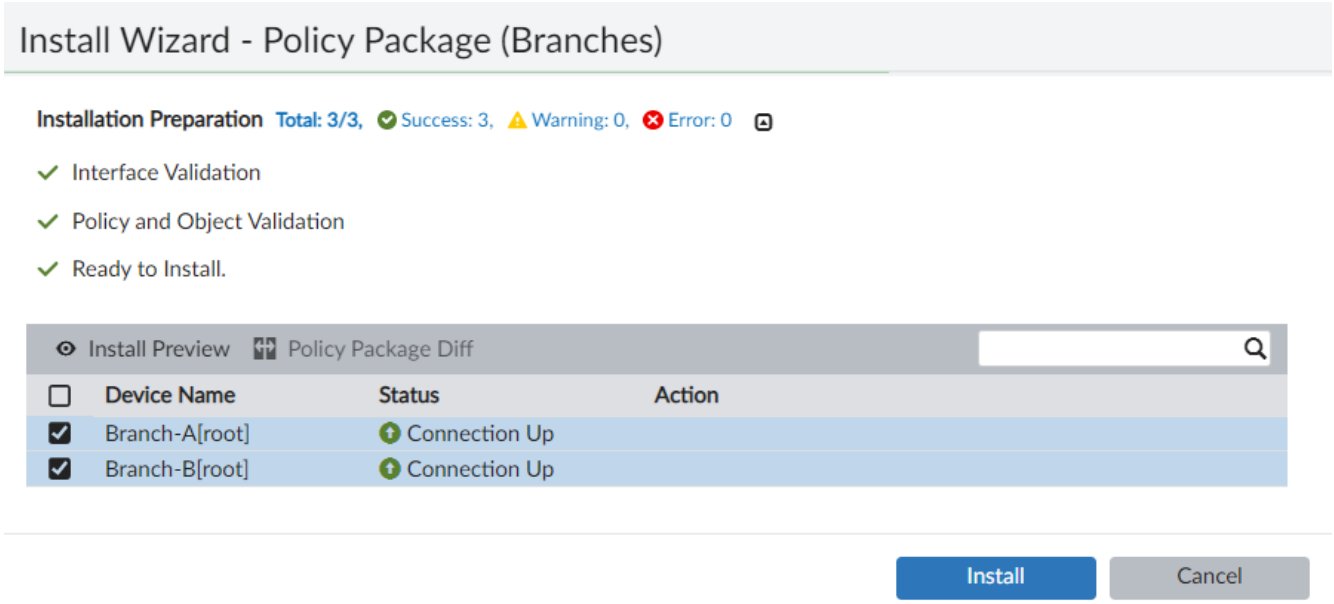
Field	Value
Name	Branches to HQ
Incoming Interface	IPsec
Outgoing Interface	LAN
IPv4 Source Address	Overlay tunnels
IPv4 Destination Address	HQ_LAN
Action	Accept

3. Click OK to save.



To install the policy packages:

FortiManager can only install one policy package at a time, so install each policy package in turn. The IPsec tunnel template configuration will be installed along with the policy package.

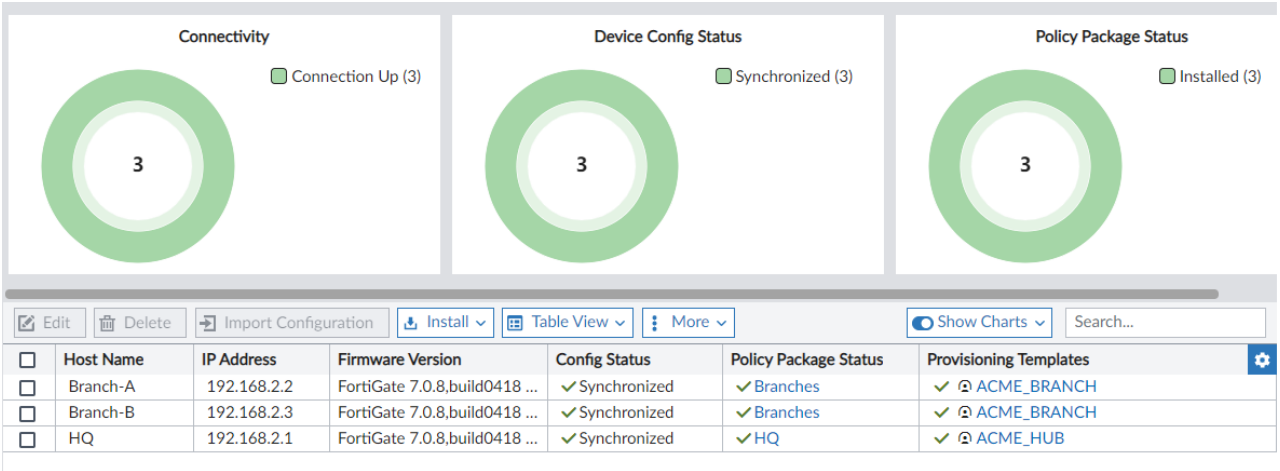


For more information about installing policies and policy packages, see Install a policy package on page 419.

Verifying VPN template and tunnel status

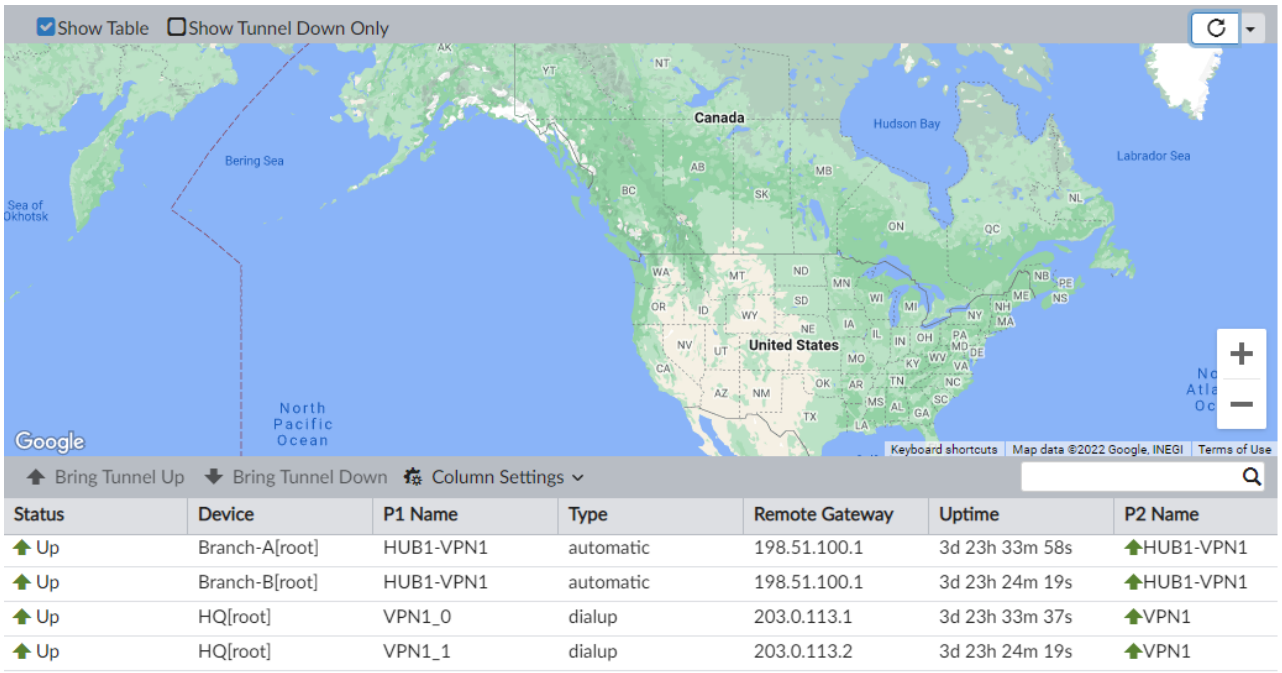
To verify the template installation status:

1. Go to *Device Manager* > *Device & Groups*. The list of *Managed FortiGate* devices is displayed.
2. Verify that *Config Status*, *Policy Package Status*, and *Provisioning Templates* all display a green checkmark to indicate that the configuration is synchronized between FortiManager and FortiGate.



To verify the VPN tunnel status:

1. Go to *Device Manager* > *Monitors* > *VPN Monitor*. A map displays.
2. Enable *Show Table* to display the table of tunnels below the map.
3. Verify that the *Status* is *Up* for each tunnel.



Status	Device	P1 Name	Type	Remote Gateway	Uptime	P2 Name
Up	Branch-A[root]	HUB1-VPN1	automatic	198.51.100.1	3d 23h 33m 58s	HUB1-VPN1
Up	Branch-B[root]	HUB1-VPN1	automatic	198.51.100.1	3d 23h 24m 19s	HUB1-VPN1
Up	HQ[root]	VPN1_0	dialup	203.0.113.1	3d 23h 33m 37s	VPN1
Up	HQ[root]	VPN1_1	dialup	203.0.113.2	3d 23h 24m 19s	VPN1

The devices are missing in this image due to the WAN IP addresses used. Because they are not public addresses (TEST-NET-2 and TEST-NET-3 are used, see RFC 5737), FortiManager cannot place them on the map.

SD-WAN templates

You can use SD-WAN templates to configure SD-WAN for one or more devices. When you assign SD-WAN templates to a device, you are using SD-WAN central management.

If you want to use SD-WAN per-device management, do not assign SD-WAN templates to devices, and see Device DB - Network SD-WAN on page 217.

SD-WAN templates help you do the following:

- Deploy a single SD-WAN template from FortiManager across multiple FortiGate devices.
- Perform a zero-touch deployment without manual configuration locally at the FortiGate devices.
- Roll out a uniform SD-WAN configuration across your network.
- Eliminate errors in SD-WAN configuration across multiple FortiGate devices since the SD-WAN template is applied centrally from FortiManager.
- Monitor network Performance SLA across multiple FortiGate devices centrally from FortiManager.
- Monitor the performance of your SD-WAN with multiple views.

If you are implementing overlays (IPsec tunnels) in your SD-WAN solution, you may consider SD-WAN Overlay Templates to automate and simplify the process using Fortinet's recommended IPsec and BGP templates. See SD-WAN overlay templates on page 327.

Using SD-WAN templates consists of the following steps:

1. Create an SD-WAN template. See SD-WAN templates on page 305.
2. Assign the SD-WAN templates to FortiGate devices and device groups. See Assign SD-WAN templates to devices and device groups on page 318.
3. Install device settings using the *Install Wizard*. See Install device settings only on page 183.
   Templates should be executed in the following order:
   a. Interface template
   b. IPsec template
   c. SD-WAN template
4. Go to *SD-WAN* > *Monitor* to monitor the FortiGate devices. See SD-WAN Monitor on page 386.



The SD-WAN template takes effect on the FortiGate device only after it is installed using the *Install Wizard*. After installing the SD-WAN template on the FortiGate device, changing settings in *SD-WAN*, *Performance SLA*, or *SD-WAN Rules* locally on the FortiGate device will result in the SD-WAN template on the FortiManager being out of sync with the FortiGate device. You must configure the same settings on the FortiManager SD-WAN template, and install it again by using the *Install Wizard* to be in sync with the settings on the FortiGate.



Some FortiGate model devices include a default policy to allow initial management access to the device using a specified interface.

As SD-WAN members may not use interfaces that are referenced directly in firewall policies, you must remove this reference by deleting the policy before installing the SD-WAN template.

This can be done manually through the CLI or GUI, or by installing a new policy package to the device that does not contain the default policy.

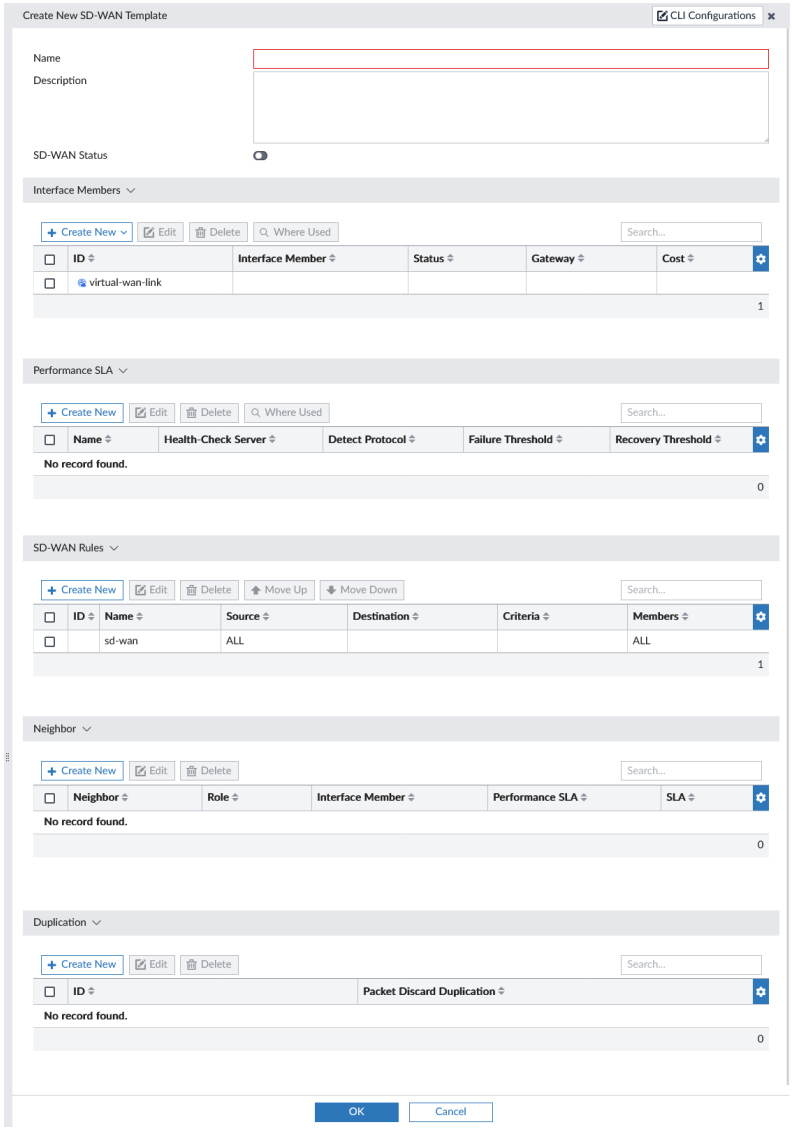
SD-WAN templates

You can create SD-WAN templates, and assign the templates to one or more devices.

To create a new SD-WAN template:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager* > *Provisioning Templates* > *SD-WAN Templates*.

3. Click *Create New* in the content pane toolbar. The *Create New SD-WAN Template* page opens.



4. In the *Name* box, type a name for the template.
5. Complete the following sections:
   a. In the *Interface Members* section, create SD-WAN zones and interface members. See Zones and interface members on page 307.
   b. In the *Performance SLA* section, use the defaults, or create new performance SLA. See Performance SLA on page 310.
   c. In the *SD-WAN Rules* section, create SD-WAN rules. See SD-WAN rules on page 312.
   d. (Optional) In the *Neighbor* section, create neighbors. See Neighbors on page 316.
   e. (Optional) In the *Duplication* section, configure packet duplication. See Duplication on page 317.
   f. (Optional) In the *Advanced Options* section, set advanced options.
   Hover the mouse over each advanced option to view a description of the option.
6. Click *OK*.
   The SD-WAN template is created.

To edit an SD-WAN template:

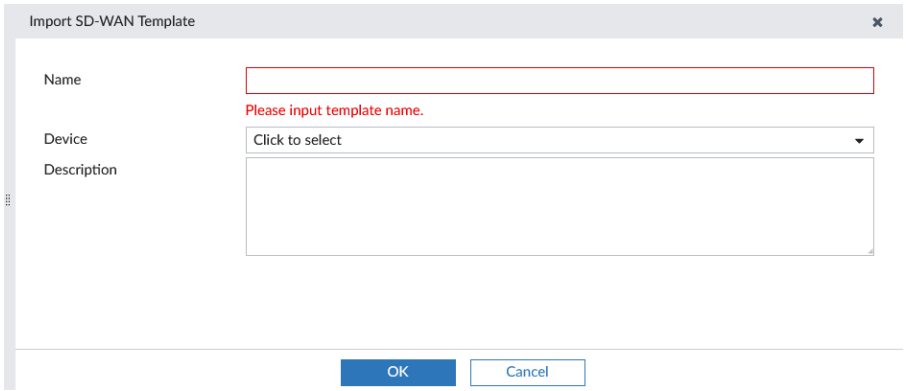
1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > Provisioning Templates > SD-WAN Templates*.
3. Double-click the template, or select the template, and click *Edit* in the toolbar. The *Edit* page opens.
4. Edit the template as required, and click *OK* to apply your changes.

To delete an SD-WAN template:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > Provisioning Templates > SD-WAN Templates*.
3. Select the template, and click *Delete* in the toolbar, or right-click the template and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the template or templates.

To import an SD-WAN template or templates:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > Provisioning Templates > SD-WAN Templates*.
3. Click *Import*. The Import SD-WAN templates screen is shown.



4. Configure the following settings and click OK:
   - Name - specify a name for the SD-WAN template.
   - Device - select the FortiGate device from where to select the SD-WAN template.
   - Description - optionally provide a description.

   The SD-WAN template is imported.



A prefix *Import* is automatically added to SD-WAN templates that are imported from the FortiGate devices.

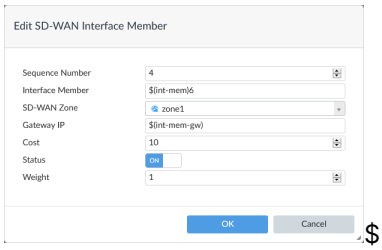
Zones and interface members

When creating an SD-WAN template, you can create SD-WAN zones and add interface members. Normalized interfaces are not supported for SD-WAN templates. You must bind the interface members by name to physical interfaces or VPN interfaces.

You can select SD-WAN zones as source and destination interfaces in firewall policies. You cannot select interface members of SD-WAN zones in firewall policies.

The default SD-WAN zone is named `virtual-wan-link`.

You can use meta fields of type *Device VDOM* for interface members and gateway IP addresses. The following example shows the *Interface Member* option and the *Gateway IP* option with meta fields:

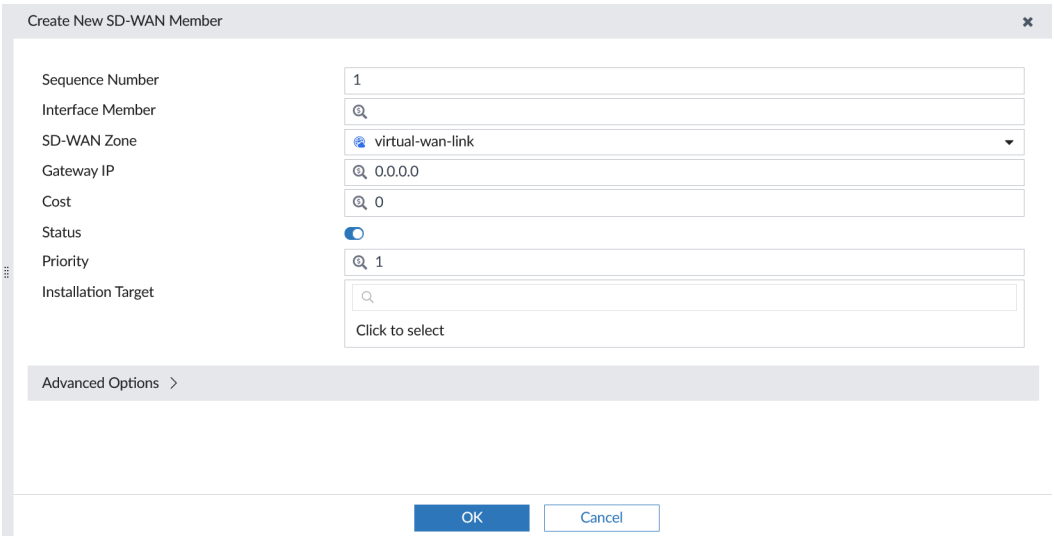


$

This topic describes how to create SD-WAN interface members. It also describes how to create SD-WAN zones and add interface members. It also describes how to edit and delete interface members.

To create SD-WAN interface members:

1. Go to *Device Manager* > *Provisioning Templates* > *SD-WAN Templates*.
   The SD-WAN templates are displayed in the content pane.
2. Double-click a template to open it for editing, or click *Create New* in the toolbar.
   The SD-WAN template opens.
3. In the *Interface Members* section, click *Create New* > *SD-WAN Member*. The *Create New SD-WAN Interface Member* page opens.



4. Enter the following information, then click *OK* to create the new WAN interface:

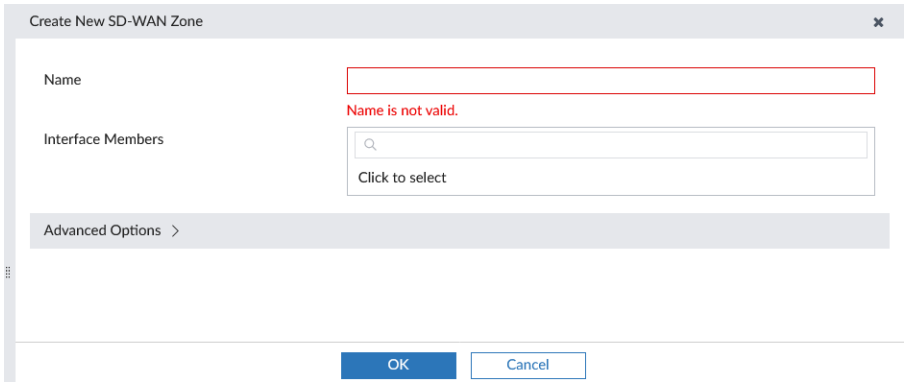
Sequence Number	Type a number to identify the sequence of the interface in the SD-WAN zone.
Interface Member	Type the name of the port. You can use meta fields for *Interface Members*.

SD-WAN Zone	Select the SD-WAN zone for the interface member.
Gateway IP	The default gateway for this interface. Usually the default gateway of the Internet service provider that this interface is connected to. You can use meta fields for *Gateway IP*.
Status	Toggle On to enable the interface member. Toggle Off to disable the interface member.
Installation Target	Click the box to specify installation targets for the SD-WAN member.

The interface member is added to the SD-WAN zone.

To create SD-WAN zones:

1. Go to *Device Manager > Provisioning Templates > SD-WAN Templates*.
   The SD-WAN templates are displayed in the content pane.
2. Double-click an SD-WAN template to open it for editing, or click *Create New* in the toolbar.
   The SD-WAN template opens.
3. In the *Interface Members* section, click *Create New > SD-WAN Zone*. The *Create New WAN Interface* page opens.



4. Enter the following information, and click *OK*:

Name	Type a name for the SD-WAN zone.
Interface Members	Click the box to select interface members for the zone.
Advanced Options	Expand to specify advanced options.

The SD-WAN zone with interface members is created.

To edit an interface member:

1. Go to *Device Manager > Provisioning Templates > SD-WAN Templates*.
   The SD-WAN templates are displayed in the content pane.
2. Double-click a template to open it for editing.
   The SD-WAN template opens.
3. In the *Interface Members* section, double-click an interface member to open it for editing.
   The *Edit SD-WAN Interface Member* page is displayed.
4. Edit the interface as required, and click *OK* to apply your changes.

To delete an interface member or members:

1. Go to *Device Manager > Provisioning Templates > SD-WAN Templates*.
   The SD-WAN templates are displayed in the content pane.
2. Double-click a template to open it for editing.
   The SD-WAN template opens.
3. Select the interface or interfaces from the list and click *Delete* in the toolbar, or right-click the interface and select *Delete*.
   A *Confirm Deletion* page is displayed.
4. Click *OK* in the confirmation dialog box to delete the interface or interfaces.

Performance SLA

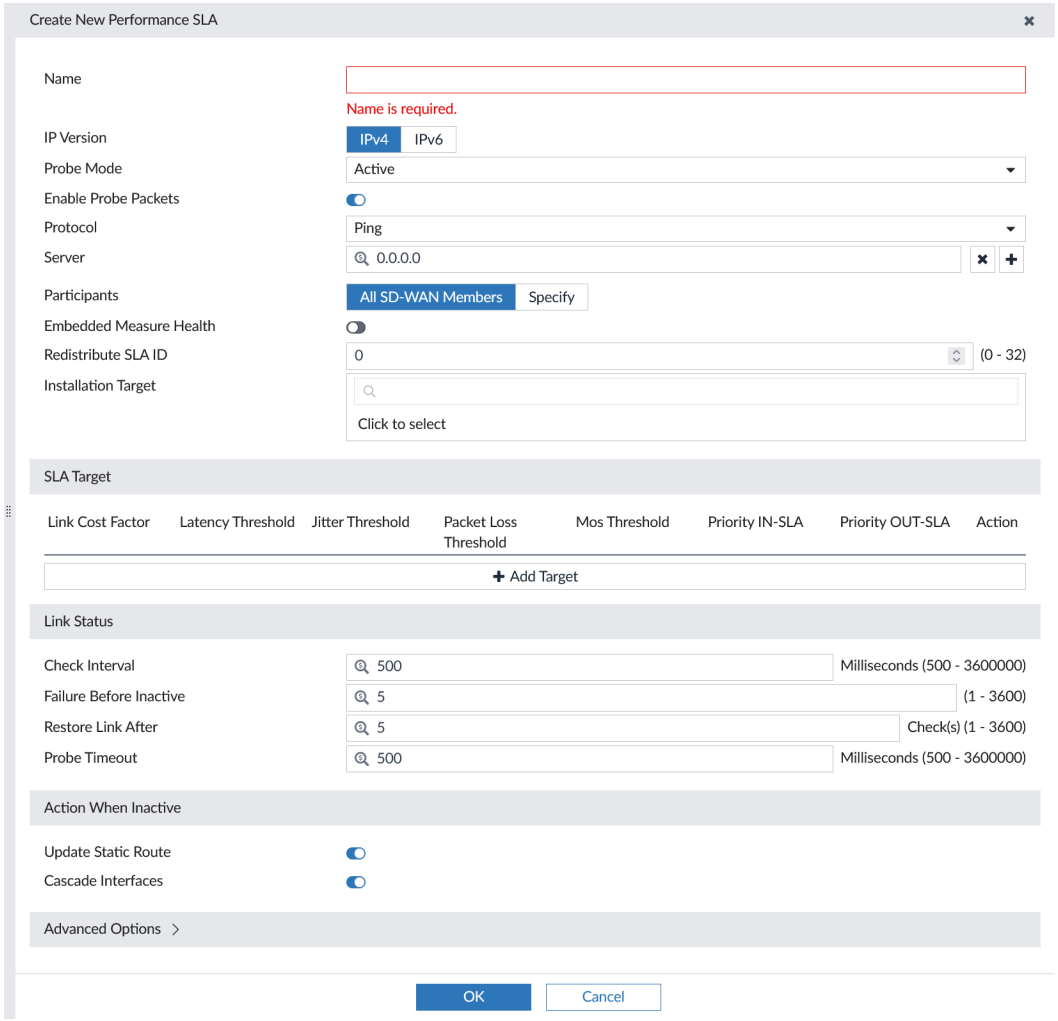
Create a Performance SLA in FortiManager that can be used to monitor the SD-WAN performance in FortiGate devices.

If all links meet the SLA criteria, the FortiGate uses the first link, even if that link isn't the best quality. If at any time, the link in use doesn't meet the SLA criteria, and the next link in the configuration meets the SLA criteria, the FortiGate changes to that link. If the next link doesn't meet the SLA criteria, the FortiGate uses the next link in the configuration if it meets the SLA criteria, and so on.

To create a new performance SLA:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > Provisioning Templates > SD-WAN Templates*.
3. Double-click an SD-WAN template to open it for editing, or click *Create New* in the toolbar.
   The SD-WAN template opens.

4. In the *Performance SLA* toolbar, click *Create New*. The *Create Performance SLA* dialog-box opens



5. Enter the following information, and click *OK* to create the performance SLA:

Name	Enter the name of the performance SLA.
IP Version	Select *IPv4* or *IPv6*.
Probe Mode	Set the mode that determines how to detect the server: • *Active*: the probes are sent actively (default). • *Agent Based*: traffic health is measured using FortiMonitor. FortiMonitor mimics a real user, and the probes return accurate application level performance statistics. • *Passive*: the traffic measures health without probes. • *Prefer-passive*: the probes are sent in case of no new traffic. • *Remote*: the link health is obtained from remote peers.
Enable Probe Packets	Set *Enable probe packets* to enable or disable sending probe packets.
Protocol	Select the detection method for the profile check: • Ping • TCP ECHO

	• UDP ECHO • HTTP • TWAMP • DNS • TCP Connect • FTP
Server	Click *Add* (+), and type the IP address of the health-check server.
Participants	Select available interface members or select *All SD-WAN Members*. The interfaces must already be added to the template.
Embedded Measure Health	Enable/disable embedding SLA information in ICMP probes (default = disable).
Redistribute SLA ID	Set the SLA entry (ID) that will be applied to the IKE routes (0 - 31, default = 0).
Installation Target	Click the box to specify installation targets for the performance SLA.
SLA Targets	Click *Add Target* to add a new SLA. Enable and enter the *Latency Threshold* (in milliseconds), *Jitter Threshold* (in milliseconds), *Packet Loss Threshold* (in percent), *Priority IN-SLA*, and *Priority OUT-SLA*, then click *OK* to create the SLA. SLAs can also be edited and deleted as required.
Link Status	
Interval	Status check interval, or the time between attempting to connect to the server, in seconds (1 - 3600, default = 1).
Failure Before Inactive	Specify the number of failures before the link becomes inactive (1 - 10, default = 5).
Restore Link After	Specify the number of successful responses received before server is considered recovered (1 - 10, default = 5).
Action When Inactive	Specify what happens with the WAN link becomes inactive.
Update Static Route	Select to update the static route when the WAN link becomes inactive.
Cascade Interfaces	Select to cascade interfaces when the WAN link becomes inactive.
Advanced Options	Expand to display the advanced options. Hover the mouse over each advanced option to view a description of the option. Set the options as desired.

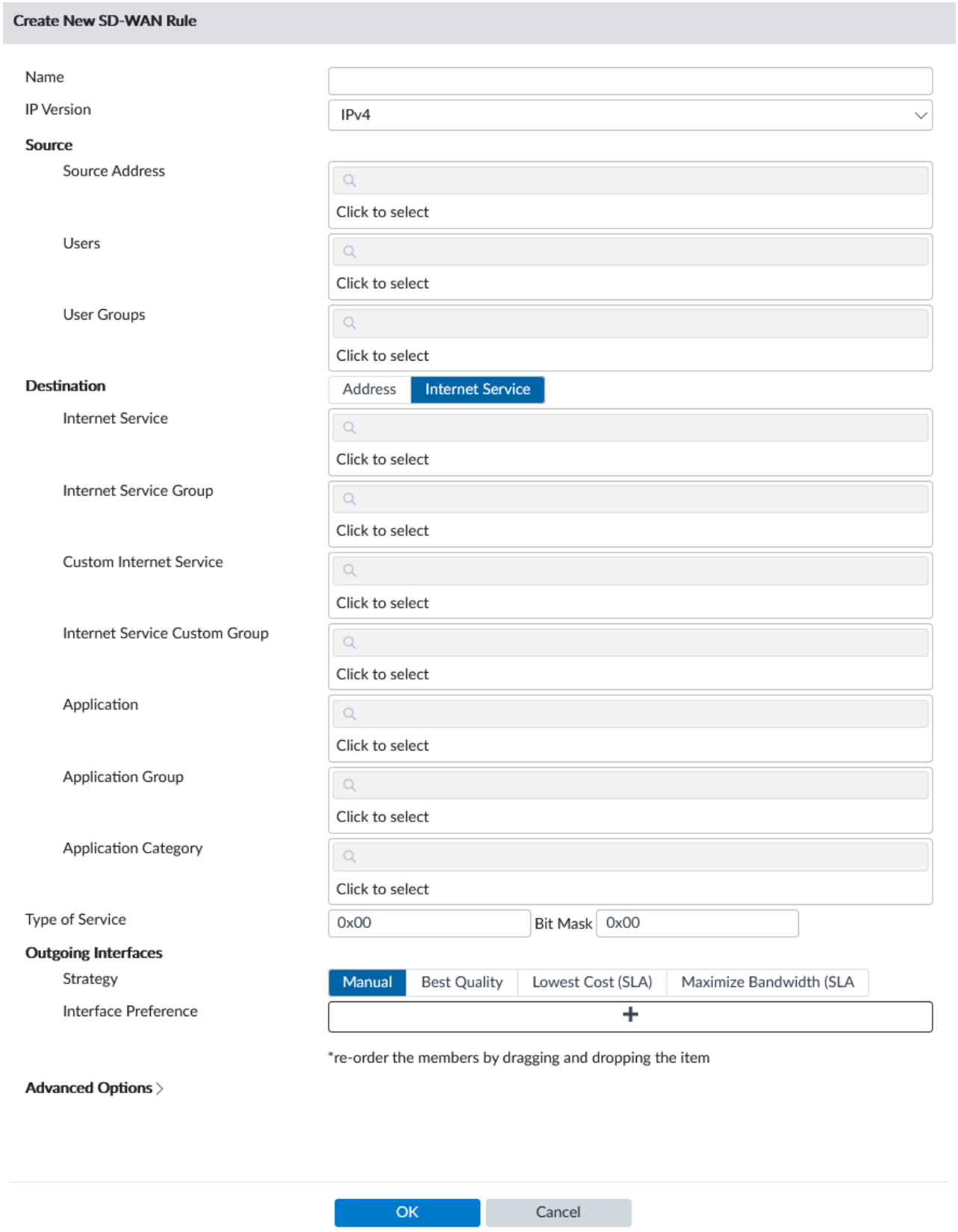
SD-WAN rules

Configure SD-WAN rules for WAN links by specifying the required network parameters. The SD-WAN rules are applied to the FortiGate device when the SD-WAN template is applied.

To create a new SD-WAN rule:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > Provisioning Templates > SD-WAN Templates*.
   The SD-WAN templates are displayed in the content pane.
3. Double-click an SD-WAN template to open it for editing, or click *Create New* in the toolbar.
   The SD-WAN template opens.

4. In the *SD-WAN Rules* toolbar, click *Create New*. The *Create New SD-WAN Rule* dialog-box opens.



5. Enter the following information, then click *OK* to create the new SD-WAN rule:

Name		Enter the name of the rule.
IP Version		Select either *IPv4* or *IPv6*.
Source		
	Source Address	Add one or more address from the drop-down.
	Users	Add one or more users from the drop-down.
	User Groups	Add one or more groups from the drop-down.
Destination		
	Address	Select an address or addresses from the drop-down list. This option is only available when *Destination* is *Address*.
	Route Tag	Select a tag from the drop-down list. This option is only available when *Destination* is *Address*.
	Internet Service	Select a service or services from the dropdown list. This option is only available when *Destination* is *Internet Service*.
	Internet Service Group	Select a service group or groups from the dropdown list. This option is only available when *Destination* is *Internet Service*.
	Custom Internet Service	Select a service or services from the dropdown list. This option is only available when *Destination* is *Internet Service*.
	Custom Internet Service Group	Select a service group or groups from the dropdown list. This option is only available when *Destination* is *Internet Service*.
	Application	Select an application or applications from the dropdown list. This option is only available when *Destination* is *Internet Service*.
	Application Group	Select an application group or groups from the dropdown list. This option is only available when *Destination* is *Internet Service*.
	Application Categories	Choose one or more application categories from the selection window. The application category field uses the default internet service database (ISDB) categories received from FortiGuard. This option is only available when *Destination* is *Internet Service*, and you are in a 7.2 or later ADOM.
Protocol		Select the protocol, or specify the protocol number.
Port Range		Enter the port range. This option is only available when the protocol is *TCP* or *UDP*.
Type of Service		Specify the type of service and bit mask.
Outgoing Interface		
	Strategy	Select one of the following to specify how the traffic flows through the outgoing interface: • *Manual* to specify what outgoing interface members to use.

		• *Best Quality* to identify outgoing interface members and have traffic flow based on quality status. • *Lowest Cost (SLA)* to identify outgoing interface members and have traffic flow based on the lowest cost. • *Maximize Bandwidth SLA* to identify outgoing interface members and have traffic flow to maximize bandwidth.
	Interface Preference	For the selected strategy, specify what interfaces you would like to be used. The top of the list is the highest priority, if SLA targets are met.
	Measured SLA	Select the SLA measurement for the selected strategy. This option is only available when *Strategy* is *Best Quality*.
	Zone Prefrence	Select the zone preference. This option is only available when *Strategy* is *Lowest Cost (SLA)* or *Maximize Bandwidth (SLA)*.
	Required SLA Target	Select the required SLA target. This option is only available when *Strategy* is *Lowest Cost (SLA)* or *Maximize Bandwidth (SLA)*.
Advanced Options		Expand to display the advanced options. Hover the mouse over each advanced option to view a description of the option. Set the options as desired.

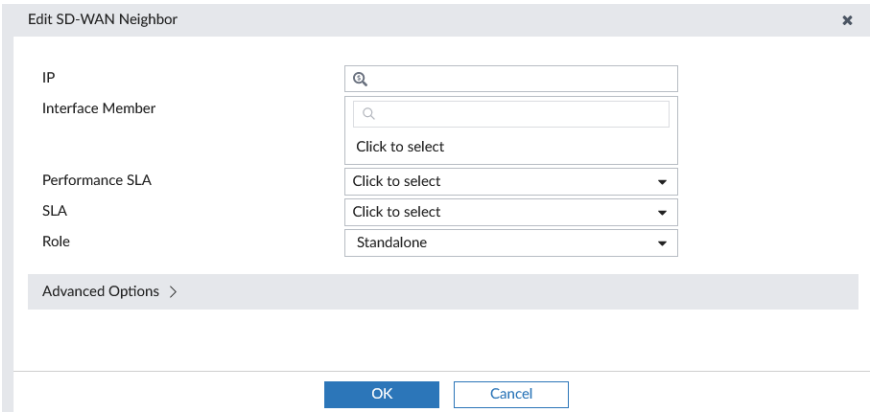
Neighbors

You can create SD-WAN rules that include Border Gateway Protocol (BGP) neighbors.

You must create BGP neighbors for FortiGate devices before you can add them to SD-WAN templates.

To configure BGP neighbors for SD-WAN templates:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > Provisioning Templates > SD-WAN Templates*.
3. Double-click an SD-WAN template to open it for editing, or click *Create New* in the toolbar.
   The SD-WAN template opens.
4. In the *Neighbor* toolbar, click *Create New*.
   The *Create New Neighbor* pane opens:



5. Configure the following:

IP	Type the IP address for the BGP neighbor.
Interface Member	Click the box, and select interface members. Multiple interface members can be selected for a neighbor. This allows the SD-WAN neighbor feature to support topologies where there are multiple SD-WAN overlays and/or underlays to a neighbor. When multiple interface members are selected, route failover will only occur if both tunnels to a neighbor are down.
Performance SLA	Click the list, and select the performance SLA.
Role	Select *Standalone*, *Primary*, or *Secondary*.

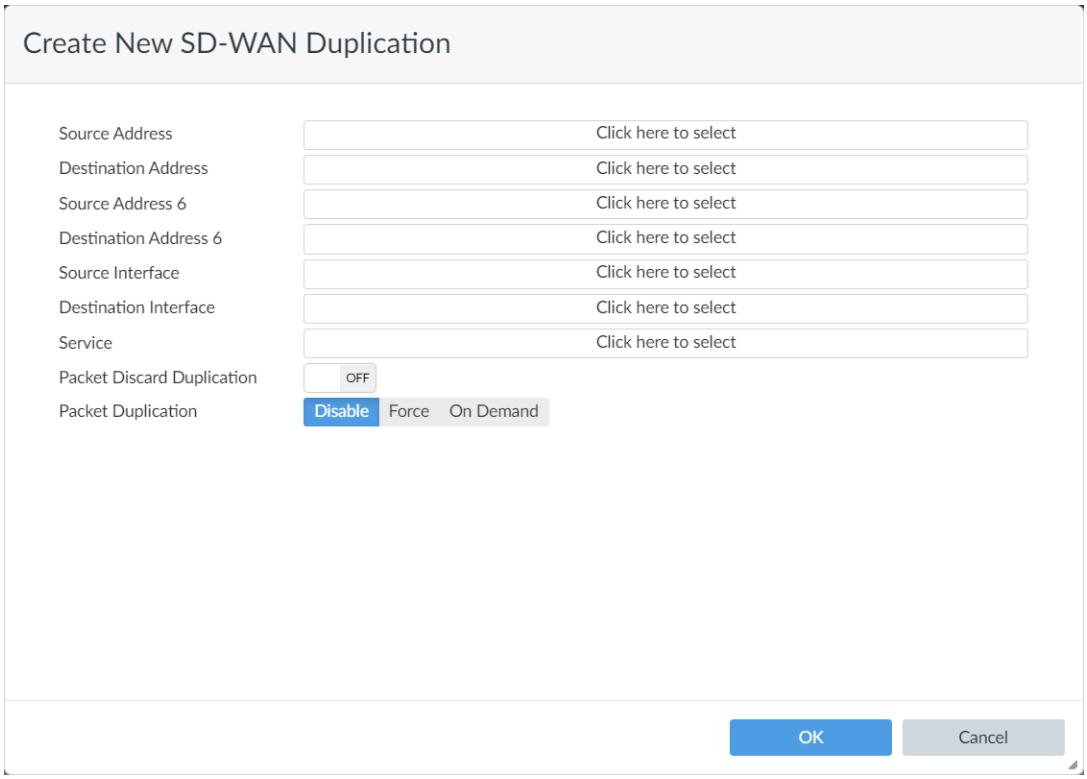
6. Click *OK*.

Duplication

You can configure packet duplication for the SD-WAN network.

To configure packet duplication:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > Provisioning Templates > SD-WAN Templates*.
   The SD-WAN templates are displayed in the content pane.
3. Double-click an SD-WAN template to open it for editing, or click *Create New* in the toolbar.
   The SD-WAN template opens.
4. In the *Duplication* toolbar, click *Create New*.
   The *Create New SD-WAN Duplication* dialog box opens.



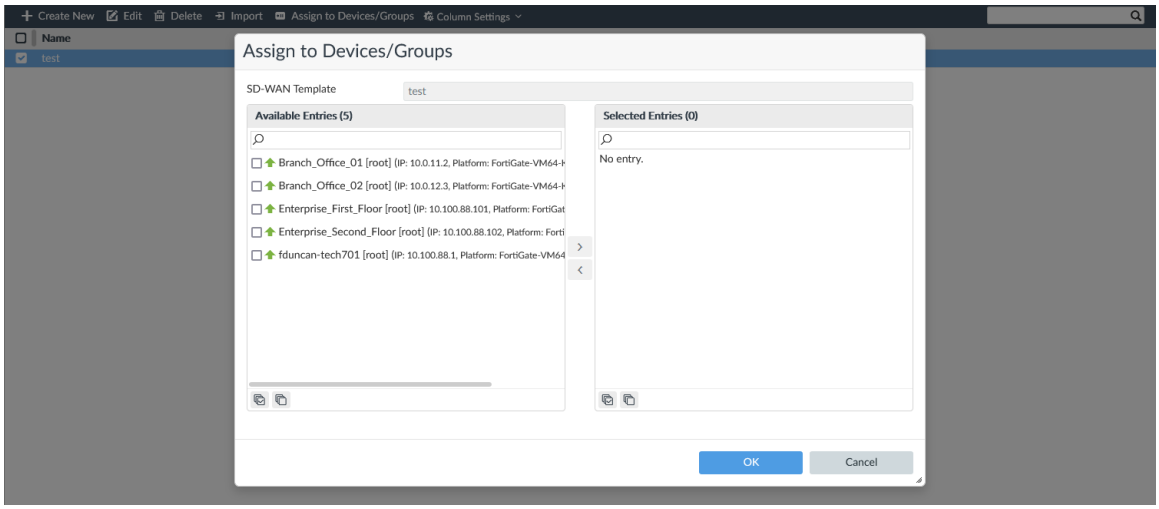
5. Enter the options, then click *OK*:

Assign SD-WAN templates to devices and device groups

You can assign SD-WAN templates to FortiGate devices. The network parameters specified in the SD-WAN template are used to measure the performance of the WAN link on the FortiGate device.

To assign an SD-WAN template to a FortiGate device or device group:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager* > *Provisioning Templates* > *SD-WAN Templates*.
   The SD-WAN templates are displayed in the content pane.
3. Select a template, and click *Assign to Device/Group*.
   The *Assign to Device/Group* dialog opens.



4. In the *Available Entries* list, select a *FortiGate*, and click > to move the FortiGate to the *Selected Entries* list.
5. Click *OK*.

To edit an assigned device:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager* > *Provisioning Templates* > *SD-WAN Templates*.
   The SD-WAN templates are displayed in the content pane.
3. Select the template with the assigned device, and click *Assign to Device/Groups* in the toolbar, or right-click the device and select *Assign to Device/Groups*.
   The *Assign to Device/Groups* page opens.
4. Edit the assigned devices or device groups, and click *OK* to apply your changes.

Migrate an SD-WAN Orchestrator configuration into SD-WAN templates

This topic includes an example of migrating your SD-WAN Orchestrator configuration into SD-WAN templates. As a part of this migration, the FortiManager and managed FortiGate devices are all upgraded to version 7.0 or later.

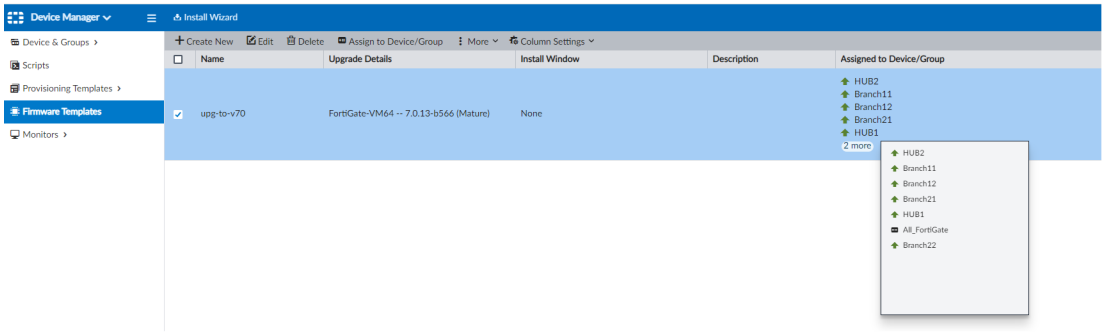
The SD-WAN network used in this example is based on the solution described in the *Planning your network* topic included in the FortiManager 6.4 SD-WAN Orchestrator Administration Guide.

- The ADOM is on version 6.4 ADOM.
- The FortiGate devices are on version 6.4.
- There are two regions, and each region has one hub and two branches.
  In the example used in this topic, region one includes hub1, branch11, and branch12, and region two includes hub2, branch21, and branch 22.

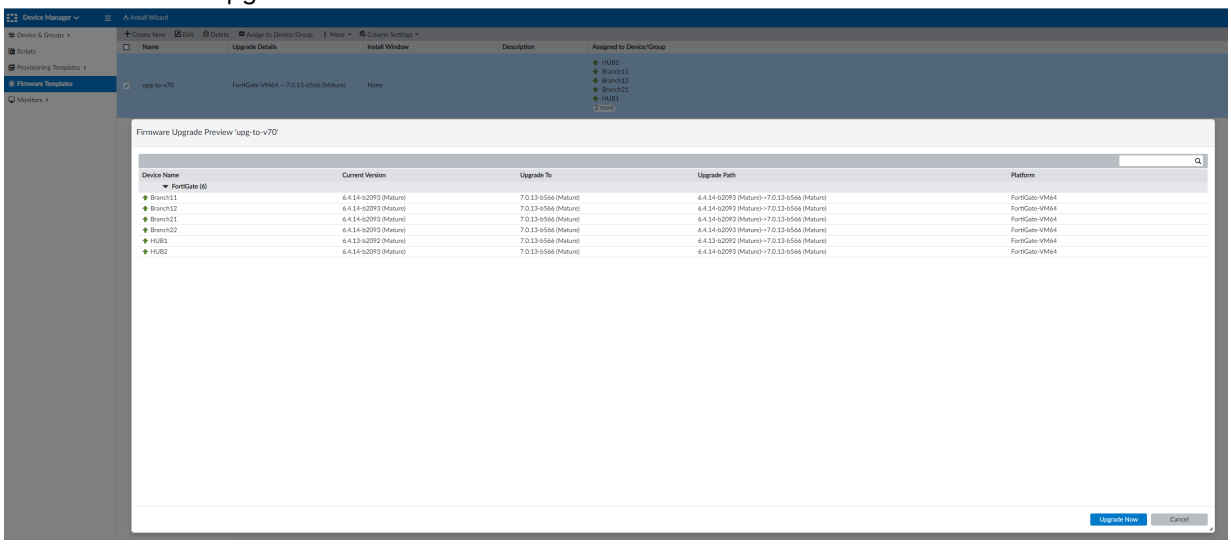
To migrate the SD-WAN Orchestrator configuration into SD-WAN templates:

1. Upgrade the FortiManager to the latest 7.0 version.
   This example uses FortiManager 7.0.10. For more information, see the FortiManager 7.0.10 Upgrade Guide.

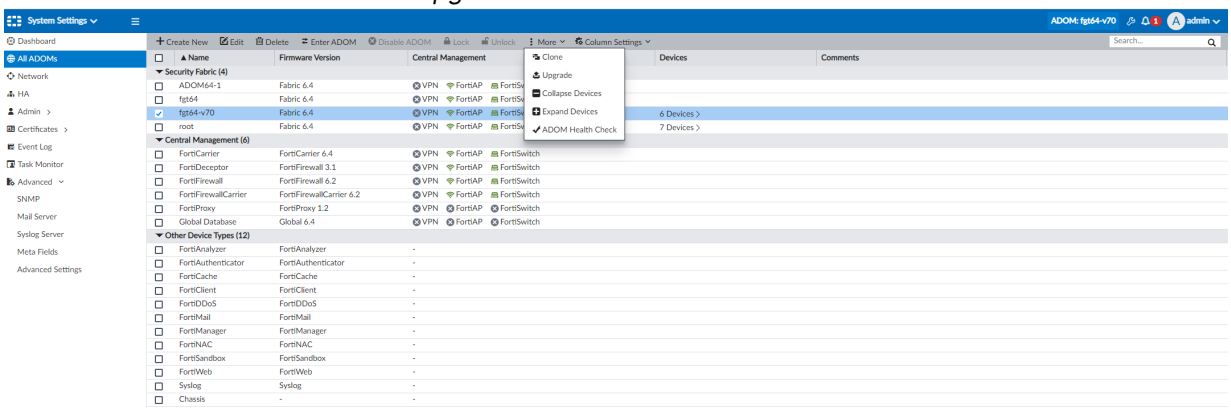
2. Using FortiManager *Firmware Templates*, upgrade FortiGate devices to the latest 7.0 version. This example uses FortiOS 7.0.13. For more information, see Firmware templates on page 378.
   a. Go to *Device Manager* > *Firmware Templates*, and click *Create new*.
   b. Assign the firmware template to the device/group that contains the FortiGate devices.



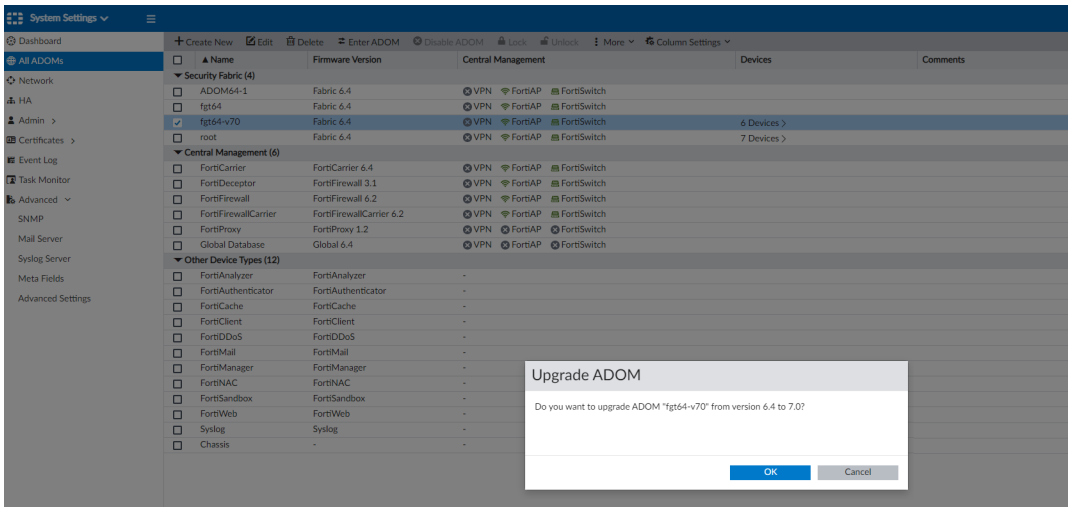
   c. Proceed with the upgrade.



3. Upgrade the ADOM to version 7.0. For more information, seeUpgrading an ADOM on page 948.
   a. Go to *System Settings* > *All ADOMs*.
   b. Select the ADOM and click *More* > *Upgrade*.



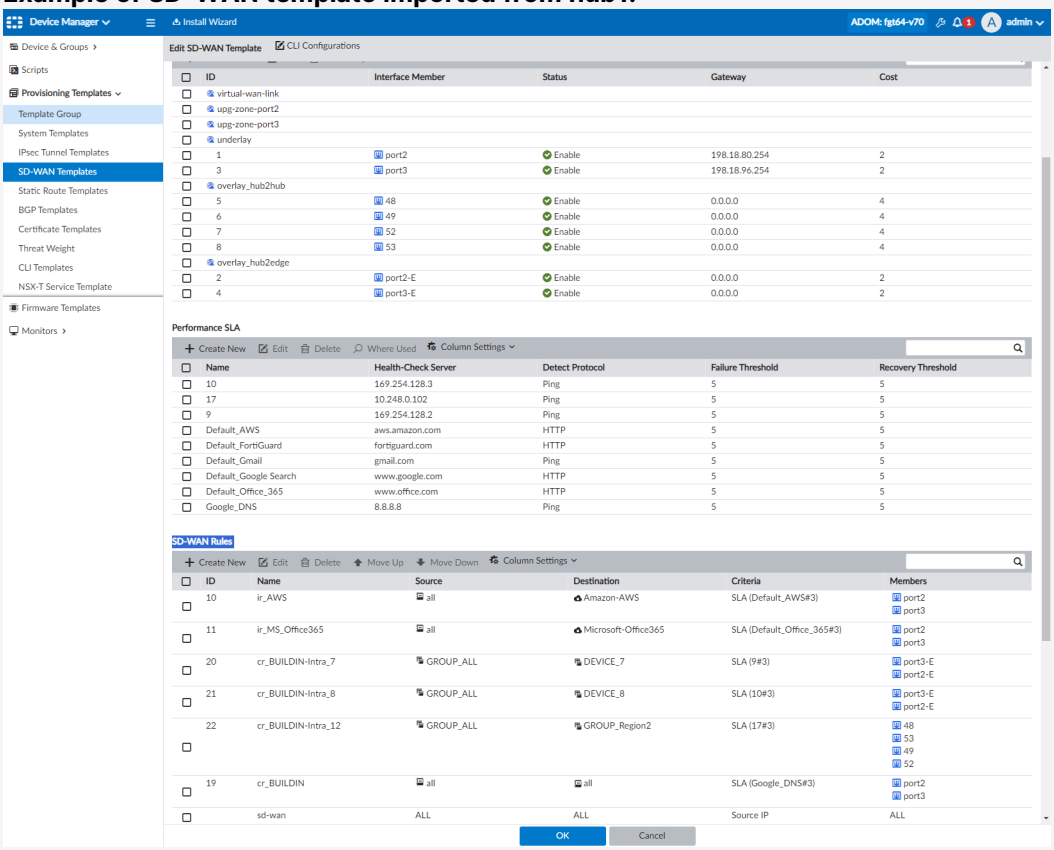
c. Click *OK*.



4. Go to *Device Manager* > *Provisioning Templates* > *SD-WAN Templates*, and import the SD-WAN configuration from hub devices (e.g. hub1 and hub2).
   When comparing the SD-WAN templates imported from hub1 and hub2, there are a number of differences. As a result of these differences, and the templates cannot be combined into a singular template for hubs. An example of the differences between imported templates include:
   - In *Interface Members* > *Underlay*, there are different gateways.
   - In *Performance SLA*, there are different names and health-check servers.
   - In *SD-WAN Rules*, there is a different *Destination*, *Criteria*, and *Member* order which is not supported by meta variables.

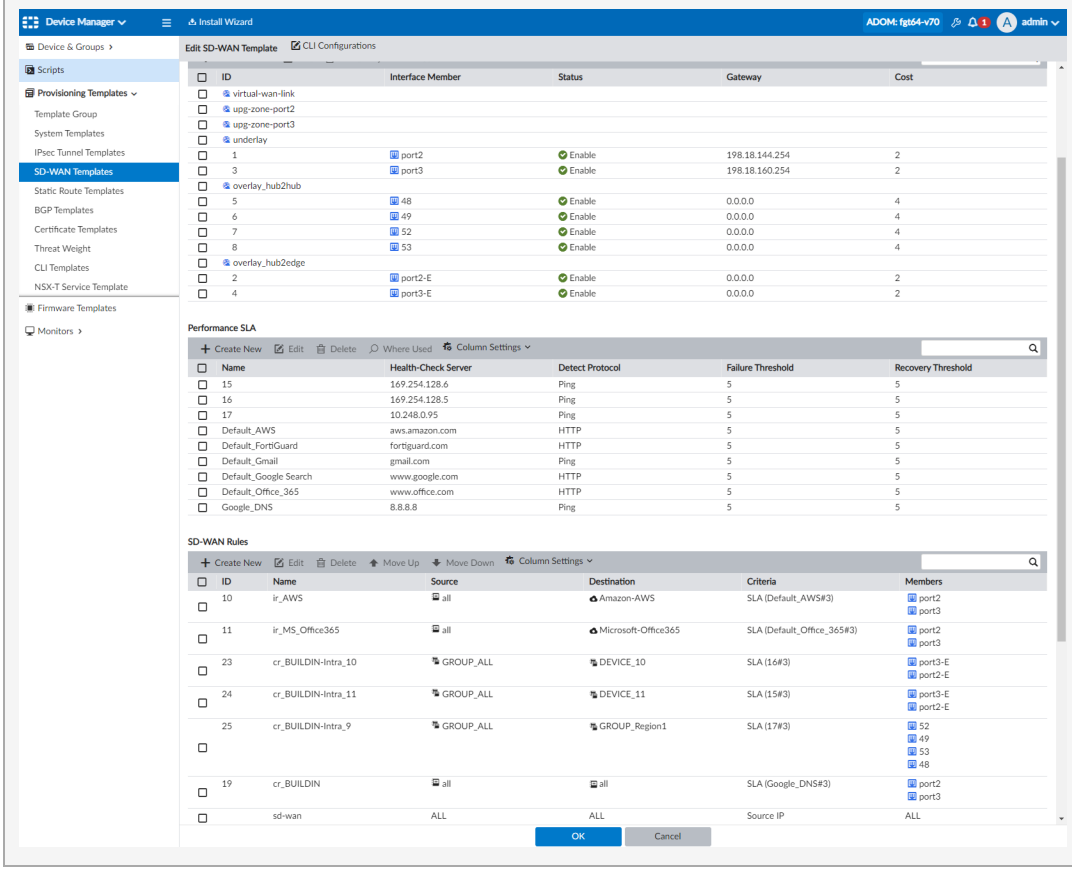
Example Comparison of Imported HUB templates

Example of SD-WAN template imported from hub1:



Example of SD-WAN template imported from hub2:

Example Comparison of Imported HUB templates

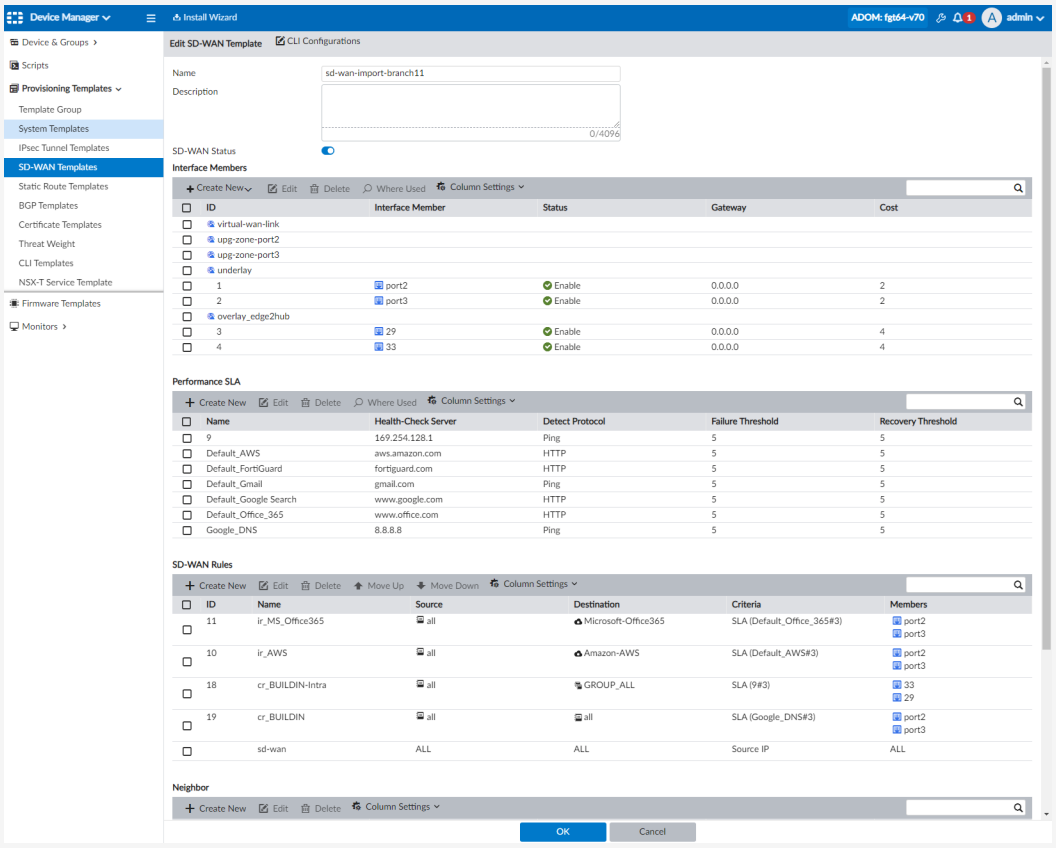


5. Assign the imported hub1 SD-WAN template to the hub1 device, and the imported hub2 SD-WAN template to the hub 2 device.
6. Go to *Device Manager* > *Provisioning Templates* > *SD-WAN Templates*, and import the SD-WAN templates from branch devices (e.g. branch11, branch12, branch21, and branch22). When comparing the SD-WAN templates imported from branch devices, there are a number of differences. An example of the differences between imported templates include:
   - In *Interface Members* > *overlay_edge2hub*, there are different interface members.
   - In *Performance SLA*, there are different names and health-check servers.
   - In *SD-WAN Rules*, there is a different *Criteria* and *Member* order which is not supported by meta variables.

Example Comparison of Imported Branch Templates

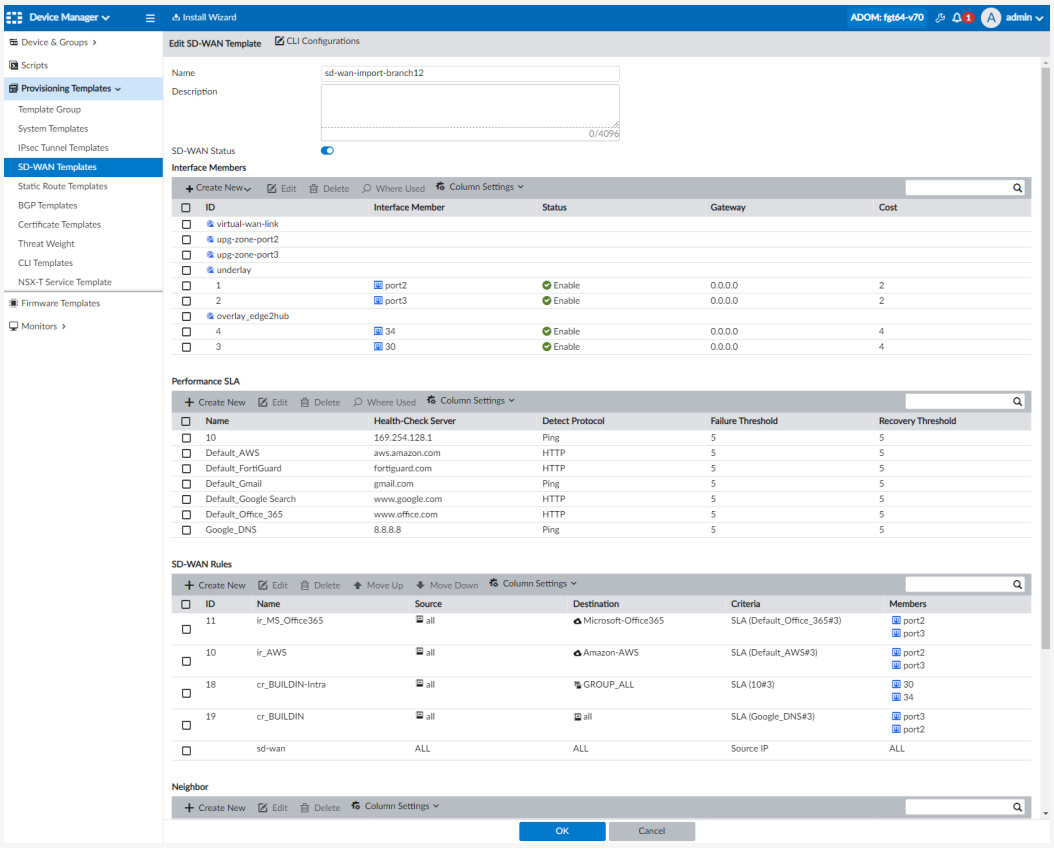
Example of SD-WAN template imported from branch11:

Example Comparison of Imported Branch Templates



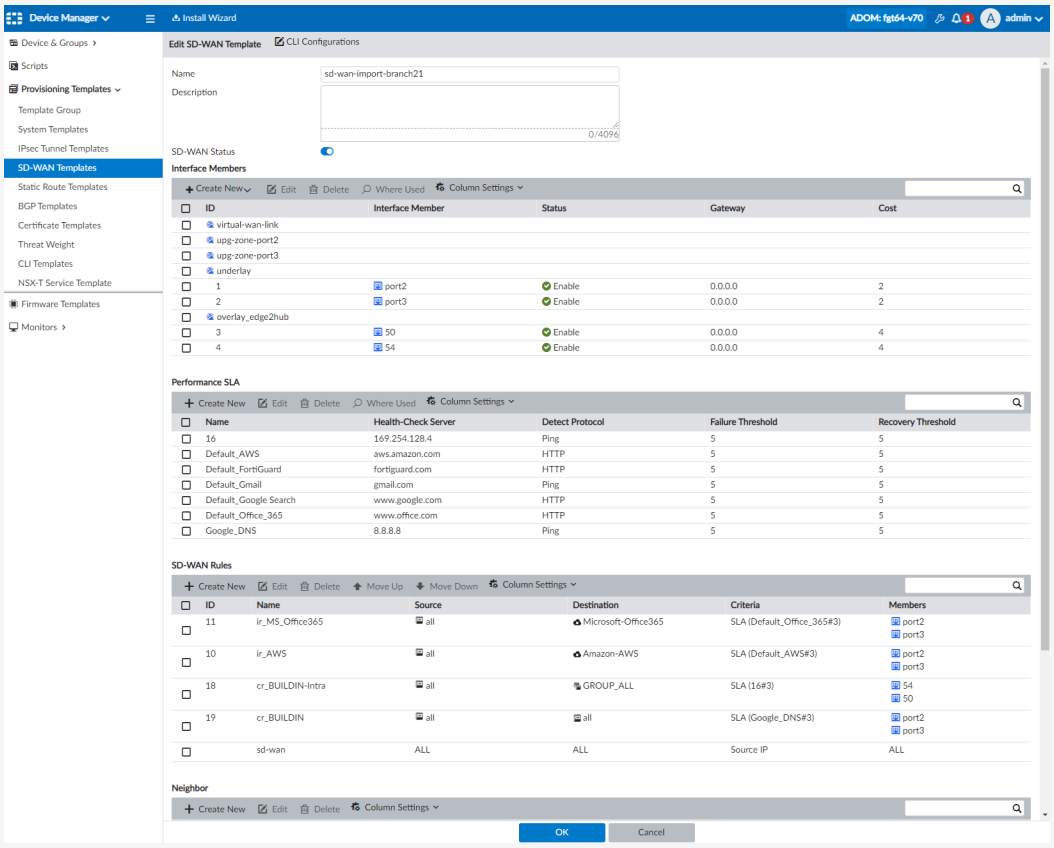
Example of SD-WAN template imported from branch12:

Example Comparison of Imported Branch Templates



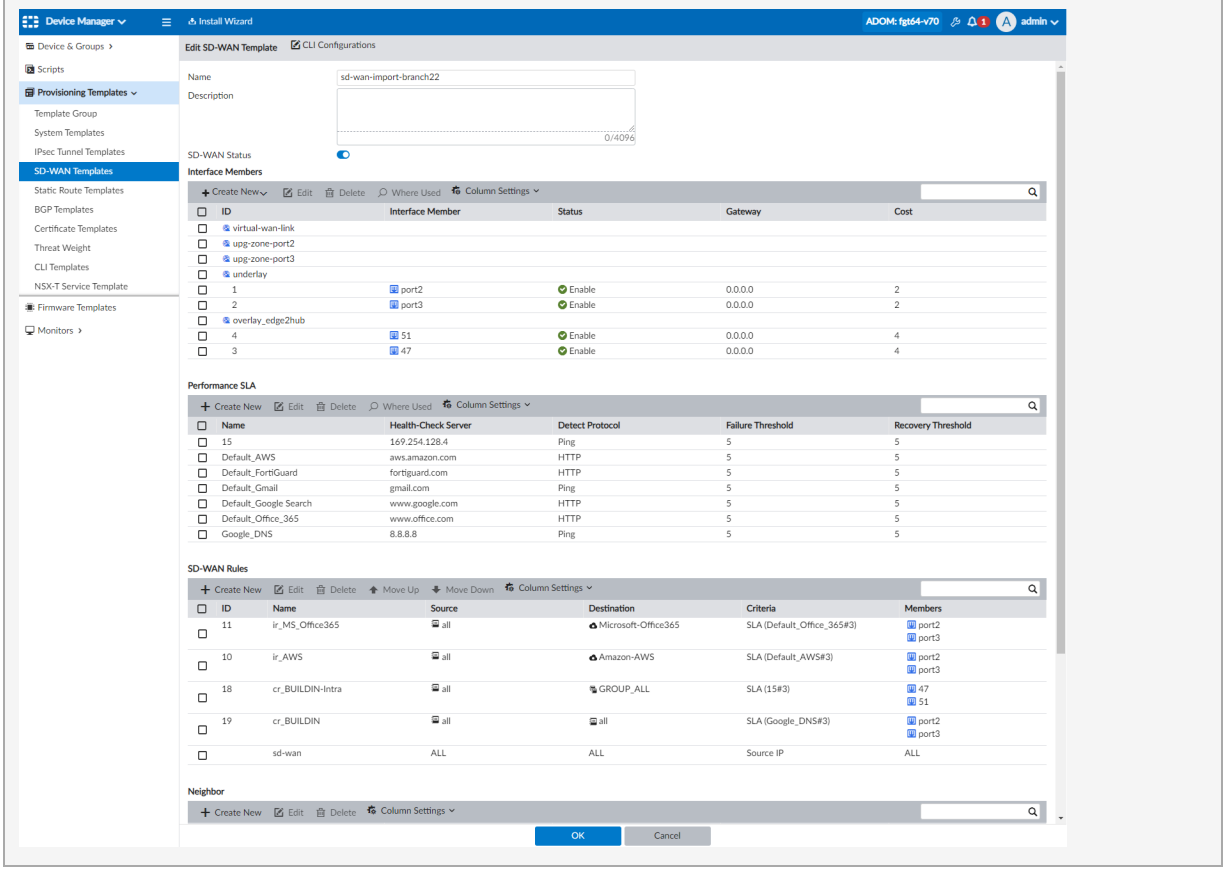
Example of SD-WAN template imported from branch21:

Example Comparison of Imported Branch Templates



Example of SD-WAN template imported from branch22:

Example Comparison of Imported Branch Templates



7. Assign the imported branch SD-WAN template to each branch device from which it was imported. For example:
   - Assign the template imported from branch11 to the branch11 device.
   - Assign the template imported from branch12 to the branch12 device.
   - Assign the template imported from branch21 to the branch21 device.
   - Assign the template imported from branch22 to the branch22 device.
8. (Optional) Continue to upgrade FortiManager to the latest available versions following the recommended upgrade path. For example, upgrade to FortiManager 7.2.4 and then to 7.4.2. See the FortiManager documentation for more information on upgrade paths and the latest available versions.

SD-WAN overlay templates

Most SD-WAN deployments require complex overlay configurations for datacenter or cloud connectivity. The SD-WAN overlay template includes a wizard to automate and simplify the process using Fortinet's recommended IPsec and BGP templates.

Note that the overlay template does not provide any SD-WAN intelligence. Please configure an SD-WAN template to complete the SD-WAN configuration. The overlay template also assumes connectivity between the HUB and branch in order to build the overlay tunnels. This can be accomplished in a variety of ways, such as static routes, dynamic routing protocol (BGP) or through a DHCP provided static route.

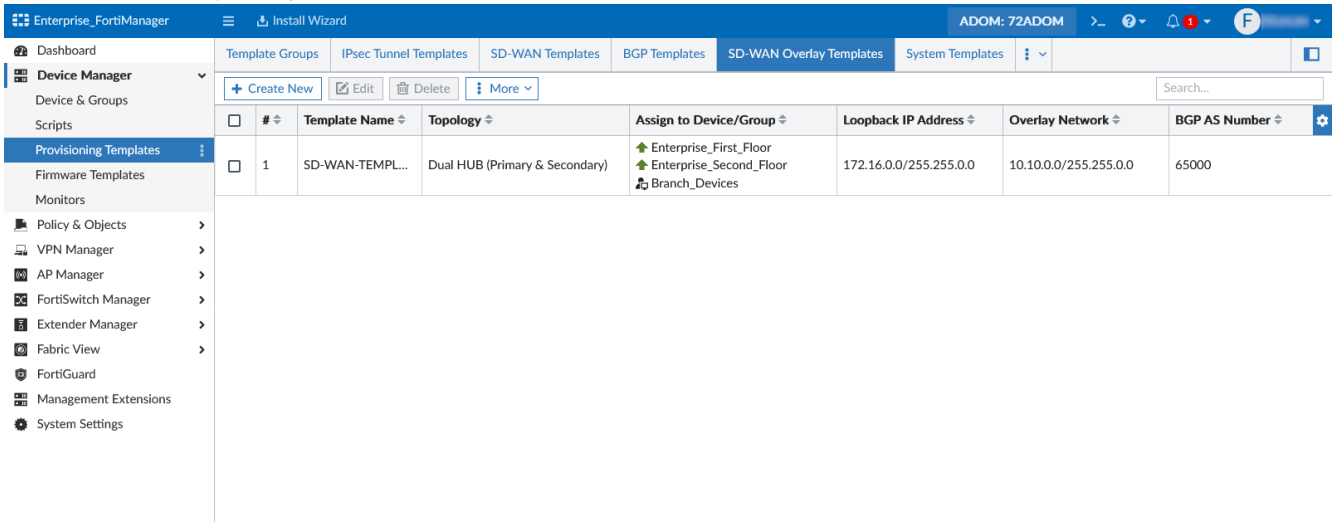
When the SD-WAN overlay template has been configured, it generates the necessary IPsec, BGP and CLI provisioning templates that are required for the creation of your SD-WAN overlays. These provisioning templates are automatically assigned to the SD-WAN branch and hub devices identified in the template's wizard. Provisioning templates created by the SD-WAN overlay template are also automatically organized into template groups for each hub and branch configuration. See Template groups on page 274.

To deploy the SD-WAN overlays in your environment, you can install the branch and hub provisioning templates to your devices using the FortiManager Device Manager. See Using the SD-WAN overlay template on page 329.

By default, the `branch_id` metadata variable is created by the template and each SD-WAN branch device must be configured with a unique branch ID value. When *Automatic Branch ID Assignment* setting is enabled in the wizard, the branch ID is automatically applied to devices in the branch device group. See Automatic Branch ID Assignment on page 332.

Additional meta variables can be created for use in the template's text fields to further improve deployment scalability. See ADOM-level metadata variables on page 557.

You can configure a new SD-WAN Overlay Template by going to *Device Manager > Provisioning Templates > SD-WAN Overlay Templates*.



The following options are available:

Create New	Create a new SD-WAN overlay template.
Edit	Edit a template. Right-click a template, and select *Edit*.
Delete	Delete a template. Right-click a template, and select *Delete*.
More	View additional options, including the option to clone a template.
Column Settings	Configure which columns are displayed in the SD-WAN overlay template table.

Template prerequisites and network planning

Before creating the SD-WAN overlay template, the following prerequisites and network planning steps should be completed:

Prerequisites

- Import the FortiGate devices that will make up the hub and branch devices into FortiManager. See Add devices on page 91.
- Configure the ISP links and other interfaces on your imported devices.
- Create a device group for your branch devices. See Device groups on page 147

Network planning

- Allocate the overlay network address space. By default, the template uses `10.10.0.0/16`.
- Allocate the loopback IP address space. By default, the template uses `172.16.0.0/16`.
- Select an AS number for BGP for the new SD-WAN overlay region. By default, the template uses `65000`.

For more information, see SD-WAN overlay template IP network design on page 342



Note that the overlay template does not provide any SD-WAN intelligence. Please configure an SD-WAN template to complete the SD-WAN configuration. The overlay template also assumes connectivity between the HUB and branch in order to build the overlay tunnels. This can be accomplished in a variety of ways, such as static routes, dynamic routing protocol (BGP) or through a DHCP provided static route.

Using the SD-WAN overlay template

To use the SD-WAN overlay template:

1. Pre-configure your network and SD-WAN devices. See Template prerequisites and network planning on page 329.
2. Create an SD-WAN overlay template. See Configuring an SD-WAN overlay template on page 330.
3. Assign metadata variables to devices.
   - The `branch_id` variable is automatically created by the template, and each branch device must be assigned a unique value. When *Automatic Branch ID Assignment* setting is enabled in the wizard, the branch ID is automatically applied to devices in the branch device group. See Automatic Branch ID Assignment on page 332.
   - Additional custom metadata variables can be used if required. See ADOM-level metadata variables on page 557.
4. Configure the SD-WAN rules to include the newly created overlays by creating or editing an SD-WAN template. See SD-WAN rules on page 312 and SD-WAN templates on page 304.
5. Create the Policy Package for your branch and hub devices. See Managing policy packages on page 414.
6. Install the changes to SD-WAN devices using the Install Wizard. See Install wizard on page 180
7. (Optional) Edit the SD-WAN overlay template. See Editing the SD-WAN overlay template on page 337.
8. (Optional) Add new branch devices. See Onboarding new branch devices on page 337.

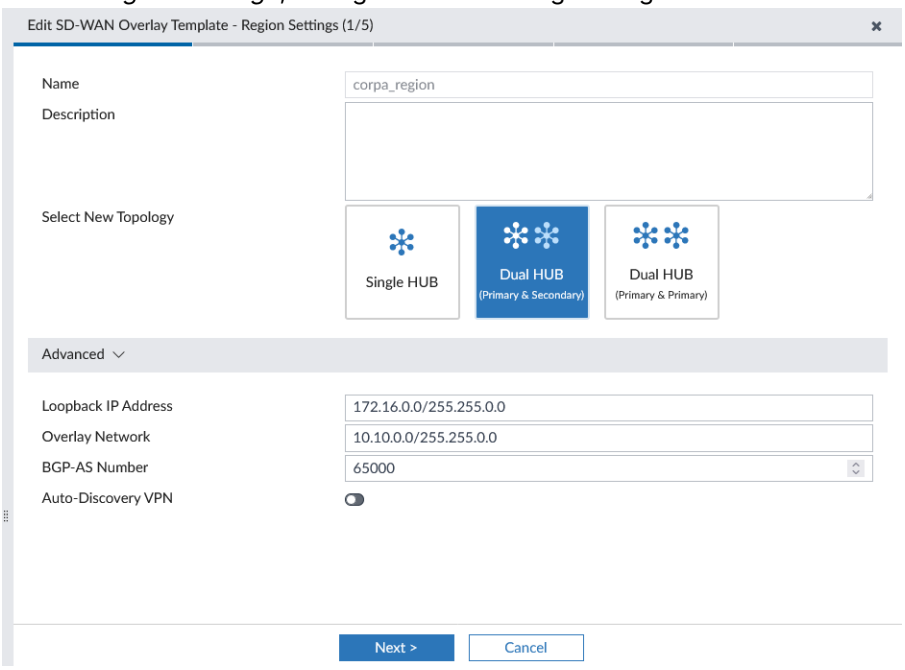
Configuring an SD-WAN overlay template

The SD-WAN overlay template wizard guides you through deployment of SD-WAN overlays in your network. After the configuration of the template is finished, multiple provisioning templates are generated for use in your SD-WAN environment.

The SD-WAN overlay template wizard can be run again to re-generate the provisioning templates later if required. See Editing the SD-WAN overlay template on page 337.

To create an SD-WAN overlay template:

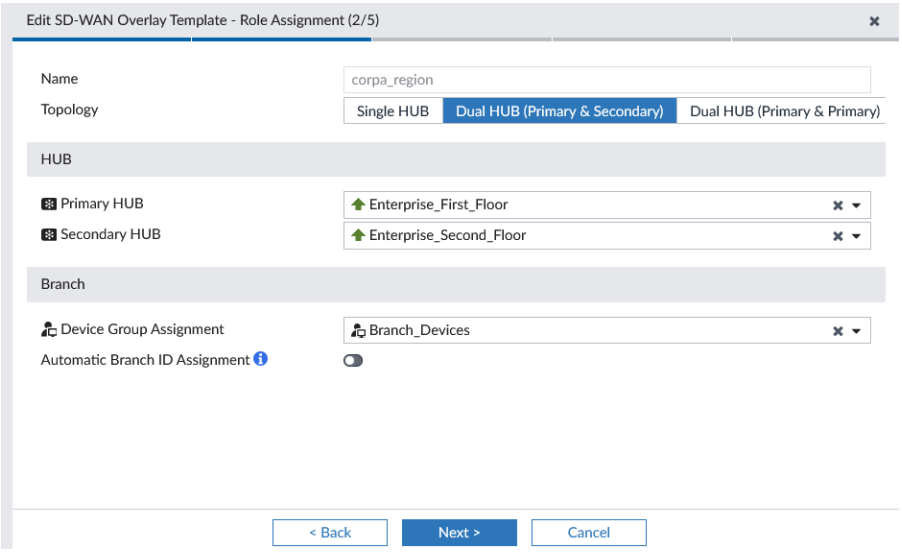
1. Go to *Device Manager > Provisioning Templates > SD-WAN Overlay Templates*.
2. Click *Create New*.
   The Create New SD-WAN Overlay Template wizard opens.
3. Enter a name and description for the new SD-WAN overlay template, and click *OK*.
4. For the *Region Settings*, configure the following settings and click *Next*.



Select New Topology	Select a topology type based on your environment. Topologies include the following: • Single Hub • Dual Hub (Primary/Secondary) • Dual Hub (Primary/Primary) The options presented in the wizard change based on the topology selected.

	Primary/Secondary and Primary/Primary are the same configuration, with the difference being that in a Primary/Secondary deployment, the Secondary hub is given a higher cost than the Primary. This cost is controlled by the SDWAN rule.
Advanced	Expand to view additional configurable settings. These fields are preconfigured with settings that will work in many situations, but you may need to adjust these to match your own networking environment. They should match the addresses you identified when considering the SD-WAN overlay template prerequisites. SeeTemplate prerequisites and network planning on page 329 .
Loopback IP Address	Optionally, you can configure the loopback IP address. By default, this setting is set to `172.16.0.0/255.255.0.0`.
Overlay Network	Optionally, you can configure the overlay network. By default, this setting is set to `10.10.0.0/255.255.0.0`.
BGP-AS Number	Optionally, you can configure the BGP AS number. By default, this setting is set to `65000`.
Auto-Discovery VPN	Optionally, you can toggle this setting ON to enable Auto Discovery VPN (ADVPN).

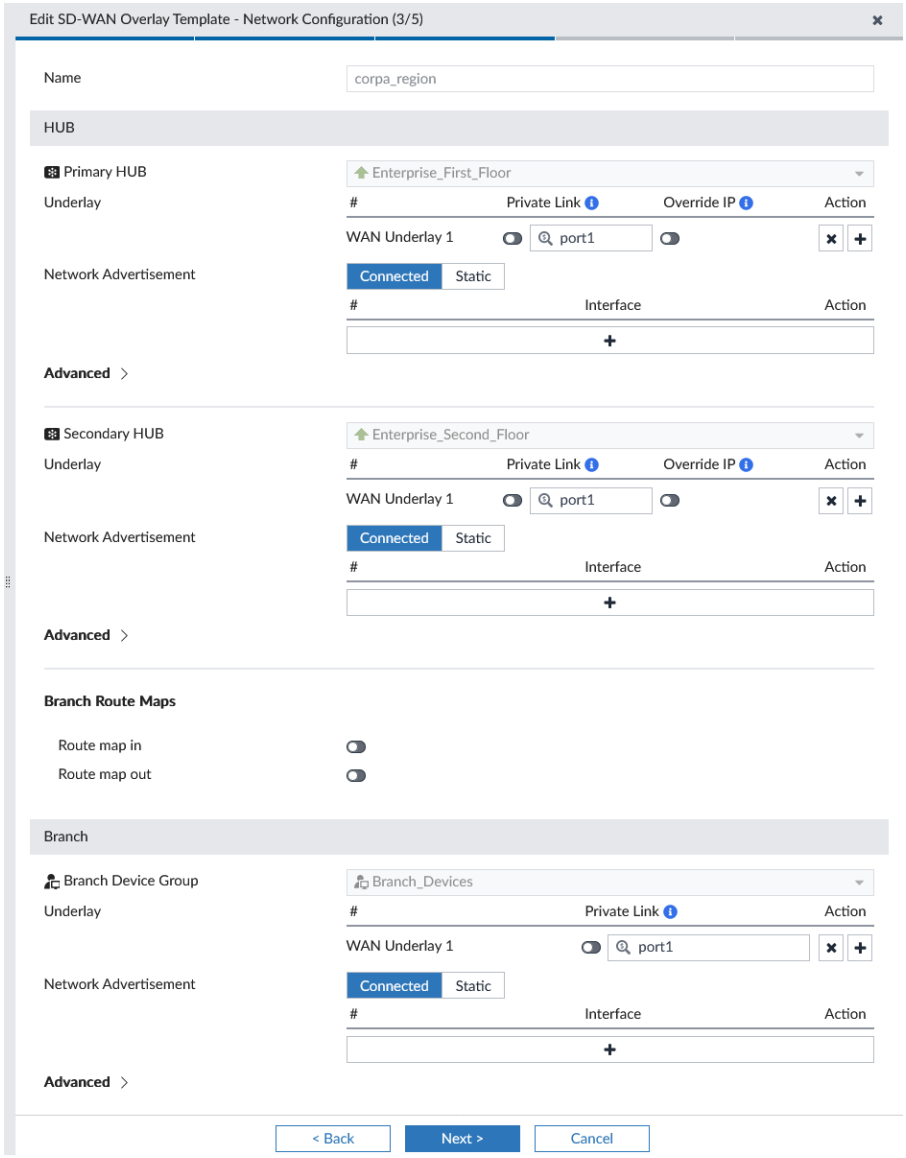
5. For the *Role Assignment*, configure the following settings and click *Next*.



Topology	Optionally, you can change the topology type that you selected on the previous screen.
Hub	Select the SD-WAN hubs. The number of hubs required depend on the topology selected: • *Single Hub*: One standalone hub.

		• *Dual Hub (Primary & Secondary)*: One primary and one secondary hub. • *Dual Hub (Primary & Primary)*: Two primary hubs. Hub devices must be added to FortiManager before creating the SD-WAN overlay template.
Branch		
	Device Group Assignment	Select the device group containing your SD-WAN branch devices. Devices included in this device group are configured as SD-WAN branch devices as a part of this template. Additional devices can be added to the selected device group later to receive the SD-WAN branch configuration when performing an installation on that device. This simplifies the onboarding of new branch devices. See Onboarding new branch devices on page 337.
	Automatic Branch ID Assignment	Enable to automatically assign a branch ID to each device in the branch device group. This will also apply to devices added to the branch device group in the future, as well as those added to the device group using a zero-touch provisioning device blueprint. Branch ID values are between one and the maximum number allowed by the subnet. For example, the default 10.10.0.0/255.255.0.0 overlay network uses the /19 subnet when your setup includes 5 - 8 overlays. The maximum allowed branch IDs in this range is 8190 based on the maximum number of number of usable IPs/FortiGates supported per overlay. See SD-WAN overlay template IP network design on page 342. When this setting is not enabled, you must manually configure the branch ID for each branch device.

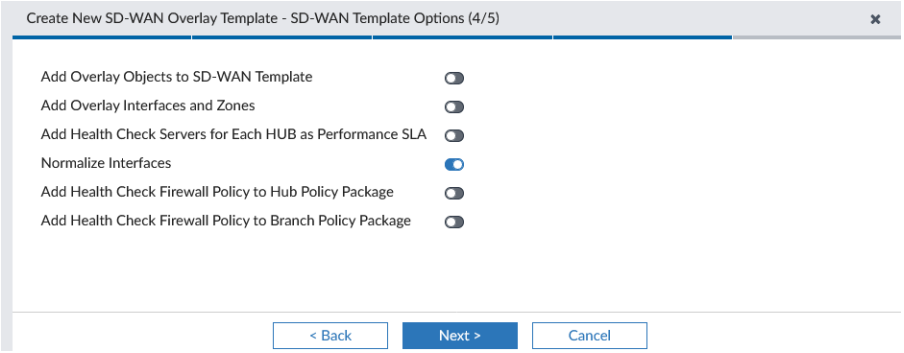
6. For the *Network Configuration*, configure the following settings and click *Next*.



Hub	Configure the network settings for each hub in your configuration. The number and types of hubs present depend on the topology you selected.
WAN Underlay	Type the interfaces for each WAN underlay. You can add additional WAN underlays by clicking the add icon. For each WAN underlay, you can optionally enable the following settings: • *Private Link*: No overlays will be created on private links. • *Override IP*: Override the IP address for the WAN underlay with the provided IP address. This option is not available when *Private Link* is enabled.

	Network Advertisement	1. Configure network advertisement for the hub. Network advertisement can be set to one of the following: • *Connected*: Type the network interface to advertise. Additional interfaces can be added by clicking the add icon. • *Static*: Type the network prefix to advertise. Additional network prefixes can be added by clicking the add icon.
	Advanced	Expand to view advanced settings, including configuration of SD-WAN neighbors. Click *Neighbors > Create New* to add a new SD-WAN neighbor for the hub.
Branch Route Maps		Optionally, move the toggle to the ON position to enable branch maps, and then select the corresponding route map. You can create a new route map by clicking the add icon, or select one of the default route maps. See also Using preconfigured route maps for self-healing with BGP on page 336.
Branch		Configure the network settings for the branch devices in your configuration.
	WAN Underlay	Type the interfaces for the SD-WAN branch WAN underlay. You can add additional WAN underlays by clicking the add icon. For each WAN underlay, you can optionally enable the following settings: • *Private Link*: No overlays will be created on private links.
	Network Advertisement	Configure network advertisement for the branch. Network advertisement can be set to one of the following: • *Connected*: Type the network interface to advertise. Additional interfaces can be added by clicking the add icon. • *Static*: Type the network prefix to advertise. Additional network prefixes can be added by clicking the add icon.
	Advanced	Expand to view advanced settings, including configuration of route maps for hub overlays. You can apply the route map settings to all hub overlays or specify them individually. See also Using preconfigured route maps for self-healing with BGP on page 336.

7. For the *Template Options*, configure the following settings and click *Next*.



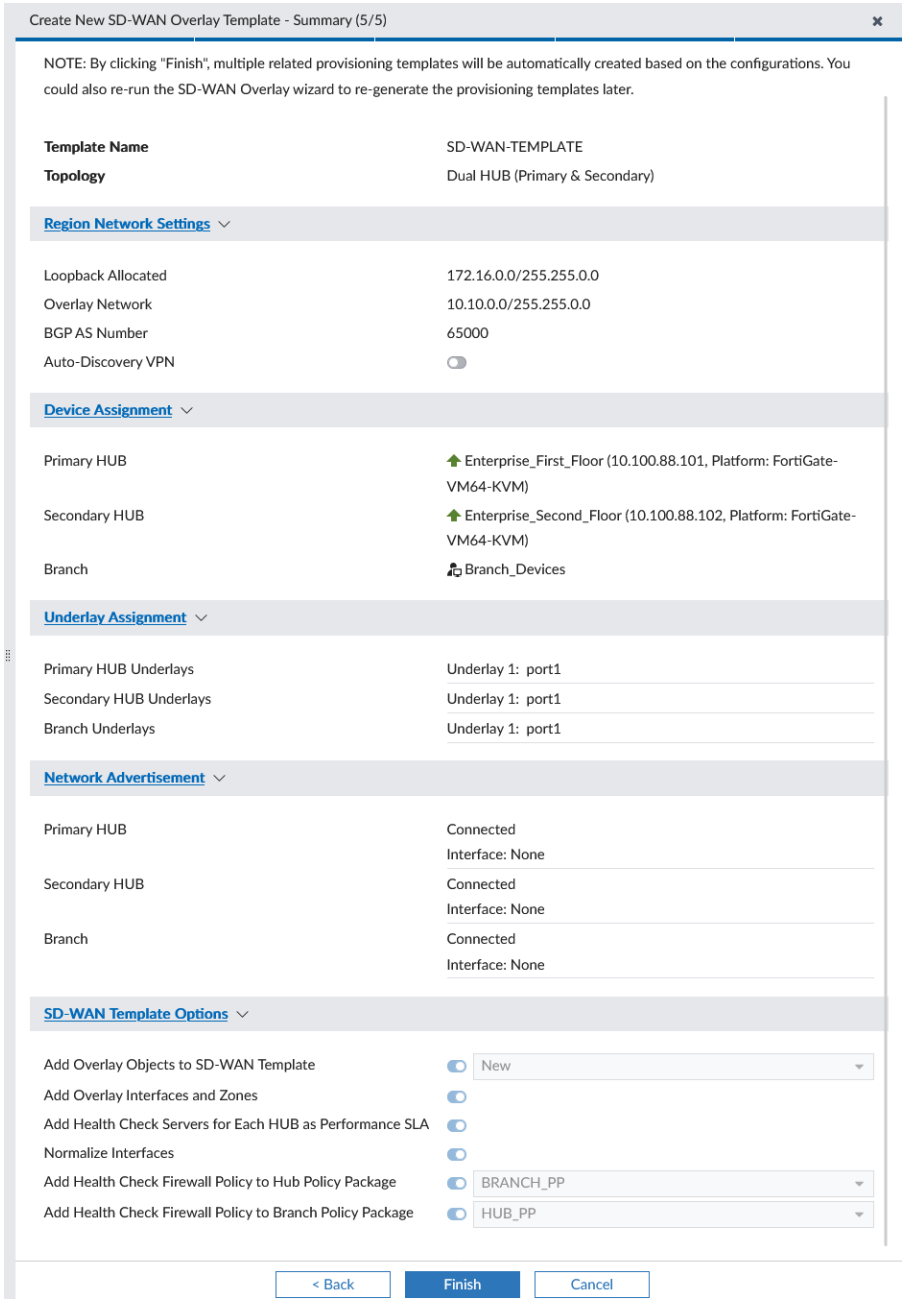
Add Overlay Objects to SD-WAN Template	Toggle this setting ON to automatically add the overlay objects configured by this template to a new or existing SD-WAN template. Select an existing SD-WAN template or click the add icon to create a new SD-WAN template. See SD-WAN templates on page 304.
Add Overlay Interfaces and Zones	You can toggle this setting ON to add overlay interfaces and zones.
Add Healthcheck Servers for Each HUB as Performance SLA	You can toggle this setting ON to add health check servers for each hub as performance SLAs.

Normalize Interfaces	Enable this setting to automatically normalize the SD-WAN zones created by the template.
	The template creates the following normalized interfaces:
	• HUB-Lo with the following per-device mapping:
	  • HUB1-Lo for HUB1.
	  • HUB2-Lo for HUB2 (dual-HUB topology).
	• HUB1 SD-WAN zone mapped per-platform to HUB1.
	• HUB2 SD-WAN zone mapped per-platform to HUB2 (dual-HUB topology).
	• Normalized interfaces for VPN IPsec tunnel templates created by the wizard are added to the normalized interface list as VPN1/VPN2.

Add Health Check Firewall Policy to HUB/Branch Policy Package	Enable this setting to automatically create health check firewall policies and policy blocks for HUBs and branches. When enabled, you must select a new or existing policy package. Based on the selection, firewall policies and policy blocks are created to allow SLA health checks to each device loopback.

8. The summary window displays a summary of the SD-WAN overlay configurations that will be created by this template. When you click *Finish*, multiple provisioning templates are created based on the information

you provided. The templates are automatically assigned to the devices specified by the wizard.



9. Once complete, you can continue to deploy the SD-WAN provisioning templates in your environment. See Using the SD-WAN overlay template on page 329.

Using preconfigured route maps for self-healing with BGP

Preconfigured route maps are available for selection in the SD-WAN overlay template to take advantage of SD-WAN self-healing using BGP.

FortiManager includes the following preconfigured route maps:

- **Hubs**: *RM-VPN-Priority*.
- **Branches**: *Priority_1*, *Priority_2*, *Priority_3*, *Priority_4*, and *Priority_999* (used as a catch all).

Hubs are automatically configured with five communities, with a corresponding route map matched to each community. Each route map will advertise a given community based on the SD-WAN overlay template AS. Based on the advertised community from the branch, the priority value will determine the preferred routing. For example, the *priority_1* route is preferred over *priority_2*.

Editing the SD-WAN overlay template

When editing an existing SD-WAN overlay template, the provisioning templates that were generated by the SD-WAN overlay template previously are updated. These updated provisioning templates can then be reinstalled to applicable SD-WAN branch and hub devices.

You can also directly edit the provisioning templates generated by the SD-WAN overlay template (for example, BGP and IPsec templates), but further edits to the SD-WAN overlay template may overwrite those changes. For example, you can change the Local AS setting in the BGP hub template, but when the SD-WAN overlay template is run again, the field is updated with the value specified by the SD-WAN overlay template. Fields not included by the SD-WAN overlay template, such as descriptions, are not affected.

To edit an SD-WAN overlay template:

1. Go to *Device Manager > Provisioning Templates > SD-WAN Overlay Templates*.
2. Select a template from the list, and click *Edit* in the toolbar.
3. Edit the template details by following the wizard, and click *Finish* to save your changes.
   Previously generated provisioning templates are updated to match the newly configured settings, and can be installed to devices.

Onboarding new branch devices

The SD-WAN overlay template uses a device group to determine which devices receive the SD-WAN provisioning templates.

When a new device is added to the device group, the SD-WAN provisioning templates are automatically assigned to the device, and you can install the changes using the Install Wizard.

Branch onboarding can be further simplified with the use of device blueprints and metadata variables:

- Device blueprints can be used when adding model devices to FortiManager to simplify configuration of device settings, including device groups, configuring pre-run templates, policy packages, provisioning templates, and more. See Using device blueprints for model devices on page 114.
- Metadata variables can be used as variables in provisioning templates. The `branch_id` variable is automatically created by the template and each branch device must be assigned a unique value. A branch ID value can be automatically assigned to devices in the SD-WAN branch device group when the *Automatic Branch ID Assignment* setting is enabled in the SD-WAN overlay template wizard. See ADOM-level metadata variables on page 557.

When onboarding multiple new branch devices, you can import devices from a CSV file using device blueprints. Metadata fields including the `branch_id` variable can be specified directly in the CSV file. See Import model devices from a CSV file on page 116.

To onboard new branch devices:

1. Add the new FortiGate model device to FortiManager using the Device Manager.
   Optionally, you can configure a device blueprint to simplify device onboarding. See Using device blueprints for model devices on page 114.
2. Assign the FortiGate device to the template's branch device group.
   The branch provisioning templates are automatically assigned to the device.
3. Specify the metadata variables used by the SD-WAN overlay template. By default, the `branch_id` metadata variable must be specified. When *Automatic Branch ID Assignment* setting is enabled in the wizard, the branch ID is automatically applied to devices in the branch device group. See Automatic Branch ID Assignment on page 332.
4. Assign policy package for the branch device, and then install the changes using the Install Wizard. See Install wizard on page 180.

Objects and templates created by the SD-WAN overlay template

The SD-WAN overlay wizard automatically creates templates and objects required for deployment of SD-WAN in your environment. Generated templates and objects are assigned to the hub(s) specified by the template, and branch devices are identified by membership in the specified device group. See Configuring an SD-WAN overlay template on page 330.

The following template and objects are created by the SD-WAN overlay template wizard:

- IPsec templates
- BGP templates
- SD-WAN template configuration
- CLI templates
- Templates groups
- Metadata variables

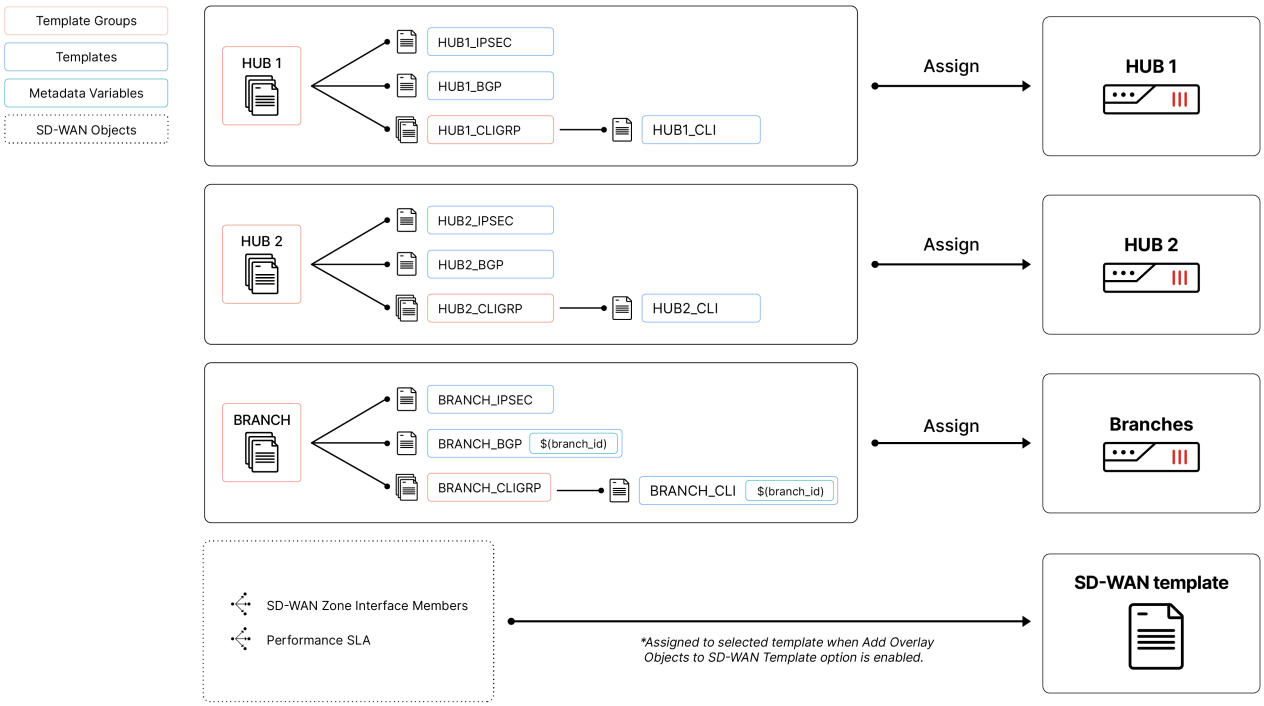
The SD-WAN overlay template wizard also configures the SD-WAN overlay network. The default overlay network used by the wizard is 10.10.0.0, but this can be configured for your environment. The number of subnets created from the overlay network depends on the number of overlays and hubs that are configured.

Below details the various templates and associated components that are defined in dual-hub and single-hub deployment scenarios.

- Dual-hub deployments on page 339
- Single-hub deployments on page 341

Dual-hub deployments

Template and object assignment (dual-hub)



Category	Templates and Objects
IPsec Templates	The following IPsec templates are created for configuration of IPsec in your SD-WAN environment: • **BRANCH_IPsec**: The IPsec template for IPsec tunnels for branch devices. This template includes the following IPsec tunnels to allow connection from branch devices to the hubs through VPN1 and VPN2: *HUB1-VPN1*, *HUB1-VPN2*, *HUB2-VPN1*, and *HUB2-VPN2*. • **HUB1_IPsec**: The IPsec template created for hub 1. This template includes the IPsec tunnels *VPN1* and *VPN2* to allow secure communication from hub 1 to branch devices. • **HUB2_IPsec**: The IPsec template created for hub 2. This template includes the IPsec tunnels *VPN1* and *VPN2* to allow secure communication from hub 2 to branch devices.
BGP Templates	The following BGP templates are created for configuration of BGP in your SD-WAN environment: • **BRANCH_BGP**:The BGP template generated for your SD-WAN branch devices. This template uses the *branch_id* metadata variable to configure the Router ID for each branch device. • **HUB1_BGP**: The BGP template created for hub 1. • **HUB2_BGP**: The BGP template created for hub 2.

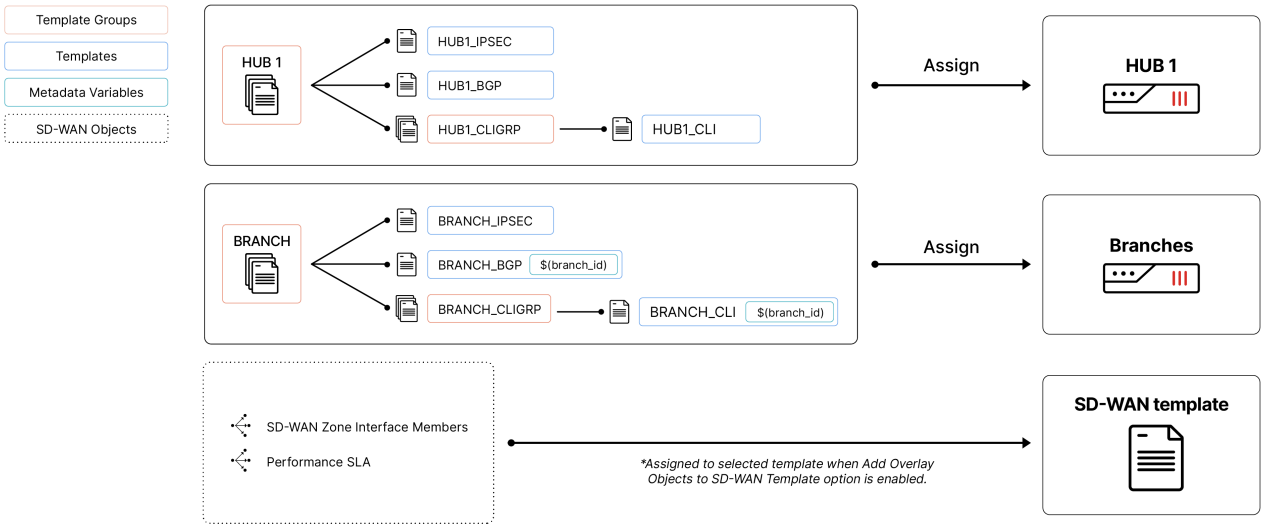
Category	Templates and Objects
SD-WAN Template configurations	The following SD-WAN zones/members and health check servers are configured for the SD-WAN template specified in the wizard. • **SD-WAN Zone/Interface Member**: WAN1/port1, WAN2/port2, HUB1/HUB1-VPN1 and HUB1-VPN2, HUB2/HUB2-VPN1 and HUB2-VPN2 • **Performance SLA**: HUB1_HC and HUB2_HC  These settings are only applied when the *Add Overlay Objects to SD-WAN Template* option is enabled in the wizard.
CLI Templates	The following CLI templates are created to configure the device interfaces and BGP router ID. • **BRANCH_CLI**: Configure the interface and BGP router id for branch devices. This template uses metadata variables to configure unique values for each branch device. This template is added to the *BRANCH_CLIGRP* template group. • **HUB1_CLI**: Configure the HUB1-Lo interface on the hub 1 device. This template is added to the *HUB1_CLIGRP* template group. • **HUB2_CLI**: Configure the HUB2-Lo interface on the hub 2 device. This template is added to the *HUB2_CLIGRP* template group.
Template Groups	A template group is created for hub and branch devices. These template groups include the provisioning templates created by the SD-WAN overlay template wizard for that device. • **HUB1**: Includes provisioning templates for the hub 1 device. • **HUB2**: Includes provisioning templates for the hub 2 device. • **BRANCH**: Includes provisioning templates for branch devices. This template is automatically applied to all devices included in the branch device group specified in the wizard. For information about onboarding new branch devices using template groups, see Onboarding new branch devices on page 337
Metadata Variables	ADOM-level metadata variables are used as variables in scripts and templates. • **branch_id**: The `branch_id` variable is automatically created by the template. Each branch device must be assigned a unique value. The *branch_id* metadata variable is used in branch provisioning templates to configure certain settings, such as the BGP router ID. When *Automatic Branch ID Assignment* setting is enabled in the wizard, the branch ID is automatically applied to devices in the branch device group. See Automatic Branch ID Assignment on page 332.

Normalized Interfaces	When normalized interfaces is enabled in the template, the following normalized interfaces are created:
	• HUB-Lo with the following per-device mapping:
	  • HUB1-Lo for HUB1.
	  • HUB2-Lo for HUB2 (dual-HUB topology).

Category	Templates and Objects
	• HUB1 SD-WAN zone mapped per-platform to HUB1. • HUB2 SD-WAN zone mapped per-platform to HUB2 (dual-HUB topology). • Normalized interfaces for VPN IPsec tunnel templates created by the wizard are added to the normalized interface list as VPN1/VPN2.

Single-hub deployments

Template and object assignment (single-hub)



Category	Templates and Objects
IPsec Templates	The following IPsec templates are created for configuration of IPsec in your SD-WAN environment: • **BRANCH_IPsec**: The IPsec template for IPsec tunnels for branch devices. This template includes the following IPsec tunnels to allow connection from branch devices to the hubs through VPN1 and VPN2: *HUB1-VPN1* and *HUB1-VPN2*. • **HUB1_IPsec**: The IPsec template created for the hub. This template includes the IPsec tunnels *VPN1* and *VPN2* to allow secure communication from the hub to branch devices.
BGP Templates	The following BGP templates are created for configuration of BGP in your SD-WAN environment: • **BRANCH_BGP**:The BGP template generated for your SD-WAN branch devices. This template uses the *branch_id* metadata variable to configure the Router ID for each branch device. • **HUB1_BGP**: The BGP template created for the hub.
SD-WAN Template configurations	The following SD-WAN zones/members and health check servers are configured for the SD-WAN template specified in the wizard. • **SD-WAN Zone/Interface Member**: WAN1/port1, WAN2/port2, HUB1/HUB1-VPN1 and HUB1-VPN2.

Category	Templates and Objects
	• **Performance SLA**: HUB1_HC.  These settings are only applied when the *Add Overlay Objects to SD-WAN Template* option is enabled in the wizard.
CLI Templates	The following CLI templates are created to configure the device interfaces and BGP router ID. • **BRANCH_CLI**: Configure the interface and BGP router id for branch devices. This template uses metadata variables to configure unique values for each branch device. This template is added to the *BRANCH_CLIGRP* template group. • **HUB1_CLI**: Configure the HUB1-Lo interface on the hub device. This template is added to the *HUB1_CLIGRP* template group.
Template Groups	A template group is created for hub and branch devices. These template groups include the provisioning templates created by the SD-WAN overlay template wizard for that device. • **HUB1**: Includes provisioning templates for the hub 1 device. • **BRANCH**: Includes provisioning templates for branch devices. The template is automatically applied to all devices included in the branch device group selected in the wizard. For information about onboarding new branch devices using template groups, see Onboarding new branch devices on page 337
Metadata Variables	ADOM-level metadata variables are used as variables in scripts and templates. • **branch_id**: The `branch_id` variable is automatically created by the template. Each branch device must be assigned a unique value. The *branch_id* metadata variable is used in branch provisioning templates to configure certain settings, such as the BGP router ID. When *Automatic Branch ID Assignment* setting is enabled in the wizard, the branch ID is automatically applied to devices in the branch device group. See Automatic Branch ID Assignment on page 332.
Normalized Interfaces	When normalized interfaces is enabled in the template, the following normalized interfaces are created: • HUB-Lo with the following per-device mapping: HUB1-Lo for HUB1. • HUB1 SD-WAN zone mapped per-platform to HUB1. • Normalized interfaces for VPN IPsec tunnel templates created by the wizard are added to the normalized interface list as VPN1/VPN2.

SD-WAN overlay template IP network design

The SD-WAN overlay template creates the overlay IP network and subnets for your SD-WAN environment. The wizard uses the default range of `10.10.0.0/16`, but this network range can be customized in the SD-WAN overlay template wizard under *Region Settings* > *Advanced*.

The overlay network is used to define the VPN tunnel interfaces for hubs and spokes, and is subnetted so that each overlay network is unique and distinct. The number of subnets created is determined based on the number

of physical underlay ports that are identified in the *Network Configuration* section of the wizard. Each configured underlay requires one overlay subnet.

By default, single-hub topologies have a minimum of four subnets, and dual-hub topologies have a minimum of eight subnets. When more than four underlays are configured, the overlay network is further subnetted into the nearest power of two. For example, configuring five physical underlays in the wizard for a single-hub topology results in the creation of eight overlay subnets, with only the first five being used.

The table below shows an example of the subnet ranges that are created based on the number of underlay ports configured in the wizard using the default `10.10.0.0/16` network.

Number of Underlays	Overlay Subnet Address	Overlay's Usable IPs	Number of FortiGates per Overlay
1 - 4 underlays Only possible with single-hub	10.10.0.0/18	10.10.0.1 - 10.10.63.254	16382
	10.10.64.0/18	10.10.64.1 - 10.10.127.254	16382
	10.10.128.0/18	10.10.128.1 - 10.10.191.254	16382
	10.10.192.0/18	10.10.192.1 - 10.10.255.254	16382
5 - 8 underlays Minimum required for dual-hub.	10.10.0.0/19	10.10.0.1 - 10.10.31.254	8190
	10.10.32.0/19	10.10.32.1 - 10.10.63.254	8190
	10.10.64.0/19	10.10.64.1 - 10.10.95.254	8190
	10.10.96.0/19	10.10.96.1 - 10.10.127.254	8190
	10.10.128.0/19	10.10.128.1 - 10.10.159.254	8190
	10.10.160.0/19	10.10.160.1 - 10.10.191.254	8190
	10.10.192.0/19	10.10.192.1 - 10.10.223.254	8190
	10.10.224.0/19	10.10.224.1 - 10.10.255.254	8190
9 - 16 underlays	10.10.0.0/20	10.10.0.1 - 10.10.15.254	4094
	10.10.16.0/20	10.10.16.1 - 10.10.31.254	4094
	...	...	...



In dual-hub topologies, overlay subnets are assigned so that hub 1 receives the first half and hub 2 receives the second. The colors in the table above for "5 - 8 underlays" is an example of how the overlays are assigned when there are two hubs: Blue = Hub 1. Red = Hub 2.



It may be necessary to adjust the default overlay network to something larger than `10.10.0.0/16` if you have a large number of overlays and/or branches. For example, if you have a dual-hub topology with 18 total overlays, each overlay can only support 2046 FortiGates. If you have 2100 branches, you will need to supply a larger overlay network such as `10.0.0.0/8`.

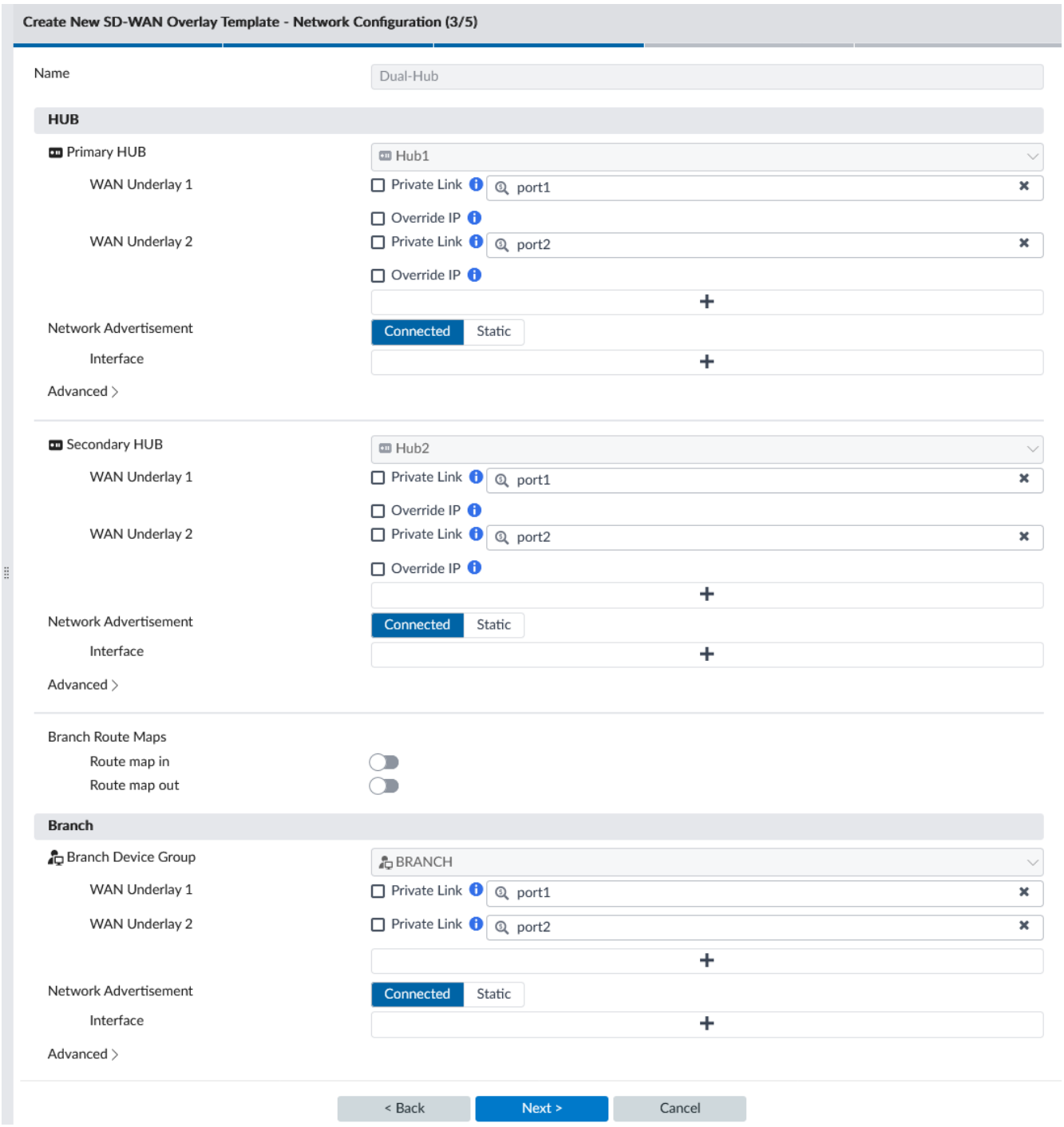
Examples

The wizard includes topologies for single-hub, dual-hub (primary & secondary), and dual-hub (primary & primary). Here you can find an example of how the IP overlya network is designed in a dual-hub (primary & secondary) and single-hub topology using the default overlay network.

Dual-hub (primary & secondary)

In dual-hub topologies, overlay subnets are assigned so that hub 1 receives the first half and hub 2 receives the second.

In this example, four underlays (two for the primary hub and two for the secondary hub) are configured in the default dual-hub (primary & secondary) topology.



With this configuration:

- Hub 1 uses overlay subnet 1 (`10.10.0.0/19`) for *HUB1_VPN1* and subnet 2 (`10.10.32.0/19`) for *HUB1_VPN2*.
- Hub 2 uses overlay subnet 5 (`10.10.128.0/19`) for *HUB2_VPN1* and subnet 6 (`10.10.160.0/19`) for *HUB2_VPN2*.
- Subnets 3, 4, 7, and 8 are not used because the wizard has only been configured with four underlays.

The topology diagram below demonstrates how the overlay subnets are applied in this dual-hub scenario:

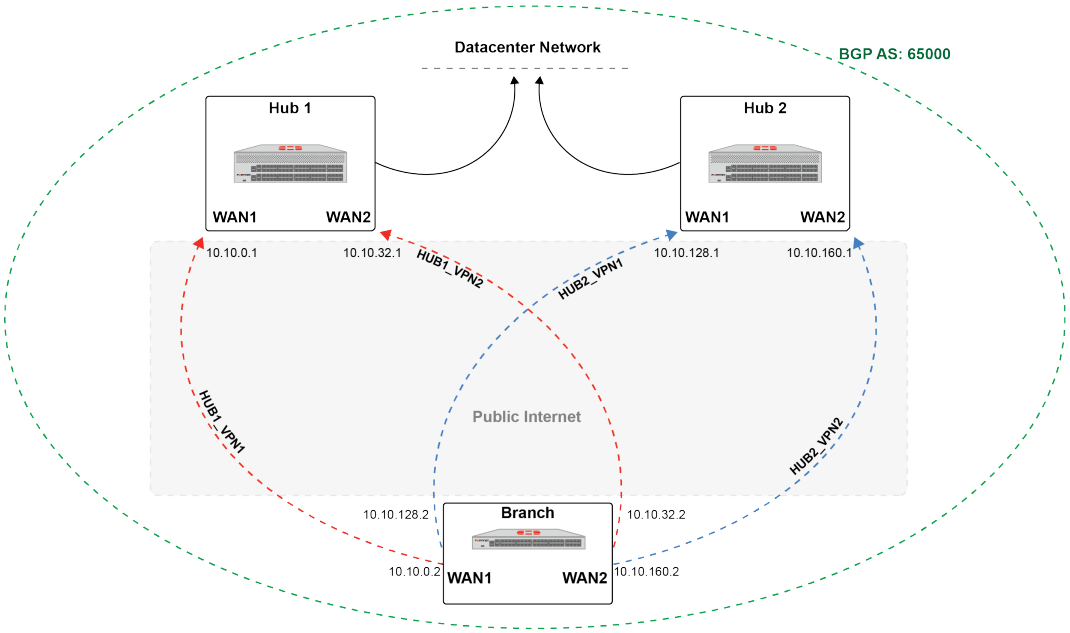
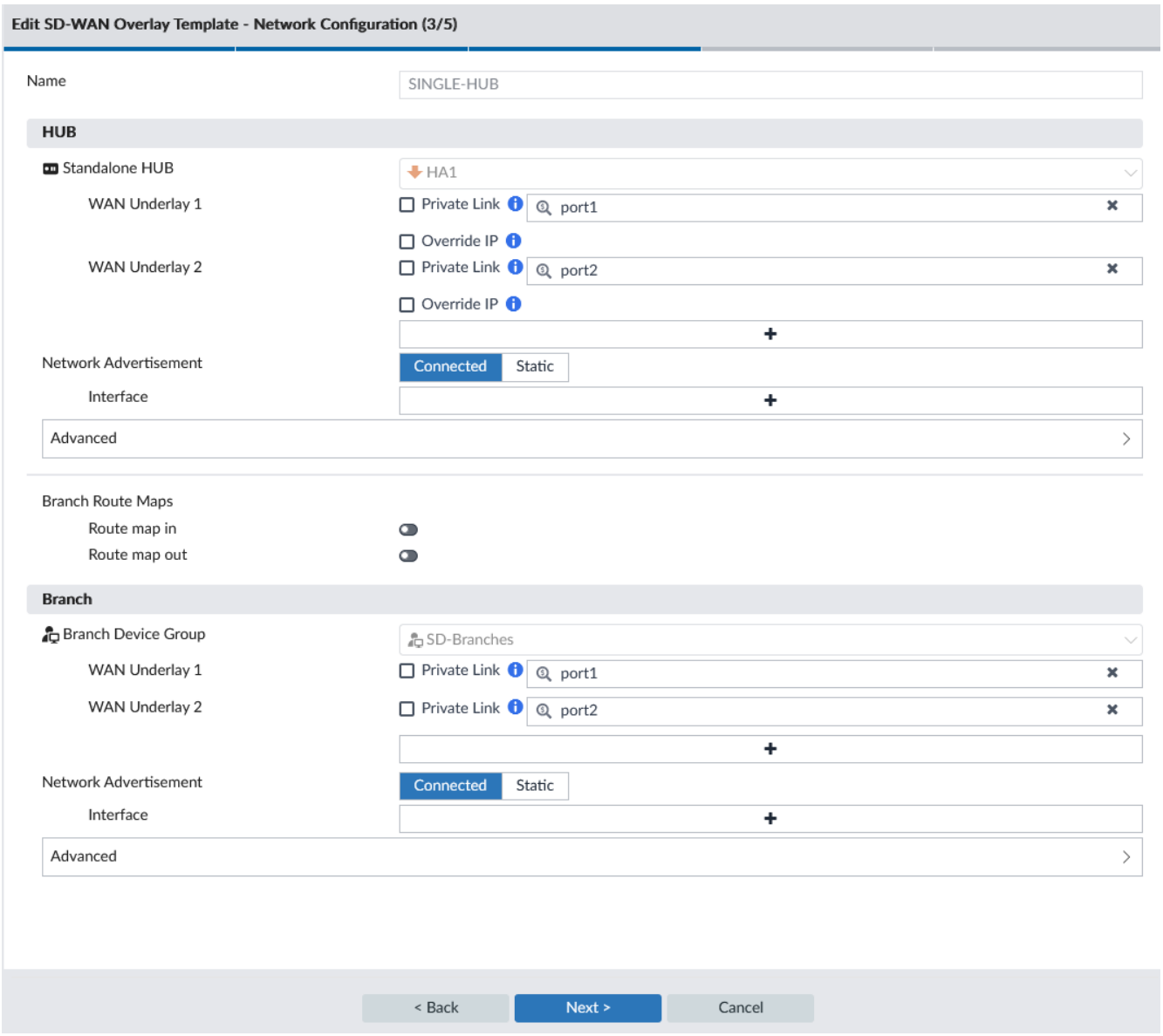


Figure 1 - SD-WAN overlay network topology for the default dual-hub (primary & secondary) configuration.

Single-hub

In single-hub topologies, at least four overlay networks are created by the wizard. If more than four WAN underlays are configured, the overlay network will be further subnetted to allow for additional overlay subnets to be created.

In this example, two physical WAN underlays are configured in this single-hub topology.



With this configuration:

- Hub 1 uses overlay subnet 1 (`10.10.0.0/18`) for *HUB1_VPN1* and subnet 2 (`10.10.64.0/18`) for *HUB1_VPN2*.
- Subnets 3 and 4 are not used because the wizard has only been configured with two underlays.

The topology diagram below demonstrates how the overlay subnets are applied in this single-hub scenario:

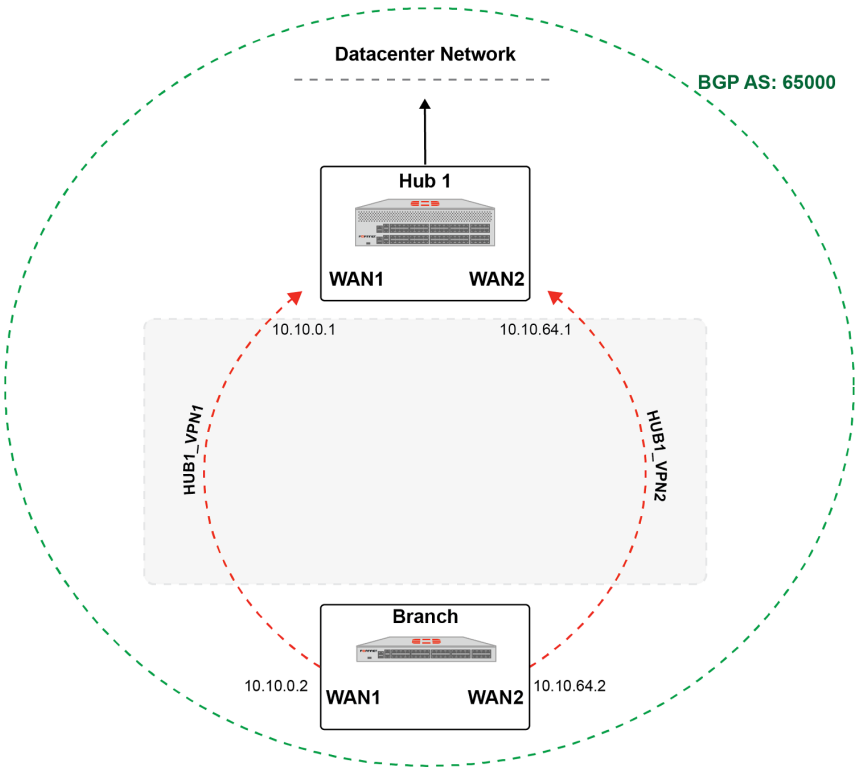


Figure 2 - SD-WAN overlay network topology for the default single-hub configuration.

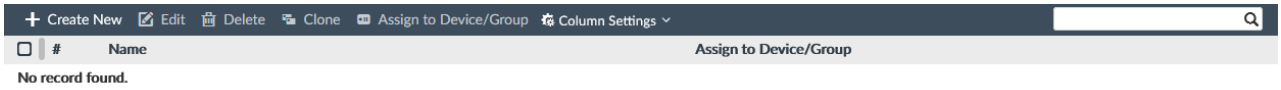
Static route templates

You can provision static routes to FortiGate devices by using a static route template.

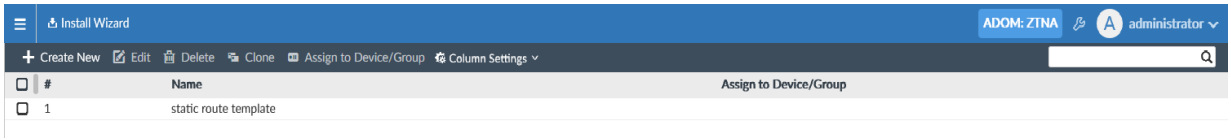
When creating static routes for IPv4 and subnets, you can use meta field variables for objects of type *device VDOM*. See Meta Fields on page 967.

To create a new static route template:

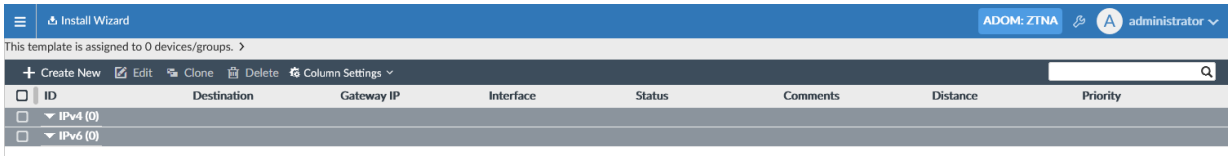
1. Go to *Device Manager* > *Provisioning Templates* > *Static Route Templates*.



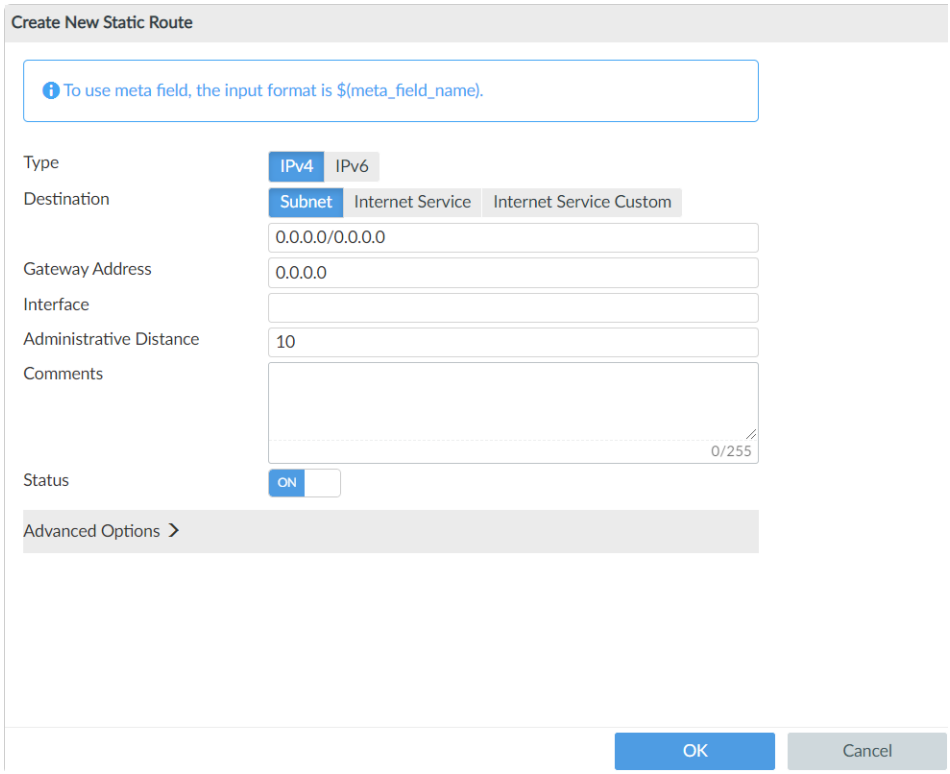
2. Create a static route template:
   a. In the toolbar, click *Create New*. The *Create New Route Template* dialog box appears.
   b. In the *Name* box, type a name for the template, and click *OK*. The new template is created.



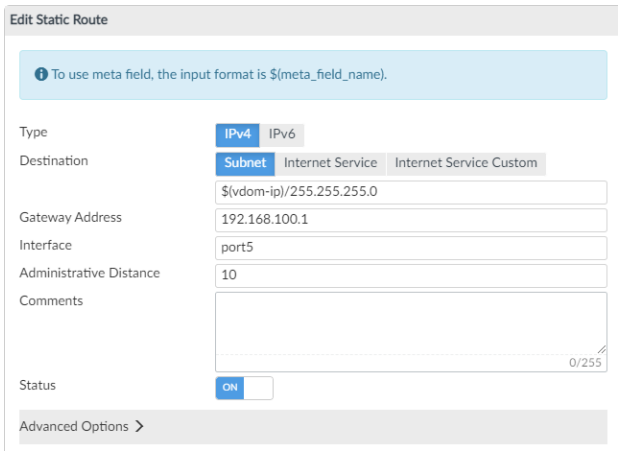
3. Open the template for editing, and create a static route:
   a. In the content pane, double-click the template. The template opens for editing.



   b. In the toolbar, click *Create New*. The *Create New Static Route* pane is displayed.



You can use meta field variables created for an object type of *Device VDOM* when creating IPv4 static routes for subnets. In the following example, variable *$(vdom-ip)* is used:



c. Complete the following options, and click *OK*.

Type	Select the type of static route. Choose between *IPv4* and *IPv6*.
Destination	Select the destination for the route. Choose between *Subnet*, *Internet Service*, and *Internet Service Custom*. When you select *Type* of *IPv4* and *Destination* of *Subnet*, you can use a meta field variable for the subnet. The input format is `$(meta_field_name)`. If not using a meta field variable, specify the subnet.
Gateway Address	Specify the IP address for the gateway.
Interface	Specify the interface.
Comments	(Optional) Type a comment about the static route.
Advanced Options	Expand to display advanced options.

The static route is created.

4. Assign the template of static routes to one or more devices or device groups.
5. Install the configuration to devices.

BGP templates

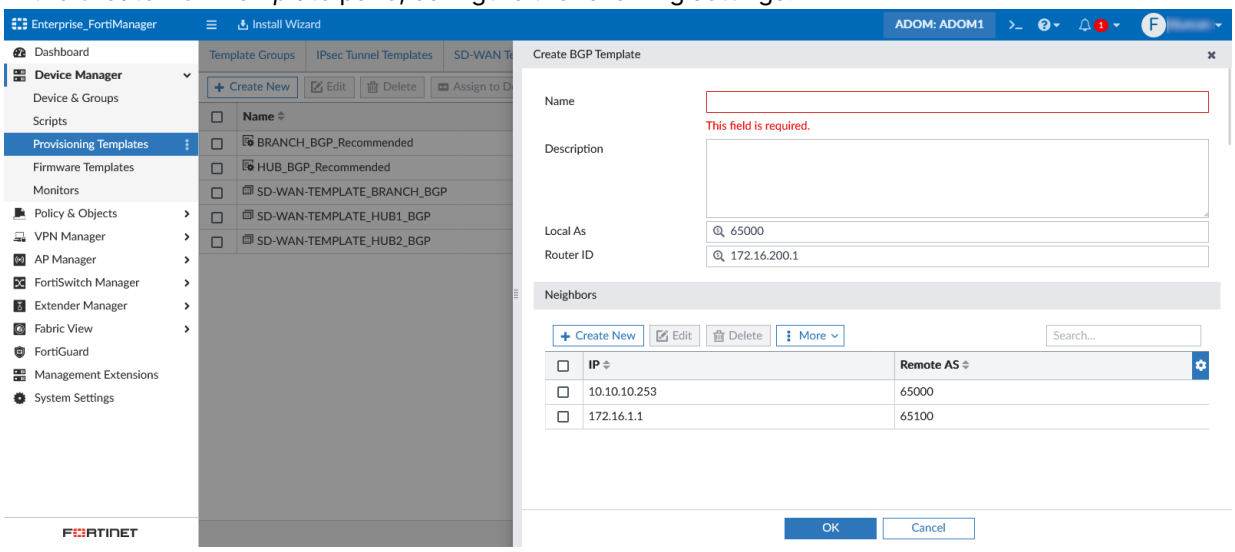
FortiManager includes Border Gateway Protocol (BGP) templates allowing you to provision BGP settings across multiple FortiGate devices.

BGP templates support the use of *Device VDOM* meta variables in the following places: router prefix-list, router-id, neighbor-range (prefix), router-map (match-ip-address), neighbor, and network (prefix).

To create a BGP template:

1. Go to *Device Manager* > *Provisioning Templates* > *BGP Template*.
2. Click *Create New* in the toolbar.

3. In the *Create BGP Template* pane, configure the following settings:



Name	Enter a name for the BGP template.
Local AS	Enter the Local AS.
Router ID	Enter the Router ID.
Neighbors	Click *Create New* to add a BGP neighbor.
Neighbor Group	The BGP neighbor group feature allows a large number of neighbors to be configured automatically based on a range of neighbors' source addresses. Click *Create New* to add a BGP neighbor group.
Neighbor Ranges	Configure the neighbor ranges to be used by neighbor groups. Click *Create New* to add a neighbor range and select the neighbor group to which the range applies.
Networks	Add IP/Netmask for networks.
IPv6 Networks	Add IP/Netmask for IPv6 networks.
IPv4 Redistribute	Enable *Connected*, *RIP*, *OSPF*, *Static*, and *ISIS* for IPv4 redistribute.
IPv6 Redistribute	Enable *Connected*, *RIP*, *OSPF*, *Static*, and *ISIS* for IPv6 redistribute.
Dampening	Expand to see dampening options.
Graceful Restart	Expand to see options for graceful restarting.
Advanced Options	Expand to see advanced options.
Best Path Selection	Expand to see options for best path selection.

When configuring a BGP *Neighbor* or *Neighbor Group*, routing objects can be created and edited inline under *IPv4 Filtering* and *IPv6 Filtering*. You can configure the following:

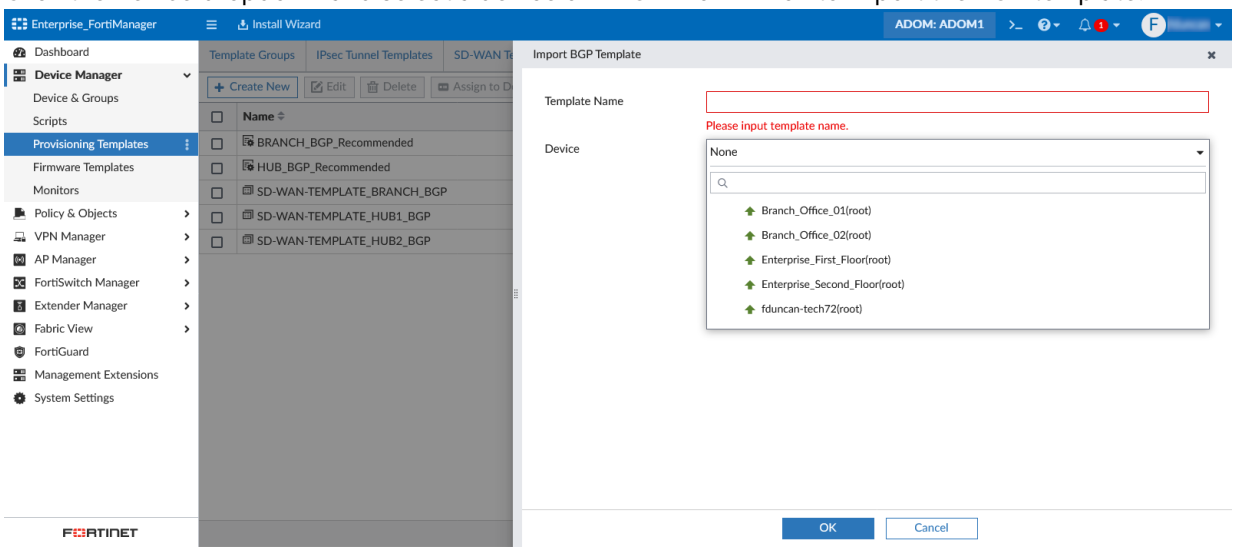
- Route Map
- Access List
- IPv6 Access List
- Prefix List
- IPv6 Prefix List
- AS Path List
- Community List

4. Click *OK* to save the template.
   See the FortiGate Administration Guide on the Fortinet Docs Libary for more information on BGP.

Importing BGP Templates

To import a BGP template:

1. Go to *Device Manager* > *Provisioning Templates* > *BGP Template*.
2. Click *Import* in the toolbar.
3. Enter a *Template Name*.
4. Click the *Device* dropdown and select a device or VDOM from which to import the BGP template.



5. Click *OK*.

Recommended BGP templates

FortiManager includes recommended BGP templates that come preconfigured with FortiManager best practices recommendations for use within your environment. These templates can be used to simplify deployment of SD-WAN interconnected sites.

Once a new BGP template has been created from a recommended template, it can be edited, deleted, and/or cloned.

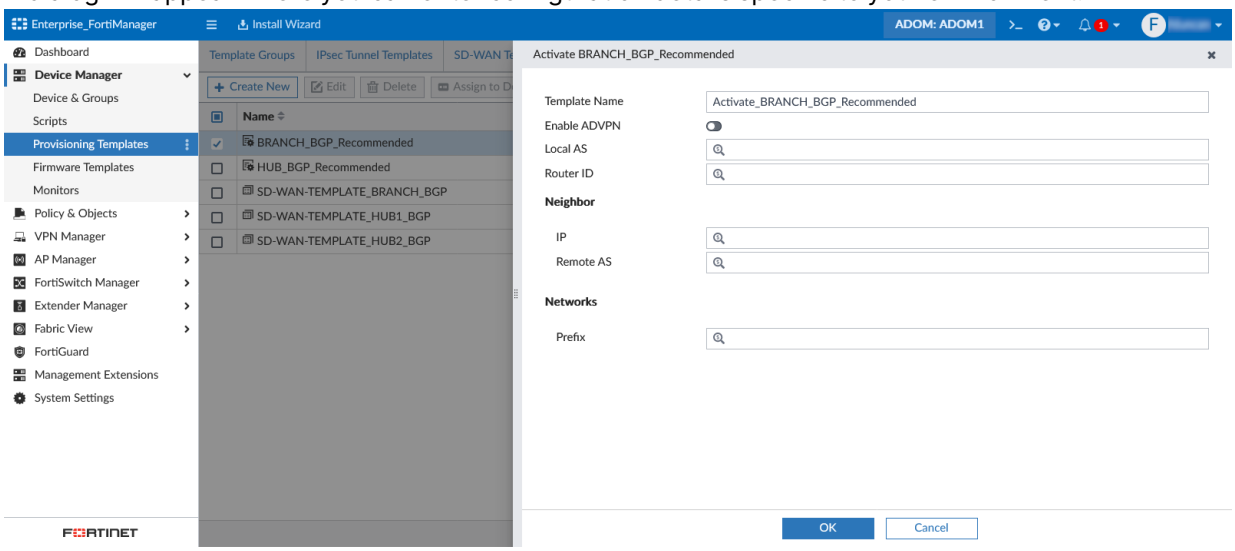
Meta fields can be used when configuring a recommended template's required fields to ensure that fields like *Router ID* are unique when the template is assigned to multiple devices. See Meta Fields on page 967.

The following BGP recommended templates are available.

Template Name	Description
BRANCH_BGP_ Recommended	Fortinet's recommended BGP template for branch device configurations.
HUB_BGP_Recommended	Fortinet's recommended BGP template for hub device configurations.

To use a default BGP template in your environment:

1. Go to *Device Manager* > *Provisioning Templates* > *BGP Templates*.
2. Select a recommended template, and click *Activate* in the toolbar.
   A dialog will appear where you can enter configuration details specific to your environment.



3. Click *OK* to save your changes.
   A new template is created in the template list based on the recommended template you selected and the configuration details provided.
4. (Optional) Edit the template to view or change the automatically configured settings.
5. (Optional) Once a template has been created, it can be added to a template group. SeeTemplate groups on page 274
6. Assign the new template or template group to a managed device/device group and then install the changes.

To create a recommended BGP hub template:

1. Activate the *HUB_BGP_Recommended* template.
2. Enter the following requested information.

Template Name	Enter a name for the template.
Enable ADVPN	Optionally, toggle this setting to enable Auto Discovery VPN (ADVPN).
Local AS	Enter the hub's local AS number.
Router ID	Enter the router ID. The router ID is the unique IP address used to identify the hub device.
Neighbor	Enter the neighbor *IP* and *Remote AS*. The neighbor IP is the IP address used while peering as a neighbor.
Neighbor Group	Enter the neighbor group's *Remote AS*.
Neighbor Range	Enter the neighbor range *Prefix*. This is the network range that branch devices use to connect to the hub.
Networks	Enter the networks *Prefix*.

3. Select *OK* to create the template.

To create a recommended BGP branch template:

1. Activate the *BRANCH_BGP_Recommended* template.
2. Enter the following requested information.

Template Name	Enter a name for the template.
Enable ADVPN	Optionally, toggle this setting to enable Auto Discovery VPN (ADVPN).
Local AS	Enter the branch's local AS number.
Router ID	Enter the router ID. The router ID is the unique IP address used to identify the branch device.
Neighbor	Enter the neighbor *IP* and *Remote AS*.
Networks	Enter the networks *Prefix*.

3. Select *OK* to create the template.

Certificate templates

The certificate templates menu allows you to create certificate templates for an external certificate authority (CA) or the local FortiManager CA.

FortiManager includes a certificate authority server for each ADOM. When you create an ADOM, the private and public key pair is created for the ADOM. The key pair is automatically used when you use FortiManager to define IPsec VPNs or SSL-VPNs for a device.

When you add a device to an IPsec VPN or SSL-VPN topology with a certificate template that uses the FortiManager CA, the local FortiManager CA is automatically used. No request for a pre-shared key (PSK) is generated. When the IPsec VPN or SSL-VPN topology is installed to the device, the following process completes automatically:

- The FortiGate device generates a certificate signing request (CSR) file.
- FortiManager signs the CSR file and installs the CSR file on the FortiGate device.
- The CA certificate with public key is installed on the FortiGate device.



Some settings may not be available in all ADOM versions.

The following options are available:

Create New	Create a new certificate template.
Edit	Edit a certificate template. Right-click a certificate template, and select *Edit*.
Delete	Delete a certificate template. Right-click a certificate template, and select *Delete*.
Generate	Create a new certificate from a device.

To create a new certificate template:

1. Go to *Device Manager > Provisioning Templates > Certificate Templates*.
2. Click *Create New*. The *Create New Certificate Template* pane opens.
3. Enter the following information, then click *OK* to create the certificate template:

Type	Specify whether the certificate uses an external or local certificate authority (CA). When you select *External*, you must specify details about online SCEP enrollment. When you select *Local*, you are using the FortiManager CA server.
Certificate Name	Type a name for the certificate.
Optional Information	Optionally, type the organization unit, organization, locality (city), province or state, country or region, and email address.
Key Type	RSA is the default key type. This field cannot be edited.
Key Size	Select the key size from the dropdown list: 512 bit, 1024 bit, 1536 bit, or 2048 bit.
Online SCEP Enrollment	These options are only available when the certificate type is *External*.
CA Server URL	Type the server URL for the external CA.
Challenge Password	Type the challenge password for the external CA server.

To edit a certificate template:

1. Select a certificate template, and click *Edit*.
2. Edit the settings as required in the *Edit Certificate Template* pane, and click *OK*.

To delete a certificate template:

1. Select a certificate template, and click *Delete*.
2. Click *OK* in the confirmation dialog box.

To renew a certificate which uses FortiManager as the CA:

1. Right click on the certificate template used to generate the certificate.
2. Select *Generate*.
3. On the next install, the device will receive a new certificate.

Threat Weight templates

User or client behavior can sometimes increase the risk of being attacked or becoming infected. For example, if one of your network clients receives email viruses on a daily basis while no other clients receive these attachments, extra measures may be required to protect that client, or a discussion with the user about this issue may be warranted.

Before you can decide on a course of action, you need to know the problem is occurring. Threat weight can provide this information by tracking client behavior and reporting on activities that you determine are risky or worth tracking.

Threat weight profiles can be created, edited, and assigned to devices. When Threat Weight Tracking is enabled, the *Log Allowed Traffic* setting is enabled on all policies.

To create a new threat weight profile:

1. Go to the *Device Manager* > *Provisioning Templates* > *Threat Weight*.
2. Click *Create New* in the toolbar.
3. In the *Create New Threat Weight* pane, type a name for the profile.
4. Click *OK* to create the new threat weight profile.

To edit a threat weight profile:

1. Select a threat weight profile and click *Edit*. The *Edit Threat Weight*pane opens.
2. Adjust the threat levels as needed, then click *OK* to save your changes:

Log Threat Weight	Turn on threat weight tracking.
Reset	Reset all the threat level definition values to their defaults.
Import	Import threat level definitions from a device in the ADOM.

Application Protection	Adjust the tracking levels for the different application types that can be tracked.
Intrusion Protection	Adjust the tracking levels for the different attack types that can be tracked.
Malware Protection	Adjust the tracking levels for the malware or botnet connections that can be detected.
Packet Based Inspection	Adjust the tracking levels for failed connection attempts and traffic blocked by firewall policies.
Web Activity	Adjust the tracking levels for various types of web activity.
Risk Level Values	Adjust the values for the four risk levels.

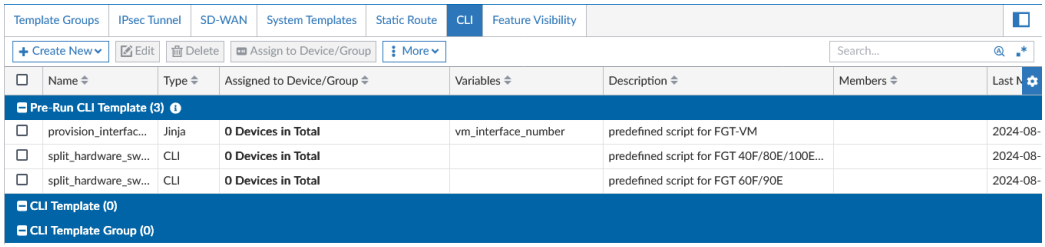
To assign a threat weight profile to a device:

1. Select a threat weight profile and click *Assign to Device*.
2. Select devices to assign to and click *OK*.
   The devices assigned to the template are shown in the *Assign to Device* column.

CLI templates

You can create CLI templates and assign them to devices. You can also create CLI template groups of multiple CLI scripts, and assign the CLI template group to devices, instead of assigning individual scripts to devices.

Go to *Device Manager* > *Provisioning Templates* > *CLI Templates* to view entries in the content pane.



The following information is displayed:

Name	The user-defined template name.
Type	The CLI template type (CLI or Jinja).
Assigned Device/Group	The device or device group to which the template is assigned.
Variables	The variables used in the script.
Description	User defined description for the template.
Members	Used for CLI template groups. Displays the CLI scripts that are members of the CLI template group.

The following options are available in the toolbar, in the *More* menu, or in the right-click menu.

Create New		Create *Pre-Run CLI Templates* and *CLI Templates*. See Adding CLI templates on page 358. You can also create a CLI template group. See CLI template groups on page 363.
Edit		Edit the selected template or template group. See Editing CLI templates on page 360.
Delete		Delete the selected template or template group. See Deleting CLI templates on page 360.
Assign to Device/Group		Assign the selected template or template group to a managed device or device group. See Assigning CLI templates to managed devices on page 360.
More		Select a template or template group, and click the *More* menu to access additional options including *Clone*, *Validate*, *Import CLI Template*, and *Export CLI Template*.
	Clone	Clone the selected CLI template or template group. See Cloning CLI templates on page 361.
	Validate	Validate the selected CLI template. Template validation is used to determine if your template is producing the correct output based on the metadata variables used. See Validate CLI templates on page 362.
	Import CLI Template	Import a template or template group from your management computer. See Importing CLI templates on page 361.
	Export CLI Template	Export a template or template group. See Exporting CLI templates on page 362.
Search		Enter a search term in the search field to search a template or template group.

CLI templates can be put into groups so that multiple templates may be assigned to managed devices at the same time. See CLI template groups on page 363.



CLI templates do not support `execute` and `diagnose` commands.

The use of `config global` and `config vdom` commands is not supported in CLI Templates.



By design, the following FortiOS settings under `system central-management` cannot be modified using FortiManager database scripts or CLI templates: `fmg`, `fmg-source-ip`, `fmg-source-ip6`, `serial-number`, `type`, and `vdom`.

Attempting to commit changes to these fields will result in the following error: *not allowed to change*.

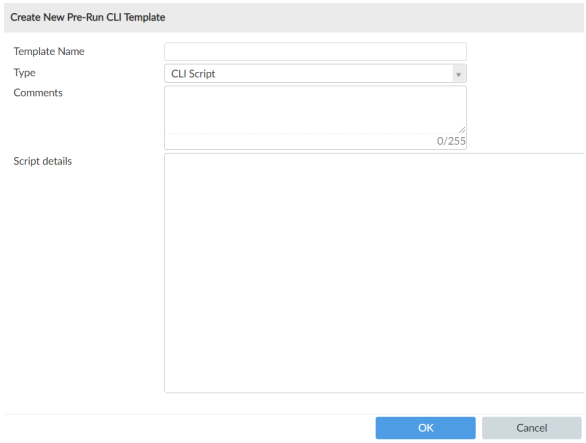
If you need to apply changes to these fields using FortiManager, a *CLI Script* can be used and run against the *Remote FortiGate Directly (via CLI)*.

Adding CLI templates

You can add *Pre-Run CLI Templates* and *CLI Templates*.

To add a CLI template:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Templates*.
2. Click *Create New* , and select either *Pre-Run CLI template* or *CLI Template*.
   The *Create New Pre-Run CLI Template*/*Create New CLI Template* pane is displayed.



3. Enter the required information:

Template Name	Type a unique name for the template.
Type	Select the template type from one of the following options: • CLI Script • Jinja Script
Comments	Optionally, type a comment for the template.
Script details	Type the script itself, either manually using a keyboard, or by copying and pasting from another editor.

4. Click *OK*.
   The CLI template is created and displayed under it's appropriate category. For example, if you created a pre-run CLI template, it displays under the *Pre-Run CLI Template* category.

Using pre-run CLI templates

Pre-Run CLI templates run once on a model device to pre-configure them with required settings, for example to add interfaces to a FortiGate-VM. Pre-run CLI templates are exclusively available to model devices, and can only be assigned to model devices.

You can assign pre-run CLI templates to model devices directly or with the use of device blueprints. See Assigning CLI templates to managed devices on page 360 and Using device blueprints for model devices on page 114.

When a pre-run CLI template has been assigned to a model device, it will be automatically applied to the model device's *Device Database* once the *Add Device* wizard completes. Once applied, the pre-run CLI template is unassigned from the model device.

If the configuration fails to apply to the Device Database, FortiManager will display an error. When this occurs, administrators can review and update the pre-run CLI template as needed and then manually reassign it to the device and perform an install to reapply the configuration to the model device's *Device Database*.

For more information see Sequence of operations for installation to managed devices on page 55.

Editing CLI templates

You can edit CLI templates to change script details. You cannot change the name of the template or the type of template.

To edit a template:

1. Go to *Device Manager > Provisioning Templates > CLI Templates*.
   Alternately, you can double-click the name of the template, or right-click the template name, and select *Edit* from the menu.
2. Select a template, and click *Edit*.
   The *Edit CLI Template* pane is displayed.
3. Edit the script details, and click *OK*.
   The changes are saved.

Deleting CLI templates

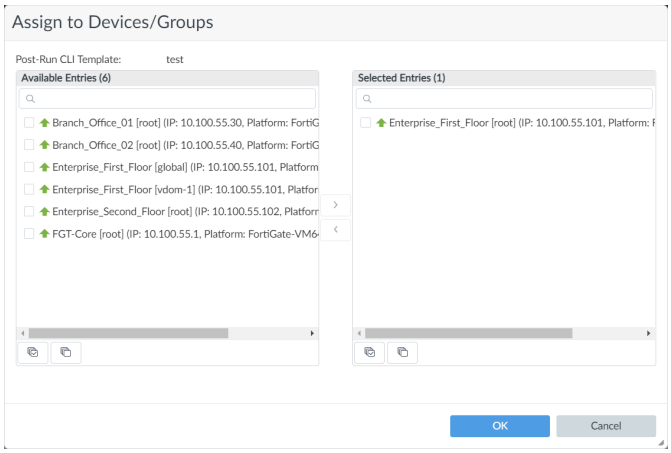
To delete a template or templates:

1. Go to *Device Manager > Provisioning Templates > CLI Templates*.
2. Select the template to be deleted, or select multiple templates by holding down the *Ctrl* or *Shift* key.
3. Right-click anywhere in the template list window, and select *Delete*, or click *Delete* from the toolbar above.
4. Click *OK* in the confirmation dialog box to delete the template or templates.

Assigning CLI templates to managed devices

To assign a template or templates to managed devices:

1. Go to *Device Manager > Provisioning Templates > CLI Templates*.
2. Select a template, and click *Assign to Device/Group*.
   The *Assign to Devices/Groups* dialog box is displayed.



3. In the *Available Entries* list, select devices or device groups, and click > to move those entries to the *Selected Entries* list.
   When a device is missing meta variables required by the script, an X icon is displayed next to the device's name, and you are not able to install the script to the device. You can hover your mouse over the icon to see which meta variables are not set.
4. Click *OK*.

Importing CLI templates

To import a template:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Templates*.
2. In the toolbar, click *Import CLI Template*. The *Import CLI Template* dialog appears.
3. Drag and drop the template file onto the dialog box, or click *Add Files* and locate the file to be imported from your local computer.
4. Click *Import* to import the template.
   If the template cannot be read, due to an incorrect file type or other issue, an error message will be displayed and the import process will be canceled.

Cloning CLI templates

Cloning a template is useful when there is a need for multiple templates that are very similar.

To clone a template:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Templates*.
2. Right-click a template, and select *Clone* from the menu, or select a template and click *More* > *Clone* from the toolbar.
   The *Clone Template* dialog appears, showing the exact same information as the original template, except *copy_* is prepended to the template name.
3. Edit the template and its settings as needed then click *OK* to create the clone.

Exporting CLI templates

Templates can be exported as text files (`.txt`) to your local computer.

To export a template:

1. Go to *Device Manager > Provisioning Templates > CLI Templates*.
2. Right-click a template, and select *Export* from the menu, or select templates from the template list and click *More > Export* from the toolbar.
3. If prompted by your web browser, open the text file to view it or select a location on your computer to save it.
4. Click *OK*.

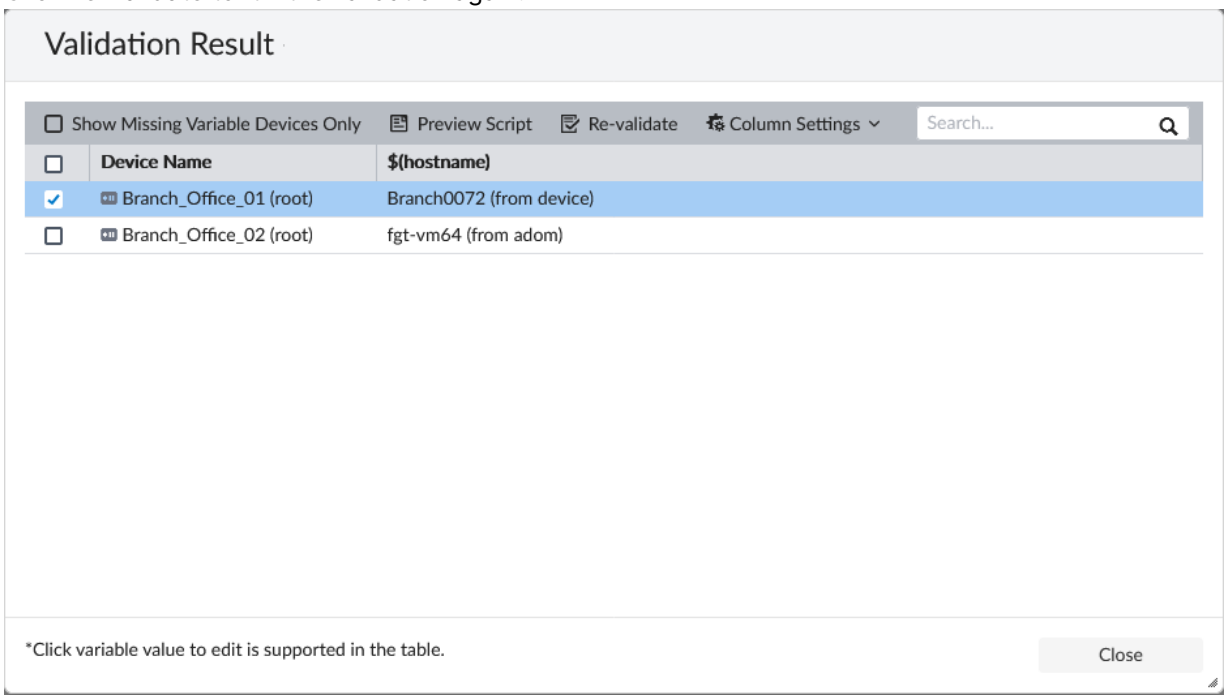
Validate CLI templates

Template validation is used to determine if your template is producing the correct output based on the meta variables used in the template. For more information on meta variables, see Meta Fields on page 967.

To validate the meta variables used in a CLI template:

1. Go to *Device Manager > Provisioning Templates > CLI Templates*.
2. Select a template from the table that is assigned to one or more devices.
3. In the toolbar, click *More > Validate*.
   The Validate CLI Template dialog opens and displays each device to which the template is assigned, and the status of the meta variables.
4. Click *View Validation Result* to view detailed information, including the meta variable value assigned to each device.
   The following features are available:
   - Click a variable value in the table to edit the value.
   - Click *Show Missing Variable Devices Only* to filter by devices that are missing variable values.
   - Click *Preview Script* to view the script that will be installed to the selected device.

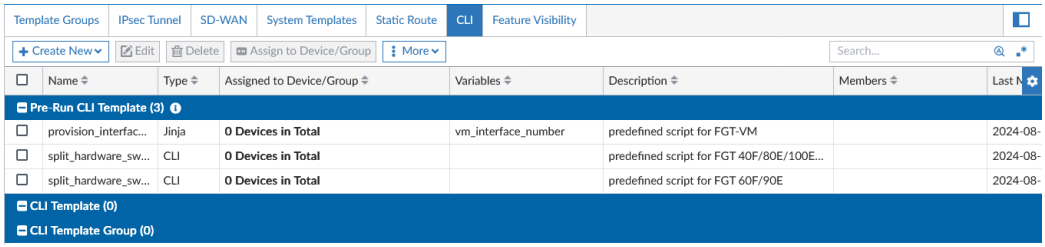
- Click *Re-validate* to run the validation again.



CLI template groups

CLI templates can be put into groups so that multiple templates may be assigned to managed devices at the same time.

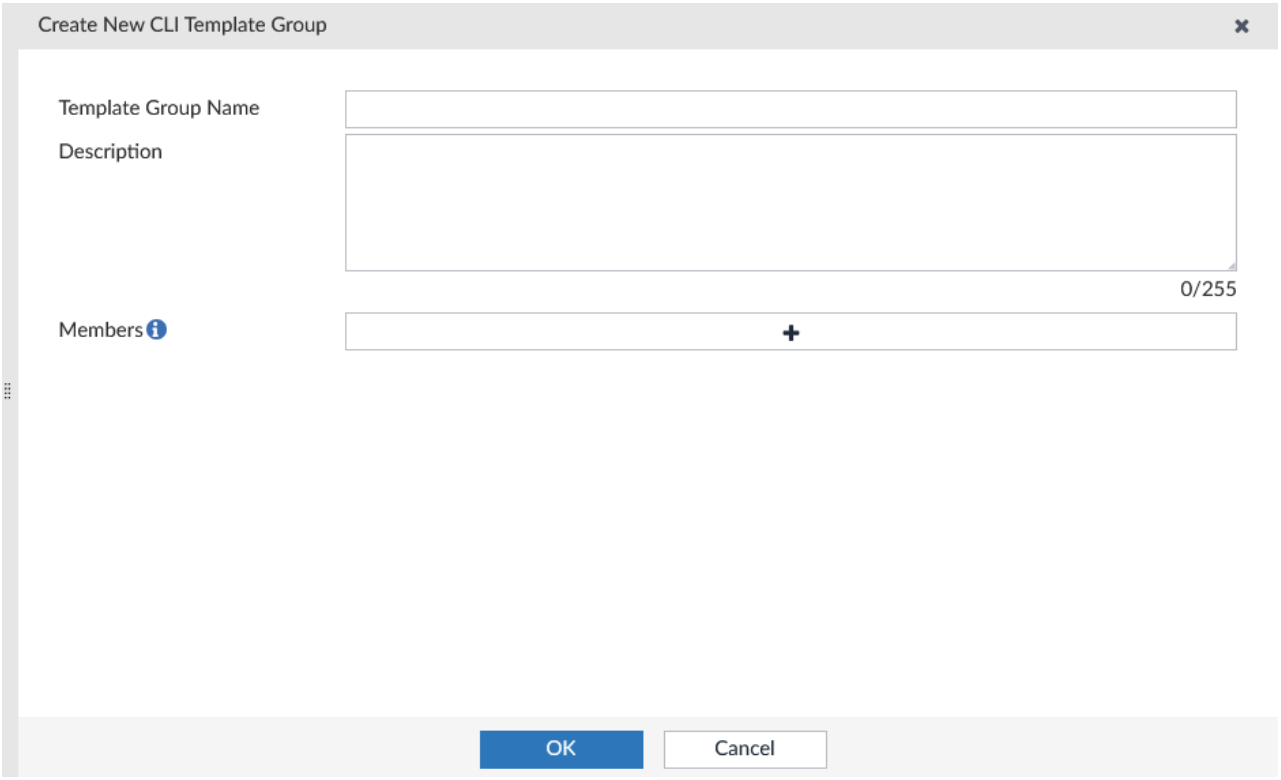
Go to *Device Manager* > *Provisioning Templates* and click on *CLI Templates* from the tree menu to view the *CLI Template* and *CLI Template Group* entries in the content pane.



The information displayed and options available for *CLI Template Group* entries are the same as for *CLI Template* entries.

To add a CLI template group:

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



3. Enter the required information:

Template Group Name	Type a unique name for the template group.
Comments	Optionally, type a comment for the template group.
Members	Click the **+** button to select templates or other template groups from the list, and click *OK* to add the selected entries as members.

4. Click *OK*.

Default CLI templates

FortiManager includes the following default CLI templates:

provision_interfaces_on_vm	This predefined CLI template allows you to configure the number of ports that are created upon initialization of a FortiGate-VM.
split_hardware_switch_ports_40_80_100	This predefined CLI template allows you to configure splitting hardware switch ports for FortiGate 40F, 80E, 100E, and 100F models.
split_hardware_switch_ports_60_90	This predefined CLI template allows you to configure splitting hardware switch ports for FortiGate 60F and 90E models.

These templates can be applied when adding offline model devices in the device manager by configuring *Port Provisioning* for FortiGate-VMs or *Split Switch Ports* for eligible FortiGate hardware devices. See Adding offline model devices on page 104.

Using FortiManager predefined Jinja variables for Device Database

You can use FortiManager variables in Jinja script to retrieve data from the FortiManager Device Database.

The following FortiManager variables are supported:

Supported Device Database Variables	Supported System Interface Variables using the `DEVDB_system_interface` predefined variable
• **Name**: `{{DVMDB.name}}` • **Serial**: `{{DVMDB.serial}}` • **OS TYPE**: `{{DVMDB.os_type}}` • **Platform**: `{{DVMDB.platform}}` • **Version**: `{{DVMDB.version}}` • **Hostname**: `{{DVMDB.hostname}}` • **UUID**: `{{DVMDB.mgmt_uuid}}` • **Mgmt Interface IP** : `{{DVMDB.mgmt_if}}` • **IP**: `{{DVMDB.ip}}` • **Tunnel IP**: `{{DVMDB.tunnel_ip}}` • **Description**: `{{DVMDB.description}}`	• **List of interfaces**: `{{DEVDB_system_interface}}` • **Interface Name**: `{{intf.name}}` • **Interface Alias**: `{{intf.alias}}` • **Interface Allowaccess**: `{{intf.allowaccess}}` • **Interface Type**: `{{intf.type}}` • **Interface IP**: `{{intf.ip}}` • **Interface Mode**: `{{intf.mode}}` • **Interface VDOM**: `{{intf.vdom}}`

This topic includes the following:

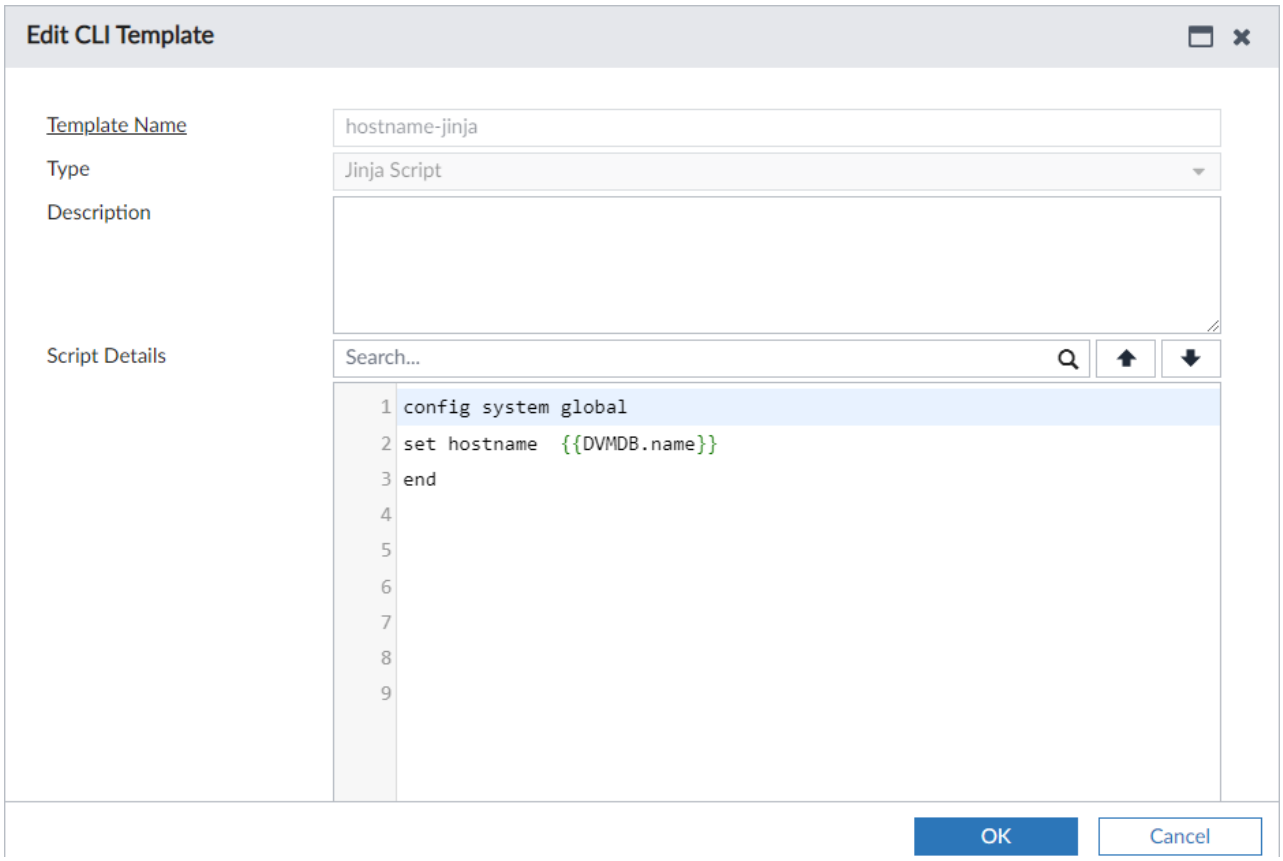
- Using FortiManager variables on page 365
- Example 1: Creating physical interfaces for FortiGate-VMs on page 367
- Example 2: View the device attributes for FortiGate-VMs on page 369
- Example 3: View the interface attributes for each physical interface on a device on page 370

Using FortiManager variables

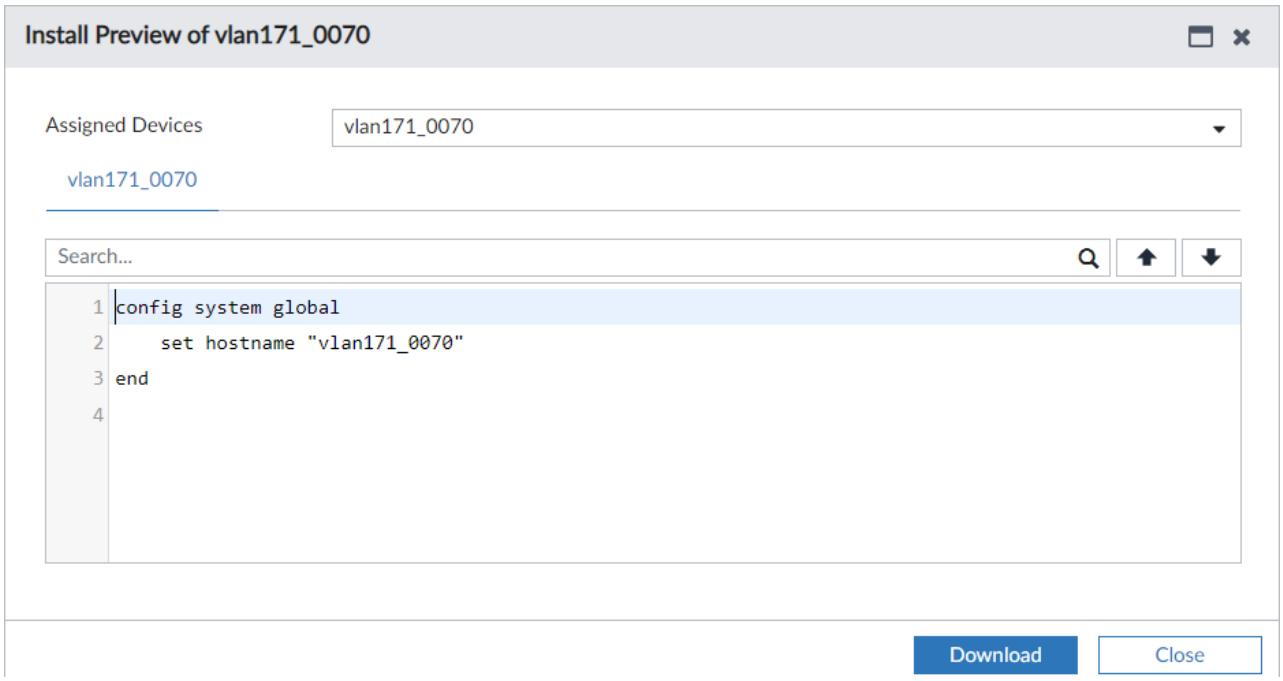
To use variables in a Jinja template:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*.
2. Create a new CLI template.
3. Select the *Type* as *Jinja Script*.
4. Configure the *Script Details* with FortiManager variables. For example, you can use *DVMDB.name* as a variable to get the device name from the Device Database:

```
config system global
set hostname {{DVMDB.name}}
end
```



When viewing the *Install Preview* for the CLI Template, the variable *DVMDB.name* is replaced with the *Name* value for the selected device.



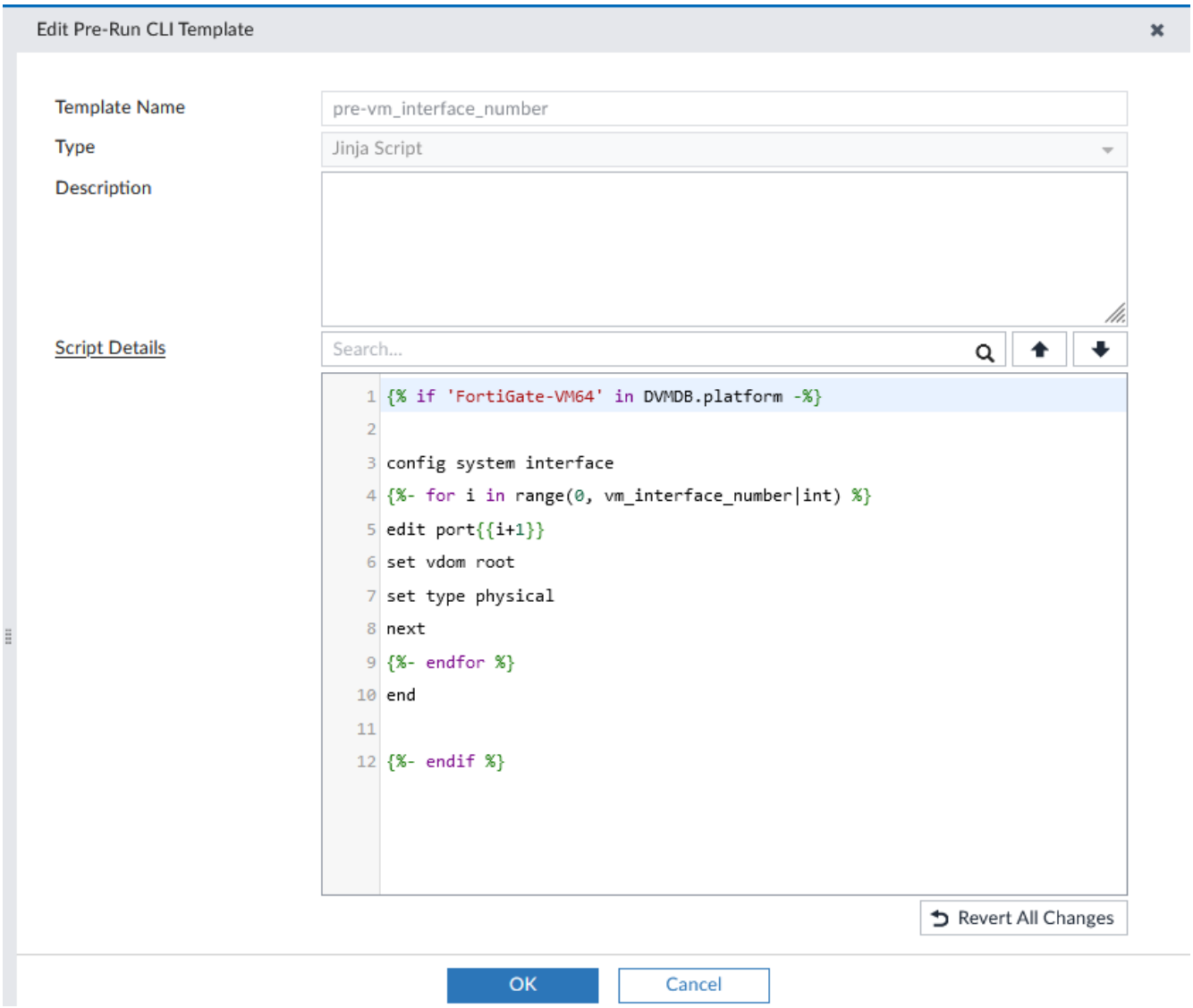
Example 1: Creating physical interfaces for FortiGate-VMs

A user is setting up a FGT-VM64 model device on FortiManager. When setting up a FortiGate-VM, the user needs to execute a script to create the physical interfaces, however, when deploying a FortiGate hardware platform, generating physical interfaces is not necessary. Previously, the user needed to create a separate device group for their FortiGate-VM devices and then runs a script to create the physical interfaces for VM devices inside the device group.

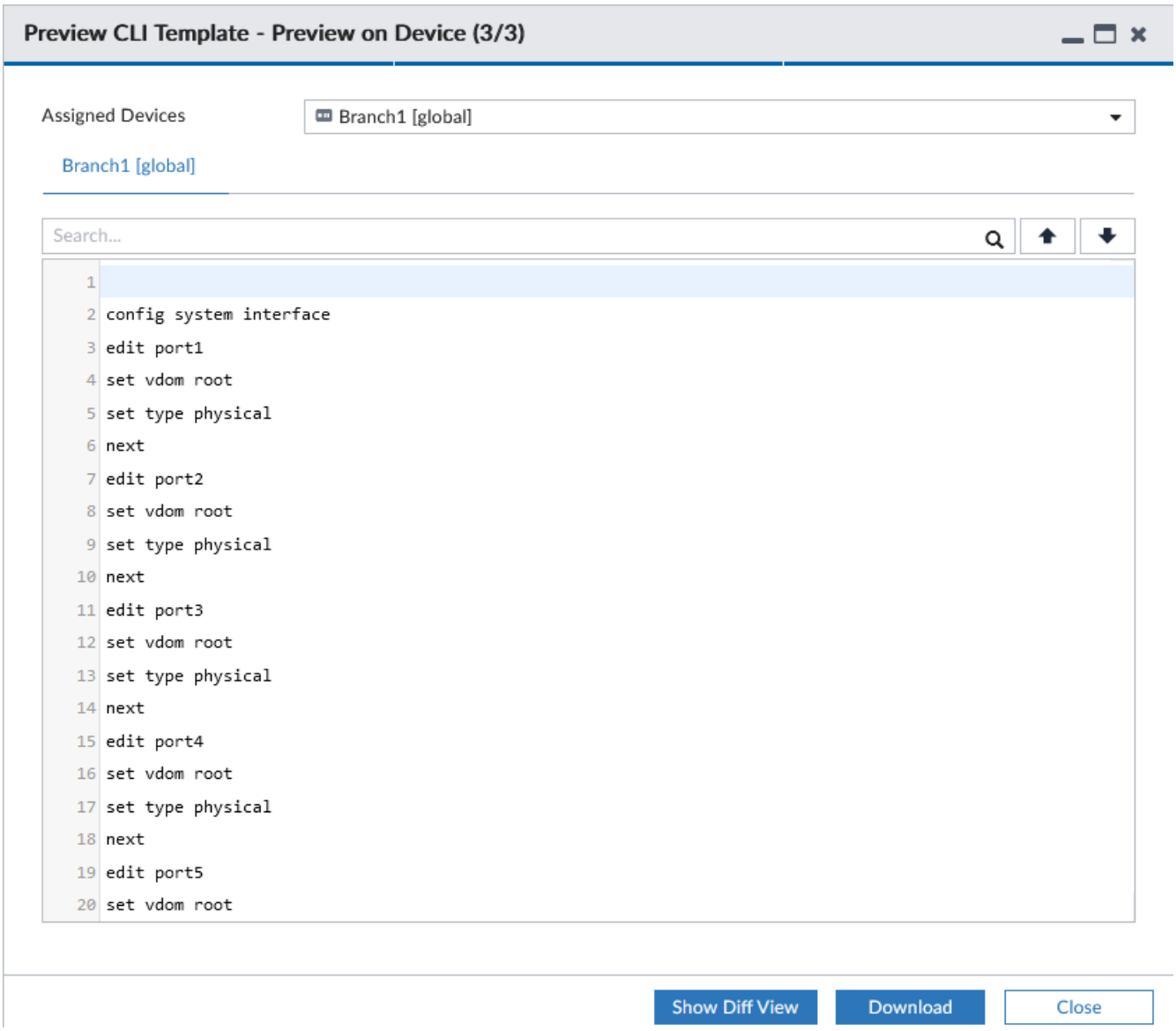
Using Jinja, the same CLI template can be applied to ANY new devices (hardware or VM-based) by using a script with FortiManager variables to determine the platform of the device and using an "if" statement to ensure that the script runs only on FortiGate-VM devices.

Example script:

```
{% if 'FortiGate-VM64' in DVMDB.platform -%}
config system interface
{%- for i in range(0, vm_interface_number|int) %}
edit port{{i+1}}
set vdom root
set type physical
next
{%- endfor %}
end
{%- endif %}
```



Previewing the script on a device shows how the variables are applied.



Example 2: View the device attributes for FortiGate-VMs

Example script:

```
{%- if DVMDB.platform == 'FortiGate-VM64' %}
Name: {{DVMDB.name}}
Serial: {{DVMDB.serial}}
OS TYPE: {{DVMDB.os_type}}
Platform: {{DVMDB.platform}}
Version: {{DVMDB.version}}
hostname: {{DVMDB.hostname}}
UUID: {{DVMDB.mgmt_uuid}}
Mgmt Interface IP : {{DVMDB.mgmt_if}}
IP: {{DVMDB.ip}}
Tunnel IP : {{DVMDB.tunnel_ip}}
Description: {{DVMDB.description}}
```

```
os_type: {{DVMDB.os_type}}
{%- endif %}
```

The rendered result for the script:

```
=======================
Name: vlan171_0040
Serial: FGVM08HZ20311040
OS TYPE: FortiGate
Platform: FortiGate-VM64
Version: 7.4.0
hostname: 3456-abc
UUID: 9c50812a-caa8-51ed-958a-4e7800e5139a
Mgmt Interface IP : port1
IP: 10.8.71.40
Tunnel IP : 169.254.0.12
Description:
os_type: FortiGate
```

Example 3: View the interface attributes for each physical interface on a device

Example script:

```
{%- for intf in DEVDB_system_interface %}
{%- if intf.type == 'physical' %}
Interface Name: {{intf.name}}
-- Interface Allowaccess: {{intf.allowaccess}}
-- Interface Type: {{intf.type}}
-- Interface IP: {{intf.ip}}
-- Interface Mode: {{intf.mode}}
-- Interface VDOM: {{intf.vdom}}
{%- endif %}
{%- endfor %}
```

The rendered result for the script:

```
==============================
Interface Name: port1
-- Interface Allowaccess: ping
-- Interface Type: physical
-- Interface IP: 10.8.71.40
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port2
-- Interface Allowaccess: https
-- Interface Type: physical
-- Interface IP: 101.71.40.1
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port3
-- Interface Allowaccess: ping
-- Interface Type: physical
-- Interface IP: 200.71.40.1
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port4
-- Interface Allowaccess:
-- Interface Type: physical
```

```
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port5
-- Interface Allowaccess: ping
-- Interface Type: physical
-- Interface IP: 172.71.40.1
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port6
-- Interface Allowaccess:
-- Interface Type: physical
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port7
-- Interface Allowaccess:
-- Interface Type: physical
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port8
-- Interface Allowaccess:
-- Interface Type: physical
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port9
-- Interface Allowaccess:
-- Interface Type: physical
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port10
-- Interface Allowaccess:
-- Interface Type: physical
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
```

NSX-T service templates

NSX-T Service templates allow you to manage multiple FortiGate VMs running on NSX-T by automatically applying VDOM, policy, and configuration settings to each VM that belongs on the same registered service.

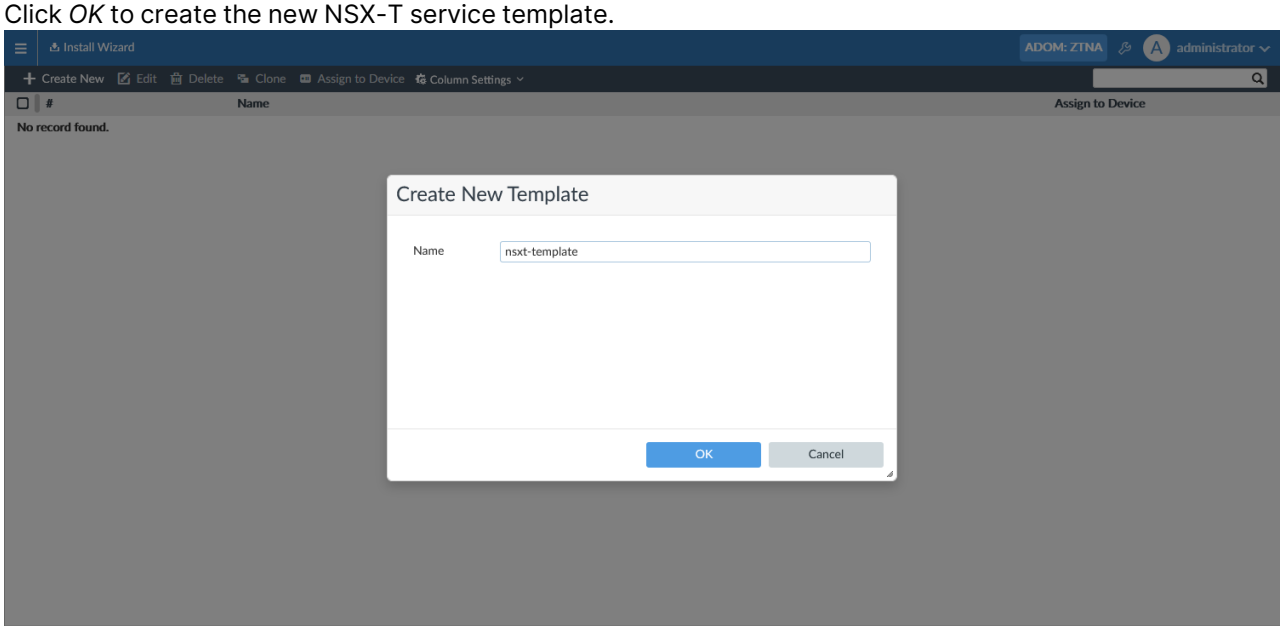
There are two main use cases for this feature:

1. You need to deploy an additional VM in NSX-T.
   When a new VM is authorized in FortiManager, it has no configuration or policy. Using the NSX-T template, FortiManager automatically creates the VDOMs, links them to a policy package, and configures the service profile/VDOM association, log settings, etc.
2. You need to change the existing configuration, for example adding a VDOM.
   FortiManager applies the same change to all VMs from the same service where the template is applied.

NSX-T templates can be created, cloned, deleted, and assigned in *Device Manager > Provisioning Templates > NSX-T Service Template*.

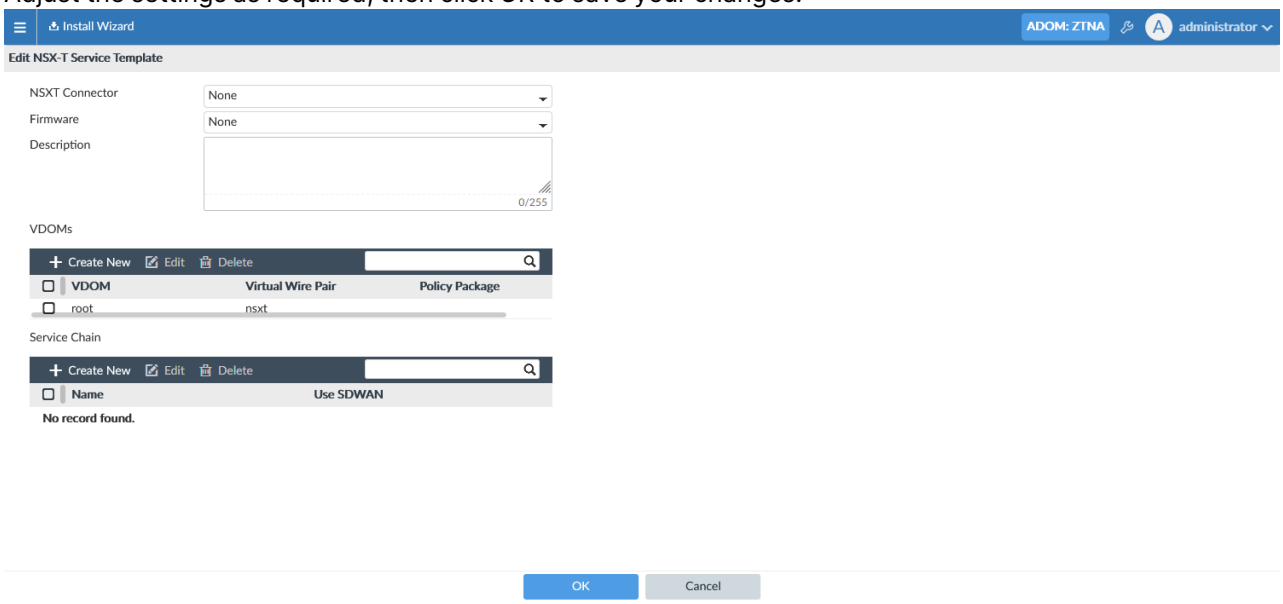
To create a new NSX-T service template:

1. Go to *Device Manager > Provisioning Templates > NSX-T Service Template*.
2. Click *Create New* in the toolbar.
3. In the *Create New Template* pane, type a name for the template.
4. Click *OK* to create the new NSX-T service template.



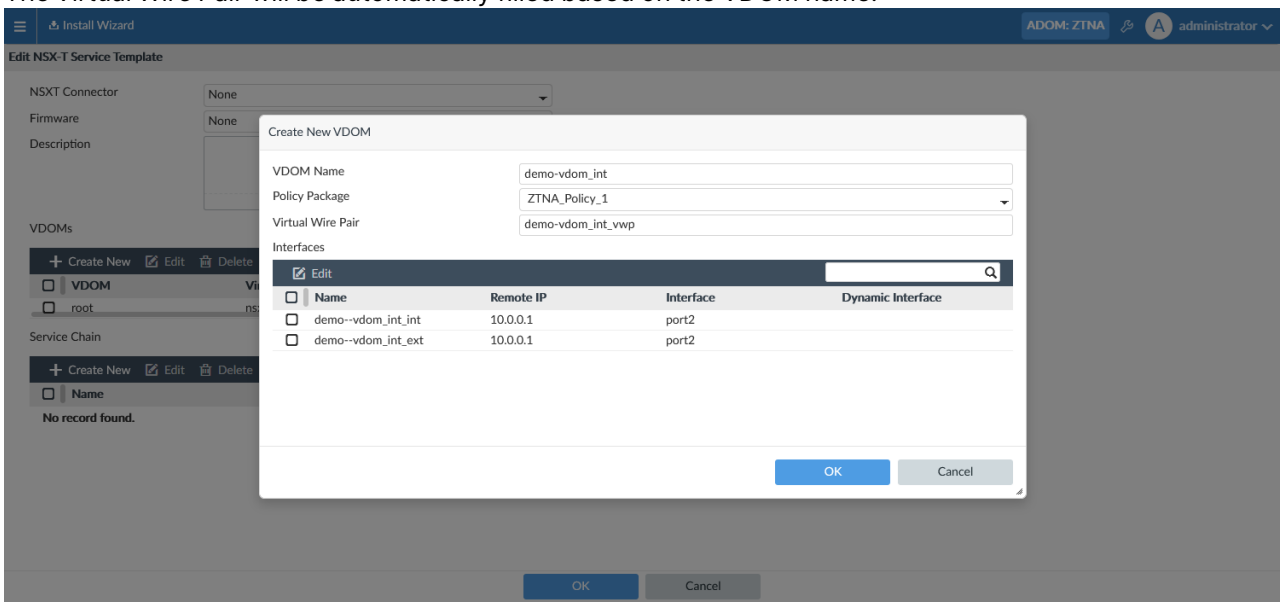
To edit a NSX-T service template:

1. Go to *Device Manager* > *Provisioning Templates* > *NSX-T Service Template*.
2. Select an NSX-T service template and click *Edit*. The *Edit NSX-T Service Template* pane opens.
3. Adjust the settings as required, then click *OK* to save your changes:

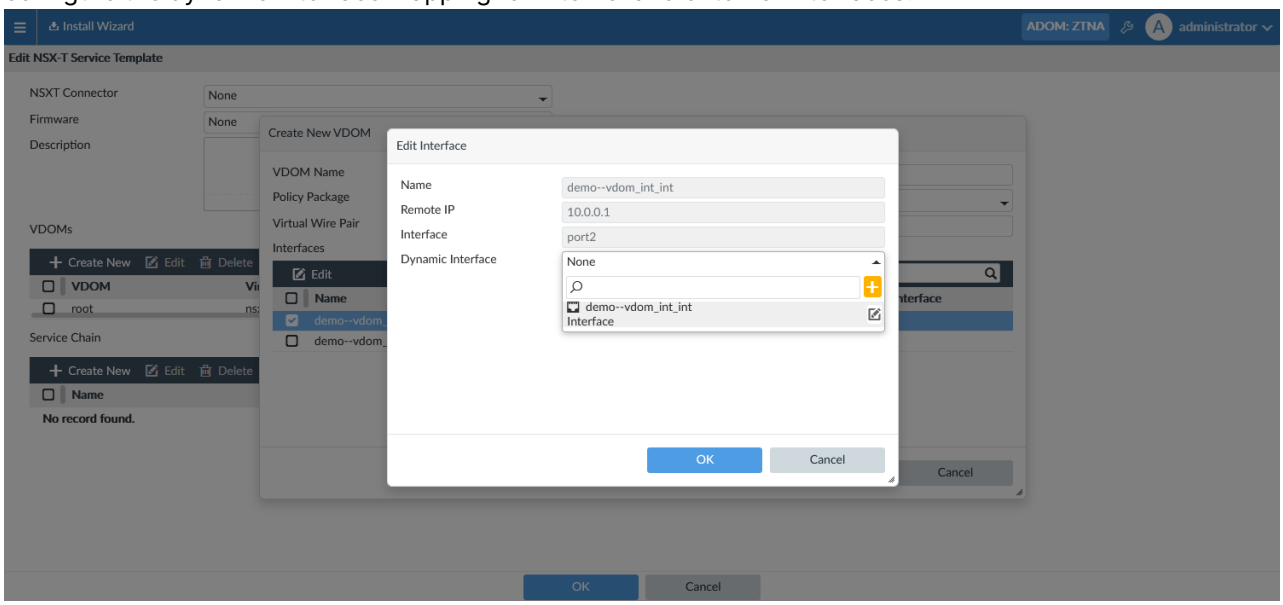


To create a new VDOM:

1. When editing an NSX-T service template, click *Create New* under the VDOMs section.
   The *Create New VDOM* pane opens.
2. Enter a name for the VDOM, and select a *Policy Package* from the dropdown which will be applied to the template.
3. The *Virtual Wire Pair* will be automatically filled based on the VDOM name.



4. Dynamic interface mapping is mandatory to create a VDOM. Select the interface name and click *Edit* to configure the dynamic interface mapping for internal and external interfaces.



The dynamic interface dropdown will only show normalized interfaces that have a default mapping. The default mapping name must be the same as the name of the interface on the *Edit Interface* page.

You can create new interfaces using the + icon in the dropdown.

To assign an NSX-T service template to a device:

1. Go to *Device Manager* > *Provisioning Templates* > *NSX-T Service Template*.
2. Select a template to assign to managed devices.
3. Right-click anywhere in the template list window, and select *Assign to Device* from the menu, or click *Assign to Device* from the toolbar above.
4. Select the managed devices to which you want to assign the selected template from the *Available Entries* field, and move those entries to the *Selected Entries* field.

In order for a device to show up in the list it must meet the following conditions.

1. The VDOM feature must be enabled on the FortiGate.
2. The FortiGate platform type must match the one selected in the template.
3. The NSX-T Service name should match with devices.

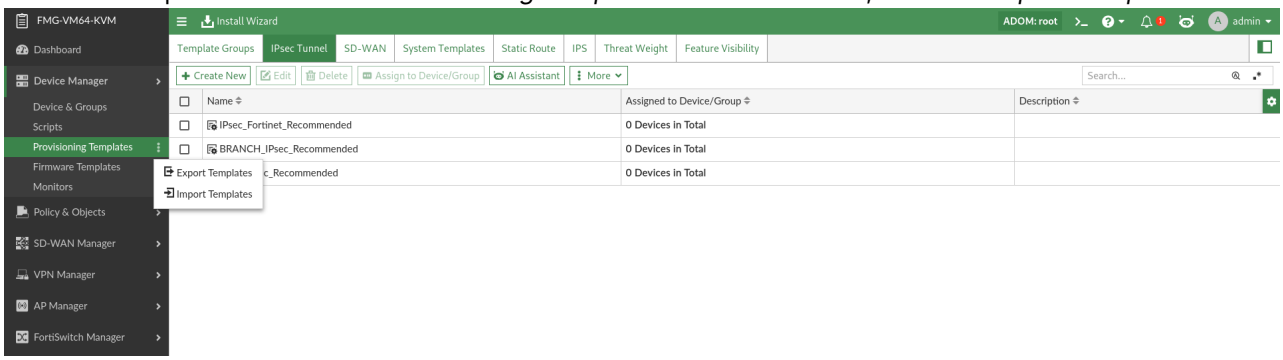
5. Once the template has been assigned to the device, you can install the changes using the *Install Wizard* at the top of the page.

Export and import provisioning template configurations

Provisioning templates are available per-ADOM. Administrators can export templates and profiles as an unencrypted JSON file. The exported file can be edited offline, if needed, and imported to another FortiManager or ADOM.

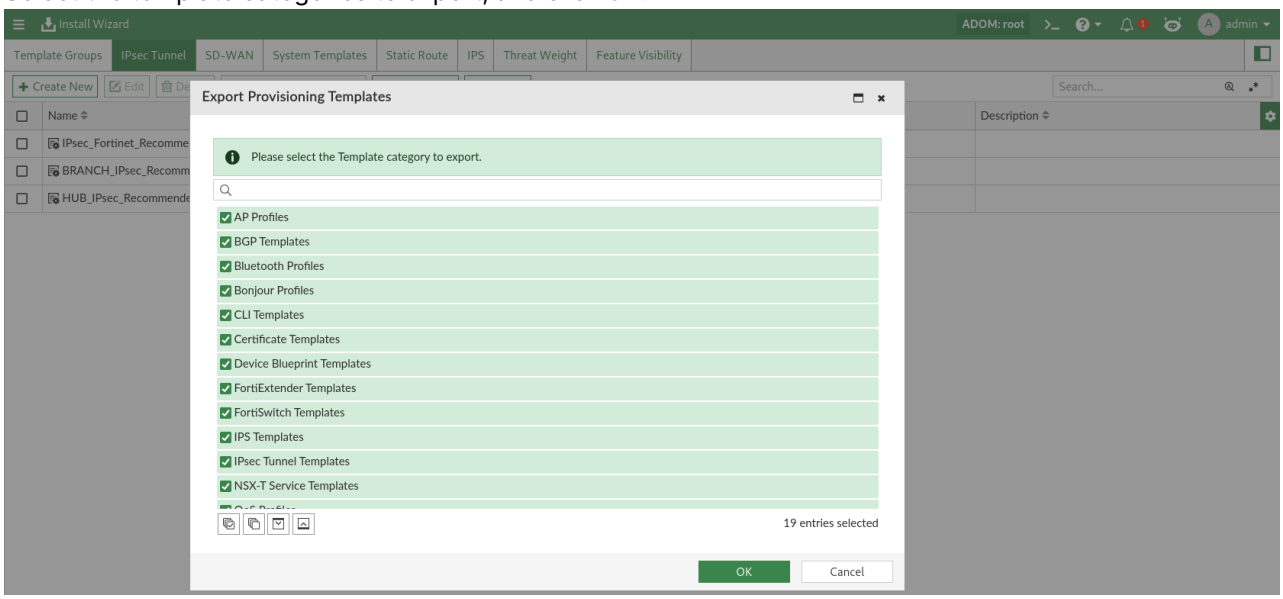
To export templates and import them to another FortiManager or ADOM:

1. In the ADOM that contains the templates to export, go to *Device Manager > Provisioning Templates*.
2. Click on the options icon next to *Provisioning Templates* in the tree menu, and click *Export Templates*.



The *Export Provisioning Templates* dialog displays.

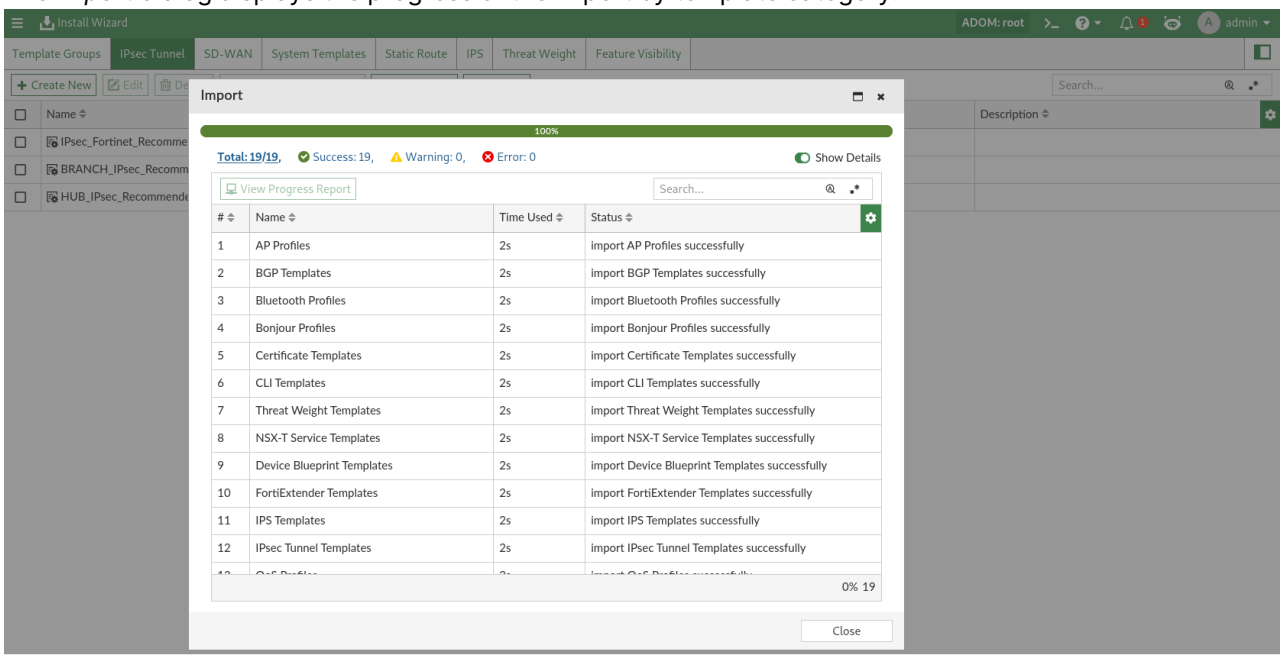
3. Select the template categories to export, and click *OK*.



The *Export Provisioning Templates* dialog displays the progress of the export by template category.

4. When the export is complete, click *Finish*.
   The exported JSON file can be edited offline, if needed, before it is imported to another ADOM.
5. Go to the second FortiManager and/or ADOM to import the template(s).
6. In the ADOM, go to *Device Manager > Provisioning Templates*.
7. Click on the options icon next to *Provisioning Templates* in the tree menu, and click *Import Templates*.
   The *Import Template* dialog displays.
8. Drag and drop the exported JSON file in the *Upload Package* field, and click *OK*.

The *Import* dialog displays the progress of the import by template category.



9. When the import is complete, click *Close*.
   The provisioning templates are now available to edit and assign in the ADOM.

Viewing the CLI preview for provisioning templates

FortiManager includes the ability to preview CLI configuration changes for provisioning templates.

You can view the CLI preview for all provisioning template types, including: *Template Groups*, *IPsec Tunnel Templates*, *SD-WAN Templates*, *BGP Templates*, *SD-WAN Overlay Templates*, *System Templates*, *Static Route Templates*, *CLI Templates*, and *Threat Weight Templates*.

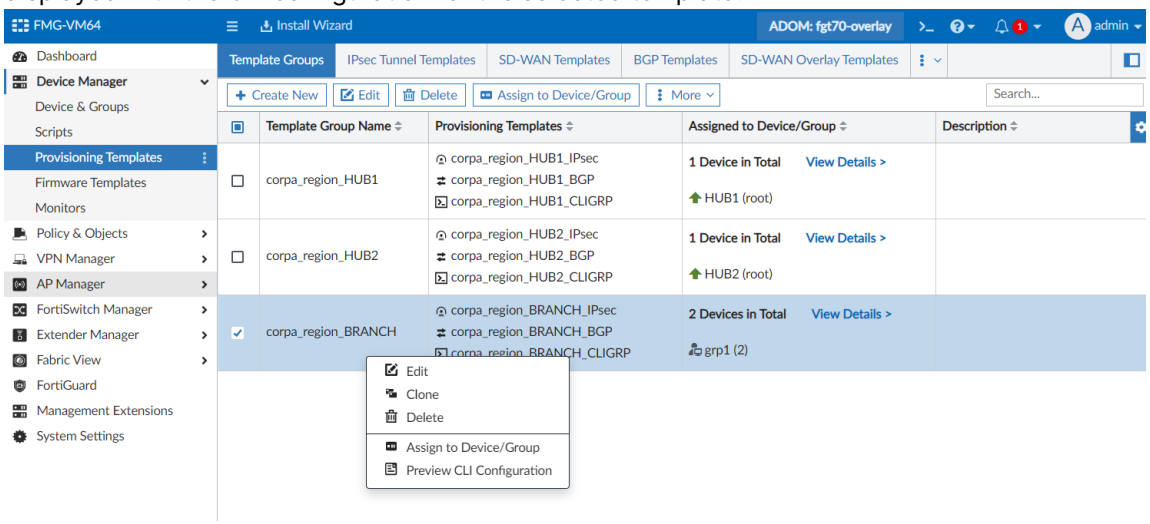
When a provisioning template includes CLI changes for multiple devices, you can select the device in the *Device* dropdown when previewing the CLI configuration. You can view the preview for both real and model devices.

If metadata variables are included in the template, the metadata variable names and not their resolved values are displayed in the preview.

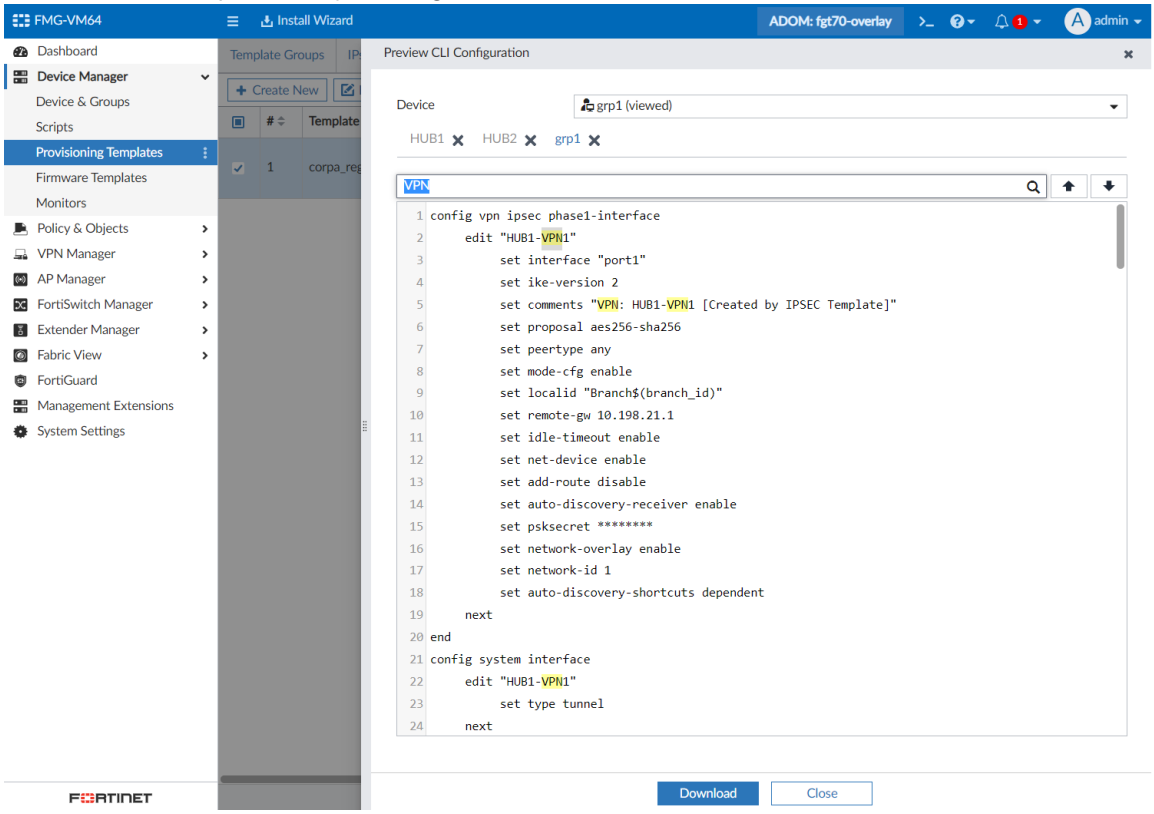
To view the CLI configuration preview for provisioning templates:

1. Go to *Device Manager* > *Provisioning Templates*.
   Select a template type by choosing the corresponding tab.

2. Right-click on a template, and choose *Preview CLI Configuration*. The *Preview CLI Configuration* window is displayed with the CLI configuration for the selected template.



3. When the provisioning template includes multiple devices, you can select a device from the *Device* dropdown. The CLI preview for the selected device is displayed in the content pane.
4. In the *Preview CLI Configuration* window, you can search in the CLI using the search bar, and you can download the CLI preview by clicking the *Download* button.



Firmware templates

Firmware templates define what firmware version should be installed on FortiGates and all access devices, such as FortiAP, FortiSwitch, and FortiExtender. You can assign the templates to one or more devices.

After the template is assigned to a device, the device is required to have the specified version installed. You can use the *Firmware Template* column on the *Device Manager > Device & Groups* pane to view the status of the device with the firmware version specified in the assigned template.

The template can include a schedule to automatically start the firmware upgrades, or you can manually initiate firmware upgrades.

Following is an overview of how to use firmware templates:

1. Create a firmware template for one or more products. See Creating firmware templates on page 379.
2. Assign the firmware template to one or more devices. See Assigning firmware templates to devices on page 382.

   Firmware templates with a schedule will automatically start the firmware upgrades on assigned devices at the scheduled day and time.

   For firmware templates without a schedule, you can manually initiate the firmware upgrades on assigned devices when you are ready. See Upgrading devices now on page 384.
3. Preview the upgrade. See Previewing upgrades on page 383.
4. View upgrade history. See Reviewing upgrade history on page 383.
5. View the firmware upgrade report. See Viewing the firmware upgrade report on page 384.
6. Monitor device adherence to the firmware template by using the *Firmware Template* column on the *Device Manager > Device & Groups* pane in *Table View*.

You can also edit and delete firmware templates. See Editing firmware templates on page 382 and Deleting firmware templates on page 382.



FortiGate devices must have a valid Firmware & General Updates (FMWR) contract in order for firmware updates to be performed through FortiManager. This applies to firmware images from FortiGuard and images that are manually uploaded to FortiManager.

When a FortiGate device is added to the FortiManager, a 24 hour grace period is provided in which firmware updates can be applied without a license to allow time for the FMWR contract information to synchronize from FortiCare. FortiManager expects the managed device to be on the same FortiCloud account, or have the device serial number added in FortiGuard's auth list.

Firmware template upgrade sequence

When a firmware template's upgrade process is triggered, assigned FortiGate devices and their fabric devices will be upgraded in the following order:

1. FortiGate
2. FortiSwitch (when a FortiGate manages multiple FortiSwitch devices, the upgrade process occurs sequentially, with each FortiSwitch being updated one at a time)
3. FortiAP
4. FortiExtender

When a device in the sequence is offline, the upgrade process and all subsequent tasks will be forced to stop (for example, if a FortiSwitch upgrade fails because a device is offline, the firmware template will not proceed to upgrade the FortiAP devices). However, this does not affect other assigned FortiGate devices being upgraded concurrently under the same template.

Creating firmware templates

With firmware templates, you can specify what firmware to install on FortiGate and the following associated access device: FortiAP, FortiSwitch, and FortiExtender.



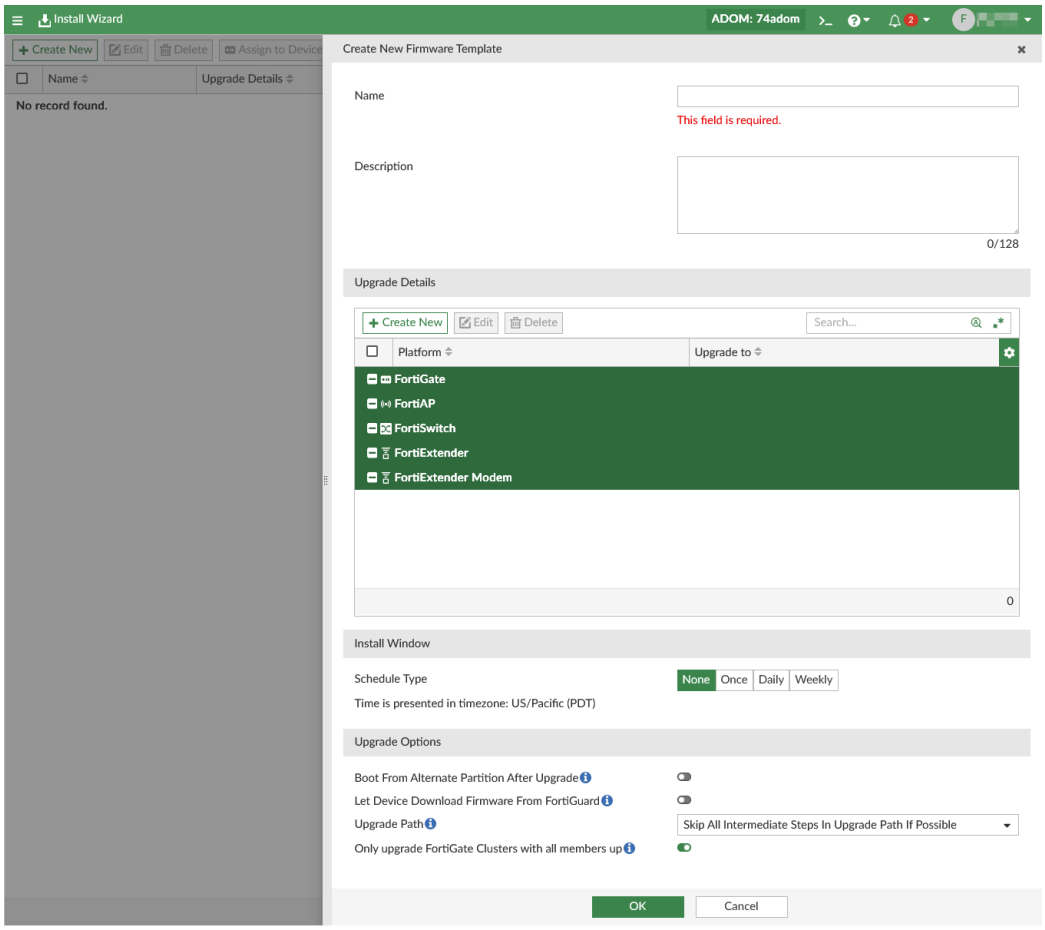
Firmware images for FortiExtender are not available on FortiGuard. Before you can select a firmware image for FortiExtender in a firmware template, you must download the firmware image from the Customer Service & Support site, and import the image to FortiManager by using the FortiGuard module. See Firmware images on page 806.

You can schedule when to automatically start the firmware upgrades. Alternately, you can create a firmware template without a schedule, and manually initiate the firmware upgrade when you are ready.

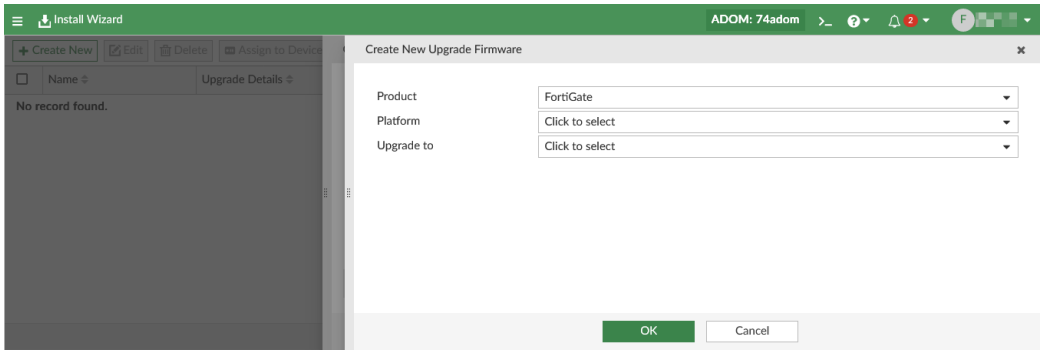
You can also specify what type of upgrade path to use.

To create firmware templates:

1. Go to *Device Manager* > *Firmware Templates*.
2. In the toolbar, click *Create New*.
   The *Create New Firmware Template* pane is displayed.



3. In the *Name* box, type a name.
4. Create upgrade details:
   a. In the *Upgrade Details* area, click *Create New*.
      The *Create New Upgrade Firmware* dialog box is displayed.



   b. In the *Product* dropdown, select a product to upgrade.
   c. In the *Platform* dropdown, select the platform for the product.
   d. In the *Upgrade to* dropdown, select the target firmware version for the upgrade.
   e. Click *OK*. The upgrade details are saved.
5. In the *Install Window* area, you can schedule the upgrade:

Schedule Type	Specify whether to schedule the upgrade by selecting one of the following options: • *None*: Select to have no schedule. • *Once*: Select to schedule the upgrade to occur once. • *Daily*: Select to schedule the upgrade to occur daily. • *Weekly*: Select to schedule the upgrade to occur weekly.
Day	Available when you select *Weekly*. Select what day of the week to run the upgrade.
Start Time	Available when you select *Once*, *Daily*, or *Weekly*. Specify what time to start the upgrade.
End Time	Available when you select *Once*, *Daily*, or *Weekly*. Specify what time to end the upgrade. If the upgrade is not completed by the end time, the upgrade stops.

6. In the *Upgrade Options* area, set the following options:

Boot from Alternate Partition After Upgrade	Applies only to FortiGates. Select to upgrade the inactive partition. Clear to skip the inactive partition during upgrade. Selecting this option causes the device to reboot twice during the upgrade process: first to upgrade the inactive partition, and second to boot back into the active partition.
Let Device Download Firmware from FortiGuard	Select to have the device download the firmware from FortiGuard for the upgrade. Clear to have the device download the firmware from FortiManager.
Upgrade Path	Select one of the following options: • *Skip All Intermediate Steps in Upgrade Path If Possible*: Select to skip some builds in an upgrade path. • *Follow The Recommended Upgrade Path*: Select to install all builds in an upgrade path.  The *Follow The Recommended Upgrade Path* feature is not supported when FortiManager is operating in a closed network. Each image in the path must instead be imported to FortiManager and manually pushed to the managed devices in the correct order. You can view the recommended upgrade path at support.fortinet.com.
Only upgrade FortiGate Clusters with all members up	When enabled, if any HA secondary node is down, the firmware upgrade will be skipped for the HA cluster.

7. Click *OK*. The upgrade template is created.
8. Assign the template to one or more devices. See Assigning firmware templates to devices on page 382.

Editing firmware templates

After creating firmware templates, you can edit them as needed.

To upgrade devices now:

1. Go to *Device Manager* > *Firmware Templates*.
   The firmware templates are displayed in the content pane.
2. Select a template, and click *Edit*.
   Alternately you can double-click a template, or right-click the template, and select *Edit*.
   The template opens for editing.
3. Make changes, and click *OK* to save the changes.

Deleting firmware templates

After creating firmware templates, you can delete them.

To delete firmware templates:

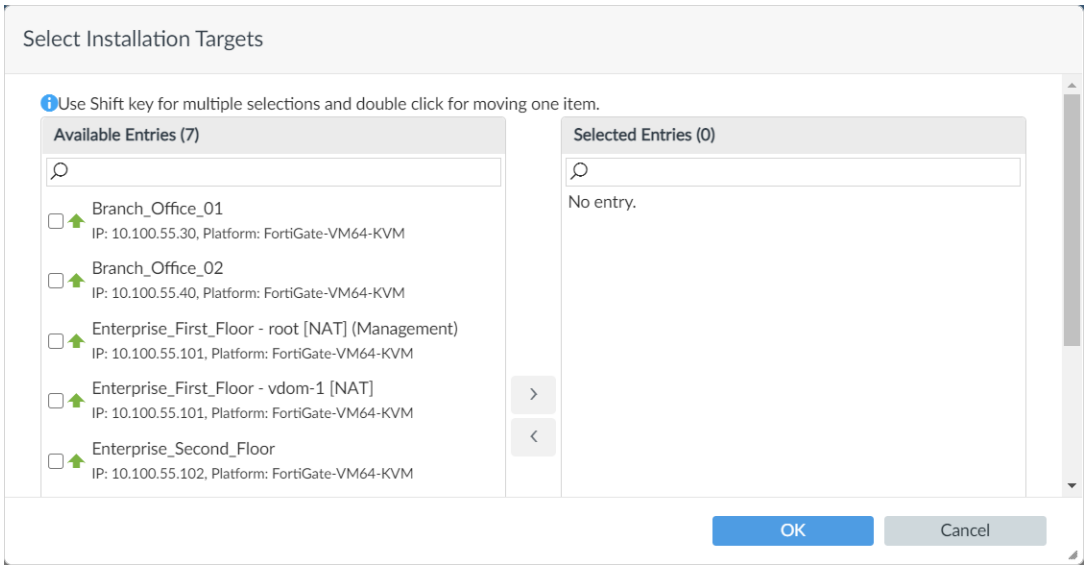
1. Go to *Device Manager* > *Firmware Templates*.
   The firmware templates are displayed in the content pane.
2. Select a template, and click *Delete*.
   Alternately you can right-click the template, and select *Delete*.
   The template is deleted.

Assigning firmware templates to devices

You must assign firmware templates to one or more devices to use the templates.

To assign firmware templates to devices:

1. Go to *Device Manager* > *Firmware Templates*.
   The firmware templates are displayed in the content pane.
2. Select a template, and click *Assign to Device*.
   Alternately you can right-click the template, and select *Assign to Device*.
   The *Select Installation Targets* dialog box is displayed.



3. In the *Available Entries* list, select one or more devices, and click > to move the devices to the *Selected Entries List*.
   The firmware template will be applied to devices in the *Selected Entries List*.
4. Click *OK*.
   The firmware template is assigned to the devices in the *Selected Entries List*.

Previewing upgrades

After assigning templates to one or more devices, you can preview the upgrade changes.

To preview upgrades:

1. Go to *Device Manager* > *Firmware Templates*.
   The firmware templates are displayed in the content pane.
2. Select a template, and from the *More* menu, select *Upgrade Preview*.
   Alternately you can right-click the template, and select *Upgrade Preview*.
   The *Firmware Upgrade Preview* dialog box is displayed.
3. Review the upgrade details, and click *Close*.

Reviewing upgrade history

After using a firmware template, you can review the upgrade history for the template.

To review upgrade history:

1. Go to *Device Manager* > *Firmware Templates*.
   The firmware templates are displayed in the content pane.

2. Select a template, and from the *More* menu, select *Upgrade History*.
   Alternately you can right-click the template, and select *Upgrade History*.
   The *Upgrade History* dialog box is displayed.
3. Review the history, and click *Close*.

Upgrading devices now

You can manually initiate a firmware template upgrade to upgrade assigned devices right now.

To upgrade devices now:

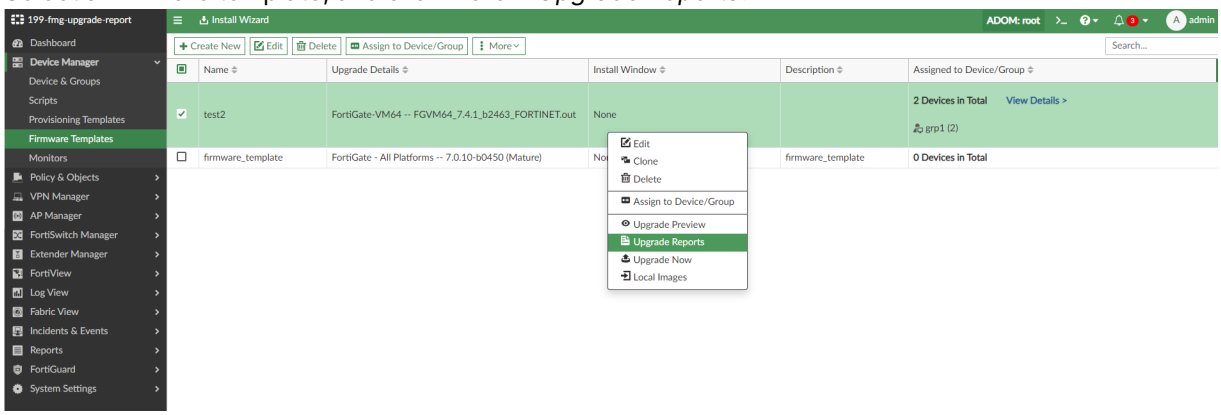
1. Go to *Device Manager* > *Firmware Templates*.
   The firmware templates are displayed in the content pane.
2. Select a template, and from the *More* menu, select *Upgrade Now*.
   Alternately you can right-click the template, and select *Upgrade Now*.
   The *Upgrade Now* dialog box is displayed.
3. Click *OK* to upgrade devices assigned to the template.

Viewing the firmware upgrade report

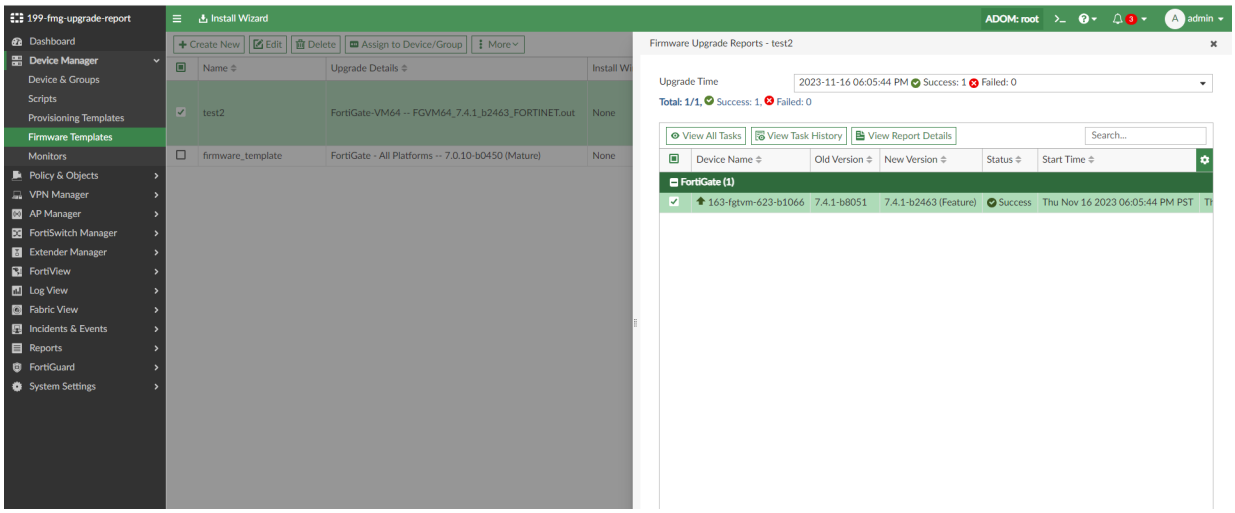
In FortiManager, you can view the firmware upgrade report to see information about the firmware upgrade.

To view the firmware upgrade report:

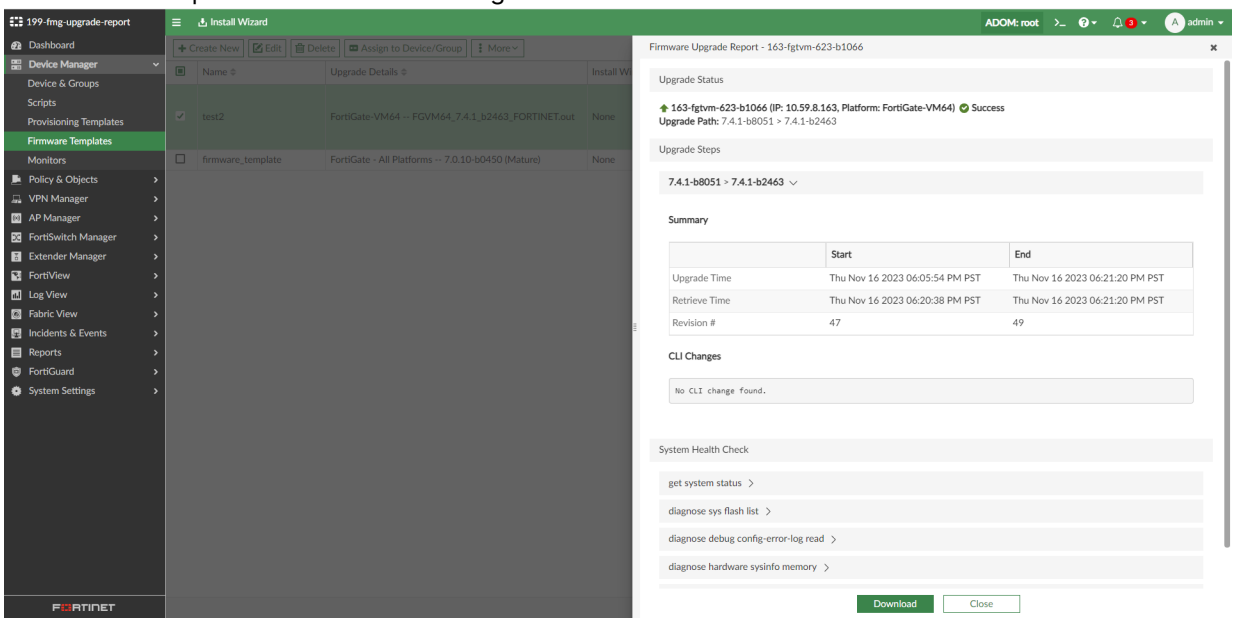
1. After the firmware upgrade template has finished running, go to *Device Manager* > *Firmware Templates*.
2. Open the firmware upgrade report dialog using one of the following methods:
   a. Right-click on a firmware template, and select *Upgrade Reports*.
   b. Select a firmware template, and click *More* > *Upgrade Reports*.



3. Select an entry from the table, and click *View Report Details* to view the report for the selected device.



The firmware report includes the following information:

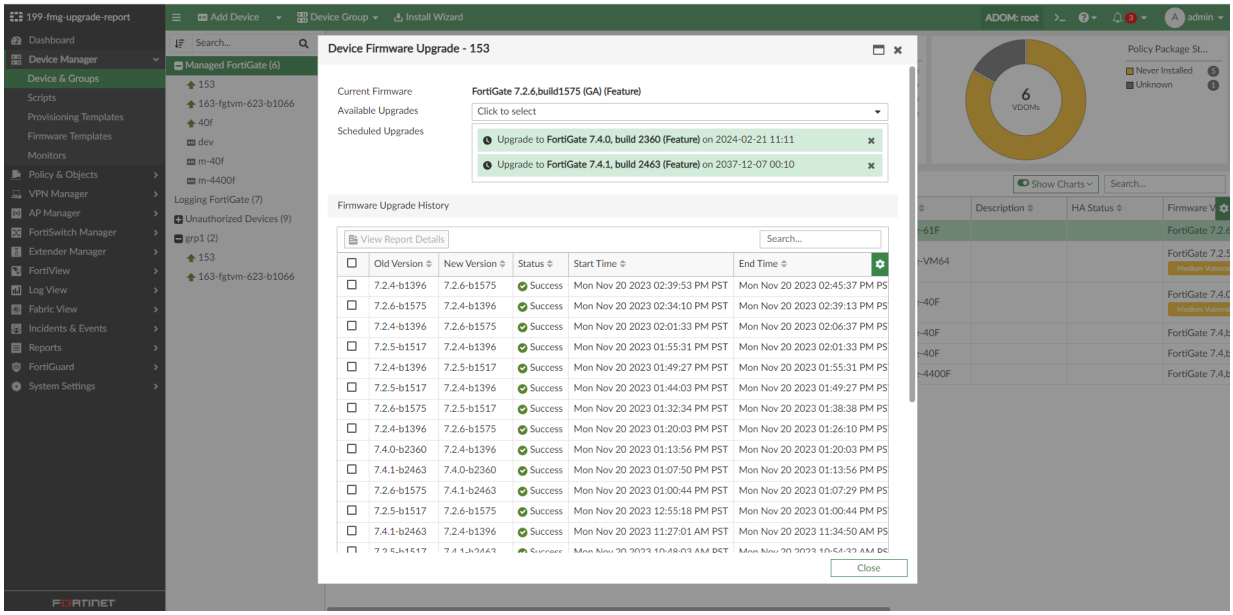


Upgrade Status	Status information about the upgrade.
Upgrade Steps	The upgrade path applied by the firmware upgrade template. Click to expand and view the summary and CLI changes.
Summary	The upgrade time, retrieve time, and revision number.
CLI Changes	The CLI changes implemented with the upgraded version.
System Health Check	Reports the results of the following system health checks from the FortiGate: • `get system status` • `diagnose sys flash list` • `diagnose debug config-error-log read` • `diagnose hardware sysinfo memory`

	• `diagnose debug crashlog read`
Download	Download a PDF copy of the report.

To view the device-level firmware upgrade report:

1. After the device's firmware is updated, go to *Device Manager* and right-click on the upgraded device.
2. Click *Upgrade Firmware*.
3. Under the *Firmware Upgrade History* header, select an entry and click *View Report Details*.



Monitors

Use the monitors tree menu to access the following monitors:

- SD-WAN Monitor on page 386
- VPN Monitor on page 396
- Asset Identity Center on page 398
- AI Analysis on page 400
- LTE modem monitors on page 401

SD-WAN Monitor

You can use the *Device Manager* > *Monitors* > *SD-WAN Monitor* pane to monitor SD-WAN networks on FortiGate devices.

The FortiGate devices can be monitored from the following views:

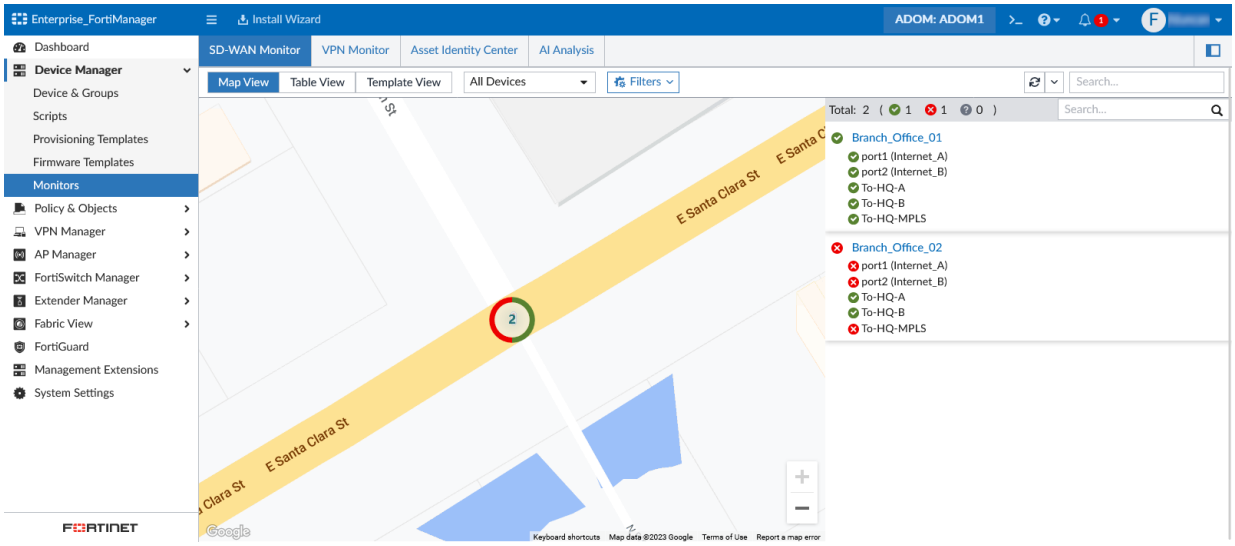
- Map View on page 387
- Table View on page 387
- Template View on page 391
- Enabling SD-WAN monitoring history on page 393
- SD-WAN cloud assisted monitoring speed test on page 395

Map View

In order to see the port bandwidth usage, you must configure the estimated bandwidth on the interface used by SD-WAN.

To monitor SD-WAN with Map View:

1. Go to the *Device Manager* > *Monitors* > *SD-WAN Monitor* pane, and click *Map View*.
   Devices in the SD-WAN network are displayed on Google Maps.



2. (Optional) Click the *Filters* dropdown to view options to *Show Unhealthy Devices Only* and/or *Show Unhealthy Interfaces Only*.
3. Click a device to display its details on the right pane.

Select *Show Unhealthy Devices only* to show only the devices that do not meet the Performance SLA criteria.

Table View

You can monitor SD-WAN networks in *Table View*. You can monitor all devices, or you can drill-down to view details of individual devices.

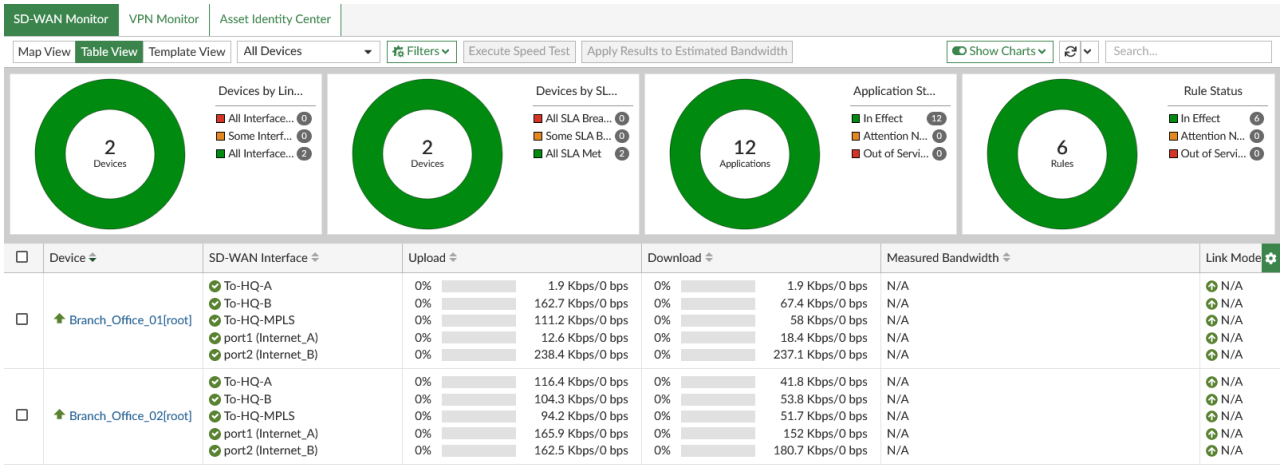
When you view details for individual devices, the graphs reflect both the static underlay and overlay interfaces as well as dynamic interfaces, such as ADVPN or shortcuts when used.

The following charts are included in the SD-WAN Monitor Table View:

Devices by Link Status	Displays devices *by All Interfaces Up*, *Some Interfaces Down*, and *All Interfaces Down*.
Devices by SLA Status	Displays devices by *All SLA Met*, *Some SLA Breached*, *and All SLA Breached*.
Application Status	Displays the application status as *In Effect*, *Attention Needed*, and *Out of Service*.
Rules Status	Displays the rules status as *In Effect*, *Attention Needed*, and *Out of Service*.

To monitor SD-WAN with Table View:

1. Click *Table View* to view the SD-WAN parameters for each device.



The following columns of information are shown for each device:

Device	Name of the device.
SD-WAN Interface	Interface members.
Upload	Volume of data transmitted up stream
Download	Volume of data transmitted down stream.
Link Mode	Displays the link status, speed, and duplex. Speed and duplex information is only available for physical interfaces.
Errors (TX/RX)	Displays the number of errors that have occurred during transmission (TX) and receiving (RX).
Applications	Add or remove the *Applications* from the *Services Settings* dropdown. The data is shown for the selected applications. The applications are specified in *SD-WAN Rules* > *Destination type* > *Internet Service* in FortiGate.
Automatic Refresh	FortiManager extracts the data from FortiGate devices based on the refresh settings. Select the automatic refresh interval from *Every 5 Minutes* to *Every 30 Minutes*.

When a single device is specified, additional realtime refresh options from *Every 30 Seconds* to *Every 3 Minutes* are available.

You can select *Manual Refresh* to refresh the data manually.

Hover over a service for a device that is shown in red. A pop-up shows the parameters that have failed the SLA criteria.

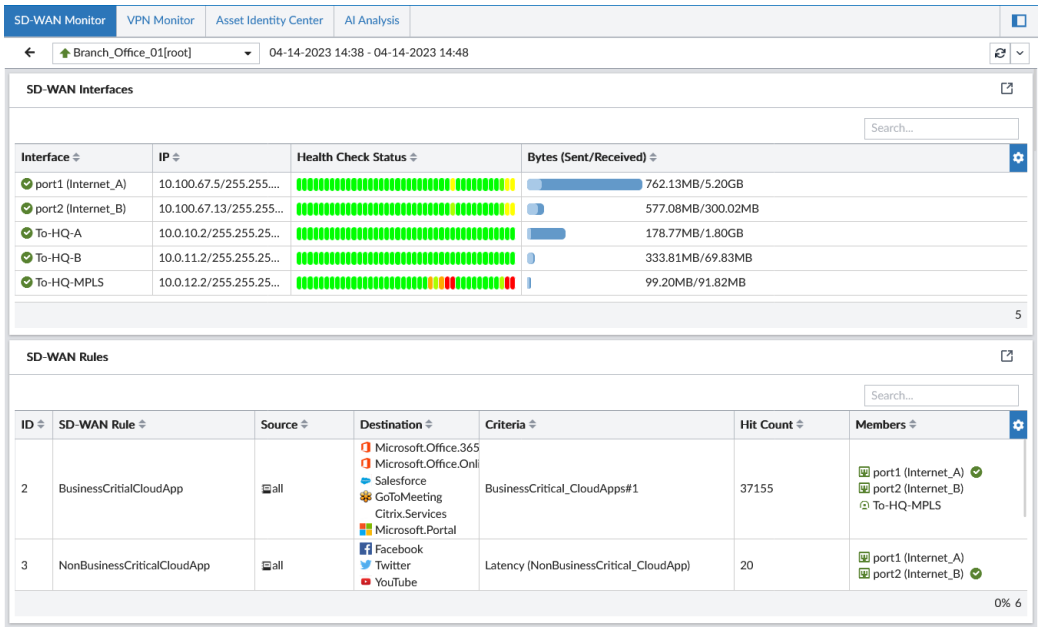
2. (Optional) Click the *Filters* dropdown to view options to *Show Unhealthy Devices Only* and/or *Show Unhealthy Interfaces Only*.

To view device details:

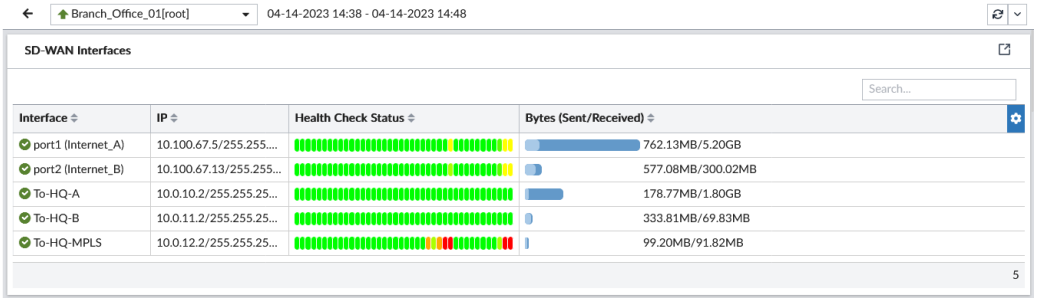
1. Select a device in the list to display graphs of its details.

   By default, SD-WAN Monitoring History is disabled. When this feature is disabled, data for only the last 10 minutes is displayed. You can refresh to view the data directly from FortiGate devices. No historical data is stored in FortiManager when this feature is disabled.

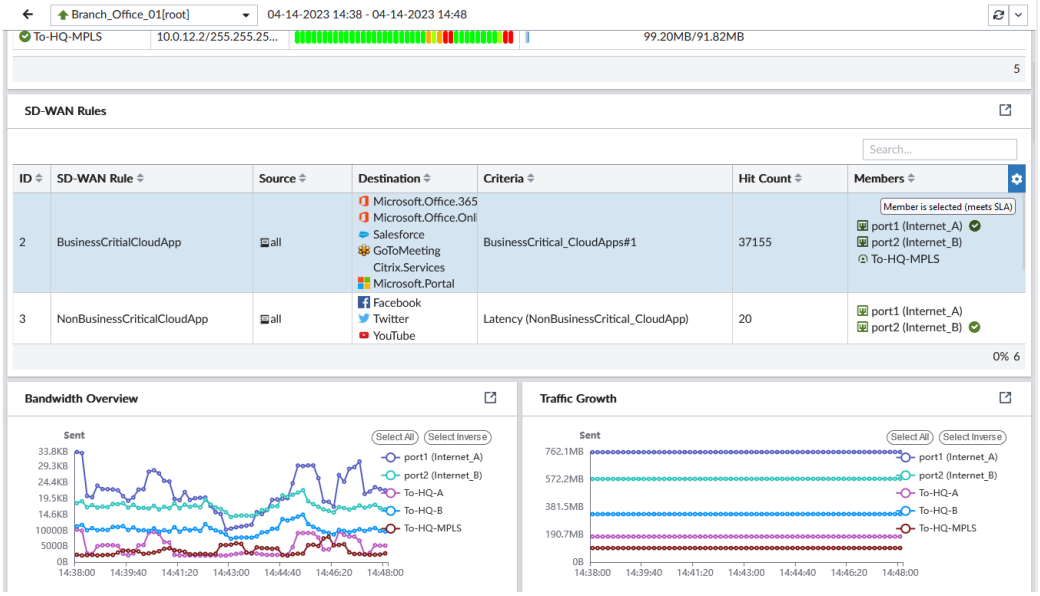
   See also Enabling SD-WAN monitoring history on page 393.



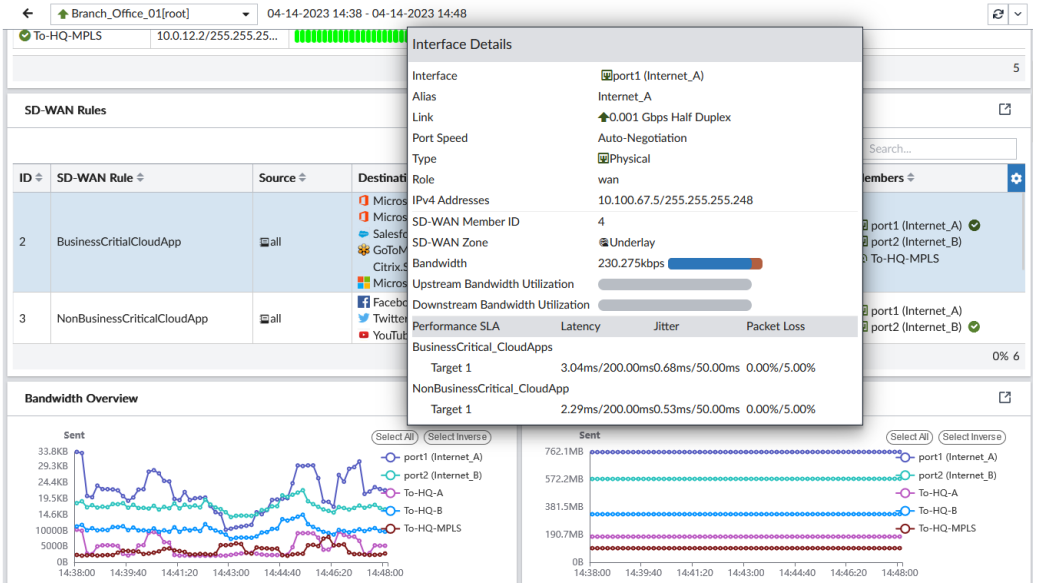
2. In 7.0 ADOMs and later, you can view realtime information for a specific device by selecting *Every 30 Seconds*, *Every 1 Minute*, or *Every 3 Minutes* from the *Automatic Refresh* dropdown menu. Only data from the past ten minutes is displayed when realtime refresh options are selected.
3. Hover over the charts to view additional details.
4. The *SD-WAN Rules* widget includes the following features:
   - Rule statuses are indicated by color. Red interfaces indicate that the interface is down and the rule is inactive.



- Active (referred to as *selected*) interfaces are identified with check mark icon in the SD-WAN Rules table. You can see why an interface is selected by hovering your mouse over the interface.



- View interface statistics, including SLAs tied to that interface, upstream and downstream bandwidth, IP addresses, link speed, and more.



5. In the toolbar, click the *Go Back* arrow to exit the pane.

Widget layout configuration

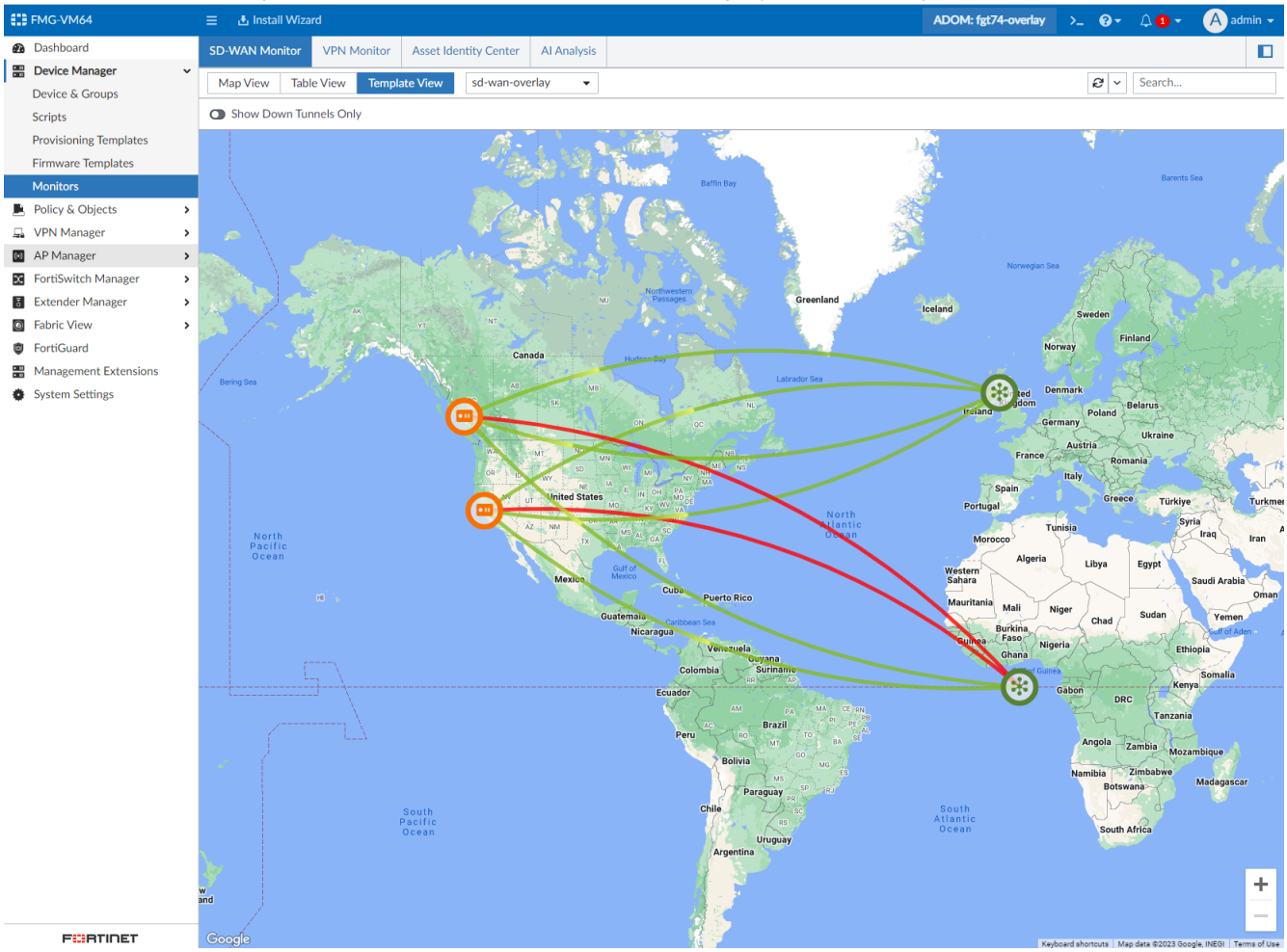
When viewing the detailed view, you can configure the dashboard by dragging and resizing widgets. Widget layout persists between devices based on the following:

- All SD-WAN devices assigned to the same template use the same layout. Only devices assigned to the template directly are supported, not devices assigned through Template Group or SD-WAN Overlay Template.
- If an SD-WAN device is not part of the SD-WAN template, it will use its own layout.

Template View

The Template View monitor grants visibility for devices that have been provisioned using the selected SD-WAN template.

The SD-WAN Overlay Template is the default map view. You can use the dropdown in the toolbar to select different SD-WAN templates so that the related devices are displayed on the map.



To monitor SD-WAN with the Template View:

1. Go to the *Device Manager > Monitors > SD-WAN Monitor* pane, and click *Template View*.
   - SD-WAN devices provisioned using the currently selected SD-WAN template are displayed on the map.
   - Only devices provisioned using the selected SD-WAN template are displayed. You can change the selected SD-WAN template by clicking the dropdown in the toolbar and selecting a new template.
   - Devices on the map are identified with icons as either a HUB (star icon) or spoke device (device icon).
2. Hovering your mouse over a device on the map displays the following information:
   - Device name and whether it is a HUB or spoke.
   - Interfaces that have a failed health check.
   - Down underlays.
3. The map shows lines connecting the HUB and spoke devices.
   The line color depends on if the tunnel is up (green) or down (red). Device color is based off of the following logic:
   a. If the SD-WAN health checks are defined on the device (usually a spoke):
      - Green: All health checks pass.
      - Orange: Some health checks pass.
      - Red: All health checks fail.
   b. When no SD-WAN health checks are defined on the device (usually a HUB):
      - Green: All underlays are up.
      - Orange: Some underlays are up.
      - Red: All underlays are down.
4. Hovering over a line displays a tooltip showing both device names.
5. Clicking on a line opens a pane with the following information:
   - Underlay Status table of HUB and spoke devices.
   - Health check table for the spoke devices.
6. Clicking on a spoke device opens a pane with the following information.
   - SD-WAN health check table.
   - Underlay status table.
   - IPsec VPN table.
   - Routing - Static Dynamic table.
7. Clicking on a HUB device opens a pane with the following information:
   - Underlay Status table.
   - IPsec VPN table.
   - Routing - Static Dynamic table.

To view the per-device SD-WAN History View:

1. Go to *Device Manager > Monitors > SD-WAN Monitor > Template View*.
2. Select a device from the SD-WAN Template View map.
3. Open the *SD-WAN History View* from one of two places:
   - Click the name of the SD-WAN device in the header (spokes).
   - Click *Drilldown to History View* beneath the *Performance SLAs* table (spokes).

Enabling SD-WAN monitoring history

FortiManager provides an option to collect and store SD-WAN Monitor data. Go to *SD-WAN > Monitor > Table View* to view the following drill-down data:

- Click each FortiGate device to view graphs of its details.
- Click each application to view graphs of its details.

By default, SD-WAN Monitoring History is disabled. When this feature is disabled, data for only the last 10 minutes is displayed. You can refresh to view the data directly from FortiGate devices. No historical data is stored in FortiManager when this feature is disabled.

You can enable the SD-WAN Monitoring history using the following command line:

```
config system admin setting
   set sdwan-monitor-history enable
```

When this feature is enabled, you can view the SD-WAN Monitoring history in the following ways:

- SD-WAN Monitoring data can be viewed for the past 5 minutes, 30 minutes, 1 hour, 4 hours, 12 hours, 1 day, 1 week, N hours, N days, N weeks, or custom.
- By default, SD-WAN Monitoring history is stored in FortiManager for 180 days. You can configure this setting in the CLI. See Monitoring history storage on page 393.

Monitoring history storage

In FortiManager (versions 7.6.3+ and 7.4.7+), a new log-based storage design has been implemented to replace the existing SD-WAN history database. Log-based storage enables more efficient handling of SD-WAN history data, reducing the strain on system resources and overall disk usage, and allows for more precise management of the disk space allocated for SD-WAN history.

To upgrade your SD-WAN history database to the log-based format:

If you have upgraded from an earlier FortiManager version, you can run the following command to upgrade the database to the new log-based storage format:

- `diagnose cdb upgrade force-retry upgrade-rtm-history-db`: Converts the old format real-time monitor (RTM) history database to the new log-based format, and provides the option to remove the old database.
- `diagnose cdb upgrade force-retry remove-old-rtm-history-db`: Removes the old format RTM history database.

For example, to upgrade the SD-WAN history to the new storage design:

```
diagnose cdb upgrade force-retry upgrade-rtm-history-db

Changes will be made to the database, however it is recommended to perform a backup first.
Do you want to continue? (y/n)y

Upgrading: Upgrade RTM history database to new format
This command will convert old RTM history data to new database format, and optionally delete old
history database.

  * Old RTM history database size: 0.00 GB
  * Estimated RTM history size after upgrade: 0.00 GB
```

```
  * Current free space in /Storage: 12.76 GB

Please make sure there is enough disk space to perform upgrade.
If there is not enough space, old history file may be removed during the conversion process.
Note that THIS OPERATION CANNOT BE UNDONE and old history will be forever lost, even with a
configuration backup!

  * Estimated largest history file after upgrade: 0.00 MB
  * Maximum RTM history file size: 1000 MB

If the largest history file size after upgrade is larger than the configured maximum history file
size, old history data may be immediat
ely purged after upgrade. If necessary, maximum history file size can be increased through system
admin setting.

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

Select YES to delete old databases during conversion. Once deleted, they CANNOT be recovered!
Select NO to keep old databases.
Do you want to continue? (y/n)y

Database upgrade complete.
```

To configure SD-WAN monitoring:

You can configure SD-WAN monitoring history using the following commands in the CLI.

- `rtm-max-monitor-by-days`: Sets the maximum real-time monitor (SD-WAN, traffic shaping, etc.) history by days (1-180).
- `rtm-max-monitor-by-size`: Sets a hard limit for the maximum real-time monitor (SD-WAN, traffic shaping, etc.) history by size in MB per device per and data type (10 - 200000).
- `rtm-temp-file-limit`: Set the real-time monitor temporary file limit by hours. A lower value will reduce disk usage, but may cause data loss (1 -120).



These commands are only available when SD-WAN monitoring history is enabled.

For example:

```
config system admin setting
  set sdwan-monitor-history enable
  set rtm-max-monitor-by-days <1-180>
  set rtm-max-monitor-by-size <10-200000>
  set rtm-temp-file-limit <1-120>
```

When to enable SD-WAN history

SD-WAN monitoring history should be enabled when you need to view historical SD-WAN data from FortiGate devices beyond the default 10 minutes that is kept when the feature is disabled.

Because SD-WAN monitoring history can consume a large amount of disk storage when FortiManager receives data from many FortiGate devices, it should only be enabled when there is adequate disk resources available to support the feature. In FortiManager 7.2.2 and later, you can configure the monitoring history storage settings in the FortiManager CLI to reduce disk usage. See Monitoring history storage on page 393. In earlier versions of FortiManager it is recommended that you monitor your disk usage while the SD-WAN history feature is enabled.

Furthermore, it's important to take into account the tunnel limitation of the central management unit. In order to ensure smooth performance of the system and stable connections for all the devices being managed, we highly recommend disabling data-intensive monitoring features like SD-WAN historical monitoring. By applying an add-on license to the central management unit, you can expand its support for devices beyond the default management tunnel limit. It's worth noting, though, that even with this enhancement, simultaneous management of all live tunnels may not be completely seamless. While the SD-WAN historical monitoring feature is designed to effectively handle live tunnels, it can put a strain on system resources.

If FortiManager is unable to process the data as it arrives due to the number of FortiGate devices, data that is held and unprocessed for more than two days will be dropped, and you may see gaps in the SD-WAN history.



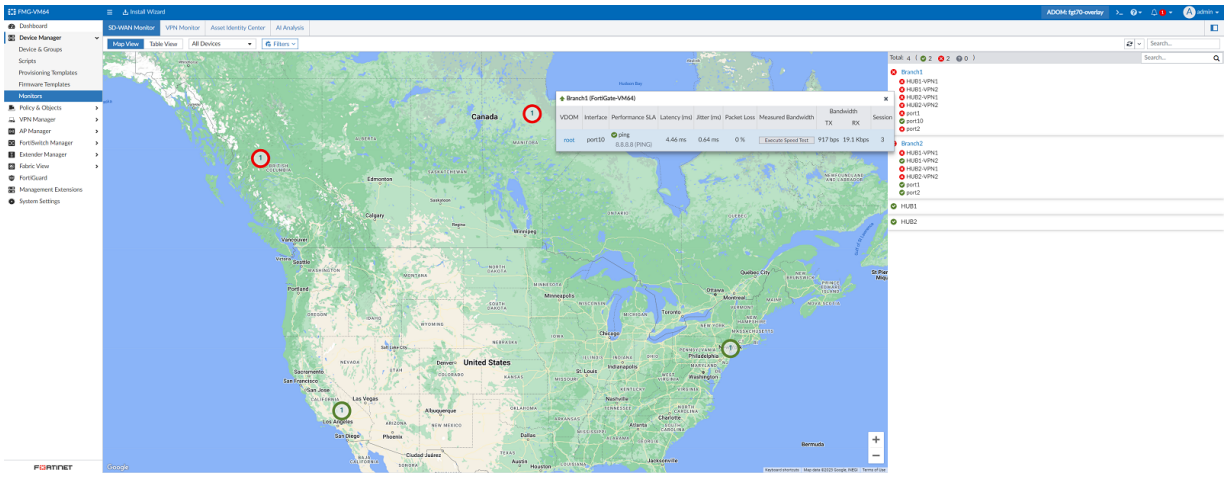
In 6.4.8, 7.0.1 and earlier releases, FortiManager's SD-WAN API calls to FortiGate can consume a lot of memory when there are many FortiGate devices, causing FortiManager to enter conserve mode. If you encounter this issue in these versions it is recommended to disable SD-WAN History or to upgrade to a later version of FortiManager.

SD-WAN cloud assisted monitoring speed test

FortiManager devices with the *FortiGuard SD-WAN Underlay Bandwidth and Quality Monitoring Service* subscription have the ability to execute a speed test on-demand from the SD-WAN Monitor page. The speed test can be executed on interfaces that have the WAN role.

To execute an SD-WAN speed test:

1. Execution of speed tests can be performed from the SD-WAN Monitor page.
2. For devices with a valid license and an interface configured with the WAN role, the *Execute Speed Test* option is displayed for the interface.
   - If there is a valid route to the cloud server, you will get measured bandwidth when executing the speed test.



- If there is not a valid route to the cloud server, you will see an error message when executing the speed test.
- You can perform the speed test up to 10 times per day. Attempts to perform additional speed tests will present an error message.
- For devices without a valid license, or for devices with a valid license but without an interface configured to the WAN role, the *Execute Speed Test* option is not displayed.

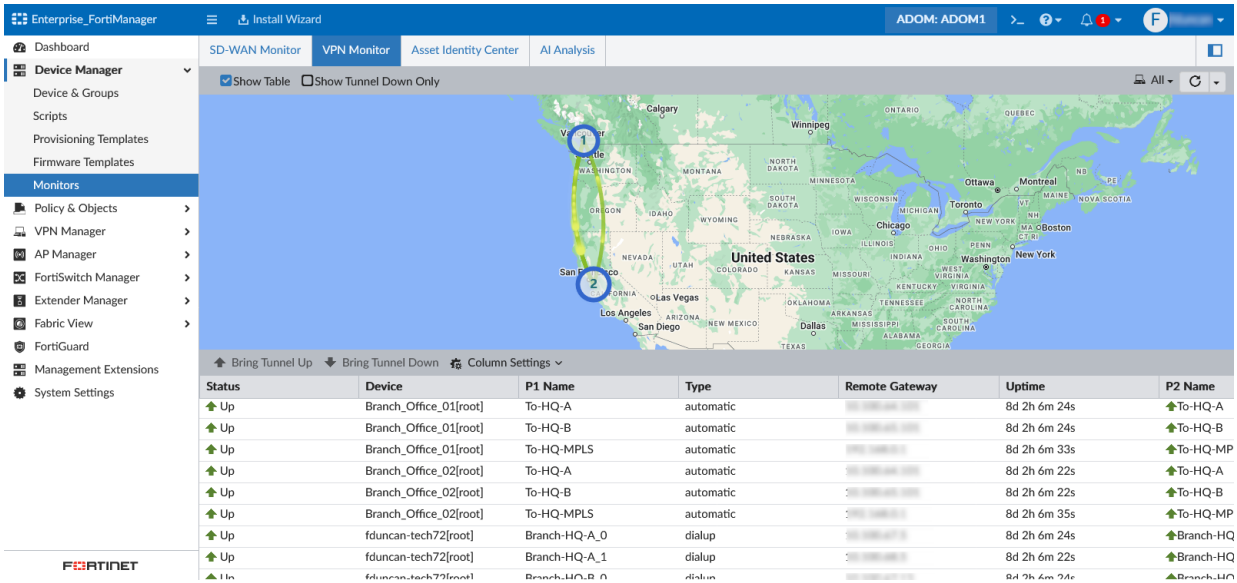
3. The results of the latest speed test are displayed on the SD-WAN Monitor pages in Map View, Table View, and when drilling down on a device. You can also see the results in *Device Manager > Device Dashboard > SD-WAN Monitor*.

VPN Monitor

You can use the *VPN Monitor* to view IPsec VPN tunnel information when the IPsec VPN is configured with VPN manager, IPsec templates, or created directly on FortiOS. For additional VPN monitoring options, see VPN Manager on page 650.

To view the IPsec tunnels in the VPN Monitor:

1. Go to *Device Manager* > *Monitors* > *VPN Monitor*.The map view of traffic for all IPsec tunnels is displayed.



2. The map includes the following information:
   - Green lines indicate that a tunnel is up.
     - When the green lines are animated, there is traffic flowing through the VPN tunnel.
     - You can hover your mouse over a green line to view the VPN tunnel name and source port information.
   - Red lines indicate that a tunnel is down.
   - HUB device(s) are identified with a star icon.
3. To view a single device's IPsec VPN tunnel information, change *All* to *Others* in the toolbar menu, and select a device from the dropdown.
4. To view a device group's IPsec VPN tunnel information, change *All* to *Others* in the toolbar menu, and select a device group from the dropdown.
5. To view IPsec VPN tunnel information in a table, select the *Show Table* option from the toolbar and the table will be displayed under the map.
   At the top of the table is a toolbar with the following options:
6.

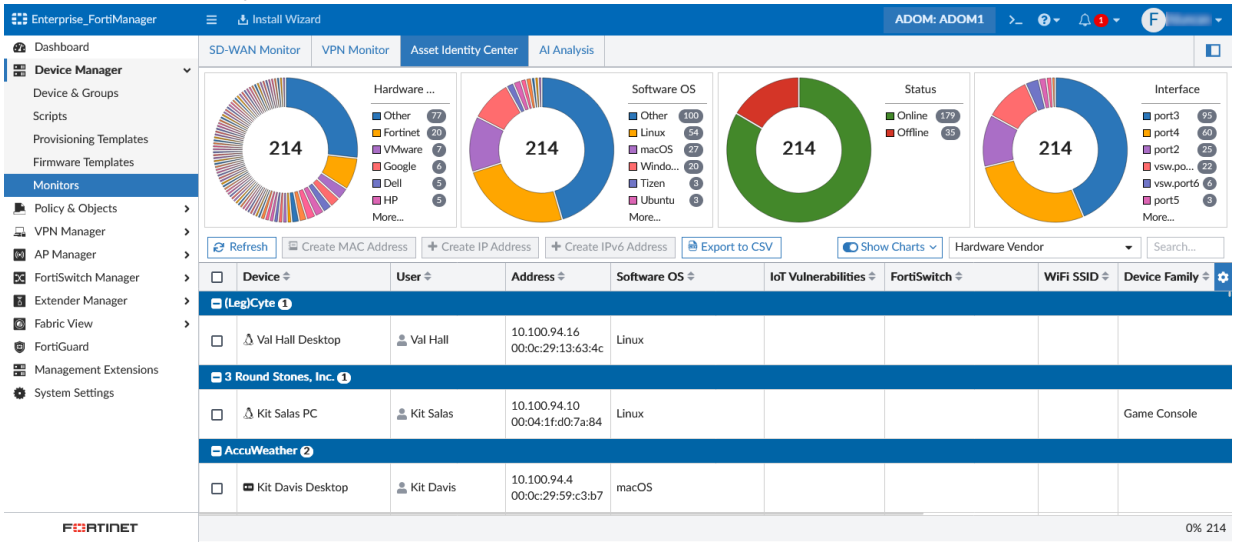
Bring Tunnel Up	Select a device in the table with a status of *Down*, and click *Bring Tunnel Up*.
Bring Tunnel Down	Select a device in the table with a status of *Up*, and click *Bring Tunnel Down*.
Column Settings	Click to select which columns to hide and display.



You can filter the VPN monitor table view. For example, you can use the greater than (>) or less than (<) signs on the incoming/outgoing bandwidth columns.

Asset Identity Center

You can use the *Asset Identity Center* for a central view of all devices detected by each FortiGate in the current ADOM. *Asset Identity Center* includes charts for FortiAP, FortiSwitch, and WiFi SSID.



To view the Asset Identity Center:

1. Go to *Device Manager > Monitors > Asset Identity Center*.
   The *Asset Identity Center* displays charts and the device inventory table. Click *Refresh* in the toolbar to refresh the chart and table data.
2. Set the *Show Charts* toggle to the *ON* position. You can choose which charts are visible by selecting them in the *Show Charts* dropdown menu. The *Device Inventory* includes the following charts:

Hardware Vendor	Displays the distribution of hardware vendors for detected devices.
Software OS	Displays the distribution of software OS for detected devices.
Status	Displays the status (online or offline) of detected devices.
Interface	Displays the distribution of interfaces used in detected devices.
FortiSwitch	Displays the distribution of FortiSwitch devices.
FortiAP	Displays the distribution of FortiAP devices.
WiFi SSID	Displays the distribution of WiFi SSIDs.

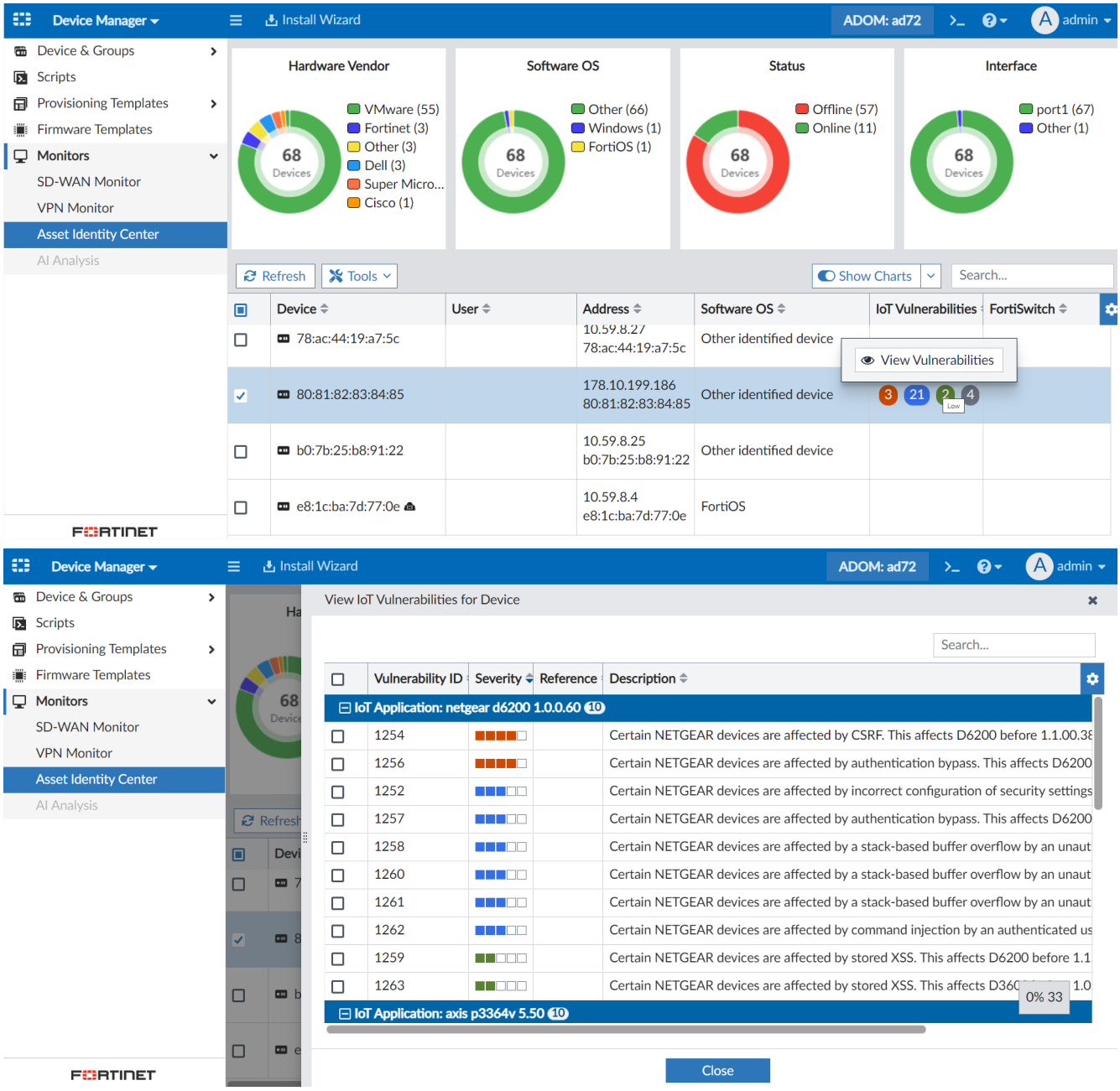
3. Click *Column Settings* in the toolbar to change which columns are displayed in the table.
4. Click *Tools* in the toolbar to access additional options. The following actions are available.
   - Create MAC Address
   - Create IP Address
   - Create IPv6 Address
   - Export to CSV

IoT Devices

The device table also includes IoT devices if they are collected by your FortiOS device. This requires an *IoT Detection Service* license. For more information, see IoT detection service in the FortiOS Administration Guide.

IoT devices are indicated by a cloud icon (☁) in the *Device* column. Mouse over the IoT device in the table to view detailed information.

Vulnerabilities affecting IoT devices are indicated in the *IoT Vulnerabilities* column. When vulnerabilities are present, you can click *View Vulnerabilities* to view detailed information about the detected vulnerabilities.

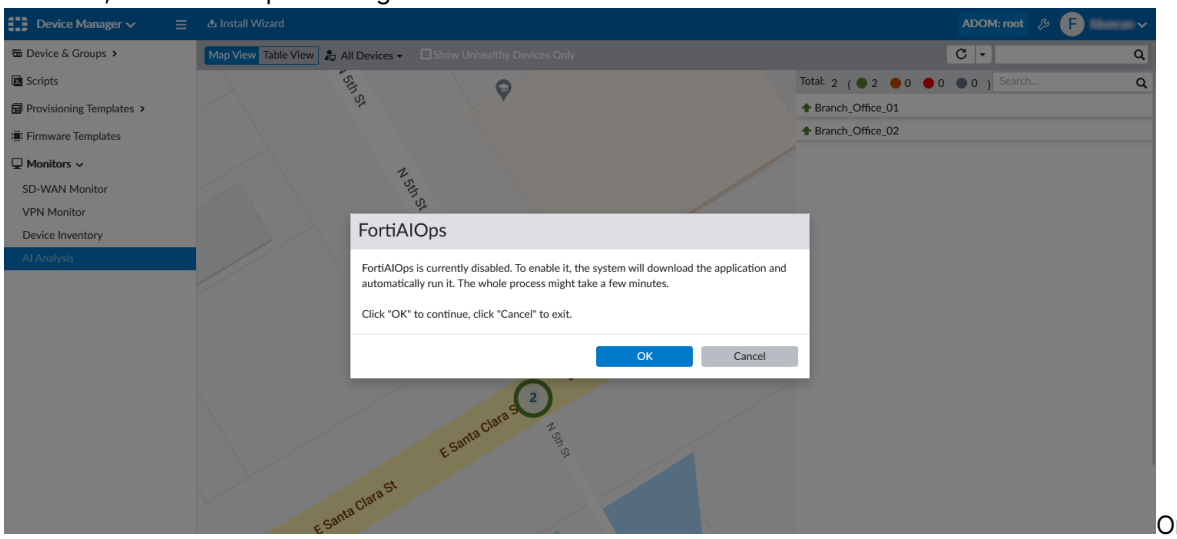


AI Analysis

The AI Analysis monitor can be enabled in *Device Manager* > *Monitors* to redirect to the FortiAIOps management extension.

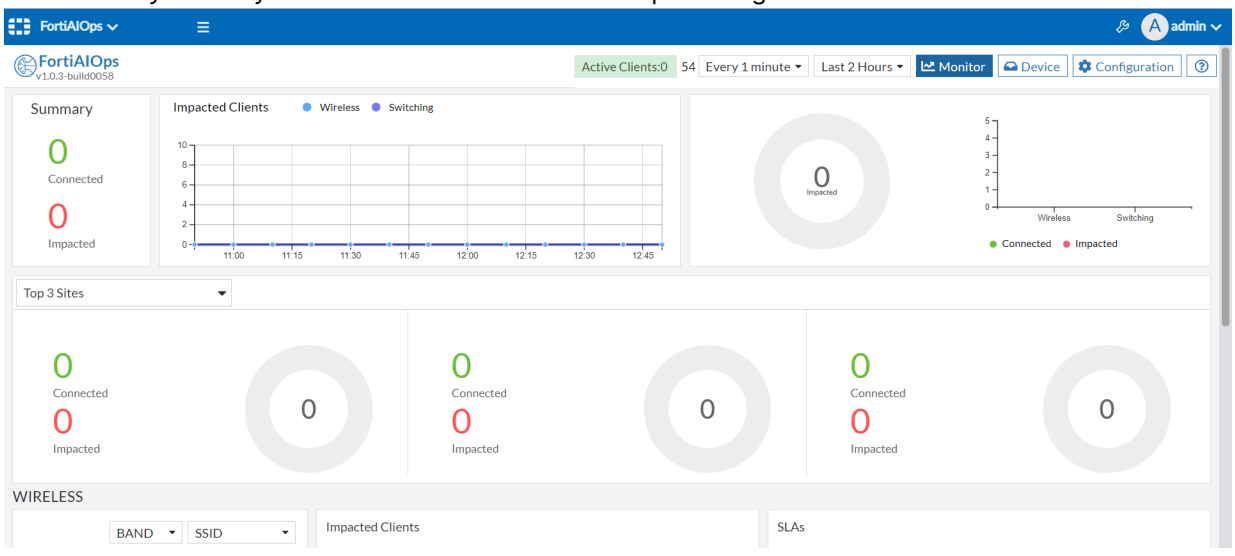
To enable the AI Analysis monitor:

1. In FortiManager, go to *Device Manager* > *Monitors*.
   By default, the AI Analysis monitor is grayed out.
2. Click *AI Analysis*, and a window to enable FortiAIOps is displayed.
3. Click *OK*, and FortiAIOps will begin to download.



Once the download has finished, the AI Analysis monitor link is no longer grayed out.

4. Click *AI Analysis* and you are redirected to the FortiAIOps management extension.

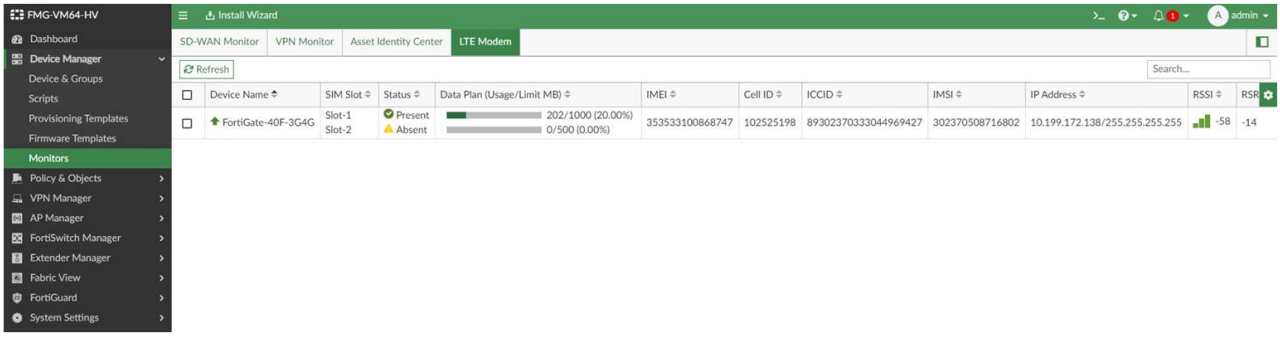


LTE modem monitors

The *LTE Modem* monitor can be viewed in *Device Manager > Monitors* when the FortiManager is managing a FortiGate 3G4G device in the ADOM.

To view the LTE modem monitor:

1. If using ADOMs, ensure you are in an ADOM with a managed 3G4G FortiGate.
2. Go to *Device Manager > Monitors > LTE Modem*. The LTE Modem monitor displays a table with LTE signal information and data usage displayed.



FortiGate chassis devices

Select FortiManager systems can work with the Shelf Manager to manage FortiGate 5050, 5060, 5140, and 5140B chassis. The Shelf Manager runs on the Shelf Management Mezzanine hardware platform included with the FortiGate 5050, 5060, 5140, and 5140B chassis. You can install up to five FortiGate 5000 series blades in the five slots of the FortiGate 5050 ATCA chassis and up to 14 FortiGate 5000 series blades in the 14 slots of the FortiGate 5140 ATCA chassis. For more information on FortiGate 5000 series including Chassis and Shelf manager, see the Fortinet Document Library.

You need to enable chassis management before you can work with the Shelf Manager through the FortiManager system.

To enable chassis management:

1. Go to *System Settings > Advanced > Advanced Settings*. See Miscellaneous Settings on page 973 for more information.
2. Under *Advanced Settings*, select *Chassis Management*.
3. Set the *Chassis Update Interval*, from 4 to 1440 minutes.
4. Click *Apply*.

To add a chassis:

1. Go to *Device Manager* > *Device & Groups*,
2. Right-click in the tree menu and select *Chassis* > *Add*. The *Create Chassis* window opens.
3. Complete the following fields, then click *OK*:

Name	Type a unique name for the chassis.
Description	Optionally, type any comments or notes about this chassis.
Chassis Type	Select the chassis type: Chassis 5050, 5060, 5140 or 5140B.
IP Address	Type the IP address of the Shelf Manager running on the chassis.
Authentication Type	Select Anonymous, MD5, or Password from the dropdown list.
Admin User	Type the administrator user name.
Password	Type the administrator password.
Chassis Slot Assignment	You cannot assign FortiGate-5000 series blades to the slot until after the chassis has been added.

To edit a chassis and assign FortiGate 5000 series blade to the slots:

1. Go to *Device Manager* > *Device & Groups*.
2. Right-click the chassis, and select *Edit*.
3. Modify the fields, except *Chassis Type*.
4. For *Chassis Slot Assignment*, from the dropdown list of a slot, select a FortiGate 5000 series blade to assign it to the slot. You can select a FortiGate, FortiCarrier, or FortiSwitch unit.



You can only assign FortiSwitch units to slot 1 and 2.

5. Click *OK*.

Viewing chassis dashboard

You can select a chassis from the chassis list in the content pane, and view the status of the FortiGate blades in the slots, power entry module (PEM), fan tray (FortiGate-5140 only), Shelf Manager, and shelf alarm panel (SAP).

Viewing the status of the FortiGate blades

In the *Device Manager* tab, select the Blades under the chassis whose blade information you would like to view.

The following is displayed:

Refresh	Select to update the current page. If there are no entries, Refresh is not displayed.
Slot #	The slot number in the chassis. • The FortiGate 5050 chassis contains five slots numbered 1 to 5. • The FortiGate 5060 chassis contains six slots numbered 1 to 6. • The FortiGate 5140 and 5140B chassis contains fourteen slots numbered 1 to 14.
Extension Card	If there is an extension card installed in the blade, this column displays an arrow you can select to expand the display. The expanded display shows details about the extension card as well as the blade.
Slot Info	Indicates whether the slot contains a node card (for example, a FortiGate 5001SX blade) or a switch card (for example, a FortiSwitch 5003 blade) or is empty.
State	Indicates whether the card in the slot is installed or running, or if the slot is empty.
Temperature Sensors	Indicates if the temperature sensors for the blade in each slot are detecting a temperature within an acceptable range. • *OK*: All monitored temperatures are within acceptable ranges. • *Critical*: A monitored temperature is too high (usually about 75°C or higher) or too low (below 10°C).
Current Sensors	Indicates if the current sensors for the blade in each slot are detecting a current within an acceptable range. • *OK*: All monitored currents are within acceptable ranges. • *Critical*: A monitored current is too high or too low.
Voltage Sensors	Indicates if the voltage sensors for the blade in each slot are detecting a voltage within an acceptable range. • *OK*: All monitored voltages are within acceptable ranges. • *Critical*: A monitored voltage is too high or too low.
Power Allocated	Indicates the amount of power allocated to each blade in the slot.
Action	Select *Activate* to turn the state of a blade from *Installed* into *Running*. Select *Deactivate* to turn the state of a blade from *Running* into *Installed*.
Edit	Select to view the detailed information on the voltage and temperature of a slot, including sensors, status, and state. You can also edit some voltage and temperature values.
Update	Select to update the slot.

To edit voltage and temperature values:

1. Go to *[chassis name] > Blades* and, in the content pane, select the *Edit* icon of a slot.
   The detailed information on the voltage and temperature of the slot including sensors, status, and state is displayed.

2. Select the *Edit* icon of a voltage or temperature sensor.
3. For a voltage sensor, you can modify the *Upper Non-critical, Upper Critical, Lower Non-critical*, and *Lower Critical* values.
4. For a temperature sensor, you can modify the *Upper Non-critical* and *Upper Critical* values.
5. Select *OK*.

Viewing the status of the power entry modules

You can view the status of the PEMs by going to *[chassis name] > PEM*. The FortiGate 5140 chassis displays more PEM information than the FortiGate 5050.

The following is displayed:

Refresh	Select to update the current page.
PEM	The order numbers of the PEM in the chassis.
Presence	Indicates whether the PEM is present or absent.
Temperature	The temperature of the PEM.
Temperature State	Indicates whether the temperature of the PEM is in the acceptable range. • *OK*: The temperature is within acceptable range.
Threshold	PEM temperature thresholds.
Feed -48V	Number of PEM fuses. There are four pairs per PEM.
Status	PEM fuse status: present or absent.
Power Feed	The power feed for each pair of fuses.
Maximum External Current	Maximum external current for each pair of fuses.
Maximum Internal Current	Maximum internal current for each pair of fuses.
Minimum Voltage	Minimum voltage for each pair of fuses.
Power Available	Available power for each pair of fuses.
Power Allocated	Power allocated to each pair of fuses.
Used By	The slot that uses the power.

Viewing fan tray status (FG-5140 and FG-5140B chassis only)

Go to *[chassis name] > Fan Tray* to view the chassis fan tray status.

The following is displayed:

Refresh	Select to update the current page.
Thresholds	Displays the fan tray thresholds.
Fan Tray	The order numbers of the fan trays in the chassis.

Model	The fan tray model.
24V Bus	Status of the 24V Bus: present or absent.
-48V Bus A	Status of the -48V Bus A: present or absent.
-48V Bus B	Status of the -48V Bus B: present or absent.
Power Allocated	Power allocated to each fan tray.
Fans	Fans in each fan tray.
Status	The fan status. • *OK*: It is working normally.
Speed	The fan speed.

Viewing shelf manager status

Go to *[chassis name]* > *Shelf Manager* to view the shelf manager status.

The following is displayed:

Refresh	Select to update the current page.
Shelf Manager	The order numbers of the shelf managers in the chassis.
Model	The shelf manager model.
State	The operation status of the shelf manager.
Temperature	The temperature of the shelf manager.
-48V Bus A	Status of the -48V Bus A: present or absent.
-48V Bus B	Status of the -48V Bus B: present or absent.
Power Allocated	Power allocated to each shelf manager.
Voltage Sensors	Lists the voltage sensors for the shelf manager.
State	Indicates if the voltage sensors for the shelf manager are detecting a voltage within an acceptable range. • *OK*: All monitored voltages are within acceptable ranges. • *Below lower critical*: A monitored voltage is too low.
Voltage	Voltage value for a voltage sensor.
Edit	Select to modify the thresholds of a voltage sensor.

Viewing shelf alarm panel (SAP) status

You can view the shelf alarm panel (SAP) status for a chassis. The shelf alarm panel helps you monitor the temperature and state of various sensors in the chassis.

Go to *[chassis name]* > *SAP* to view the chassis SAP status.

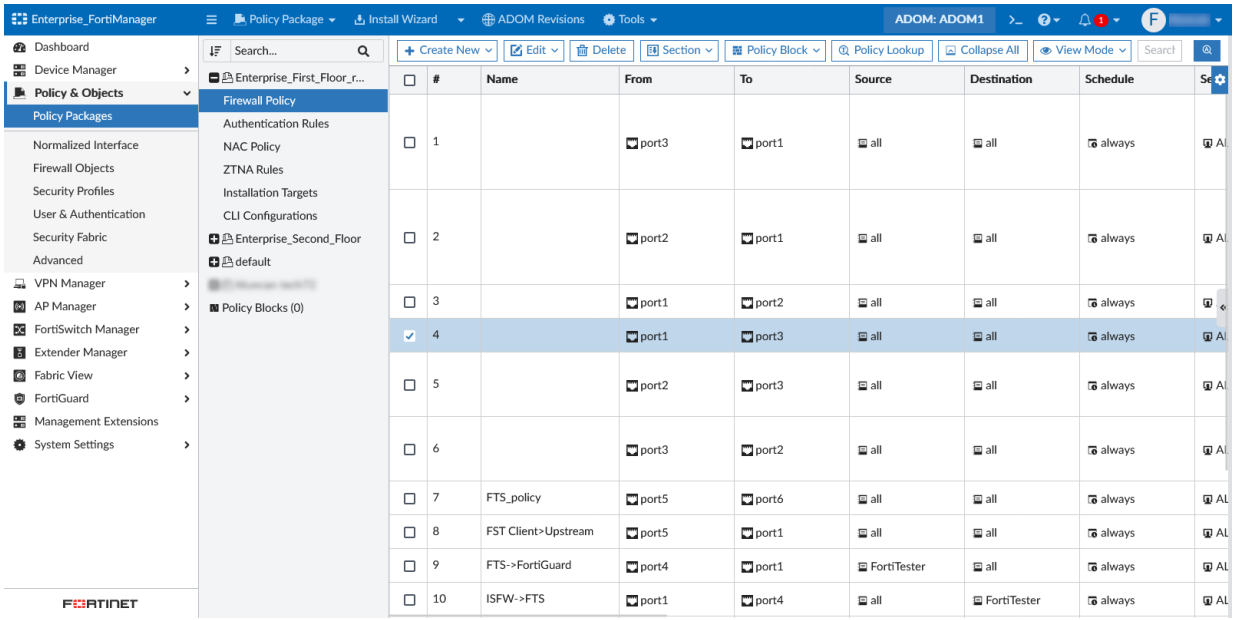
The following is displayed:

Presence	Indicates if the SAP is present or absent.
Telco Alarm	Telco form-c relay connections for minor, major and critical power faults provided by the external dry relay Telco alarm interface (48VDC).
Air Filter	Indicates if the air filter is present or absent.
Model	The SAP model.
State	The operation status of the shelf manager.
Power Allocated	Power allocated to the SAP.
Temperature Sensors	The temperature sensors of the SAP
Temperature	The temperature of the SAP read by each sensor.
State	Indicates if the temperature sensors for the SAP are detecting a temperature below the set threshold.
Edit	Select to modify the thresholds of a temperature sensor.

Policy & Objects

Policy & Objects enables you to centrally manage policies and any objects used by those policies for devices that are managed by the FortiManager.

All changes related to policies and objects should be made on the FortiManager device, and not on the managed devices.



This chapter includes the following sections:

- About policies on page 410
- Policy workflow on page 412
- Feature visibility on page 413
- Managing policy packages on page 414
- Managing policies on page 427
- Using Policy Blocks on page 517
- Managing objects and dynamic objects on page 532
- ADOM revisions on page 577

Administrator permissions

If the administrator account you logged on with does not have the appropriate permissions, you will not be able to edit or delete settings, or apply any changes. Instead you are limited to browsing. To modify these settings, see Administrator profiles on page 1010.



Object selection pane

You can determine the way that objects are displayed in *Policy & Objects* using the following object selection pane settings under the *Tools* menu.

- *Classic Dual Pane*: The *Policy Packages* and *Object Configurations* tabs are displayed on the same pane, with object configurations on the lower half of the screen.
- *Dock to Right*: You can open the objects window by clicking the expand icon on the right side of the screen. See Feature visibility on page 413.



Workspace and Workflow mode

If workspace is enabled, the ADOM must be locked before changes can be made. See Locking an ADOM on page 947.

If workflow is enabled, the ADOM must be locked and a session must be started before changes can be made. See Workflow mode on page 1026.

The following sections are available in the tree menu under *Policy & Objects*:

Policy Packages	Click to view and configure policy packages.
Normalized Interface	Click to view and configure normalized interfaces.
Firewall Objects	Click to view and configure firewall objects.
Security Profiles	Click to view and configure security profiles.
User & Authentication	Click to view and configure user and authentication objects.
Security Fabric	Click to view and configure Fortinet Security Fabric objects.
Advanced	Click to view and configure advanced objects including metadata variables and CLI configurations.

The following options are available in the *Policy Packages* pane:

Policy Package	Click to access the policy package menu. The menu options are the same as the right-click menu options.
Install Wizard	Click to access the Install Wizard. You can start the Install Wizard where you can install policy packages and device settings. You can also re-install a policy by clicking the dropdown arrow and choosing *Re-install Policy*.
ADOM Revisions	Click to create, edit, delete, restore, lock, and unlock ADOM Revisions.
Tools	Click to select one of the following tools from the menu: *Find Unused Objects*, *Find Duplicate Objects*, *Find Unused Policies*, *Refresh Hit Counts*, *Feature Visibility*, or *Object Selection Pane*.
Create New	Create a new policy. See Creating policies on page 429.
Edit	Edit a policy. See Editing policies on page 501.
Delete	Delete a policy.

Section	Create a new policy section. You can apply colors to policy sections to help differentiate your different policies in the table. See Managing policies on page 427.
Policy Lookup	Perform a policy lookup. See Policy Lookup on page 516
Collapse/Expand All	Collapse or expand all the categories in the policy list.
View Mode	Toggle between the *By Sequence* and *Interface Pair View* display modes. See Managing policies on page 427.  View Mode is disabled when policy packages include policies using multiple source/destination interfaces (including the "Any" interface) or when policy blocks are used.
Search	The tree menu can be searched and sorted using the search field and sorting button at the top of the menu.
Column Settings	Select which columns are displayed in the policy table.

The following options are available on the objects configuration panes:

Install Wizard	Click to access the Install Wizard. You can start the Install Wizard where you can install policy packages and device settings. You can also re-install a policy by clicking the dropdown arrow and choosing *Re-install Policy*.
ADOM Revisions	Click to create, edit, delete, restore, lock, and unlock ADOM Revisions.
Tools	Click to select one of the following tools from the menu: *Find Unused Objects*, *Find Duplicate Objects*, *Find Unused Policies*, *Refresh Hit Counts*, *Feature Visibility*, or *Object Selection Pane*.
Create New	Create a new object. See Creating objects on page 533.
Edit	Edit an object. See Edit an object on page 536.
Delete	Delete an object. See Remove an object on page 537.
More	Select the dropdown to view additional options for objects.
Column Settings	Select which columns are displayed in the objects table.

If workspace is enabled, you can select to lock and edit the policy package in the right-click menu. You do not need to lock the ADOM first. The policy package lock status is displayed in the toolbar.

The following options are available:

Lock | Unlock	Select to lock or unlock the ADOM.
Sessions	Click to display the sessions list where you can save, submit, or discard changes made during the session.

About policies

FortiManager provides administrators the ability to customize policies within their organization as they see fit. Typically, administrators may want to customize access and policies based on factors such as geography, specific security requirements, or legal requirements.

Within a single ADOM, administrators can create multiple policy packages. FortiManager provides you the ability to customize policy packages per device or VDOM within a specific ADOM, or to apply a single policy package for all devices within an ADOM. These policy packages can be targeted at a single device, multiple devices, all devices, a single VDOM, multiple VDOMs, or all devices within a single ADOM. By defining the scope of a policy package, an administrator can modify or edit the policies within that package and keep other policy packages unchanged.

FortiManager can help simplify provisioning of new devices, ADOMs, or VDOMs by allowing you to copy or clone existing policy packages.

Policy theory

Security policies control all traffic attempting to pass through a unit between interfaces, zones, and VLAN subinterfaces.

Security policies are instructions that units use to decide connection acceptance and packet processing for traffic attempting to pass through. When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a security policy matching the packet.

Security policies can contain many instructions for the unit to follow when it receives matching packets. Some instructions are required, such as whether to drop or accept and process the packets, while other instructions, such as logging and authentication, are optional.

Policy instructions may include Network Address Translation (NAT), or Port Address Translation (PAT), or they can use virtual IPs or IP pools to translate source and destination IP addresses and port numbers.

Policy instructions may also include Security Profiles, which can specify application-layer inspection and other protocol-specific protection and logging, as well as IPS inspection at the transport layer.

You configure security policies to define which sessions will match the policy and what actions the device will perform with packets from matching sessions.

Sessions are matched to a security policy by considering these features of both the packet and policy:

- Policy Type and Subtype
- Incoming Interface
- Source Address
- Outgoing Interface
- Destination Address
- Schedule and time of the session's initiation
- Service and the packet's port numbers.

If the initial packet matches the security policy, the device performs the configured action and any other configured options on all packets in the session.

Packet handling actions can be *ACCEPT*, *DENY*, *IPSEC*, or *SSL-VPN*.

- ACCEPT policy actions permit communication sessions, and may optionally include other packet processing instructions, such as requiring authentication to use the policy, or specifying one or more Security Profiles to apply features such as virus scanning to packets in the session. An ACCEPT policy can also apply interface-mode IPsec VPN traffic if either the selected source or destination interface is an IPsec virtual interface.
- DENY policy actions block communication sessions, and you can optionally log the denied traffic. If no security policy matches the traffic, the packets are dropped, therefore it is not required to configure a DENY security policy in the last position to block the unauthorized traffic. A DENY security policy is needed when it is required to log the denied traffic, also called “violation traffic”.
- IPSEC and SSL VPN policy actions apply a tunnel mode IPsec VPN or SSL VPN tunnel, respectively, and may optionally apply NAT and allow traffic for one or both directions. If permitted by the firewall encryption policy, a tunnel may be initiated automatically whenever a packet matching the policy arrives on the specified network interface, destined for the local private network.

Create security policies based on traffic flow. For example, in a policy for POP3, where the email server is outside of the internal network, traffic should be from an internal interface to an external interface rather than the other way around. It is typically the user on the network requesting email content from the email server and thus the originator of the open connection is on the internal port, not the external one of the email server. This is also important to remember when viewing log messages, as the source and destination of the packets can seem backwards.

Global policy packages

Global policies and objects function in a similar fashion to local policies and objects, but are applied universally to all ADOMs and VDOMs inside your FortiManager installation. This allows users in a carrier, service provider, or large enterprise to support complex installations that may require their customers to pass traffic through their own network.

For example, a carrier or host may allow customers to transit traffic through their network, but do not want their customer to have the ability to access the carrier’s internal network or resources. Creating global policy header and footer packages to effectively surround a customer’s policy packages can help maintain security.

Global policy packages must be assigned to ADOMs to be used. When configuring global policies, a block of space in the policy table is reserved for *Local Domain Policies*. All of the policies in an ADOM’s policy table are inserted into this block when the global policy is assigned to an ADOM.

You can specify which policy packages to assign the global policy to when assigning policy packages to an ADOM. Each policy package can only have one global policy package assigned to it, but multiple global policy packages can be used in an ADOM. See Assign a global policy package on page 417.

Policy Blocks can be used within Global Policy packages. See Using Policy Blocks on page 517.

Feature visibility options for policies and objects can be configured in *Policy & Objects > Tools > Feature Visibility*.

	Global policies and objects are not supported on all FortiManager platforms. Please review the products' data sheets to determine support.
	A global policy license is not required to use global policy packages.
	The use of local Policy Blocks simplifies the process for upgrading your ADOMs and can be considered as an alternative to Global Policy Packages. For more information, see Using Policy Blocks versus Global Policy Packages on page 525 and Migrating global policies to policy blocks on page 526.

Policy workflow

An administrator will typically carry out two main functions with their devices through FortiManager: provisioning new devices or VDOMs on the network and managing the day-to-day operations of managed devices and VDOMs.

Provisioning new devices

There are multiple steps to provision a new device or VDOM to be managed by the FortiManager unit:

1. In the *Device Manager* pane, create a new VDOM or add a new device.
2. Assign a system template to the provisioned device (optional).
3. In the *Policy & Objects* pane, configure any dynamic objects you wish to assign to the new VDOM or device.
4. Determine how a policy will be defined for the new device: does the new device or VDOM have a new policy package unique to itself, or will the device or VDOM use a package that is implemented elsewhere?
5. Run the *Install Wizard* to install any objects and policies for the new device, or create a new policy package.
6. If the new device uses an existing policy package, modify the installation targets of that package to include the new device.

Day-to-day management of devices

An administrator will often have to modify various objects for the devices they are responsible for managing. A typical set of tasks to manage an already provisioned device will include:

1. Adding, deleting, or editing various objects, such as firewall information, security profiles, user access rights, antivirus signatures, etc.

2. Adding, deleting, or editing all of the policy packages or individual policies within a policy package. This can include changing the order of operation, adding new policies, or modifying information or access permissions in the policy package.
3. Installing updates to devices.

Feature visibility

The policy and objects that are displayed on the *Policy & Objects* pane can be customized, and Policy Packages and object configurations can be displayed on a single pane.

Configuring feature visibility settings

To adjust the policies and objects that are displayed, go to *Tools* > *Feature Visibility*.

You can turn the options on or off (visible or hidden). To turn on an option, select the checkbox beside the option name. To turn off an option, clear the checkbox beside the option name. You can turn on all of the options in a category by selecting the checkbox beside the category name. For example, you can turn on all firewall objects by selecting the checkbox beside *Firewall Objects*. You can also turn on all of the categories by clicking the *Check All* button at the bottom of the window.



Various feature visibility options are enabled by default and cannot be turned off.

Once turned on, you can configure the corresponding options from the appropriate location on the *Policy & Objects* > *Object Configurations* pane.

Reset all of the options by clicking the *Reset to Default* button at the bottom of the screen, or reset only the options in a category by clicking the *Reset to Default* button beside the category name.

By default, feature visibility settings are applied to the ADOM. All administrators using the ADOM will share the same visibility settings. Optionally, you can change this by making feature visibility settings applicable per-administrator. Changing between these modes can be done using the FortiManager CLI:

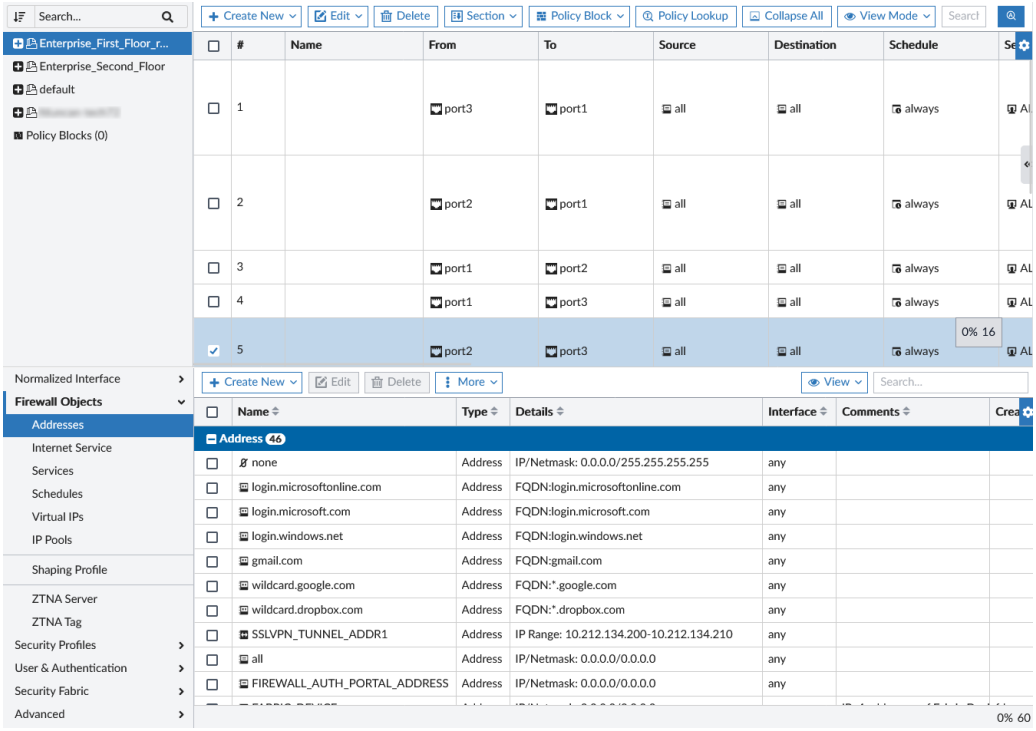
```
config system global
   set gui-feature-visibility-mode {per-admin | per-adom}
end
```

Viewing policies and objects in a single pane

To view policies and objects on a single pane:

1. Go to *System Settings* > *Advanced* > *Misc Settings* and enable *Display Policy & Objects in Classic Dual Pane*, or go to *Policy & Objects* > *Tools* and select *Classic Dual Pane*.

The *Policy & Objects* pane will now display both the *Policy Packages* and *Object Configuration* tree menu panes at the same time.



Managing policy packages

Policy packages can be created and edited, and then assigned to specific devices in the ADOM. Folders can be created for the policy packages to aid in the organization and management of the packages.

Not all policy and object options are enabled by default. To configure the enabled options, go to *Policy & Objects* > *Tools* > *Feature Visibility* and select your required options.

All of the options available from the *Policy Packages* menu can also be accessed by right-clicking anywhere in the policy tree menu.

FortiManager shows the last opened Policy Package for easy navigation. After opening a Policy Package, log off and log on in the same browser. Navigate to *Policy and Objects* in the same ADOM. The last opened Policy Package is shown.

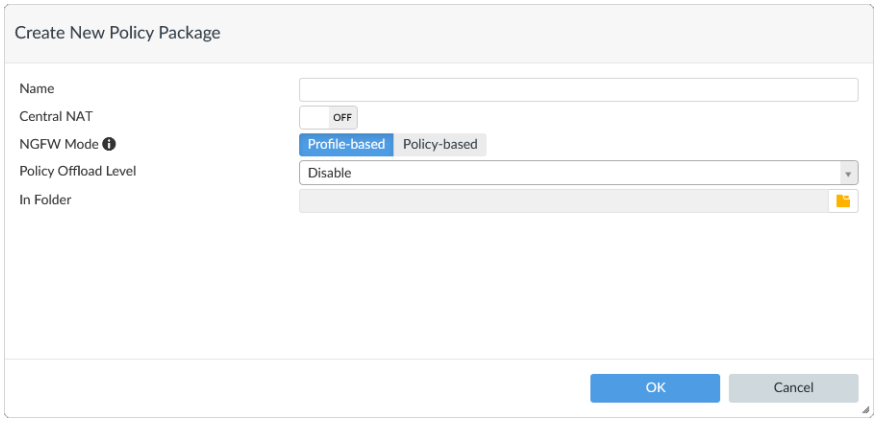
Create new policy packages

To create a new global policy package:

1. Ensure that you are in the *Global Database* ADOM.
2. Go to *Policy & Objects*.
3. From the *Policy Package* dropdown menu, select *New* or right-click beneath *Policy Packages* in the tree menu and select *New*. The *Create New Policy Package* window opens.
4. Enter a name for the new global policy package.
5. (Optional) Click the *In Folder* button to select a folder.
6. (Optional) Select the *Central NAT* checkbox to enable *Central SNAT* and *Central DNAT* policy types.
7. Click *OK* to add the policy package.

To create a new policy package:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* .
3. From the *Policy Package* dropdown menu select *New* or right-click beneath *Policy Packages* in the tree menu and select *New*. The *Create New Policy Package* window opens.



4. Configure the following details, then click *OK* to create the policy package.

Name	Enter a name for the new policy package.
Central NAT	Select the *Central NAT* check box to enable *Central SNAT* and *Central DNAT* policy types.
NGFW Mode	Select the NGFW mode, *Profile-based* (default) or *Policy-based*.
SSL/SSH Inspection	Select an SSL/SSH inspection type from the dropdown list. This option is only available for version 5.6 and later ADOMs when *NGFW Mode* is *Policy-based*.
Consolidated Firewall Mode	Toggle the *Consolidated Firewall Mode* button to *ON* to create a consolidated IPv4 and IPv6 policy. By default, the button is turned to *OFF*.

Policy Offload Level	Select the policy offload level. When configuring hyperscale policies, select *Full Offload*.
In Folder	Optionally, click the *In Folder* button to select a folder for the package.



The *Consolidated Firewall Mode* option is not available in the Global Database.



After turning the *Consolidated Firewall Mode* option to *ON*, and creating a consolidated IPv4 and IPv6 policy, turning the *Consolidated Firewall Mode* to OFF will make the consolidated IPv4 and IPv6 policy inaccessible. To access the consolidated IPv4 and IPv6 policy, you must keep the *Consolidated Firewall Mode* option *ON*.

Create new policy package folders

You can create new policy package folders within existing folders to help you better organize your policy packages.

To create a new policy package folder:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. From the *Policy Package* dropdown menu select *New Folder* or right-click in the tree menu beneath *Policy Packages* and select *New Folder*. The *Create New Policy Folder* window opens.
4. Enter a name for the new policy folder.
5. (Optional) Click the *In Folder* button to nest the new folder inside another folder.
6. Click *OK*. The new policy folder is displayed in the tree menu.

Edit a policy package or folder

Policy packages and policy package folders can be edited and moved as required. You can also review the revision history to troubleshoot issues.

Changes made to a policy package are displayed in the *Revision History* table at the bottom of the page. To view the history, select a revision in the table and click *View Diff*, or double-click the revision. You can also access the table by right-clicking a policy in the tree menu and selecting *Policy Revision*.

To edit a policy package or folder:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Select the package or folder in the tree menu then select *Policy Package* > *Edit* from the toolbar, or right-click on the package or folder and select *Edit* from the menu.

4. Edit the settings as required.
5. In the *Change Note* field, enter a description of the edit.
6. Click *OK* to apply all your changes.



Deselecting *Central NAT* does not delete Central SNAT or Central DNAT entries.

To move a policy package or folder:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Select the package or folder in the tree menu then select *Policy Package* > *Move* from the toolbar, or right-click on the package or folder and select *Move* from the menu.
4. Change the location of the package or folder as required, then click *OK*.

Clone a policy package

To clone a policy package:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Select the package or folder in the tree then select *Policy Package* > *Clone* from the toolbar, or right-click on the package or folder and select *Clone* from the menu.
4. Edit the name and location of the clone as required.
5. Click *OK* to create the cloned policy package.

Remove a policy package or folder

To remove a policy package or folder:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Select the package or folder in the tree menu then select *Policy Package* > *Delete* from the toolbar, or right-click on the package or folder and select *Delete* from the menu.

Assign a global policy package

Global policy packages can be assigned or installed to all policies in an ADOM or to specific policies packages within an ADOM.

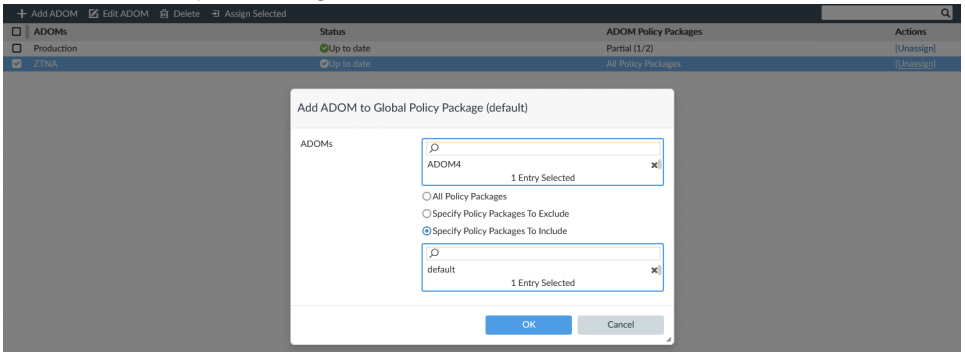
Only ADOMs of the same version as the global database or the next higher major release are presented as options for assignment. Each policy package can only have one global policy package assigned to it, but multiple global policy packages can be used in an ADOM.

To assign a global policy package:

1. Ensure you are in the *Global Database* ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package, click *Assignment*. The ADOM assignment list is displayed in the content pane.



4. If required, select *Add ADOM* to add an ADOM to the assignment list.
   The *Add ADOM to Global Policy Package* dialog opens.
   a. In the assignment list, select an ADOM, or click *Select All*.
   b. Select the global policy packages that will be assigned to the specified ADOM(s) from one of the following options:
      - *All Policy Packages*: Assigns the global policy package to all policy packages.
      - *Specify Policy Packages to Exclude*: Assigns the global policy package to all *except* the specified policy packages.
      - *Specify Policy Packages to Include*: Assigns the global policy package to *only* the specified policy packages.
   c. Click *OK* to save your changes.



5. Select an ADOM in the *Assignment* table, and click *Assign Selected* from the content toolbar.
   The *Assign* dialog box opens.
6. Select whether you want to assign only used objects or all objects, and if policies will be automatically installed to ADOM devices.
7. Click *OK* to assign the global policy package to the selected ADOMs.
   The *ADOM Policy Packages* column in the *Assignment* table displays if the global policy package is assigned to all policy packages or a partial number of policy packages in the ADOM.



In the *Assignment* pane you can also edit the ADOM list, delete ADOMs from the list, and assign and unassign ADOMs.

Install a policy package

When installing a policy package, objects that are referenced in the policy will be installed to the target device. Default or per-device mapping must exist or the installation will fail.



Some objects that are not directly referenced in the policy will also be installed to the target device, such as FSSO polling objects, address and profile groups, and CA certificates.

Some objects that are not referenced will be removed from the FortiGate. This may be particularly noticeable when installing a policy package for the first time after adding a device to FortiManager.

If you anticipate needing those objects in the future, make sure those objects are present in Policy & Objects before proceeding with the installation. To ensure that those objects are present in *Policy & Objects* you can use the *Add ALL Objects* option when importing a policy.



Policies within a policy package can be configured to install only on specified target devices. See Installing policies to specific devices on page 503.

To install a policy package to a target device:

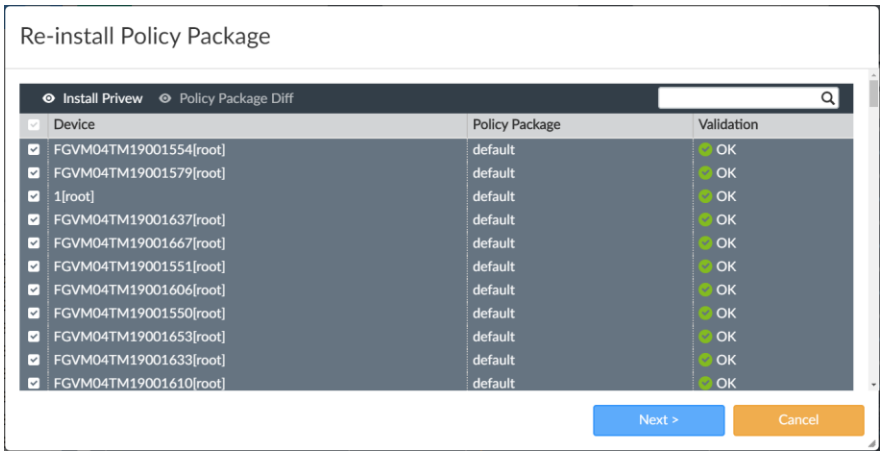
1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Click *Install* > *Install Wizard* from the toolbar or right-click a policy and select *Install Wizard*. The *Install Wizard* opens.
4. Follow the steps in the install wizard to install the policy package. You can select to install policy package and device settings or install the interface policy only.
   For more information on the install wizard, see Installing policy packages and device settings on page 180.
   For more information on editing the installation targets, see Policy package installation targets on page 422.

Reinstall a policy package

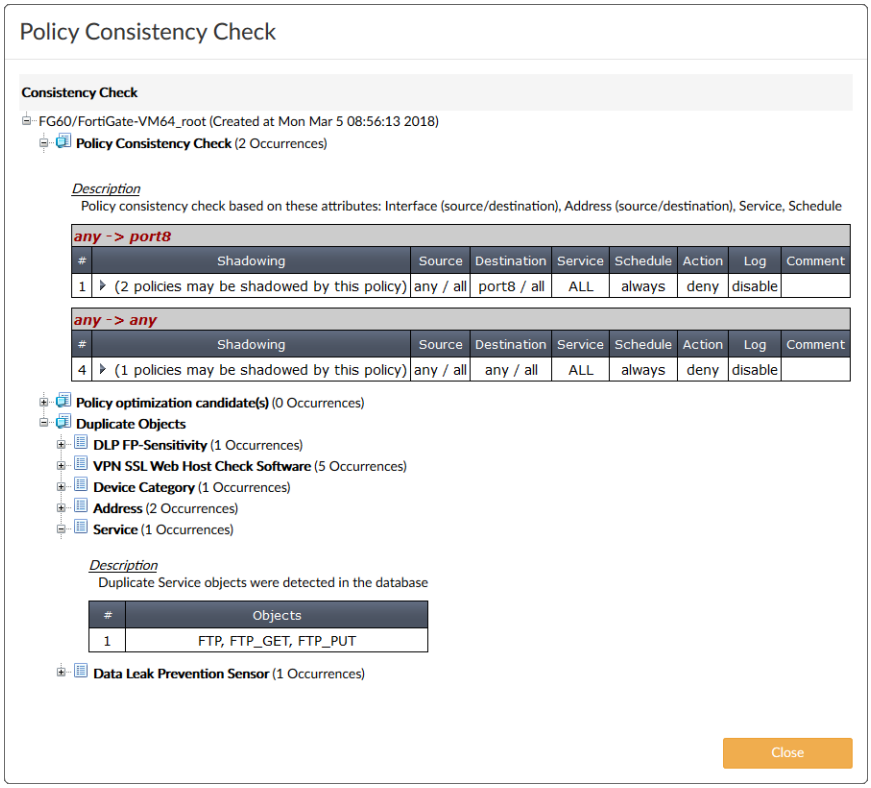
You can reinstall a policy package in *Policy & Objects* or *Device Manager*.

To reinstall a policy package:

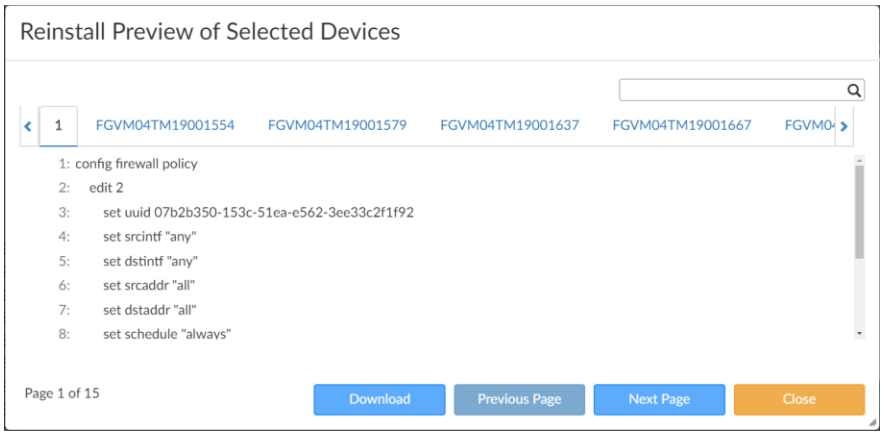
1. If using ADOMs, ensure that you are in the correct ADOM.
2. Perform one of the following actions:
   - Go to *Policy & Objects* > *Policy Packages*, and select a policy package.
   - Go to *Device Manager*, and select devices or VDOMs. You can select more than one device at a time.
3. In the toolbar, select *Install* > *Re-install Policy*.
   After data is gathered, the *Re-install Policy Package* window is displayed.



4. (Optional) View policy consistency check results (see Perform a policy consistency check on page 424).
   a. Click the *Policy Check Result* button.



   b. Click the *Close* button to close the page and return to the wizard.
5. (Optional) View a preview of the installation. You can preview multiple devices at the same.
   a. Click the *Install Preview* button.
   After data is gathered, the *Install Preview* page is displayed.



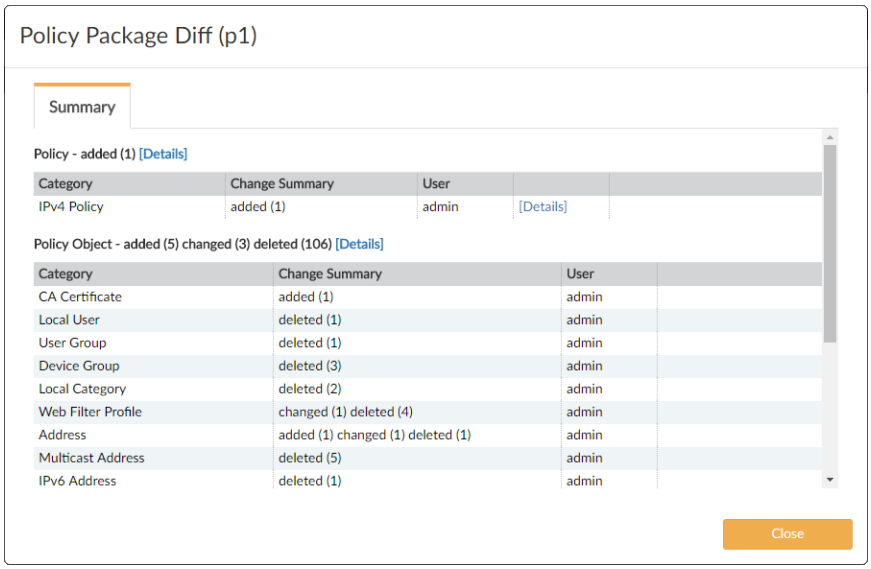
b. Click *Next Page* or *Previous page* to view multiple devices

c. Click the *Download* button to download a text file of the preview information.

d. Click the *Close* button to close the page and return to the wizard.

6. (Optional) View the difference between the current policy package and the policy in the device.

a. Click the *Policy Package Diff* button.
After data is gathered, the *Policy Package Diff* page is displayed.



b. Click the *Details* links to view details about the changes to the policy, specific policies, and policy objects.

c. Click *Close* to close the page and return to the wizard.

7. Click *Next*.
8. Click *Install*.
The policy package is reinstalled to the target devices.

Schedule a policy package install

In FortiManager you can create, edit, and delete install schedules for policy packages. The *Schedule Install* menu option has been added to the *Install* wizard when selecting to install policy package and device settings.

You can specify the date and time to install the latest policy package changes.

Select the clock icon which is displayed beside the policy package name to create an install schedule. Select this icon to edit or cancel the schedule. When a scheduled install has been configured and is active, hover the mouse over the icon to view the scheduled date and time.

To schedule the install of a policy package to a target device:

1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects* > *Policy Packages*.
3. From the *Install* menu, select *Install Wizard*. The *Install Wizard* opens.
4. Select *Schedule Install*, and set the install schedule date and time.
5. Select *Next*. In the device selection screen, edit the installation targets as required.
6. Select *Next*. In the interface validation screen, edit the interface mapping as required.
7. Select *Schedule Install* to continue to the policy and object validation screen. In the ready to install screen you can copy the log and download the preview text file.

To edit or cancel an install schedule:

1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Click the clock icon next to the policy package name in the *Policy Package* tree. The *Edit Install Schedule* dialog box is displayed.
4. Select *Cancel Schedule* to cancel the install schedule, then select *OK* in the confirmation dialog box to cancel the schedule. Otherwise, edit the install schedule as required and select *OK* to save your changes.

Export a policy package

You can export a policy package as a Microsoft Excel or CSV file.

To export a policy package:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Select a policy package or folder then, from the *Policy Package* menu, select *Export to Excel* or *Export to CSV*.
   The policy package is downloaded to your management computer.

Policy package installation targets

The *Installation Targets* pane allows you to view the installation target, config status, policy package status, and schedule install status, as well as edit installation targets for policy package installs.

To view installation targets, go to *Policy & Objects* > *Policy Packages*. In the tree menu for the policy package, select *Installation Targets*.

The following information is displayed:

Installation Target	The installation target and connection status.
Config Status	See the table below for config status details.
Policy Package Status	See the table below for policy package status details.

The following table identifies the different available config statuses.

Config Status	Icon	Description
Synchronized	Green check	Configurations are synchronized between FortiManager and the managed device.
Modified	Yellow triangle	Configurations are modified on FortiManager and not synchronized between FortiManager and the managed device.
Auto-update	Green check	Configurations modified on the managed device are auto synced to FortiManager.
Modified (recent auto-updated)	Yellow triangle	Configurations are modified on FortiManager and configurations modified on the managed device are auto synced to FortiManager.
Out of Sync	Red X	Configurations are modified on the managed device and not synced to FortiManager.
Conflict	Red X	When one of the following happens: • Install failed • Configurations are modified on both FortiManager and the managed device, and not auto synced to FortiManager.
Unknown	Gray question mark	When one of the following happens: • Connection goes down • No revision is generated, like added model device

The following table identifies the different available policy package statuses.

Policy Package Status	Icon	Description
Imported	Green check	Policies and objects are imported into FortiManager.

Policy Package Status	Icon	Description
Synchronized	Green check	Policies and objects are synchronized between FortiManager and the managed device.
Modified	Yellow triangle	Policies or objects are modified on FortiManager.
Out of Sync	Red X	Policies or objects are modified on the managed device.
Unknown with policy package name	Gray question mark	Configurations of the managed device are retrieved on FortiManager after being imported/installed.
Never Installed	Yellow triangle	No policy package is imported or installed.



When importing a device with agentless FSSO configured (that is, the device polls the AD servers), the status of all policy packages that reference *user fsso-polling* is *Modified*. This is because FortiManager sends all fsso-polling objects to all devices that are using agentless FSSO.

The following options are available:

Add	Select to add installation targets (device/group) for the policy package selected. Select the add icon beside *Device/Group* to select devices.
Delete	Select to delete the selected entries from the installation target for the policy package selected.
Install	Select an entry in the table and, from the *Install* menu, select *Install Wizard* or *Re-install Policy*.
Search	Use the search field to search installation targets. Entering text in the search field will highlight matches.

Perform a policy consistency check

The policy check tool allows you to check all policy packages within an ADOM to ensure consistency and eliminate conflicts that may prevent your devices from passing traffic. This allows you to optimize your policy sets and potentially reduce the size of your databases.

The check will verify:

- Object duplication: two objects that have identical definitions
- Object shadowing: a higher priority object completely encompasses another object of the same type
- Object overlap: one object partially overlaps another object of the same type
- Object orphaning: an object has been defined but has not been used anywhere.

The policy check uses an algorithm to evaluate policy objects, based on the following attributes:

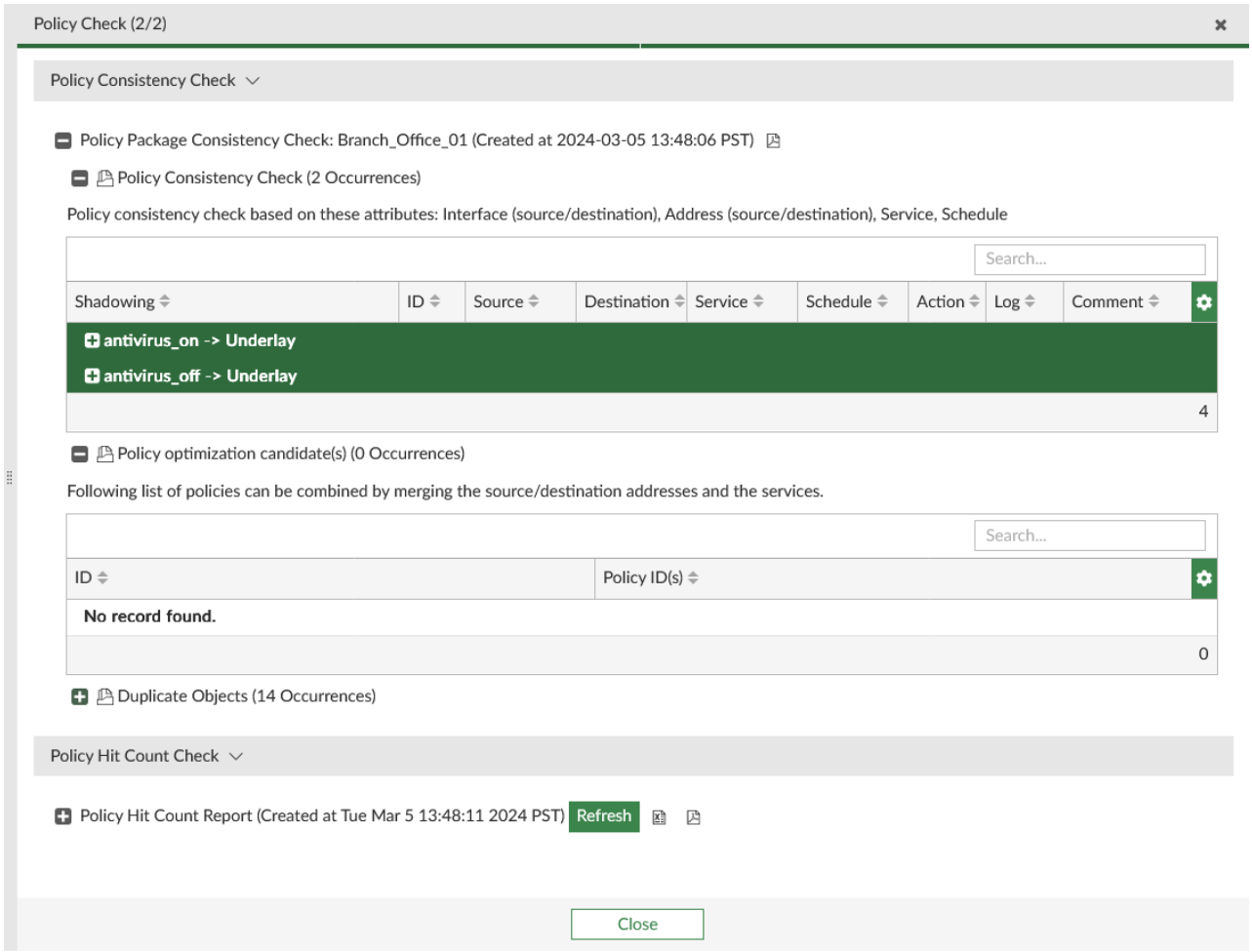
- The source and destination interface policy objects
- The source and destination address policy objects
- The service and schedule policy objects.

A policy consistency check can be automatically performed during every install. When doing the install, only modified or added policies are checked, decreasing the performance impact when compared to a full consistency check.

This function can be enabled when editing the ADOM (see Editing an ADOM on page 938).

To perform a policy check:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Select a policy package or folder, and from the *Policy Package* menu, select *Policy Check*. The *Policy Consistency Check* dialog box opens.
4. To perform a new consistency check, select *Perform Policy Consistency Check*, then click *OK*.
   A policy consistency check is performed, and the results screen is shown.



5. (Optional) Click the *Export to PDF* icon next to the *Policy Package Consistency Check* to download a copy of the consistency check.
6. (Optional) Click the *Export to CSV* or *Export to PDF* icons next to the *Policy Hit Count Report* to download a copy of the hit count report.

To view the results of the last policy consistency check:

1. Select the ADOM for which you performed a consistency check.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Select a policy package or folder, and from the *Policy Package* menu, select *Policy Check*. The *Policy Consistency Check* dialog box opens.
4. To view the results of the most recent consistency check, select *View Last Policy Consistency Check Result*, then click *OK*.
   The *Policy Consistency Check* window opens, showing the results of the last policy consistency check.

View logs related to a policy rule

After you add a FortiAnalyzer device to FortiManager by using the Add FortiAnalyzer wizard, you can view the logs that it receives. In the *Policy & Objects* pane, you can view logs related to the UUID for a policy rule. You can also use the UUID to search related policy rules.

See also Add FortiAnalyzer or FortiAnalyzer BigData on page 134.

To view logs related to a policy rule:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. From the *Column Settings* menu in the toolbar, select *UUID*.
   The UUID column is displayed.
4. Select a policy package.
5. In the content pane, right click a number in the *UUID* column, and select *View Log*.
   The *View Log by UUID: <UUID>* window is displayed and lists all of the logs associated with the policy ID.

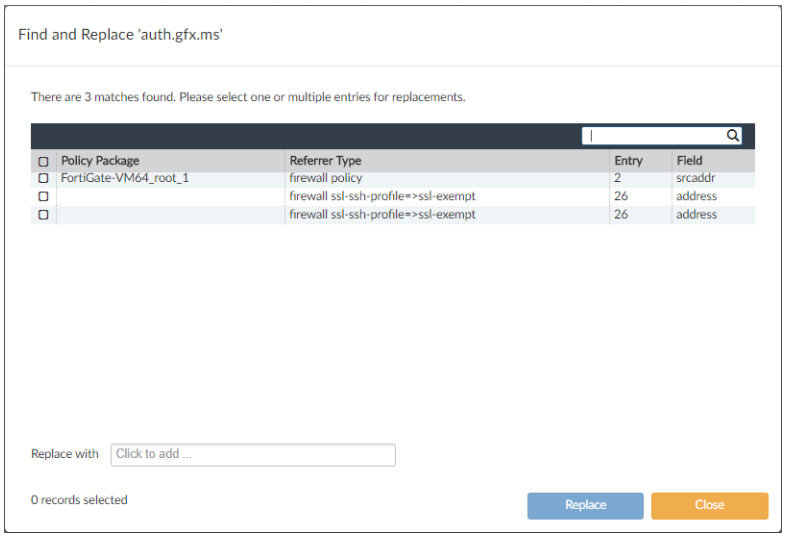
Find and replace objects

You can find and replace objects used in multiple policies and policy packages. Some objects can be replaced with multiple objects.

To find and replace objects:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Select a policy package, and then select a policy.
   Details for the policy are displayed in the content pane.

4. In the content pane, right-click an object in one of the columns, for example an interface in the *From* column, and select *Find and Replace*.
   All policies in all policy packages are searched, and all occurrences of the found object are displayed in the *Find and Replace* dialog box.



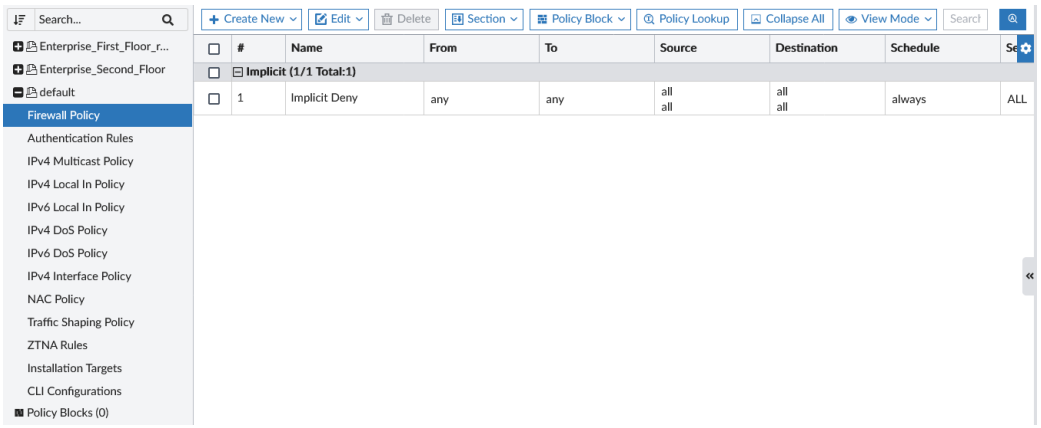
5. Select the checkbox for the entries that include the object you want to replace.
6. In the *Replace with* box, select one or more objects to use instead.
7. Click *Replace*.
   The objects are replaced, and the results are displayed.
8. (Optional) Click *Export to PDF* to download a PDF summary of what objects were replaced.

Managing policies

Policies in policy packages can be created and managed by selecting an ADOM, and then selecting the policy package whose policies you are configuring.

For some policy types, sections can be added to the policy list to help organize your policies, and the policies can be listed in sequence, or by interface pairs. When creating a section, you can optionally assign the section title a color to help better organize your policies.

On the *Policy & Objects* > *Policy Packages* pane, the tree menu lists the policy packages and the policies in each policy package. The policies that are displayed for each policy package are controlled by the feature visibility. See Feature visibility on page 413 for more information.



You can configure the following policies for a policy package:

- Firewall policy
- Firewall virtual wire pair policy
- SSL inspection and authentication policy
- Virtual wire pair SSL inspection and authentication policy
- Security policy
- Security virtual wire pair policy
- Proxy policy
- Central SNAT policy
- Central DNAT policy
- DoS policy
- Interface policy
- Multicast policy
- Local-in policy
- Traffic shaping policy
- Authentication rule
- Zero Trust Network Access (ZTNA) rule
- FortiProxy firewall policy
- FortiProxy proxy auto-configuration (PAC) policy
- Hyperscale policies

Various options are also available from column specific right-click menus, for more information see Column options on page 510.

If workspace or workflow is enabled, the ADOM must be locked before changes can be made. See Locking an ADOM on page 947.

Not all policy and object options are enabled by default. To configure the enabled options, from the *Tools* menu, select *Feature Visibility*.

Section view will be disabled if one or more policies are using the *Any* interface, or if one or more policies are configured with multiple source or destination interfaces.

Creating policies

To create a new policy:

Policy creation varies depending on the type of policy that is being created. See the following section that corresponds to the type of policy you are creating for specific instructions on creating that type of policy.



Policy creation will vary by ADOM version.

To insert a policy:

1. Select a policy.
2. From the *Create New* menu or the right-click menu, select *Insert Above*, *Insert Empty Above*, *Insert Below*, or *Insert Empty Below*. By default, new policies will be inserted at the bottom of the list.
   - *Insert Above* and *Insert Below* insert a copy of the selected policy.
   - *Insert Empty Above* and *Insert Empty Below* insert a new policy with all values set to empty or "none". Not all policy types support these options.



The name of the admin who creates the policy will be displayed in the *Created* field along with the timestamp.

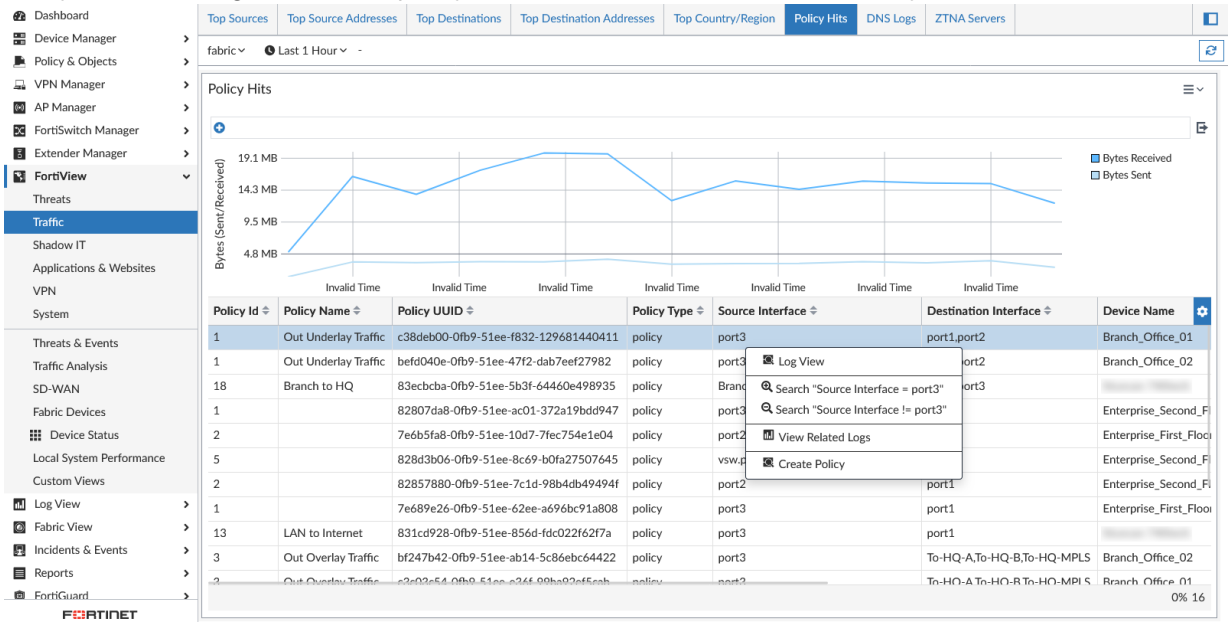
Creating policies based on logged traffic

When FortiManager has a managed FortiAnalyzer device, administrators can create new policies based on Policy Hit traffic in FortiView using the policy creation wizard. This feature is only available when FortiAnalyzer is added to FortiManager as a managed device; it is not supported on a FortiManager with FortiAnalyzer features enabled.

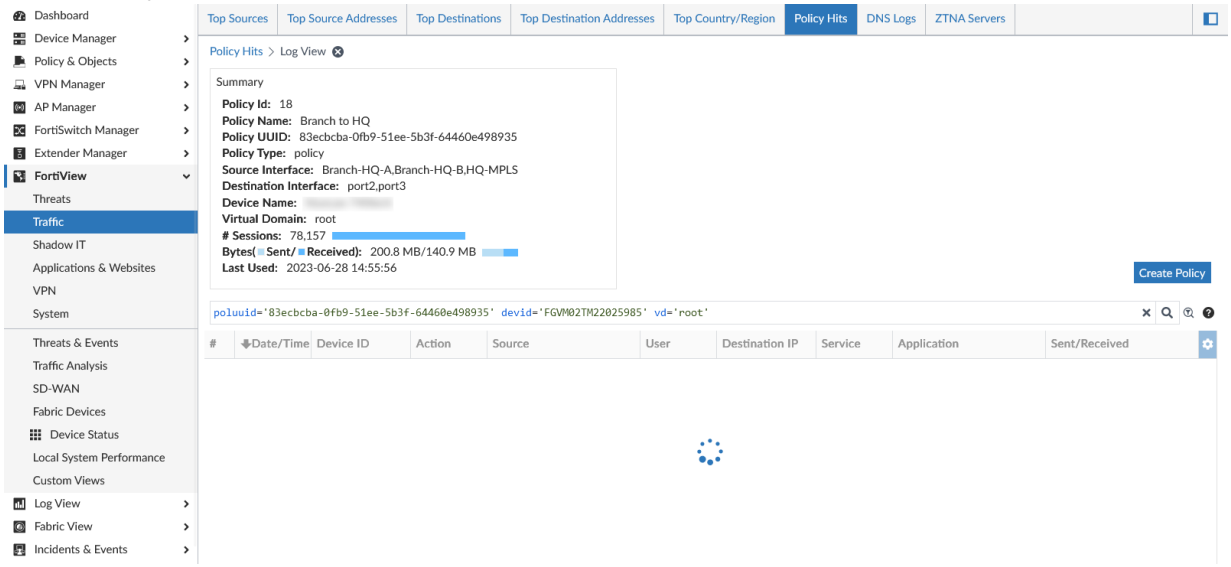
To create policies from policy hits:

1. Add a managed FortiAnalyzer to FortiManager. See Add FortiAnalyzer or FortiAnalyzer BigData on page 134
2. Go to *FortiView* > *Traffic* > *Policy Hits*.
3. Create a new policy from the *Policy Hits* table or from the *Log View* drilldown view, after which the policy creation wizard opens.

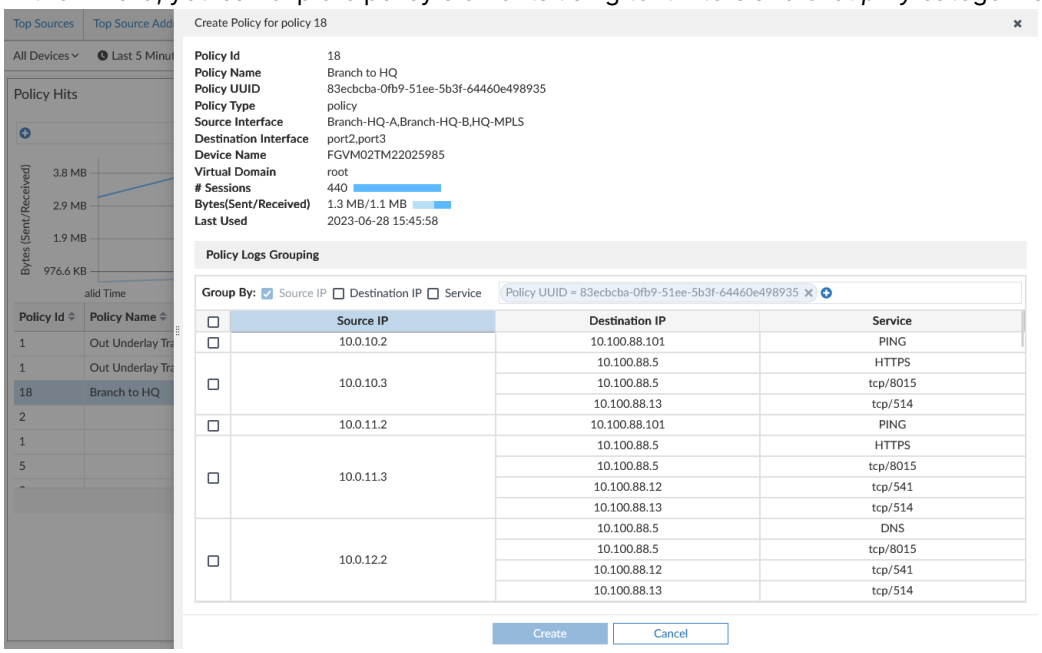
a. *Policy Hits table*: Right-click on a policy hit in the table, and click *Create Policy*.



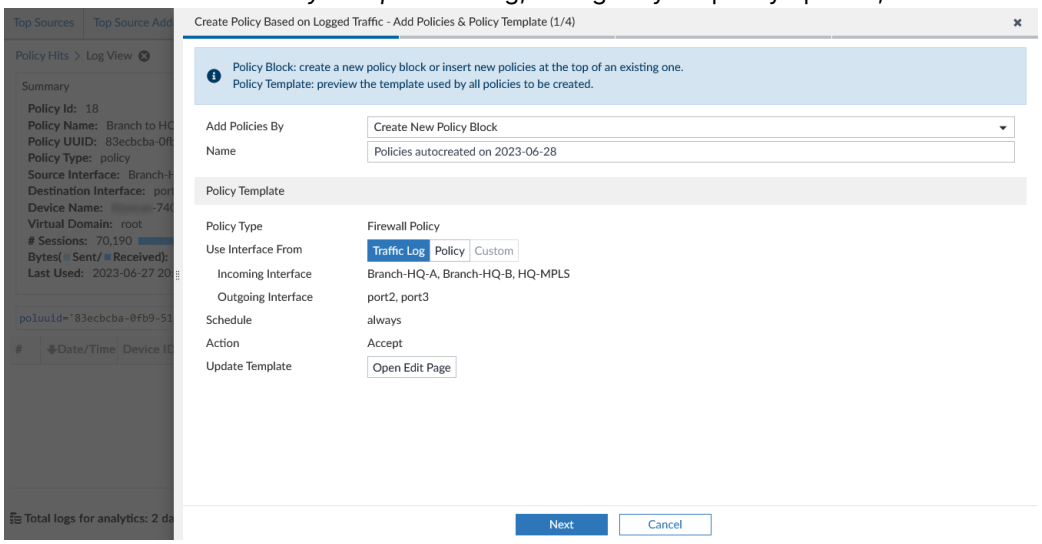
b. *Log View drilldown*: Double click on a log in the Policy Hits table to drilldown to Log View, and click *Create Policy*.



4. In the wizard, you can explore policy elements using text filters and *Group By* categorization.



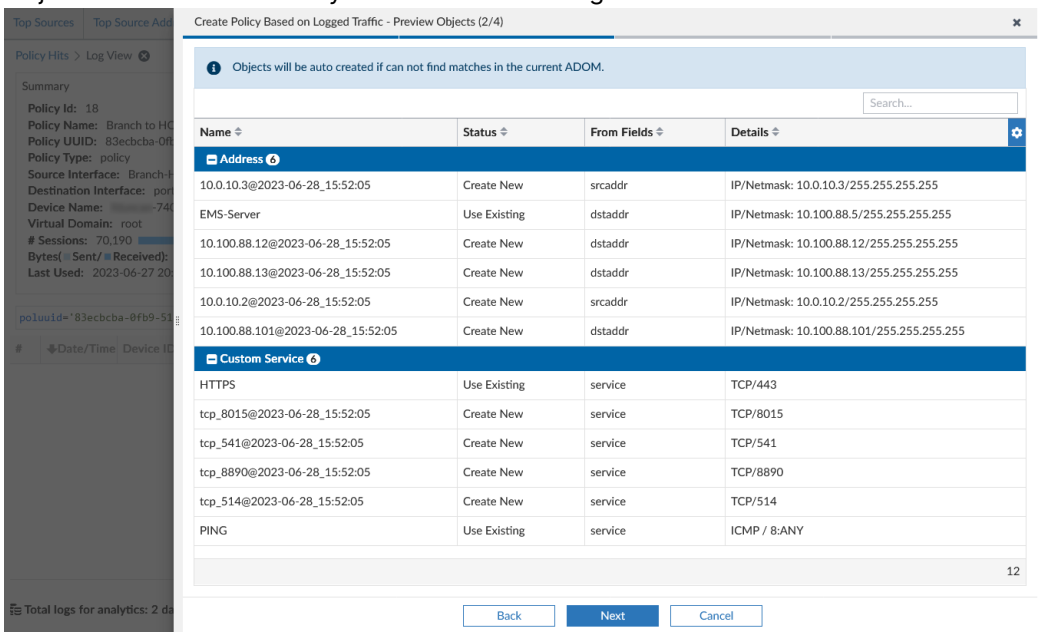
5. Select one or more entries in the log table, and click *Create*.
6. In the *Add Policies & Policy Template* dialog, configure your policy options, and then click *Next*:



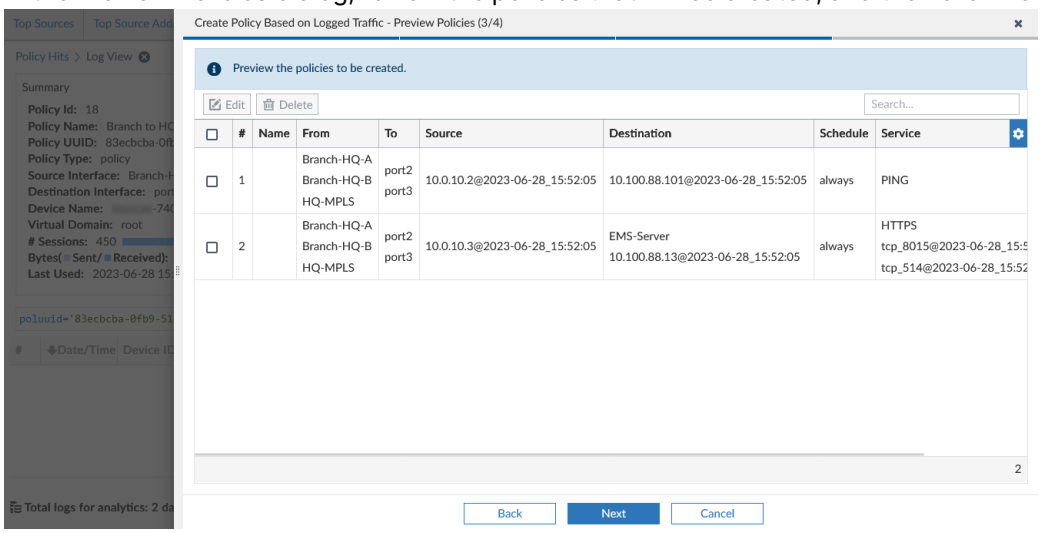
Add Policies By	Select one of the following options for adding the policy: • *Create New Policy Block*: Policies are added to a new Policy Block. When this option is selected, you must enter a name for the Policy Block or use the default name provided. • *Add to Existing Policy Block*: Policies are added to an existing Policy Block. Select the existing Policy Block from the *Policy Block* dropdown menu. • *Insert Before Package Policy*: Policies are inserted above the policy that it originated from.

Policy Block Visibility	The Policy Block feature must be enabled in *Policy & Objects > Feature Visibility* in order to manage Policy Blocks in the GUI. This field is displayed when the *Add Policies By* setting is configured to *Create New Policy Block* or *Add to Existing Policy Block*, and the Policy Block feature visibility is not enabled in the ADOM. Enable this setting to enable Policy Block feature visibility for the current ADOM. Disable this setting (default) to leave Policy Block visibility disabled.
Policy Type	Displays the type of policy that will be created.
Use Interface From	Select where the Incoming Interface and Outgoing Interface are from: • Traffic Log • Policy • Custom
Schedule	Displays the schedule.
Action	Displays the policy action.
Update Template	Manually update the policy template by clicking *Open Edit Page*.

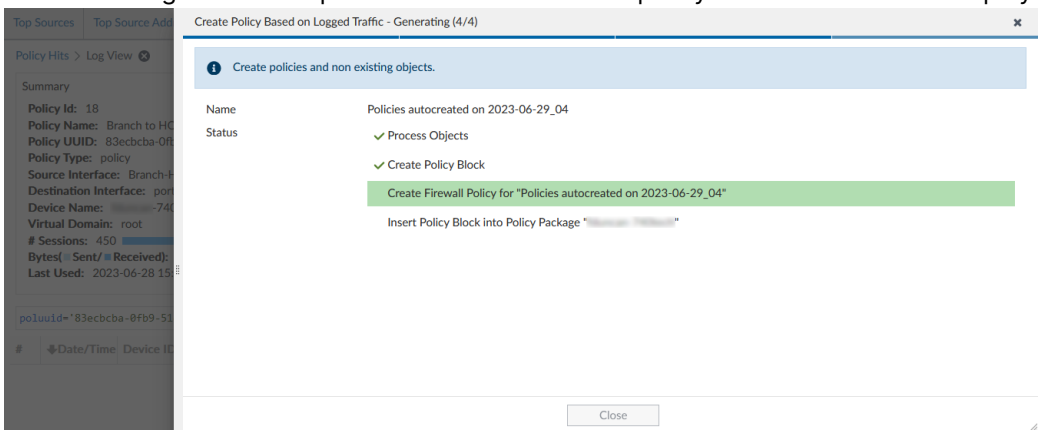
7. In the *Preview Objects* dialog, review the objects that will be used by the policy, and then click *Next*. Objects will be automatically created if FortiManager cannot find a match in the current ADOM.



8. In the *Preview Policies* dialog, review the policies that will be created, and then click *Next*.



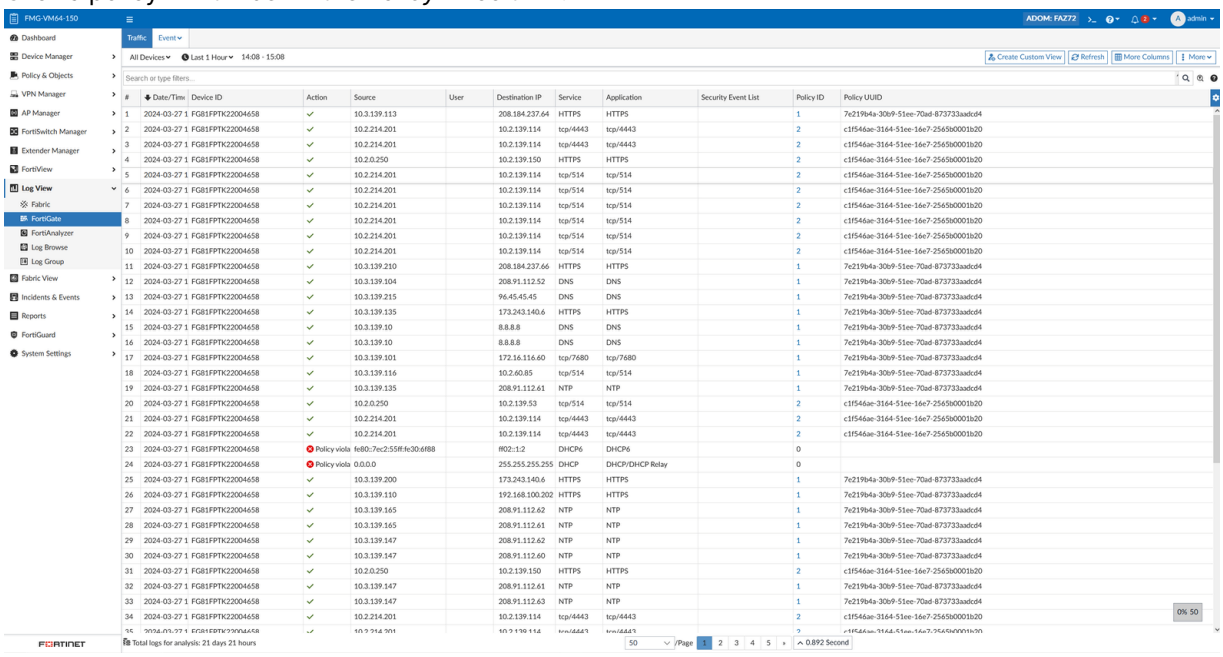
9. Click *Next* to generate the policies. The results of the policy creation wizard are displayed.



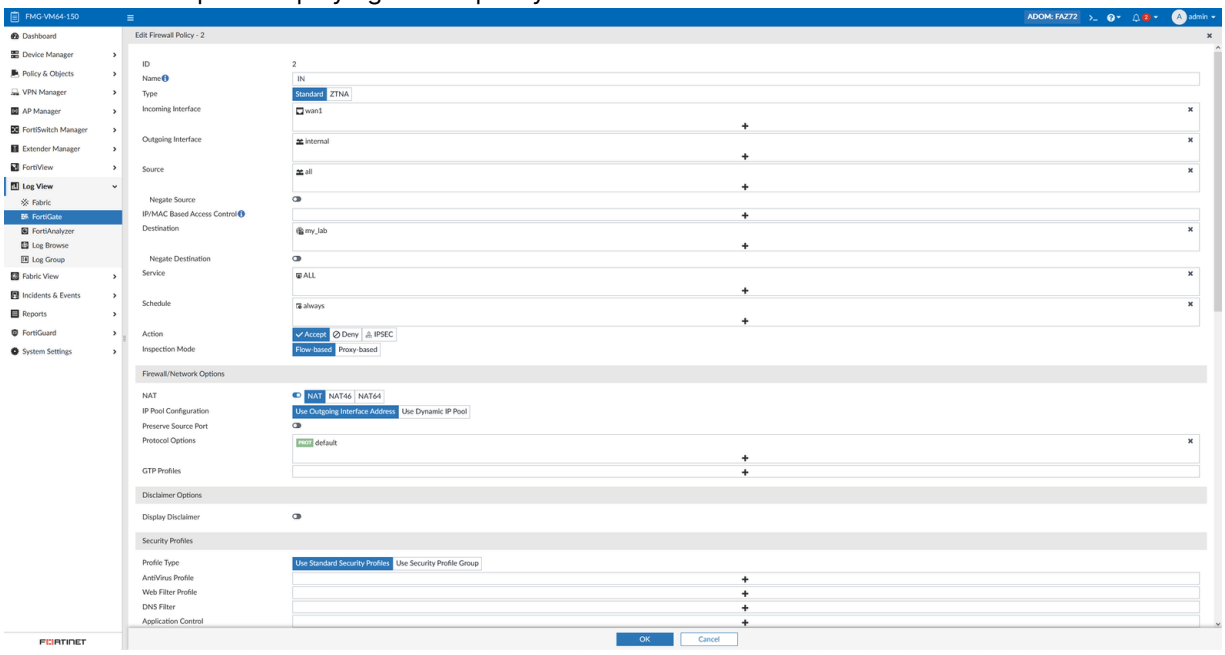
Once created, policies can be viewed in *Policy & Objects*.

To view policy details from Log View:

1. Go to *Log View*.
2. Click a policy ID number in the *Policy ID* column.

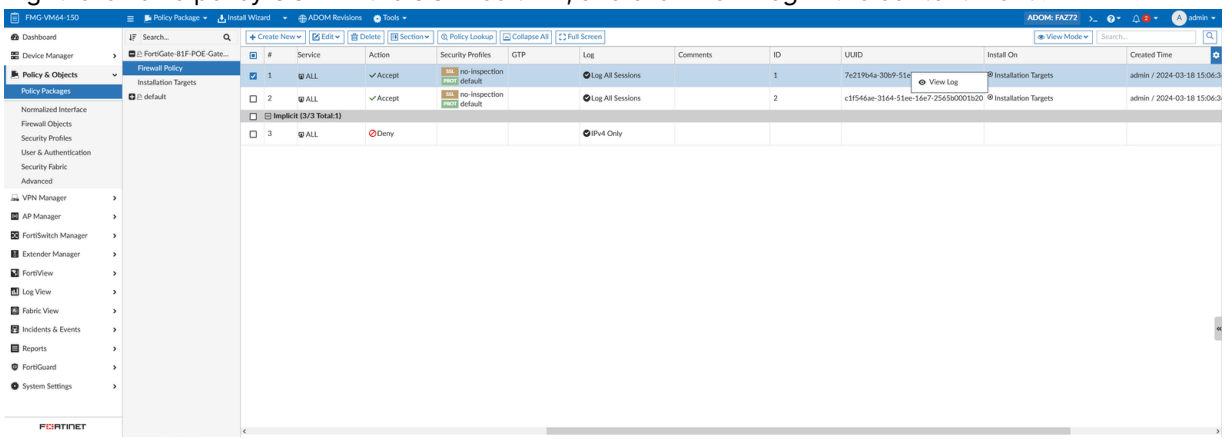


A new window opens displaying the full policy details.

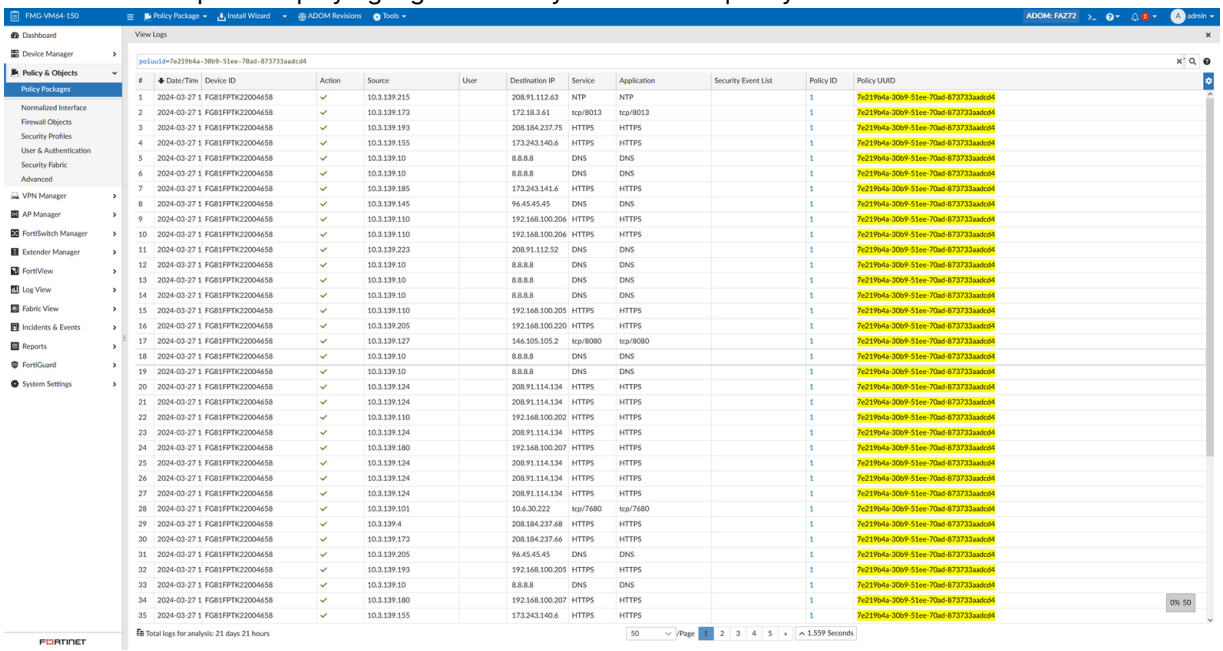


To view logs filtered by policy UUID:

1. Go to *Policy & Objects* > *Policy Packages*.
2. Right-click on a policy UUID in the *UUID* column, and click *View Log* in the context menu.



A new window opens displaying logs filtered by the selected policy UUID.



Create a new firewall policy

This section describes how to create a new firewall policy. The firewall policy is the axis around which most features of the FortiGate firewall revolve. Many settings in the firewall end up relating to or being associated with the firewall policies and the traffic that they govern. Any traffic going through a FortiGate unit has to be associated with a policy. These policies are essentially discrete compartmentalized sets of instructions that control the traffic flow going through the firewall. These instructions control where the traffic goes, how it is processed, if it is processed, and even whether or not it is allowed to pass through the FortiGate.

See Firewall policy in the FortiOS Administration Guide for more information.



The firewall policy option is visible only if the *NGFW Mode* is selected as *Profile-based* in the policy package.

To create a new firewall policy:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *Firewall Policy*.
4. Click *Create New*.
5. Enter the following information:

Option	Description
ID	Enter a unique number as the policy ID, or use the default (0) to automatically assign a policy ID. Policy IDs can be up to a maximum of 9 digits in length. Once a policy ID has been configured it cannot be changed.
Name	Enter a unique name for the policy. Each policy must have a unique name.
Incoming Interface	Click the field then select interfaces. Click the remove icon to remove interfaces. New objects can be created by clicking the *Create New* icon in the *Object Selector* frame. See Creating objects on page 533 for more information.
Outgoing Interface	Select outgoing interfaces in the same manner as *Incoming Interface*.
Source	Select the source address, address groups, virtual IPs, virtual IP groups, user, user groups, and FSSO groups.
IP/MAC Based Access Control	Use security posture tags to allow access based on the IP/MAC address of a device.
Destination	Select the destination address, address groups, virtual IPs, virtual IP groups, and services.
Service	Select services and service groups. This option is only available when *Destination Internet Service* is off.
Schedule	Select a one-time schedule, recurring schedule, or schedule group.
Action	Select an action for the policy to take: *DENY*, *ACCEPT*, or *IPSEC*.
Deny options	
Block Notification	Turn block notification display on or off.
Customize Messages	Select or create a message to be displayed when traffic is blocked by this policy. This option is only available when *Block Notification* is on.

Deny options	
Log Violation Traffic	Turn violation logging on or off. Select whether to generate logs when the session starts.

Accept options	
Inspection Mode	Select *Flow-based* or *Proxy-based* inspection.
Proxy HTTP(S) Traffic	Select whether to redirect HTTP(S) traffic to matching transparent web proxy policy. This option is only available when the inspection mode is set to *Proxy-based*.
NAT	Select to enable NAT. If enabled, select *NAT*, *NAT46*, or *NAT64*.
IP Pool Configuration	If *NAT* is selected, select *Use Outgoing Interface Address* or *Use Dynamic IP Pool*.
IPv4 Pool Name	If *NAT64* is selected or *NAT* and *Use Dynamic IP Pool* are selected, select or create an IPv4 pool.
IPv6 Pool Name	If *NAT46* is selected or *NAT* and *Use Dynamic IP Pool* are selected, select or create an IPv6 pool.
Preserve Source Port	If *NAT* is on, select whether to preserve the source port.
Protocol Options	Select a protocol options profile.
Display Disclaimer	Turn the disclaimer display on or off.
Customize Messages	Select or create a disclaimer message to be displayed when traffic is allowed by this policy. This option is only available when *Display Disclaimer* is on.
Security Profiles	Select whether to apply security profiles to this policy, then select the security profiles.
SSL/SSH Inspection	Select one of the following options for SSL/SSH Inspection: • certificate-inspection • custom-deep-inspection • deep-inspection • no-inspection
Shared Shaper	Select shared traffic shapers.
Reverse Shaper	Select reverse traffic shapers.
Per-IP Shaper	Select per IP traffic shapers.
Log Allowed Traffic	Select one of the following options: • *No Log* • *Log Security Events* • *Log All Sessions*

Accept options	
	If logging is on, select whether to capture packets. Select whether to generate logs when the session starts.

IPSEC options	
Protocol Options	Select a protocol options profile.
VPN Tunnel	Select or create a VPN tunnel dynamic object. Select whether to allow traffic to be initiated from the remote site.
Security Profiles	Select whether to apply security profiles to this policy, then select the security profiles.
SSL/SSH Inspection	Select one of the following options for SSL/SSH Inspection: • certificate-inspection • custom-deep-inspection • deep-inspection • no-inspection
Shared Shaper	Select shared traffic shapers.
Reverse Shaper	Select reverse traffic shapers.
Per-IP Shaper	Select per IP traffic shapers.
Log Allowed Traffic	Select one of the following options: • *No Log* • *Log Security Events* • *Log All Sessions* If logging is on, select whether to capture packets. Select whether to generate logs when the session starts.

Advanced	
WCCP	Turn Web Cache Communication Protocol (WCCP) web caching on or off.
Exempt from Captive Portal	Select whether this traffic is exempt from any captive portals.
Comments	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the *FortiOS CLI Reference*.

Revisions	
Change Note	Add a description of the changes being made to the policy. This field is required.

6. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

Advanced options

Option	Description	Default
anti-replay	Enable or disable anti-replay checking.	enable
auth-cert	Select the HTTPS server certificate for policy authentication.	none
auth-path	Enable or disable authentication-based routing.	disable
auth-redirect-addr	Select the HTTP-to-HTTPS redirect address for firewall authentication.	none
auto-asic-offload	Enable or disable policy traffic ASIC offloading.	enable
block-notification	Enable or disable block notification.	disable
cgn-eif	Enable or disable CGN endpoint independent filtering.	disable
cgn-eim	Enable or disable CGN endpoint independent mapping.	disable
cgn-log-server-grp	Select the NP log server group.	none
cgn-resource-quota	Set the allowed number of blocks assigned to a source IP address.	16
cgn-session-quota	Set the allowed concurrent sessions available for a source IP address.	16777215
custom-log-fields	Select custom fields to append to log messages for this policy.	none
delay-tcp-npu-session	Enable or disable TCP NPU session delay to guarantee packet order of 3-way handshake.	disable
diffserv-copy	Enable or disable copying of the DSCP values from the original direction to the reply direction.	disable
diffserv-forward	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic. If enabled, also configure `diffservcode-forward`.	disable
diffserv-reverse	Enable or disable application of the DSCP value to the DSCP field of reverse (reply) traffic. If enabled, also configure `diffservcode-rev`.	disable
diffservcode-forward	Enter the DSCP value that the FortiGate unit will apply to the field of originating (forward) packets. The value is 6 bits binary. The valid range is 000000-111111.	000000
diffservcode-rev	Enter the DSCP value that the FortiGate unit will apply to the field of reply (reverse) packets. The value is 6 bits binary. The valid range is 000000-111111.	000000

Option	Description	Default
dlp-profile	Select an existing data loss prevention (DLP) profile.	none
dsri	Enable to ignore HTTP server responses.	disable
dstaddr-negate	Enable to negate the destination IP address.	disable
dstaddr6-negate	Enable to negate the destination IPv6 address.	disable
dynamic-shaping	Enable or disable dynamic RADIUS-defined traffic shaping.	disable
email-collect	Enable or disable email collection.	disable
fec	Enable or disable forward error correction (FEC) on traffic matching this policy on a FEC device.	disable
firewall-session-dirty	Select how to handle sessions if the configuration of this firewall policy changes.	check-all
ffsso-agent-for-ntlm	Select the FSSO agent for NTLM authentication.	none
geoip-anycast	Enable or disable recognition of anycast IP addresses using the geography IP database.	disable
geoip-match	Select whether to match the address based on the physical or registered location.	physical-location
identity-based-route	Select the identity-based routing rule.	none
internet-service-negate	Enable to negate the internet service set in the policy.	disable
internet-service-src-negate	Enable to negate the source internet service set in this policy.	disable
internet-service6	Enable or disable the use of IPv6 internet services for this policy. If enabled, the destination address and service set in the policy are not used.	disable
internet-service6-custom	Select a custom IPv6 internet service.	none
internet-service6-custom-group	Select a custom IPv6 internet service group.	none
internet-service6-group	Select an IPv6 internet service group.	none
internet-service6-name	Select an IPv6 internet service.	none
internet-service6-negate	Enable to negate the source IPv6 internet service set in this policy.	disable
internet-service6-src	Enable or disable use of the IPv6 internet services in the source for this policy. If enabled, the source address is not used.	disable

Option	Description	Default
internet-service6-src-custom	Select the custom IPv6 internet service source.	none
internet-service6-src-custom-group	Select the custom IPv6 source group.	none
internet-service6-src-group	Select the IPv6 source group.	none
internet-service6-src-name	Select the IPv6 source.	none
internet-service6-src-negate	Enable to negate the value set in `internet-service6-src`.	disable
match-vip	Enable or disable matching of packets that have had their destination address changed by a VIP.	disable
match-vip-only	Enable or disable matching only those packets that have had their destination addresses change by a VIP.	disable
natinbound	Enable or disable applying destination NAT to inbound traffic.	disable
natip	Set the source NAT IP address for inbound traffic.	0.0.0.0/0.0.0.0
natoutbound	Enable or disable applying destination NAT to outbound traffic.	disable
network-service-dynamic	Select a dynamic network service.	none
network-service-src-dynamic	Select a dynamic network service source.	none
np-acceleration	Enable or disable UTM network processor acceleration.	disable
ntlm	Enable or disable NTLM authentication.	disable
ntlm-enabled-browsers	Set the HTTP-User-Agent value of supported browsers.	none
ntlm-guest	Enable or disable NTLM guest user access.	disable
outbound	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic.	disable
passive-wan-health-measurement	Enable or disable passive WAN health measurement. When enabled, `auto-asic-offload` is disabled.	disable.
permit-any-host	Enable or disable accepting UDP packets from any host.	disable
permit-stun-host	Enable or disable accepting UDP packets from any session traversal utilities for NAT (STUN) host.	disable
policy-expiry	Enable or disable policy expiry.	disable
policy-expiry-date	If policy-expiry is enabled, set the policy expiry date.	0000-00-

Option	Description	Default
		00,00:00:00
policy-offload	Enable or disable hardware session setup for CGNAT.	disable
radius-mac-auth-bypass	Enable or disable MAC authentication bypass. The bypassed MAC address must be received from the RADIUS server.	disable
redirect-url	Set the URL to which users are redirected after seeing and accepting the disclaimer or authenticating.	none
reputation-direction	Set the destination of the initial traffic for reputation to take effect.	destination
reputation-direction6	Set the destination of the initial traffic for IPv6 reputation to take effect.	destination
reputation-minimum	Set the minimum reputation to take action.	0
reputation-minimum6	Set the minimum IPv6 reputation to take action.	0
rtp-addr	If this is an RTP NAT policy, set the address names.	none
rtp-nat	Enable or disable real time protocol (RTP) NAT.	disable
schedule-timeout	Enable or disable ending current sessions when the schedule object times out. Disable allows sessions to end from inactivity.	disable
sctp-filter-profile	Select an existing SCTP filter profile.	none
send-deny-packet	Enable or disable sending a reply when a session is denied or blocked by a firewall policy.	disable
service-negate	Enable or disable negation of the service set in the policy.	disable
session-ttl	Enter a value for the session time-to-live (TTL) from 300 to 604800, or type 0 for no limitation.	0
sgt	Enter security group tags (SGT).	none
sgt-check	Enable or disable SGT check.	disable
src-vendor-mac	Select the vendor MAC source.	none
srcaddr-negate	Enable or disable negation of the source address.	disable
srcaddr6-negate	Enable or disable negation of the source IPv6 address.	disable
ssh-filter-profile	Select an SSH filter profile from the drop-down list.	None
ssh-policy-redirect	Enable or disable SSH policy redirect.	disable
tcp-mss-receiver	Enter the receiver's TCP maximum segment size (MSS).	0
tcp-mss-sender	Enter the sender's TCP MSS.	0

Option	Description	Default
tcp-session-without-syn	Enable or disable creation of a TCP session without the SYN flag.	disable
tcp-timeout-pid	Select the TCP timeout profile.	none
timeout-send-rst	Enable or disable the sending of RST packets when TCP sessions expire	disable
tos	Enter the type of service (TOS) value used for comparison.	0
tos-mask	Enter the bit mask for TOS. Non-zero bit positions are used for comparison while zero bit positions are ignored.	0
tos-negate	Enable or disable to negate the TOS match.	disable
udp-timeout-pid	Select the UDP timeout profile.	none
uuid	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000
vlan-cos-fwd	Select the VLAN forward direction user priority. The available values are: • 255 (passthrough) • 0 (lowest) - 7 (highest)	255
vlan-cos-rev	Select the VLAN reverse direction user priority. The available values are: • 255 (passthrough) • 0 (lowest) - 7 (highest)	255
vlan-filter	Set VLAN filters.	none
wanopt	Enable or disable WAN optimization (IPv4 only).	disable
wanopt-detection	Select the WAN optimization as active, passive, or off.	active
wanopt-passive-opt	Select WAN optimization passive mode options. This option decides what IP address will be used to connect server (IPv4 only).	default
wanopt-peer	Select a WAN optimization peer (IPv4 only).	none
wanopt-profile	Select a WAN optimization profile (IPv4 only).	none
webcache	Enable or disable web cache (IPv4 only).	disable
webcache-https	Enable or disable the web cache for HTTPS (IPv4 only).	none
webproxy-forward-server	Select the webproxy forward server (IPv4 only).	none
webproxy-profile	Select the webproxy profile (IPv4 only).	none

Create a new SSL inspection and authentication policy

This section describes how to create a new SSL inspection and authentication policy. This policy type is essentially a firewall policy for policy-based policy packages.

See NGFW policy in the FortiOS Administration Guide for more information.



The *SSL Inspection & Authentication* policy option is visible only if the *NGFW Mode* is selected as *Policy-based* in the policy package.

To create a new SSL inspection and authentication policy:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *SSL Inspection & Authentication*.
4. Click *Create New*.
5. Enter the following information:

Option	Description
ID	Enter a unique number as the policy ID, or use the default (0) to automatically assign a policy ID. Policy IDs can be up to a maximum of 9 digits in length. Once a policy ID has been configured it cannot be changed.
Name	Enter a unique name for the policy. Each policy must have a unique name.
Incoming Interface	Click the field then select interfaces. Click the remove icon to remove interfaces. New objects can be created by clicking the *Create New* icon in the *Object Selector* frame. See Creating objects on page 533 for more information.
Outgoing Interface	Select outgoing interfaces in the same manner as *Incoming Interface*.
Source	Select the source address, address groups, virtual IPs, virtual IP groups, user, user groups, and FSSO groups.
Enforce ZTNA	Enable or disable ZTNA.
EMS Tag	Select the FortiClient EMS tag to match. This option is only available if Enforce ZTNA is enabled.
Geographic IP Tag	Select the Geographic IP tag to match. This option is only available if Enforce ZTNA is enabled.
Destination	Select the destination address, address groups, virtual IPs, virtual IP groups, and services.

Option	Description
Service	Select services and service groups. This option is only available when *Destination Internet Service* is off.
SSL/SSH Inspection	Select one of the following options for SSL/SSH Inspection:certificate-inspectioncustom-deep-inspectiondeep-inspectionno-inspection
Comments	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the *FortiOS CLI Reference*.
Change Note	Add a description of the changes being made to the policy. This field is required.

6. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

Advanced options

Option	Description	Default
anti-replay	Enable or disable anti-replay checking.	enable
auth-cert	Select the HTTPS server certificate for policy authentication.	none
auth-path	Enable or disable authentication-based routing.	disable
auth-redirect-addr	Select the HTTP-to-HTTPS redirect address for firewall authentication.	none
auto-asic-offload	Enable or disable policy traffic ASIC offloading.	enable
block-notification	Enable or disable block notification.	disable
cgn-eif	Enable or disable CGN endpoint independent filtering.	disable
cgn-eim	Enable or disable CGN endpoint independent mapping.	disable
cgn-log-server-grp	Select the NP log server group.	none
cgn-resource-quota	Set the allowed number of blocks assigned to a source IP address.	16
cgn-session-quota	Set the allowed concurrent sessions available for a source IP address.	16777215
custom-log-fields	Select custom fields to append to log messages for this policy.	none
delay-tcp-npu-session	Enable or disable TCP NPU session delay to guarantee packet order of 3-way handshake.	disable

Option	Description	Default
diffserv-copy	Enable or disable copying of the DSCP values from the original direction to the reply direction.	disable
diffserv-forward	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic. If enabled, also configure `diffservcode-forward`.	disable
diffserv-reverse	Enable or disable application of the DSCP value to the DSCP field of reverse (reply) traffic. If enabled, also configure `diffservcode-rev`.	disable
diffservcode-forward	Enter the DSCP value that the FortiGate unit will apply to the field of originating (forward) packets. The value is 6 bits binary. The valid range is 000000-111111.	000000
diffservcode-rev	Enter the DSCP value that the FortiGate unit will apply to the field of reply (reverse) packets. The value is 6 bits binary. The valid range is 000000-111111.	000000
dlp-profile	Select an existing data loss prevention (DLP) profile.	none
dsri	Enable to ignore HTTP server responses.	disable
dstaddr-negate	Enable to negate the destination IP address.	disable
dstaddr6-negate	Enable to negate the destination IPv6 address.	disable
dynamic-shaping	Enable or disable dynamic RADIUS-defined traffic shaping.	disable
email-collect	Enable or disable email collection.	disable
fec	Enable or disable forward error correction (FEC) on traffic matching this policy on a FEC device.	disable
firewall-session-dirty	Select how to handle sessions if the configuration of this firewall policy changes.	check-all
ffsso-agent-for-ntlm	Select the FSSO agent for NTLM authentication.	none
geoip-anycast	Enable or disable recognition of anycast IP addresses using the geography IP database.	disable
geoip-match	Select whether to match the address based on the physical or registered location.	physical-location
identity-based-route	Select the identity-based routing rule.	none
internet-service-negate	Enable to negate the internet service set in the policy.	disable
internet-service-src-negate	Enable to negate the source internet service set in this policy.	disable

Option	Description	Default
internet-service6	Enable or disable the use of IPv6 internet services for this policy. If enabled, the destination address and service set in the policy are not used.	disable
internet-service6-custom	Select a custom IPv6 internet service.	none
internet-service6-custom-group	Select a custom IPv6 internet service group.	none
internet-service6-group	Select an IPv6 internet service group.	none
internet-service6-name	Select an IPv6 internet service.	none
internet-service6-negate	Enable to negate the source IPv6 internet service set in this policy.	disable
internet-service6-src	Enable or disable use of the IPv6 internet services in the source for this policy. If enabled, the source address is not used.	disable
internet-service6-src-custom	Select the custom IPv6 internet service source.	none
internet-service6-src-custom-group	Select the custom IPv6 source group.	none
internet-service6-src-group	Select the IPv6 source group.	none
internet-service6-src-name	Select the IPv6 source.	none
internet-service6-src-negate	Enable to negate the value set in `internet-service6-src`.	disable
match-vip	Enable or disable matching of packets that have had their destination address changed by a VIP.	disable
match-vip-only	Enable or disable matching only those packets that have had their destination addresses change by a VIP.	disable
natinbound	Enable or disable applying destination NAT to inbound traffic.	disable
natip	Set the source NAT IP address for inbound traffic.	0.0.0.0/0.0.0.0
natoutbound	Enable or disable applying destination NAT to outbound traffic.	disable
network-service-dynamic	Select a dynamic network service.	none
network-service-src-dynamic	Select a dynamic network service source.	none

Option	Description	Default
np-acceleration	Enable or disable UTM network processor acceleration.	disable
ntlm	Enable or disable NTLM authentication.	disable
ntlm-enabled-browsers	Set the HTTP-User-Agent value of supported browsers.	none
ntlm-guest	Enable or disable NTLM guest user access.	disable
outbound	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic.	disable
passive-wan-health-measurement	Enable or disable passive WAN health measurement. When enabled, `auto-asic-offload` is disabled.	disable.
permit-any-host	Enable or disable accepting UDP packets from any host.	disable
permit-stun-host	Enable or disable accepting UDP packets from any session traversal utilities for NAT (STUN) host.	disable
policy-expiry	Enable or disable policy expiry.	disable
policy-expiry-date	If policy-expiry is enabled, set the policy expiry date.	0000-00-00,00:00:00
policy-offload	Enable or disable hardware session setup for CGNAT.	disable
radius-mac-auth-bypass	Enable or disable MAC authentication bypass. The bypassed MAC address must be received from the RADIUS server.	disable
redirect-url	Set the URL to which users are redirected after seeing and accepting the disclaimer or authenticating.	none
reputation-direction	Set the destination of the initial traffic for reputation to take effect.	destination
reputation-direction6	Set the destination of the initial traffic for IPv6 reputation to take effect.	destination
reputation-minimum	Set the minimum reputation to take action.	0
reputation-minimum6	Set the minimum IPv6 reputation to take action.	0
rtp-addr	If this is an RTP NAT policy, set the address names.	none
rtp-nat	Enable or disable real time protocol (RTP) NAT.	disable
schedule-timeout	Enable or disable ending current sessions when the schedule object times out. Disable allows sessions to end from inactivity.	disable
sctp-filter-profile	Select an existing SCTP filter profile.	none
send-deny-packet	Enable or disable sending a reply when a session is denied or blocked by a firewall policy.	disable

Option	Description	Default
service-negate	Enable or disable negation of the service set in the policy.	disable
session-ttl	Enter a value for the session time-to-live (TTL) from 300 to 604800, or type 0 for no limitation.	0
sgt	Enter security group tags (SGT).	none
sgt-check	Enable or disable SGT check.	disable
src-vendor-mac	Select the vendor MAC source.	none
srcaddr-negate	Enable or disable negation of the source address.	disable
srcaddr6-negate	Enable or disable negation of the source IPv6 address.	disable
ssh-filter-profile	Select an SSH filter profile from the drop-down list.	None
ssh-policy-redirect	Enable or disable SSH policy redirect.	disable
tcp-mss-receiver	Enter the receiver's TCP maximum segment size (MSS).	0
tcp-mss-sender	Enter the sender's TCP MSS.	0
tcp-session-without-syn	Enable or disable creation of a TCP session without the SYN flag.	disable
tcp-timeout-pid	Select the TCP timeout profile.	none
timeout-send-rst	Enable or disable the sending of RST packets when TCP sessions expire	disable
tos	Enter the type of service (TOS) value used for comparison.	0
tos-mask	Enter the bit mask for TOS. Non-zero bit positions are used for comparison while zero bit positions are ignored.	0
tos-negate	Enable or disable to negate the TOS match.	disable
udp-timeout-pid	Select the UDP timeout profile.	none
uuid	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000
vlan-cos-fwd	Select the VLAN forward direction user priority. The available values are: • 255 (passthrough) • 0 (lowest) - 7 (highest)	255
vlan-cos-rev	Select the VLAN reverse direction user priority. The available values are: • 255 (passthrough) • 0 (lowest) - 7 (highest)	255
vlan-filter	Set VLAN filters.	none

Option	Description	Default
wanopt	Enable or disable WAN optimization (IPv4 only).	disable
wanopt-detection	Select the WAN optimization as active, passive, or off.	active
wanopt-passive-opt	Select WAN optimization passive mode options. This option decides what IP address will be used to connect server (IPv4 only).	default
wanopt-peer	Select a WAN optimization peer (IPv4 only).	none
wanopt-profile	Select a WAN optimization profile (IPv4 only).	none
webcache	Enable or disable web cache (IPv4 only).	disable
webcache-https	Enable or disable the web cache for HTTPS (IPv4 only).	none
webproxy-forward-server	Select the webproxy forward server (IPv4 only).	none
webproxy-profile	Select the webproxy profile (IPv4 only).	none

Create a new security policy

This section describes how to create a new security policy. A security policy consists of rules related to proxy, antivirus, IPS, email, and DLP sensor.

See NGFW policy in the FortiOS Administration Guide for more information.



The security policy option is visible only if the *NGFW Mode* is selected as *Policy-based* in the policy package.



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.

To create a new security policy:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *Security Policy*.
4. Click *Create New*.
5. Enter the following information:

ID	Enter a unique number as the policy ID, or use the default (0) to automatically assign a policy ID. Policy IDs can be up to a maximum of 9 digits in length. Once a policy ID has been configured it cannot be changed.

Name	Enter a unique name for the policy. Each policy must have a unique name.
Policy Mode	Select the mode for this policy: *Standard* or *Learn Mode*. Learn mode allows and logs all traffic between the specified interfaces. Use learn mode with FortiAnalyzer to understand traffic patterns and design policy changes. See *Learn mode in security policies in NGFW mode* in the FortiOS Administration Guide for more information.
Incoming Interface	Click the field then select interfaces. Click the remove icon to remove interfaces. New interfaces can be created by clicking the *Create New* icon in the *Interfaces* frame. See Creating objects on page 533 for more information.
Outgoing Interface	Select outgoing interfaces in the same manner as the incoming interfaces.
Source	Select the source address, address groups, virtual IPs, virtual IP groups, user, user groups, and FSSO groups.
Destination	Select the destination address, address groups, virtual IPs, virtual IP groups, and services.
Schedule	Select a one-time schedule, recurring schedule, or schedule group.
Service	Select the service. Select *App Default* or *Specify*. If *Specify* is selected, select the Service.
Application	Select applications.
URL Category	Select URL categories.
Action	Select an action for the policy to take: *DENY* or *ACCEPT*.
Log Traffic	When the *Action* is *DENY*, select *Log Violation Traffic* to log violation traffic. When the *Action* is *ACCEPT*, select one of the following options: • *No Log* • *Log Security Events* • *Log All Sessions* Select whether to generate logs when the session starts.
Protocol Options	Select protocol options profiles for handling protocol-specific traffic. This option is available when the *Action* is *ACCEPT*.
Security Profiles	Select to add security profiles or profile groups. This option is available when the *Action* is *ACCEPT*. If *Use Standard Security Profiles* is selected, the following standard security profile types can be added: • AntiVirus Profile • Web Filter Profile • IPS Profile

	• Email Filter • File Filter Profile If *Use Security Profile Group* is selected, select the *Profile Group*.
Comments	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the *FortiOS CLI Reference*.
Change Note	Add a description of the changes being made to the policy. This field is required.

6. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

Advanced options

Option	Description	Default
application-list	Select ...an existing application list.	none
comments	Add a description of the policy, such as its purpose, or the changes that have been made to it. A comment added here will overwrite the comment added in the above *Comments* field.	none
dlp-profile	Select an existing data loss prevention (DLP) profile.	none
dnsfilter-profile	Select an existing DNS filter profile.	none
dstaddr-negate	Enable to negate the values set in *IPv4 Destination Address* and *IPv6 Destination Address*.	disable
global-label	Set the label for the policy to be displayed when the GUI is in *Global View* mode.	none
icap-profile	Select an existing Internet Content Adaptation Protocol (ICAP) profile.	none
internet-service-negate	When enabled, Internet services match against any Internet service except the selected Internet service.	disable
internet-service-src-negate	Enables or disables the use of Internet Services in source for this policy. If enabled, `internet-service-src` specifies what the service must NOT be.	disable
internet-service6	Enable or disable the use of IPv6 internet services for this policy. If enabled, the destination address and service set in the policy are not used.	disable
internet-service6-custom	Select a custom IPv6 internet service.	none

Option	Description	Default
internet-service6-custom-group	Select a custom IPv6 internet service group.	none
internet-service6-group	Select an IPv6 internet service group.	none
internet-service6-name	Select an IPv6 internet service.	none
internet-service6-negate	Enable to negate the source IPv6 internet service set in this policy.	disable
internet-service6-src	Enable or disable use of the IPv6 internet services in the source for this policy. If enabled, the source address is not used.	disable
internet-service6-src-custom	Select the custom IPv6 internet service source.	none
internet-service6-src-custom-group	Select the custom IPv6 source group.	none
internet-service6-src-group	Select the IPv6 source group.	none
internet-service6-src-name	Select the IPv6 source.	none
internet-service6-src-negate	Enable to negate the value set in `internet-service6-src`.	disable
nat46	Enable or disable NAT46.	disable
nat64	Enable or disable NAT64.	disable
sctp-filter-profile	Select an existing stream control transmission protocol (SCTP) filter profile.	none
send-deny-packet	Enable or disable sending a reply packet when a session is denied or blocked by this policy.	disable
service-negate	Enable or disable negation of the selected *Service*.	disable
srcaddr-negate	Enable or disable negation of the *IPv4 Source Address* or *IPv6 Source Address* address.	disable
ssh-filter-profile	Select an existing SSH filter profile.	none
ssl-ssh-profile	Select an existing SSL SSH profile.	no-inspection
utm-status	Enable or disable the Unified Threat Management status.	disable
uuid	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000
voip-profile	Select an existing VOIP profile.	None

Create a new firewall virtual wire pair policy

This section describes how to create virtual wire pair policies. Before you can create a policy, you must create a virtual wire pair. See Configuring virtual wire pairs on page 741.

You can create a firewall virtual wire pair policy in a policy package that is set to *Profile-based*. If the policy package is set to *Policy-based*, see Create a new security virtual wire pair policy on page 467.

See Virtual wire pair in the FortiOS Administration Guide for more information about virtual wire pairs and virtual wire pair policies.



The security virtual wire pair policy is visible only if the *NGFW Mode* is selected as *Policy-based* in the policy package.



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.

To create a new firewall virtual wire pair policy:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *Firewall Virtual Wire Pair Policy*.
4. Click *Create New*.
5. Enter the following information:

Option	Description
ID	Enter a unique number as the policy ID, or use the default (0) to automatically assign a policy ID. Policy IDs can be up to a maximum of 9 digits in length. Once a policy ID has been configured it cannot be changed.
Name	Enter a unique name for the policy. Each policy must have a unique name.
IP/MAC Based Access Control	Use security posture tags to allow access based on the IP/MAC address of a device.
Virtual Wire Pair Interface	Select one or more virtual wire pair interfaces. This field is required. New objects can be created by clicking the *Create New* icon in the *Object Selector* frame. See Creating objects on page 533 for more information.
Virtual Wire Pair	Select an arrow to indicate the flow of traffic between the ports in the selected *Virtual Wire Pair Interface*.

Option	Description
Source	Select the source address, address groups, virtual IPs, virtual IP groups, user, user groups, and FSSO groups.
Destination	Select the destination address, address groups, virtual IPs, virtual IP groups, and services.
Service	Select services and service groups. This option is only available when *Destination Internet Service* is off.
Schedule	Select a one-time schedule, recurring schedule, or schedule group.
Action	Select an action for the policy to take: *DENY* or *ACCEPT*.
Deny options	
Block Notification	Turn block notification display on or off.
Log Violation Traffic	Turn violation logging on or off. Select whether to generate logs when the session starts.
Accept options	
NAT	Select to enable NAT. If enabled, select *NAT*, *NAT46*, or *NAT64*.
IP Pool Configuration	If *NAT* is selected, select *Use Outgoing Interface Address* or *Use Dynamic IP Pool*. *Use Outgoing Interface Address* is disabled in a firewall virtual pair policy.
IPv4 Pool Name	If *NAT64* is selected or *NAT* and *Use Dynamic IP Pool* are selected, select or create an IPv4 pool.
IPv6 Pool Name	If *NAT46* is selected or *NAT* and *Use Dynamic IP Pool* are selected, select or create an IPv6 pool.
Preserve Source Port	If *NAT* is on, select whether to preserve the source port.
Protocol Options	Select a protocol options profile.
Display Disclaimer	Turn the disclaimer display on or off.
SSL/SSH Inspection	Select one of the following options for SSL/SSH Inspection:certificate-inspectioncustom-deep-inspectiondeep-inspectionno-inspection
Shared Shaper	Select shared traffic shapers.
Reverse Shaper	Select reverse traffic shapers.
Per-IP Shaper	Select per IP traffic shapers.
Log Allowed Traffic	Select one of the following options:*No Log**Log Security Events**Log All Sessions*If logging is on, select whether to capture packets.Select whether to generate logs when the session starts.

Advanced	
WCCP	Turn Web Cache Communication Protocol (WCCP) web caching on or off.
Exempt from Captive Portal	Select whether this traffic is exempt from any captive portals.
Comments	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the *FortiOS CLI Reference*.

Revision	
Change Note	Add a description of the changes being made to the policy. This field is required.

6. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

Advanced options

Option	Description	Default
anti-replay	Enable or disable anti-replay checking.	enable
auth-cert	Select the HTTPS server certificate for policy authentication.	none
auth-path	Enable or disable authentication-based routing.	disable
auth-redirect-addr	Select the HTTP-to-HTTPS redirect address for firewall authentication.	none
auto-asic-offload	Enable or disable policy traffic ASIC offloading.	enable
block-notification	Enable or disable block notification.	disable
cgn-eif	Enable or disable CGN endpoint independent filtering.	disable
cgn-eim	Enable or disable CGN endpoint independent mapping.	disable
cgn-log-server-grp	Select the NP log server group.	none
cgn-resource-quota	Set the allowed number of blocks assigned to a source IP address.	16
cgn-session-quota	Set the allowed concurrent sessions available for a source IP address.	16777215
custom-log-fields	Select custom fields to append to log messages for this policy.	none
delay-tcp-npu-session	Enable or disable TCP NPU session delay to guarantee packet order of 3-way handshake.	disable

Option	Description	Default
diffserv-copy	Enable or disable copying of the DSCP values from the original direction to the reply direction.	disable
diffserv-forward	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic. If enabled, also configure `diffservcode-forward`.	disable
diffserv-reverse	Enable or disable application of the DSCP value to the DSCP field of reverse (reply) traffic. If enabled, also configure `diffservcode-rev`.	disable
diffservcode-forward	Enter the DSCP value that the FortiGate unit will apply to the field of originating (forward) packets. The value is 6 bits binary. The valid range is 000000-111111.	000000
diffservcode-rev	Enter the DSCP value that the FortiGate unit will apply to the field of reply (reverse) packets. The value is 6 bits binary. The valid range is 000000-111111.	000000
dlp-profile	Select an existing data loss prevention (DLP) profile.	none
dsri	Enable to ignore HTTP server responses.	disable
dstaddr-negate	Enable to negate the destination IP address.	disable
dstaddr6-negate	Enable to negate the destination IPv6 address.	disable
dynamic-shaping	Enable or disable dynamic RADIUS-defined traffic shaping.	disable
email-collect	Enable or disable email collection.	disable
fec	Enable or disable forward error correction (FEC) on traffic matching this policy on a FEC device.	disable
firewall-session-dirty	Select how to handle sessions if the configuration of this firewall policy changes.	check-all
ffsso-agent-for-ntlm	Select the FSSO agent for NTLM authentication.	none
geoip-anycast	Enable or disable recognition of anycast IP addresses using the geography IP database.	disable
geoip-match	Select whether to match the address based on the physical or registered location.	physical-location
identity-based-route	Select the identity-based routing rule.	none
internet-service-negate	Enable to negate the internet service set in the policy.	disable
internet-service-src-negate	Enable to negate the source internet service set in this policy.	disable

Option	Description	Default
internet-service6	Enable or disable the use of IPv6 internet services for this policy. If enabled, the destination address and service set in the policy are not used.	disable
internet-service6-custom	Select a custom IPv6 internet service.	none
internet-service6-custom-group	Select a custom IPv6 internet service group.	none
internet-service6-group	Select an IPv6 internet service group.	none
internet-service6-name	Select an IPv6 internet service.	none
internet-service6-negate	Enable to negate the source IPv6 internet service set in this policy.	disable
internet-service6-src	Enable or disable use of the IPv6 internet services in the source for this policy. If enabled, the source address is not used.	disable
internet-service6-src-custom	Select the custom IPv6 internet service source.	none
internet-service6-src-custom-group	Select the custom IPv6 source group.	none
internet-service6-src-group	Select the IPv6 source group.	none
internet-service6-src-name	Select the IPv6 source.	none
internet-service6-src-negate	Enable to negate the value set in `internet-service6-src`.	disable
match-vip	Enable or disable matching of packets that have had their destination address changed by a VIP.	disable
match-vip-only	Enable or disable matching only those packets that have had their destination addresses change by a VIP.	disable
natinbound	Enable or disable applying destination NAT to inbound traffic.	disable
natip	Set the source NAT IP address for inbound traffic.	0.0.0.0/0.0.0.0
natoutbound	Enable or disable applying destination NAT to outbound traffic.	disable
network-service-dynamic	Select a dynamic network service.	none
network-service-src-dynamic	Select a dynamic network service source.	none

Option	Description	Default
np-acceleration	Enable or disable UTM network processor acceleration.	enable
ntlm	Enable or disable NTLM authentication.	disable
ntlm-enabled-browsers	Set the HTTP-User-Agent value of supported browsers.	none
ntlm-guest	Enable or disable NTLM guest user access.	disable
outbound	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic.	enable
passive-wan-health-measurement	Enable or disable passive WAN health measurement. When enabled, `auto-asic-offload` is disabled.	disable.
permit-any-host	Enable or disable accepting UDP packets from any host.	disable
permit-stun-host	Enable or disable accepting UDP packets from any session traversal utilities for NAT (STUN) host.	disable
policy-expiry	Enable or disable policy expiry.	disable
policy-expiry-date	If policy-expiry is enabled, set the policy expiry date.	0000-00-00,00:00:00
policy-offload	Enable or disable hardware session setup for CGNAT.	enable
radius-mac-auth-bypass	Enable or disable MAC authentication bypass. The bypassed MAC address must be received from the RADIUS server.	disable
redirect-url	Set the URL to which users are redirected after seeing and accepting the disclaimer or authenticating.	none
reputation-direction	Set the destination of the initial traffic for reputation to take effect.	destination
reputation-direction6	Set the destination of the initial traffic for IPv6 reputation to take effect.	destination
reputation-minimum	Set the minimum reputation to take action.	0
reputation-minimum6	Set the minimum IPv6 reputation to take action.	0
rtp-addr	If this is an RTP NAT policy, set the address names.	none
rtp-nat	Enable or disable real time protocol (RTP) NAT.	disable
schedule-timeout	Enable or disable ending current sessions when the schedule object times out. Disable allows sessions to end from inactivity.	disable
sctp-filter-profile	Select an existing SCTP filter profile.	none
send-deny-packet	Enable or disable sending a reply when a session is denied or blocked by a firewall policy.	disable

Option	Description	Default
service-negate	Enable or disable negation of the service set in the policy.	disable
session-ttl	Enter a value for the session time-to-live (TTL) from 300 to 604800, or type 0 for no limitation.	0
sgt	Enter security group tags (SGT).	none
sgt-check	Enable or disable SGT check.	disable
src-vendor-mac	Select the vendor MAC source.	none
srcaddr-negate	Enable or disable negation of the source address.	disable
srcaddr6-negate	Enable or disable negation of the source IPv6 address.	disable
ssh-filter-profile	Select an SSH filter profile from the drop-down list.	None
ssh-policy-redirect	Enable or disable SSH policy redirect.	disable
tcp-mss-receiver	Enter the receiver's TCP maximum segment size (MSS).	0
tcp-mss-sender	Enter the sender's TCP MSS.	0
tcp-session-without-syn	Enable or disable creation of a TCP session without the SYN flag.	disable
tcp-timeout-pid	Select the TCP timeout profile.	none
timeout-send-rst	Enable or disable the sending of RST packets when TCP sessions expire	disable
tos	Enter the type of service (TOS) value used for comparison.	0
tos-mask	Enter the bit mask for TOS. Non-zero bit positions are used for comparison while zero bit positions are ignored.	0
tos-negate	Enable or disable to negate the TOS match.	disable
udp-timeout-pid	Select the UDP timeout profile.	none
uuid	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000
vlan-cos-fwd	Select the VLAN forward direction user priority. The available values are: • 255 (passthrough) • 0 (lowest) - 7 (highest)	255
vlan-cos-rev	Select the VLAN reverse direction user priority. The available values are: • 255 (passthrough) • 0 (lowest) - 7 (highest)	255
vlan-filter	Set VLAN filters.	none

Option	Description	Default
wanopt	Enable or disable WAN optimization (IPv4 only).	disable
wanopt-detection	Select the WAN optimization as active, passive, or off.	active
wanopt-passive-opt	Select WAN optimization passive mode options. This option decides what IP address will be used to connect server (IPv4 only).	default
wanopt-peer	Select a WAN optimization peer (IPv4 only).	none
wanopt-profile	Select a WAN optimization profile (IPv4 only).	none
webcache	Enable or disable web cache (IPv4 only).	disable
webcache-https	Enable or disable the web cache for HTTPS (IPv4 only).	none
webproxy-forward-server	Select the webproxy forward server (IPv4 only).	none
webproxy-profile	Select the webproxy profile (IPv4 only).	none

Create a new virtual wire pair SSL inspection and authentication policy

This section describes how to create a new virtual wire pair SSL inspection and authentication policy. This policy type is essentially a firewall virtual wire pair policy for policy-based policy packages.

See NGFW policy in the FortiOS Administration Guide for more information.



The *Virtual Wire Pair SSL Inspection & Authentication* policy option is visible only if the *NGFW Mode* is selected as *Policy-based* in the policy package.



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects > Tools > Feature Visibility*, and add or remove a checkmark for the corresponding feature.

To create a new virtual wire pair SSL inspection and authentication policy:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *Virtual Wire Pair SSL Inspection & Authentication*.
4. Click *Create New*.

5. Enter the following information:

Option	Description
ID	Enter a unique number as the policy ID, or use the default (0) to automatically assign a policy ID. Policy IDs can be up to a maximum of 9 digits in length. Once a policy ID has been configured it cannot be changed.
Name	Enter a unique name for the policy. Each policy must have a unique name.
Virtual Wire Pair Interface	Select one or more virtual wire pair interfaces. This field is required. New objects can be created by clicking the *Create New* icon in the *Object Selector* frame. See Creating objects on page 533 for more information.
Virtual Wire Pair	Select an arrow to indicate the flow of traffic between the ports in the selected *Virtual Wire Pair Interface*.
Source	Select the source address, address groups, virtual IPs, virtual IP groups, user, user groups, and FSSO groups.
Enforce ZTNA	Enable or disable ZTNA.
EMS Tag	Select the FortiClient EMS tag to match. This option is only available if Enforce ZTNA is enabled.
Geographic IP Tag	Select the Geographic IP tag to match. This option is only available if Enforce ZTNA is enabled.
Destination	Select the destination address, address groups, virtual IPs, virtual IP groups, and services.
Service	Select services and service groups. This option is only available when *Destination Internet Service* is off.
SSL/SSH Inspection	Select one of the following options for SSL/SSH Inspection:certificate-inspectioncustom-deep-inspectiondeep-inspectionno-inspection
Comments	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the *FortiOS CLI Reference*.
Change Note	Add a description of the changes being made to the policy. This field is required.

6. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

Advanced options

Option	Description	Default
anti-replay	Enable or disable anti-replay checking.	enable
auth-cert	Select the HTTPS server certificate for policy authentication.	none
auth-path	Enable or disable authentication-based routing.	disable
auth-redirect-addr	Select the HTTP-to-HTTPS redirect address for firewall authentication.	none
auto-asic-offload	Enable or disable policy traffic ASIC offloading.	enable
block-notification	Enable or disable block notification.	disable
cgn-eif	Enable or disable CGN endpoint independent filtering.	disable
cgn-eim	Enable or disable CGN endpoint independent mapping.	disable
cgn-log-server-grp	Select the NP log server group.	none
cgn-resource-quota	Set the allowed number of blocks assigned to a source IP address.	16
cgn-session-quota	Set the allowed concurrent sessions available for a source IP address.	16777215
custom-log-fields	Select custom fields to append to log messages for this policy.	none
delay-tcp-npu-session	Enable or disable TCP NPU session delay to guarantee packet order of 3-way handshake.	disable
diffserv-copy	Enable or disable copying of the DSCP values from the original direction to the reply direction.	disable
diffserv-forward	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic. If enabled, also configure `diffservcode-forward`.	disable
diffserv-reverse	Enable or disable application of the DSCP value to the DSCP field of reverse (reply) traffic. If enabled, also configure `diffservcode-rev`.	disable
diffservcode-forward	Enter the DSCP value that the FortiGate unit will apply to the field of originating (forward) packets. The value is 6 bits binary. The valid range is 000000-111111.	000000
diffservcode-rev	Enter the DSCP value that the FortiGate unit will apply to the field of reply (reverse) packets. The value is 6 bits binary. The valid range is 000000-111111.	000000
dlp-profile	Select an existing data loss prevention (DLP) profile.	none
dsri	Enable to ignore HTTP server responses.	disable
dstaddr-negate	Enable to negate the destination IP address.	disable

Option	Description	Default
dstaddr6-negate	Enable to negate the destination IPv6 address.	disable
dynamic-shaping	Enable or disable dynamic RADIUS-defined traffic shaping.	disable
email-collect	Enable or disable email collection.	disable
fec	Enable or disable forward error correction (FEC) on traffic matching this policy on a FEC device.	disable
firewall-session-dirty	Select how to handle sessions if the configuration of this firewall policy changes.	check-all
ffsso-agent-for-ntlm	Select the FSSO agent for NTLM authentication.	none
geoip-anycast	Enable or disable recognition of anycast IP addresses using the geography IP database.	disable
geoip-match	Select whether to match the address based on the physical or registered location.	physical-location
identity-based-route	Select the identity-based routing rule.	none
internet-service-negate	Enable to negate the internet service set in the policy.	disable
internet-service-src-negate	Enable to negate the source internet service set in this policy.	disable
internet-service6	Enable or disable the use of IPv6 internet services for this policy. If enabled, the destination address and service set in the policy are not used.	disable
internet-service6-custom	Select a custom IPv6 internet service.	none
internet-service6-custom-group	Select a custom IPv6 internet service group.	none
internet-service6-group	Select an IPv6 internet service group.	none
internet-service6-name	Select an IPv6 internet service.	none
internet-service6-negate	Enable to negate the source IPv6 internet service set in this policy.	disable
internet-service6-src	Enable or disable use of the IPv6 internet services in the source for this policy. If enabled, the source address is not used.	disable
internet-service6-src-custom	Select the custom IPv6 internet service source.	none

Option	Description	Default
internet-service6-src-custom-group	Select the custom IPv6 source group.	none
internet-service6-src-group	Select the IPv6 source group.	none
internet-service6-src-name	Select the IPv6 source.	none
internet-service6-src-negate	Enable to negate the value set in `internet-service6-src`.	disable
match-vip	Enable or disable matching of packets that have had their destination address changed by a VIP.	disable
match-vip-only	Enable or disable matching only those packets that have had their destination addresses change by a VIP.	disable
natinbound	Enable or disable applying destination NAT to inbound traffic.	disable
natip	Set the source NAT IP address for inbound traffic.	0.0.0.0/0.0.0.0
natoutbound	Enable or disable applying destination NAT to outbound traffic.	disable
network-service-dynamic	Select a dynamic network service.	none
network-service-src-dynamic	Select a dynamic network service source.	none
np-acceleration	Enable or disable UTM network processor acceleration.	enable
ntlm	Enable or disable NTLM authentication.	disable
ntlm-enabled-browsers	Set the HTTP-User-Agent value of supported browsers.	none
ntlm-guest	Enable or disable NTLM guest user access.	disable
outbound	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic.	enable
passive-wan-health-measurement	Enable or disable passive WAN health measurement. When enabled, `auto-asic-offload` is disabled.	disable.
permit-any-host	Enable or disable accepting UDP packets from any host.	disable
permit-stun-host	Enable or disable accepting UDP packets from any session traversal utilities for NAT (STUN) host.	disable
policy-expiry	Enable or disable policy expiry.	disable
policy-expiry-date	If policy-expiry is enabled, set the policy expiry date.	0000-00-00,00:00:00

Option	Description	Default
policy-offload	Enable or disable hardware session setup for CGNAT.	enable
radius-mac-auth-bypass	Enable or disable MAC authentication bypass. The bypassed MAC address must be received from the RADIUS server.	disable
redirect-url	Set the URL to which users are redirected after seeing and accepting the disclaimer or authenticating.	none
reputation-direction	Set the destination of the initial traffic for reputation to take effect.	destination
reputation-direction6	Set the destination of the initial traffic for IPv6 reputation to take effect.	destination
reputation-minimum	Set the minimum reputation to take action.	0
reputation-minimum6	Set the minimum IPv6 reputation to take action.	0
rtp-addr	If this is an RTP NAT policy, set the address names.	none
rtp-nat	Enable or disable real time protocol (RTP) NAT.	disable
schedule-timeout	Enable or disable ending current sessions when the schedule object times out. Disable allows sessions to end from inactivity.	disable
sctp-filter-profile	Select an existing SCTP filter profile.	none
send-deny-packet	Enable or disable sending a reply when a session is denied or blocked by a firewall policy.	disable
service-negate	Enable or disable negation of the service set in the policy.	disable
session-ttl	Enter a value for the session time-to-live (TTL) from 300 to 604800, or type 0 for no limitation.	0
sgt	Enter security group tags (SGT).	none
sgt-check	Enable or disable SGT check.	disable
src-vendor-mac	Select the vendor MAC source.	none
srcaddr-negate	Enable or disable negation of the source address.	disable
srcaddr6-negate	Enable or disable negation of the source IPv6 address.	disable
ssh-filter-profile	Select an SSH filter profile from the drop-down list.	None
ssh-policy-redirect	Enable or disable SSH policy redirect.	disable
tcp-mss-receiver	Enter the receiver's TCP maximum segment size (MSS).	0
tcp-mss-sender	Enter the sender's TCP MSS.	0
tcp-session-without-syn	Enable or disable creation of a TCP session without the SYN flag.	disable

Option	Description	Default
tcp-timeout-pid	Select the TCP timeout profile.	none
timeout-send-rst	Enable or disable the sending of RST packets when TCP sessions expire	disable
tos	Enter the type of service (TOS) value used for comparison.	0
tos-mask	Enter the bit mask for TOS. Non-zero bit positions are used for comparison while zero bit positions are ignored.	0
tos-negate	Enable or disable to negate the TOS match.	disable
udp-timeout-pid	Select the UDP timeout profile.	none
uuid	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000
vlan-cos-fwd	Select the VLAN forward direction user priority. The available values are: • 255 (passthrough) • 0 (lowest) - 7 (highest)	255
vlan-cos-rev	Select the VLAN reverse direction user priority. The available values are: • 255 (passthrough) • 0 (lowest) - 7 (highest)	255
vlan-filter	Set VLAN filters.	none
wanopt	Enable or disable WAN optimization (IPv4 only).	disable
wanopt-detection	Select the WAN optimization as active, passive, or off.	active
wanopt-passive-opt	Select WAN optimization passive mode options. This option decides what IP address will be used to connect server (IPv4 only).	default
wanopt-peer	Select a WAN optimization peer (IPv4 only).	none
wanopt-profile	Select a WAN optimization profile (IPv4 only).	none
webcache	Enable or disable web cache (IPv4 only).	disable
webcache-https	Enable or disable the web cache for HTTPS (IPv4 only).	none
webproxy-forward-server	Select the webproxy forward server (IPv4 only).	none
webproxy-profile	Select the webproxy profile (IPv4 only).	none

Create a new security virtual wire pair policy

This section describes how to create virtual wire pair policies. Before you can create a policy, you must create a virtual wire pair. See Configuring virtual wire pairs on page 741.

You can create a security virtual wire pair policy in a policy package that is set to *Policy-based*. If the policy package is set to *Profile-based*, see Create a new firewall virtual wire pair policy on page 454.

See Virtual wire pair in the FortiOS Administration Guide for more information about virtual wire pairs and virtual wire pair policies.



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects > Tools > Feature Visibility*, and add or remove a checkmark for the corresponding feature.

To create a new security virtual wire pair policy:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *Security Virtual Wire Pair Policy*.
4. Click *Create New*.
5. Enter the following information:

Option	Description
ID	Enter a unique number as the policy ID, or use the default (0) to automatically assign a policy ID. Policy IDs can be up to a maximum of 9 digits in length. Once a policy ID has been configured it cannot be changed.
Name	Enter a unique name for the policy. Each policy must have a unique name.
Virtual Wire Pair Interface	Select one or more virtual wire pair interfaces. This field is required..
Virtual Wire Pair	Select an arrow to indicate the flow of traffic between the ports in the selected *Virtual Wire Pair Interface*.
Source	Select the source address, address groups, virtual IPs, virtual IP groups, user, user groups, and FSSO groups.
Destination	Select the destination address, address groups, virtual IPs, virtual IP groups, and services.
Schedule	Select a one-time schedule, recurring schedule, or schedule group.
Service	Select the service. Select *App Default* or *Specify*. If *Specify* is selected, select the Service.
Application	Select applications.
URL Category	Select URL categories.
Action	Select an action for the policy to take: *DENY* or *ACCEPT*.
Log Traffic	When the *Action* is *DENY*, select *Log Violation Traffic* to log violation traffic. When the *Action* is *ACCEPT*, select one of the following options:

Option	Description
	• *No Log* • *Log Security Events* • *Log All Sessions* Select whether to generate logs when the session starts.
Protocol Options	Select protocol options profiles for handling protocol-specific traffic. This option is available when the *Action* is *ACCEPT*.
Security Profiles	Select to add security profiles or profile groups. This option is available when the *Action* is *ACCEPT*. If *Use Standard Security Profiles* is selected, the following standard security profile types can be added: • AntiVirus Profile • Web Filter Profile • IPS Profile • Email Filter • File Filter Profile If *Use Security Profile Group* is selected, select the *Profile Group*.
Comments	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the *FortiOS CLI Reference*.
Change Note	Add a description of the changes being made to the policy. This field is required.

6. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

Advanced options

Option	Description	Default
application-list	Select ...an existing application list.	none
comments	Add a description of the policy, such as its purpose, or the changes that have been made to it. A comment added here will overwrite the comment added in the above *Comments* field.	none
dlp-profile	Select an existing data loss prevention (DLP) profile.	none
dnsfilter-profile	Select an existing DNS filter profile.	none
dstaddr-negate	Enable to negate the values set in *IPv4 Destination Address* and *IPv6 Destination Address*.	disable

Option	Description	Default
global-label	Set the label for the policy to be displayed when the GUI is in *Global View* mode.	none
icap-profile	Select an existing Internet Content Adaptation Protocol (ICAP) profile.	none
internet-service-negate	When enabled, Internet services match against any Internet service except the selected Internet service.	disable
internet-service-src-negate	Enables or disables the use of Internet Services in source for this policy. If enabled, `internet-service-src` specifies what the service must NOT be.	disable
internet-service6	Enable or disable the use of IPv6 internet services for this policy. If enabled, the destination address and service set in the policy are not used.	disable
internet-service6-custom	Select a custom IPv6 internet service.	none
internet-service6-custom-group	Select a custom IPv6 internet service group.	none
internet-service6-group	Select an IPv6 internet service group.	none
internet-service6-name	Select an IPv6 internet service.	none
internet-service6-negate	Enable to negate the source IPv6 internet service set in this policy.	disable
internet-service6-src	Enable or disable use of the IPv6 internet services in the source for this policy. If enabled, the source address is not used.	disable
internet-service6-src-custom	Select the custom IPv6 internet service source.	none
internet-service6-src-custom-group	Select the custom IPv6 source group.	none
internet-service6-src-group	Select the IPv6 source group.	none
internet-service6-src-name	Select the IPv6 source.	none
internet-service6-src-negate	Enable to negate the value set in `internet-service6-src`.	disable
nat46	Enable or disable NAT46.	disable
nat64	Enable or disable NAT64.	disable

Option	Description	Default
sctp-filter-profile	Select an existing stream control transmission protocol (SCTP) filter profile.	none
send-deny-packet	Enable or disable sending a reply packet when a session is denied or blocked by this policy.	disable
service-negate	Enable or disable negation of the selected *Service*.	disable
srcaddr-negate	Enable or disable negation of the *IPv4 Source Address* or *IPv6 Source Address* address.	disable
ssh-filter-profile	Select an existing SSH filter profile.	none
ssl-ssh-profile	Select an existing SSL SSH profile.	no-inspection
utm-status	Enable or disable the Unified Threat Management status.	disable
uuid	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000
voip-profile	Select an existing VOIP profile.	None

Create a new proxy policy

This section describes how to create web, FTP, WAN optimization (WANOpt), and ZTNA proxy policies.



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.



In earlier versions, ZTNA rules were special proxy policies that controlled access to the ZTNA servers, and they could be configured from the *Policy & Objects* > *Policy Packages* > *ZTNA Rules*. However, on this version and above, ZTNA rules are now configured as a proxy policy by selecting the *ZTNA* proxy type in *Policy & Objects* > *Policy Pagackages* > *Proxy Policy*.

To create a new proxy policy:

1. Go to *Policy & Objects* > *Policy Packages*.
2. In the tree menu for the policy package in which you will be creating the new policy, select *Proxy Policy*.
3. Click *Create New*.
4. Enter the following information:

Option	Description
Name	Enter a unique name for the policy. Each policy must have a unique name.

Option	Description
Explicit Proxy Type	Select the explicit proxy type: *Explicit Web*, *Transparent Web*, *FTP*, or *WAN Optimize*.
Incoming Interface	Click the field then select interfaces. Click the remove icon to remove interfaces. This option is only available when the proxy type is set to *Transparent Web*.
Outgoing Interface	Select outgoing interfaces in the same manner as *Incoming Interface*.
Source	Select source aaddresses, address groups, virtual IPs, and virtual IP groups.
Security Posture Tag	For ZTNA proxy policies, select the security posture tags and tag groups. See Zero Trust Network Access (ZTNA) objects on page 572. This option is only available when the proxy type is set to *ZTNA*.
Destination	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
ZTNA Server	For ZTNA proxy policies, select a ZTNA server. See Configuring a ZTNA server on page 574. This option is only available when the proxy type is set to *ZTNA*.
Service	Select services and service groups from the object selector pane.
Schedule	Select a one-time schedule, recurring schedule, or schedule group.
Action	Select an action for the policy to take: *Deny*, *Accept*, or *Redirect*. *Redirect* is only available when the proxy type is set to *Explicit Web* or *Transparent Web*.
Log Allowed Traffic	Select one of the following options: • *No Log* • *Log Security Events* • *Log All Sessions* If logging is set to *Log All Sessions*, select whether to generate logs when the session starts. This option is available when the *Action* is *Accept*.
Log Violation Traffic	Select to log violation traffic. This option is available when the *Action* is *Deny*.
Display Disclaimer	Set the Display Disclaimer: *Disable*, *By Domain*, *By Policy*, or *By User*. Optionally, if enabled, select a custom message in the *Customize Messages* field. This option is available when the *Action* is *Accept*.
Security Profiles	Select to add security profiles or profile groups. If *Use Standard Security Profiles* is selected the following profile types can be added:

Option	Description
	• Antivirus Profile • Web Filter Profile (not available when the proxy type is set to *FTP*) • Video Profile Filter • Application Control (not available when the proxy type is set to *FTP*) • IPS Profile (not available when the proxy type is set to *FTP*) • File Filter Profile • ICAP (not available when the proxy type is set to *FTP*) • Web Application Firewall (not available when the proxy type is set to *FTP*) In *Protocol Options*, select a protocol options group. If *Use Security Profile Group* is selected, select the *Profile Group*. This option is available when the *Action* is *Accept*.
SSL/SSH Inspection	Select one of the following options for SSL/SSH Inspection:certificate-inspectioncustom-deep-inspectiondeep-inspectionno-inspection This option is not available when the *Security Profiles Profile Type* is set to *Use Security Profile Group*.
Redirect URL	Enter the redirect URL. This option is only available when the *Action* is *Redirect*. When the *Action* is *Redirect*, this field is required.
Web Proxy Forwarding Server	Select a web proxy forwarding server. This option is not available when the proxy type is set to *FTP*.
Comments	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the *FortiOS CLI Reference*.
Change Note	Add a description of the changes being made to the policy. This field is required.

5. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

Advanced options

Option	Description	Default
access-proxy	Select an IPv4 access proxy.	none
access-proxy6	Select an IPv6 access proxy.	none
block-notification	Enable or disable block notification.	disable
device-ownership	Enable or disable ownership enforcement at the policy level.	disable

Option	Description	Default
dlp-profile	Select an existing data loss prevention (DLP) profile.	none
dstaddr-negate	Enable or disable negation of the values set in *Destination*.	disable
global-label	Enter the label for the policy to be displayed when the GUI is in *Global View* mode.	none
http-tunnel-auth	Enable or disable HTTP tunnel authentication	disable
internet-service-negate	Enable or disable negation of the internet service.	disable
label	Set the label for the policy to be displayed in the VDOM.	none
sctp-filter-profile	Select an existing stream control transmission protocol (SCTP) filter profile.	none
service-negate	Enable or disable negation of the service specified in *Service*.	disable
session-ttl	Session TTL for sessions accepted by this policy (300 - 6040800 seconds, 0 = use system default).	0
srcaddr-negate	Enable or disable negation of the source address.	disable
ssh-filter-profile	Select an existing SSH filter profile.	none
ssh-policy-redirect	Enable or disable SSH policy redirect.	disable
transparent	Enable or disable using the IP address of the client to connect to the server.	disable
uuid	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000
webcache	Enable or disable web cache.	disable
webcache-https	Enable or disable web cache for HTTPS.	disable
webproxy-profile	Select a webproxy profile.	none
ztna-ems-tag	Select ZTNA EMS tags.	none
ztna-tags-match-logic	Set the logic used for matching security posture tags. The available options are **and** and or.	or

Create a new central SNAT policy

Central SNAT (source NAT) enables you to define and control (with more granularity) the address translation performed by the FortiGate unit. With the NAT table, you can define the rules which dictate the source address or address group and which IP pool the destination address uses.

While similar in functionality to IP pools, where a single address is translated to an alternate address from a range of IP addresses, with IP pools there is no control over the translated port. When using the IP pool for source NAT, you can define a fixed port to guarantee the source port number is unchanged. If no fixed port is

defined, the port translation is randomly chosen by the FortiGate unit. With the central NAT table, you have full control over both the IP address and port translation.

The FortiGate unit reads the NAT rules in a top-down methodology, until it hits a matching rule for the incoming address. This enables you to create multiple NAT policies that dictate which IP pool is used based on the source address. The NAT policies can be rearranged within the policy list as well. NAT policies are applied to network traffic after a security policy.

If NGFW mode is policy-based, then it is assumed that central NAT (specifically SNAT) is enabled implicitly.

See Central SNAT in the FortiOS Administration Guide for more information about central SNAT.



Central SNAT does not support *Section View*.



Central NAT must be enabled when creating or editing the policy package for this option to be available in the tree menu. See Create new policy packages on page 415.

Central SNAT must also be enabled in *Feature Visibility* for the option to be visible in the tree menu. On the *Policy & Objects* tab, from the *Tools* menu, select *Feature Visibility*. In the *Policy* section, select the *Central SNAT* check box to display this option.

To create a new central SNAT policy:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *Central SNAT Policy*.
4. Click *Create New*.
5. Enter the following information:

Option	Description
Type	Select whether to perform SNAT on IPv4 or IPv6.
Incoming Interface	Click the field then select interfaces. Click the remove icon to remove interfaces. New objects can be created by clicking the *Create New* icon in the *Object Selector* frame. See Creating objects on page 533 for more information.
Outgoing Interface	Select outgoing interfaces in the same manner as *Incoming Interface*.
Source Address	Select source addresses, address groups, virtual IPs, and virtual IP groups.
Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups.

Option	Description
NAT	Select to enable NAT.If enabled, select *NAT*, *NAT46*, or *NAT64*. If *Type* is set to *IPv4*, *NAT64* is not available. If *Type* is set to *IPv6*, *NAT46* is not available.
IP Pool Configuration	If *NAT* is selected, select *Use Outgoing Interface Address* or *Use Dynamic IP Pool*.
Protocol	Select the protocol: *ANY*, *TCP*, *UDP*, *SCTP*, or *Specify*. If *Specify* is selected, specify the protocol number. This option is only available when *NAT* is selected.
Explicit Port Mapping	Enable or disable port mapping, then set the *Original Source Port* to match. Choose an original source port from one to 65535. The NAT'd port will be chosen by the FortiGate based on the IP Pool configuration. Explicit port mapping cannot apply to some protocols which do not use ports, such as ICMP. When enabling a NAT policy which uses Explicit port mapping, always consider that ICMP traffic will not match this policy. When using IP Pools, only the Overload type IP Pool allows Explicit port mapping. When Explicit port mapping is applied, you must define an original source port range and a translated sort port range. The source port will map one to one with the translated port. See Dynamic SNAT in the FortiOS Administration Guide for more information about how each IP pool type works.
Comments	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	Configure advanced options, see Advanced options below.For more information on advanced option, see the *FortiOS CLI Reference*.
Change Note	Add a description of the changes being made to the policy. This field is required.

6. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

Advanced options

Option	Description	Default
uuid	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000

Create a new central DNAT or IPv6 central DNAT policy

Destination NAT (DNAT) is typically applied to traffic from the Internet that is going to be directed to a server on a network behind the FortiGate device. The actual address of the internal network is hidden. When a request is received, FortiGate checks the NAT table and determines if the destination IP address for incoming traffic must be changed using DNAT.

DNAT must take place before routing so that the unit can route packets to the correct destination.

DNAT policies can be created, or imported from Virtual IP (VIP) objects. Virtual servers can also be imported from ADOM objects to DNAT policies. DNAT policies are automatically added to the Virtual IP (VIP) object table (*Firewall Objects* > *Virtual IPs*) when they are created.

VIPs can be edited from either the DNAT or VIP object tables by double-clicking on the VIP, right-clicking on the VIP and selecting *Edit*, or selecting the VIP and clicking *Edit* in the toolbar. The network type cannot be changed. DNAT policies can also be copied, pasted, cloned, and moved using the right-click or *Edit* menus.

Deleting a DNAT policy does not delete the corresponding VIP object, and a VIP object cannot be deleted if it is in the DNAT table.

DNAT policies support overlapping IP address ranges; VIPs do not. DNAT policies do not support VIP groups.

See Destination NAT in the FortiOS Administration Guide for more information.



Central DNAT does not support *Section View*.



Central NAT must be enabled when creating or editing the policy package for this option to be available in the tree menu. See Create new policy packages on page 415.

Central DNAT must be enabled in *Feature Visibility* as well for the option to be visible in the tree menu. On the *Policy & Objects* tab, from the *Tools* menu, select *Feature Visibility*. In the *Policy* section, select the *Central DNAT* check box to display this option.

To create a new central DNAT policy:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *Central DNAT Policy*.
4. Click *Create New*.
5. Enter the following information:

Option	Description
Name	Enter a unique name for the policy. Each policy must have a unique name.
Comments	Add a description of the policy, such as its purpose, or the changes that have been made to it.

Option	Description
Color	Select a color. This color will be used to indentify this DNAT in the fabric view.
Status	Enable or disable the policy. This option is not available for IPv6 policies.
Interface	Select an interface.
Configure Default Value	Enable or disable the default value.
Type	Select the network type: *Static NAT*, *DNS Translation*, *FQDN*, or *Load balance*. This option is only available when *Configure Default Value* is enabled. For IPv6 policies, only *Static NAT* is available.
External IP Address/Range	Enter the start and end external IP addresses in the fields. If there is only one address, enter it in both fields. This option is only available when *Configure Default Value* is enabled and the network type is not *FQDN*.
Mapped IP [v4/v6] Address/Range	Enter the mapped IP address or address range. These options are only available when *Configure Default Value* is enabled and the network type is not *FQDN*. For IPv6 policies, select Use Embedded to use the lower 32 bits of the external IPv6 address as the mapped IPv4 address.
External IP Address	Enter the external IP address. This option is only available when *Configure Default Value* is enabled and the network type is *FQDN*.
Mapped Address	Select the mapped address. This option is only available when *Configure Default Value* is enabled and the network type is *FQDN*.
Source Interface Filter	Select a source interface filter. This option is only available when *Configure Default Value* is enabled.
Optional Filters	Enable or disable optional filters. This option is only available when *Configure Default Value* is enabled.
Source Address	If *Optional Filters* is enabled, add source IP, range, or subnet filters. Multiple filters can be added using the *Add* icon.
Services	If *Optional Filters* is enabled, enable or disable and then select services.
Port Forwarding	Enable or disable port forwarding and then configure the ports to map. This option is only available when *Configure Default Value* is enabled.
Protocol	If *Port Forwarding* is enabled, select the protocol: *TCP*, *UDP*, *SCTP*, or *ICMP*. *ICMP* is not available for IPv6 policies.
External Service Port	If *Port Forwarding* is enabled, enter the external service port.

Option	Description
	This option is not available when *Protocol* is *ICMP*.
Map to [IPv4/IPv6] Port	If *Port Forwarding* is enabled, enter the map to port. This option is not available when *Protocol* is *ICMP*.
Enable ARP Reply	Select to enable address resolution protocol (ARP) reply. This option is only available when *Configure Default Value* is enabled.
Add To Groups	Select the groups to which the virtual IP should be added.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the *FortiOS CLI Reference*.
Per-Device Mapping	Enable or disable per-device mapping. If multiple imported VIP objects have the same name but different details, the object type will become *Dynamic Virtual IP*, and the per-device mappings will be listed here. Mappings can also be manually added, edited, and deleted as needed.
Change Note	Add a description of the changes being made to the policy. This field is required.

6. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

To import VIPs from the VIP object table:

1. Ensure you are in the correct ADOM.
2. Go to *Policy &Objects* > *Policy Packages*.
3. In the tree menu for the policy package, click *Central DNAT*.
4. Click *Import* in the toolbar. The *Import* dialog box will open.
5. Select the VIP object or objects that need to be imported. If necessary, use the search box to locate specific objects.
6. Click *OK* to import the VIPs to the *Central DNAT* table.

Advanced options

Option	Description	Default
add-nat46-route	Enable or disable adding NAT46 to a route. This option is not available for IPv6 policies.	enable
add-nat64-route	Enable or disable adding NAT64 to a route. This option is only available for IPv6 policies.	enable
dns-mapping-ttl	Enter time-to-live for DNS response, from 0 to 604 800. Set to to 0 to use the DNS server's response time.	0

Option	Description	Default
	This option is not available for IPv6 policies.	
extaddr	Select an external FQDN. This option is not available for IPv6 policies.	None
gratuitous-arp-interval	Set the time intervalin seconds between sending of gratuitous address resolution protocol (ARP) packets by a virtual IP. Set to 0 to disable this feature. Set from 5 to 8640000 seconds to enable This option is not available for IPv6 policies.	0
http-cookie-age	Set the time in minutes that client web browsers should keep a cookie. Set to 0 for no time limit.	60
http-cookie-domain	Enter the domain name to which cookie persistence should apply.	none
http-cookie-domain-from-host	Enable or disable use of the HTTP cookie domain from the `host` field in HTTP.	disable
http-cookie-generation	Set the generation of HTTP cookies to be accepted. The exact value is not important, only that it is different from any generation that has already been used. Changing this value invalidates all existing cookies.	0
http-cookie-path	Specify the path to which cookie persistence is limited.	none
http-cookie-share	Configure to control the sharing of cookies across virtual servers. Using `same-ip` means that any cookie generated by one virtual server can be used by another virtual server in the same virtual domain. Disable stops cookie sharing between virtual servers.	same-ip
http-ip-header	For HTTP multiplexing, enable or disable to add teh original client IP address in the `X-Forwarded-For` HTTP header.	disable
http-ip-header-name	For HTTP multiplexing, enter a custom HTTP header name. The original client IP address is added to this header. If empty, `X-Forwarded-For` is used.	none
http-multiplex	Enable or disable HTTP multiplexing.	disable
http-redirect	Enable or disable redirection of HTTP to HTTPS.	disable
https-cookie-secure	Enable or disable verification that HTTPS cookies are secure.	disable
id	Enter a unique number as the policy ID, or use the default (0) to automatically assign a policy ID. Policy IDs can be up to a maximum of 9 digits in length. Once a policy ID has been configured it cannot be changed.	0
ldbd-method	Select the method used to distribute sessions to real servers.	static

Option	Description	Default
max-embryonic-connections	Set the maximum number of incomplete connections, from 0 to 100000.	1000
monitor	Select the health check monitor to use when polling to determine a virtual server's connectivity status.	none
nat-source-vip	Enable or disable forcing the source NAT mapped IP to the external IP for all traffic.	disable
nat44	Enable or disable NAT44. This option is not available for IPv6 policies.	enable
nat46	Enable or disable NAT46. This option is not available for IPv6 policies.	disable
nat64	Enable or disable NAT64. This option is only available for IPv6 policies.	enable
nat66	Enable or disable NAT66. This option is only available for IPv6 policies.	disable
outlook-web-access	Enable to add the `Front-End-Https` header for Microsoft Outlook Web Access.	disable
persistence	Configure the method used to ensure that clients connect to the same server every time they make a request that is part of the same session.	none
portmapping-type	Select the port mapping type, either `1-to-1` or `m-to-n` (many to many). This option is not available for IPv6 policies.	1-to-1
server-type	Select the protocol to be load balanced by the virtual server (also called the server load balance virtual IP).	none
ssl-accept-ffdhe-groups	Enable or disable using the FFDHE cipher suite for SSL key exchange.	enable
ssl-algorithm	Set the permitted encryption algorithms for SSL sessions according to encryption strength: • `high`: permit only high encryption algorithms: AES or 3DES. • `medium`: permit high or medium (RC4) algorithms. • `low`: permit high, medium, or low (DES) algorithms. • `custom`: only allow some preselected cipher suites to be used.	high
ssl-certificate	Select the certificate to use for SSL handshake.	none
ssl-client-fallback	Enable or disable support for preventing downgrade attacks on client connections.	enable

Option	Description	Default
ssl-client-rekey-count	Set the maximum length of data in MB before triggering a client rekey. Set to 0 to disable.	0
ssl-client-renegotiation	Select the SSL secure renegotiation policy. • `allow`: allow, but do not require secure renegotiation. • `deny`: do not allow renegotiation. • `secure`: require secure renegotiation.	allow
ssl-client-session-state-max	Set the maximum number of SSL session states to keep between the client and FortiGate, from 0 to 100000.	1000
ssl-client-session-state-timeout	Set the number of minutes to keep the SSL session states between the client and FortiGate, from 1 to 14400.	30
ssl-client-session-state-type	Select the method to use to expire SSL sessions between the client and FortiGate. • `both`: expire SSL session states when either `ssl-client-session-state-max` or `ssl-client-session-state-timeout` is exceeded, regardless of which occurs first. • `count`: expire SSL session states when `ssl-client-session-state-max` is exceeded. • `disable`: expire all SSL session states. • `time`: expire SSL session states when `ssl-client-session-state-timeout` is exceeded.	both
ssl-dh-bits	Select the number of bits used in the Diffie-Hellman exchange for RSA encryption of the SSL connection: `768`, `1024`, `1536`, `2048`, `3072`, or `4096`.	2048
ssl-hpkp	Enable or disable including HPKP header in the response.	disable
ssl-hpkp-age	Set the number of seconds that the client should honor the HPKP setting (60 - 157680000).	5184000
ssl-hpkp-backup	Select the certificate used to generate the backup HPKP pin from.	none
ssl-hpkp-include-subdomains	Enable or disable indicating that the HPKP header applies to all subdomains.	disable
ssl-hpkp-primary	Select the certificate used to generate the primary HPKP pin from.	none
ssl-hpkp-report-uri	Set the URL to report HPKP violations to (maximum size = 255).	none
ssl-hsts	Enable or disable including HSTS header in response.	disable
ssl-hsts-age	Set the number of seconds that the client should honour the HSTS setting (60 - 157680000).	5184000

Option	Description	Default
ssl-hsts-include-subdomains	Enable or disable indicating that the HSTS header applies to all subdomains.	disable
ssl-http-location-conversion	Enable to replace HTTP with HTTPS in the reply's `Location` HTTP header field.	disable
ssl-http-match-host	Enable or disable HTTP host matching for location conversion.	disable
ssl-max-version	Select the highest version of SSL/TLS to allow in SSL sessions: `ssl-3.0`, `tls-1.0`, `tls-1.1`, `tls-1.2`, or `tls-1.3`.	tls-1.3
ssl-min-version	Select the lowest version of SSL/TLS to allow in SSL sessions: `ssl-3.0`, `tls-1.0`, `tls-1.1`, `tls-1.2`, or `tls-1.3`.	tls-1.1
ssl-mode	Select the method to use for SSL offloading between the client and FortiGate (`half`) or from the client to FortiGate and from FortiGate to the server (`full`).	half
ssl-pfs	Select the cipher suites that can be used for SSL perfect forward secrecy (PFS): • `allow`: allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected. • `deny`: allow only non-Diffie-Hellman cipher suites, so PFS is not applied. • `require`: allow only Diffie-Hellman cipher suites, so PFS is applied. This setting applies to both client and server sessions.	require
ssl-send-empty-frags	Enable or disable sending empty fragments to avoid CBC IV attacks (SSL 3.0 and TLS 1.0 only). This setting may need to be disabled for compatibility with older systems.	enable
ssl-server-algorithm	Set the permitted encryption algorithms for SSL server sessions according to encryption strength: • `high`: permit only high encryption algorithms: AES or 3DES. • `medium`: permit high or medium (RC4) algorithms. • `low`: permit high, medium, or low (DES) algorithms. • `custom`: only allow some preselected cipher suites to be used. • `client`: Use the same encruption algorithms for both client and server sessions.	client
ssl-server-max-version	Select the highest version of SSL/TLS to allow in SSL server sessions: `client`, `ssl-3.0`, `tls-1.0`, `tls-1.1`, `tls-1.2`, or `tls-1.3`.	client

Option	Description	Default
ssl-server-min-version	Select the lowest version of SSL/TLS to allow in SSL server sessions: `client`, `ssl-3.0`, `tls-1.0`, `tls-1.1`, `tls-1.2`, or `tls-1.3`.	client
ssl-server-session-state-max	Set the maximum number of FortiGate to server SSL session states to keep, from 0 to 100000.	100
ssl-server-session-state-timeout	Set the number of minutes to keep FortiGate to server SSL session states, from 1 to 14400.	60
ssl-server-session-state-type	Select the method to use to expire FortiGate to server SSL sessions: • `both`: expire SSL session states when either `ssl-client-session-state-max` or `ssl-client-session-state-timeout` is exceeded, regardless of which occurs first. • `count`: expire SSL session states when `ssl-client-session-state-max` is exceeded. • `disable`: expire all SSL session states. • `time`: expire SSL session states when `ssl-client-session-state-timeout` is exceeded.	both
uuid	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000
weblogic-server	Enable or disable adding an HTTP header to indicate SSL offloading for a WebLogic server.	disable
websphere-server	Enable or disable adding an HTTP header to indicate SSL offloading for a WebSphere server.	disable

Create a new DoS policy

This section describes how to create denial of service (DoS) policies.

See DoS policy in the FortiOS Administration Guide for more information.



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.

To create a new DoS policy:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package, click *IPv4 DoS Policy* or *IPv6 DoS Policy*.
4. Click *Create New*.

5. Enter the following information:

Option	Description
Name	Enter a unique name for the policy. Each policy must have a unique name.
Interface	Click the field then select interfaces. Click the remove icon to remove interfaces.
Source	Select source addresses, address groups, virtual IPs, and virtual IP groups.
Destination	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
Service	Select services and service groups.

L3/L4 Anomalies	Configure the anomalies:
	Logging — Enable or disable logging for the anomaly. Anomalous traffic will be logged when the action is Block or Monitor.
	Action — Select the action to take when the threshold is reached:
	• *Disable*: Do not scan for the anomaly.
	• *Block*: Block the anomalous traffic.
	• *Monitor*: Allow the anomalous traffic but record a log message if logging is enabled.
	Threshold — Set the number of detected instances per minute that triggers the anomaly action.
	Quarantine — Select which system quarantine to use for blocked anomalous traffic. This setting is set to *None* by default. Click *None* in the Quarantine column to configure quarantine settings:
	• *None*: Disable quarantine.
	• *Attacker*: Block all traffic from the attacker's IP address, and add the attacker's IP address to the banned user list.
	  • *Expiry*: Set the duration of the quarantine, in days, hours, and minutes.
	  • *Log*: Enable/disable quarantine logging.
	See below for descriptions of each anomaly type.

Comments	Add a description of the policy, such as its purpose, or the changes that have been made to it. A comment added here will overwrite the comment added in the above *Comments* field.
Change Note	Add a description of the changes being made to the policy. This field is required.

L3 Anomalies		
Anomaly	**Description**	**Default Threshold**
ip_src_session	If the number of concurrent IP connections from one source IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
ip_dst_session	If the number of concurrent IP connections to one destination IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.

L4 Anomalies		
Anomaly	**Description**	**Default Threshold**
tcp_syn_flood	If the SYN packet rate of new TCP connections, including retransmission, to one destination IP address exceeds the configured threshold value, the action is executed. An additional *Proxy* action is available for this anomaly type. The anomalous traffic will be buffered and scanned when the complete file is downloaded. The *Proxy* action is only available on these platforms: FGC_3000D, FGC_3100D, FGC_3200D, FGC3700D, FGC3700DX, FGC_5001D, FGT_1500D, FGT_3000D, FGT_3100D, FGT_3200D, FGT3700D, FGT3700DX, and FGT_5001D.	2000 packets per second.
tcp_port_scan	If the SYN packet rate of new TCP connections, including retransmission, from one source IP address exceeds the configured threshold value, the action is executed.	1000 packets per second.
tcp_src_session	If the number of concurrent TCP connections from one source IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
tcp_dst_session	If the number of concurrent TCP connections to one destination IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
udp_flood	If the UDP traffic to one destination IP address exceeds the configured threshold value, the action is executed.	2000 packets per second.
udp_scan	If the UDP sessions setup rate originating from one source IP address exceeds the configured threshold value, the action is executed.	2000 sessions per second.
udp_src_session	If the number of concurrent UDP connections from one source IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.

L4 Anomalies		
Anomaly	**Description**	**Default Threshold**
udp_dst_session	If the number of concurrent UDP connections to one destination IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
icmp_flood	If the number of ICMP packets sent to one destination IP address exceeds the configured threshold value, the action is executed.	250 packets per second.
icmp_sweep	If the ICMP sessions setup rate originating from one source IP address exceeds the configured threshold value, the action is executed.	100 sessions per second.
icmp_src_session	If the number of concurrent ICMP connections from one source IP address exceeds the configured threshold value, the action is executed.	300 concurrent sessions.
icmp_dst_session	If the number of concurrent ICMP connections to one destination IP address exceeds the configured threshold value, the action is executed.	1000 concurrent sessions.
sctp_flood	If the number of SCTP packets sent to one destination IP address exceeds the configured threshold value, the action is executed.	2000 packets per second.
sctp_scan	If the number of SCTP sessions originating from one source IP address exceeds the configured threshold value, the action is executed.	1000 packets per second.
sctp_src_session	If the number of concurrent SCTP connections from one source IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
sctp_dst_session	If the number of concurrent SCTP connections to one destination IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.

6. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

Create a new interface policy

The section describes how to create new IPv4 and IPv6 interface policies.

See Interface policies in the FortiOS Administration Guide for more information.



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.

To create a new interface policy:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package, click *IPv4 Interface Policy* or *IPv6 Interface Policy*.
4. Click *Create New*.
5. Enter the following information:

Option	Description
Source > Interface	Select the source interface.
Source > Address	Select source addresses, address groups, virtual IPs, and virtual IP groups.
Destination > Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
Service	Select services and service groups.
Log Traffic	Select the traffic to log: *No Log*, *Log Security Events*, or *Log All Sessions*.
AntiVirus Profile	Enable or disable, and then select, the antivirus profile.
Web Filter Profile	Enable or disable, and then select, the web filter profile.
Application Control	Enable or disable, and then select, the application control profile.
IPS Profile	Enable or disable, and then select the IPS profile.
Email Filter Profile	Enable or disable, and then select, the email filter profile.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the *FortiOS CLI Reference*.
Change Note	Add a description of the changes being made to the policy. This field is required.

6. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

Advanced options

Option	Description	Default
address-type	Select	none
comments	Add a description of the policy, such as its purpose, or the changes that have been made to it.	none
dlp-profile	Select an existing data loss prevention (DLP) profile.	none
dlp-profile-status	Enable or disable DLP.	disable
dsri	Enable or disable DSRI.	disable

Create a new multicast policy

This section describes how to create a new multicast policy.

Multicasting consists of using a single source to send data to many receivers simultaneously, while conserving bandwidth and reducing network traffic.

See Multicast in the FortiOS Administration Guide for more information about multicasting.



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.



Starting in FortiManager 7.2.0, up to a maximum of 2560 multicast policies can be created.

To create a new multicast policy:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select either *IPv4 Multicast Policy* or *IPv6 Multicast Policy*.
4. Click *Create New*.
5. Enter the following information:

Option	Description
Name	Enter a unique name for the policy. Each policy must have a unique name.
Incoming Interface	Click the field then select interfaces. Click the remove icon to remove interfaces. New objects can be created by clicking the *Create New* icon in the *Object Selector* frame. See Creating objects on page 533 for more information.
Outgoing Interface	Select outgoing interfaces in the same manner as *Incoming Interface*.
Source Address	Select the source firewall address.
Destination Address	Select the destination multicast addresses.
Action	Select an action for the policy to take: *ACCEPT* or *DENY*.
Source NAT	Enable or disable source NAT, then enter the source NAT IP Address. This option is only available when *Action* is *Accept*.
Destination NAT	Enter the destination NAT IP address.
Protocol Option	Select a protocol option: *ANY*, *ICMP*, *IGMP*, *TCP*, *UDP*, *OSFP*, or *Others*.

Option	Description
Port Range	Set the port range. This option is only available when *Protocol Option* is *TCP* or *UDP*.
Protocol Number	Enter the protocol number, from 1 to 256. This option is only available when *Protocol Option* is *Others*.
Log Traffic	Enable or disable traffic logging.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the *FortiOS CLI Reference*.
Change Note	Add a description of the changes being made to the policy. This field is required.

6. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

Advanced options

Option	Description	Default
auto-asic-offload	Enable or disable policy traffic ASIC offloading.	enable
comments	Add a description of the policy, such as its purpose, or the changes that have been made to it. A comment added here will overwrite the comment added in the above *Comments* field.	none
uuid	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000
traffic-shaper	Select the traffic shaper to apply to traffic forwarded by the multicast policy. This option is only available in an IPv4 multicast policy.	none

Create a new local-in policy

The section describes how to create new IPv4 and IPv6 local-in policies to control inbound traffic that is going to a FortiGate interface.

See Local-in policy in the FortiOS Administration Guide for more information.



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.

To create a new local-in policy:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *IPv4 Local In Policy* or *IPv6 Local In Policy*.
4. Click *Create New*.
5. Enter the following information:

Option	Description
Interface	Select the interface.
Source Address	Select souce addresses, address groups, virtual IPs, and virtual IP groups.
Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
Service	Select services and service groups.
Schedule	Select a one-time schedule, recurring schedule, or schedule group.
Action	Select an action for the policy to take: *DENY* or *ACCEPT*.
HA Management Interface Only	Enable to dedicate the interface as an HA management interface. This option is only available for IPv4 policies.
Change Note	Add a description of the changes being made to the policy. This field is required.

6. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

Create a new traffic shaping policy

The section describes how to create new traffic shaping policies.

See Traffic shaping in the FortiOS Administration Guide for more information.



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.

To create a new traffic shaping policy:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *Traffic Shaping Policy*. If you are in the Global Database ADOM, select *Traffic Shaping Header Policy* or *Traffic Shaping Footer Policy*.

4. Click *Create New*.
5. Enter the following information:

Option	Description
IP Version	Select the IP address version: *IPv4* or *IPv6*.
Name	Enter a unique name for the policy. Each policy must have a unique name.
Status	*Enable* or *Disable* this policy.
Comments	Add a description of the policy, such as its purpose, or the changes that have been made to it.
If Traffic Matches:	
Source Internet Service	*Enable or disable source internet service, then select services.* This option is only available when the *IP Version* is *IPv4*.
Source Address	Select source addresses, address groups, virtual IPs, and virtual IP groups. This option is only available when *Source Internet Service* is off.
Source User	Select source users. This option is only available when *Source Internet Service* is off.
Source User Group	Select source user groups. This option is only available when *Source Internet Service* is off.
Destination Internet Service	Turn destination internet service on or off, then select services.
Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups. This option is only available when *Destination Internet Service* is off.
Schedule	Select a one-time schedule, recurring schedule, or schedule group.
Service	Select services and service groups. This option is only available when *Destination Internet Service* is off.
Application	Select applications.
Application Category	Select application categories.
Application Group	Select application groups.
URL Category	Select URL categories.
Type of Service	Specify the type of service (ToS) hexidecimal value.
Type of Service Mask	Specify the hexidecimal mask to be matched against the ToS.
Then:	

Option	Description
Action	Select the action to take if traffic matches: *Apply Shaper* or *Assign Group*.
Outgoing Interface	Select outgoing interfaces.
Shared Shaper	Select a shared traffic shaper. This option is only available when *Action* is set to *Apply Shaper*.
Reverse Shaper	Select a reverse traffic shaper. This option is only available when *Action* is set to *Apply Shaper*.
Per-IP Shaper	Select s per-IP traffic shaper. This option is only available when *Action* is set to *Apply Shaper*.
Traffic Shaping Class ID	Select the shaping class to which this traffic should be assigned. This option is only available when *Action* is set to *Assign Group*.
Differentiated Services	Enable or disable application of a differentiated services tag to a packet's DiffServ value, then enter the tag.
Differentiated Services Reverse	Enable or disable application of a differentiated services tag to a packet's reverse DiffServ value, then enter the tag.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the *FortiOS CLI Reference*.
Change Note	Add a description of the changes being made to the policy. This field is required.

6. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

Advanced options

Option	Description	Default
srcintf	Select one or more incoming interfaces.	none
tos-negate	Enable or disable negation of the ToS value.	disable
uuid	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000

Create a new authentication rule

The authentication rule defines the sources and destination that require authentication and what authentication scheme is applied.



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.

To configure an authentication rule:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *Authentication Rules*.
4. Click *Create New*.
5. Enter the following information:

Option	Description
Name	Enter a unique name for the policy. Each policy must have a unique name.
Source Address	Select source addresses, address groups, virtual IPs, and virtual IP groups.
Protocol	Select the protocol this rule applies to.
Authentication Scheme	Select or create a new authentication scheme. For more information on authentication schemes, see the FortiOS Administration Guide.
IP-based Authentication	Enable or disable IP-based authentication.
SSO Authentication Scheme	Select or create a new authentication scheme for single sign-on.
Comments	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the *FortiOS CLI Reference*.
Change Note	Add a description of the changes being made to the policy. This field is required.

6. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

Advanced options

Option	Description	Default
dstaddr	Select an IPv4 destination address. Required for web proxy authentication.	none

Option	Description	Default
dstaddr6	Select an IPv6 destination address. Required for web proxy authentication.	none
srcintf	Select the incoming (ingress) interface.	none
transaction-based	Enable or disable transaction-based authentication.	disable
transaction-based	Enable or disable web authentication cookies.	disable
web-portal	Enable or disable the web portal for proxy transparent policy	disable

Create a new hyperscale policy

In FortiManager, you can create hyperscale policies by configuring the policy package's policy offload level to *Full Offload*. For more information on hyperscale firewalls, see the FortiGate Administration Guide.



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.

To use hyperscale policies in a policy package:

1. Go to *Policy & Objects* in supported a ADOM version on FortiManager.
2. Create a new policy package, or right click an existing policy package from the tree menu, and select *Edit*.
3. Under the *Policy Offload Level* option, select *Full Offload*, and click *OK*.
   Hyperscale policy types enabled in *Feature Visibility* are now available in the policy package.

To configure a hyperscale policy:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package, click the selected hyperscale policy.
4. Click *Create New*. The *Create New Policy* pane opens.
5. Configure the hyperscale policy settings:

Name	Enter a name for the policy.
Incoming Interface	Select the incoming interface.
Outgoing Interface	Select the outgoing interface.
Source Address	Select the source address.
Destination Address	Select the destination address.
Service	Select services and service groups.
Action	Select an action for the policy to take: *ACCEPT* or *DENY*.

Comments	Optionally, enter comments about the policy.
Advanced Options	Expand to view advanced options for the policy.

When configuring a *Hyperscale Policy*, there are fields to define IPv4 and IPv6 source addresses and destination addresses.

6. Click *OK* to create the policy. By default, policies will be added to the bottom of the list.

Create a new NAC policy

This section describes how to create a new FortiSwitch network access control (NAC) policy.

You can create a NAC policy that matches devices with the specified criteria, devices belonging to a specified user group, or devices with a specified FortiClient EMS tag. Devices that match the policy are assigned to a specific VLAN or have port-specific settings applied to them.

For more information about NAC, see FortiSwitch network access control in the FortiSwitch Administration Guide.

NAC policies can be created whether the FortiSwitch is in central management mode or per-device management mode, and the changes are saved to the FortiGate database.

You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.

To create a NAC policy:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *NAC Policy*.
4. Click *Create New*.
5. Enter the following information:

Option	Description
Name	Enter a unique name for the policy. Each policy must have a unique name. This field is required.
Status	Set the policy to *Enabled* or *Disabled*.
FortiLink Interface	Use the search field to find and select the FortiLink interface.
FortiSwitch Groups	Select *All* or *Specify* the FortiSwitch groups.
Description	Add a description of the policy, such as its purpose, or the changes that have been made to it.

Option	Description
Device Patterns	
Category	Select *Device*, *User*, *EMS Tag* or *Vulnerability*. *Vulnerability* is only available in 7.4 and later ADOMs. For *Device* pattern fields, you can use the wildcard * character when entering the value to be matched.
MAC Address	Enable or disable matching a MAC address, then enter a MAC address. Only available if *Category* is *Device*.
Hardware Vendor	Enable or disable matching a hardware vendor, then enter a hardware vendor name. Only available if *Category* is *Device*.
Device Family	Enable or disable matching a device family, then enter a device family name. Only available if *Category* is *Device*.
Type	Enable or disable matching a device type, then enter a device type. Only available if *Category* is *Device*.
Operating System	Enable or disable matching an operating system, then enter an operating system. Only available if *Category* is *Device*.
User group	Select a user group. Only available if *Category* is *User*.
FortiClient EMS Tag	Select a FortiClient EMS tag. Only available if *Category* is *EMS Tag*.
Severity	Configure the severity number (0 = Info, 1 = Low, 2 = Medium, 3 = High, 4 = Critical). Only available if *Category* is *Vulnerability*.
Switch Controller Action	
Assign VLAN	Enable to select a VLAN interface for the switch controller action.
Bounce Port	Enable or disable the bounce port.
Assign device to dynamic address	Enable to use a dynamic firewall address for matching a device, then select the address. For more information, see To create a dynamic firewall address for the NAC policy.
Wireless Controller Action	
Assign VLAN	Enable to select a VLAN interface for the wireless controller action.
Revision	
Change Note	Add a description of the changes being made to the policy. This field is required.

6. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

To create a dynamic firewall address for the NAC policy:

1. Go to *Policy & Objects* > *Firewall Objects* > *Addresses*.
2. Click *Create New*.
3. From the *Type* dropdown, select *Dynamic*.
4. For the *Sub Type* field, select *Switch Controller NAC Policy Tag*.
5. From the *Interface* dropdown, select the FortiLink interface.
6. Configure the other options, as needed.
7. Click *OK* to save the dynamic firewall address.
   You can now use the dynamic firewall address in a NAC policy through the *Assign device to dynamic address option*. The dynamic firewall address will be included when the NAC policy is deployed.

Create a new FortiProxy firewall policy



FortiProxy firewall policies are only available in FortiProxy ADOMs. See FortiProxy ADOMs on page 926.

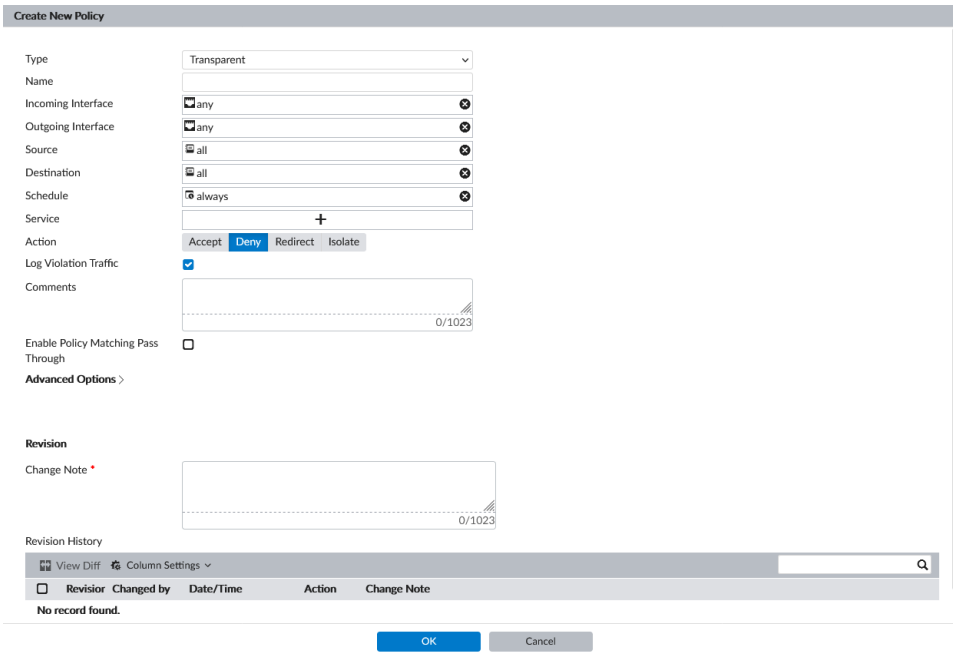
For more information on configuring a FortiProxy firewall policy, see the FortiProxy Administration Guide on the Fortinet Document Library.

In FortiManager, you can create FortiProxy policies while in a FortiProxy ADOM.

To create a new FortiProxy policy:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *FortiProxy Policy*.

4. Click *Create New*.



5. Enter the following information:

Type	Select the policy type from *Explicit*, *Transparent*, *FTP*, *SSH Tunnel*, *SSH Proxy*, and *Wanopt*.
Name	Enter a name for the policy.
Incoming Interface	Select the incoming interface(s) from the object selector pane.
Outgoing Interface	Select the outgoing interface(s) from the object selector pane.
Source	Select the source.
Destination	Select the destination.
Schedule	Select the schedule.
Service	Click the plus icon to add services to the policy, and then add services from the service selector pane.
Action	Select a policy action. Available actions include *Accept*, *Deny*, *Redirect*, and *Isolate*. Depending on which option is selected, additional settings are available. For more information, see the FortiProxy Administration Guide on the Fortinet Document Library.
Enable Policy Matching Pass Through	Check the box to enable policy matching pass through.

6. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

Create a new FortiProxy proxy auto-configuration (PAC) policy

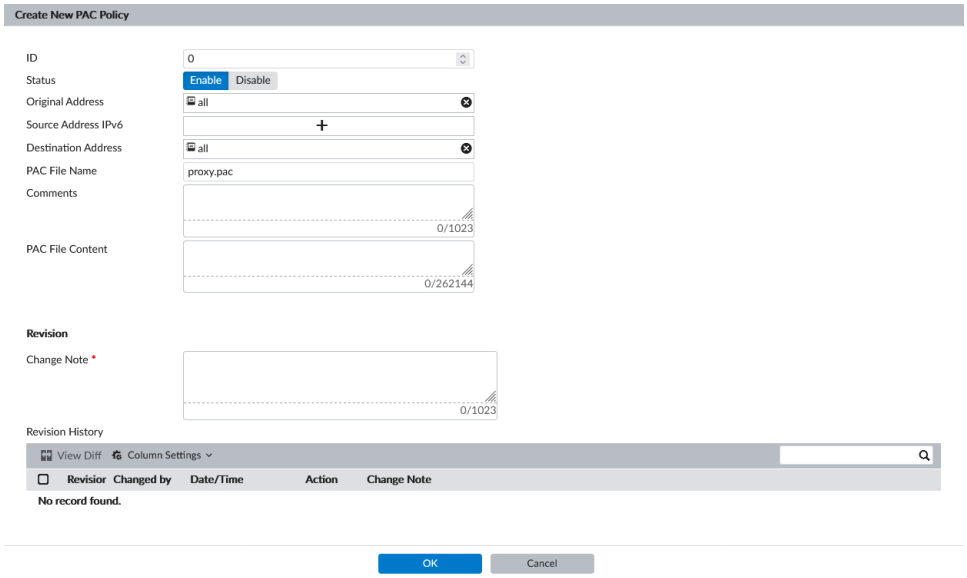
Proxy auto-configuration (PAC) policies are only available in FortiProxy ADOMs. See FortiProxy ADOMs on page 926.

For more information on configuring a PAC policy, see the FortiProxy Administration Guide on the Fortinet Document Library.

You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.

To create a PAC policy:

1. Ensure that you are in a FortiProxy ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Select *Firmware Visibility* from the *Tools* dropdown, and add a check mark next to the *PAC Policy* type.
4. In the tree menu for the policy package in which you will be creating the new policy, select *PAC Policy*.
5. Click *Create New*.



6. Enter the following information:

ID	Enter a policy ID or leave the field as the default to automatically assign a policy ID.
Status	*Enable* or *Disable* the policy.
Original Address	Select the original address.
Source Address IPv6	Optionally, provide the source IPv6 address.
Destination Address	Select the destination address.

PAC File Name	The name of the PAC file.
Comments	Optionally, provide comments.
PAC File Content	Enter the PAC file content. For more information, see the FortiProxy Administration Guide on the Fortinet Document Library.

7. Click *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number. By default, policies will be added to the bottom of the list, but above the implicit policy.

Editing policies

Policies can be edited in a variety of different way, often directly on the policy list.



The name of the admin who last modified the policy will be displayed in the *Last Modified* field along with the timestamp.

To edit a policy:

Select a policy and select *Edit* from the *Edit* menu, or double-click on a policy, to open the *Edit Policy* pane.

You can also edit a policy inline using the object pane (either the *Object Selector* frame or the *Object Configurations* pane when dual pane is enabled), the right-click menu, and by dragging and dropping objects. See Using the object selector on page 502 and Drag and dropping objects on page 503.

The right-click menu changes based on the cell or object that is clicked on. When available, selecting *Add Object(s)* opens the *Add Object(s)* dialog box, where one or more objects can be selected to add to the policy, or new objects can be created and then added. Selecting *Remove Object(s)* removes the object from the policy.

To clone a policy:

Select a policy, and from the *Edit* menu, select *Clone*. The *Clone Policy* dialog box opens with all of the settings of the original policy. Edit the settings as required and select *OK* to create the clone.

To Clone Reverse a policy:

Select a policy, and from the *Edit* menu, select *Clone Reverse*. Alternatively, you can also select *Clone Reverse* from the right-click context menu.

The policy is cloned with the *Incoming Interface* and *Outgoing Interface* switched with each other. The *Source* and *Destination* are also switched with each other.

The policy is cloned without a name. Click the *Name* for the policy and specify a name.



A policy cloned using the Clone Reverse option is disabled for security. The administrator can enable the policy after reviewing the settings.

When NAT is enabled for a policy, Clone Reverse is disabled.

To copy, cut, or paste a policy or object:

You can copy, cut, and paste policies. Select a policy, and from the *Edit* menu, select *Cut* or *Copy*. When pasting a copied or cut policy, you can insert it above or below the currently selected policy.

You can also copy, cut, and paste objects within a policy. Select an object in a cell, or select multiple objects using the control key, then right-click and select *Copy* or *Cut*. Copied or cut objects can only be pasted into appropriate cells; an address cannot be pasted into a service cell for example.

A copied or cut policy or object can be pasted multiple times without having to be recopied.

To delete a policy:

You can delete a policy. Select a policy, and select *Delete*. When deleting a policy, you will see the *Confirm Deletion* pane which displays information about the selected policies to be deleted. Click *OK* to confirm the deletion.

To add a section:

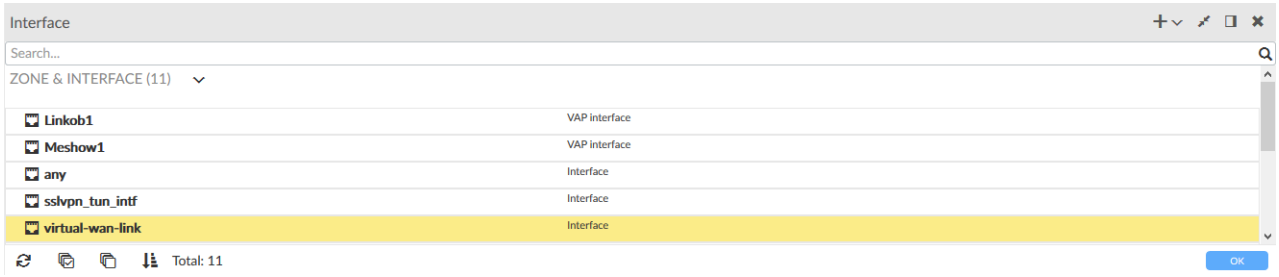
You can use sections to help organize your policy list. Policies can also be appended to sections.

Select a policy, and from the *Section* menu, click *Add*. Type a section name, and click *OK* to add a section to the currently selected policy.

Using the object selector

The *Object Selector* frame opens when a cell in the policy list is selected.

The *Object Selector* frame is only available when *Display Policy & Objects in Dual Pane* is disabled. See Feature visibility on page 413.



Create New	Click the create new dropdown list, then select the object type to make a new object. See Creating objects on page 533.
Collapse / Expand All	Expand or collapse all of the object groups shown in the pane.

Dock to bottom / right	Move the *Object Selector* frame to the bottom or right side of the content pane.
Close	Close the *Object Selector* frame.
Search	Enter a search term to search the object list.
Refresh	Refresh the list.
Select All	Select all objects in the list.
Deselect All	Deselect all objects in the list.
Sort	Sort the object list alphabetically.

Objects can be added or removed from the selected cell by clicking on them, and then selecting OK to apply the change and close the *Object Selection* pane.

Objects can also be dragged and dropped from the pane to applicable, highlighted cells in the policy list.

Right-click on an object in the pane to *Edit* or *Clone* the object, and to see where it is used. See Edit an object on page 536 and Clone an object on page 538.

Drag and dropping objects

On the *Policy & Objects > Policy Packages* pane, objects can be dragged and dropped from the object pane, and can also be dragged from one cell to another, without removing the object from the original cell.

One or more objects can be dragged at the same time. When dragging a single object, a box beside the pointer will display the name of the object being dragged. When dragging multiple objects, the box beside the pointer will show a count of the number of objects that are being dragged. To select multiple objects, click them while holding the control key on your keyboard.

The cells or columns that the object or objects can be dropped into will be highlighted in the policy package pane. After dropping the object or objects into a cell or column, the object will immediately appear in the cell as part of the policy, or in all the cells of that column.

Installing policies to specific devices

Policies can be configured to install only to specific installation targets within the policy package. This allows a single policy package to be applied to multiple different types of devices. For example, FortiGate and FortiWiFi devices can share the same policy, even though FortiGate devices do not have WiFi interfaces.

To install a policy only to specific devices:

1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu, select the policy package
4. Select *Column Settings > Install On* from the content pane toolbar.
5. Click *Installation Targets* in the *Install On* column of the policy that will be applied to specific devices.
6. In the *Object Selector* frame, select the devices that the policy will be installed on (see Policy package installation targets on page 422), then click *OK*.

The policy will now be installed only on the selected installation targets, and not the other devices to which the policy package is assigned.

Configuring policy details

Various policy details can be configured directly from the policy tables, such as the policy schedule, service, action, security profiles, and logging.

To edit a policy schedule with dual pane disabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
4. In the *Schedule* column, click the cell in the policy that you want to edit. The *Object Selector* frame is displayed.
5. In the *Object Selector* frame, locate the schedule object, then drag and drop the object onto the cell in the *Schedule* column for the policy that you want to change.
6. Click *OK* to close the *Object Selector* frame.

To edit a policy schedule with dual pane enabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
4. In the object pane, go to *Firewall Objects* > *Schedules*.
5. Locate the schedule object, then drag and drop the object onto the cell in the *Schedule* column for the policy that you want to change.

To edit a policy service with dual pane disabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
4. In the *Service* column, click the cell in the policy that you want to edit. The *Object Selector* frame opens.
5. In the *Object Selector* frame, locate the service object, and then drag and drop the object onto the cell in the *Service* column for the policy that you want to change.
6. Click *OK* to close the *Object Selector* frame.

To edit a policy service with dual pane enabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
4. In the object pane, go to *Firewall Objects* > *Services*. The services objects are displayed in the content pane.

5. Locate the service object, then drag and drop the object onto the cell in the *Service* column for the policy that you want to change.

To edit a services object:

1. Go to *Policy & Objects > Object Configuration*.
2. In the tree menu, go to *Firewall Objects > Services*. The services objects are displayed in the content pane.
3. Select a services object, and click *Edit*. The *Edit Service* dialog box is displayed.
4. Configure the following settings, then click *OK* to save the service. The custom service will be added to the available services.

Name	Edit the service name as required.
Comments	Type an optional comment.
Service Type	Select *Firewall* or *Explicit Proxy*.
Show in service list	Select to display the object in the services list.
Category	Select a category for the service.
Protocol Type	Select the protocol from the dropdown list. Select one of the following: *TCP/UDP/SCTP*, *ICMP*, *ICMP6*, or *IP*.
IP/FQDN	Type the IP address or FQDN. This menu item is available when *Protocol* is set to *TCP/UDP/SCTP*. You can then define the protocol, source port, and destination port in the table.
Type	Type the service type in the text field. This menu item is available when *Protocol* is set to *ICMP* or *ICMP6*.
Code	Type the code in the text field. This menu item is available when *Protocol* is set to *ICMP* or *ICMP6*.
Protocol Number	Type the protocol number in the text field. This menu item is available when *Protocol Type* is set to *IP*.
Advanced Options	For more information on advanced option, see the *FortiOS CLI Reference*.
check-reset-range	Configure ICMP error message verification. • `disable`: The FortiGate unit does not validate ICMP error messages. • `strict`: If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) | TCP(C,D) header, then if FortiManager can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. If it is enabled, the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the `anti-replay` option checks packets. • `default`: Use the global setting defined in `system global`. This field is available when *Protocol* is *TCP/UDP/SCTP*.

		This field is not available if *explicit-proxy* is enabled.
	Color	Click the icon to select a custom, colored icon to display next to the service name.
	session-ttl	Type the default session timeout in seconds. The valid range is from 300 - 604 800 seconds. Type `0` to use either the `per-policy session-ttl` or `per-VDOM session-ttl`, as applicable. This is available when *Protocol* is *TCP/UDP/SCTP*.
	tcp-halfclose-timer	Type how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded.The valid range is from 1 to 86400 seconds. Type `0` to use the global setting defined in `system global`. This is available when *Protocol* is *TCP/UDP/SCTP*.
	tcp-halfopen-timer	Type how many seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded. The valid range is from 1 to 86400 seconds. Type `0` to use the global setting defined in `system global`. This is available when *Protocol* is *TCP/UDP/SCTP*.
	tcp-timewait-timer	Set the length of the TCP TIME-WAIT state in seconds.As described in RFC 793, the "...TIME-WAIT state represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request." Reducing the length of the TIME-WAIT state means the FortiGate unit can close terminated sessions faster, which means that more new sessions can be opened before the session limit is reached. The valid range is 0 to 300 seconds. A value of 0 sets the TCP TIME-WAIT to 0 seconds. Type `0` to use the global setting defined in `system global`. This is available when *Protocol* is *TCP/UDP/SCTP*.
	udp-idle-timer	Type the number of seconds before an idle UDP connection times out.The valid range is from 1 to 86400 seconds. Type `0` to use the global setting defined in `system global`. This is available when *Protocol* is *TCP/UDP/SCTP*.

To edit a policy action:

1. Select desired policy type in the tree menu.
2. Select the policy, and from the *Edit* menu, select *Edit*.
3. Set the *Action* option, and click *OK*.

To edit policy logging:

1. Select desired policy type in the tree menu.
2. Right-click the *Log* column, and select options from the menu.

To edit policy security profiles with dual pane disabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
4. In the *Security Profiles* column, click the cell in the policy that you want to edit. The *Object Selector* frame is displayed.
5. In the *Object Selector* frame, locate the profiles, then drag and drop the object onto the cell in the *Security Profiles* column for the policy that you want to change.
6. Click *OK* to close the *Object Selector* frame.

To edit policy security profiles with dual pane enabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
4. In the object pane, go to *Security Profiles*.
5. Locate the profile object, then drag and drop the object onto the cell in the *Security Profiles* column for the policy that you want to change.



The policy action must be *Accept* to add security profiles to the policy.

Reverting a Policy to a previous version

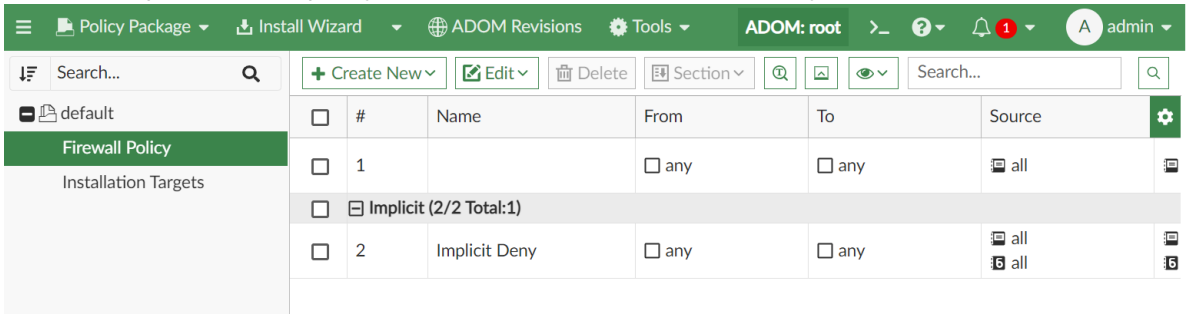
When a policy is created or edited, the history of the change is saved as a revision. You can view a policy's revisions in the *Revision History* table when editing the policy.

Select a revision from the table and then click *Revert* to revert the policy to the selected revision.

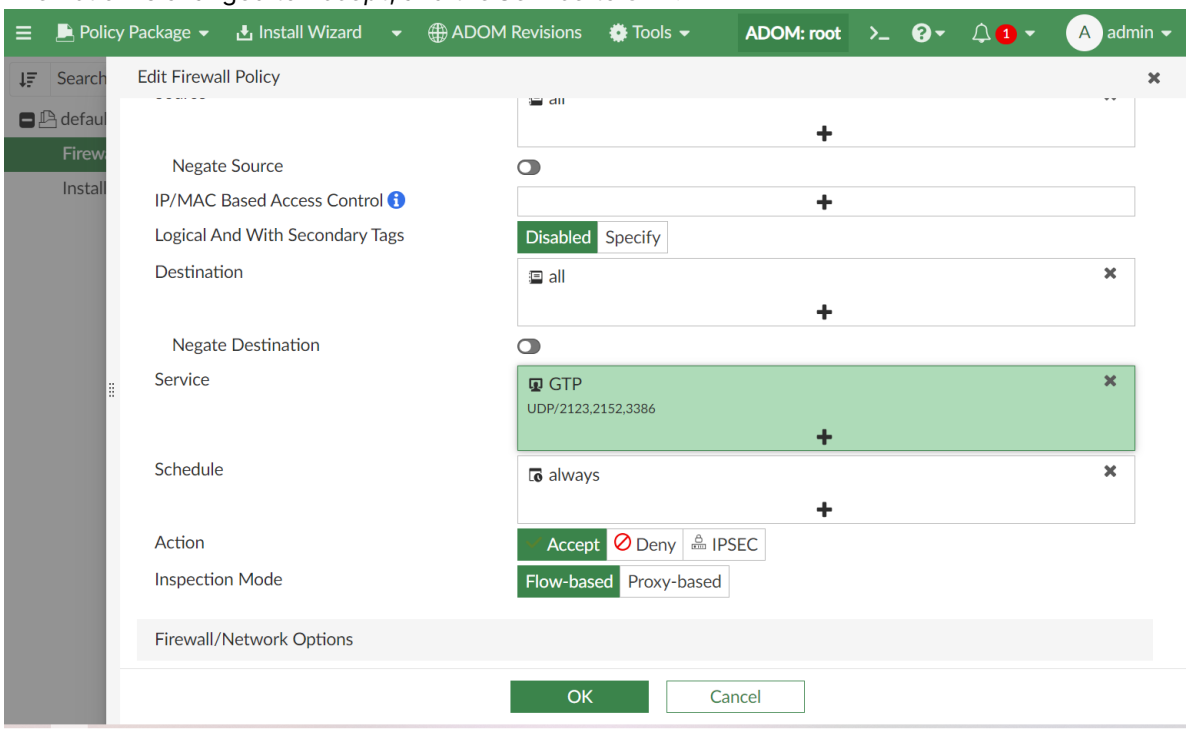
The example below demonstrates how you can revert a policy to a previous version.

To revert a policy to a previous version:

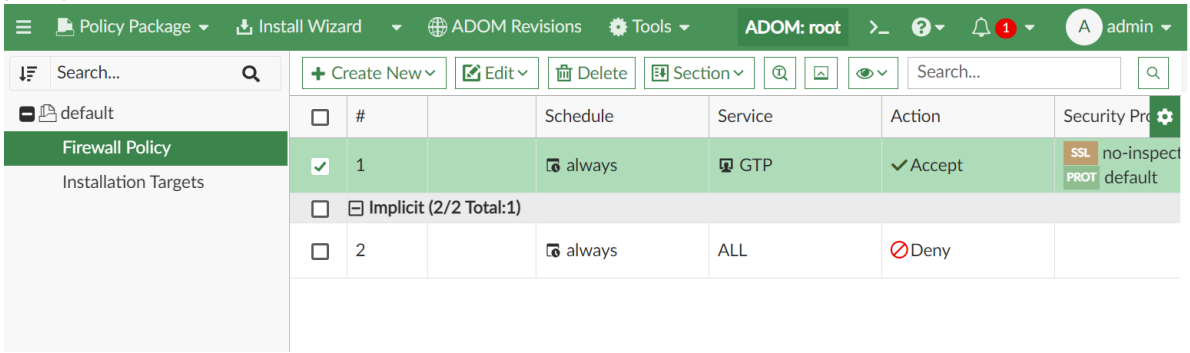
1. Create a new policy.
   In this example, a firewall policy is created with the action set to *Deny*.



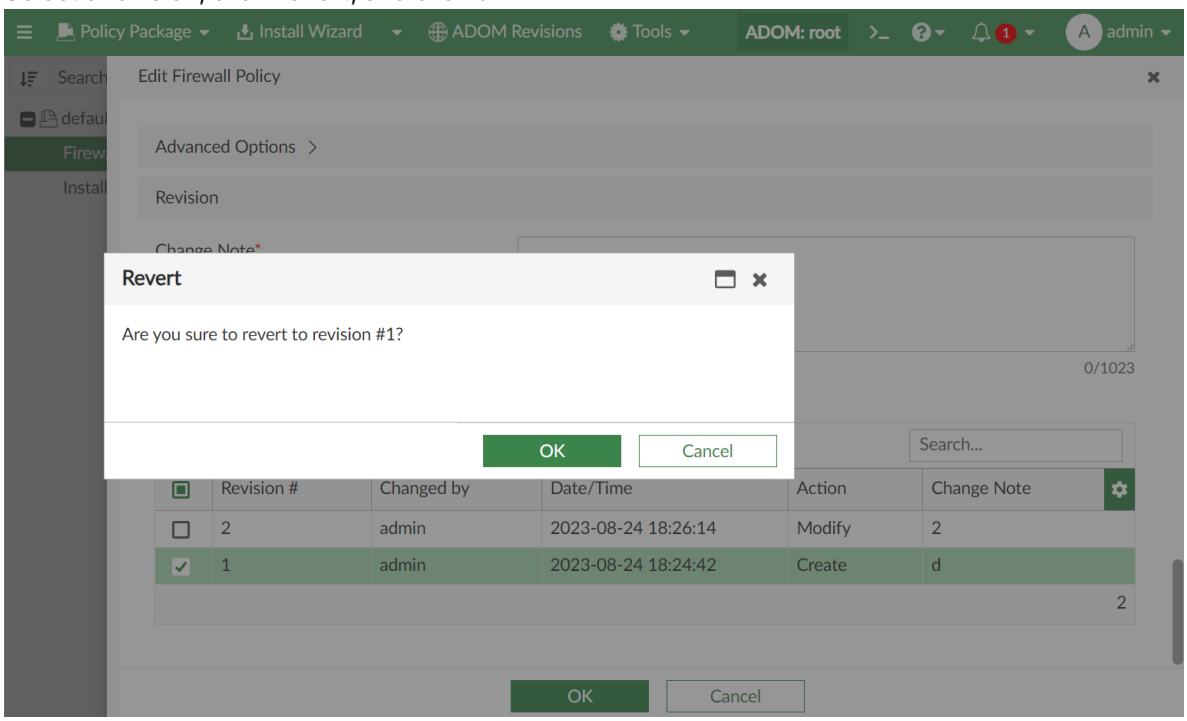
2. Edit the policy, and save the changes.
   The *Action* is changed to *Accept*, and the *Service* to *GTP*.



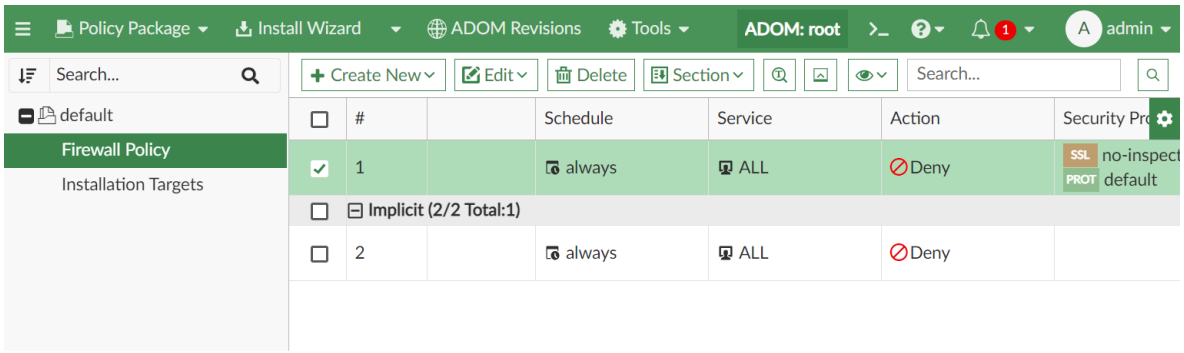
3. Edit the policy again, and review the *Revision History* log. You can see that revisions were added when the policy was created and edited.



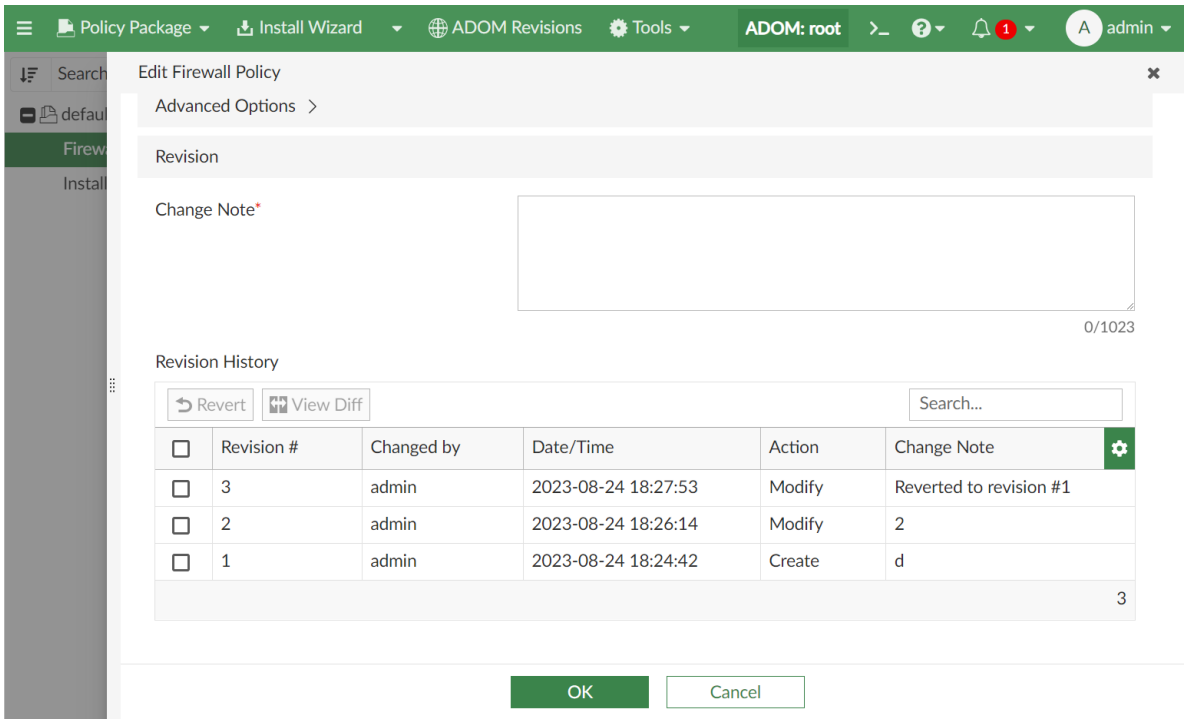
4. Select a revision, click *Revert*, and click *OK*.



The policy is reverted to the previous state. In this example, the policy is reverted to use the Deny action and the GTP service is removed.



A new revision is added to the table to log the change with the note "Reverted to revision #".



Viewing policies

You can view policies in the following ways:

- Column options on page 510
- Policy search and filter on page 512
- Policy hit count on page 513
- Viewing unused policies on page 515
- Policy Lookup on page 516

Column options

The visible columns can be adjusted, where applicable, using the *Column Settings* menu in the content pane toolbar. The columns and columns filters available are dependent on the policy and the ADOM firmware version.

Click and drag an applicable column to move it to another location in the table.

Policy views

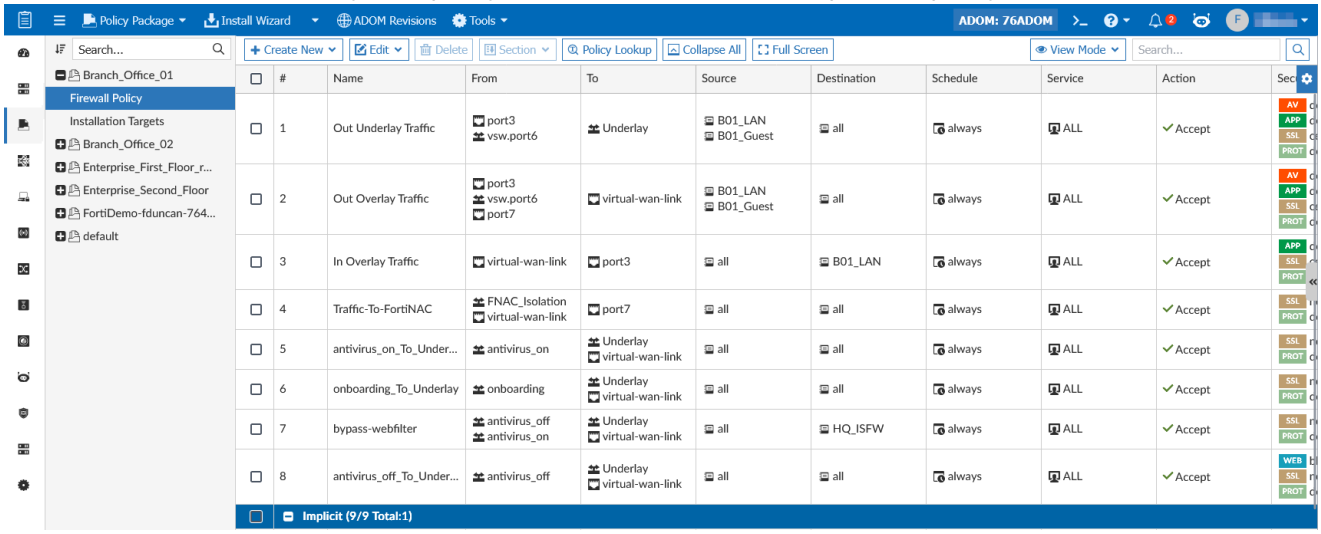
FortiManager supports the following policy view modes:

- By Sequence on page 511
- Interface Pair View on page 511

By Sequence

By Sequence displays policies in the order that they are checked for matching traffic without any grouping.

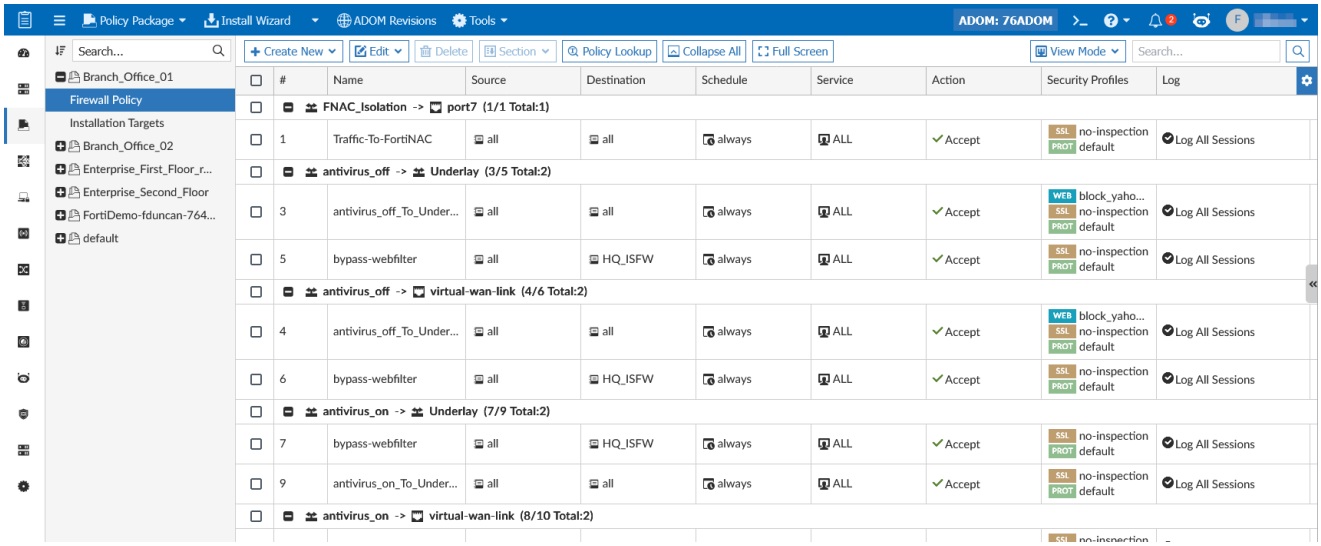
Policies can then be moved by their policy ID before or after another specified policy ID.



Interface Pair View

Interface Pair View displays the policies in the order that they are checked for matching traffic, grouped by the pairs of incoming and outgoing interfaces in collapsible sections.

The section names match the *Incoming Interface* and *Outgoing Interface* of the policy, therefore those fields (*To* and *From*) are not displayable as columns in the table.



The *Interface Pair View* can be used when a policy is configured with multiple interfaces. Policies with multiple *Incoming Interfaces* and/or *Outgoing Interfaces* are split into separate entries in the table so that each entry is displayed in a section with only one incoming interface and one outgoing interface. When editing an entry from *Interface Pair View*, all applicable incoming and outgoing interfaces are displayed as per normal.

For example, if a policy is created with the *Incoming Interface* of *port1* and *port2*, and the *Outgoing Interface* of *port3* and *port4*, the policy will be displayed in the table under four section names:

- *port1->port3*
- *port2->port3*
- *port1->port4*
- *port2->port4*

Policy search and filter

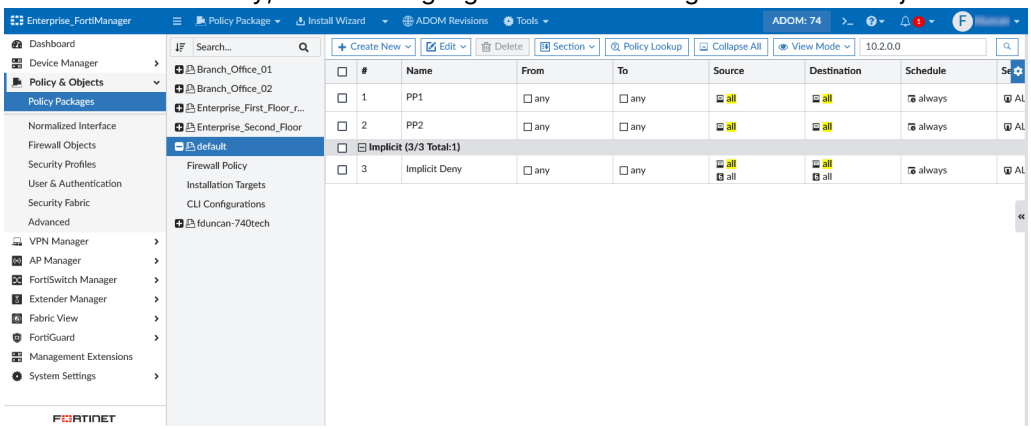
Go to *Policy & Objects* > *Policy Packages*, and use the search box to search or filter policies for matching rules or objects.

When searching for a VIP object defined as an IP range by the first or last IP in that range, search results will return the VIP object in the search results using either *Simple* and *Strict* search.

Simple search

The default *Simple Search* will highlight text that matches the string entered in the search field, including "all" objects.

For example, when searching for an IP address in a firewall policy, simple search will show results that include the IP address exactly, as well as highlight the fields configured with "all" objects.



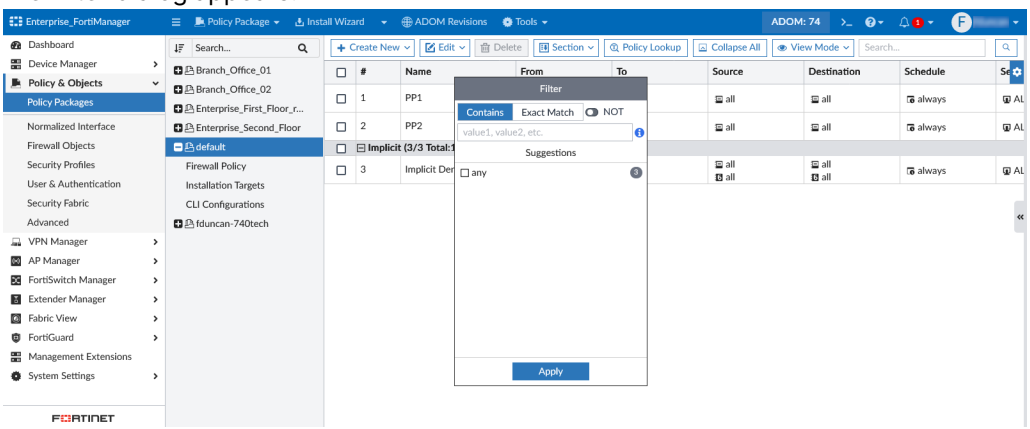
Strict search

You can enable *Strict Search* to display only results that match the exact search entered, excluding "all". *Strict Search* can be toggled on and off by clicking on the icon  next to the search field.

Column Filters

To add column filters:

1. Hover your mouse over a column header and select the filter icon. For example, in the *From* header. The *Filter* dialog appears.



2. In the *Filter* dialog, you can use the *Contains*, *Exact Match* and *NOT* options along with filter values to configure your filter.
   Suggested filter values appear in the *Suggestions* field. Multiple values can be OR'd together using ",".
3. Click *Apply* to apply the filter. Multiple column filters can be configured and applied simultaneously. When a column filter is applied, the filter icon appears in green.
   Select the filter icon and click *Remove* to remove a filter.

Policy hit count

You can use FortiManager to view FortiGate policy hit counters. When you run a policy check on a policy package or select the *Find Unused Policies* option from the *Tools* dropdown for a policy package, FortiManager shows hit count information for unused policies with zero hit count.

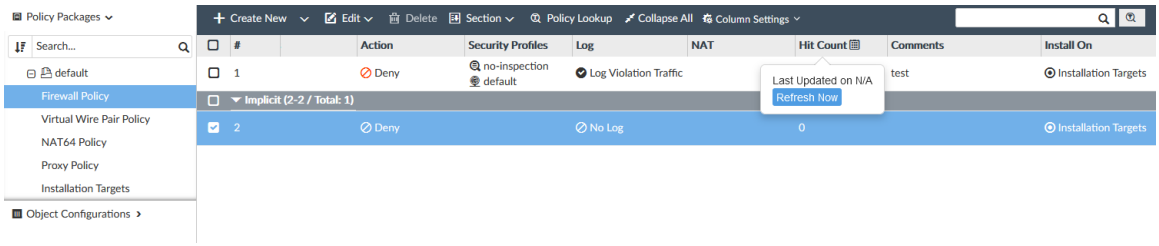


The *Find Unused Policies* option is unavailable when classic dual pane is enabled. To disable classic dual pane, go to *System Settings* > *Advanced* > *Advanced Settings*, and set the *Display Policy & Object in Classic Dual Pane* option to *Disable*.

In FortiManager, the policy hit counts are aggregated across all managed FortiGate units for the policy.

You can add policy hit count information to a policy package pane by enabling it in the *Column Settings* dropdown. The hit count is collected from managed FortiGate units when either the *Refresh Now* button in the *Hit Counts* column header or *Refresh Hit Counts* in the *Tools* dropdown is clicked.

The hit count information is excluded from the FortiManager event log, but it's included in the debug log for troubleshooting purposes.



To view policy hit counts:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for a policy package, select a policy. The content pane for the policy is displayed.
4. In the toolbar, click *Column Settings*, and enable the *Hit Count* column.
   Hit count information for each policy is displayed within the *Hit Count* column.
5. In the toolbar, click *Tools* > *Refresh Hit Counts* to fetch an updated hit count report, or hover your mouse over the *Hit Count* column header and click *Refresh Now*.

To view the hit count information for unused policies using the *Find Unused Policies* option:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the toolbar, from the *Tools* dropdown, select *Find Unused Policies*.
   The *Unused Policies* window opens.
4. In the tree menu, select the policy package, and expand the policy table of your choice in the content pane to see the hit count information for the unused policies only.
5. To view all the policies and their hit count information, select *No Filter* from the *Show Unused Policy* field.

To view hit count information for unused policies in the Policy Check Report:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu, right-click the policy package and select *Policy Check*.
   The *Policy Check* dialog opens.
4. In the *Policy Check* dialog, click *Perform Policy Check*, and then click *OK*.
   Once the policy check finishes, the results are displayed in the *Policy Check* window.
   The *Policy Check* window displays the hit count information for all the policies in a policy package.
5. Select the *Unused Only* checkbox to view the hit count information for the unused policies only.

Saving Last Used values

FortiManager can be configured to save the *Last Used* timestamp value which allows it to retain the timestamp if the hit count is reset on the managed device. This feature is disabled by default.

When enabled, FortiManager discards any *Last Used* values that it receives from managed devices that are blank or older than the currently stored value. Non-blank values that are more recent than the stored value will be updated and displayed.

To enable saved last used values:

1. In the FortiManager CLI, enter the following command to enable `save-last-hit-in-adomdb`.
```
config system global
   set save-last-hit-in-adomdb enable
end
```
2. Enter the following command to view the "Last Used" timestamp value in the CLI.
```
exe fmpolicy print-adom-packager <adom> <packageName> <policy-id>
```

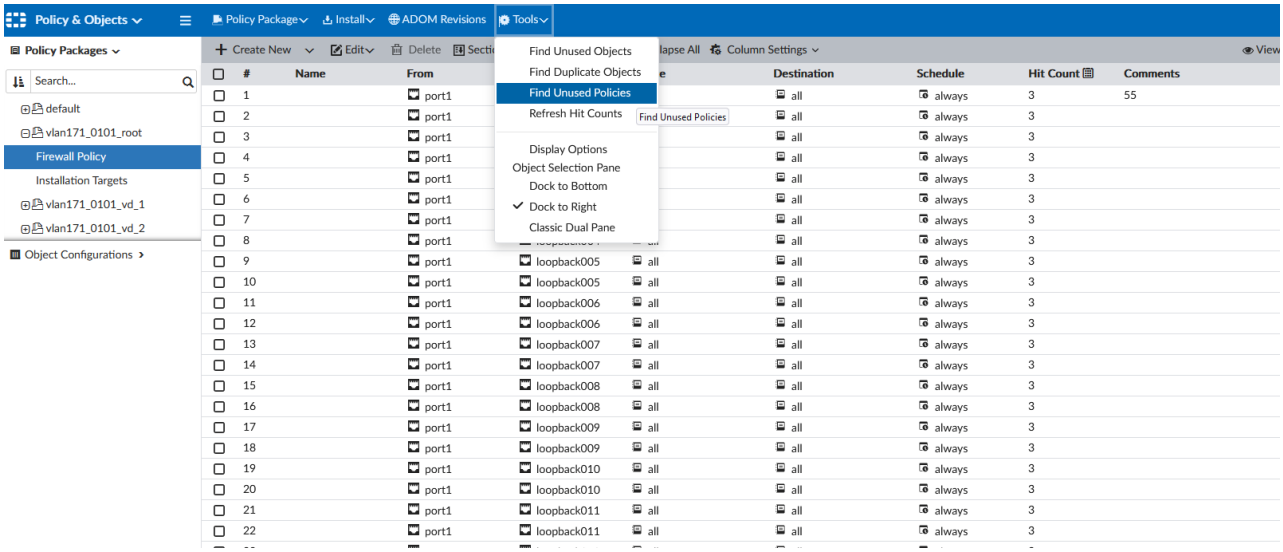
Viewing unused policies

Use the Unused polices report to view and delete unused policies.

You may filter the unused policies report by date range to find policies that have not been used within a particular date range.

To view the report:

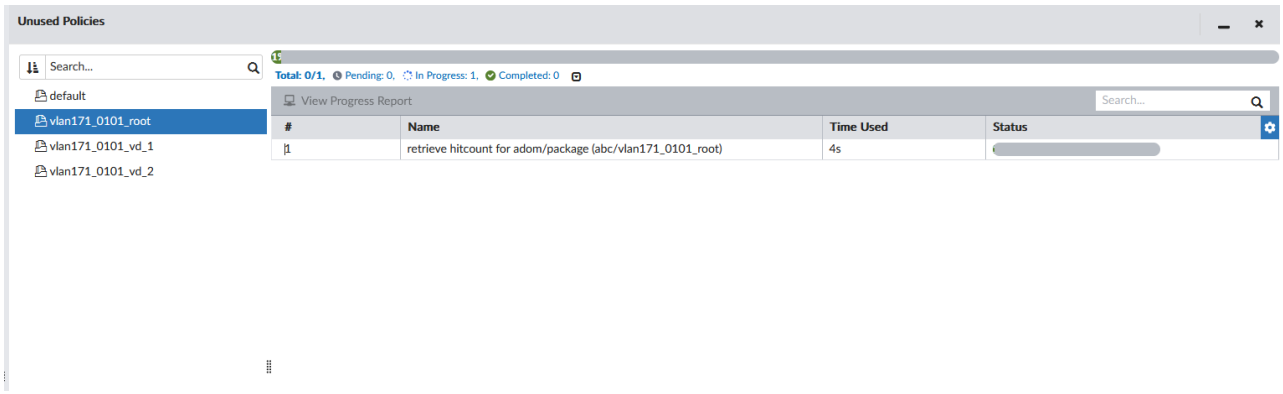
1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. From the *Tools* dropdown menu in the toolbar, select *Find Unused Policies*.



.

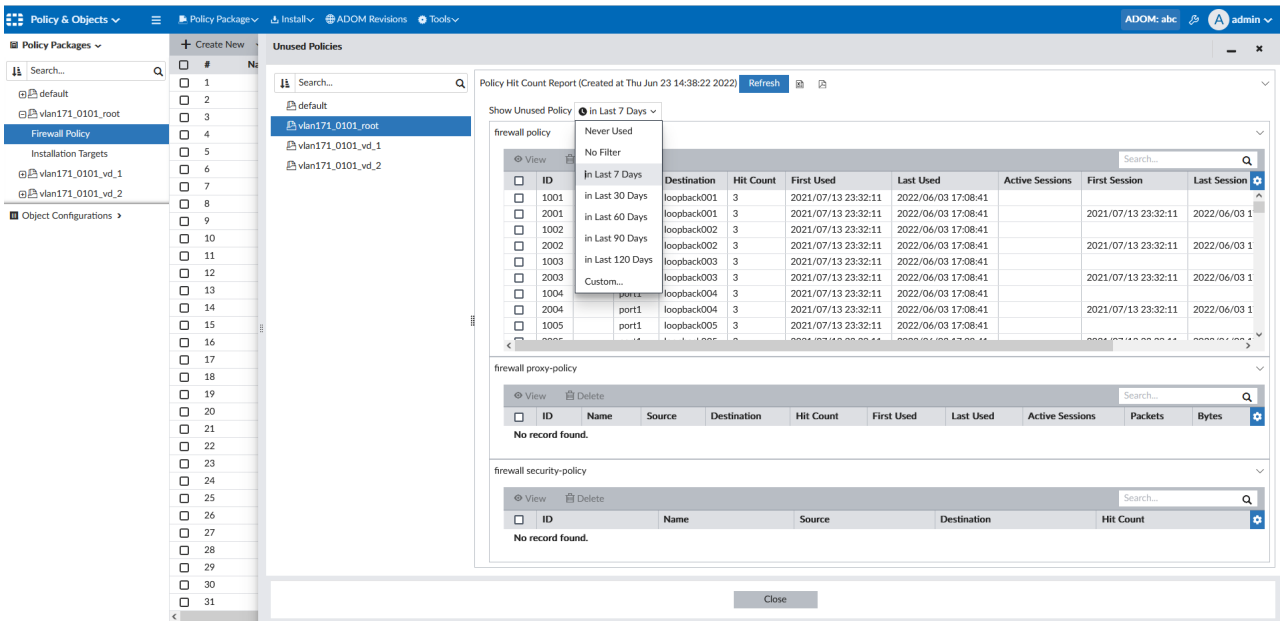
The *Unused Policies* window opens.

4. If needed, click the *Refresh* button to retrieve the hitcount data from the FGT. Wait for the process to finish.



To filter the report by timestamp:

1. In the *Show Unused Policy* dropdown menu, select the date range within which the report should be filtered.



Any policies that have not been used within this date range are displayed. For example, to find policies that have not been used in the last 60 days, select "in Last 60 Days" from the dropdown menu.

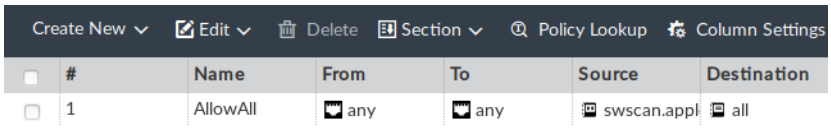
Policy Lookup

Policy Lookup allows you to search for policies on a FortiGate device or a VDOM based on certain parameters.

To perform a Policy Lookup:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for a policy package, select a policy type. For example, select *IPv4* policy.

4. Click *Policy Lookup*. The *IPv4 Policy lookup from remote device* dialog is displayed.



5. Select or specify the values for the following fields and click *OK* to search for a policy.

Device/VDOM	Select the FortiGate device or the VDOM from the drop-down.
Source Interface	Select the source interface from the drop-down.
Protocol	Select the protocol from the drop-down.
Protocol Number	Specify a number between 1 to 255.
Source	Specify the source IP address.
Destination	Specify the destination IP address or a Fully Qualified Domain Name (FQDN).

The Policy Lookup feature is available only for IPv4 and IPv6 policies.

FortiManager must be in sync with the FortiGate devices or VDOMs either by installing or importing the policy. If FortiManager is not in sync with the FortiGate devices, a message will be shown that the device is out of sync. You can still perform the policy lookup, but the results may not be accurate.

Using Policy Blocks

Policy Blocks are created to store multiple policies. Policy Blocks can be appended to a Policy Package. When creating a Policy Package, the administrator does not need to add one policy at a time. By appending a Policy Block to a Policy Package, the administrator can ensure that all policies in the Policy Block are added to the policy package together.

Policy Blocks can be used within the Global Database ADOM and appended to global header and footer poilicies, and then assigned to an ADOM's policies. With Policy Blocks, you can use policies across multiple Global Policy Packages. See Global policy packages on page 411.

You must enable Policy Blocks before you can use them. On the *Policy & Objects* pane, from the *Tools* menu, select *Feature Visibility*, and then select the *Policy Block* checkbox to display the option.

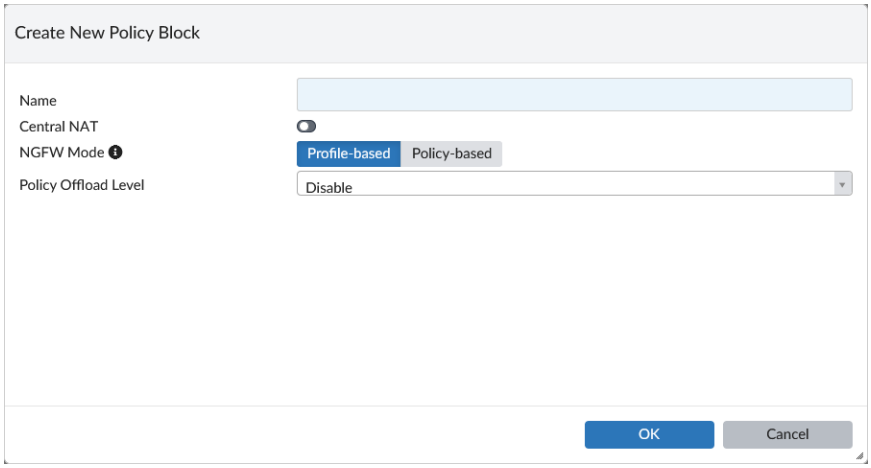
This topic includes the following sections:

- Creating Policy Blocks on page 518
- Editing Policy Blocks on page 519
- Adding policies to a Policy Block on page 520
- Appending a Policy Block to a Policy Package on page 521
- Installing Policy Blocks to target devices on page 522
- Using Policy Blocks versus Global Policy Packages on page 525
- Role-based access control for Policy Blocks on page 526
- Migrating global policies to policy blocks on page 526

Creating Policy Blocks

To create a new Policy Block:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. Right-click *Policy Blocks* and click *New*. The *Create New Policy Block* window opens. If *Policy Blocks* is not visible, you can enable it in *Feature Visibility*.



4. Configure the following details, then click *OK* to create the Policy Block.

Name	Enter a name for the new Policy Block.
Central NAT	Toggle *Central NAT* to *ON* to enable *Central SNAT* and *Central DNAT* policy types. This option is not available in the Global Database ADOM.
NGFW Mode	Select the NGFW mode, *Profile-based* (default) or *Policy-based*. This option is not available in the Global Database ADOM.
Policy Offload Level	Select the policy offload level. Available options include *Disable*, *Default*, *DoS Offload*, or *Full Offload*.

Editing Policy Blocks

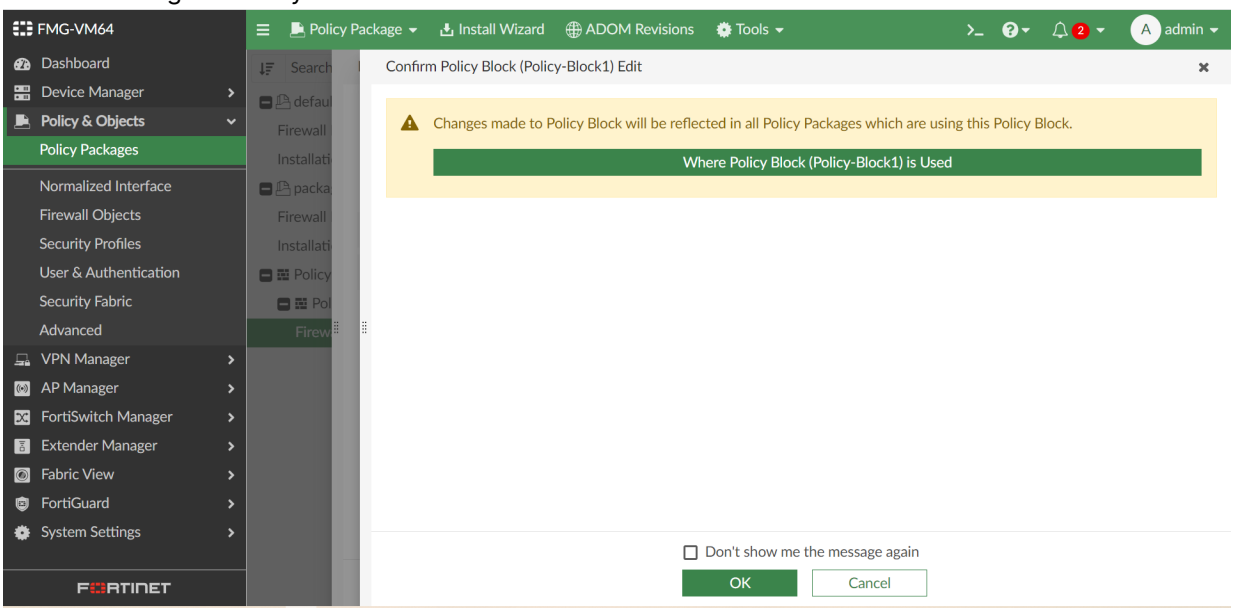
You can edit Policy Blocks from within the Policy Blocks section or from within a Policy Package.

Policy Blocks must be enabled in Policy & Object's *Feature Visibility* before they can be created and edited in an ADOM.

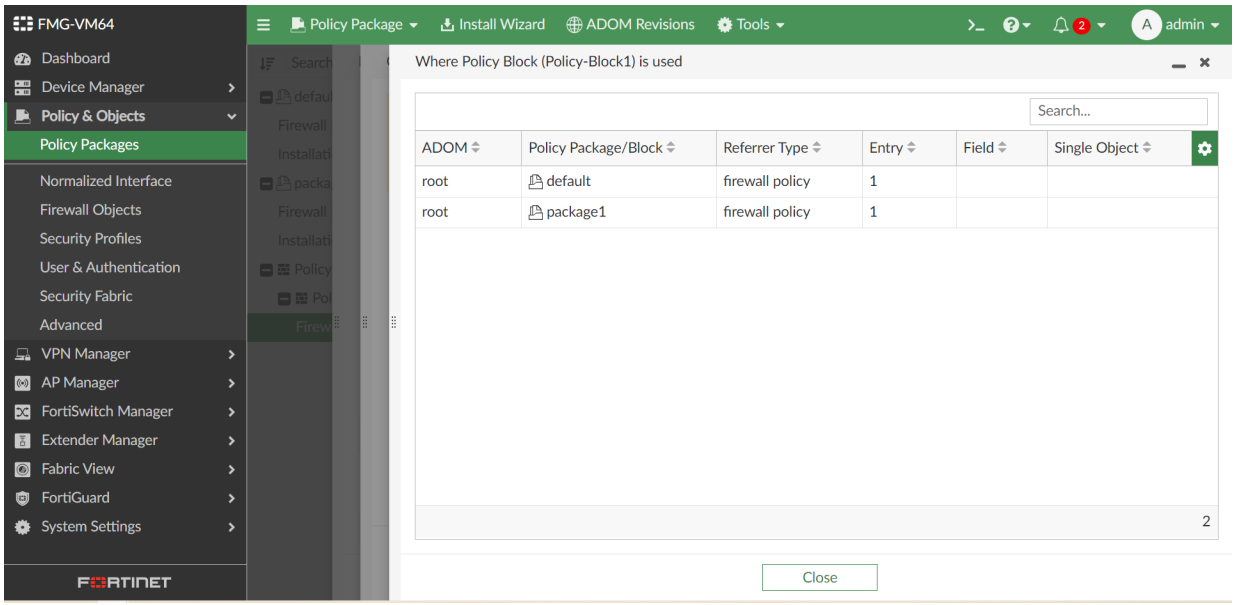
To edit a Policy Block:

1. Go to *Policy & Objects* > *Policy Packages* > *Policy Blocks* or select the Policy Block from within a Policy Package to which it is appended.
2. Double click on a Policy Block or select it from the table and click *Edit*.
3. Edit the details of the Policy Block, and click *OK*.

   A reminder message is displayed that changes to the Policy Block will be reflected in all Policy Packages which are using the Policy Block.



4. (Optional) Click on *Where Policy Block is Used* to see all Policy Packages to which the Policy Block is assigned.



Adding policies to a Policy Block

Policies can be added to a Policy Block in two ways. Create a new policy within a Policy Block or append an existing policy from a Policy Package to a Policy Block.

To create a new policy in a Policy Block:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. Go to *Policy Blocks* > *[Policy_Block_Name]*.
4. Click *Create New*. See Creating policies on page 429 for more information about how to create a new policy.

To copy a policy into a Policy Block:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. Click *[Policy_Package_Name]*. For example, click *default*.
4. Select one or more policies.
5. Right-click and select *Copy*.
6. Go to *Policy Blocks* > *[Policy_Block_Name]*.
7. Right-click and select *Paste*.

Once a policy is copied from an existing Policy Package (source) to a Policy Block (destination), it becomes an independent policy with no link to the original policy. Modifying or deleting the original policy will not affect the policy in the Policy Block.

Add a selection of existing policies to a Policy Block:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. Click *[Policy_Package_Name]*. For example, click *default*.
4. Select multiple policies within the policy package.
5. Right-click, and select *Add to Policy Block*. You have two choices:
   - *Add to Existing*: The selected policies will be added to the chosen existing policy block.
   - *Create New*: The selected policies will be added to a new policy block.

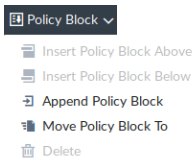
Appending a Policy Block to a Policy Package

Once a Policy Block is created, it can be appended to a Policy Package. After appending the Policy Block to a Policy Package, assigning installation targets and installing the Policy Package to the installation targets, all the policies in the Policy Block are installed to the target.

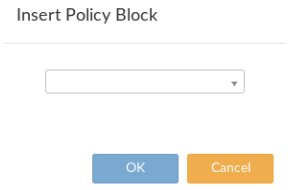
After a Policy Block is appended to a Policy Package, you can add or remove policies from the Policy Block. You need to append the Policy Block to the Policy Package only once. It is not required to append the Policy Block to the Policy Package again after adding or removing policies from the Policy Block.

To append an existing policy to a Policy Block:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. Click *[Policy_Package_Name]*. For example, click *default*.
4. Select *Policy Block* > *Append Policy Block*.



5. Select the Policy Block from the drop-down and click *OK*.

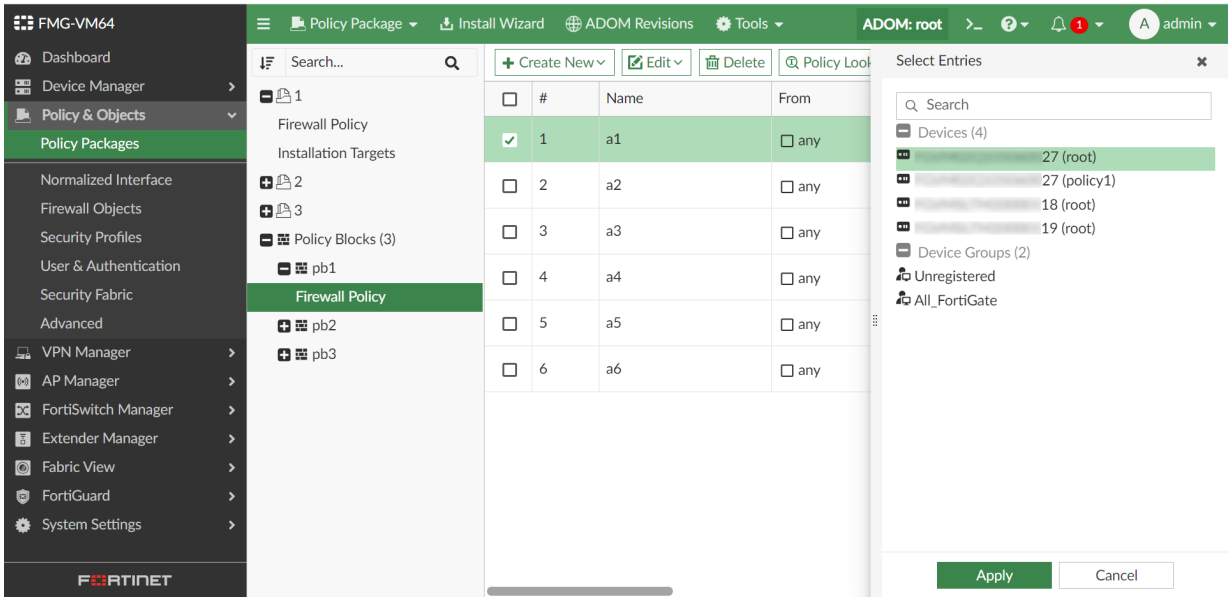


Deleting a Policy Block after it is appended to a Policy Package will automatically remove the Policy Block (and the included policies) from the Policy Package.

Installing Policy Blocks to target devices

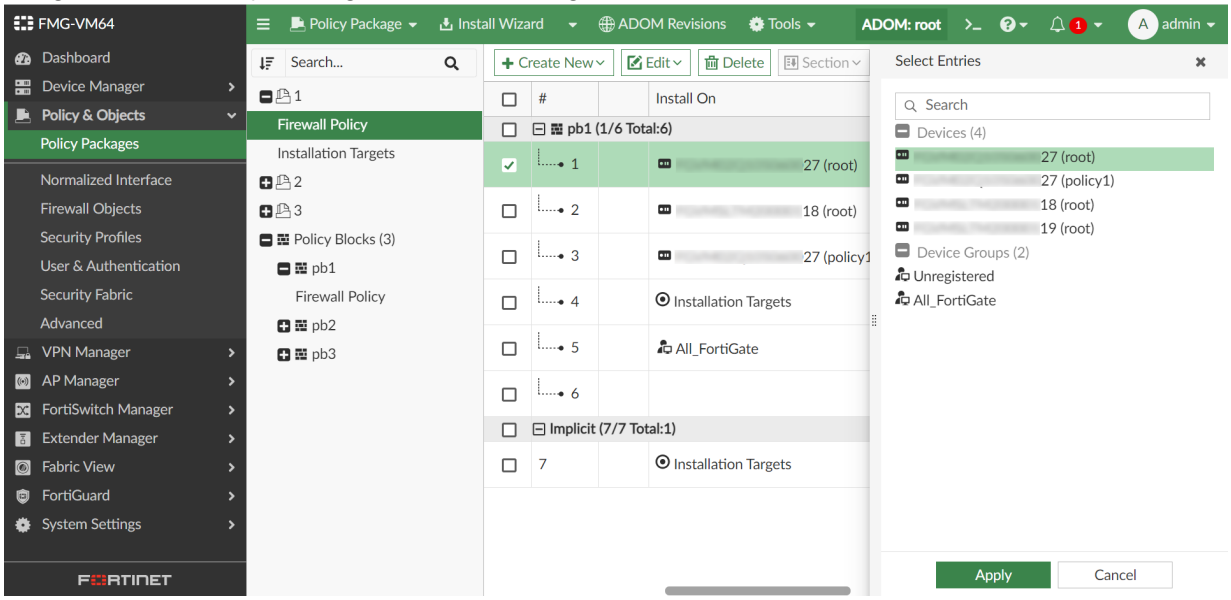
To install Policy Blocks to targets using *Install On*:

1. Go to *Policy & Objects* > *Policy Packages*.
2. From the *Tools* menu, select *Feature Visibility*, and enable *Policy Block*.
3. Install from the Policy Blocks menu:
   a. Select a Policy Block from the tree menu.
   b. Click the edit icon in the *Install On* column.
   c. Select the target device(s) for installation. You can select any installation targets.

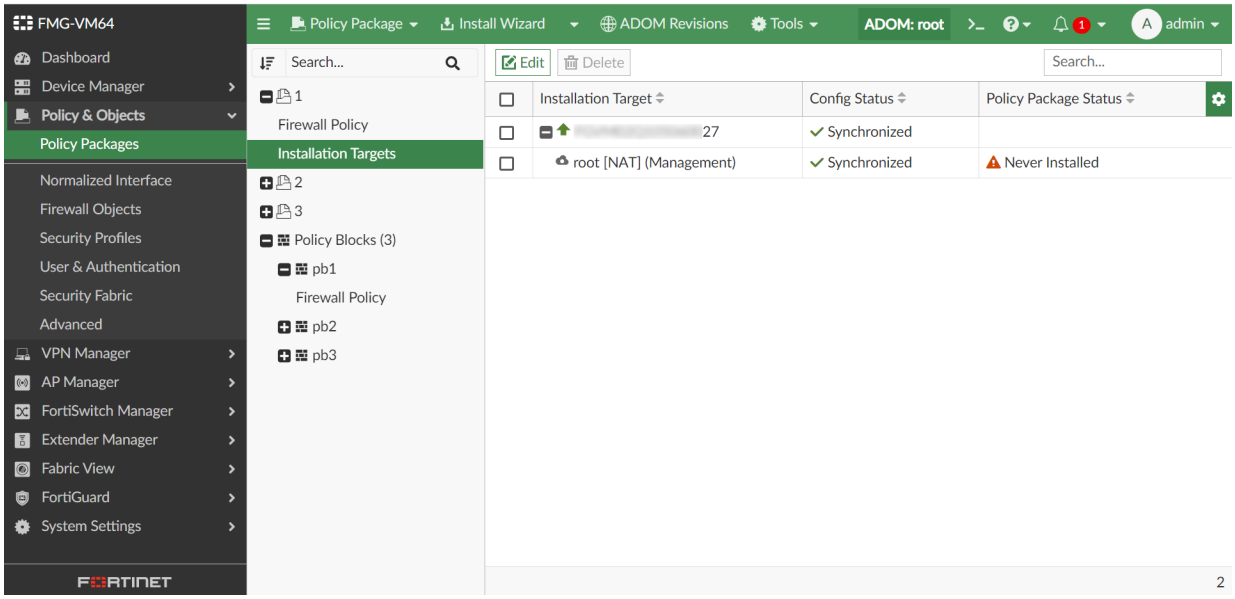


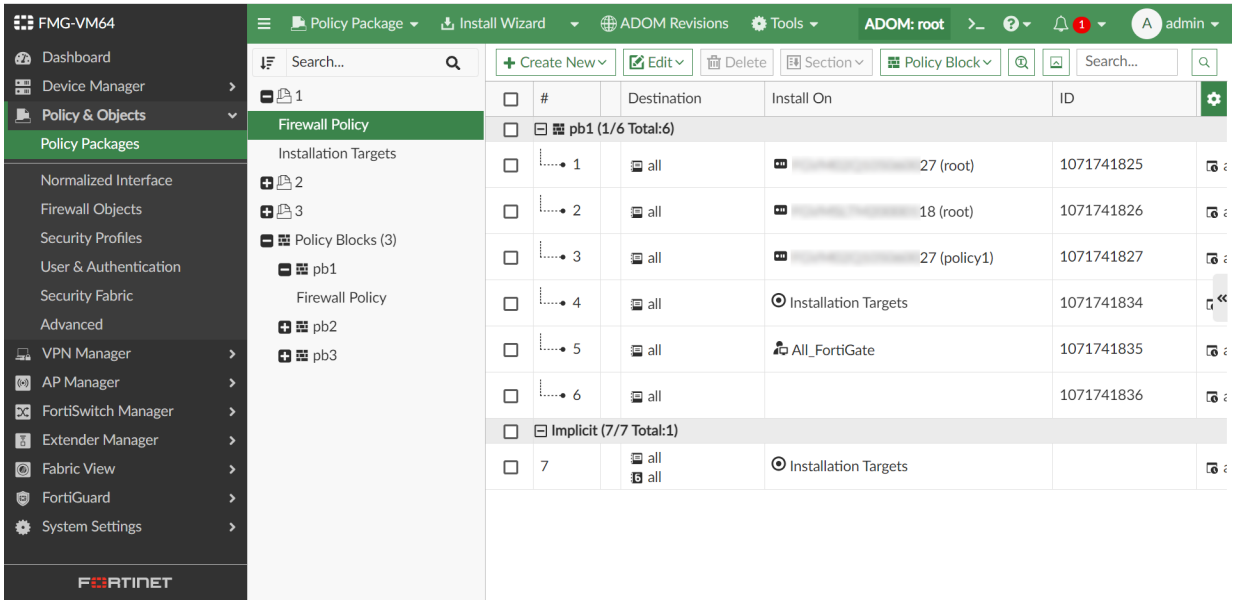
4. Install from the Policy Package:
   a. Go to a Policy Package where the Policy Block is installed, and select the Policy Block.
   b. Click the edit icon in the *Install On* column.

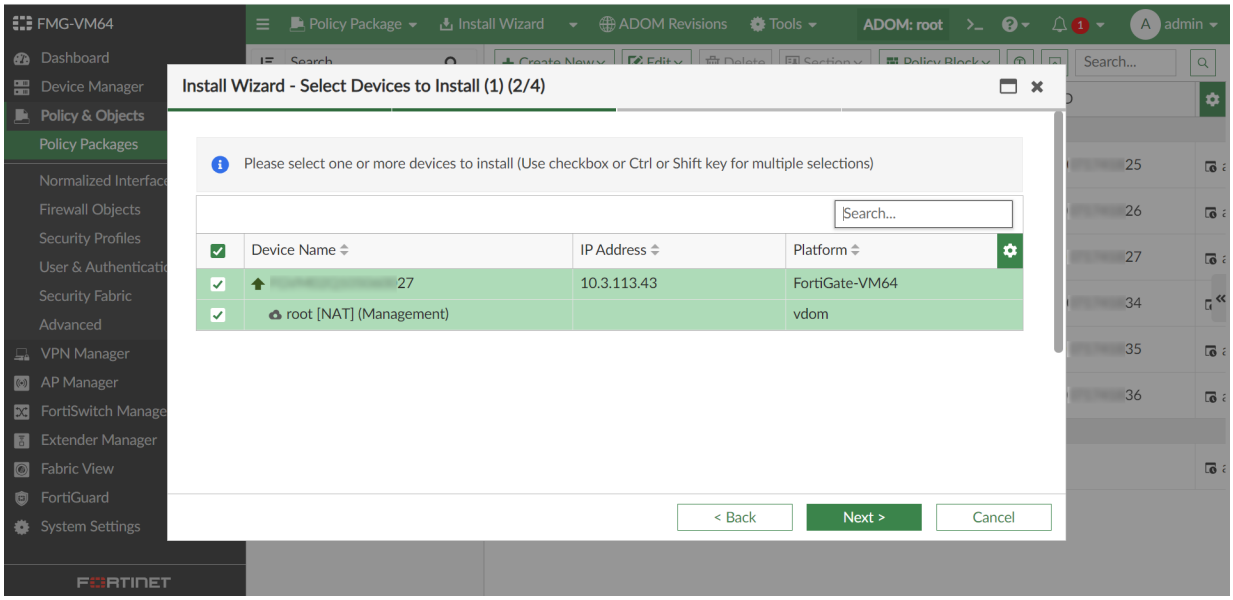
c. Select the target device(s) for installation. You can select any installation targets, including ones not assigned to the Policy Package's installation targets.



5. Click *Apply*, and install the Policy Block using Installation Targets. In the example below, Policy *a1*, *a4*, and *a5* are installed.







Below is the example copy log:

```
config firewall policy
   edit 1071741825
      set name "pb1-a1"
      set uuid 0722adfadea-729d-51ee-0fad-************
      set srcintf "any"
      set dstintf "any"
      set srcaddr "all"
      set dstaddr "all"
      set schedule "always"
      set service "ALL"
      set logtraffic all
   next
   edit 1071741834
      set name "pb1-a4"
      set uuid 99adsfadsf34e-7375-51ee-c3a4-************
```

```
            set srcintf "any"
            set dstintf "any"
            set srcaddr "all"
            set dstaddr "all"
            set schedule "always"
            set service "ALL"
            set logtraffic all
        next
        edit 1071741835
            set name "pb1-a5"
            set uuid 9ffdca46-7375-51ee-ca51-************
            set srcintf "any"
            set dstintf "any"
            set srcaddr "all"
            set dstaddr "all"
            set schedule "always"
            set service "ALL"
            set logtraffic all
        next
    end
```

Using Policy Blocks versus Global Policy Packages

The use of Policy Blocks over Global Policy Packages simplifies the process of upgrading your ADOMs in order to use policy features or objects introduced in later versions.

To upgrade a Global Database ADOM with Global Header and Footer policies, all of the local ADOMs that the Global Policy Package is assigned to must first be upgraded to the *same version or one version higher* than the desired Global Database ADOM version.

For example, to upgrade the Global Database ADOM to version 7.0, all of the local ADOMs and their managed devices making use of the Global Policy Package must be on version 7.0 or 7.2 before upgrading the Global Database ADOM. For more information, see Global database version on page 944.

In cases where some of the local ADOMs cannot be upgraded to a later version (for example, they include FortiGate devices that are unsupported on later versions), the Global Database ADOM would not be able to be upgraded.

Policy Blocks store multiple policies so they can be appended to a local Policy Package together to simplify the administration of a large number of policies. Because local Policy Blocks are configured per-ADOM, you only need to update the local ADOM where the Policy Blocks are stored. This means you don't need to worry about other ADOMs which may not be upgradable.

Policy Blocks are also supported in the Global Database ADOM, however, using Global Policy Blocks introduces the same upgrade limitations that exist when using Global Header and Footer Policies.

Example of upgrading the Global Database ADOM with Global Policy Packages:

1. Upgrade each local ADOM and its managed devices to the same or higher version as the desired Global Database ADOM version.
2. Upgrade the Global Database ADOM version.
3. Edit the Global Header and Footer policies
4. Re-assign the policies to the relevant ADOMs and then install the changes to your managed devices.

Example of upgrading local ADOMs with Policy Blocks:

1. Upgrade your local ADOM and its managed devices to the desired version.
2. Edit the policies included in the Policy Block as desired.
3. Install the changes to your managed devices.

To limit who is able to edit Policy Blocks, you can enable role-based access control settings for Policy and Objects in the desired ADOM. See Role-based access control for Policy Blocks on page 526

Migrating Global Policies to local Policy Blocks

Direct migration of Global Header and Footer policies to local policy blocks is not currently supported. To migrate Global Header and Footer policies from the Global Database ADOM into local policy blocks, you must manually recreate the policies in the local ADOM and then group them into a Policy Block. See Creating policies on page 429 and Creating Policy Blocks on page 518

Role-based access control for Policy Blocks

FortiManager supports role-based access control (RBAC) for Policy Packages and objects. In order to configure read-only access to Policy Blocks, an administrator profile must be created with *Read-Only* permissions for *Policy Packages & Objects*. This permission level limits the administrator to read-only permissions for all FortiManager policy and object configuration, including Policy Blocks.

For more information on configuring an administrator profile, see Creating administrator profiles on page 1015 and Permissions on page 1011.

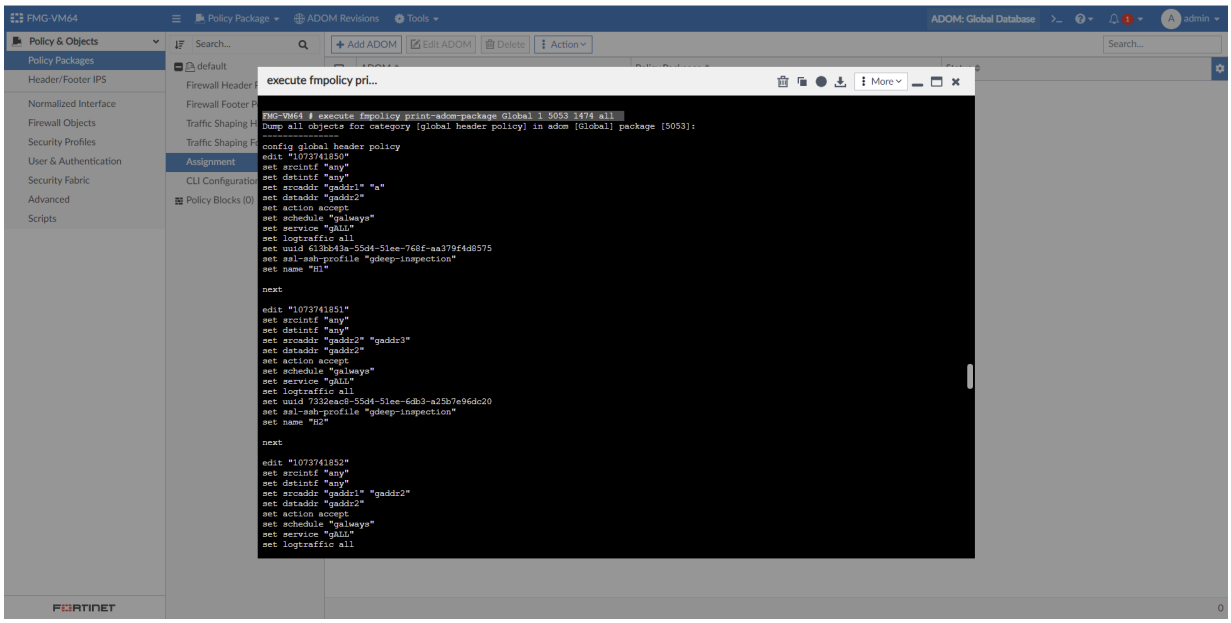
Migrating global policies to policy blocks

Existing global policies can be migrated to local policy blocks using the CLI to get the configuration and using FortiManager scripts to recreate the policies in a local ADOM.

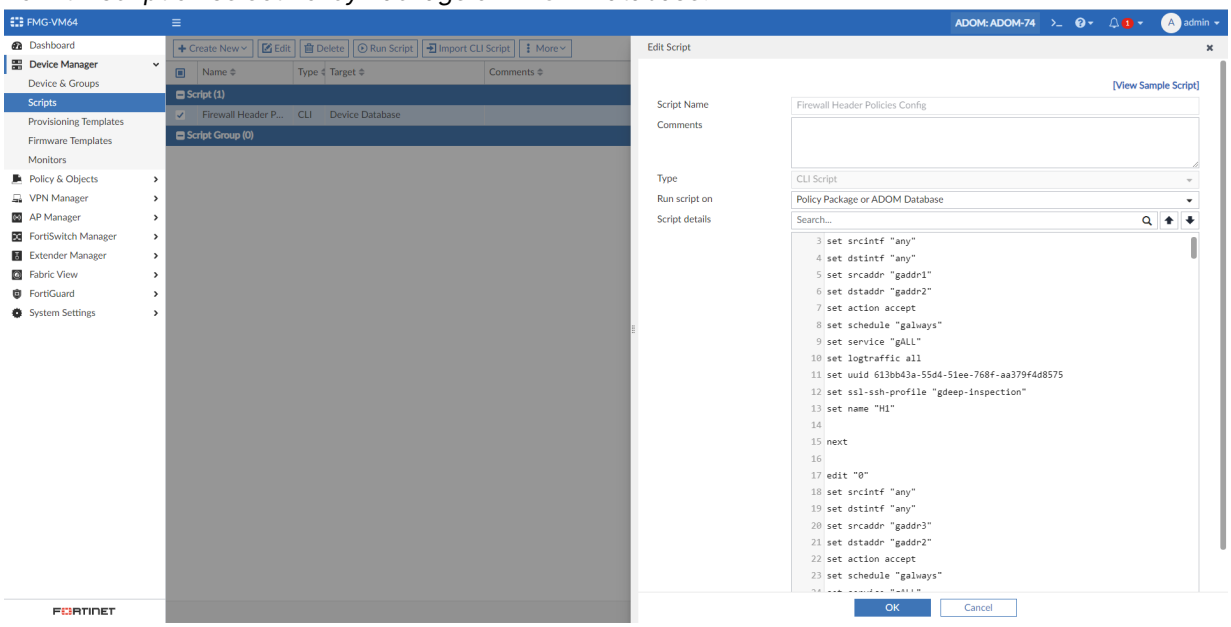
In the example below, the global policy package contains 20 firewall header and footer policies. These policies are assigned to a local ADOM and installed to FortiGate devices.

To migrate global policies to a Policy Block:

1. Get the header and footer policy configuration from the Global Database ADOM.
   a. Open the FortiManager CLI terminal and enter the following command to get the header policy configurations:
      ```
      execute fmpolicy print-adom-package Global 1 <package ID> 1474 all
      ```
   b. Copy the output from the script.
   c. Repeat these steps for the footer policy using the following command:
      ```
      execute fmpolicy print-adom-package Global 1 <package ID> 1476 all
      ```

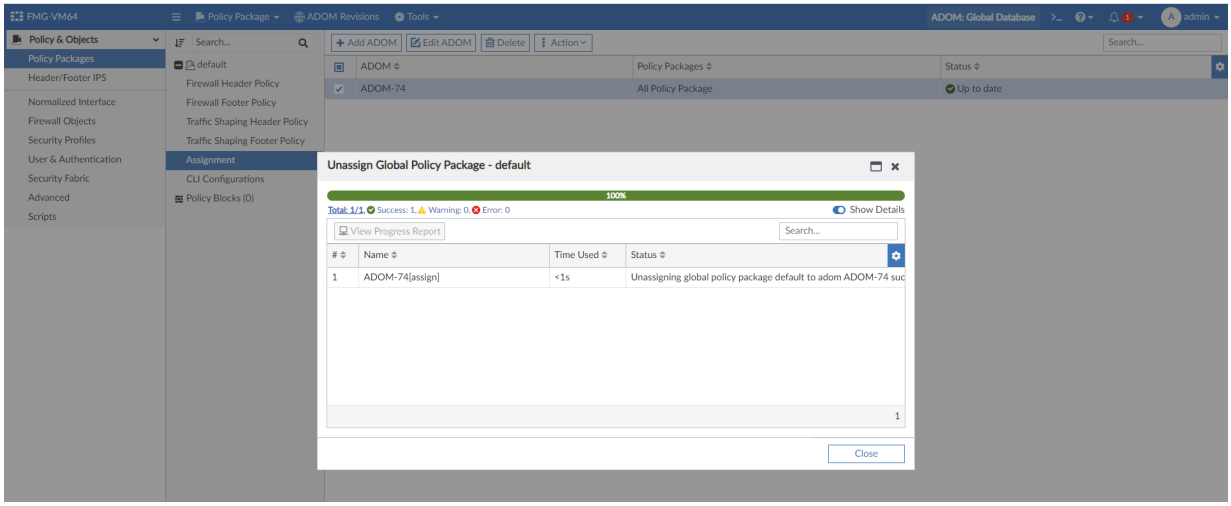


2. Save the policy configuration into FortiManager scripts in the local ADOM.
   a. In the local ADOM, go to *Device Manager* > *Scripts* and click *Create New* > *Script*.
   b. Paste the contents from the CLI output from the previous step into a separate header and footer script.
   c. In the pasted *Script Details*, change the *Policy ID* to `0` and change the script's first line from '`config global header policy`' to '`config firewall policy`' and save the changes, otherwise the local ADOM will not recognize when the script is run using global syntax and gives an error.
   d. For *Run script on* select *Policy Package or ADOM Database*.

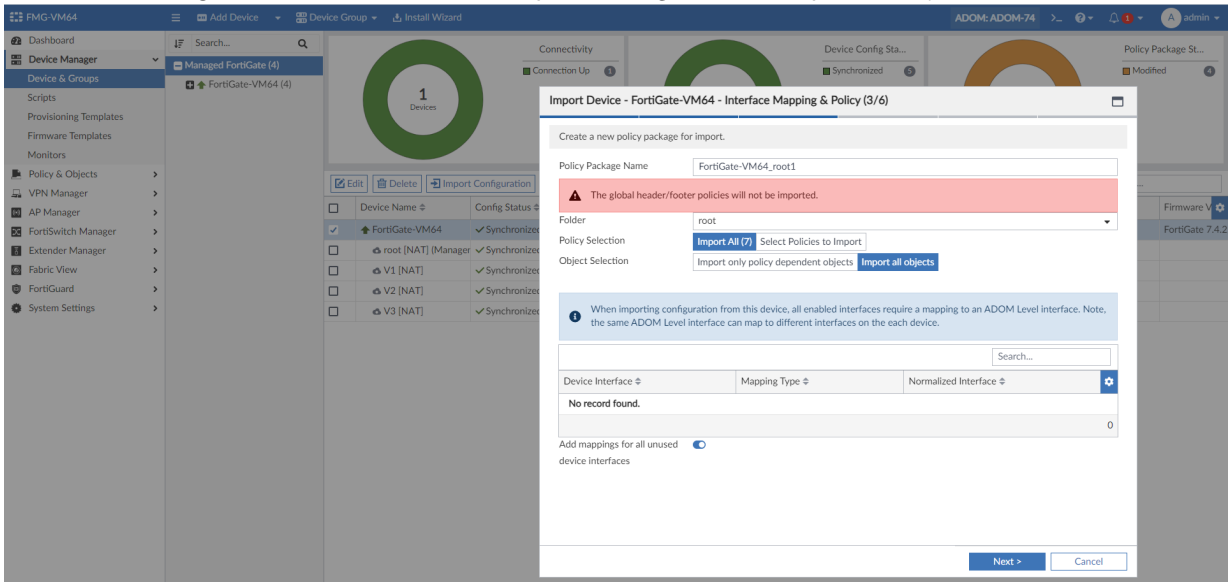


3. Unassign the global policy package. This removes the global configuration from the local ADOM so that you can re-create the policies as policy blocks using the configured script.

a. In the Global Database ADOM, go to *Policy & Objects* > *Policy Packages*.
b. Select the policy package and click *Action* > *Unassign*.

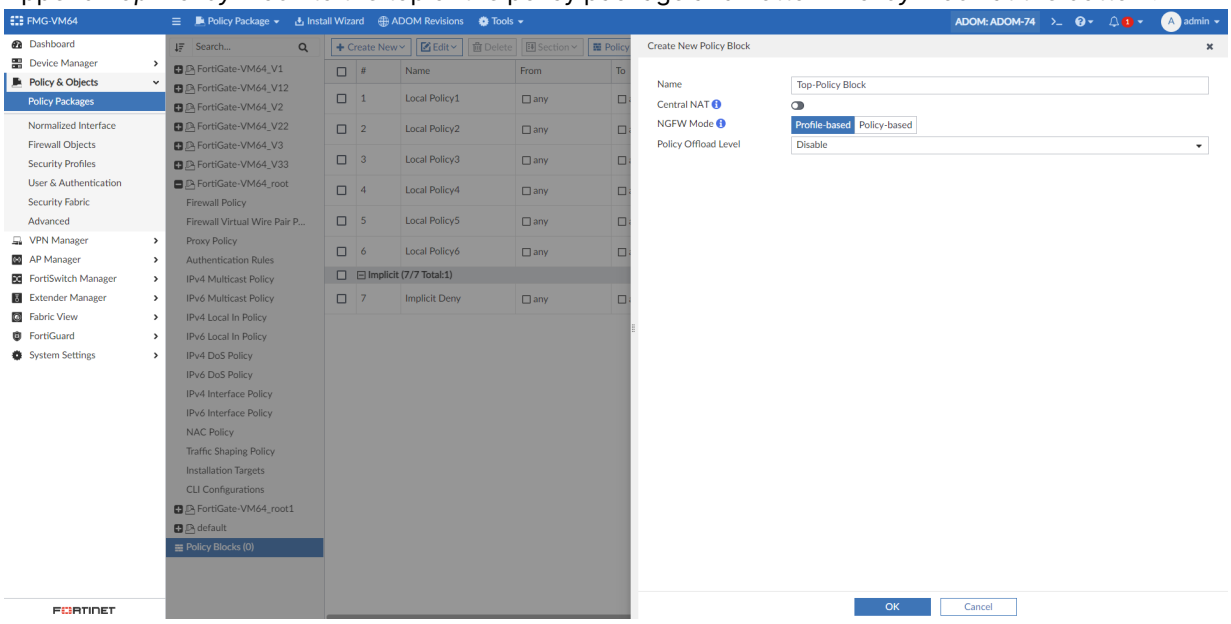


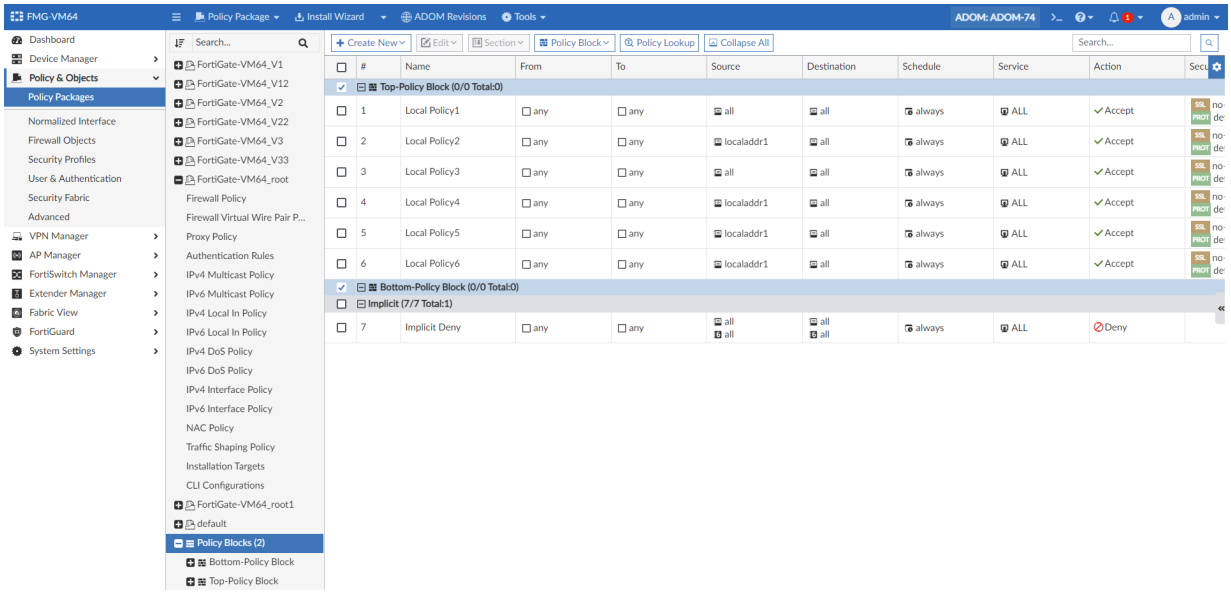
4. Import the objects used by the Global policy package into the local ADOM.
   a. In the local ADOM, go to *Device Manager* > *Device & Groups*.
   b. Select the managed FortiGate and choose *Import Configuration* > *Import all objects*.



5. Create the header and footer policy blocks.
   a. In the local ADOM, create two policy blocks named *Top-Policy Block* and *Bottom-Policy Block* respectively. The purpose is to append one policy block to the top of the local policy package as the header and the other at the bottom as the footer.

b. Append *Top-Policy Block* to the top of the policy package and *Bottom-Policy Block* at the bottom.



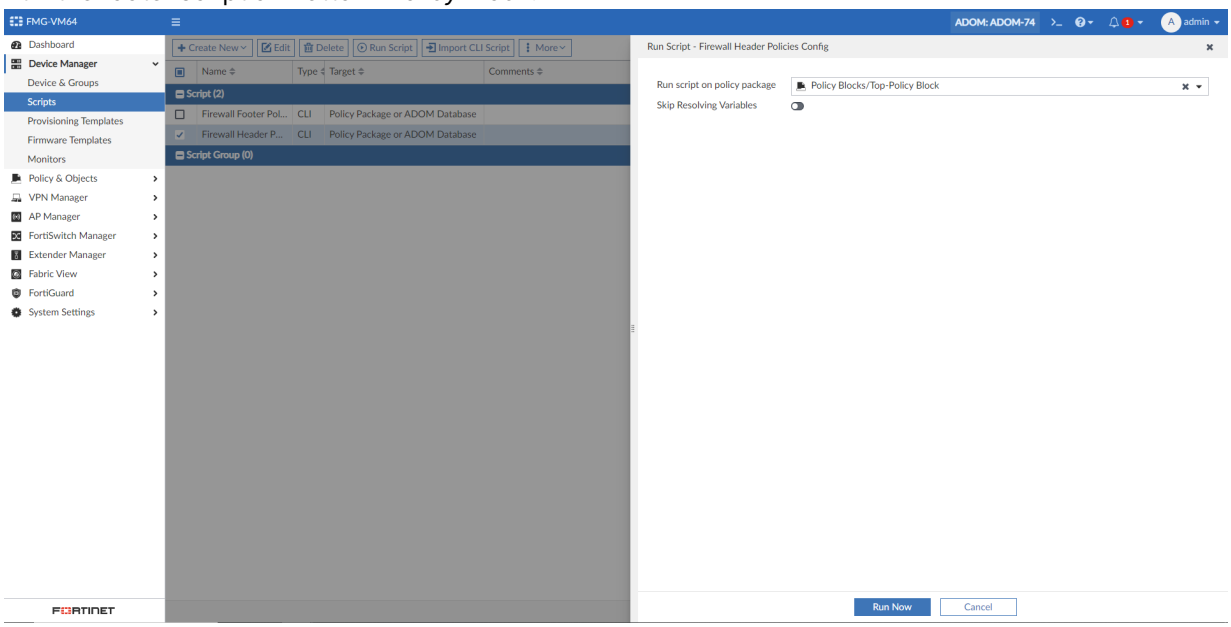


6. Run the script to create the local policies.

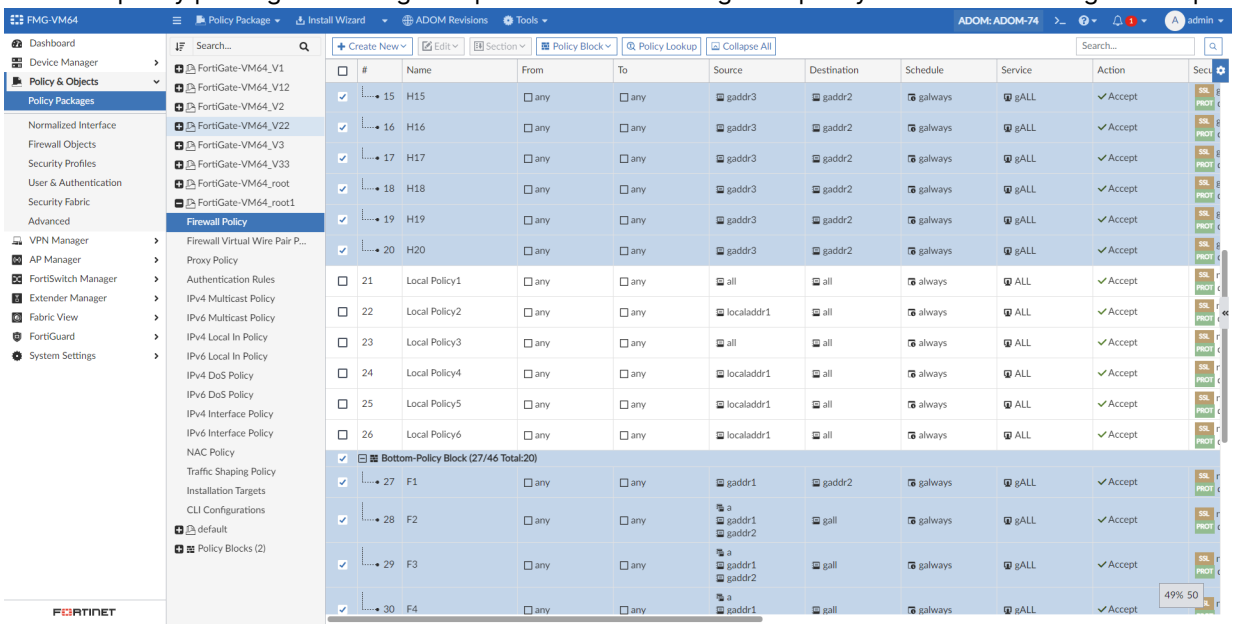
a. Go to *Device Manager* > *Scripts*.

b. Run the header script on *Top-Policy Block*.

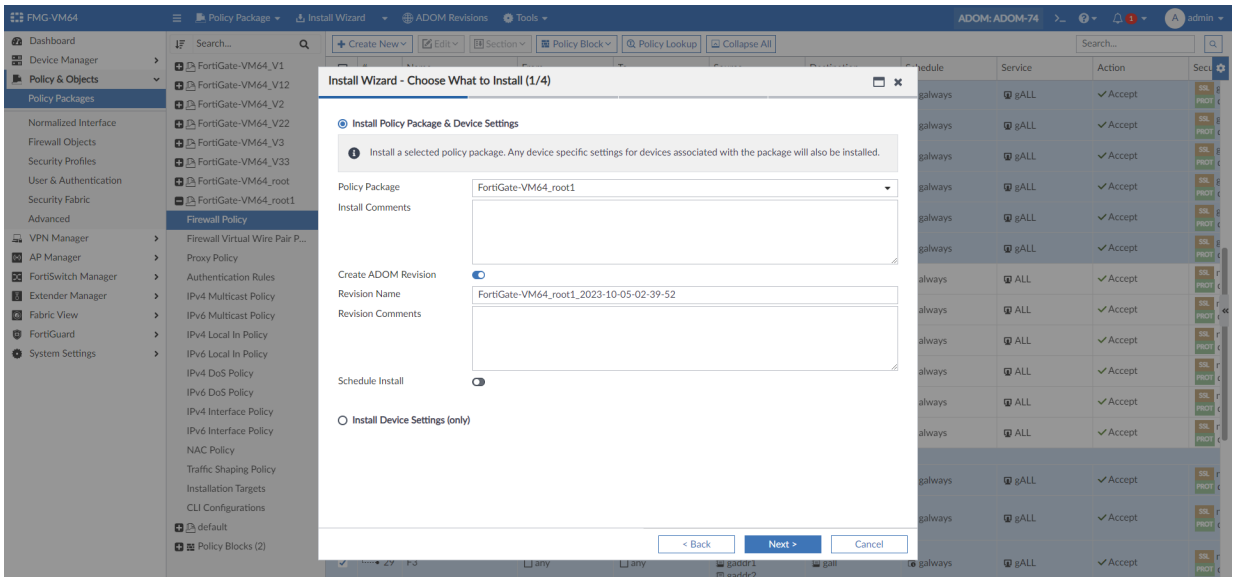
c. Run the footer script on *Bottom-Policy Block*.

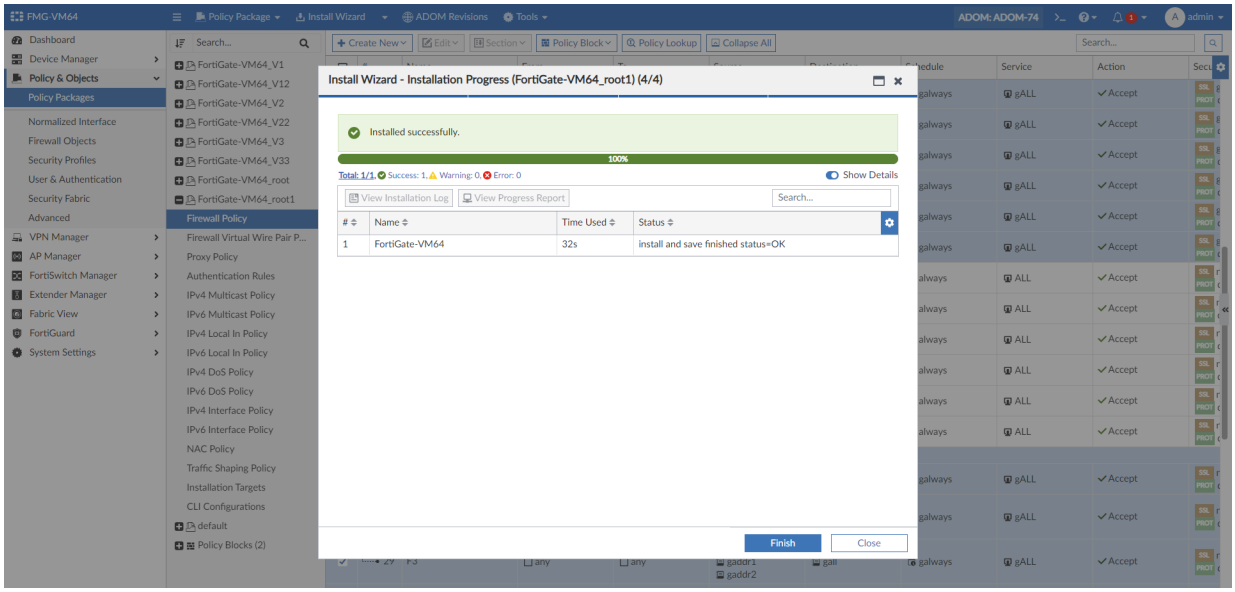


7. In the local ADOM, go to *Policy & Objects* > *Policy Packages* > *Firewall Policy*.
The local policy package has the global policies added through the policy block after running the scripts.

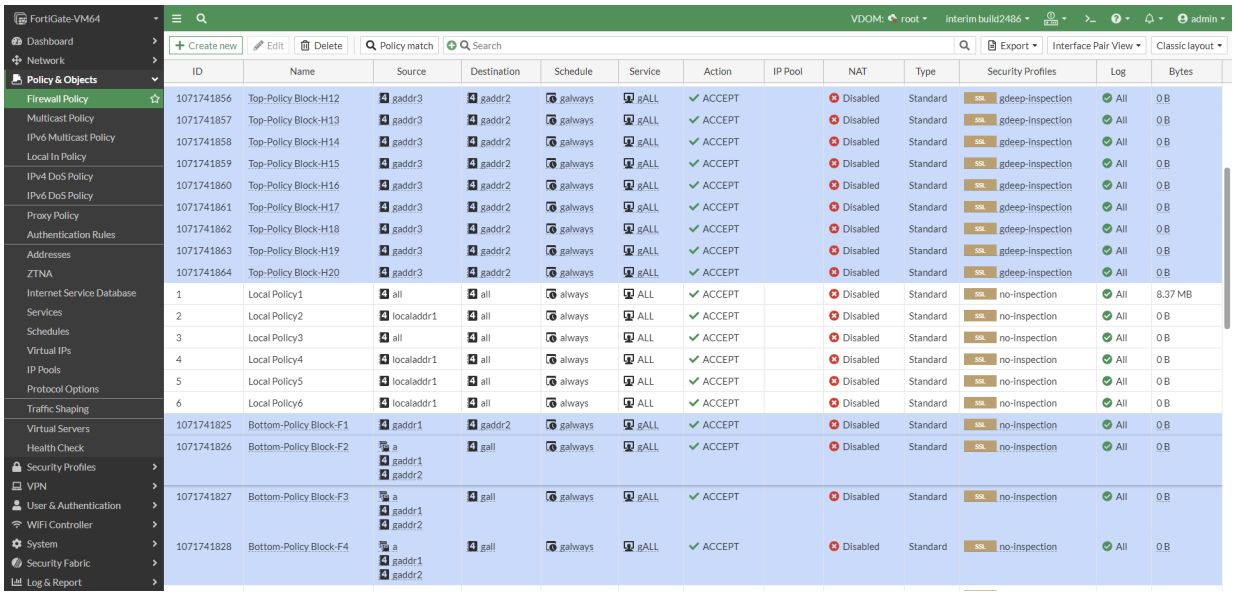


8. Install the policy package to the managed FortiGate devices to remove the global policy and re-create the policy with thew new local policy blocks.





On FortiGate, the policies re-created through the *Top-Policy Block* and *Bottom-Policy Block* are shown in sequence, and the migration from the global policy package to policy blocks is complete.



Managing objects and dynamic objects

All objects within an ADOM are managed by a single database unique to that ADOM. Objects inside that database can include items such as addresses, services, intrusion protection definitions, antivirus signatures, web filtering profiles, etc. For more information on the ADOM database, see the ADOM and policy layer on page 50.

Some objects include the option to enable dynamic mapping to map a single logical object to a unique definition based on the device or platform. When this feature is enabled, a table is displayed within the object configuration pane which lists the dynamic mapping information. See Dynamic mapping on page 552.

When making changes to an object within the object database, changes are reflected immediately within the policy table in the GUI; no copying to the database is required. If partial install is enabled, the edited object can be pushed to all the devices that currently use it. Installing objects on page 539

Not all objects are enabled by default. Some features must be enabled before they are visible in the GUI. See Feature visibility on page 413.

Some objects can only be configured using the *CLI Configurations* menu. See CLI configurations on page 556

Objects and dynamic objects are managed from the tree menu under *Policy & Objects* (or on the bottom half of the screen when dual pane is enabled). The available objects vary, depending on the specific ADOM selected.

Objects are used to define policies, and policies are assembled into policy packages that you can install on devices. Policy packages are managed under *Policy Packages* in *Policy & Objects* (on the top half of the screen when dual pane is enabled).

When you view a policy in a policy package, you can edit the policy by dragging objects from other columns, policies, or the object selector frame and dropping the objects in cells in the policy. For more information see Drag and dropping objects on page 503.

On the object configuration panes, you can see whether an object is used in the *Used* column, and you can right-click on an object to find out where the object is used (*Where Used*) or to add the object to a group (*Grouping*).

FortiManager objects are defined either per ADOM or at a global level.

When managing objects, you can click the *Full Screen/Exit Full Screen* option in the toolbar to toggle full screen mode for the currently displayed table.

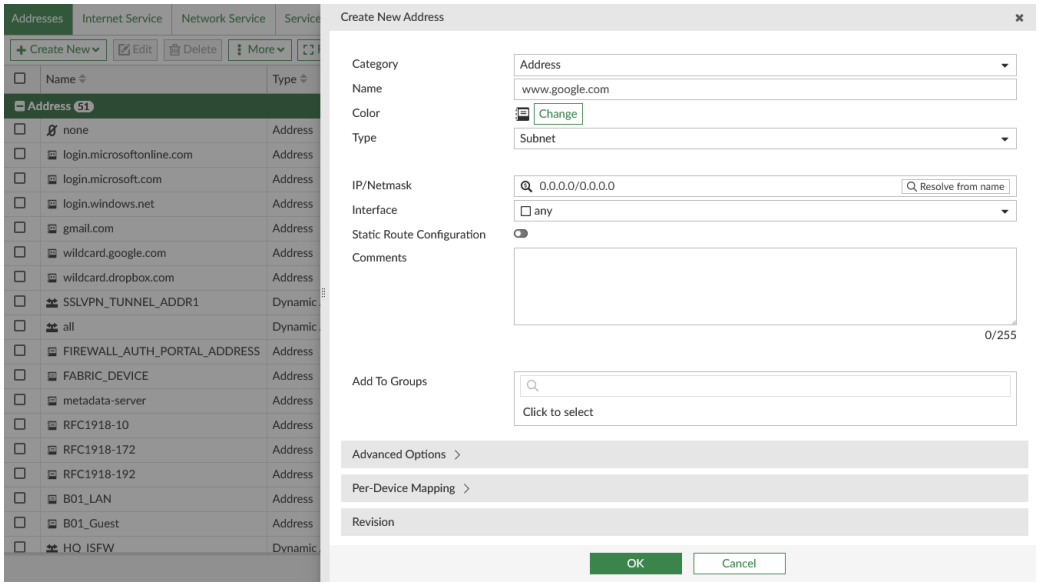
Creating objects

Objects can be created as global objects or for specific ADOMs.

To create a new object:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and select the object type the tree menu. For example, view firewall addresses by going to *Firewall Objects* > *Addresses*.

   The firewall address list is displayed in the content pane. The available address or address group lists are selectable on the content pane toolbar.
3. From the *Create New* menu, select the type of address. In this example, *Address* was selected. The *Create New Address* pane opens.



Some object configurations allow you to add the object to a group. This options are not available for all objects.

4. Enter the required information, then click *OK* to create the new object.
   A change note is required when creating or editing objects.

If you create Security Profiles that include Application Signature or Custom IPS Signature with the same ID for multiple VDOMs, FortiManager will automatically change the ID. For example, multiple VDOMs in a FortiGate device having the same Custom IPS Signature will have different IDs assigned by FortiManager while installing the policy. The Custom IPS Signature name will remain the same, but the ID will be different for each VDOM.

The automatic change of ID affects the `attack_id` in Custom IPS Signature and `attack_id` or `vuln_id` in Application Signature. The change in ID may occur even when importing a policy from FortiGate device and re-installing the policy.

You can view the modified ID in the Install Wizard by clicking *Install Preview*. Alternatively, you can also go to *Device Manager > [FortiGate_Name] > CLI Configurations> ips* or *Device Manager > [FortiGate_Name] > CLI Configurations> application* to view the modified ID for the particular VDOM.

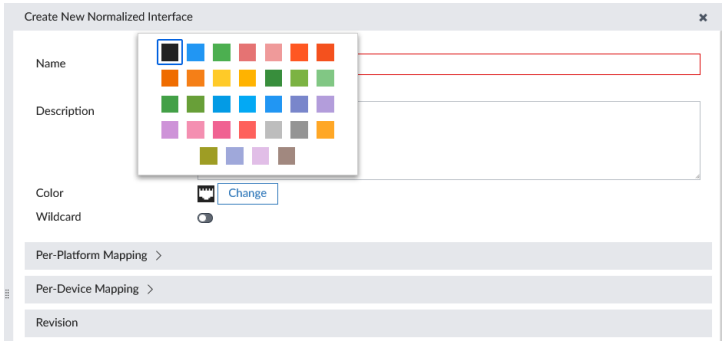
If you create an object in the Global Database, and assign the object to a regular ADOM, you cannot delete the object from the Global Database. You must unassign the object from the regular ADOM before deleting it from the Global Database.

Color code an object

Objects can be color coded for easy identification.

To color code an object from the object configuration menu:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and select the object type the tree menu. For example, view normalized interfaces by going to *Normalized Interface*.
3. In the content pane, click *Create New*.
   The object configuration window opens.



4. In the *Color* field, click *Change* to select a new color code for the object.
5. Click *OK*.

To color code an object from the toolbar:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and select the object type the tree menu.

3. Select an existing object from the table, and click *More* > *Change Color* in the toolbar.
4. Select a color code, and click *OK*.

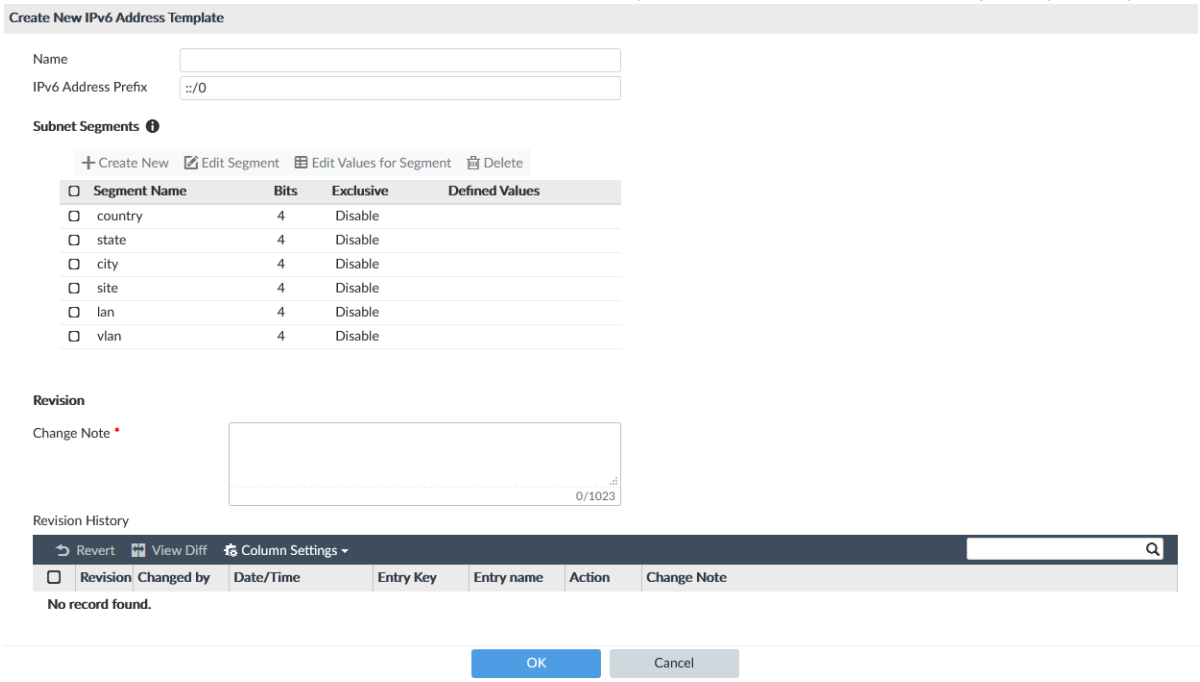
If a color code is not selected while creating an object, black is assigned as the default color.

Creating an IPv6 address template

Create an IPv6 address template with predefined parameters. The template can then be applied when creating a new IPv6 address.

To create an IPv6 address template:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Firewall Objects* > *Addresses*.
   The address list is displayed in the content pane. The available interfaces are selectable on the content pane toolbar.
3. From the *Create New* menu, select *IPv6 Address Template*. The *IPv6 Address Template* pane opens.



4. Select or specify the values for the following and click *OK*:

Name	Specify the name for the IPv6 address template.
IPv6 Address Prefix	Specify a prefix for the IPv6 address.
Subnet Segments	There can only be six subnet segments. These can either be predefined or user created subnet segments.

	Select one of the following predefined subnet segments: • country • state • city • site • lan • vlan
Create New	To create a new segment, you must delete one of the existing predefined segments if you already have six subnet segments. Click *Create New*. Specify the *Segment Name*, *Bits*, and toggle *Exclusive* to *Enable* or *Disable*. Click *OK*.
Edit Segment	Click *Edit Segment*. Edit the *Segment Name*, *Bits*, and toggle *Exclusive* to *Enable* or *Disable*. Click *OK*.
Edit Values for Segment	Click *Edit values for Segment*. Click *+* to add a row. Specify the *Name*, select the *Format*, and specify the *Value*. Click *OK*.
Delete	Select one or more subnet segments and click *Delete*.



The administrator can only define 6 segments and each segment can have a maximum of 16 bits. The administrator can toggle *Exclusive* to *Enable* to only choose from the predefined segments.



The length of the IPv6 address prefix must be greater than 1 bit.

Managing objects

Once an object has been created, you can manage it in various ways:

- Edit an object on page 536
- Remove an object on page 537
- Clone an object on page 538
- Promote an object to Global Database on page 538
- Installing objects on page 539
- Export IPS and Application Control signatures to CSV file format on page 540

Edit an object

After editing an object in the object database, the changes are immediately reflected within the policy table in the GUI; no copying to the database is required. If partial install is enabled, the edited object can be manually pushed to all devices currently using that object, see Installing objects on page 539.

Changes made to an object are displayed in the *Revision History* table at the bottom of the page. To view the history, select a revision in the table and click *View Diff*, or double-click the revision.

To edit an object:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. In the tree menu, select an object type. The content pane displays the objects for the object type.
4. Select an object, then click *Edit*.
5. Edit the information as required.
6. In the *Change Note* field, describe the edit.
7. Click *OK*.



Objects can also be edited directly from the policy list and *Object Selector* frame by right-clicking on the object and selecting *Edit*.



When an object is added to a policy package and assigned to an ADOM, the object is available in all devices that are part of the ADOM. If the object is renamed on a device locally, FortiManager automatically syncs the object to the ADOM and applies the change to all devices in the ADOM.

To revert a change:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. In the tree menu, select an object type. The content pane displays the objects for the object type.
4. Select an object, then click *Edit*.
5. In the *Revision History* table, select a revision and click *Revert*.
6. Click *OK*.

Remove an object

To delete an object:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. In the tree menu, select an object type. The content pane displays the objects for the object type.
4. Select the object, and click *Delete*.

Deleting used objects

You can delete objects referenced by a policy or other objects. When deleting a used object, a dialog appears allowing you to view where the object is being used.

- Click *Where Used* to see where the object is being used.
- Click *Delete Anyway* to delete the object.

You can configure whether forced deletion of used objects is allowed using the following CLI command:

```
config system admin setting
set objects-force-deletion {enable | disable}
```

This setting is enabled by default, allowing administrators to force the deletion of used objects. Disabling this setting prevents the deletion of used objects.

Clone an object

If a new object that you are creating is similar to a previously created object, the new object can be created by cloning the previous object.

To clone an object:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and locate the object to clone.
3. Right-click an object, and select *Clone*. The *Clone* pane is displayed.
4. Adjust the information as required, and click *OK* to create the new object.

Promote an object to Global Database

Existing or newly created ADOM-level objects can be promoted to the Global Database.

To promote an object:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and select the object type that you want to promote.
   For example, view the interface by going to *Normalized Interface*.

   The interface list is displayed in the content pane. The available interfaces are selectable on the content pane toolbar.
3. Right-click the object and select *Promote to Global*.

4. If you want to rename the object, specify a new name in the *New Name* field. Leave the *New Name* field blank to keep the original name for the object.
5. Click *Promote*.

   The object is now promoted to the Global Database.

Installing objects

Objects can be manually installed to all devices that are currently using that object. Partial install must be enabled in the CLI for this option to be available.

To enable partial install:

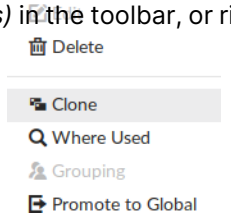
In the FortiManager CLI, enable partial install::

```
config system global
   set partial-install enable
end
```

To install objects to devices:

1. Locate the objects to install.
2. Select the objects then click *More > Install Object(s)* in the toolbar, or right-click on the objects and select *Install Object(s)*.

   The *Install Object(s)* dialog opens.
3. Select the target devices.
4. (Optional) Click the *Install Preview* button to preview the installation.



- If you attempt to install an object that is not used in a policy, the device list displays *No record found*.
- If you attempt to install an object with invalid configuration, *Install Preview* displays the configuration errors.
- In *Install Preview*, metadata variables used in objects display the real value.
- Administrators with a restricted profile can use *Install Preview* for partial installs.

5. Click *Install*. The objects are installed to the selected devices.

After an object is installed to a device, policy packages will be flagged as modified until the next time the packages are installed.

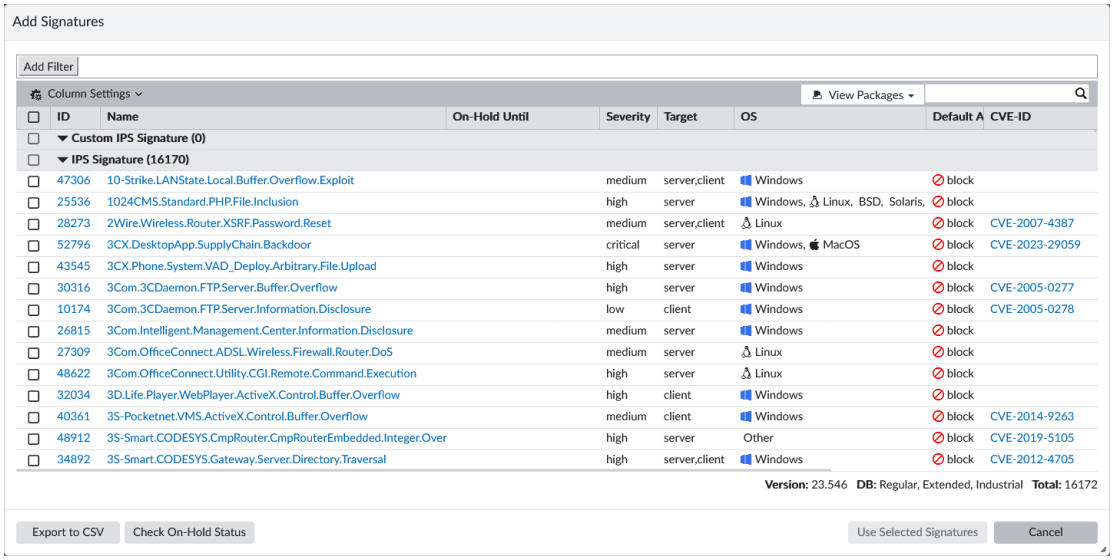
Global database objects cannot be installed to devices.

Export IPS and Application Control signatures to CSV file format

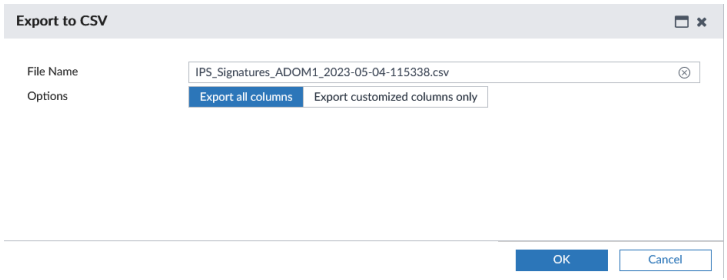
You can export Intrusion Prevention signatures (IPS) and Application Control signatures to a file CSV format.

To export signatures to CSV format:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Security Profiles* > *Application Control/Intrusion Prevention*
3. Click *Create New* to create a new object, or double-click an exiting object to open it for editing.
4. Under *IPS Signatures and Filters*, click *Create New*.
5. Select the *Type* as *Signature*, and click *Add Signature*.
6. The *Add Signatures* dialog box is displayed.



7. Click *Export to CSV*.
   The *Export to CSV* dialog box is displayed.



8. (Optional) Change the file name.
9. Select whether to export all columns or only customized columns.
10. Click *Download*.

Viewing objects

Once an object has been created, you can use the FortiManager GUI to find objects in the following ways:

- Search objects on page 541
- Search for objects while viewing a policy on page 541
- Find unused objects on page 543
- Find and merge duplicate objects on page 543

Search objects

The search objects tool allows you to search objects based on keywords.

To dynamically search objects:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and select an object type from the tree menu, for example *Firewall Objects*.
3. In the search box on the right side of the toolbar, type a search keyword. The results of the search are updated as you type and displayed in the object list.



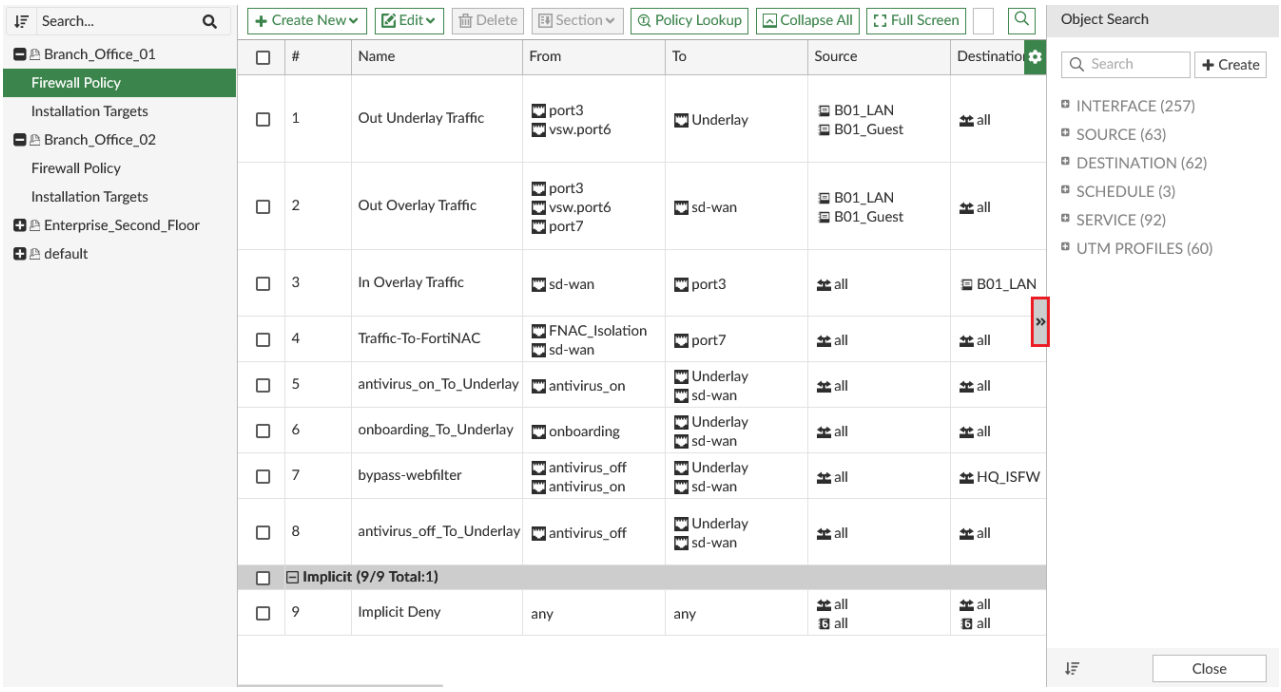
Select *View* > *Icon View* to view the objects as icons. Select *View* > *Table View* to view the objects in a table format.

Search for objects while viewing a policy

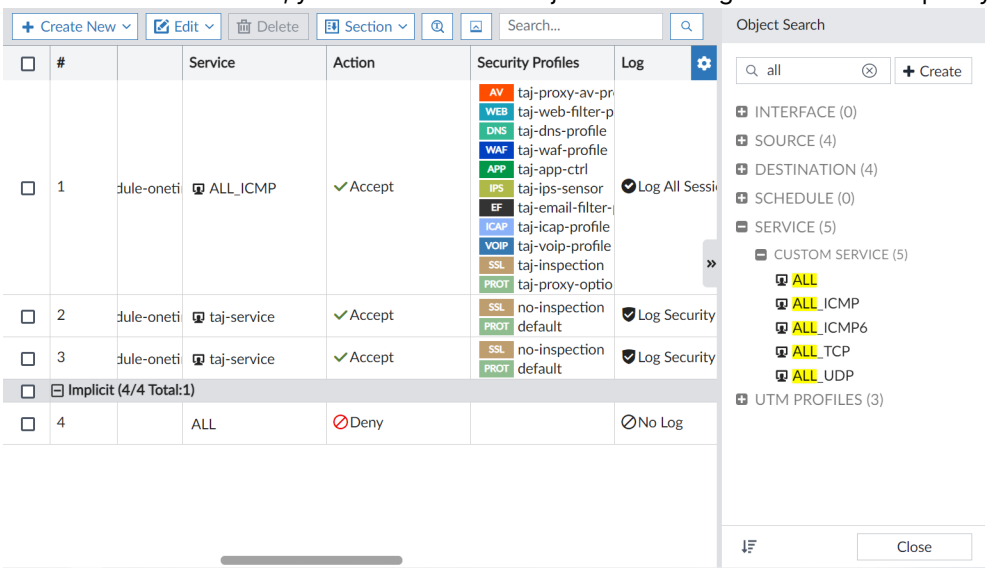
Object search can be done using a persistent search menu which is available when viewing policies, and the search extends to all object types.

To use the persistent search menu:

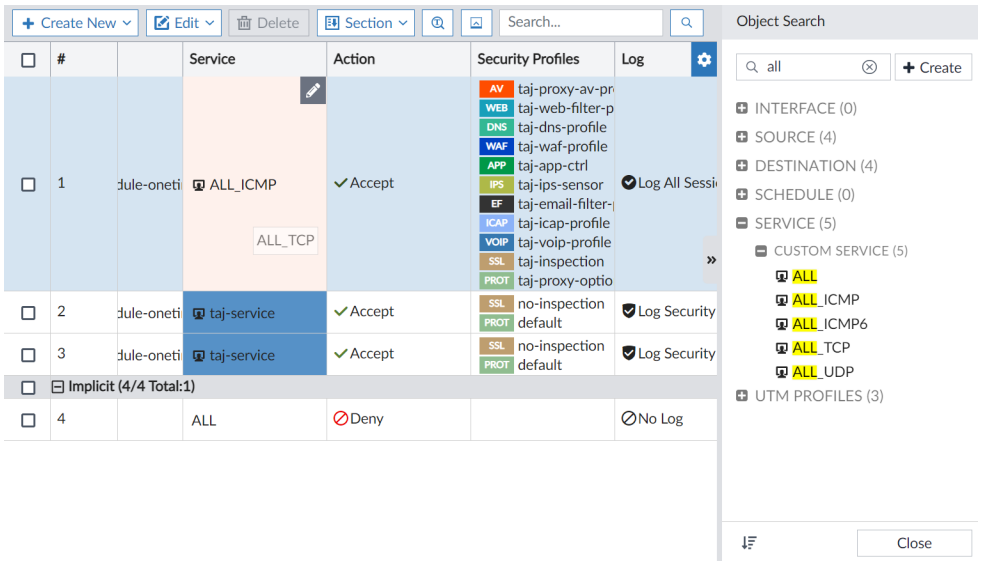
1. Go to *Policy & Objects* > *Policy Packages* and select a policy.
2. In the policy table, users can click the double arrow icon () to open the *Object Search* panel, and search for objects.
   You can also create or edit existing objects from the *Object Search* panel.



3. From the search results, you can see which objects are configurable to which policy fields.



4. You can assign objects from the search panel to a policy by dragging and dropping the object into the corresponding column. FortiManager only supports the drag-and-drop object feature when the object is placed in the column of the came category.



Find unused objects

To find unused objects:

1. Go to *Policy & Objects*.
2. From the *Tools* menu, select *Find Unused Objects*. The *Unused Objects* dialog box is displayed.
3. When you are done, click *Close*.

The *Used* column on the *Object Configurations* pane will also show you if an object is used or not.

Find and merge duplicate objects

Duplicate objects have the same definition, but different names. You can find duplicate objects and review them. You then have the option to merge duplicate objects into one object.

To find duplicate objects:

1. Go to *Policy & Objects*.
2. From the *Tools* menu, select *Find Duplicate Objects*. The *Duplicate Objects* dialog box is displayed.
3. Review the groups of duplicate objects.
4. Click *Merge* to merge a group of duplicate objects into one object.
5. When you are done, click *Close*.

Normalized interfaces

A normalized interface defines mapping rules. In mapping rules, interfaces are mapped per-device and/or per platform. You can have both per-device and per-platform mappings in a normalized interface. When the normalized interface is used in a policy, the per-device mappings have higher priority than per-platform mappings. The first match is used.

Default normalized interfaces are created when ADOMs are created. Default normalized interfaces contain a number of per-platform mapping rules for all FortiGate models. For example, port1 is mapped to port1, and WAN is mapped to WAN in default per-platform mapping rules. Default per-platform mapping rules allow you to install policies to FortiGates without first creating custom mapping rules.

You can map normalized interface names to different physical interface names on different FortiGate models. For example, you can map a normalized interface named *LAN* to port1 on one FortiGate and to port2 on another FortiGate.

You can delete default normalized interfaces and create new normalized interfaces. You can also delete per-platform mappings in a default normalized interface.

Zones are created using *Device Manager*, and you can map zones to normalized interfaces. See also Device zones on page 211.

You can also select normalized interfaces when you create virtual wire pairs.

This section contains the following topics:

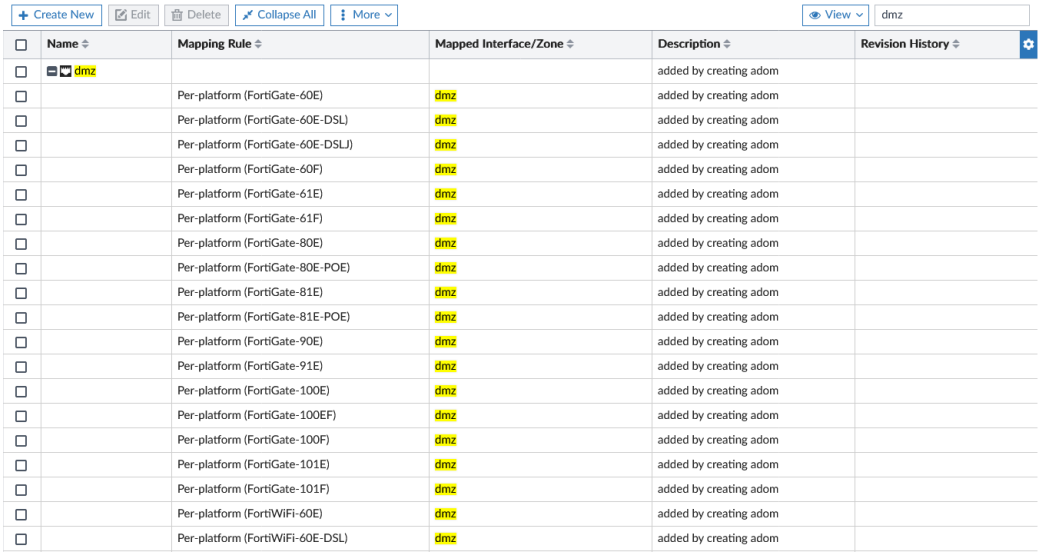
- Viewing normalized interfaces on page 544
- Viewing normalized interfaces mapped to devices and platforms on page 545
- Viewing where normalized interfaces are used on page 546
- Configuring normalized interface per-platform mapping rules on page 547
- Configuring normalized interface per-platform mapping rules on page 547
- Deleting per-platform mapping rules on page 548
- Deleting default normalized interfaces on page 548
- Creating normalized interfaces on page 548
- Creating virtual wire pairs on page 550
- Modify existing interface-zone mapping on page 551

Viewing normalized interfaces

You can view all normalized interfaces and their mapping rules. You can also collapse or expand all mapping rules and mapped interface/zones for normalized interfaces.

To view normalized interfaces:

1. Go to *Policy & Objects* > *Normalized Interface*.
   The list of normalized interfaces are displayed in the content pane.
   In the following example, the normalized interface named *dmz* is displayed, and it contains per-platform mappings for a number of FortiGate devices. The *dmz* normalized interface was added when an ADOM was created.



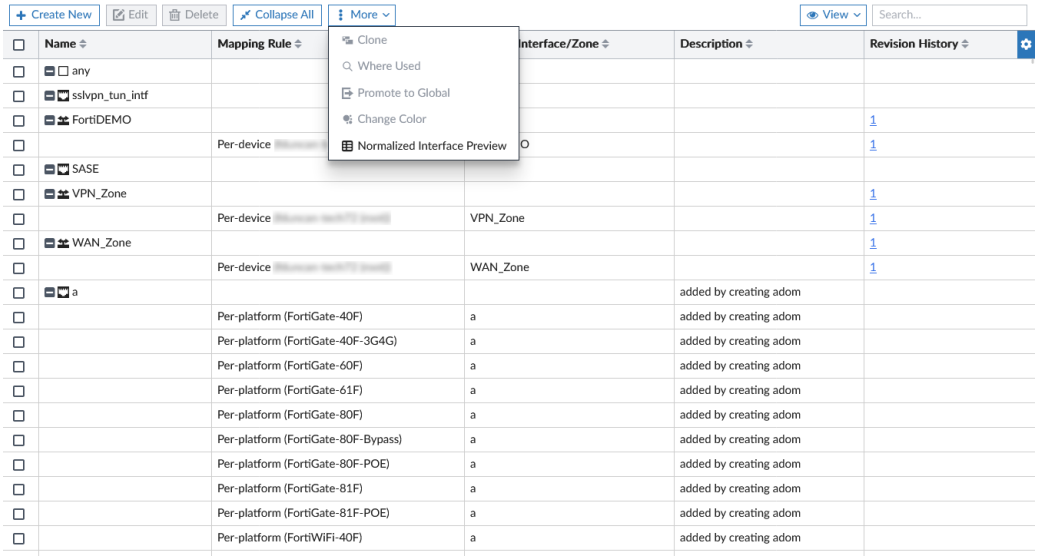
2. From the toolbar, select *Collapse All*.
   The list of normalized interfaces is displayed, but the mapping rules and mapped interface/zone information is hidden.
3. From the toolbar, select *Expand All* .
   The list of normalized interfaces and the mapping rules as well as mapped interface/zone information are displayed.

Viewing normalized interfaces mapped to devices and platforms

For each managed FortiGate device or platform, you can view the number of normalized interfaces mapped to it.

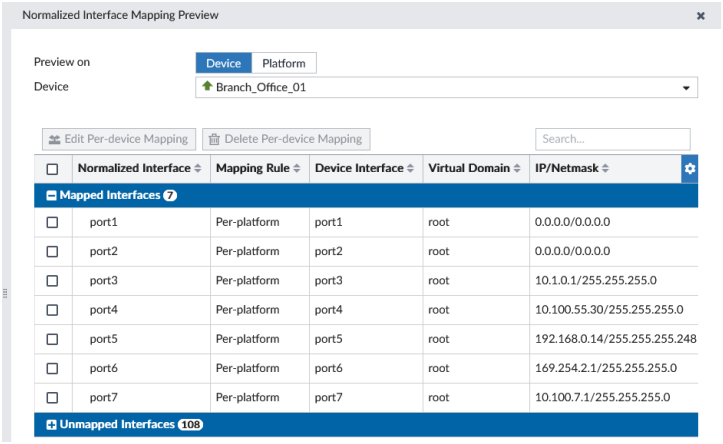
To view normalized interfaces mapped to devices/platforms:

1. Go to *Policy & Objects* > *Normalized Interface*.
2. From the *More* menu, select *Normalized Interface Preview*.



The *Normalized Interface Mapping Preview* window is displayed.

3. Select the option to preview on either *Device* or *Platform*.
4. From the dropdown list, select a device/device model.
   The mapping preview for the selected device/device model is displayed.



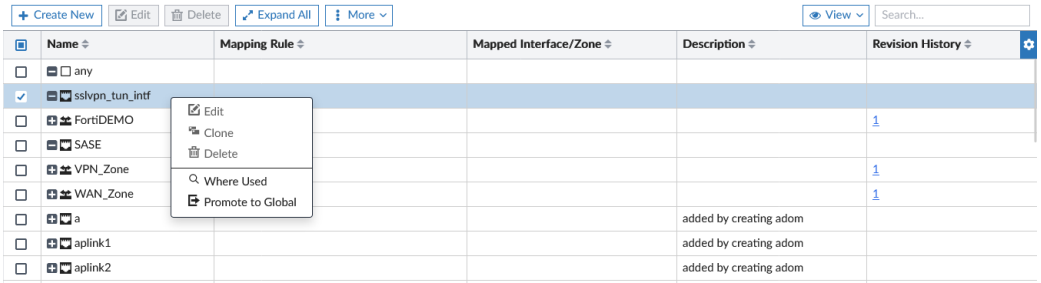
   Scroll to the bottom to view unmapped interfaces.
5. (Optional) Select a mapping, and click *Edit Per-device Mapping* or *Delete Per-device Mapping*.
6. Click *Close*.

Viewing where normalized interfaces are used

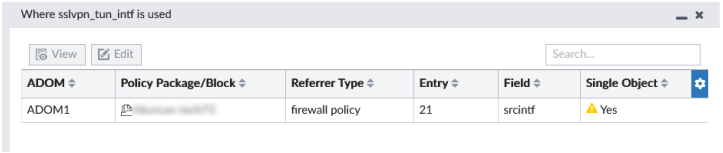
You can view what policy packages use a normalized interface.

To view where normalized interfaces are used:

1. Go to *Policy & Objects* > *Normalized Interface*.
2. In the content pane, right-click a normalized interface, and select *Where Used*.



   The *Where <normalized interface name> is used* window displays. The name of the policy package that uses the selected normalized interface is identified.



3. Click *Close*.

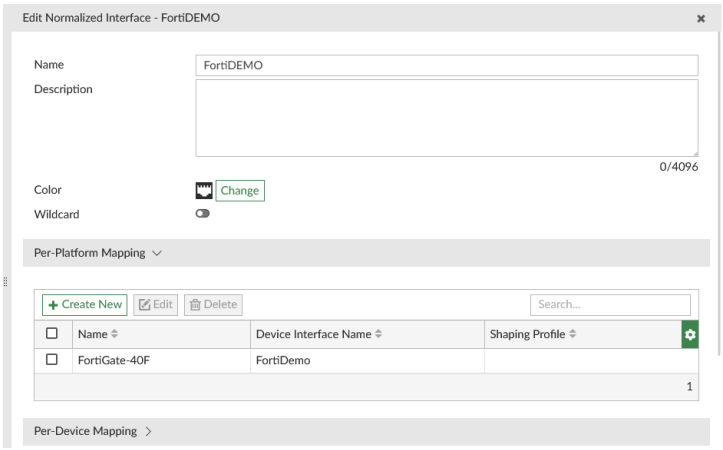
Configuring normalized interface per-platform mapping rules

You can edit per-platform mapping rules in normalized interfaces.

When you change mapping rules, the object is modified, and the status for any policy package that uses the modified object changes to *Modified* on the *Device Manager* pane. You must reinstall the affected policy packages again to provide the changes to the device.

To configure per-platform mapping rules:

1. Go to *Policy & Objects* > *Normalized Interface*.
2. In the content pane, right-click a normalized interface, and select *Edit*.
   The *Edit Normalized Interface* pane appears.
3. In the *Per-Platform Mapping* table, right-click a mapped device, and select *Edit* or click *Create New* to create a new rule.



4. Configure the options, and click *OK*. The mapping rule is saved.



The *Mapped Interface Name* fields supports metadata variables. See ADOM-level metadata variables on page 557.

This field does not currently support the metadata variable selection window, but you can enter the variable manually using the following format: `$(variable_name)`.

5. Click *OK*. The normalized interface is saved.

Configuring normalized interface per-device mapping rules

After creating an interface on the FortiManager, an interface mapping must be created so that the new interface can be used when creating policies. To do this, create a new dynamic interface with per-device mapping.

To create a new dynamic interface with per-device mapping:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Normalized Interface*, and click *Create New* .
3. Enter a name and description for the interface.

4. Expand *Per-Device Mapping*, and click *Create New*. The *Per-Device Mapping* dialog box opens.
5. Select the device or VDOM in the *Mapped Device* field, select the interface in the *Device Interface* field, then click *OK*.
6. Click *OK* to create the new dynamic interface object.
   The mapped interface can now be used when creating policies.

To edit a dynamic interface's per-device mapping rules:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Normalized Interface*, and edit an existing interface.
3. Expand *Per-Device Mapping*. Select a mapped device and click *Edit*. The *Edit Per-Device Mapping* dialog box opens.
4. Configure the *Mapped Device* and/or *Mapped Interface Name* field, then click *OK*.
5. Click *OK* to save the dynamic interface object.

Deleting per-platform mapping rules

A number of normalized interfaces are created by default when an ADOM is created. You can edit default normalized interfaces to delete per-platform mapping rules.

To delete per-platform mapping rules:

1. Go to *Policy & Objects* > *Normalized Interface*.
2. In the content pane, right-click a default normalized interface, and select *Edit*.
   The *Edit Normalized Interface* pane appears.
3. In the *Per-Platform Mapping* table, select a mapped device, and click *Delete*.
4. Click *OK*.
   The normalized interface is saved.

Deleting default normalized interfaces

You can delete the default normalized interfaces that are automatically created when ADOMs are created.

To delete default normalized interfaces:

1. Go to *Policy & Objects* > *Normalized Interface*.
2. In the content pane, right-click a normalized interface, and select *Delete*.
3. Click *OK*.
   The normalized interface is deleted.

Creating normalized interfaces

If you want to use a physical interface name in a per-platform mapping rule in a normalized interface, you must first delete the default per-platform mapping rule from the default per-platform interface. Otherwise the

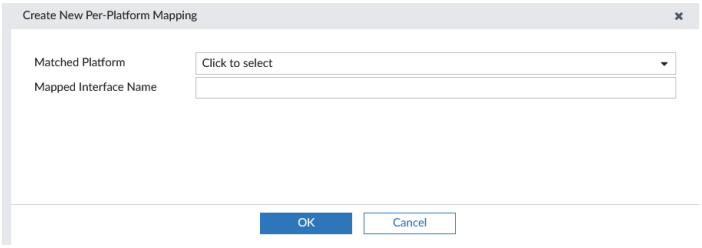
dynamic-interface default mapping has been used error is displayed, and you cannot create the normalized interface.

To delete the default per-platform mapping rule:

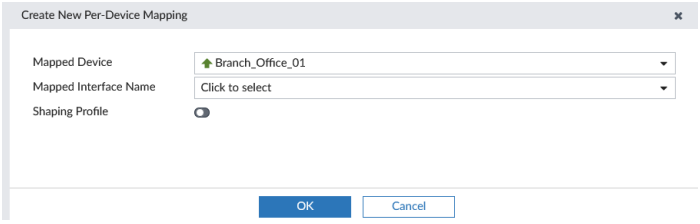
1. Go to *Policy & Objects* > *Normalized Interface*.
2. In the content pane, right-click the default per-platform normalized interface, and select *Edit*.
   The *Edit Normalized Interface* page appears.
3. In the *Per-Platform Mapping* table, right-click the default per-platform mapping rule, and select *Delete*.
4. Click *OK*.

To create normalized interfaces for zones:

1. Go to *Policy & Objects* > *Normalized Interface*.
2. Click *Create New*.
   The *Create New Normalized Interface* pane is displayed.
3. Complete the *Name*, *Description*, and *Color* options.
4. Add a per-platform mapping.
   a. Click *Create New* under *Per-Platform Mapping*.
      The Create new Per-Platform Mapping dialog box is displayed.



   b. In the *Model* list, select the model for which you created the zone.
   c. In the *Device Interface Name* box, type the name of the interface.
   d. Click *OK*.
5. Add a per-device mapping.
   a. Click *Create New* under *Per-Device Mapping*.
      The *Create new Per-Device Mapping* dialog box is displayed.



   b. In the *Mapped Device* list, select the model for which you created the zone.
   c. In the *Device Interface* list, select the zone.
   d. Click *OK*.
6. Click *OK*.

To create a wildcard interface:

1. Go to *Policy & Objects* > *Normalized Interface*.
2. Click *Create New*.
   The *Create New Normalized Interface* pane is displayed.
3. Complete the *Name*, *Description*, and *Color* options.
4. Set the *Wildcard* toggle to the *ON* position, and enter the *Wildcard Interface* in the text field below.



When using wildcards, a "." (period) represents a single alpha-numeric character, similar to regex = [a-zA-Z0-9].

An "*" (asterisk) represents zero or more characters regex =.*

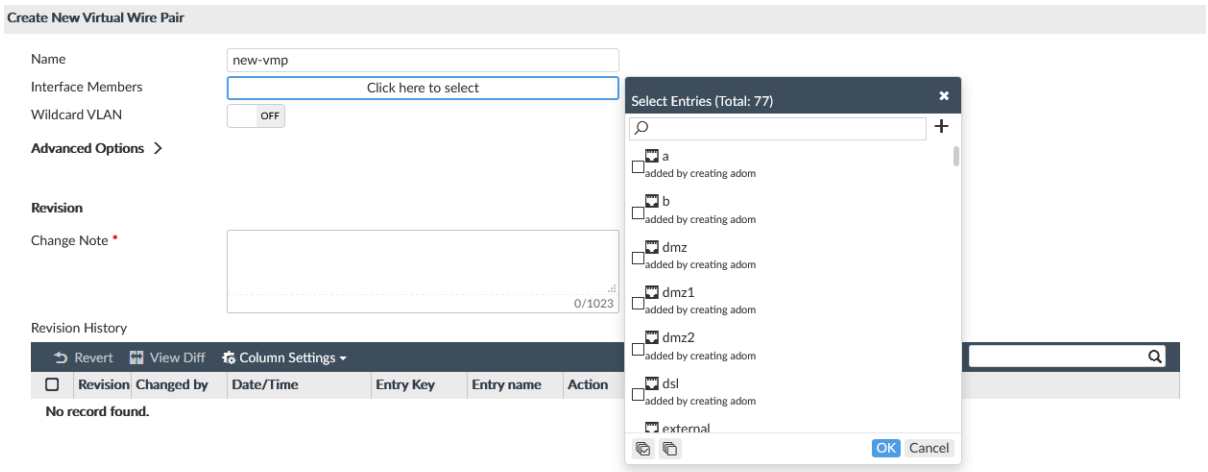
5. Add a *Change Note* and click *OK*.
   The wildcard interface can be used in Firewall policies similar to a regular interface but will be interpreted as one or more interfaces that matched the defined wildcard pattern.
   During install, all matched objects are installed.

Creating virtual wire pairs

You select normalized interfaces when you create virtual wire pairs.

To create virtual wire pairs:

1. Enable *Virtual Wire Pair Policy* in *Feature Visibility*.
2. Go to *Policy & Objects* > *Normalized Interface* and select the *Virtual Wire Pair* tab.
3. Click *Create New*.
   The *Create New Virtual Wire Pair* pane is displayed.
4. In the *Name* box, type a name for the virtual wire pair.
5. Click the *Interface Members* box.
   The list of normalized interfaces is displayed.



6. Select one or more normalized interfaces, and click *OK*.
7. Complete the remaining options, and click *OK*.

Modify existing interface-zone mapping

Interfaces mapped to a zone locally on FortiGate devices are not visible in *Device Manager* on FortiManager. It is recommended to create objects in FortiManager instead of creating it on FortiGate devices locally. If an interface is already mapped to a zone in FortiGate, it must be unmapped first. A zone must be created in FortiManager, added to a policy and installed to FortiGate. For convenience and ease of use, it is better to manage Object Configuration and Interface Mapping from FortiManager.

If an Interface is mapped to a Zone in FortiGate:

1. Log on to the FortiGate device.
2. Delete the Interface/Zone mapping from *Interfaces* > *[Interface_Name]* > *Delete*.
3. Log on to FortiManager.
4. Create a device zone named *Zone_One*, and map it to a physical interface:
   a. Go to *Device Manager* > *Device & Groups*.
   b. In the tree menu, select a device group. The devices are displayed in the lower tree menu.
   c. In the lower tree menu, double-click a device. The device database is displayed.
   d. Go to *Network* > *Interfaces*.
   e. Click *Create New* > *Device Zone*.
   f. In the *Zone Name* box type, *Zone_One*.
   g. Click the *Interface Member* box, select one or more physical interfaces, and click *OK*. The device zone is created.
5. Map the device zone to a normalized interface:
   a. Go to *Policy & Objects* > *Normalized Interface*.
   b. Click *Create New*. The *Create New Normalized Interface* pane is displayed.
   c. In the *Name* box, type a name for the normalized interface.
   d. Under *Per-Device Mapping*, click *Create New*. The *Per-Mapping* dialog box is displayed.
   e. In the *Mapped Device* list, select the device.

   f. In the *Mapped Interface Name* select the device zone that you created, and click *OK*. The per-device mapping is created.
   g. Click *OK*. The normalized interface is created and mapped to the device zone.
6. Create a new policy package named *New_Policy_Package*.
   a. Go to *Policy & Objects* > *Policy Packages*.
   b. From the *Policy Package* menu, select *New*.
   c. In the *Name* box, type a name for the policy package, such as *New_Policy_Package*.
   d. Set the remaining options, and click *OK*. The policy package named *New_Policy_Package* is created.
7. Create a new policy for the policy package, and select the device zone.
   a. In the tree menu, select the new policy package, for example, the policy package named *New_Policy_Package*, and click *Create New*. The *Create New Firewall Policy* pane is displayed.
   b. In the *Name* box, type a name, such as *New_IPv4_Policy*.
   c. Include *Zone_One* in the policy, and click *OK*. The policy is saved.
8. Assign the policy package to the device:
   a. In the tree menu, expand *New_Policy_Package*, and click *Installation Targets*.
   b. Click *Edit*, select the FortiGate, and click *OK*.
9. Install the policy package to the FortiGate:
   a. Right-click *New_Policy_Package*, and select *Install Wizard*.
   b. Select *Install Policy Package & Device Settings*, and select the *New_Policy_Package* from the drop-down.
   c. Complete the installation as per the Install Wizard.

   Zone_One is now available on the FortiGate device and mapped.



A zone is installed to a FortiGate device only if it is created, mapped to an interface, included in the Policy Package, assigned to a device, and installed using the Install Wizard.



An interface cannot be reused if it is already mapped to a zone. To reuse an interface, first unmap it from the zone in *Object Configurations*, and then reinstall to the FortiGate device.



After a Virtual IP is created, it must be mapped to interfaces. If per-device mapping is used, the mapping will be visible immediately in *Device Manager* > *[Device_Name]* > *Interface*.

Dynamic mapping

This section includes the following topics:

- Per-device and per-platform dynamic mapping on page 553
- Dynamic device objects on page 554
  - Create a dynamic local certificate on page 555
  - Create a dynamic VPN Tunnel on page 556

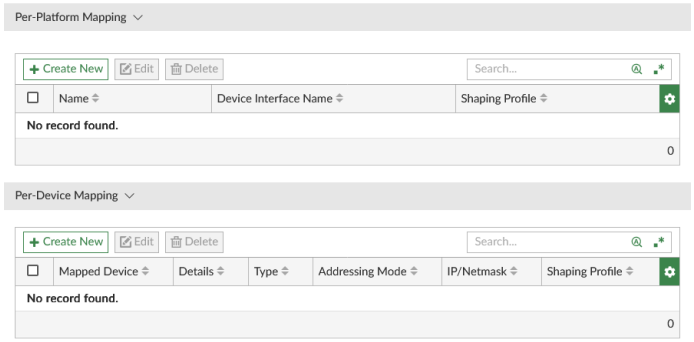
Per-device and per-platform dynamic mapping

Some objects support per-device and/or per-platform dynamic mapping allowing you to set object configurations for specific devices or platforms.

In the GUI, when the *Per-Device Mapping* or *Per-Platform Mapping* options are available, you can expand the option and click *Create New* to configure the dynamic mapping.

When using dynamic mapping, the devices or platforms specified will receive the configurations specified in the dynamic mapping rule. Devices or platforms which do not match the dynamic mapping will receive the default configuration set for the object.

For more information about configuring normalized interfaces with dynamic mapping, see Normalized interfaces on page 544.



To configure a dynamic mapping using the CLI, the configuration for the mapping must be defined for the object using the *dynamic_mapping* (per-device mapping) and/or *platform_mapping*(per-platform mapping) command when available. CLI scripts must be run on a policy package instead of the device database. For information on running CLI scripts, see Scripts on page 239



Default mapping is only used when there is no per-device mapping for a particular device. You must have either a per-device mapping or a default mapping in a policy package. Otherwise, the policy package installation will fail.

When you import a policy package, a per-device mapping is usually added when the object is already used by a FortiGate.

Dynamic mapping examples

The following are a few example objects configured with dynamic mapping in the CLI:

Example 1: Dynamic VIP

```
config firewall vip
```

```
    edit "vip1"
    …
    config dynamic_mapping
       edit "FW60CA3911000089"-"root"
          set extintf "any"
          set extip 172.18.26.100
          set mappedip 192.168.3.100
          set arp-reply disable
       next
    end
end
```

Example 2: Dynamic Address

```
config firewall address
    edit "address1"
    …
    config dynamic_mapping
       edit "FW60CA3911000089"-"root"
          set subnet 192.168.4.0 255.255.255.0
       next
    end
end
```

Example 3: Dynamic Interface

```
config dynamic interface
    edit "1a1"
       set default-mapping enable
       set defmap-intf "1a1"
       config dynamic_mapping
          edit "1"-"root"
          set local-intf "a"
       next
    end
       config platform_mapping
          edit "FortiGate-40F"
          set intf-zone "ddd"
       next
    end
    next
end
```

Dynamic device objects

Dynamic device objects can be mapped to FortiGate devices using per-device mapping.

To view the dynamic device objects:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. Go to *Tools* > *Feature Visibility*.
4. Select *Dynamic Local Certificate* and *Dynamic VPN Tunnel* and click *OK*.

The following dynamic device objects are available:

- Create a dynamic local certificate on page 555
- Create a dynamic VPN Tunnel on page 556

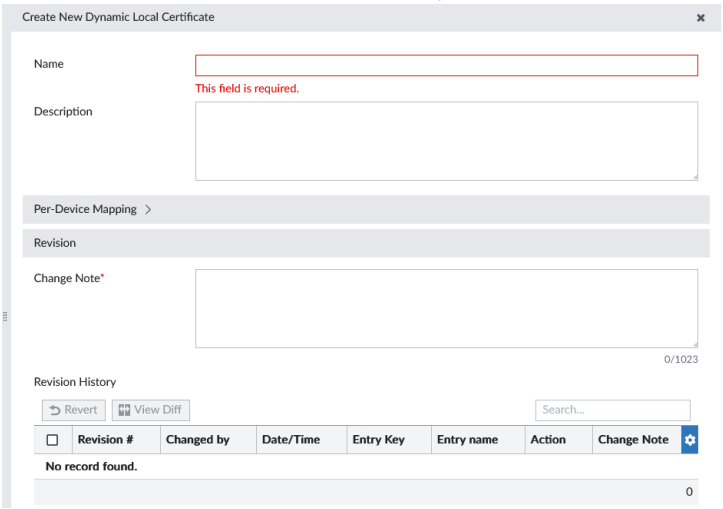
When an object is added to a policy package and assigned to an ADOM, the object is available in all devices that are part of the ADOM. If the object is renamed on a device locally, FortiManager automatically syncs the object to the ADOM.

Create a dynamic local certificate

Create a dynamic local certificate to sync with devices using per-device mapping.

To create a dynamic local certificate:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Advanced* > *Dynamic Local Certificate*.
3. Click *Create New*. The *Create New Dynamic Local Certificate* pane opens.



4. Select or specify the values for the following and click *OK*:

Name	Specify the name for the Dynamic Local Certificate.
Description	Specify a description.
Per-Device Mapping	Toggle Per-Device Mapping to *ON*. Click *Create New*. Select the *Mapped Device* and *VPN Local Certificate*. Click *OK*.

Examples using dynamic local certificates

You can find example deployment scenarios using dynamic local certificates in the FortiManager Examples Guide including the following scenarios:

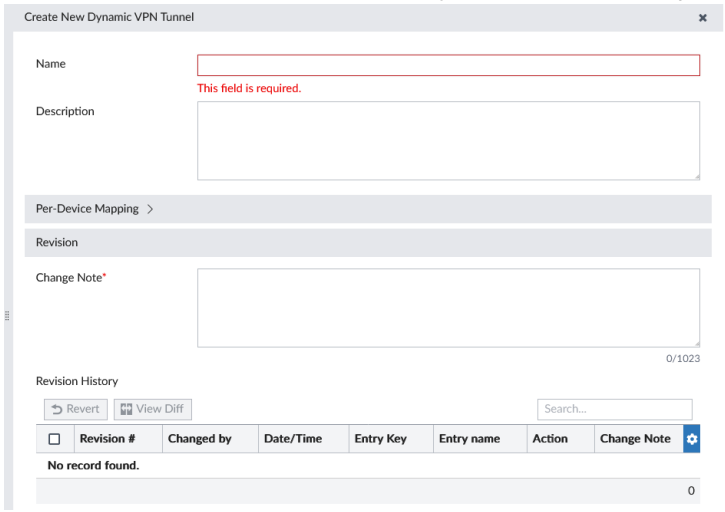
- Configuring FortiManager to deploy certificates for admin GUI access
- Configuring FortiManager to deploy certificates for deep inspection
- Configuring FortiManager and FortiAuthenticator for SCEP certificate deployment

Create a dynamic VPN Tunnel

Create a VPN tunnel to sync with devices using per-device mapping.

To create a VPN tunnel:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Advanced* > *Dynamic VPN Tunnel*.
3. Click *Create New*. The *Create New Dynamic VPN Tunnel* pane opens.



4. Select or specify the values for the following and click *OK*:

Name	Specify the name for the Dynamic VPN Tunnel.
Description	Specify a description.
Per-Device Mapping	Toggle Per-Device Mapping to *ON*. Click *Create New*. Select the *Mapped Device* and *VPN Tunnel*. Click *OK*.

CLI configurations

FortiManager includes the ability to configure objects that are available only via the FortiOS command line interface, as well as settings that are not available in the FortiManager GUI using the *CLI Configurations* menu.



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.

When this feature is enabled, you can find the *CLI Configurations* menu by going to *Policy & Objects* > *Advanced* and clicking on the *CLI Configurations* tab.

In the CLI Configurations pane, you can use the search bar to quickly search for objects, and then configure or edit object details using the FortiManager GUI.

For example:

1. Enable *CLI Configurations* in *Feature Visibility*.
2. Go to *Policy & Objects* > *Advanced* > *CLI Configurations*.
3. Enter *proxy* in the search bar to discover results matching that keyword.
4. Expand the *web-proxy* result in the tree menu, and select the *profile* menu item.
5. Create or edit a web-proxy profile.

ADOM-level metadata variables

ADOM-level metadata variables can be used as variables for certain fields in the following places:

- Scripts (excluding Tcl scripts)
- Templates
- Firewall address objects
- IP pools
- VIPs
- FortiAP SSIDs
- FortiSwitch VLAN configurations
- FortiClient EMS and FortiClient EMS Cloud connectors
- Normalized interfaces
- Firewall address groups

Fields that support metadata variables are identified with a metadata variable icon .

Typing **$** into an object's field where metadata variables are supported will display the available metadata variables for selection.

You can configure ADOM-level metadata variables in *Policy & Objects* > *Advanced* > *Metadata Variables*. Metadata variables created this way are only available in the ADOMs in which they were created.

Metadata variables can also be created in the Global Database ADOM. When creating ADOM-level metadata variables in the Global Database, you can configure per-ADOM mapping to assign specific values to all devices within an ADOM.

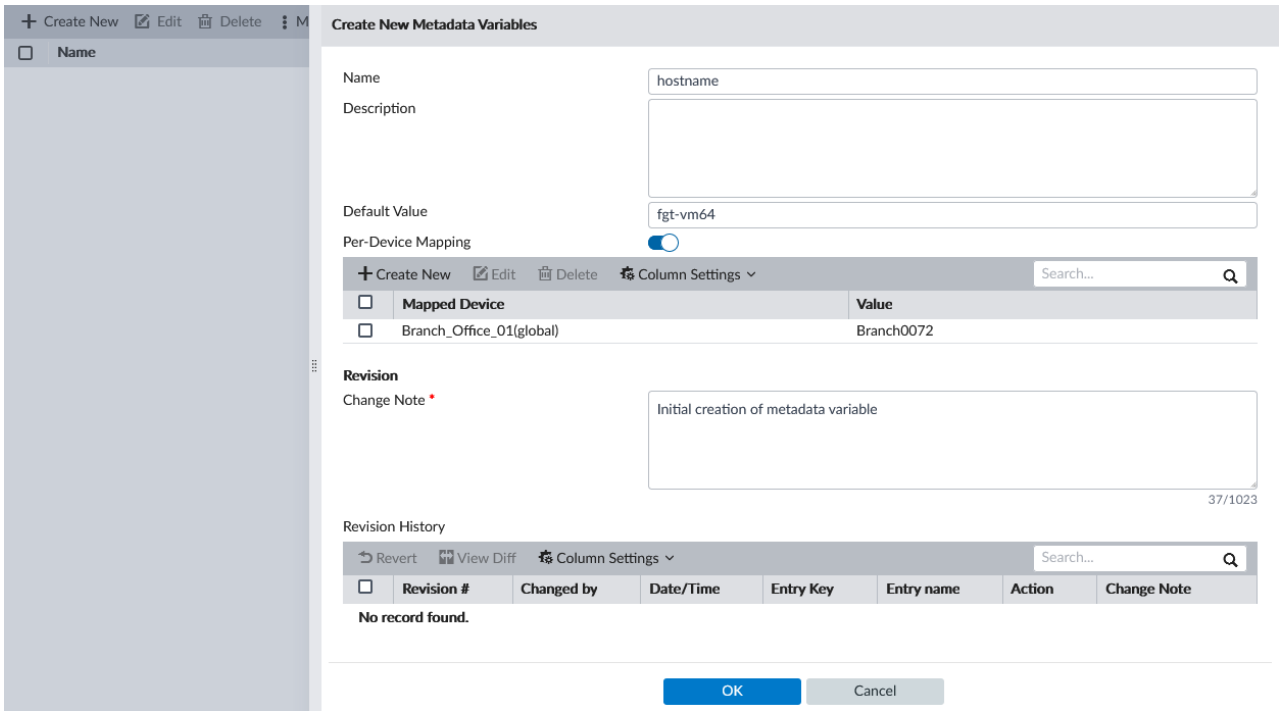
Using the *More* option in the toolbar, you can clone, group, import, and export metadata variables, as well as see where they are being used.



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.

To create an ADOM-level metadata variable:

1. Go to *Policy & Objects* > *Advanced* > *Metadata Variables*.
2. Click *Create New*.
   The *Create New Metadata Variables* window opens.



3. Enter the following information:

Name	Enter a name for the metadata variable.
Description	Optionally, enter a description.
Default Value	Set the default value for the variable. The default value is used whenever a per-device mapping is unavailable.
Per-ADOM Mapping	This setting is only available in the Global Database ADOM. Toggle ON to enable per-ADOM mapping. When enabled, click *Create New* to map an *ADOM* to a *Value*. This value will be applied to all devices in the selected ADOM.
Per-Device Mapping	This setting is not available in the Global Database ADOM. Toggle ON to enable per-device mapping. When enabled, you can configure specific value for each device by clicking *Create New* beneath *Per-Device Mapping* and specifying the *Mapped Device* and *Value*.
Revision	Enter a change note.

4. Click *OK* to save the metadata variable.
You can now use the ADOM's configured variable(s) in provisioning templates created in Device Manager. To configure metadata variable device assignment from the Device Manager, right-click on a managed device in the table and click *Edit Variable Mapping*.

To export metadata variables:

1. Go to *Policy & Objects* > *Advanced* > *Metadata Variables*.
2. Select *More* in the toolbar, and click *Export as JSON* or *Export as CSV*.
The metadata variables will be exported based on the format selected.

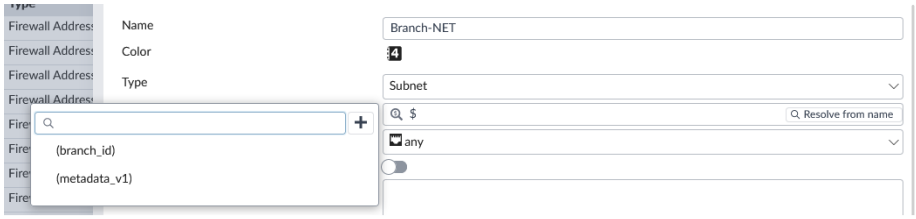
To import metadata variables :

1. Go to *Policy & Objects* > *Advanced* > *Metadata Variables*.
2. Select *More* from the toolbar and click *Import from JSON* or *Import from CSV*.
3. Browse to your exported file, or drag-and-drop it into the file selector, and click *Import*.
4. Select the metadata variables and per-device mapping values to be included in the import, and click *Next* to complete the import process.

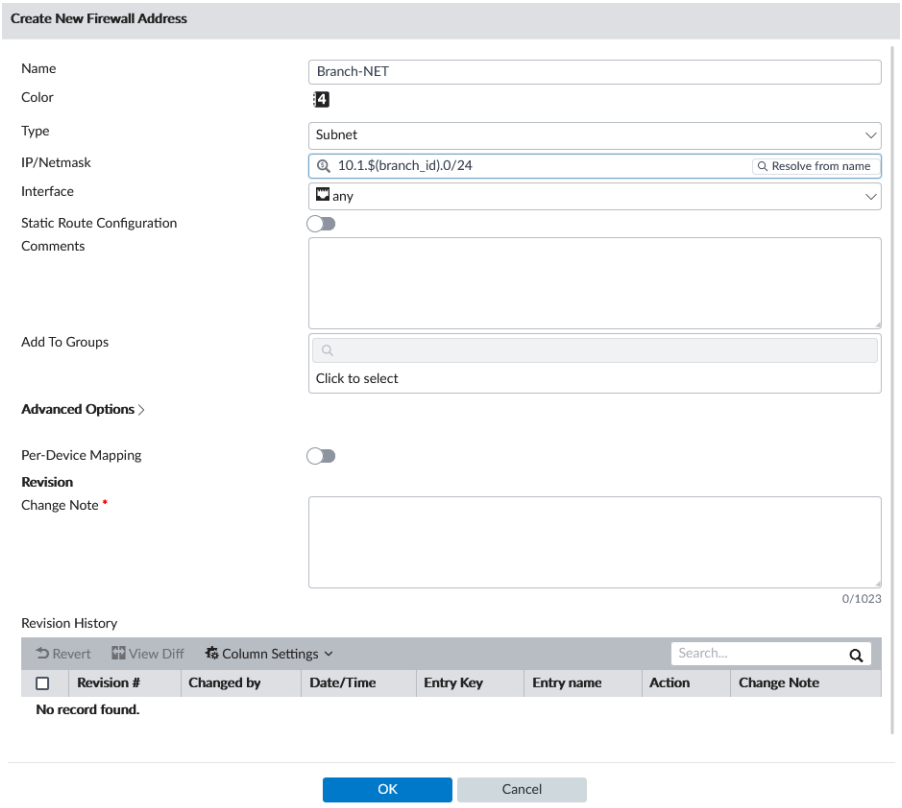
To use a metadata variable in dynamic objects:

1. Go to *Policy & Objects*.
2. Create or edit a Firewall Address, IP Pool, or Virtual IP object.
3. Add the metadata into a text field using the following format: `$<metadata_variable_name>` .

When $ is typed into a supported text field, available metadata variables are displayed for selection. You can click the add button to create a new metadata variable.



For example, when creating a firewall address, you can use a metadata variable in the *IP/Netmask* field.



FortiToken configuration

Below is an example of how FortiToken configuration can be managed on FortiManager.

To configure FortiToken objects for FortiToken management:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *User & Authentication* > *FortiTokens*
3. Click *Create New*.
4. Enter the FortiToken serial numbers and click *OK*.



Alternatively, you may import FortiTokens from a FortiGate using the following methods:

- Import FortiTokens like any other objects. See Importing policies and objects on page 173. Use *Import all objects* to import FortiTokens that are not yet assigned to a user.
- Import FortiTokens from a FortiGate using a text file as follows:
  a. Create a text file containing the FortiToken serial numbers, one per line.
     Note: these FortiTokens must already be registered on an attached FortiGate.
  b. In FortiManager, go to *Policy & Objects* > *User & Authentication* > *FortiTokens* > *Import* and upload the text file.
- Upload a FortiToken seed file (*.ftk*) through *Policy & Objects* > *User & Authentication* > *FortiTokens* > *Import*.

Hardware FortiTokens may be added directly to FortiManager and then distributed to FortiGates.

For more information about adding hardware tokens, see Setting up FortiToken Hardware in the FortiToken Comprehensive Guide.

5. Go to *User & Authentication* > *User Definition* to create a new user.
6. When creating the new user, select *FortiToken*, and then select the FortiToken from the dropdown menu.
7. Go to *User & Authentication* > *User Groups*, create a new user group, and add the previously created user to this group.
8. Install a policy package to the FortiGate, as described in Install a policy package on page 419.
9. On the FortiGate, select *User* > *FortiToken*. Select one of the newly created FortiTokens, then select *OK* to activate the FortiToken.



When your setup requires that FortiToken is added to multiple managed FortiGate devices, FortiAuthenticator can be used in your configuration to manage two-factor authentication across devices. See FortiAuthenticator in the Fortinet Document Library.



FortiToken Mobile tokens must be registered on FortiGate or FortiAuthenticator before importing into FortiManager. See Registering and provisioning FortiToken Mobile tokens in the FortiToken Comprehensive Guide.

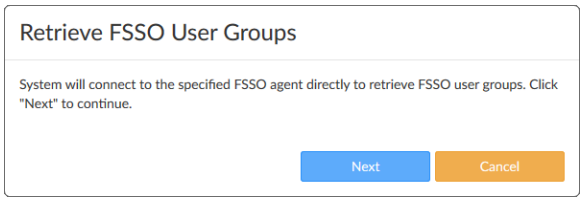
FSSO user groups

FSSO user groups can be retrieved directly from FSSO, from an LDAP server, via a remote FortiGate device, or by polling the active directory server. Groups can also be entered manually.

When user groups are retrieved from an LDAP server, the information is cached on FortiManager for 24 hours by default. After the time expires, the information is deleted from the cache. You can change the default setting by using the `config system global` command with the `ldap-cache-timeout` variable. For more information, see the *FortiManager CLI Reference*.

To get groups from FSSO:

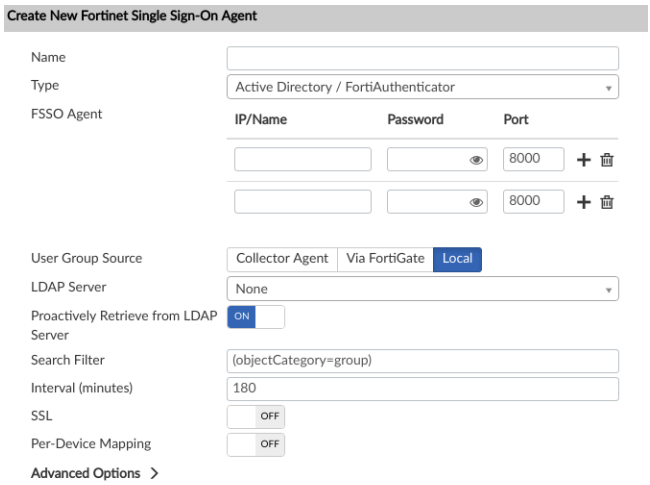
1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Security Fabric* > *Endpoint/Identity*
3. Click *Create New* > *Fortinet Single Sign-On Agent* from the dropdown list.
4. Enter a unique name for the agent in the *Name* field.
5. Enter the IP address or name, password, and port number of the FSSO servers in the FSSO Agent field. Add and remove servers as needed by clicking the *Add* and *Remove* icons at the end of the rows.
6. Select *Collector Agent* in the *User Group Source* field.
7. Click *Apply & Refresh*. The *Retrieve FSSO User Groups* dialog box will open.



8. Click *Next*. The groups are retrieved from the FSSO.
9. Click *OK*. The groups can now be used in user groups, which can then be used in policies.

To get groups from an LDAP server:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Security Fabric* > *Endpoint/Identity*.
3. Click *Create New* > *Fortinet Single Sign-On Agent* from the dropdown list.



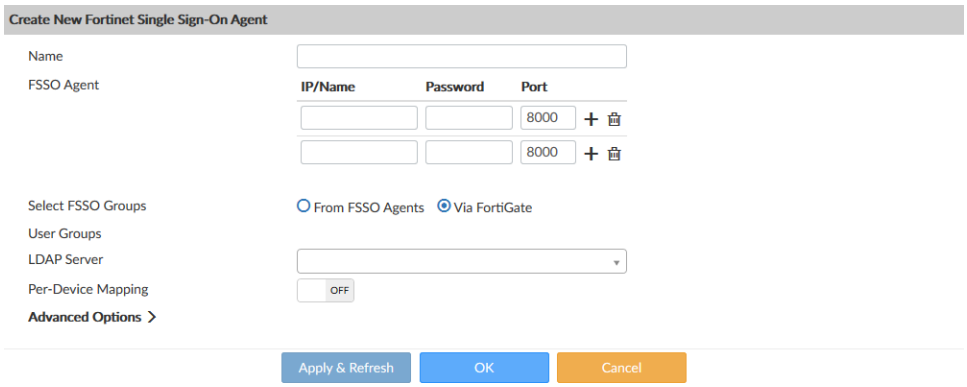
4. Enter a unique name for the agent in the *Name* field.
5. Select *Local* in the *User Group Source*.
6. Select an LDAP server from the drop-down list. LDAP Servers can be added and configured from *User & Device > LDAP Servers*.
7. Toggle *Proactively Retrieve from LDAP Server* to ON.
8. Specify the value for the *Search Filter* and the *Interval* in minutes.
9. For the Select LDAP Groups option, select *Remote Server*. Alternatively, select *Manually Specify* and specify the group names.
10. Select *OK*.

To get groups via a remote FortiGate:



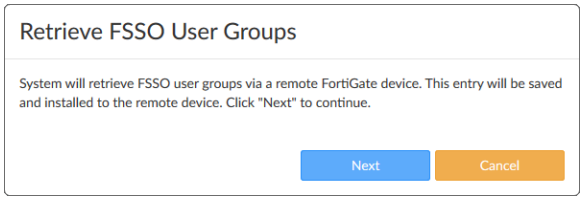
The FortiGate device configuration must be synchronized or retrieving the FSSO user groups will fail. See Checking device configuration status on page 205.

1. Go to *Policy & Objects > Security Fabric > Endpoint/Identity*.
2. Click *Create New > Fortinet Single Sign-On Agent* from the dropdown list. The *Create New Fortinet Single Sign-On Agent* window opens.



3. Enter a unique name for the agent in the *Name* field.

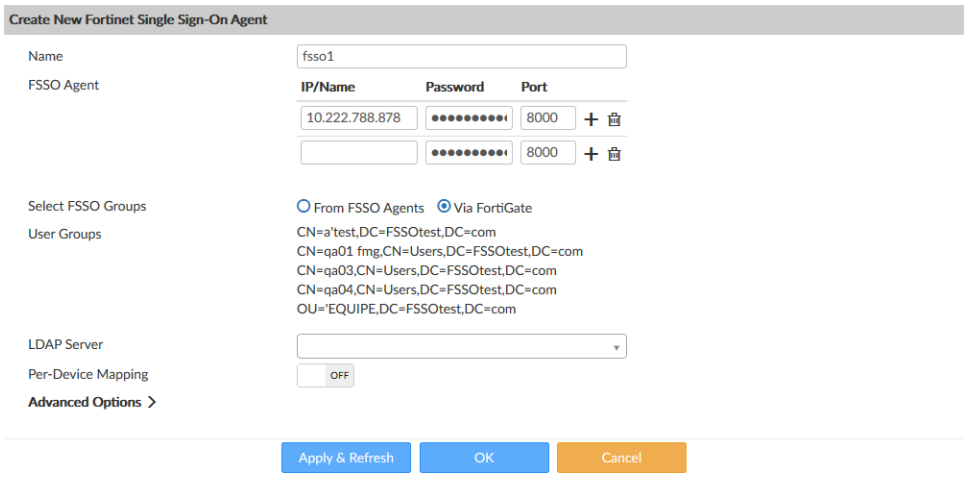
4. Enter the IP address or name, password, and port number of the FSSO servers in the FSSO Agent field. Add and remove servers as needed by clicking the *Add* and *Remove* icons at the end of the rows.
5. Select *Via FortiGate* in the *Select FSSO Groups* field.
6. Click *Apply & Refresh*. The *Retrieve FSSO User Groups* wizard will open.



7. Click *Next* to proceed with the wizard.
8. Select the device that the FSSO groups will be imported from. This device must be authorized for central management by FortiManager, its configuration must be synchronized, and it must be able to communicate with the FSSO server.
9. Click *Next*. The FSSO agent is installed on the FortiGate, the FortiGate retrieves the groups, and then the groups are imported to the FortiManager.



10. After the groups have been imported, click *Finish*. The imported groups will be listed in the *User Groups* field.



11. Click *OK*. The groups can now be used in user groups, which can then be used in policies.



You must rerun the wizard to update the group list. It is not automatically updated.

To get groups from AD:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Security Fabric > Endpoint/Identity*.
3. Click *Create New > Poll Active Directory Server* from the dropdown list.
4. Configure the server name, local user, password, and polling.
5. Select an LDAP server from the drop-down list. LDAP Servers can be added and configured from *User & Device > LDAP Servers*.
6. Select groups from the *Groups* tab, then select *Add Selected* to add the groups.

   You can also select *Manually Specify* in the *Select LDAP Groups* field, and then manually enter the group names.
7. Select *OK*.

VIP mapping

Normally, Virtual IP (VIP) objects map to a single interface, or *ANY*, just as with FortiOS. In the special case where the interface that the VIP is bound to belongs to a zone, FortiManager handles importing and installing the object in a unique way.

When importing a policy package, the VIP is bound to the zone instead of the interface. If per-device mapping is enabled for the VIP, FortiManager automatically adds dynamic mapping for that device that maps the VIP to the specific interface. To use the VIP on another FortiGate, you can add an interface mapping entry for the other FortiGate. The zone acts as filter, limiting the interfaces that can be selected. That is, you can only select an external interface that is a member of the selected zone.

FortiManager binds the VIP to a zone because it needs to know which policies the VIP could be applied to. FortiGate devices use different logic because they already know the zone membership.

In FortiOS, VIPs can only by bound to an interface, and not a zone. Consequently, if there is no matching per-device mapping, FortiManager will convert the binding to *ANY* when installing configuration changes to FortiGate. Depending on the circumstance, this can be avoided by:

- Leaving per-device mapping enabled on the VIP at the ADOM, and letting FortiManager add the required per-device mappings.
- If you are configuring FortiManager to start using the VIP on other FortiGates, adding the per-device mappings manually.

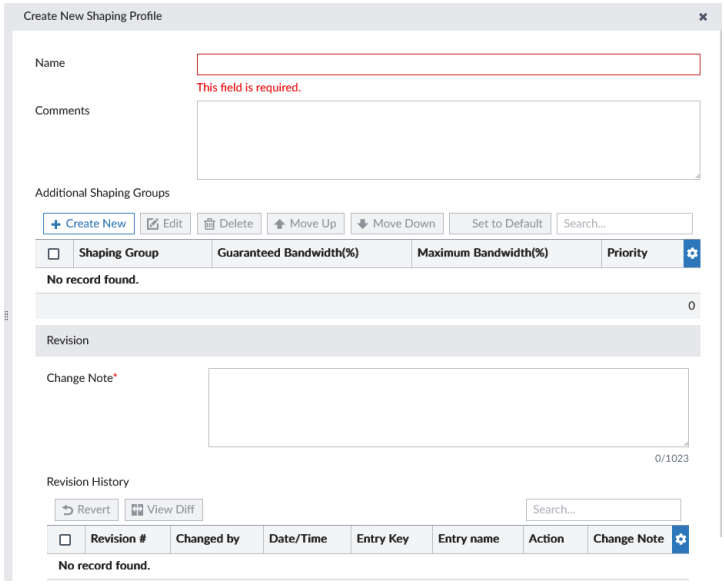
Shaping profiles

Create a new shaping profile to manage traffic. After the profile is created, you can assign it to an interface.

To create a new shaping profile:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Firewall Objects > Shaping Profile*.

3. Click *Create New*. The *Create New Shaping Profile* pane opens.



4. Select or specify the values for the following and click *OK*:

Name	Specify the name for the shaping profile.
Comments	Optionally enter comments about the shaping profile.
Additional Shaping Groups	Click *Create New*. Specify the *Shaping Group*, *Guaranteed Bandwidth (%)*, *Maximum Bandwidth(%)* and *Priority*. Click *OK*.

5. Assign the shaping profile to an interface. See Assigning a shaping profile on page 565.

After shaping profiles are defined, they can be assigned to each ADOM interface you want to do traffic shaping for egress. The shaping profile can be set as default as well as in dynamic mapping. Any changes to the shaping profile is applied to the FortiGate devices dynamically.

Assigning a shaping profile

You can assign an interface-based shaping profile for each device.

To display this option, go to *Device Manager* > *Device & Groups*. From the dashboard toolbar, select *Display Options*, and then select the *Interface* checkbox.

To assign a shaping profile:

1. Go to *Device Manager* > *Device & Groups*.
   a. In the tree menu, select the device group.
   b. Below the tree menu, select a device.
2. In the dashboard toolbar, go to *Network* > *Interfaces*.

3. Select an interface from the list. The *Edit Interface* page opens.
4. Toggle *Shaping Profile* to *ON*. The *Egress* and *Ingress* dropdowns are displayed.
5. Select a shaping profile from the dropdown, and then click *OK*.

Viewing the traffic shaping widget

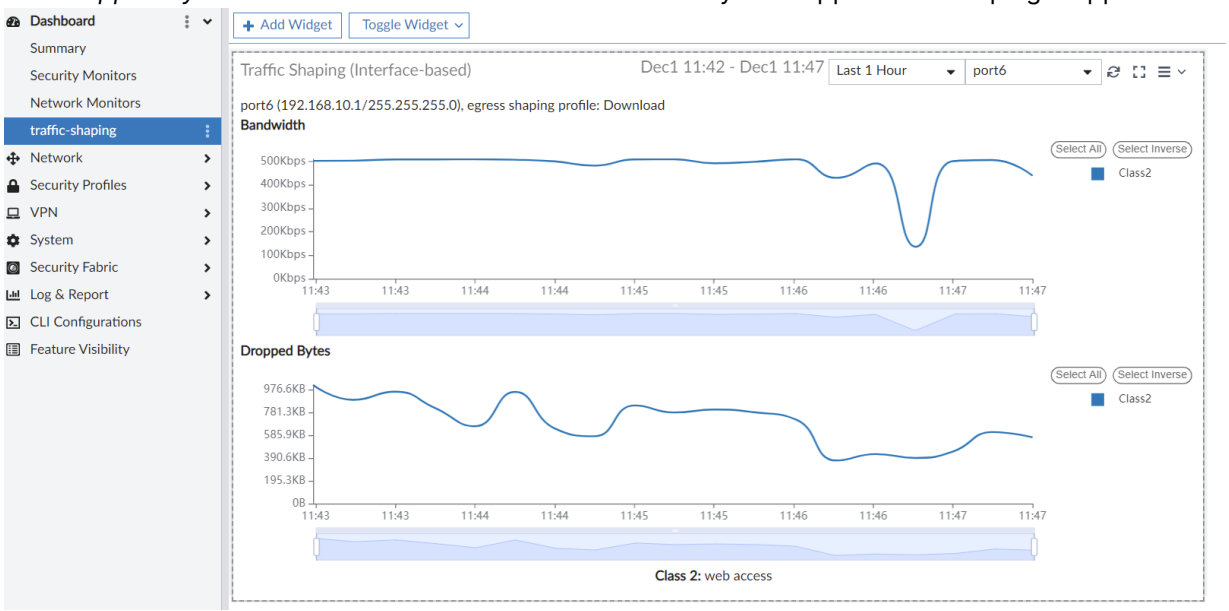
You can view the *Traffic Shaping* widget in the *Device Manager*.

To view traffic shaping information, you must enable traffic shaping history. Traffic shaping history can be enabled in the CLI using the following commands:

```
config system admin setting
   set traffic-shaping-history enable
end
```

To view the Traffic Shaping monitor:

1. Go to *Device Manager* > *Device & Groups*, and select a device.
2. In the device database's toolbar, select or create a *Dashboard*.
3. On the dashboard page, click *Add Widget* in the toolbar, and select the *Traffic Shaping (Interface-based)*. The *Traffic Shaping (Interface-based)* widget is added to the dashboard.
4. From the dropdown, select an interface.
   - The *Bandwidth* chart shows the real-time bandwidth for each class.
   - The *Dropped Bytes* chart shows the real-time statistics for bytes dropped after shaping is applied.



Intrusion prevention (IPS)

This section includes the following topics for IPS.

- Intrusion prevention filtering options on page 567
- Intrusion prevention signatures on page 569

Restricted IPS administrators can be configured in FortiManager. See the following topics for more information:

- Intrusion prevention restricted administrator on page 993
- Intrusion prevention profiles on page 995
- Intrusion prevention signatures on page 998
- Intrusion prevention diagnostics on page 998
- Intrusion prevention hold-time and CVE filtering on page 999
- Intrusion prevention FortiGuard packages on page 1000
- Intrusion prevention licenses and services on page 1001
- Intrusion prevention templates on page 1002
- Intrusion prevention global headers and footers on page 1003
- IPS administration permissions on page 1004

Intrusion prevention filtering options

Intrusion Prevention (IPS), detects and blocks network-based attacks. You can configure IPS sensors based on IPS signatures, IPS filters, outgoing connections to botnet sites, and rate-based signatures. FortiManager includes nine preloaded IPS sensors:

- *all_default*
- *all_default_pass*
- *default*
- *high_security*
- *protect_client*
- *protect_email_server*
- *protect_http_server*
- *sniffer-profile*
- *wifi-default*

You can customize these sensors, or you can create your own and apply it to a firewall policy.



This functionality requires a subscription to FortiGuard IPS Service.

Add Filter

To add an IPS filter:

1. Go to *Policy & Objects* > *Security Profiles* > *Intrusion Prevention*.
   If you are logged in as a Restricted Admin, go to *Intrusion Prevention* > *Profiles*.
2. Create a new profile or select the profile you want to update.
3. In the *IPS Signatures and Filters* section, create a new filter or select a filter to update.
   The *Create New IPS Signatures and Filters* dialog box is displayed.
4. Add the filter.
   a. Click *Add Filter*.
   b. Click the *Add Filter* option and select a filter type from the dropdown menu, and enter the corresponding filter data. Available filters include: *Applications*, *OS*, *Protocol*, *Severity*, *Target*, *Default Action*, *Default Status*, *Vulnerability Type*, and *CVE-ID*.

   Default Action, *Default Status*, and *Vulnerability Type* are only available in 7.2 ADOMs and later.
5. Click *Use Filters*, and click *OK*.

Hold-time

The hold-time option allows you to set the amount of time that signatures are held after a FortiGuard IPS signature update per VDOM. During the holding period, the signature's mode is *monitor*. The new signatures are enabled after the hold-time to avoid false positives.

The hold-time can be from 0 days and 0 hours (default) up to 7 days, in the format ##d##h.

To delay an IPS signature activation:

1. Go to *Device Manager* > *Device & Groups*.
2. Select a managed device.
3. In the toolbar, click *CLI Configuration*. To display the menu, see Device DB - CLI Configurations on page 227.
4. In configurations menu, go to *System* > *IPS*. The *system ips* dialog box is displayed.
5. Ensure *override-signature-hold-by-id* is enabled.
6. In the *signature-hold-time* field, enter the number of days or hours hold and monitor the IPS signatures.

CVE pattern

The CVE pattern option allows you to filter IPS signatures based on CVE IDs or with a CVE wildcard, ensuring that any signatures tagged with that CVE are automatically included.

To add an IPS CVE filter:

1. Go to *Policy & Objects* > *Security Profiles* > *Intrusion Prevention*.
   If you are logged in as a Restricted Admin, go to *Intrusion Prevention* > *Profiles*.

2. Create a new profile or select the profile you want to update.
3. In the *IPS Signatures and Filters* section, create a new filter or select a filter to update.
   The *Create New IPS Signatures and Filters* dialog box is displayed.
4. Add the CVE filter.
   a. Click the *Filter* icon.
   b. Click *Add Filter > CVE ID*.
   c. Enter the CVE ID, then click *Use Filters*, and click *OK*.
5. Click *OK*.

Intrusion prevention signatures

Use the *IPS Signatures* monitor page to see where a signature is used, create a new IPS profile, or add the signature to an existing profile.



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects > Tools > Feature Visibility*, and add or remove a checkmark for the corresponding feature.



To view the IPS Signatures page as a Restricted Administrator, see Intrusion prevention signatures on page 998.



The *ID* field displayed for IPS signatures in the FortiManager GUI corresponds with the following: The `attackid` log field on FortiGate, the *ID* field in the FortiOS GUI, the *Rule* field when diagnosing the IPS signature on FortiOS, and the IPS entry ID in the FortiGuard IPS encyclopedia.

Managing IPS Signatures

Right-click a signature in the page to view where the signature is used, or add it to a new or existing IPS profile.

To view where a signature is used:

1. Right-click a signature, and select *Where Used*. The *Where <signature_name> is used* window displays.
2. (Optional) Select a signature in the list, and click *Edit* to modify the signature.
3. (Optional) Select a signature in the list, and click *View* to display the signature details.

To create a new IPS profile:

1. Right-click a signature, and select *Add to IPS Profile*. The *Add to IPS Profile* dialog is displayed.
2. Click *Create New IPS Profile*.
3. In the *Profile Name* field, type a name for the profile.
4. From the *Action* dropdown, select the profile action.
5. (Optional) In the *Comments* field, describe the IPS profile.

6. (Optional) Click *Signatures* to add more signatures to the profile.
7. Click *OK*.

To add signatures to an existing profile:

1. Right-click a signature, and select *Add to IPS Profile*. The *Add to IPS Profile* dialog is displayed.
2. Click *Profile(s)* to select the profiles, and then click *OK*.
3. In the *Profile Name* field, type a name for the profile.
4. From the *Action* dropdown, select the profile action.
5. (Optional) Click *Signatures* to add more signatures to the profile.
6. Click *OK*.

To check device on-hold status:

1. Go to *Policy & Objects* > *Security Profiles* > *IPS Signatures*.
2. In the toolbar, click *More* > *Check On-Hold Status*.
3. Select a device from the *Device* list dropdown, and click *OK*.
   The *All On-Hold Signatures* monitor is displayed showing the current list of on-hold IPS signatures for the selected device.

To make a signature global:

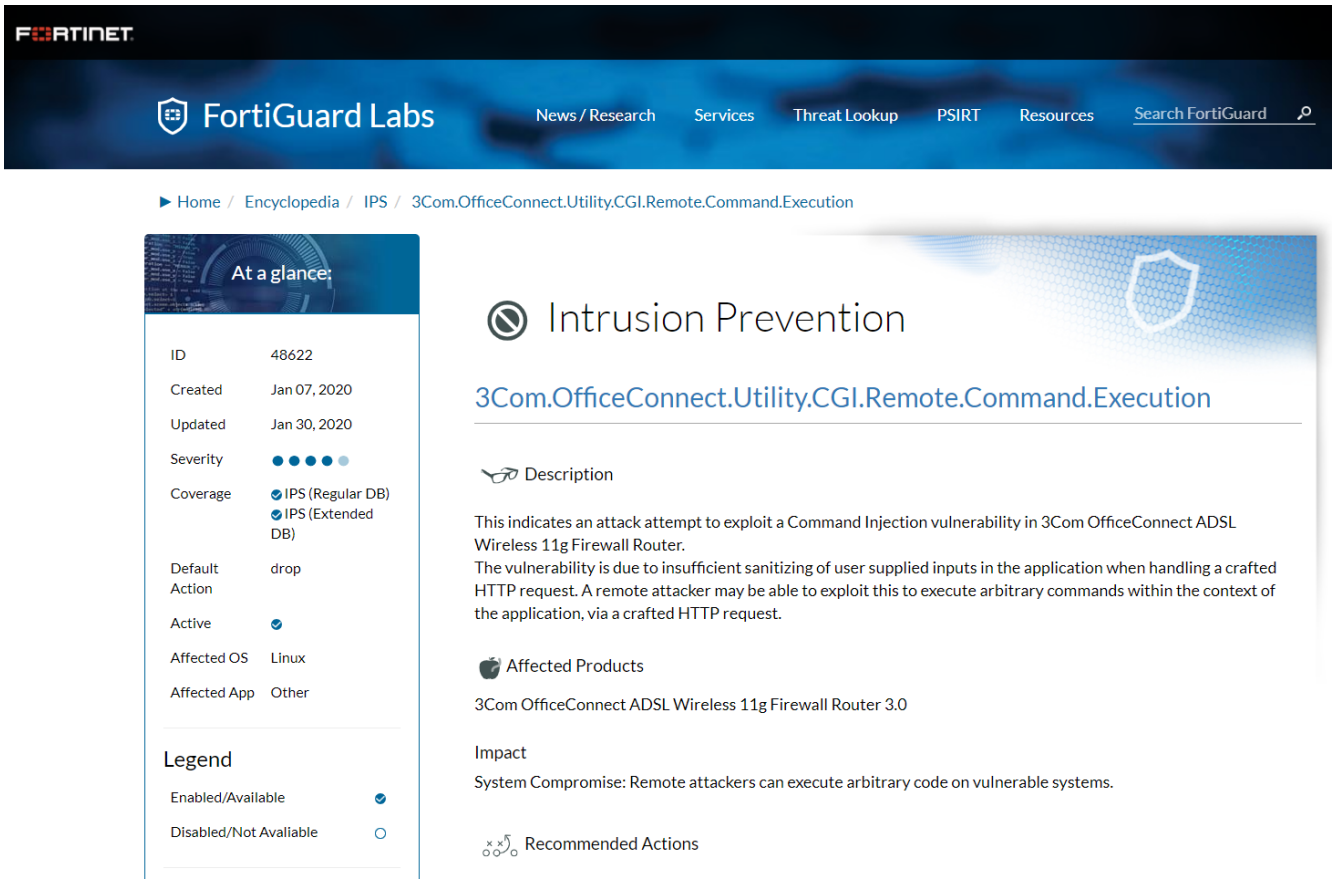
Right-click a signature, and select *Promote to Global*.

Viewing IPS Signature details

To view IPS Signature *Information* page, click the IPS signature name. The following information is displayed:

Section	Description
Name	The IPS signature name.
Risk	Displays the risk level.
Summary	Describes the threats and vulnerabilities detected by the IPS signature.
Affected Products	Displays the products that are vulnerable to the attack.
Action	Provides recommendations to prevent an attack.
Analysis	Provides specific details about how the vulnerability can be exploited.
References	A list of links you can visit for more information.
Miscellaneous	The signature ID.

To view information about the signature ID in FortiGuard, click the ID link in the *ID* column.



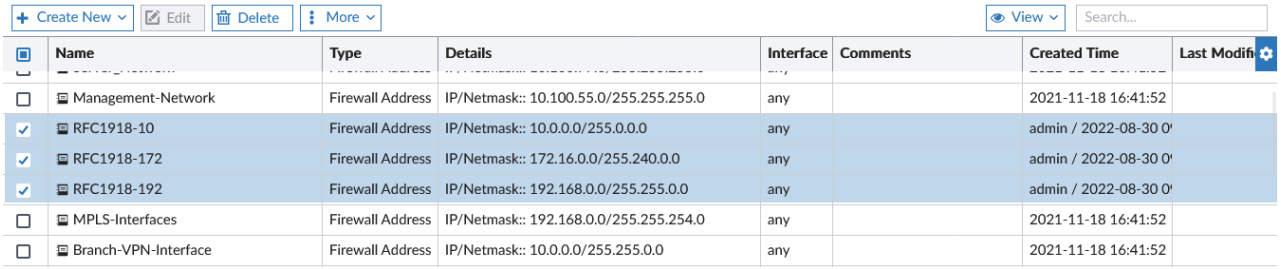
Default address space objects

FortiManager includes default addresses for RFC1918 addresses spaces which are commonly used when setting up firewall objects and policies in FortiManager. RFC1918 default addresses are included in an address group for ease of use in your policies.

To view default RFC1918 addresses and address groups, go to *Policy & Objects* > *Firewall Objects* > *Addresses*.

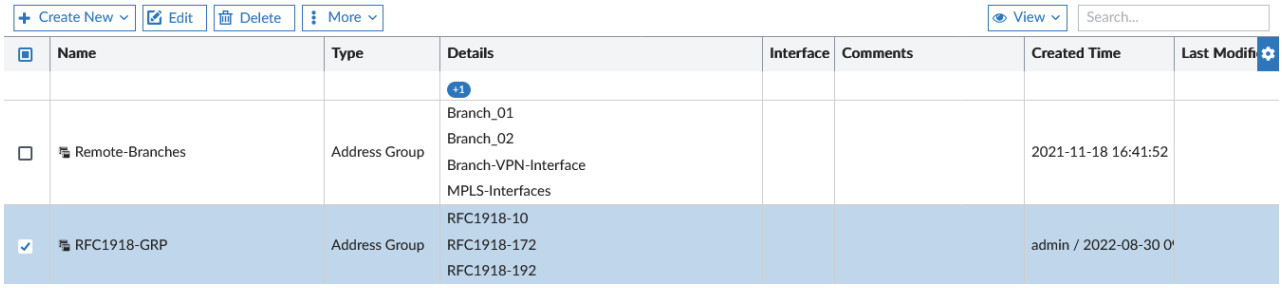
The following default RFC1918 address objects are available under *Address*:

- *RFC1918-10* with IP/Netmask: 10.0.0.0/255.0.0.0
- *RFC1918-172* with IP/Netmask: 172.16.0.0/255.240.0.0
- *RFC1918-192* with IP/Netmask: 192.168.0.0/255.255.0.0



The following default RFC1918 address group containing the three address objects is available under *Address Group*:

- *RFC1918-GRP*



Zero Trust Network Access (ZTNA) objects

Zero Trust Network Access (ZTNA) objects (security posture tags, tag groups, and geographic IP objects) and ZTNA servers can be configured in FortiManager.

For more information on configuring ZTNA, see the FortiGate Administration Guide.

Viewing security posture tags

Security Posture Tag displays the security posture tags synchronized to FortiGate from FortiClient EMS or FortiClient EMS Cloud. You can dynamically synchronize security posture tags using a FortiClient EMS connector.

Security posture tags can be edited, cloned and deleted from this dashboard.



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.

Once a security posture tag has been configured, you can select the object in a proxy policy with the ZTNA proxy type. See Create a new proxy policy on page 471.

To view security posture tags:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Firewall Objects* > *Security Posture Tag*.
   Security posture tags synchronized from the FortiGate are displayed.

To clone security posture tags:

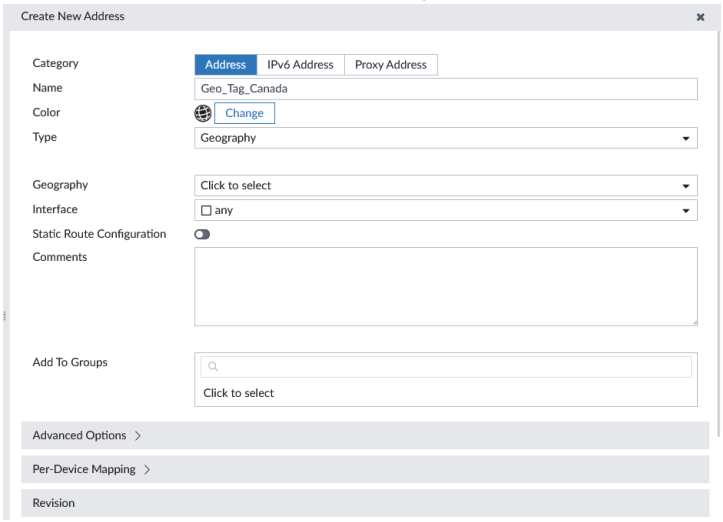
1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Firewall Objects* > *Security Posture Tag*.
3. Right-click on an existing tag, and select *Clone*.

4. Enter a name for the tag.
5. Configure the details of for the tag.
6. Click *OK* to save the *Security PostureTag*.

Creating ZTNA geographic IP objects

To create a Geographic IP address object:

1. Go to *Policy & Objects* > *Firewall Objects* > *Addresses*, click *Create New*, and select *Address*.
   The Create New Address window opens.



2. Enter a name for the address object.
3. Select *Geography* as the *Type*, and choose a location from the *Geography* dropdown.
4. Select *OK* to save the address object.

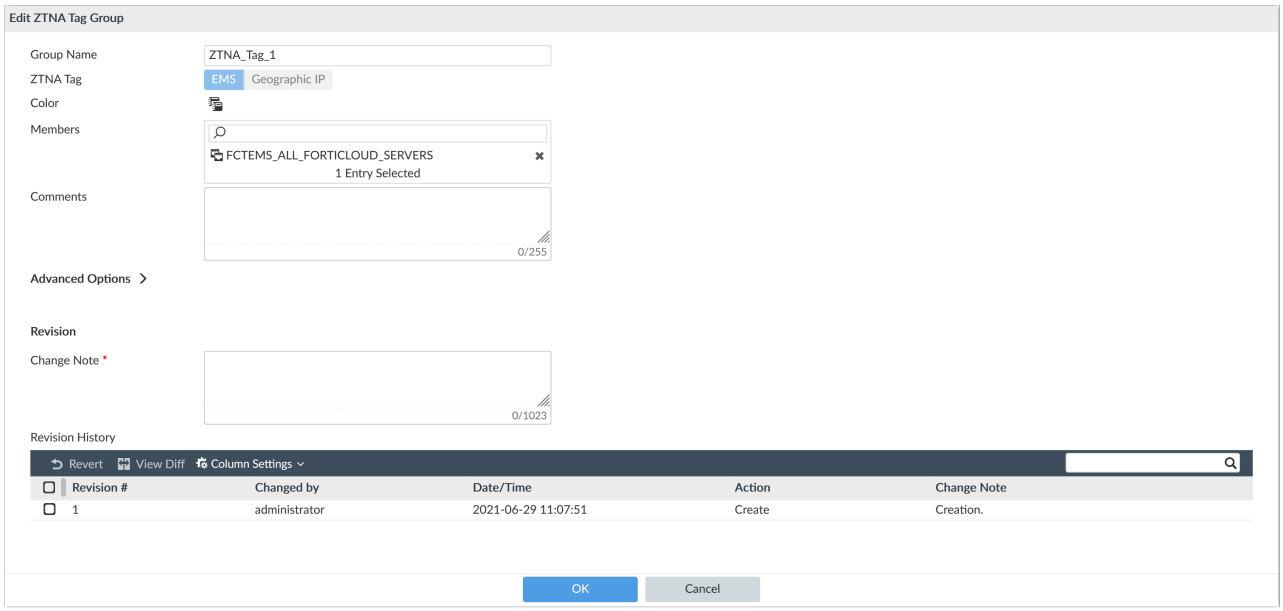
Creating security posture tag groups

You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.

Once a security posture tag group has been configured, you can select the object in a proxy policy with the ZTNA proxy type. See Create a new proxy policy on page 471.

To create a security posture tag group:

1. Go to *Policy & Objects* > *Firewall Objects* > *Security Posture Tag*, and click *Create New*.
   The *Create New Security Posture Tag Group* window opens.



2. Enter a name for the group.
3. Select a *Security Posture Tag* type from one of the following:
   - EMS
   - Geographic IP
4. Select *Members* to add to the security posture tag group.
   - When configuring an *EMS* tag group, members are configured in *Policy & Objects > Firewall Objects > Security PostureTag* with an *IP* or *MAC* object type. See Viewing security posture tags on page 572.
   - When configuring a *Geographic IP* tag group, members are configured in *Policy & Objects > Firewall Objects > Addresses* as a *Firewall Address* with the *Type* set as *Geography*. See Creating ZTNA geographic IP objects on page 573.
5. Click *OK* to save the group.

Configuring a ZTNA server

You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects > Tools > Feature Visibility*, and add or remove a checkmark for the corresponding feature.

To configure a ZTNA server, define the access proxy VIP and the real servers that clients will connect to. The access proxy VIP is the FortiGate ZTNA gateway that clients make HTTPS connections to. The service/server mappings define the virtual host matching rules and the real server mappings of the HTTPS requests.

Once a ZTNA server has been configured, you can select the object in a proxy policy with the ZTNA proxy type. See Create a new proxy policy on page 471.

To create a ZTNA Server:

1. Go to *Policy & Objects > Firewall Objects > ZTNA Server*, and click *Create New*.
2. Enter a name for the server.

3. Select an *External Interface*, enter the *External IP* address, and select the *External Port* that the clients will connect to.
4. Select the *Default Certificate*. Clients will be presented with this certificate when they connect to the access proxy VIP.
5. Add a server mapping, and a server.
6. Click *OK* to save your changes.

FortiProxy content analysis objects



Content analysis objects are only available in FortiProxy ADOMs. See FortiProxy ADOMs on page 926.

Content analysis objects can be enabled in FortiProxy ADOMs using the *Feature Visibility* menu in the the *Tools* dropdown. Content analysis objects include the following types:

- ICAP profile on page 575
- ICAP remote server on page 576
- ICAP load balancing on page 576

For more information, see the FortiProxy Administration Guide on the Fortinet Document Library.

ICAP profile



You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.



Content analysis objects are only available in FortiProxy ADOMs. See FortiProxy ADOMs on page 926.

To create an ICAP profile:

1. Go to *Policy & Objects* > *Content Analysis* > *ICAP Profile*, and click *Create New*.
   The *Create New ICAP Profile* window appears.
2. Enter the following information:

Name	Enter a name for the ICAP profile.
Enable Request Processing	Enable or disable request processing. If you enable request processing, select a server from the dropdown menu, specify the path on the server to the processing component, and then select the behavior on failure, either *Error* or *Bypass*.

Enable Response Processing	Enable or disable response processing. If you enable response processing, select a server from the dropdown menu, specify the path on the server to the processing component, and then select the behavior on failure, either *Error* or *Bypass*.
Enable Streaming Media Bypass	Enable to allow streaming media to ignore offloading to the ICAP server.

ICAP remote server

You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.

Content analysis objects are only available in FortiProxy ADOMs. See FortiProxy ADOMs on page 926.

To create an ICAP remote server:

1. Go to *Policy & Objects* > *Content Analysis* > *ICAP Remote Server*, and click *Create New*. The *Create New ICAP Remote Server* window appears.
2. Enter the following information:

Name	Enter a name for the ICAP remote server.
Address Type	Select the address type.
IP Address	Enter the IP address of the ICAP remote server.
Plain ICAP Connection and Secure ICAP Connection	Select whether the ICAP connection is plain or secure. Only one setting can be enabled at a time.
Max Connections	Configure the maximum number of connections.

ICAP load balancing

You must enable the visibility of this feature in *Policy & Objects* before it can be configured. To toggle feature visibility, go to *Policy & Objects* > *Tools* > *Feature Visibility*, and add or remove a checkmark for the corresponding feature.

Content analysis objects are only available in FortiProxy ADOMs. See FortiProxy ADOMs on page 926.

To create an ICAP load balancing object:

1. Go to *Policy & Objects* > *Content Analysis* > *ICAP Load Balancing*, and click *Create New*.
   The *Create New ICAP Load Balancing* window appears.
2. Enter the following information:

Name	Enter a name for the ICAP load balancer.
Method	Select the load balancing method from *Weighted*, *Least Session*, or *Active Passive*.
Remote Server	Click to add a remote server. You can select a remote server from the dropdown menu and then apply weighting to the selected servers.

ADOM revisions

ADOM revision history allows you to maintain a revision of the policy packages, objects, and VPN console settings in an ADOM. Revisions can be automatically deleted based on given variables, and individual revisions can be locked to prevent them being automatically deleted.

To configure ADOM revisions, go to *Policy & Objects*, and click *ADOM Revisions*.

This page displays the following:

ID	The ADOM revision identifier.
Name	The name of the ADOM revision. This field is user-defined when creating the ADOM revision. A lock icon will be displayed beside the ADOM revision name when you have selected *Lock this revision from auto deletion*.
Created by	The administrator that created the ADOM revision.
Created Time	The ADOM revision creation date and time.
Comment	Optional comments typed in the *Description* field when the ADOM revision was created.

The following options are available:

Create New	Select to create a new ADOM revision.
Edit	Right-click on a revision in the table and select *Edit* in the menu to edit the ADOM revision.
Delete	Right-click on a revision in the table and select *Delete* in the menu to delete the ADOM revision. When *Lock this revision from auto deletion* is selected, you are not able to delete the ADOM revision.

View Revision Diff	Right-click on a revision in the table and select *View Revision Diff* in the menu. The Summary page will be displayed. This page shows the revision differences between the selected revision and the current database.
Restore	Right-click on a revision in the table and select *Restore* in the menu to restore the ADOM revision. Restoring a revision will revert policy packages, objects and VPN console to the selected version. Select *OK* to continue.
More > Lock Revision	Right-click on a revision in the table and select *Lock* from the *More* menu to lock this revision from auto deletion.
More > Unlock Revision	Right-click on a revision in the table and select *Unlock* from the *More* menu to unlock this revision. When the ADOM revision is in an unlocked state, auto deletion will occur in accordance with your auto deletion settings.
Settings	Select to configure the automatic deletion settings for ADOM revisions.
Close	Select to close the *ADOM Revision* dialog box and return to the *Policy & Objects* tab.

To create a new ADOM revision:

1. Go to *Policy & Objects*, and click *ADOM Revisions*. The *ADOM Revision* dialog box opens.
2. Click *Create New*. The *Create New Revision* dialog box opens.
3. Type a name for the revisions in the *Name* field.
4. Optionally, type a description of the revision in the *Description* field.
5. To prevent the revision from being automatically deleted, select *Lock this revision from auto deletion*.
6. Click *OK* to create the new ADOM revision.

To edit an ADOM revision:

1. Open the *ADOM Revisions* dialog box.
2. Select a revision, and click *Edit*. The *Edit Revision* dialog box opens.
3. Edit the revision details as required, then click *OK* to apply your changes.

To delete ADOM revisions:

1. Open the *ADOM Revisions* dialog box.
2. Select a revision, and click *Delete*.
   You can select multiple revisions by selecting the checkbox beside each revision.
3. Click *OK* in the confirmation dialog box to delete the selected revision or revisions.

To configure automatic deletion:

1. Open the *ADOM Revisions* dialog box, and click *Settings*.
2. Select *Auto delete revision* to enable to automatic deletion of revisions.
3. Select one of the two available options for automatic deletion of revisions:
4. *Keep last x revisions*: Only keep the entered numbered of revisions, deleting the oldest revision when a new revision is created.
5. *Delete revisions older than x days*: Delete all revisions that are older than the entered number of days.

6. Click *OK* to apply the changes.

To restore a previous ADOM revision:

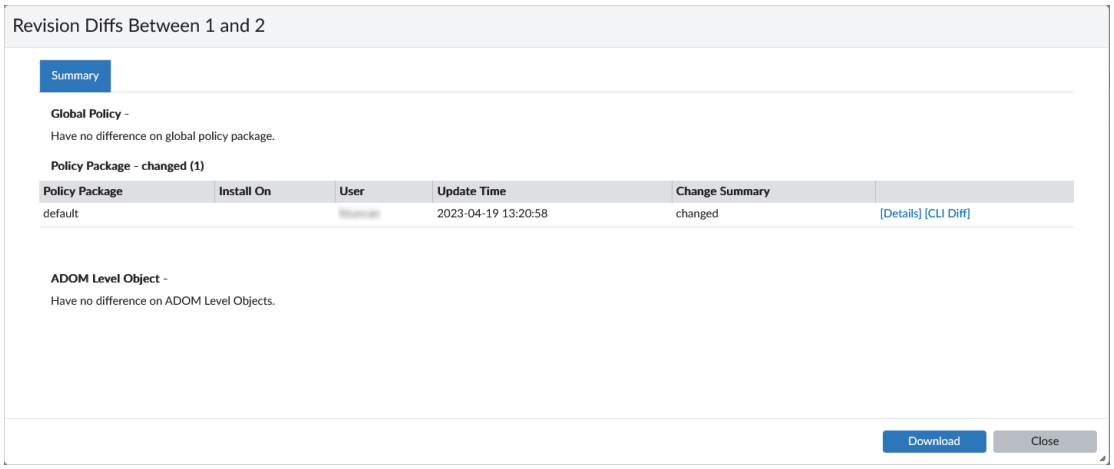
1. Open the *ADOM Revisions* window.
2. Select a revision, and click *Restore*. A confirmation dialog box will appear.
3. Click *OK* to continue.
   The *Restore Revision* dialog box opens. Restoring a revision will revert policy packages, objects and VPN console to the selected version.
4. Click *OK* to continue.

To lock or unlock an ADOM revision:

1. Open the *ADOM Revisions* window.
2. Do one of the following:
   - Select a revision, and select *Lock* or *Unlock* from the *More* menu.
   - Edit the revision, and select or clear the *Lock this revision from auto deletion* checkbox in the *Edit ADOM Revision* dialog box.

To view ADOM revision diff:

1. Open the *ADOM Revisions* window.
2. Select a revision, and click *View Revision Diff*. The *Revision Diffs Between* dialog box opens.



   This page displays all *Global Policy*, *Policy Package*, and *ADOM Level Object* changes between the revision selected and the current database.
3. Select *[Details]* to view all details on the changes made to policies and objects.
4. Select *CLI Diff* to view the CLI changes between revisions.
5. You can select to download this information as a CSV file to your management computer.
6. Click *Close* to return to the *ADOM Revisions* window.

AP Manager

The *AP Manager* pane allows you to manage FortiAP access points that are controlled by FortiGate devices and are managed by FortiManager. FortiAP devices must be added to a FortiGate and cannot be directly added to FortiManager as a standalone device.

You can use *AP Manager* for the following modes of management:

Central management of managed access points	When central management is enabled, you can view, create, edit, and import profiles. These profiles share a common database and can be applied to any device, regardless of which FortiGate controller it is connected to. Central management mode is recommended when you need to create common profiles to share between different FortiAP devices, for example in environments where you have many AP devices and managing the settings for each device individually is not practical. Configuration of AP settings is completed in the AP Manager. When an install occurs, only necessary configurations (configurations that are directly referenced in a profile assigned to the AP) are installed to the managing FortiGate.
Per-device management of managed access points	When per-device management is enabled, you can change settings for each managed access point. All FortiAP devices and WiFi profiles are managed at the device level with no shared objects. Per-device management mode is recommended when you want to manage each FortiAP configuration individually. Configuration of AP settings is completed in the AP Manager. When an install occurs, all configurations for the AP are synchronized to the managing FortiGate.

The *AP Manager* tree menu contains the following items:

Managed FortiAPs on page 581	Displays unauthorized and authorized FortiAP devices. You can view, authorize, and edit authorized FortiAP devices.
WiFi Maps on page 600	View the locations of FortiAP devices on Google Maps. You can create a floor map, add an image of a floor map, and place the FortiAP devices on the map.
SSIDs	View and create SSIDs. (Central management only)
Operational Profiles	View and create operational profiles. (Central management only)
Connectivity Profiles	View and create connectivity profiles. (Central management only)
Protection Profiles	View and create protection profiles. (Central management only)
WiFi Settings	View and configure WiFi settings. (Central management only)

Managed FortiAPs

The *Managed FortiAPs* pane allows you to manage FortiAP devices that are controlled by FortiGate devices and are managed by the FortiManager.

FortiAP devices are grouped based on the controller that they are connected to. The devices can also be further divided into groups within a controller.

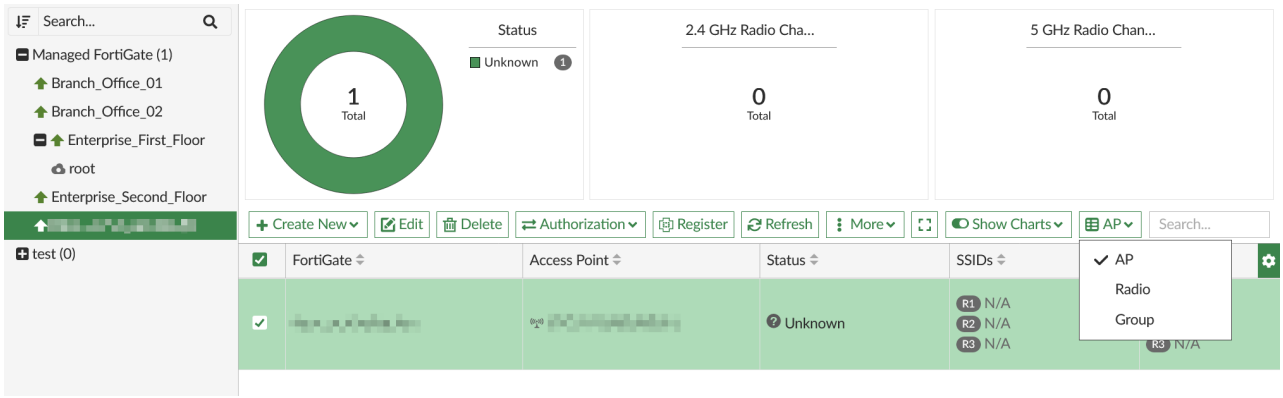
FortiAP devices can be managed centrally, or per-device (see Creating ADOMs on page 934). In per-device mode, all WiFi profiles (SSIDs, AP profiles, and others), as well as managed FortiAP devices, are managed at the device level – there are no shared objects.

Additional configuration options and short-cuts are available using the right-click content menu. Right-click on the mouse on different parts of the navigation panes on the GUI page to access these context menus.

If workspace or workflow is enabled, the ADOM must be locked before changes can be made. See Locking an ADOM on page 947.

To manage FortiAP devices:

1. Go to *AP Manager* > *Managed FortiAPs*.
2. Select a *Managed FortiGate*.
   APs for the selected managed FortiGate device are displayed.
3. (Optional) In the toolbar, click *List* > *Group*, to view FortiAP groups. See FortiAP groups on page 590



Quick status bar

You can quickly view the status of devices on the *Managed FortiAPs* pane with the quick status bar, which contains the following charts:

- Status
- 2.4 GHz Radio Channel Utilization

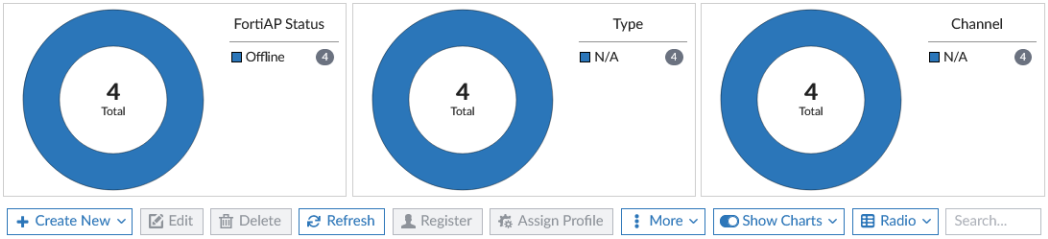
- 5 GHz Radio Channel Utilization

You can click each status in the legend to display in the content pane only the devices referenced in the quick status.

Use the *Show Charts* dropdown and toggle to show or hide charts. From the dropdown, select or de-select checkboxes to show or hide the respective chart.

To use charts in the quick status bar:

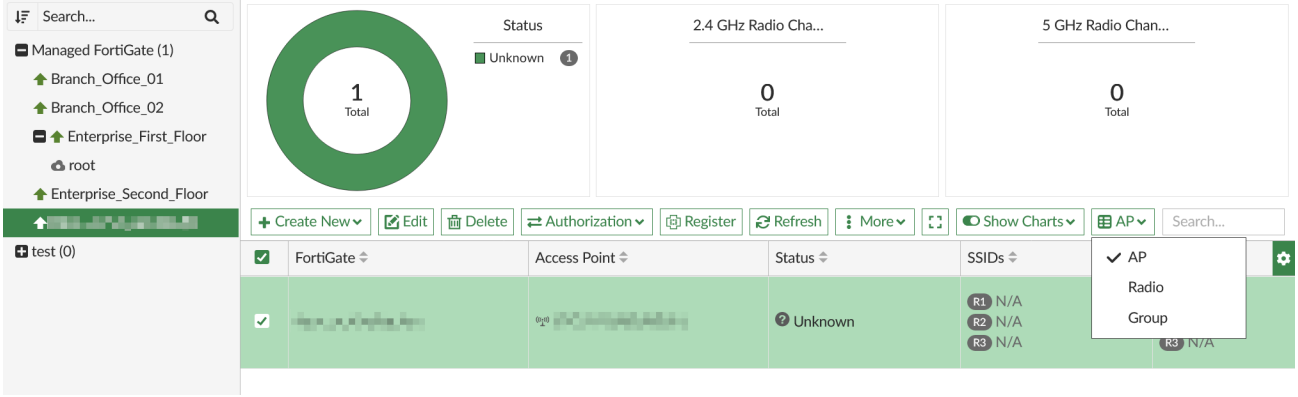
1. Ensure that you are in the correct ADOM.
2. Go to *AP Manager* > *Managed FortiAPs*.
   The quick status bar is displayed above the content pane.



3. Select a managed FortiGate.
   You can adjust the view by selecting *List*, *Radio*, or *Group* from the view dropdown. The default is *List*.
   The devices are displayed in the content pane, and the quick status bar updates the charts.
4. Mouse over the charts to see more information about the data in a tooltip.
5. Click items in the legend to filter the devices displayed on the content pane. For example, if *Offline* is available in the legend, click *Offline* to display only devices that are currently offline.
   You can click multiple items in the legend to apply multiple filters. A filter icon appears next to the chart title when it is being used to filter the devices on the *Managed FortiGate* pane.
6. To remove the filters, click the chart title with the filter icon.
7. Click *More* > *View Rogue APs* to open the rogue AP list in a pop-up window.

Managing APs

FortiAP devices can be managed from the content pane below the quick status bar. To view the managed FortiGates go to *AP Manager > Devices & Groups > Managed FortiGates (#)*.



The following options are available from the toolbar and right-click menu:

Create New		Add an AP or an AP group. The APs must be the same model to be grouped. See FortiAP groups on page 590.
Edit		Edit the selected AP.
Delete		Delete the selected AP.
Authorization		Authorize or deauthorize an AP. See Authorizing and deauthorizing FortiAP devices on page 592.
Register		Register the selected FortiAP device to your FortiCloud account.
Refresh		Refresh the AP list, or refresh the selected FortiAP devices.
More		
	Assign Profile	Assign a profile from the list to the AP. Only applicable profiles will be listed. See Assigning profiles to FortiAP devices on page 645.
	Grouping	Add the AP to a new or existing group. The APs must be the same model to be grouped. See FortiAP groups on page 590.
	Deauthorize	Deauthorize an AP. See Authorizing and deauthorizing FortiAP devices on page 592. This option is also available in the toolbar by selecting *More*.
	Upgrade	Upgrade the AP. The AP must already be authorized. You can also select two or more AP devices of the same model and upgrade the devices at the same time. Before upgrading FortiAP, go to *FortiGuard > Firmware Images > Product: FortiAP* and click the download icon to manually download the firmware images.
	Restart	Restart the AP.

	Replace	Replace a FortiAP device. Selecting this option allows you to enter a new FortiAP Serial Number for the selected device. See Replacing APs on page 599.
	Diagnostics and Tools	View the device *Summary*, *Performance*, *Clients*, *Interfering SSIDs*, and *Spectrum Analysis*. View the clients connected to the AP. See Connected clients on page 595. View the spectrum analysis for managed APs. See Spectrum analysis for managed APs on page 596.
	View Rogue APs	View the Rogue APs. See Rogue APs on page 592.
	View Health Monitor	View the AP status, clients counts, and wireless interference. See Health Monitor on page 598.
	Export to Excel/CSV	Export the selected device details to an Excel or CSV file. See Importing and exporting FortiAP devices on page 588.
	Import from CSV	Import FortiAPs from an uploaded CSV file. See Importing and exporting FortiAP devices on page 588.
LED Blink		Start LED blink on the selected FortiAP for the specified period of time. This option is only available in the right-click menu.
Show on Google Map		Show the selected AP on Google Map. See Google map on page 601. This option is only available in the right-click menu.
Show on Floor Map		Show the selected AP on the floor map. See Floor map on page 602. This option is only available in the right-click menu.
AP/Radio/Group		Change the Managed FortiAPs view. The following views are available: AP, Radio, or Group.
Search		Enter a search string into the search field to search the AP list.
Column Settings		Click to select which columns to display or select *Reset to Default* to display the default columns.

The following information is available in the content pane:

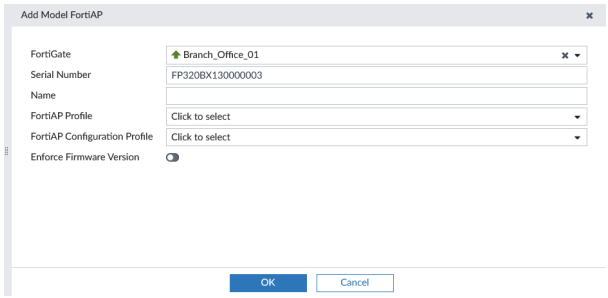
FortiGate	The FortiGate unit that is managing the AP.
Access Point	The name of the AP.
SSIDs	The SSIDs associated with the AP.
Channel	The wireless radio channels that the access point uses.
Clients	The number of clients connected to the AP. Select a value to open the View WiFi Clients window to view more details about the clients connected to that radio. See Connected clients on page 595.
Temperature	Device temperature information.

OS Version	The OS version on the FortiAP.
AP Profile	The AP Profile assigned to the device, if any.
Connected Via	The IP address of the AP.
Model	
Channel Utlization	
Comments	User entered comments.
Country/Region	The Country code that the FortiAP is using.
Join Time	The date and time that the FortiAP joined.
LLDP	The Link Layer Discovery Protocol
Operating TX Power	The transmit power of the wireless radios.
Serial #	The serial number of the device
WTP Mode	The Wireless Transaction Protocol (WTP) mode, or *0* if none.

Add a FortiAP device

To add a FortiAP device:

1. From the*Create New* dropdown, select *Managed AP*. The *Add FortiAP* dialog box opens.



2. Enter the following information, then click *OK* to add the device:

FortiGate	Select the FortiGate that the AP will be added to from the dropdown list. If you have already selected a FortiGate in the tree menu, this field will contain that FortiGate.
Serials Number	Enter the device's serial number.
Name	Enter a name for the device.
FortiAP Profile	Select an AP profile to apply to the device from the dropdown list. See FortiAP profiles on page 616.
FortiAP Configuration Profile	Select a FortiAP configuration profile to apply to the device from the dropdown list.
Enforce Firmware Version	Toggle *ON* to enforce a firmware version and select the firmware version from the drop-down menu. Toggle *OFF* to disable this feature.

Adding model devices using a wildcard SN

FortiAP model devices can be added using wildcard serial numbers. The wildcard SN format is: *PREFIX****000001*

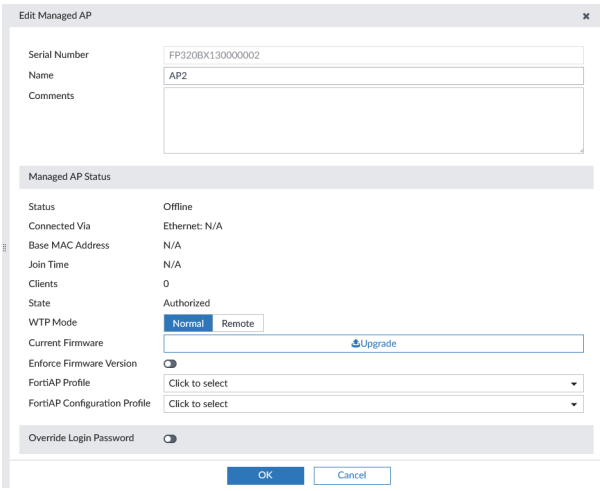
- *PREFIX*: The first 6 digits of the device's serial number. The prefix must be valid.
- ******: The wildcard characters.
- *000001*: The valid characters.

For example: `PS221E****000001`.

Editing FortiAP devices

To edit FortiAP devices:

1. In the tree menu, go to *Managed FortiAPs*, and select the FortiGate that contains the FortiAP device to be edited. Alternatively, you can select a device in a group, see FortiAP groups on page 590.
2. Locate the FortiAP device in the list in the content pane, or refine the list by selecting an option from the quick status bar.
3. Either select the FortiAP and click *Edit* from the toolbar, double-click on the FortiAP, or right-click on the FortiAP and select *Edit*. The *Edit Managed AP* window opens.



4. Edit the following options, then click *Apply* to apply your changes:

Serial Number	The device's serial number. This field cannot be edited.
Name	The name of the AP.
Comments	Comments about the AP, such as its location or function.
Managed AP Status	Various information about the AP.
Status	The status of the AP, such as *Connected*, or *Idle*. Click *Restart* to restart the AP.
Connected Via	The method by which the device is connected to the controller.

	Base MAC Address	The MAC address of the device.
	Join Time	The time that the AP joined.
	Clients	The number of clients currently connected to the AP.
	State	The state of the AP, such as *Authorized*, or *Discovered*.
	Current	The AP's current firmware version. Select *Upgrade* to upgrade the firmware to a newer version if you have one available.
	FortiAP Profile	Select a profile from the dropdown list (see FortiAP profiles on page 616)
	FortiAP Configuration Profile	Select a configuration profile from the dropdown list.
	Bonjour Profile	Select a profile from the dropdown list (see Bonjour profiles on page 626)
Override Radio		Override the selected profiles settings.
	Band	If applicable, select the wireless band, and select the wireless protocol from the dropdown list. The available options depend on the selected platform. In two radio devices, both radios cannot use the same band.
	Channels	Select the channel or channels to include, or let them be automatically assigned. The available channels depend on the selected platform and band.
	TX Power Control	Enable/disable automatic adjustment of transmit power. • *Auto*: Enter the TX power low and high values, in dBm. • *Manual*: Enter the TX power in the form of the percentage of the total available power.
	SSIDs	Manually choose the SSIDs that APs using this profile will carry, or let them be selected automatically. For more information on *Tunnel*, *Bridge*, and *Manual* settings, see FortiAP profiles on page 616.
Override AP Login Password		Enable/disable overriding the login password: • *Set*: Set the AP login password. • *Leave Unchanged*: Leave the password unchanged. • *Set Empty*: Remove the password.
Advanced Options		Configure advanced options. For information, see the *FortiOS CLI Reference*. https://help.fortinet.com/cli/fos60hlp/60/index.htm.

Deleting FortiAP devices

To delete FortiAP devices:

1. Go to *Managed FortiAPs*, and select the FortiGate that contains the FortiAP device to be deleted.
2. Locate the FortiAP device in the content pane, or refine the list by selecting an option from the quick status bar.
3. Either select the FortiAP and click *Delete* from the toolbar, or right-click the FortiAP and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the AP.
5. Perform an install to apply the changes to the managed FortiGate. See Install wizard on page 180.



A FortiAP device cannot be deleted if it is currently being used. For example, if a firewall profile has been assigned to it.

Upgrading FortiAP devices

To upgrade multiple FortiAP devices:

1. Go to *Managed FortiAPs*, and select the FortiGate that contains the FortiAP device to be upgraded. Alternatively, you can select a device in a group, see FortiAP groups on page 590.
2. Select two or more FortiAP devices of the same model in the content pane.
3. Right-click the selected FortiAP devices and select *Upgrade*.
   The Upgrade Firmware dialog box is displayed.
4. Select the firmware version for upgrade, and click *Upgrade Now*.



Before upgrading FortiAP, go to *FortiGuard > Firmware Images > Product: FortiAP* and click the download icon to manually download the firmware images.

Importing and exporting FortiAP devices

To import FortiAP devices:

1. Configure a CSV file with the following fields as column headers, and enter the corresponding information for each FortiAP to be imported in the cells below:

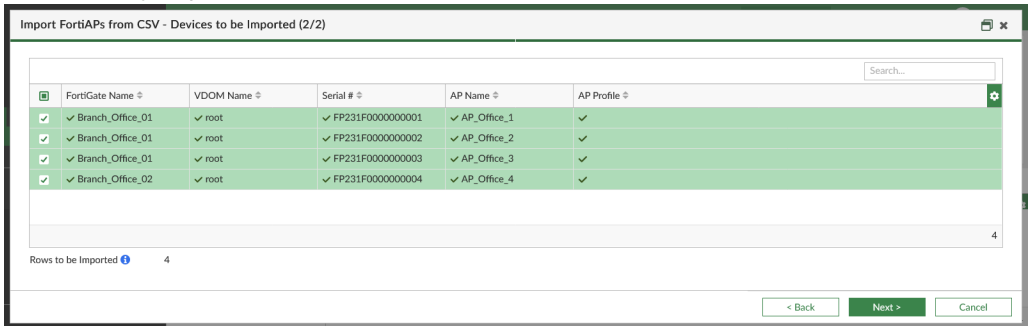
Header	Cell
FortiGate	The name of the FortiGate to which the FortiAP will be assigned.
Access Point	The access point name.
Serial #	The FortiAP serial number

Header	Cell
FAP Profile	The profile to be assigned to the FortiAP.
VDOM name	(Optional) If VDOMs are enabled on the FortiGate, specify the VDOM to which the FortiAP will be assigned. If VDOMs are disabled, leave this field blank, and the default *root* VDOM will be applied automatically.

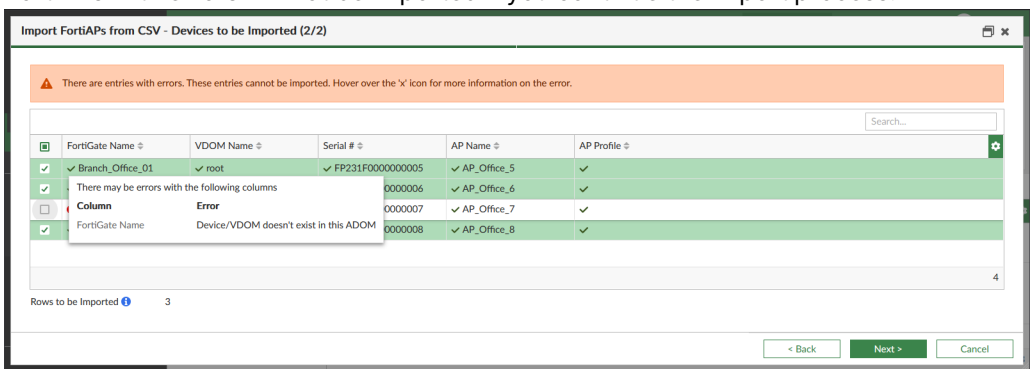
For example:

	A	B	C	D	E
1	FortiGate	Access Point	Serial #	FAP Profile	VDOM Name
2	Branch_Office_01	AP_Office_1	FP231F0000000001	FAP231F-default	
3	Branch_Office_01	AP_Office_2	FP231F0000000002	FAP231F-default	
4	Branch_Office_01	AP_Office_3	FP231F0000000003	FAP231F-default	
5	Branch_Office_02	AP_Office_4	FP231F0000000004	FAP231F-default	
6					
7					

2. Go to *AP Manager* > *Managed FortiAPs*, and select *More* > *Import from CSV* from the toolbar.
3. Browse to the CSV file location, or drag and drop the file into the *Upload* field. The results are displayed in the import results window.
   - Successfully imported fields are indicated with a checkmark icon.



   - Fields with errors are indicated with an error icon. Hover your mouse over the error icon or the FortiAP's check box to view details about the error. Fields can be directly edited from the import results window. FortiAPs with errors will not be imported if you continue the import process.



4. Click *Next* to complete the import.

To export FortiAP devices:

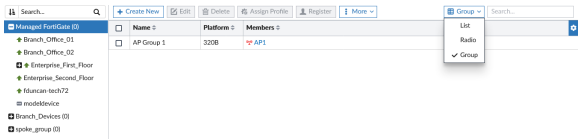
1. Go to *AP Manager > Managed FortiAPs* .
2. Select a FortiGate in the table to view its FortiAPs or select *Managed FortiGate (#)* to view all FortiAP devices.
3. Open the *More* menu in the toolbar, and select one of the following options:
   - *Export to Excel*: The FortiAP information for the selected FortiGate(s) is exported to an Excel file
   - *Export to CSV*: Configure the following information and click *OK*:
     - *File Name*: Enter the name of the CSV file.
     - *Options*: Select *Export all columns* or *Export customized columns* only.
     - *Export All Devices*: In per-device mode only, enable this toggle to include all managed FortiGate's FortiAPs in the CSV file.

FortiAP groups

FortiAP devices can be organized into groups. A FortiAP can only belong to one group.

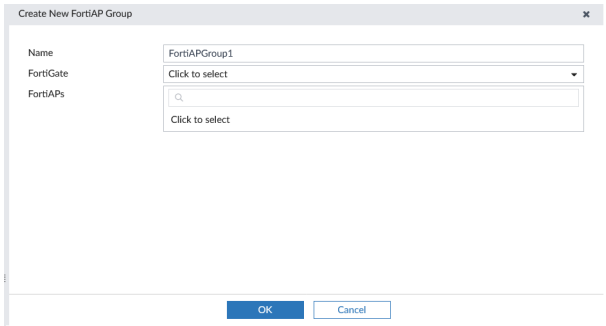
To view a FortiAP group:

1. Go to *AP Manager > Managed FortiAPs*.
2. Select a managed device.
3. In the toolbar, click *List > Group*.



To create a FortiAP group:

1. Go to *AP Manager > Managed FortiAPs*.
2. Select a managed device.
3. From the *Create New* dropdown, select *Managed AP Group*.
   Alternatively, you can click *Create New* in the *Group* view.
4. In the toolbar, click *Create New*. The *Create New FortiAP Group* dialog box opens.



5. Configure the following:

Name	Enter a name for the group.
FortiGate	Select the FortiGate under which the group will be created.
FortiAPs	Select FortiAPs to add to the group. Only FortiAPs in the selected FortiGate of the selected platform will be available for selection.

6. Click *OK* to create the group.

To edit a group:

1. Go to *AP Manager* > *Managed FortiAPs*.
2. Select a managed device.
3. Ensure *Group* view is enabled.
4. In the device pane, right-click the group and select *Edit*.
5. Edit the group name and devices in the group as needed.
6. Select *OK* to apply your changes.

To delete a group:

1. Go to *AP Manager* > *Managed FortiAPs*.
2. Select a managed device.
3. Ensure *Group* view is enabled.
4. In the device pane, right-click the group and select *Delete*.
5. Select *OK* in the confirmation dialog box to delete the group.

Device summary

The *Device Summary* tab in *Diagnostics and Tools* displays the FortiAP serial number, status, version as well other information about the device. The *General Health* view in the summary tab displays key health statisics for the device, such as *CPU Usage*, *Memory Usage*, *Connection Uptime*, and *Temprature*.

To view the FortiAP device summary:

1. Go to *AP Manager* > *Managed FortiAPs*.
2. Select a managed device. Alternatively, you can select a device in a group, see FortiAP groups on page 590.
3. Right-click a managed device and click *Diagnostics and Tools*. The *Summary* tab opens.

Authorizing and deauthorizing FortiAP devices

To authorize FortiAP devices:

1. Go to *AP Manager* > *Managed FortiAPs*.
2. Select the FortiGate that contains the unauthorized FortiAP devices. Alternatively, you can select a device in a group, see FortiAP groups on page 590.
3. In the *Status* chart legend, click *Unauthorized*. The unauthorized FortiAP devices are displayed in the content pane.
4. Select the FortiAP devices and click *More* > *Authorize* from the toolbar, or right-click and select *Authorize*. The *Authorize AP* dialog opens.
5. Click *OK* to authorize the selected devices.

To deauthorize FortiAP devices:

1. Select the FortiGate that contains the FortiAP devices to be deauthorized.
2. Select the FortiAP devices and either click *More* > *Deauthorize* from the toolbar, or right-click and select *Deauthorize*. The *Deauthorize AP* dialog opens.
3. Select *OK* to deauthorize the selected devices.

Installing changes to FortiAP devices

To install changes to FortiAP devices:

1. Go to *Device Manager*.
2. Select the FortiGate device that controls the FortiAP device
3. Right click and select *Install Wizard*, or select *Install* > *Install Wizard* from the toolbar.
4. Click *OK* in the confirmation dialog box to install the configuration to the device.

Rogue APs

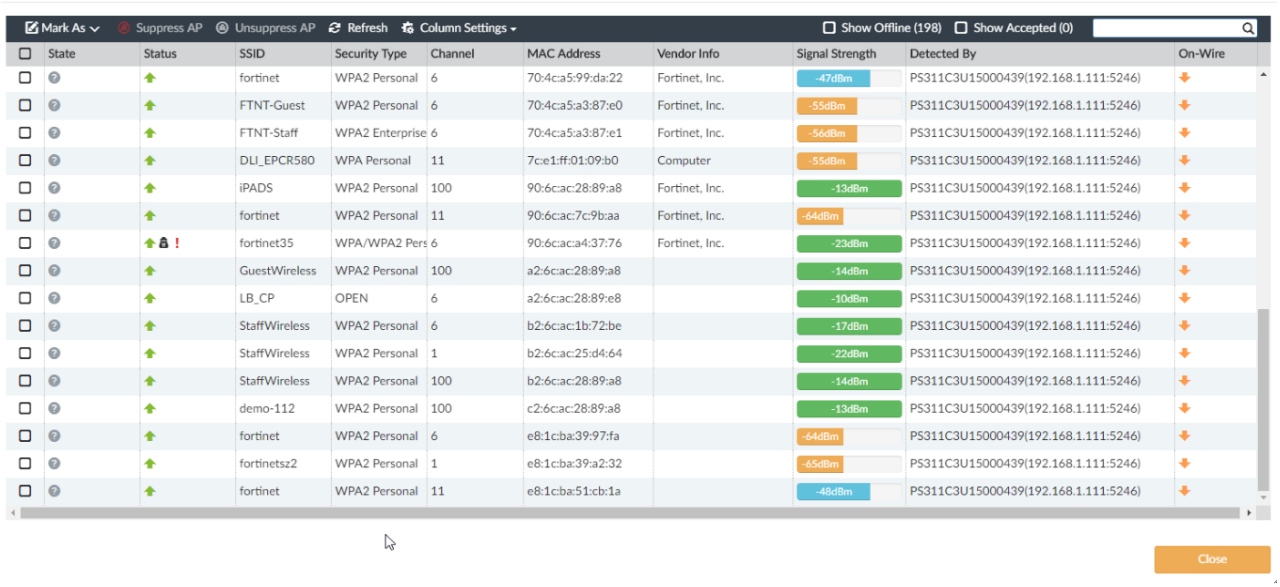
You can use Rogue AP detection to scan for and identify unauthorized wireless access points in the area. Detected APs are displayed in the *View Rogue APs* table where you can view details about the AP, including the SSID and network status. Rogue APs connected to your wired network can be identified using the *On-Wire* column in the table.

For more information about Rogue AP detection, see the FortiAP/FortiWiFi Configuration Guide.

To view Rogue APs:

1. Go to *AP Manager > Managed FortiAPs*..
2. In the toolbar, click *More > View Rogue APs*. The rogue AP list is displayed.

View Rogue APs



The following options are available:

Mark As	Mark a rogue AP as: • *Accepted*: for APs that are an authorized part of your network or are neighboring APs that are not a security threat. • *Rogue*: for unauthorized APs that On-wire status indicates are attached to your wired networks. • *Unclassified*: the initial status of a discovered AP. You can change an AP back to unclassified if you have mistakenly marked it as *Rogue* or *Accepted*.
Suppress AP	Suppress the selected APs. This will prevent users from connecting to the AP. When suppression is activated against an AP, the controller sends deauthentication messages to the rogue AP's clients posing as the rogue AP, and also sends deauthentication messages to the rogue AP posing as its clients. Before enabling this feature, verify that operation of Rogue Suppression is compliant with the applicable laws and regulations of your region.
Unsuppress AP	Turn of suppression for the selected rogue APs.
Refresh	Refresh the rogue AP list.
Column Settings	Click to select which columns to display or select *Reset to Default* to display the default columns.

The following columns are available:

State	The state of the AP: • Suppressed: red suppressed icon • Rogue: orange rogue icon • Accepted: green wireless signal mark • Unclassified: gray question mark
Status	Whether the AP is active (green) or inactive (orange).
SSID	The wireless service set identifier (SSID) or network name for the wireless interface.
Security Type	The type of security currently being used.
Channel	The wireless radio channel that the access point uses.
MAC Address	The MAC address of the wireless interface.
Vendor Info	The name of the vendor.
Signal Strength	The relative signal strength of the AP.
Detected By	The name or serial number of the AP unit that detected the signal.
On-Wire	A green up-arrow indicates a suspected rogue, based on the on-wire detection technique. An orange down-arrow indicates AP is not a suspected rogue.
First Seen	How long ago this AP was first detected. This column is not visible by default.
Last Seen	How long ago this AP was last detected. This column is not visible by default.
Rate	The data rate in, bps. This column is not visible by default.

Authorizing unknown APs

FortiManager can authorize unknown APs that are connected to a managed FortiGate.

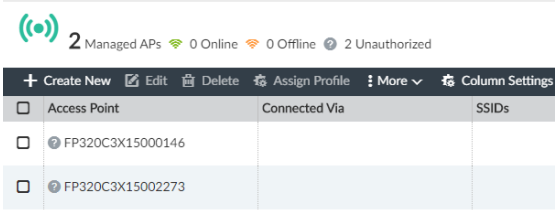
To authorize unknown APs:

1. Enable *JSON API access* to *Read-Write*. See To enable read-write JSON API access.

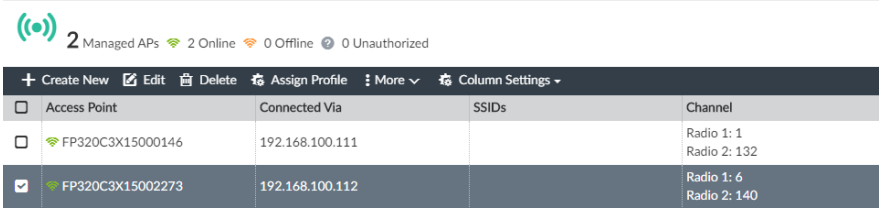


You must enable *JSON API access* to *Read-Write* to authorize unknown FortiAP devices.

2. Go to *AP Manager* > *Managed FortiAPs*.
3. Select the FortiGate that contains the unknown FortiAP devices to be authorized. Alternatively, you can select a device in a group, see FortiAP groups on page 590.



4. Select the unknown FortiAP devices and either click *More* > *Authorize* from the toolbar, or right-click and select *Authorize*. Allow a few moments for the APs to authorize.
5. Select the APs and click *More* > *Refresh*.
   The APs are now online and displayed.



Connected clients

In the *Diagnostics and Tools* pane, the *Clients* tab displays detailed information about the health of individual WiFi connections.

To view WiFi clients:

1. Go to *AP Manager* > *Managed FortiAPs*.
2. Select a managed device. Alternatively, you can select a device in a group, see FortiAP groups on page 590.
3. Select a FortiAP from the table.
4. In the toolbar, click *More* > *Diagnostics and Tools*.
5. In the *Diagnostics and Tools* pane, click the *Clients* tab. The *Clients* table displays a list of clients in the selected FortiGate.
   The following columns are available:

IP	The IP address assigned to the wireless client.
SSID	The SSID that the client connected to.
FortiAP	The name of the FortiAP unit that the client connected to.
Device	The type of device that the client is using.
Channel	The wireless radio channel that is used.
Bandwidth Tx/Rx	Client received and transmitted bandwidth, in Kbps.
Signal Strength/Noise	The signal-to-noise ratio in dBs calculated from signal strength and noise level.
Signal Strength	The relative signal strength of the AP.

Association Time	How long the client has been connected to this access point.
Authentication	The type of authentication used.
Bandwidth RX	Client received bandwidth, in Kbps.
Bandwidth TX	Client transmitted bandwidth, in Kbps.
Device OS	The connected client's OS name.
Host Information	The host name of the WiFi client, if available.
Idle Time	The amount of time that the client has been idle.
Manufacturer	The manufacturer of the client device.
Rate	The connection rate between the WiFi client and the AP.
Name	The name of the FortiGate device that the FortiAP is attached to.

Spectrum analysis for managed APs

Spectrum analysis scans managed APs for channel conditions and sources of interference which can potentially impact efficiency.



AP capabilities will be limited during spectrum analysis.

To assign an AP profile to a managed AP:

1. Enable *JSON API access* to *Read-Write*. See To enable read-write JSON API access.
2. Create a new WiFi profile or modify an existing WiFi profile, by setting the *Radio* mode to *Dedicated Monitor*. See FortiAP profiles on page 616.
3. Assign the profile to the managed AP. See Assigning profiles to FortiAP devices on page 645.
4. Use the *Install Wizard* to install the changes to FortiGate. See Install device settings only on page 183.

To view the spectrum analysis for a managed AP:

1. Go to *AP Manager > Managed FortiAPs*.
2. Select a managed device. Alternatively, you can select a device in a group, see FortiAP groups on page 590.
3. Right-click a managed AP and select *Diagnostics and Tools*, or click *More > Diagnostics and Tools* in the toolbar.
4. In the *Diagnostics and Tools* pane, click the *Spectrum Analysis* tab.
   The following information is displayed:

Chart	Description
Signal Interference	The noise levels for each channel

Chart	Description
Signal Interference Spectrogram	A spectrogram of 60 samples of noise levels for different channels at specific time intervals.
Duty Cycle	The extent of a non-WiFi device/neighbouring AP is interfering with the signal.
Duty Cycle Spectrogram	A spectrogram of 60 duty samples for each channel over a period of time
Detected Interference	The detected interference *Type*, *Frequency*, and *Last Detected* date.

Clients Monitor

The *Clients Monitor* displays detailed information about connected clients and the health of individual WiFi connections .

To view the Clients Monitor:

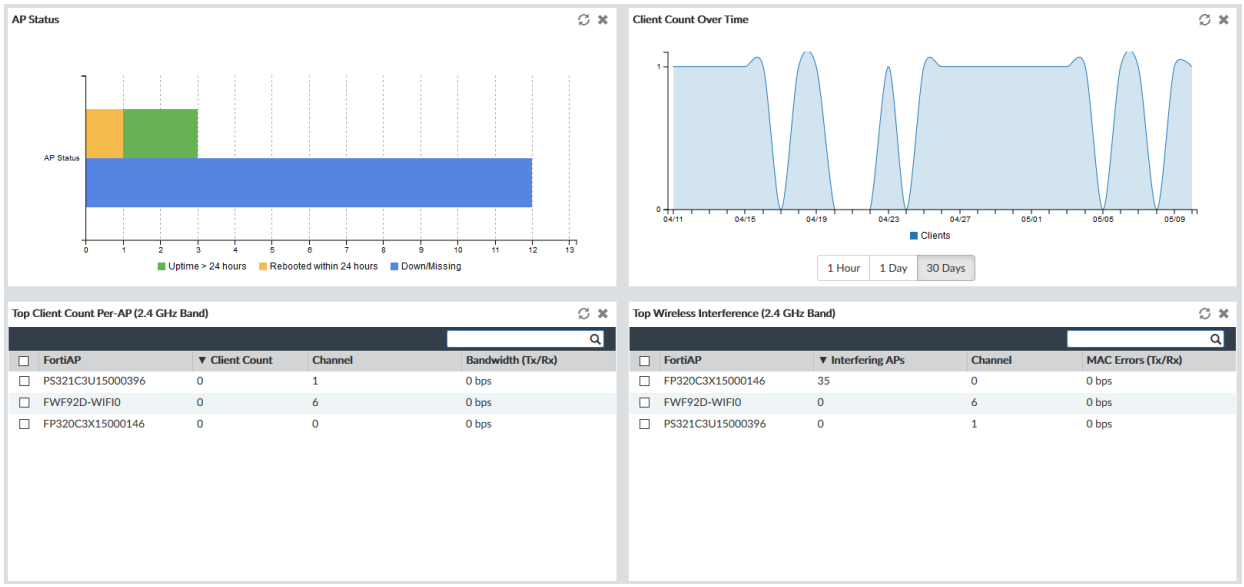
1. Go to *AP Manager > Managed FortiAPs*.
2. Select a managed device. Alternatively, you can select a device in a group, see FortiAP groups on page 590.
3. In the toolbar, click *More > Diagnostics and Tools*, or right-click and select *Diagnostics and Tools*.
4. In The *Diagnostics and Tools* pane, click the *Clients* tab.
5. (Optional) In the toolbar, enter a search term in the *Search* field to locate a specific device.
6. (Optional) In the toolbar, click *Column Settings* to add and remove columns, or reset to default.
   The following columns are available:

IP	The IP address assigned to the wireless client.
SSID	The SSID that the client connected to.
FortiAP	The serial number of the FortiAP unit that the client connected to.
Device	The type of device that the client is using.
Channel	The wireless radio channel that is used.
Bandwidth TX/RX	Client received and transmitted bandwidth, in Kbps.
Signal Strength/Noise	The signal-to-noise ratio in dBs calculated from signal strength and noise level.
Signal Strength	The relative signal strength of the AP.
Association Time	How long the client has been connected to this access point.
Authentication	The type of authentication used.
Bandwidth RX	Client received bandwidth, in Kbps.
Bandwidth TX	Client transmitted bandwidth, in Kbps.
Device OS	The OS version on the FortiAP.

Host Information	The host name of the WiFi client, if available.
Idle Time	The amount of time that the client has been idle.
Manufacturer	The manufacturer of the client device.
Rate	The connection rate between the WiFi client and the AP.

Health Monitor

The *Health Monitor* is a collection of widgets that provide an overview of the AP status, clients counts, and wireless interference.



To view the Health Monitor:

1. Go to *AP Manager > Managed FortiAPs*.
2. Select a managed device. Alternatively, you can select a device in a group, see FortiAP groups on page 590.
3. In the toolbar, click *More > View Health Monitor*.
4. (Optional) Click and drag a widget title to reposition the widget in the monitor.
5. (Optional) Click the *Refresh* button to refresh the widget data.

6. (Optional) Click the column heading in a table to sort the data in ascending or descending order.
The following widgets are displayed:

Widget	Description
AP Status	Displays a bar graph of: • *Uptime > 24 hours*: The number of APs that have been up for over 24 hours. • *Rebooted within 24 hours*: the number of APs that have been rebooted within the past 24 hours. • *Down/Missing*: Down or missing APs. Select a specific column to view a table of the APs represented in that column, along with other relevant information, such as the APs' IP address, and the time of its last reboot. Select the name of a column in the legend to add or remove it from the graph. This widget is only available when the *All FortiAPs* group is selected in the tree menu.
Client Count Over Time	A graph of the number of connected clients over the specified time period: 1 hour, 1 day, or 30 days. This widget is only available when the *All FortiAPs* group is selected in the tree menu.
Top Client Count Per-AP (2.4 GHz or 5 GHz Band)	Lists the number of clients in the 2.4GHz and 5GHz band for each FortiAP. Also includes columns for the channel and bandwidth of the AP.
Top Wireless Interference (2.4 GHz or 5 GHz Band)	Lists the number of interfering APs in the 2.4GHz and 5GHz band for each FortiAP. Also includes columns for the channel and the number of MAC Errors for each AP.
Login Failures Information	Lists the time of a log in failure, the SSID involved, the Host Name/MAC, and the User Name.

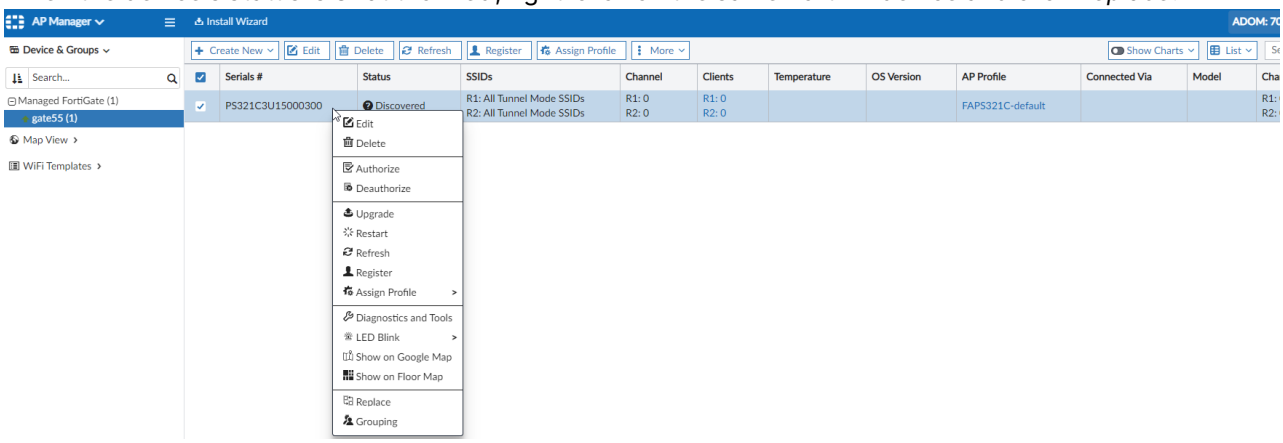
Replacing APs

FortiAP devices can be replaced from the *AP Manager > Device & Groups* pane.

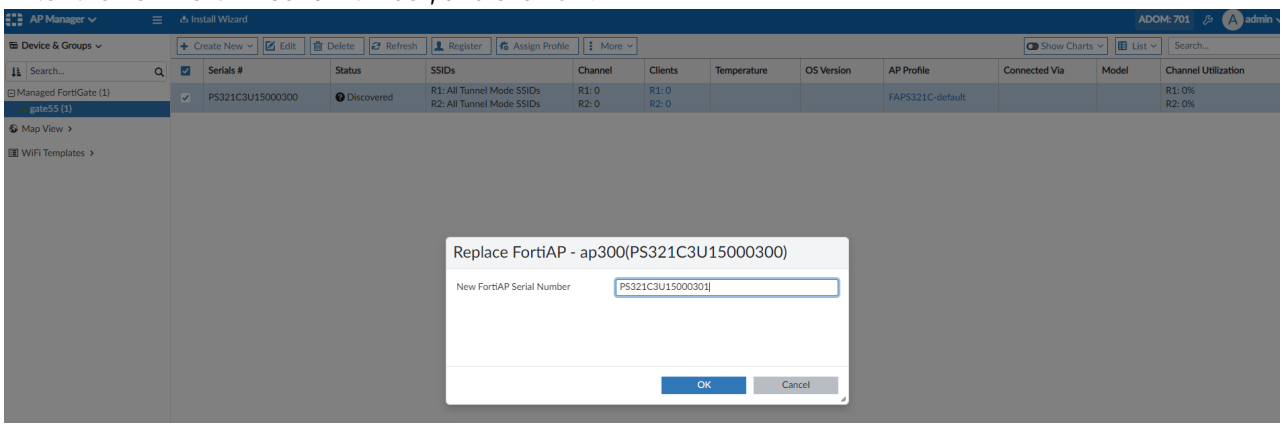
To replace a FortiAP device:

1. Go to *AP Manager > Managed FortiAPs*.
2. Select a managed FortiGate.
3. Right-click on a FortiAP device in the table and click *Deauthorize*.

4. When the device's status is *Unauthorized*, right-click on the same FortiAP device and click *Replace*.

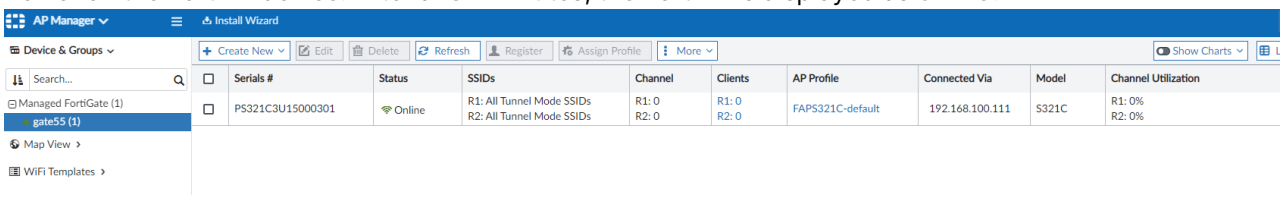


5. Enter the new FortiAP serial number, and click *OK*.



After the FortiAP has been replaced successfully, refresh the page and the new FortiAP is displayed.

6. Authorize the FortiAP device, then connect the FortiAP to the FortiGate.
7. Power on the FortiAP device. After a few minutes, the FortiAP is displayed as *Online*.



You can view the replacement serial number in the *Replacement Serial Number* column in the Managed FortiSwitches table.

WiFi Maps

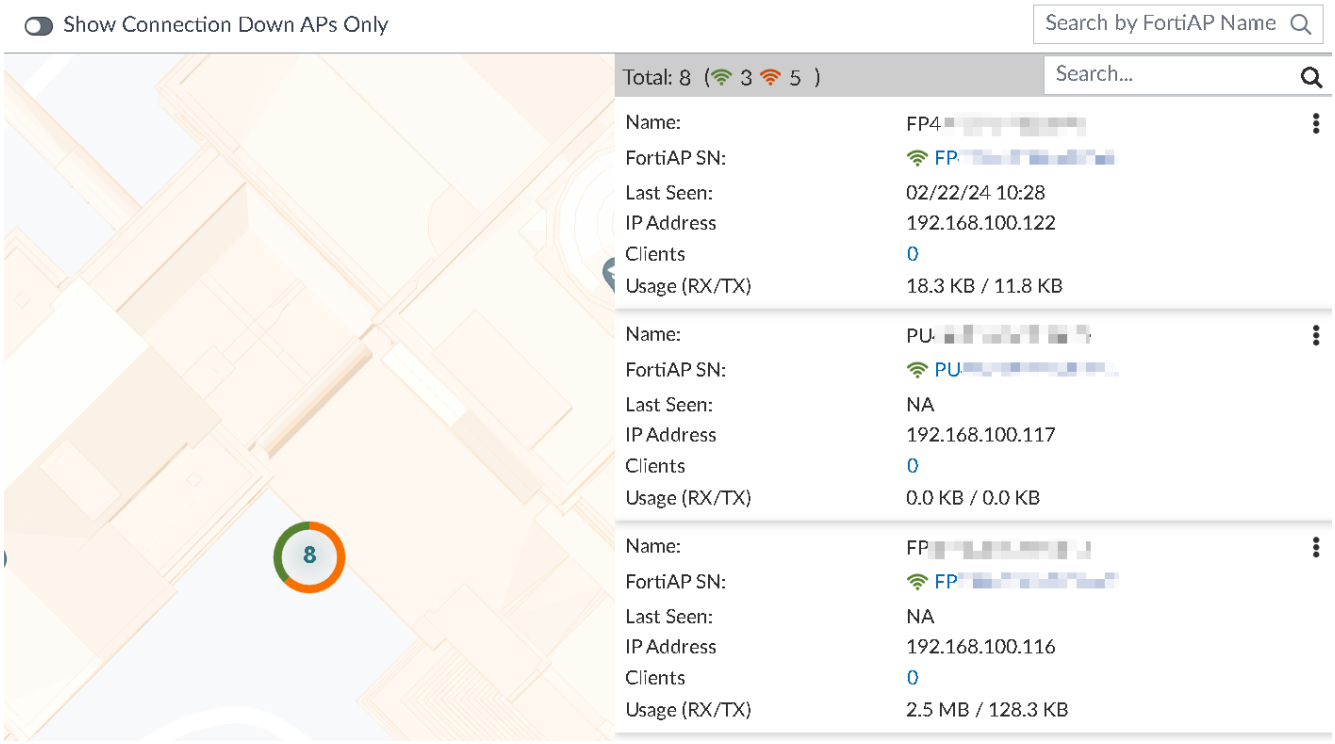
The *WiFi Map* pane in AP Manager displays the global and local locations of your FortiAP devices.

There are two types of maps in *WiFi Maps*:

- **Google Map**: Shows all of the FortiGate devices on an interactive world map. See Google map on page 601.
- **Floor Map**: Allows you to create a customized map of your building, add an image of the floor layout, and place FortiAP devices on the map. See Floor map on page 602

Google map

Google Map shows all of the FortiGate devices on an interactive world map. Each FortiGate is designated by a map pin in its geographic location on the map. The number of APs connected to the FortiGate is listed in the pin.



To view the Google Map:

1. Go to *AP Manager > WiFi Maps > Google Maps*.
2. Click a pin on the map to view a list of the APs connected to that FortiGate. The AP information pane is displayed at the right side of the map.
3. (Optional) In the toolbar, click *Connection Down APs Only*.
4. View the AP on a Google Map.

Google Map	After selecting a FortiGate in the map, the following information is displayed for its FortiAPs. AP status information is obtained from JSON response and from AP monitoring data obtained from FortiGate.

Name	The name of the FortiAP.
FortiAP SN	The serial number of the FortiAP.

	Click the serial number to open the *Edit Managed AP* pane. See Editing FortiAP devices on page 586.
Last Seen	The last time the FortiAP reported online. Last Seen reporting is based on the WTP management status received from FortiGate. If FortiGate has a *N/A* status for this AP, FortiManager also displays *N/A*. Clicking *Refresh* on the *AP Manager > Managed FortiAPs* page will update the information instantly.
IP Address	The IP address of the FortiAP.
Clients	Displays the number of connected clients. Click on the number of clients to open the *View WiFi Clients* pane. See Connected clients on page 595.
Usage (RX/TX)	The bytes received (bytes_rx) and transmitted (bytes_tx) by the FortiAP, displayed in KB/MB. Usage information is obtained through the FortiGate.



Reporting is updated on a default time interval of 600 seconds for fields excluding *IP Address*. This interval can be changed using the following command in the FortiManager CLI: `diagnose rtm profile update check-interval fap`.

Show on Floor Map — Click the menu icon next to the AP *Name*, and click *Show on Floor Map*, to view AP's physical location. See Floor map on page 602.

Floor map

Floor Map allows you to create a customized map of your building, add an image of the floor layout, and place FortiAP devices on the map.



To create a Floor Map:

1. Go to *AP Manager > WiFi Maps > Floor Map*
2. In the banner, click *Create New*. The *Add Floor Map* dialog is displayed.
3. From the *Location* dropdown, select a location or specify a new one, and click *Next*.
4. Specify the *Building Name* and *Address*, and then click *Next*.
5. Specify the floor details:
   - **Floor Description**: Enter a description of the floor. This is displayed as the name of the floor map.
   - **Floor Index**: Enter a numeric value. Floors are sorted from highest to lowest based on the Floor Index.
   - **Contact**: Enter a contact name for the floor.
   - **Phone Number**: Enter a phone number for this location.
   - **Floor Map** - Upload a file by dragging and dropping onto the field, or click *Browse* to select an image of your floor map.

     Floor map images can be uploaded in the following file types: PNG, JPG, GIF and BMP.
6. Click *Finish*. The map is added to *AP Manager > Map View > Floor Map*.

To position FortiAP devices on the floor map:

1. Click *Floor Map > [Map Name] > [Floor Map name]*.
2. In the toolbar, click *Edit Mode* to list the FortiAP devices in the *Positioning APs* pane.
3. Drag and drop the FortiAP devices from the *Positioning APs* pane to the image of the floor map.
4. In the toolbar click, *Save*.
5. Click *Save and Return*.
   The FortiAP devices are added to the floor map.

To view the properties of a FortiAP device:

1. Click *Floor Map* > *[Floor Map name]*.
2. Click the image of the floor map.
3. Hover over the FortiAP device to view the following details:
   - FortiAP Serial Number
   - IP Address
   - Number of Clients connected
   - Usage
   - Base MAC Address
   - State
   - Rogue APs

To remove FortiAP devices from the floor map:

1. Click *Floor Map* > *[Floor Map name]*.
2. Click the image of the floor map.
3. Click *Edit Mode* .
4. Right-click the FortiAP device and select *Remove from Floor Map*.
5. Click *Save and Return*.
   The FortiAP device is now removed from the Floor Map and added to the *Positioning APs* pane.

WiFi profiles and settings for central management

When using AP Manager with central management enabled, you can configure the following profiles and settings:

- SSIDs
- Operation Profiles
  - FortiAP Profiles
  - QoS Profiles
  - FortiAP Configuration Profiles
- Connectivity Profiles
  - MPSK Profiles
  - Bonjour Profiles
  - Bluetooth Profiles
- Protection Profiles
  - WIDS Profiles
  - L3 Firewall Profiles
  - ARRP Profiles
- WiFi Settings



Settings may vary for different ADOM versions.

The following steps provide an overview of using central management for access management:

1. Enable central management of access points.
   See Enabling FortiAP central management on page 605.
2. Create WiFi profiles.
3. Assign profiles to FortiAP devices.
   See Assigning profiles to FortiAP devices on page 645.
4. Install FortiAP profiles to devices.
   On the *Device Manager* pane, select the FortiGate device that controls the FortiAP device, then select *Install > Install Config* from the toolbar, and follow the prompts in the wizard. See Installing changes to FortiAP devices on page 592.

Enabling FortiAP central management

When central management is enabled, you can create templates for a variety of FortiAP configurations, and assign templates to multiple managed access points.

To enable central management:

1. Go to *System Settings > ADOMs*.
2. Double-click the ADOM to open it for editing.
3. Beside *Central Management*, select the *FortiAP* checkbox, and click *OK*.
   Central management is enabled for FortiAP.

SSIDs

You can use the AP Manager to create and manage SSID groups.

This topic includes the following:

- Creating SSIDs on page 607
- Adding SSID per-device mapping on page 612
- Adding additional DHCP options on page 614
- Adding a MAC address reservation on page 614

To view SSIDs and SSID groups:

1. Go to *AP Manager > SSIDs*.

   The following options are available in the toolbar and right-click menu:

Create New	Create a new SSID (see Creating SSIDs on page 607) or SSID group.
Edit	Edit the selected SSID or group.
Clone	Clone the selected SSID or group.
Delete	Delete the selected SSID or group.
Import	Import SSIDs from a connected FortiGate (toolbar only).
Where Used	View where the SSID is used.
Column Settings	Adjust the visible columns.

To create a new SSID group:

1. In the toolbar, click *Create New > SSID Group*. The *Create New SSID Group* windows opens.
2. In the *Name* field, enter a name for the group.
3. (Optional) In the *Comment* field, enter a brief description of the group
4. (Optional) In the *Members* field, add SSIDs to the group .
5. Click *OK* to create the SSID group.

To edit an SSID or groups:

1. Select and SSID or group to edit.
2. Open the SSID or Group.
   - Double-click the SSID or group.
   - In the toolbar, click *Edit*.
   - Right-click then select *Edit*.

   The *Edit SSID*or *Edit SSID Group* window opens.
3. Edit the settings as required. The SSID name and traffic mode cannot be edited.
4. Click *OK* to apply your changes.

To delete SSIDs or groups:

1. Select the SSIDs and groups to delete.
2. In the toolbar click *Delete*, or right-click and select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the selected SSIDs and groups.
   Deleting a group does not delete the SSIDs that are in the group.

To clone an SSID or group:

1. Select an SSID or group.
2. In the toolbar click *Clone*, or right-click the SSID or group name, and select *Clone*. The *Clone SSID* or *Clone SSID Group* dialog box opens.
3. Edit the settings as required. An SSID's traffic mode cannot be edited.
4. Click *OK* to clone the SSID.

To import an SSID:

1. in the toolbar click *Import*. The *Import* dialog box opens.
2. From the *FortiGate* dropdown, select a device from the list. The list will include all of the devices in the current ADOM.
3. From the *Profile* dropdown, select the SSID or SSIDs to be imported from the list.
4. Click *OK* to import the SSID or SSIDs.

Creating SSIDs

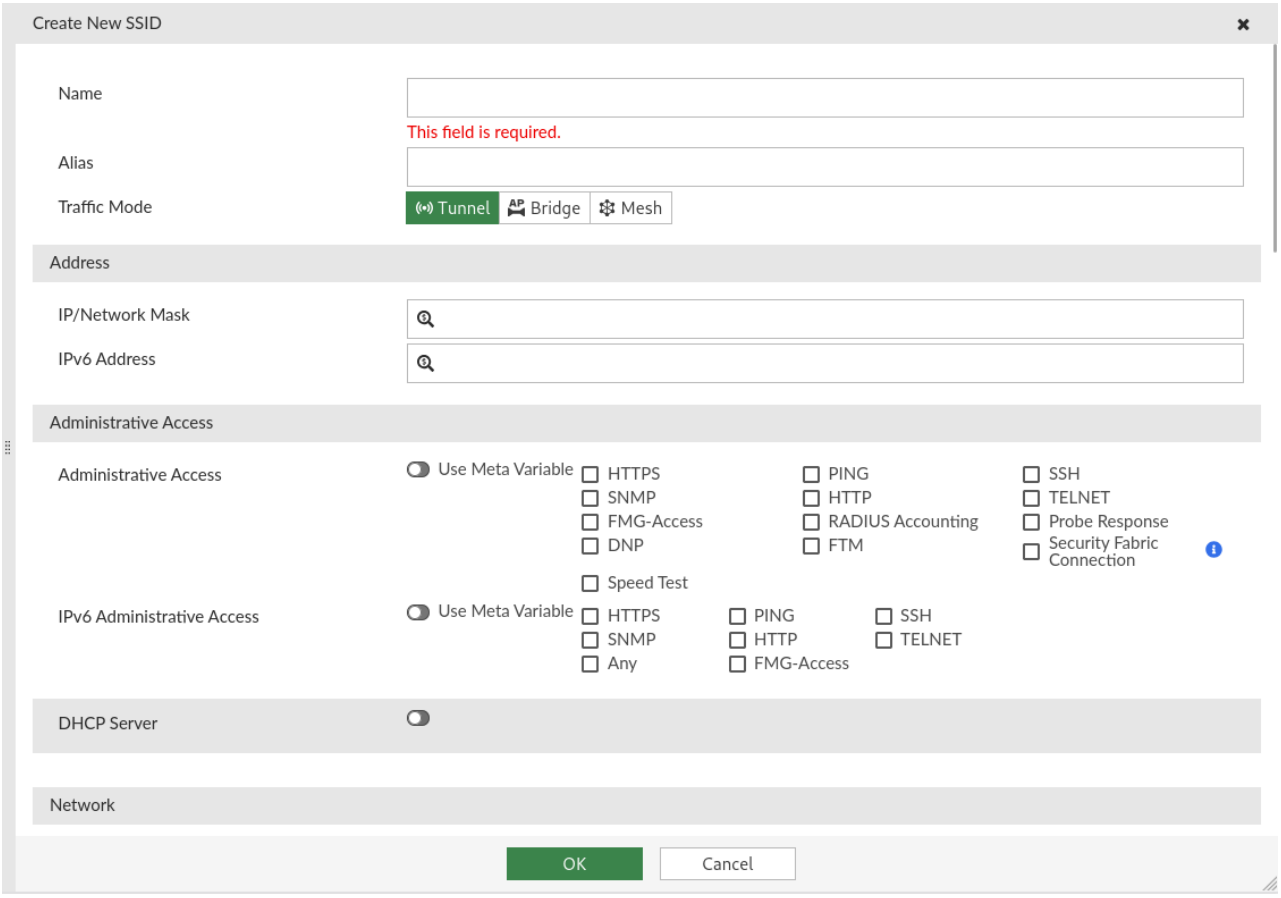
When creating a new SSID, the available options will change depending on the selected traffic mode: *Tunnel* , *Bridge*, or *Mesh*. When you create SSID profiles, you can select a QoS profile and/or an Access Control List profile.



FortiManager includes Fortinet recommended factory default SSID profiles that you can activate and use in your environment. See Using Fortinet recommended profiles on page 646.

To create a new SSID:

1. Go to *AP Manager* > *SSIDs*.
2. In the toolbar, click *Create New* > *SSID*. The *Create New SSID Profile* windows opens.



3. Enter the following information, then click *OK* to create the new tunnel to wireless controller SSID:

Name		Type a name for the SSID.
Alias		Set the alias for SSID.
Traffic Mode		Select the traffic mode: *Tunnel*, *Bridge*, or *Mesh*.
Address		These options are only available when *Traffic Mode* is *Tunnel*.
	IP/Network Mask	Enter the IP address and netmask.
	IPv6 Address	Enter the IPv6 address.
Administrative Access		
	Administrative Access	Select the allowed administrative service protocols.

IPv6 Administrative Access	Select the allowed administrative service protocols.
DHCP Server	Turn the DHCP server on or off.
Network	
Device Detection	Enable or disable device detection.

4. Configure WiFi Settings.

SSID	Type the wireless service set identifier (SSID), or network name, for this wireless interface. Users who want to use the wireless network must configure their computers with this network name.
Client Limit	The maximum number of clients that can simultaneously connect to the AP (0 - 4294967295, default = 0, meaning no limitation).
Broadcast SSID	Enable/disable broadcasting the SSID (default = enable). Broadcasting enables clients to connect to the wireless network without first knowing the SSID. For better security, do not broadcast the SSID.
Beacon Advertising	Enable/disable beacon advertising. When beacon advertising is enabled, you can select which element(s) you want to advertise from the following: • **Name**: The FortiAP name • **Model**: The FortiAP model • **Serial Number**: The FortiAP serial number.
Encrypt	Select the data encryption protocol: • *TKIP*: Temporal Key Integrity Protocol, used by the older WPA standard. • *AES*: Advanced Encryption Standard, commonly used with the newer WPA2 standard (default). • *TKIP-AES*: Use both protocols to provide backward compatibility for legacy devices. This option is not recommended, as attackers will only need to breach the weaker encryption of the two (TKIP). This option is only available when the security mode includes WPA or WPA2.
Security Mode	Select a security mode: *OSEN* — *WPA3 Enterprise* *Open* — *WPA 3 Enterprise (PMF Protection)* *Opportunistic Wireless Encryption (OWE)* — *WPA3 Enterprise Transition*

		WPA2 Enterprise / *WPA3 SAE* *WPA Personal* / *WPA3 SAE Transition* Only Open, WPA2 Personal, and WPA3 SAE modes are available when the traffic mode is *Mesh*.
	Authentication	Select the authentication method for the SSID, either *Local* or *RADIUS Server*, then select the requisite server or group from the dropdown list. This option is only available when the security mode is includes OSEN, WPA2 Enterprise, WPA3 Enterprise, WPA3 Enterprise (PMF Protection) or WPA3 Enterprise Transition.
	PMF	Set PMF settings as Disabled, Enabled, or Optional. This option is only available when the security mode is includes WPA2 Enterprise or WPA2 Personal.
	SAE-PK Authentication	Enable/disable SAE PK Authentication. When enabled, enter a *SAE-PK Private Key*.
	Hash-to-Element (H2E) only	When enabled, use hash-to-element-only mechanism for PWE derivation. This option is only available when the security mode includes WPA3 SAE or WPA3 SAE Transition.
Captive Portal		Select if you want to configure a Captive Portal to authenticate users through a customizable web page.
	Portal Type	Select the portal type: *Authentication* (default), *Authentication and MAC Authentication*, *Disclaimer Only*, *Disclaimer and Authentication*, *Email Collection*, and *External MAC Authentication*.
	Authentication Portal	Select *Local* or *External*. If *External* is selected, enter the URL of the portal.
	User Groups	Select the user group to add from the dropdown list. Select the plus symbol to add multiple groups.
	Customize Portal Messages	Select to allow for customized portal messages. Portal messages cannot be customized until after the interface has been created.
	Exempt Sources	Select exempt sources to add from the dropdown list.
	Exempt Destinations	Select exempt destinations to add from the dropdown list.
	Exempt Services	Select exempt services to add from the dropdown list.
	Redirect after Captive Portal	Select *Original Request* or *Specific URL*. If *Specific URL* is selected, enter the redirect URL.
Pre-shared Key		Select *Single* to specify a single passphrase. Select *Multiple* to specify a multiple pre-shared key group.

Client MAC Address Filtering		Enable/disable client MAC address filtering. For more information, see the FortiWiFi and FortiAP Configuration Guide.
Additional Settings		
	Dynamic VLAN Assignment	Enable/disable dynamic VLAN assignment. Dynamic VLAN assignment not available when VLAN Pooling is enabled.
	Schedule	Select a schedule to control the availability of the SSID.
	Block Intra-SSID Traffic	Enable/disable blocking communication between clients of the same AP (default = disable).
	Split Tunneling	Select to enable some subnets to remain local to the remote FortiAP. Traffic for these networks is not routed through the WiFi Controller. Specify split-tunnel networks in the FortiAP Profile.
	Optional VLAN ID	Select to enable the unit to block intra-SSID traffic.
	Broadcast Suppression	Optional suppression of broadcast message types: • *All other broadcast*: All other broadcast messages • *All other multicast*: All other multicast messages • *ARPs for known clients*: ARP for known messages • *ARP poison*: ARP poison messages from wireless clients • *ARP proxy*: ARP requests for wireless clients as a proxy • *ARP replies*: ARP replies from wireless clients • *ARPs for unknown clients*: ARP for unknown messages • *DHCP downlink*: Downlink DHCP messages • *DHCP starvation*: DHCP starvation req messages • *DHCP uplink*: Uplink DHCP messages • *IPv6*: IPv6 packets • *NetBIOS datagram service*: NetBIOS datagram services packets • *NetBIOS name service*: NetBIOS name services packets
	Quarantine Host	Enable/disable station quarantine (default = enable). This option is only available when the security mode includes WPA or WPA2.
	VLAN Pooling	Enable/disable VLAN pooling, allowing you to group multiple wireless controller VLANs into VLAN pools. These pools are used to load-balance sessions evenly across multiple VLANs. • *Managed AP Group*: Select devices to include in the group. • *Round Robin* • *Hash* This option is not available when the traffic mode is *Mesh*.

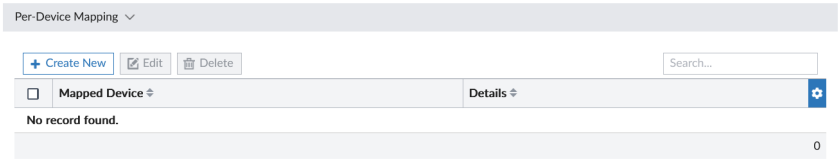


If you select WPA Enterprise, WPA Only Enterprise, or WPA2 Only Enterprise, you can add a different RADIUS server using per-device mapping. See Adding SSID per-device mapping on page 612.

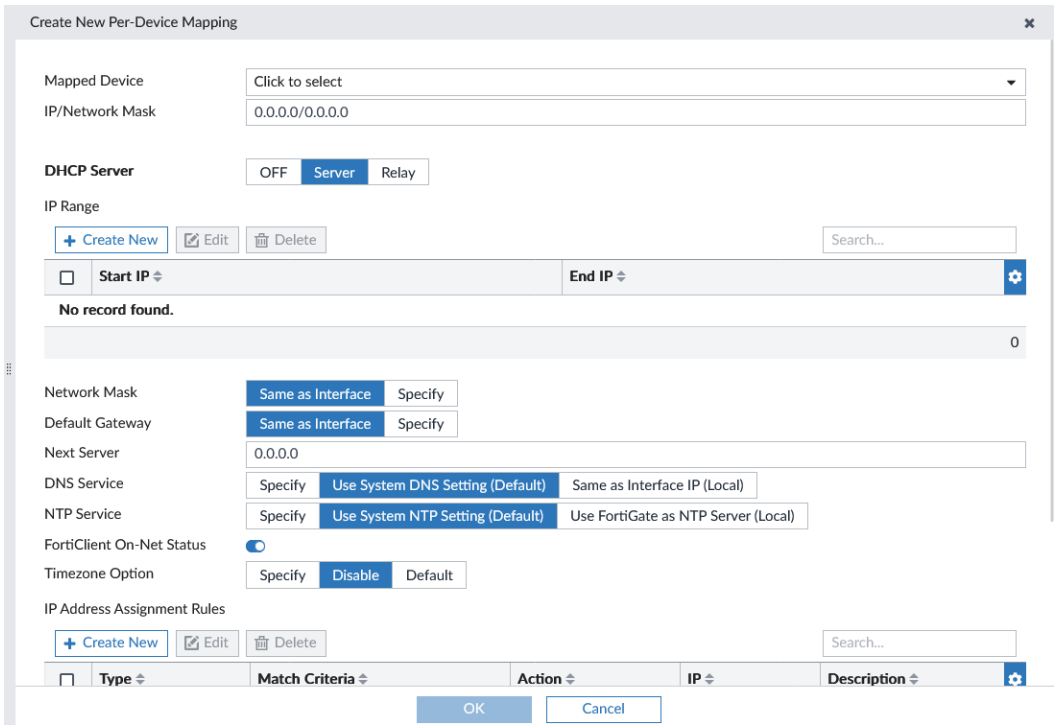
Adding SSID per-device mapping

To add SSID per-device mapping:

1. Go to *AP Manager* > *SSIDs*.
2. Double-click an SSID to edit it, or right-click the SSID and select *Edit*.
3. Enable *Per-Device Mapping*.
4. Click *Create New* in the per-device mapping toolbar. The *Per-Device Mapping* dialog-box opens.



5. Configure the following settings and click *OK*.



Mapped Device	Select the device to be mapped from the drop-down.
Mapped IP/NetMask	Specify the Mapped IP/NetMask.
Mapped DHCP Server	Set the *DHCP Server* to *ON* if you want to map a DHCP Server to this device.
Address Range	Configure address ranges for DHCP. Click *Create* to create a new range. Ranges can also be edited and deleted as required. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
Netmask	Enter the netmask.

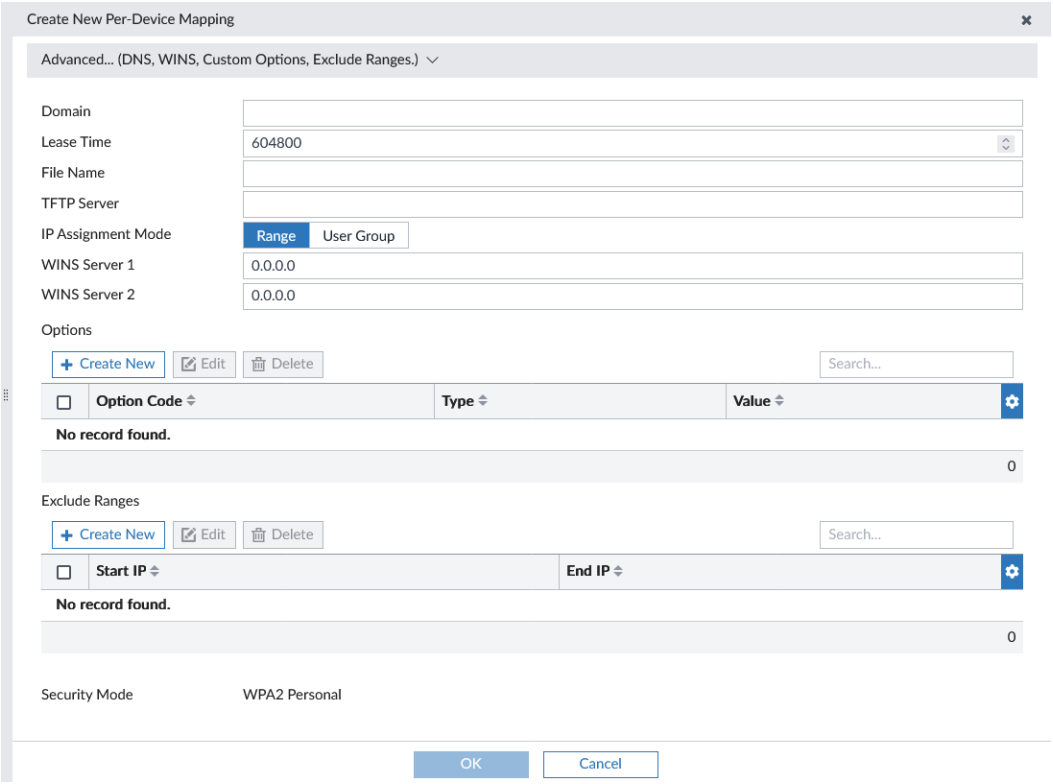
		This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
	Default Gateway	Configure the default gateway: *Same as Interface IP*, or *Specify*. If set to *Specify*, enter the gateway IP address in the field. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
	DNS Server	Configure the DNS server: *Same as System DNS*, *Same as Interface IP*, or *Specify*. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
	Mode	Select the DHCP mode: *Server* or *Relay*. This option is only available when *DHCP Server* is *ON*.
	NTP Server	Configure the NTP server: *Local*, *Same as System NTP*, or *Specify*. If set to *Specify*, enter the NTP server IP address in the field. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
	Time Zone	Configure the timezone: *Disable*, *Same as System*, or *Specify*. If set to *Specify*, select the timezone from the dropdown list. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
	Next Bootstrap Server	Enter the IP address of the next bootstrap server. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
	Additional DHCP Options	In the *Lease Time* field, enter the lease time, in seconds (default = 604800 (7 days)). Add DHCP options to the table. For details, see Adding additional DHCP options on page 614. Options can also be edited and deleted as required. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
	MAC Reservation + Access Control	Select the action to take with unknown MAC addresses: *assign* or *block*. Add MAC address actions to the table. For details, see Adding a MAC address reservation on page 614. Reservations can also be edited and deleted as required. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
	DHCP Server IP	Enter the DHCP server IP address. This option is only available when *DHCP Server* is *ON* and *Mode* is *Relay*.
	Type	Select the type: *Regular*, or *IPsec*. This option is only available when *DHCP Server* is *ON*.

Adding additional DHCP options

You can configure the *Option Code*, *Type*, and *Hexadecimal Value* in SSID profiles when *DHCP Server* is enabled.

To add additional DHCP options:

1. Go to *AP Manager* > *SSIDs*.
2. Create a new SSID profile, or double-click a profile in the list to edit it.
3. Ensure *DHCP Server* is enabled.
4. Expand *Advanced...(DNS, WINS, Custom Options, Exclude Ranges.)*.



5. In the *Options* toolbar, click *Create New*. The *Create New Options* dialog opens.
6. Configure the additional DHCP options.

Option Code	Enter the option code.
Type	Select *HEX*, *String*, *IP*, or *FQDN*
Value	Enter the corresponding hexadecimal value.

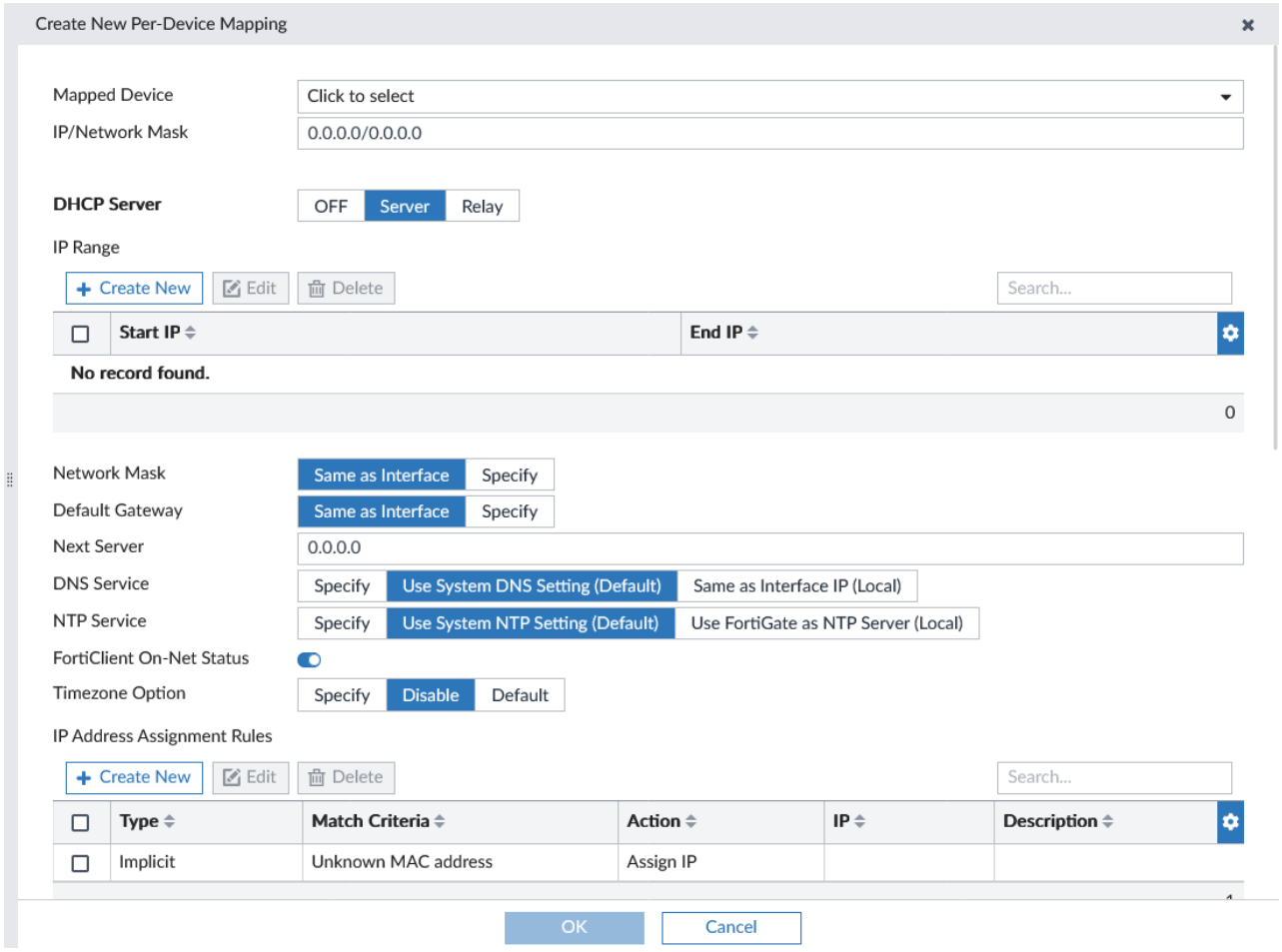
7. Click *OK*.

Adding a MAC address reservation

You can reserve a MAC address in SSID profiles when *DHCP Server* is enabled.

To add a MAC address reservation:

1. Go to *AP Manager* > *SSIDs*.
2. Create a new SSID profile, or double-click a profile in the list to edit it.
3. Ensure *DHCP Server* is enabled.



4. In the *IPAddress Assignment Rules* toolbar, click *Create New*. The *Create New IP Address Assignment Rule* dialog opens.
5. Configure IP Address Assignment Rule.

Type	Select *MAC Address*.
MAC Address	Enter the MAC address.
Action	Select *Reserve IP*.
IP	Enter the IP address.
Description	(Optional) Enter a description of the Assignment Rule.

6. Click *OK*.

FortiAP profiles

FortiAP profiles define radio settings for FortiAP models. The profile specifies details such as the operating mode of the device, SSIDs, and transmit power. Custom AP profiles can be created as needed for new devices.

When you create AP profiles, you can select a Bluetooth profile and/or a WIDS profile.



FortiManager includes Fortinet recommended factory default FortiAP profiles that you can activate and use in your environment. See Using Fortinet recommended profiles on page 646.

To view FortiAP profiles:

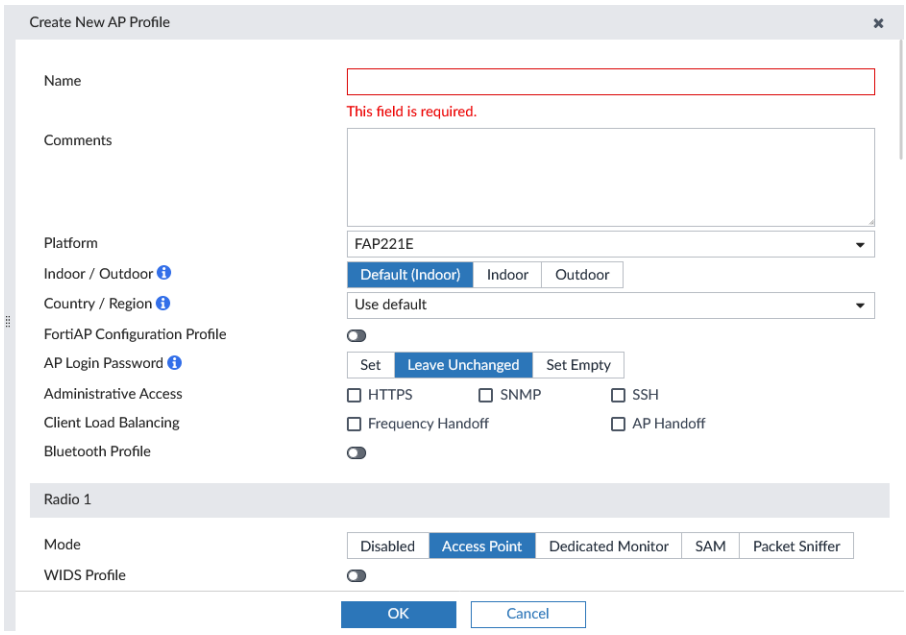
1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager* > *Operation Profiles* > *FortiAP Profiles*.

   The following options are available in the toolbar and right-click menu:

Create New	Create a new AP profile.
Edit	Edit the selected AP profile.
Delete	Delete the selected AP profile.
Clone	Clone the selected AP profile.
Where Used	View where the selected AP profile is used.
Import	Import AP profiles from a connected FortiGate (toolbar only).

To create custom FortiAP profiles:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager* > *Operation Profiles* > *FortiAP Profiles*.
3. In the toolbar, click *Create New*.
   The *Create New AP Profile* pane opens.



4. Enter the following information, and click *OK* to create the AP profile:

Name	Type a name for the profile.
Comment	Optionally, enter comments.
Platform	Select the platform that the profile will apply to from the dropdown list.
Indoor / Outdoor	Select *Default (Indoor)*, *Indoor*, or *Outdoor*. The selection can affect the available channels due to regulatory rules.
Country / Region	Select the country or region from the drop-down list.
AP Login Password	Set, leave unchanged (default), or empty the AP login password.
Administrative Access	Allow management access to the managed AP via *telnet*, *http*, *https*, and/or *ssh*.
Client Load Balancing	Select the client load balancing methods to use: Frequency Handoff and/or AP Handoff.
Bluetooth Profile	If available for the platform, select a profile from the list or click the plus (+) to create a new Bluetooth profile.
Radio 1 & 2	Configure the radio settings. The Radio 2 settings will only appear if the selected platform has two radios.

Mode	Select the radio operation mode: • *Disabled*: The radio is disabled. No further radio settings are available. • *Access Point*: The device is an access point. See options below. • *Dedicated Monitor*: The device is a dedicated monitor. See options below. • *SAM*: The device is a station that can connect to a neighboring AP for connectivity and health check. See options below.

Mode = Access Point	**WIDS Profile**	Select a WIDS profile from the dropdown list. See WIDS profiles on page 631.

Radio Resource Provision	Select to enable radio resource provisioning. This feature measures utilization and interference on the available channels and selects the clearest channel at each access point.
ARRP Profile	Select an Automatic Radio Resource Provisioning (ARRP) profile. See ARRP profiles on page 639. This option is only available if *Radio Resource Provision* is enabled.
Band	Select the wireless protocol from the dropdown list. The available bands depend on the selected platform. In two radio devices, both radios cannot use the same band.
Channel Width	Select 20MHz or 40MHz channel width. This option is only available for 802.11n bands.
Channel Plan	Select *Three Channels* or *Four Channels* to select predefined channels. Select *Custom* to specify custom channels.
Channels	Available when *Channel Plan* is set to *Custom*. Select the channel or channels to include. The available channels depend on the selected platform and band.
Short Guard Interval	Select to enable the short guard interval. This option is only available for 802.11n bands.
Transmit Power Mode	Select *Percent* or *dBm* to specify the minimum and maximum power levels by percent or dBm. Select *Auto* to specify a range of dBm and allow the level to be automatically set within the range.
Transmit Power	If *Transmit Power Mode* is *Percent* or *dBm*, specify the percentage or dBm of the total available power. If *Transmit Power Mode* is *Auto*, enter the power low and high values in dBm.
SSIDs	Choose the SSID profiles that APs using this profile will broadcast. You can select *Tunnel* or *Bridge* to choose them automatically, or *Manual* to select the SSIDs manually. • *Tunnel*: Available tunnel-mode SSIDs are automatically assigned to this radio. • *Bridge*: Available bridge-mode SSIDs are automatically assigned to this radio. • *Manual*: Manually select which available SSIDs and SSID groups to assign to this radio.  Tunnel and Bridge mode automatically assign corresponding SSID profiles that are on the FortiGate to the AP. SSID profiles on FortiManager are not pushed to the FortiGate when using these modes. Manual mode is the only mode that will distribute an SSID profile to the FortiGate.

	Monitor Channel Utilization	Enable/disable monitoring channel utilization.
Mode = Dedicated Monitor	**WIDS Profile**	Select a WIDS profile from the dropdown list. See WIDS profiles on page 631.
Mode = SAM	**SSID**	Enter the SSID for the WiFi network.
	BSSID	Enter the BSSID for the WiFi network.
	Security Type	Select *Open*, *WPA/WPA2 Personal*, or *WPA/WPA2 Enterprise* for the WiFi network.
	WiFi Username	Enter the WiFi username. This option is only available if *Security Type = WPA/WPA2 Enterprise*.
	WiFi Password	Enter the WiFi password. This option is not available if *Security Type = Open*.
	Captive Portal Authentication	Enable/disable captive portal authentication. This option is not available if *Security Type = WPA/WPA2 Enterprise*.
	Test Type	Select *ping* or *Iperf* for the SAM test type.
	Test Server Type	Select *ip* or *fqdn* for the SAM server type.
	Test Server	Enter the SAM IP address or the FQDN according to the Test Server Type.
	Iperf Server Port	Enter the Iperf service port number.
	Iperf Protocol	Select *UDP* or *TCP* for the Iperf test protocol.
	Report Interval (seconds)	Enter the SAM report interval in seconds (60-864000, default = 0). Enter `0` for a one-time report.
LAN Configuration		
	Port ESL Mode	Select *Offline*, *NAT to WAN*, *Bridge to WAN*, or *Bridge to SSID*.
	Port ESL SSID	Available when *Port ESL Mode* is set to *Bridge to SSID*. Select the SSID.
	Handoff STA Thresh	Threshold value for AP handoff (default = 55).
	WAN Port Mode	Enable/disable using a WAN port as a LAN port. Select *wan-lan* or *wan-only* (default = *wan-only*).
ESL SES Dongle Configuration		
	APC FQDN	Enter the FQDN of the ESL SES-imagotag Access Point Controller (APC).
Location Based Services		
FortiPresence		

Mode		Select the FortiPresence mode: • *Disable* • *Foreign channels only* • *Foreign and home channels*
	Project name	The FortiPresence project name.
	Password	FortiPresence secret password.
FortiPresence	**Server Type**	Select *IP* or *FQDN*.
	FortiPresence server IP/FQDN	FortiPresence server IP address or FQDN.
	FortiPresence server port	FortiPresence server UDP listening port (default = 3000).
	Report rogue APs	Enable/disable FortiPresence reporting of Rogue APs.
	Report unassociated clients	Enable/disable FortiPresence reporting of unassociated devices.
	Report transmit frequency (in seconds)	FortiPresence report transmit frequency, in seconds (5 - 65535, default = 30).
Ekahau blink		Enable/disable Ekahau blink location based services.
	RTLS controller server IP	Enter the realtime location services (RTLS) controller server IP address.
	RTLS controller server port	The RTLS controller server port (default = 8569).
	Ekahau tag MAC address	Enter the Ekahau tag MAC address.
AeroScout		Enable/disable AeroScout location based services.
	AeroScout server IP	Enter the AeroScout server IP address.
	AeroScout server port	Enter the AeroScout server port.
	MU mode dilution factor	Enter the MU mode dilution factor (default = 20).
	MU mode dilution timeout	Enter the MU mode dilution timeout (default = 5).
Locate WiFi clients when not connected		Enable/disable locating WiFi client when they are not connected.
Advanced Options		Expand to display and set the advanced options. Hover the mouse over the *i* icon to view a tooltip of each advanced option.

For more information, refer to the *FortiOS CLI Reference*.

You can edit, delete, clone and import existing profiles, as well as see where the profile is being used.

To edit a profile:

1. Select the profile to edit.
2. In the toolbar, click *Edit*.
   Alternatively, you can right-click the profile and select *Edit*, or double-click a profile.
3. Edit the settings as required.
4. Click *OK* to apply your changes.

To delete profiles:

1. Select the profile(s) to be deleted.
2. In the toolbar, click *Delete*.
   Alternatively, right-click the profile and select *Delete*.
3. Click *OK*.

To clone a profile:

1. Select a profile in the list.
2. In the toolbar, click *Clone*.
   Alternatively, right-click a profile and select *Clone*.
3. Edit the name of the profile, then edit the remaining settings as required.
4. Click *OK* to clone the profile.

To import a profile:

1. In the toolbar, click *Import*.
   The *Import* dialog opens.
2. From the *FortiGate* dropdown, select a device. The list will include all of the devices in the current ADOM.
3. From the *Profiles* dropdown, select a profile.
4. Click *OK*.

To view where a profile is used:

1. Select the profile.
2. In the toolbar, click *More* > *Where Used*.
   Alternatively, you can right-click the profile and select *Where Used*.
   The *Where <profile name> is used* pane opens.
3. Click *Close*.



AP profiles can also be imported through the Device Manager. See Importing AP profiles and FortiSwitch templates on page 179.

QoS profiles

You can create, edit, and import QoS profiles, or view where a profile is used. When you create SSID profiles, you can select a QoS profile.

To view Quality of Service (QoS) profiles:

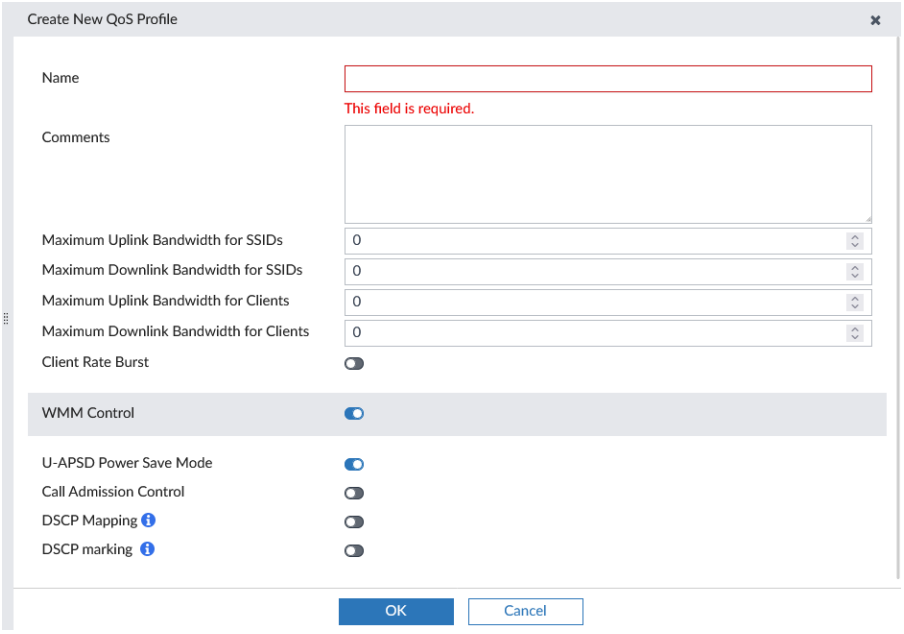
1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager* > *Operation Profiles* > *QoS Profiles*.

   The following options are available in the toolbar and right-click menu:

Create New	Create a new QoS profile.
Edit	Edit the selected QoS profile.
Delete	Delete the selected QoS profile.
Clone	Clone the selected QoS profile.
Where Used	View where the selected QoS profile is used.
Import	Import QoS profiles from a connected FortiGate (toolbar only).

To create a new QoS profile:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager* > *Operation Profiles* > *QoS Profiles*.
3. In the toolbar, click *Create New*.
   The *Create New QoS Profile* pane opens.



4. Enter the following information, and click *OK* to create the QoS profile:

Name	Enter a name for the profile.
Comments	Optionally, enter comments.
Max Uplink Speed (VAPs)	The maximum uplink speed (VAPs), in Kbps (0 - 2097152, default = 0).
Max Downlink Speed (VAPs)	The maximum downlink speed (VAPs), in Kbps (0 - 2097152, default = 0).
Max Uplink Speed (Clients)	The maximum uplink speed (Clients), in Kbps (0 - 2097152, default = 0).
Max Downlink Speed (Clients)	The maximum downlink speed (Clients), in Kbps (0 - 2097152, default = 0).
Client Rate Burst	Enable/disable client rate burst (default = disable).
Wi-Fi MultiMedia	Enable/disable WiFi Multimedia (WMM) control (default = enable).
U-APSD Power Save Mode	Enable/disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode (default = enable). This option is only available if *Wi-Fi MultiMedia* is enabled.
Call Admission Control	Enable/disable WMM call admission control (default = disable). This option is only available if *Wi-Fi MultiMedia* is enabled.
Call Capacity	The maximum number of VoWLAN phones allowed (0 - 60, default = 10). This option is only available if *Call Admission Control* is enabled.
Bandwidth Admission Control	Enable/disable WMM bandwidth admission control (default = disable). This option is only available if *Call Admission Control* is enabled.
Bandwidth Capacity	The maximum bandwidth capacity allowed, in Kbps (1 - 600000, default = 2000). This option is only available if *Bandwidth Admission Control* is enabled.
DSCP Mapping	Enable/disable differentiated Services Code Point (DSCP) mapping (default = disable).
Voice Access	DSCP mapping for voice access category (default = 48, 56). This option is only available if *DSCP Mapping* is enabled.
Video Access	DSCP mapping for video access category (default = 32, 40). This option is only available if *DSCP Mapping* is enabled.
Best Effort Access	DSCP mapping for best effort access category (default = 0, 24). This option is only available if *DSCP Mapping* is enabled.
Background Access	DSCP mapping for background access category (default = 8, 16). This option is only available if *DSCP Mapping* is enabled.

You can edit, delete, clone and import existing profiles, as well as see where the profile is being used.

To edit a profile:

1. Select the profile to edit.
2. In the toolbar, click *Edit*.
   Alternatively, you can right-click the profile and select *Edit*, or double-click a profile.
3. Edit the settings as required.
4. Click *OK* to apply your changes.

To delete profiles:

1. Select the profile(s) to be deleted.
2. In the toolbar, click *Delete*.
   Alternatively, right-click the profile and select *Delete*.
3. Click *OK*.

To clone a profile:

1. Select a profile in the list.
2. In the toolbar, click *Clone*.
   Alternatively, right-click a profile and select *Clone*.
3. Edit the name of the profile, then edit the remaining settings as required.
4. Click *OK* to clone the profile.

To import a profile:

1. In the toolbar, click *Import*.
   The *Import* dialog opens.
2. From the *FortiGate* dropdown, select a device. The list will include all of the devices in the current ADOM.
3. From the *Profiles* dropdown, select a profile.
4. Click *OK*.

To view where a profile is used:

1. Select the profile.
2. In the toolbar, click *More* > *Where Used*.
   Alternatively, you can right-click the profile and select *Where Used*.
   The *Where <profile name> is used* pane opens.
3. Click *Close*.

Bonjour profiles

You can create, edit, and import Bonjour profiles, or view where a profile is used.

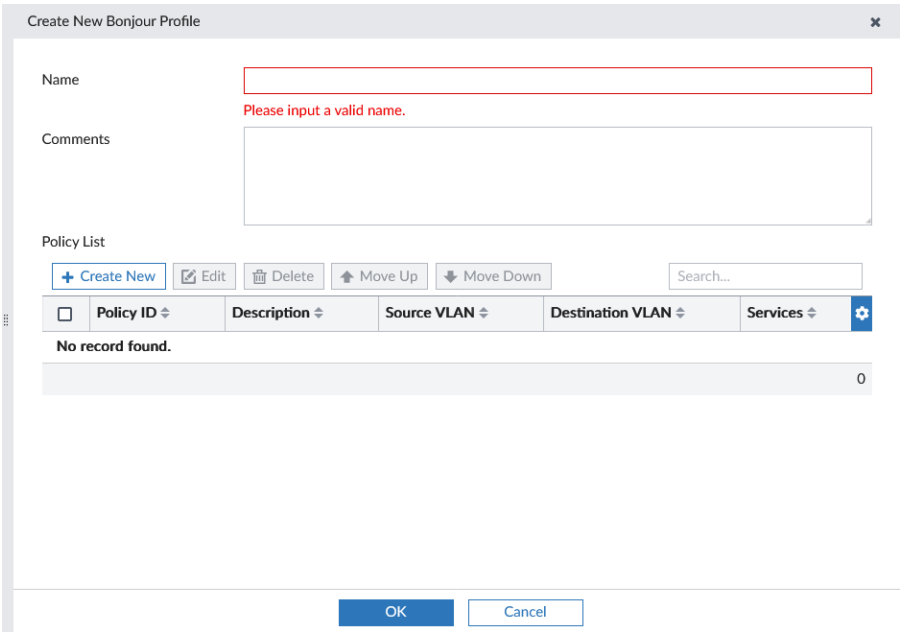
To view Bonjour profiles:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager* > *Connectivity Profiles* > *Bonjour Profiles*.
   The following options are available in the toolbar and right-click menu:

Create New	Create a new Bonjour profile.
Edit	Edit the selected Bonjour profile.
Delete	Delete the selected Bonjour profile.
Clone	Clone the selected Bonjour profile.
Where Used	View where the selected Bonjour profile is used.
Import	Import Bonjour profiles from a connected FortiGate (toolbar only).

To create a new Bonjour profile:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager* > *Connectivity Profiles* > *Bonjour Profiles*.
3. In the toolbar, click *Create New*.
   The *Create New Bonjour Profile* pane opens.



4. Enter the following information, and then click *OK* to create the Bonjour profile:

Name	Enter a name for the profile.
Comments	Optionally, enter comments.
Policy List	Configure the policy list.
Create New	Create a new policy list entry.

	Select the following, then click *OK*: • *Description*: Description of the Bonjour profile policy. • *From VLAN*: The VLAN ID that the Bonjour service will be advertised from (0 - 4094, default = 0). • *To VLAN*: The VLAN ID that the Bonjour service will be made available to (0 - 4094, default = all). • *Services*: Services for the VLAN.
Edit	Edit the selected entry.
Delete	Delete the selected entries.

You can edit, delete, clone and import existing profiles, as well as see where the profile is being used.

To edit a profile:

1. Select the profile to edit.
2. In the toolbar, click *Edit*.
   Alternatively, you can right-click the profile and select *Edit*, or double-click a profile.
3. Edit the settings as required.
4. Click *OK* to apply your changes.

To delete profiles:

1. Select the profile(s) to be deleted.
2. In the toolbar, click *Delete*.
   Alternatively, right-click the profile and select *Delete*.
3. Click *OK*.

To clone a profile:

1. Select a profile in the list.
2. In the toolbar, click *Clone*.
   Alternatively, right-click a profile and select *Clone*.
3. Edit the name of the profile, then edit the remaining settings as required.
4. Click *OK* to clone the profile.

To import a profile:

1. In the toolbar, click *Import*.
   The *Import* dialog opens.
2. From the *FortiGate* dropdown, select a device. The list will include all of the devices in the current ADOM.
3. From the *Profiles* dropdown, select a profile.
4. Click *OK*.

To view where a profile is used:

1. Select the profile.
2. In the toolbar, click *More* > *Where Used*.
   Alternatively, you can right-click the profile and select *Where Used*.
   The *Where <profile name> is used* pane opens.
3. Click *Close*.

Bluetooth profiles

You can create, edit, and import Bluetooth profiles, or view where a profile is used. When you create AP profiles, you can select a Bluetooh profile.



Bluetooth profiles are not available in version 5.4 ADOMs.

To view and Bluetooth profiles:

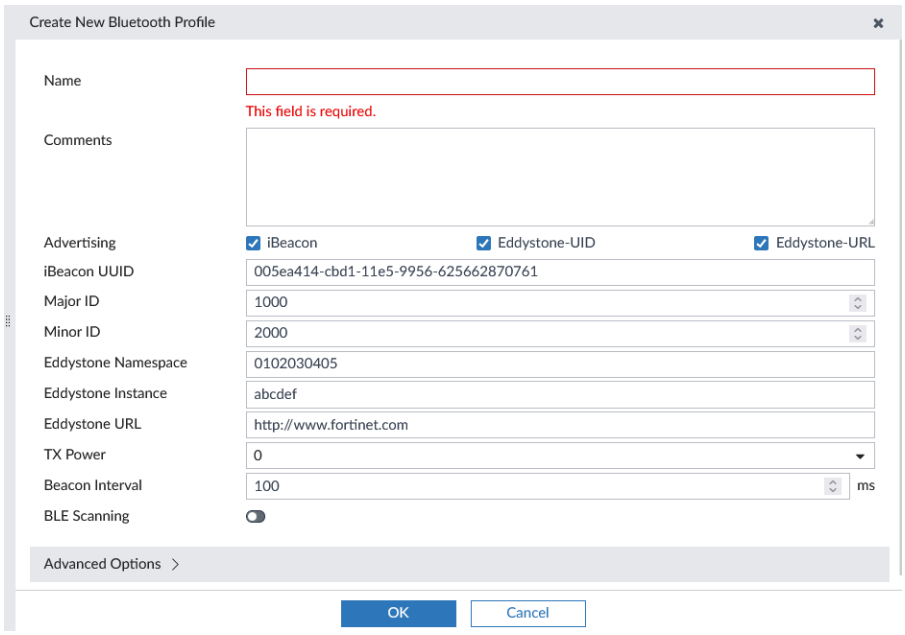
1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager* > *Connectivity Profiles* > *Bluetooth Profiles*.

   The following options are available in the toolbar and right-click menu:

Create New	Create a new Bluetooth profile.
Edit	Edit the selected Bluetooth profile.
Delete	Delete the selected Bluetooth profile.
Clone	Clone the selected Bluetooth profile.
Import	Import Bluetooth profiles from a connected FortiGate (toolbar only).

To create a new Bluetooth profile:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager* > *Connectivity Profiles* > *Bluetooth Profiles* (or from the tabs in version 5.6 ADOMs).
3. In the toolbar, click *Create New*.
   The *Create New Bluetooth Profile* pane opens.



4. Enter the following information, and click *OK* to create the Bluetooth profile:

Name	Enter a name for the profile.
Comments	Optionally, enter comments.
Advertising	Select the advertising types: *iBeacon*, *Eddystone-UID*, and *Eddystone-URL*.
iBeacon UUID	The iBeacon Universally Unique Identifier (UUID) is automatically assigned, but can be manually reset (63 characters).
Major ID	The major ID (1 - 65535, default = 1000).
Minor ID	The minor ID (1 - 65535, default = 2000).
Eddystone Namespace	The eddystone namespace ID (10 characters).
Eddystone Instance	The eddystone instance ID (6 characters).
Eddystone URL	The eddystone URL (127 characters).
TX Power	Transmit power level: *0* = -21 dBm, *1* = -18 dBm, *2* = -15 dBm, *3* = -12 dBm, *4* = -9 dBm, *5* = -6 dBm, *6* = -3 dBm, *7* = 0 dBm, *8* = 1 dBm, *9* = 2 dBm, *10* = 3 dBm, *11* = 4 dBm, *12* = 5 dBm
Beacon Interval	The beacon interval, in milliseconds (40 - 3500, default = 100).
BLE Scanning	Enable/disable Bluetooth Low Energy (BLE) scanning.
Advanced Options	Enter the eddystone encoded URL hexadecimal string size (54 characters) in the *eddystone-url-encode-hex* field.

You can edit, delete, clone and import existing profiles, as well as see where the profile is being used.

To edit a profile:

1. Select the profile to edit.
2. In the toolbar, click *Edit*.
   Alternatively, you can right-click the profile and select *Edit*, or double-click a profile.
3. Edit the settings as required.
4. Click *OK* to apply your changes.

To delete profiles:

1. Select the profile(s) to be deleted.
2. In the toolbar, click *Delete*.
   Alternatively, right-click the profile and select *Delete*.
3. Click *OK*.

To clone a profile:

1. Select a profile in the list.
2. In the toolbar, click *Clone*.
   Alternatively, right-click a profile and select *Clone*.
3. Edit the name of the profile, then edit the remaining settings as required.
4. Click *OK* to clone the profile.

To import a profile:

1. In the toolbar, click *Import*.
   The *Import* dialog opens.
2. From the *FortiGate* dropdown, select a device. The list will include all of the devices in the current ADOM.
3. From the *Profiles* dropdown, select a profile.
4. Click *OK*.

To view where a profile is used:

1. Select the profile.
2. In the toolbar, click *More* > *Where Used*.
   Alternatively, you can right-click the profile and select *Where Used*.
   The *Where <profile name> is used* pane opens.
3. Click *Close*.

WIDS profiles

The WIDS monitors wireless traffic for a wide range of security threats by detecting and reporting on possible intrusion attempts. When an attack is detected, a log message is recorded. When you create AP profiles, you can select a WIDS profile.

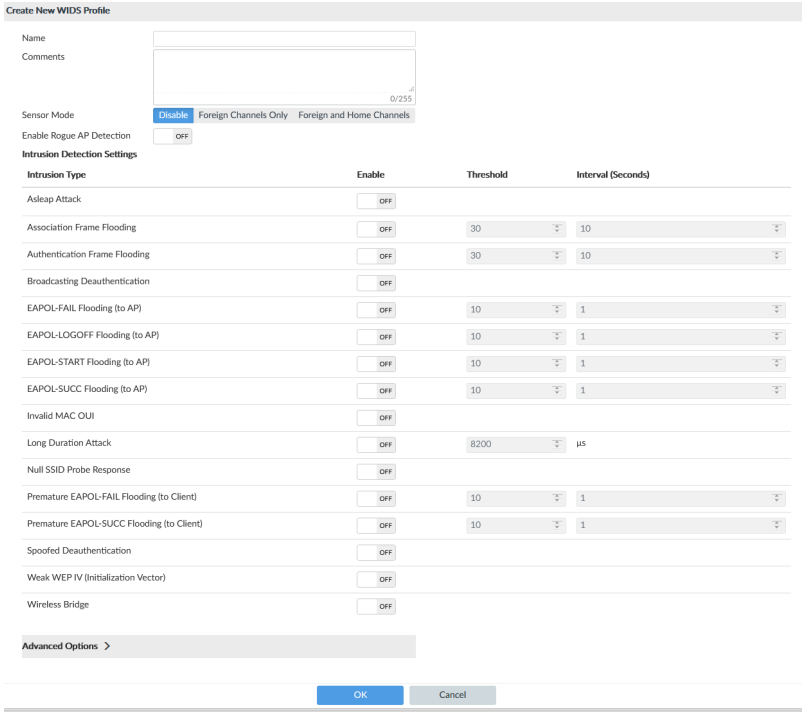
To view WIDS profiles:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager* > *Protection Profiles* > *WIDS Profiles*.
   The following options are available in the toolbar and right-click menu:

Create New	Create a new WIDS profile.
Edit	Edit the selected WIDS profile.
Delete	Delete the selected WIDS profile.
Clone	Clone the selected WIDS profile.
Where Used	Displays the ADOM where the profile is used as well as the Policy Package/Block.
Import	Import WIDS profiles from a connected FortiGate (toolbar only).

To create a new WIDS profile:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager* > *Protection Profiles* > *WIDS Profiles*.
3. In the toolbar, click *Create New*.
   The *Create New WIDS Profile* pane opens.



4. Enter the following information, and click *OK* to create the WIDS profile:

Name	Enter a name for the profile.
Comments	Optionally, enter comments.

Sensor Mode	
Enable Rogue AP Detection	Select to enable rogue AP detection.
Background Scan Every	Enter the number of seconds between background scans.
Enable Passive Scan Mode	Enable/disable passive scan mode.
Auto Suppress Rouge APs in Foreground Scan	Enable/disable automatically suppressing rogue APs in foreground scans. This options is only available when the sensor mode is not disabled.
Disable Background Scan During Specified Time	Enable/disable background scanning during the specified time. Specify the days of week, and the start and end times.
Intrusion Type	The intrusion types that can be detected. See Intrusion types on page 634.
Enable	Select to enable the intrusion type.
Threshold	If applicable, enter a threshold for reporting the intrusion, in seconds except where specified.
Interval (Seconds)	If applicable, enter the interval for reporting the intrusion, in seconds.
Advanced Options	
ap-bgscan-duration	Listening time on a scanning channel, in milliseconds (10 - 1000, default = 20).
ap-bgscan-idle	Waiting time for channel inactivity before scanning this channel, in milliseconds (0 - 1000, default = 0).
ap-bgscan-intv	Period of time between scanning two channels, in seconds (1 - 600, default = 1).
ap-bgscan-report-intv	Period of time between background scan reports, in seconds (15 - 600, default = 30).
ap-fgscan-report-intv	Period of time between foreground scan reports, in seconds (15 - 600, default = 15).
deauth-broadcast	Enable/disable broadcasting deauthentication detection (default = disable).
deauth-unknown-src-thresh	Threshold value per second to deauthenticate unknown sources for DoS attacks, in seconds (0 - 65535, 0 = no limit, default = 10).
invalid-mac-oui	Enable/disable invalid MAC OUI detection (default = disable).

You can edit, delete, clone and import existing profiles, as well as see where the profile is being used.

To edit a profile:

1. Select the profile to edit.
2. In the toolbar, click *Edit*.
   Alternatively, you can right-click the profile and select *Edit*, or double-click a profile.
3. Edit the settings as required.
4. Click *OK* to apply your changes.

To delete profiles:

1. Select the profile(s) to be deleted.
2. In the toolbar, click *Delete*.
   Alternatively, right-click the profile and select *Delete*.
3. Click *OK*.

To clone a profile:

1. Select a profile in the list.
2. In the toolbar, click *Clone*.
   Alternatively, right-click a profile and select *Clone*.
3. Edit the name of the profile, then edit the remaining settings as required.
4. Click *OK* to clone the profile.

To import a profile:

1. In the toolbar, click *Import*.
   The *Import* dialog opens.
2. From the *FortiGate* dropdown, select a device. The list will include all of the devices in the current ADOM.
3. From the *Profiles* dropdown, select a profile.
4. Click *OK*.

To view where a profile is used:

1. Select the profile.
2. In the toolbar, click *More* > *Where Used*.
   Alternatively, you can right-click the profile and select *Where Used*.
   The *Where <profile name> is used* pane opens.
3. Click *Close*.

Intrusion types

Intrusion Type	Description
Asleap Attack	ASLEAP is a tool used to perform attacks against LEAP authentication.

Intrusion Type	Description
Association Frame Flooding	A Denial of Service attack using association requests. The default detection threshold is 30 requests in 10 seconds.
Authentication Frame Flooding	A Denial of Service attack using association requests. The default detection threshold is 30 requests in 10 seconds.
Broadcasting Deauthentication	This is a type of Denial of Service attack. A flood of spoofed de-authentication frames forces wireless clients to de-authenticate, then re-authenticate with their AP.
EAPOL Packet Flooding (to AP)	Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the AP with these packets can be a denial of service attack. Several types of EAPOL packets can be detected: • EAPOL-FAIL • EAPOL-LOGOFF • EAPOL-START • EAPOL-SUCC
Invalid MAC OUI	Some attackers use randomly-generated MAC addresses. The first three bytes of the MAC address are the Organizationally Unique Identifier (OUI), administered by IEEE. Invalid OUIs are logged.
Long Duration Attack	To share radio bandwidth, WiFi devices reserve channels for brief periods of time. Excessively long reservation periods can be used as a denial of service attack. You can set a threshold between 1000 and 32 767 microseconds. The default is 8200µ.
Null SSID Probe Response	When a wireless client sends out a probe request, the attacker sends a response with a null SSID. This causes many wireless cards and devices to stop responding.
Premature EAPOL Packet Flooding (to client)	Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the client with these packets can be a denial of service attack. Two types of EAPOL packets can be detected: • EAPOL-FAIL • EAPOL-SUCC
Spoofed Deauthentication	Spoofed de-authentication frames form the basis for most denial of service attacks.
Weak WEP IV Detection	A primary means of cracking WEP keys is by capturing 802.11 frames over an extended period of time and searching for patterns of WEP initialization vectors (IVs) that are known to be weak. WIDS detects known weak WEP IVs in on-air traffic.
Wireless Bridge	WiFi frames with both the FromDS and ToDS fields set indicate a wireless bridge. This will also detect a wireless bridge that you intentionally configured in your network.

L3 firewall profiles

Layer 3 firewall rules provide granular access control of client traffic in your wireless network. An L3 firewall profile allows or denies traffic between wireless clients based on the configured source and destination IP addresses/ports and specific protocols. The L3 firewall profile must be assigned to an SSID profile.

To view access control lists:

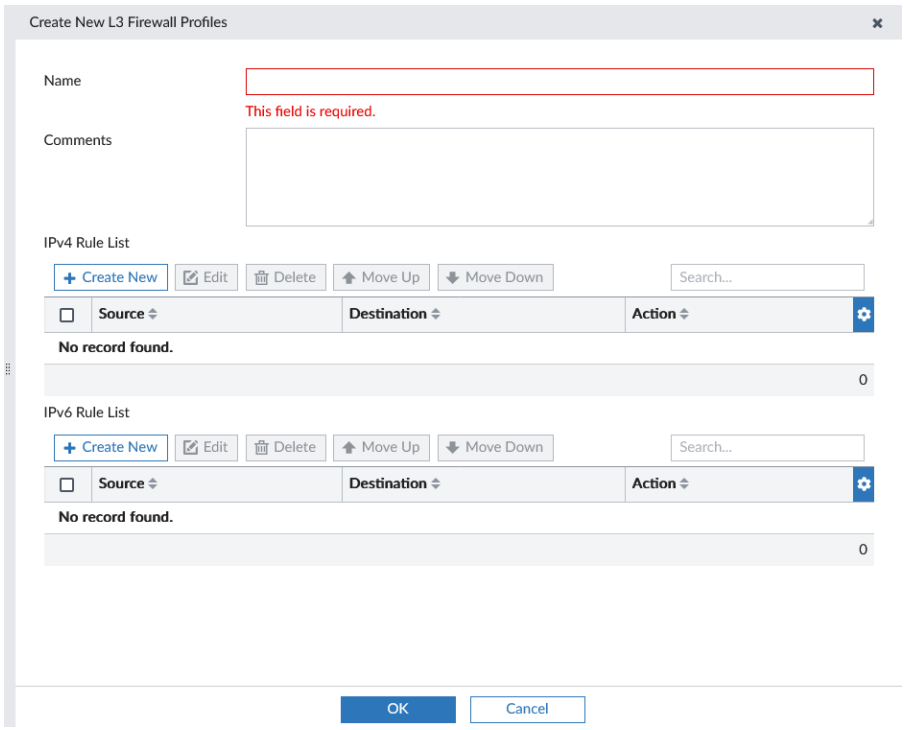
1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager > Protection Profiles > L3 Firewall Profiles*.

   The following options are available in the toolbar and right-click menu:

Create New	Create a new access control list.
Edit	Edit the selected access control list.
Delete	Delete the selected access control list.
Clone	Clone the selected access control list.
Where Used	View where the selected access control list is used.
Import	Import access control lists from a connected FortiGate (toolbar only).

To create access control lists:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager > Protection Profiles > L3 Firewall Profiles*.
3. In the toolbar, *Create New*.
   The *Create New Access Control List* pane opens.



4. Enter the following information:

Name	Type a name for the access control list.
Comment	Optionally, enter comments.
Layer3 IPv4 Rules	Click *Create New* to define access control rules for IPv4 addresses in layer 3. Select the following, then click *OK*: • *Rule ID*: Enter an ID for the rule. • *Comments*: Optionally, enter a description. • *Source Address*: Enter the source IP address. • *Source Port*: Enter the source port. • *Destination Address*: Enter the destination IP address. • *Destination Port*: Enter the destination port. • *Protocol*: Enter the protocol. • *Action*: Select the policy action. Select *Allow* or *Deny* to allow or deny traffic matching the policy.
Layer 3 IPv6 Rules	Click *Create New* to define access control rules for IPv6 addresses in layer 3. Select the following, then click *OK*: • *Rule ID*: Enter an ID for the rule. • *Comments*: Optionally, enter a description. • *Source Address*: Enter the source IP address. • *Source Port*: Enter the source port. • *Destination Address*: Enter the destination IP address.

- *Destination Port*: Enter the destination port.
- *Protocol*: Enter the protocol.
- *Action*: Select the policy action. Select *Allow* or *Deny* to allow or deny traffic matching the policy.

5. Click *OK* to create the new access control list.

You can edit, delete, clone and import existing profiles, as well as see where the profile is being used.

To edit a profile:

1. Select the profile to edit.
2. In the toolbar, click *Edit*.
   Alternatively, you can right-click the profile and select *Edit*, or double-click a profile.
3. Edit the settings as required.
4. Click *OK* to apply your changes.

To delete profiles:

1. Select the profile(s) to be deleted.
2. In the toolbar, click *Delete*.
   Alternatively, right-click the profile and select *Delete*.
3. Click *OK*.

To clone a profile:

1. Select a profile in the list.
2. In the toolbar, click *Clone*.
   Alternatively, right-click a profile and select *Clone*.
3. Edit the name of the profile, then edit the remaining settings as required.
4. Click *OK* to clone the profile.

To import a profile:

1. In the toolbar, click *Import*.
   The *Import* dialog opens.
2. From the *FortiGate* dropdown, select a device. The list will include all of the devices in the current ADOM.
3. From the *Profiles* dropdown, select a profile.
4. Click *OK*.

To view where a profile is used:

1. Select the profile.
2. In the toolbar, click *More > Where Used*.
   Alternatively, you can right-click the profile and select *Where Used*.
   The *Where <profile name> is used* pane opens.
3. Click *Close*.

ARRP profiles

A default Automatic Radio Resource Provisioning (ARRP) profile named *arrp-default* is available. You can also create custom ARRP profiles. These ARRP profiles can be assigned in AP profiles. See FortiAP profiles on page 616

To view ARRP profiles:

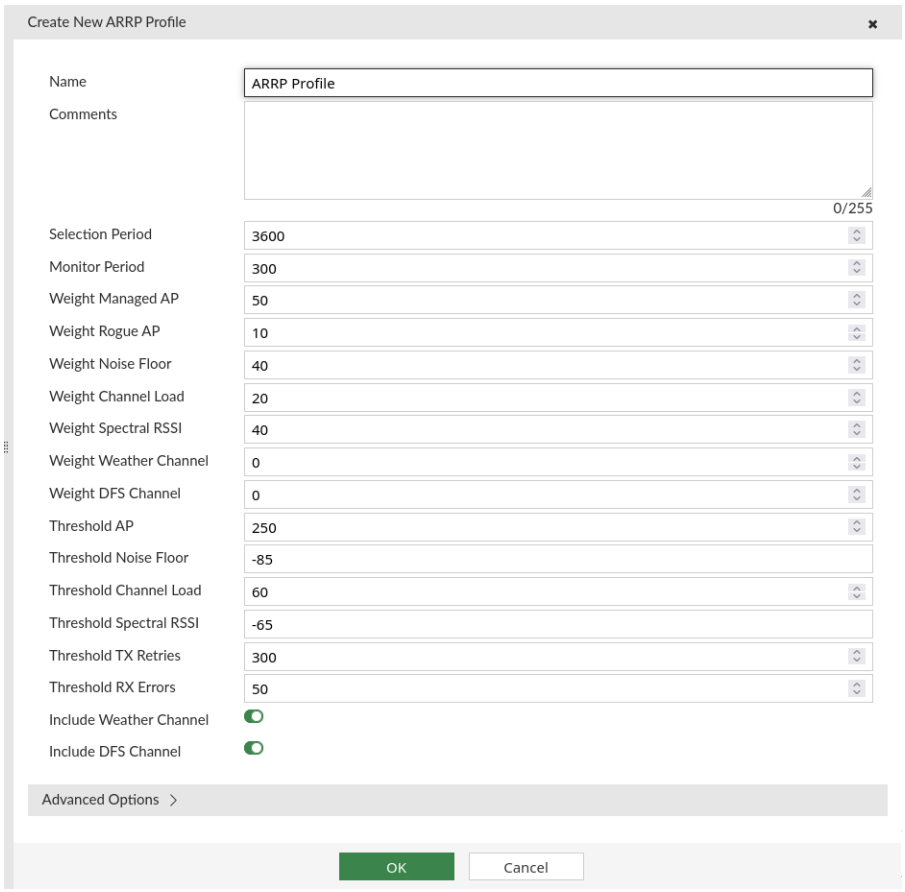
1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager > Operation Profiles > AARP Profiles*.

   The following options are available in the toolbar and right-click menu:

Create New	Create a new ARRP profile.
Edit	Edit the selected ARRP profile.
Delete	Delete the selected ARRP profile.
Clone	Clone the selected ARRP profile.
Where Used	View where the selected ARRP profile is used.
Import	Import ARRP profiles from a connected FortiGate (toolbar only).

To create custom ARRP profiles:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager > Operation Profiles > AARP Profiles*.
3. In the toolbar, click *Create New*.
   The *Create New ARRP Profile* pane opens.



4. Configure the ARRP profile settings, and click *OK* to create the ARRP profile.
   For more information on available ARRP profile settings, see the FortiWiFi and FortiAP Configuration Guide.

You can edit, delete, clone and import existing profiles, as well as see where the profile is being used.

To edit a profile:

1. Select the profile to edit.
2. In the toolbar, click *Edit*.
   Alternatively, you can right-click the profile and select *Edit*, or double-click a profile.
3. Edit the settings as required.
4. Click *OK* to apply your changes.

To delete profiles:

1. Select the profile(s) to be deleted.
2. In the toolbar, click *Delete*.
   Alternatively, right-click the profile and select *Delete*.
3. Click *OK*.

To clone a profile:

1. Select a profile in the list.
2. In the toolbar, click *Clone*.
   Alternatively, right-click a profile and select *Clone*.
3. Edit the name of the profile, then edit the remaining settings as required.
4. Click *OK* to clone the profile.

To import a profile:

1. In the toolbar, click *Import*.
   The *Import* dialog opens.
2. From the *FortiGate* dropdown, select a device. The list will include all of the devices in the current ADOM.
3. From the *Profiles* dropdown, select a profile.
4. Click *OK*.

To view where a profile is used:

1. Select the profile.
2. In the toolbar, click *More* > *Where Used*.
   Alternatively, you can right-click the profile and select *Where Used*.
   The *Where <profile name> is used* pane opens.
3. Click *Close*.

WiFi settings

You can create a profile of WiFi settings. After you create the profile, assign the profile to devices, and install the changes to devices. You can assign WiFi settings profiles to FortiGate VDOMs.

To view WiFi settings profile list:

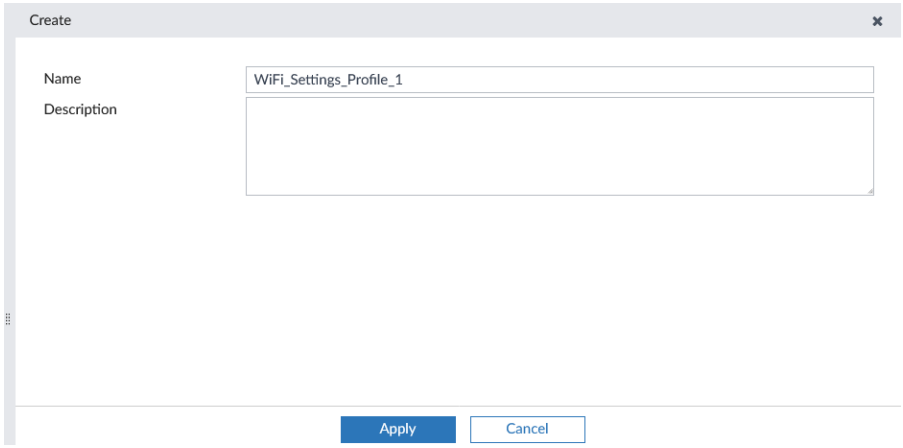
1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager* > *WiFi Settings*.

   The following options are available in the toolbar and right-click menu:

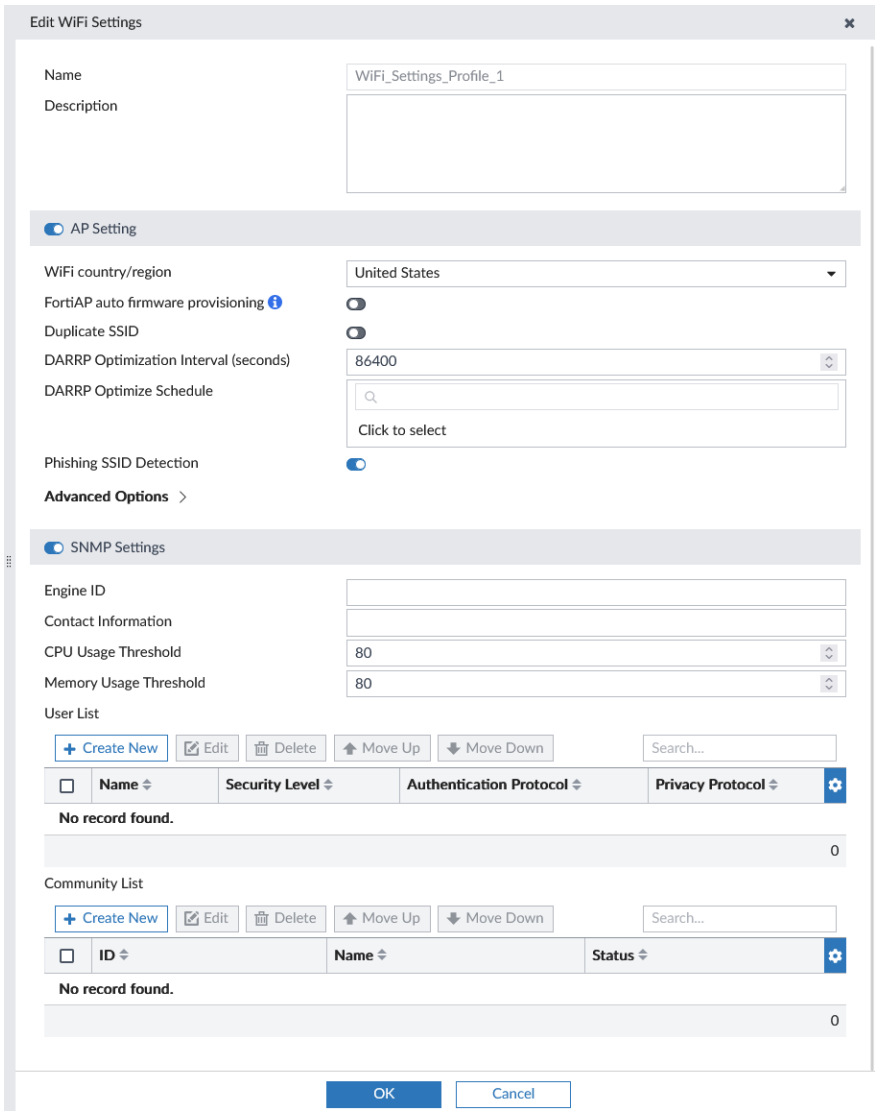
Create New	Create a new WiFi settings profile.
Edit	Edit the selected WiFi settings profile.
Delete	Delete the selected WiFi settings profile.
Assign to Device/Group	Assign the selected WiFi settings profile to one or more devices.
Clone	Clone the selected WiFi settings profile.

To create WiFi settings profiles:

1. Ensure you are in the correct ADOM.
2. Go to *AP Manager* > *WiFi Settings*.
3. In the toolbar, click *Create New*.
   The *Create* dialog opens.



4. Type a name and description (optional), and click *Apply*.
   The *Edit WiFi Settings* pane opens.



5. Enter the following information, and click *OK* to create the WiFi settings profile:

Description		Optionally, enter a description of the settings.
AP Setting		Enable to access and set AP settings.
	Duplicate SSID	Enable/disable allowing Virtual Access Points (VAPs) to use the same SSID name in the same VDOM (default = disable).
	Phishing SSID Detect	Enable/disable phishing SSID detection (default = enable).
	DARRP Optimize	Enter the time for running Dynamic Automatic Radio Resource Provisioning (DARRP) (0 to 86400, default = 86400).
	DARRP Optimize Schedule	Select the schedule name. Firewall schedules for DARRP running time. DARRP will run periodically based on darrp-optimize within the schedules.

	Advanced Options	Expand to display and set the advanced options. Hover the mouse over the *i* icon to view a tooltip of each advanced option. For more information, refer to the *FortiOS CLI Reference*.
SNMP Profile		Enable to access and set SNMP profile settings.
	Engine ID	Enter the SNMP engine ID (maximum 24 characters).
	Contact Info	Enter the contact information for the contact information for the SNMP (maximum 31 characters).
	Trap High CPU threshold	Enter CPU usage when trap is sent (10 to 100, default = 80).
	Trap High MEM threshold	Enter the memory usage when trap is sent (10 to 100, default = 80).
	Community	Click *Create New* to create a community. Select the following, then click *OK*: • *ID*: Enter the ID for the community. • *Name*: Enter a name for the community. • *Status*: Enable/disable this SNMP community. • *Query V1 Status*: Enable/disable SNMP v1 queries. • *Query V2c Status*: Enable/disable SNMP v2c queries. • *Trap V1 Status*: Enable/disable SNMP v1 traps. • *Trap V2c Status*: Enable/disable SNMP v2c traps. • *Hosts*: Create new hosts. Enter the IP/netmask for the SNMP manager (host).
	User	Click *Create New* to create a new user. Select the following, then click *OK*: • *Name*: Enter a name for the SNMP user. • *Status*: Enable/disable this user. • *Queries*: Enable/disable SNMP queries for this user. • *Trap Status*: Enable/disable traps for this SNMP user. • *Security Level*: Select the security level for message authentication and encryption. Configure the authentication and encryption, as needed. • *Notify Hosts*: Enter the IPv4-address to configure SNMP User Notify Hosts.

To assign WiFi settings profiles to devices:

1. Select the WiFi settings profile, and click *Assign to Device/Group*.
   The *Assign to Devices/Groups* dialog opens.
2. In the *Available Entries* list, select the devices, and click the *right arrow* (>) to move the devices to the *Selected Entries* list.
3. Click *OK* to save the changes.
4. Click *Install Wizard* to install the changes to the selected devices.

You can edit, delete, clone and import existing profiles, as well as see where the profile is being used.

To edit a profile:

1. Select the profile to edit.
2. In the toolbar, click *Edit*.
   Alternatively, you can right-click the profile and select *Edit*, or double-click a profile.
3. Edit the settings as required.
4. Click *OK* to apply your changes.

To delete profiles:

1. Select the profile(s) to be deleted.
2. In the toolbar, click *Delete*.
   Alternatively, right-click the profile and select *Delete*.
3. Click *OK*.

To clone a profile:

1. Select a profile in the list.
2. In the toolbar, click *Clone*.
   Alternatively, right-click a profile and select *Clone*.
3. Edit the name of the profile, then edit the remaining settings as required.
4. Click *OK* to clone the profile.

To import a profile:

1. In the toolbar, click *Import*.
   The *Import* dialog opens.
2. From the *FortiGate* dropdown, select a device. The list will include all of the devices in the current ADOM.
3. From the *Profiles* dropdown, select a profile.
4. Click *OK*.

To view where a profile is used:

1. Select the profile.
2. In the toolbar, click *More* > *Where Used*.
   Alternatively, you can right-click the profile and select *Where Used*.
   The *Where <profile name> is used* pane opens.
3. Click *Close*.

Assigning profiles to FortiAP devices

You use the AP Manager pane to assign profiles to FortiAP devices, and you use the Device Manager pane to install profiles to FortiAP devices when you install a configuration to the FortiGate that controls the FortiAP

device.

For more information about creating and managing AP profiles, see FortiAP profiles on page 616.

To assign profiles to FortiAP devices:

1. Go to *AP Manager > Managed FortiAPs*.
2. Select a Managed FortiGate device. Alternatively, you can select a device in a group, see FortiAP groups on page 590.
3. Locate the FortiAP device in the list in the content pane, or refine the list by selecting an option from the quick status bar.
4. Select the device.
5. In the toolbar, click *Assigned Profile*, or right-click the FortiAP and select *Assigned Profile*. The *Assign AP Profile* window opens.
6. Select a FortiAP profile from the dropdown list, then click *OK* to assign the profile.

Using Fortinet recommended profiles

FortiManager includes factory default SSID and FortiAP profiles recommended by Fortinet.

The Fortinet recommended profiles are based on Fortinet security best practices, and they are created based on the most relevant network topologies Fortinet sees with customer implementation. The configuration is validated by Fortinet field engineers and security experts.

The following Fortinet recommended FortiAP profiles and SSIDs are available:

AP Profiles	SSIDs
• Basic_Data_Fortinet_Default • High_Throughput_Data_Dual5GHz_Fortinet_Default • High_Throughput_Data_Fortinet_Default • RTLS_Presence_Fortinet_Default • Voice_Enterprise_Fortinet_Default	• Enterprise_Fortinet_Default • Guest_Fortinet_Default • IoT_Fortinet_Default • Voice_Fortinet_Default

You can use recommended templates by activating them from the *AP Manager > Operation Profiles > FortiAP Profiles* and *AP Manager > SSIDs*menu in FortiManager and then configuring them to meet your requirements.

This topic includes the following information:

- Fortinet recommended SSID profiles on page 646
- Fortinet recommended FortiAP profiles on page 648

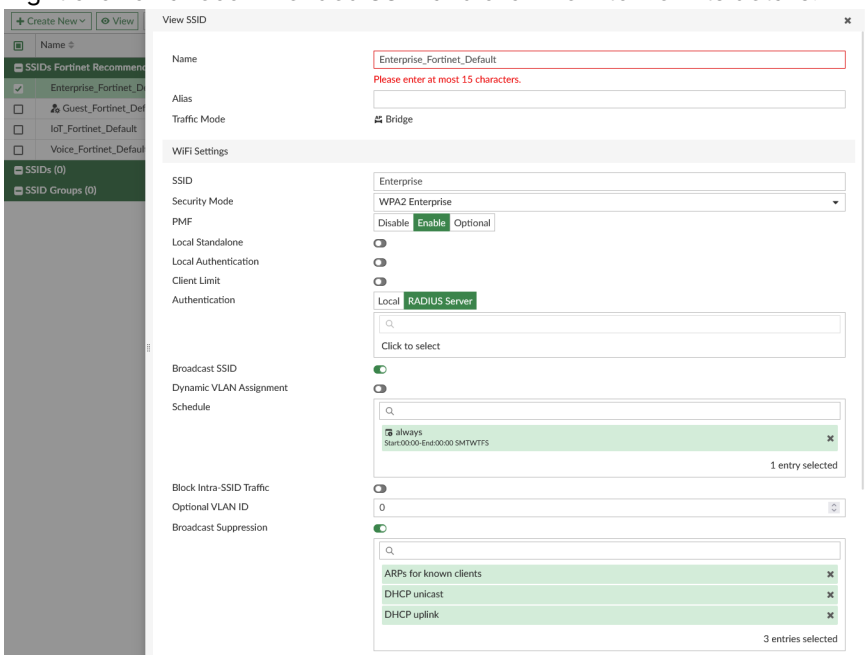
Fortinet recommended SSID profiles

To use Fortinet recommended SSID profiles:

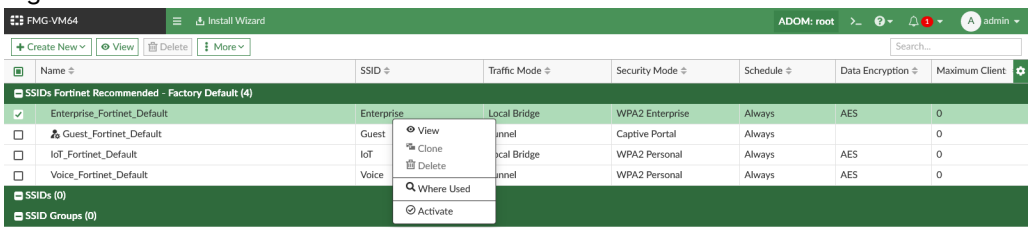
1. Go to *AP Manager > SSIDs* to view the default SSID profiles.
   The recommended default SSID profiles are displayed.



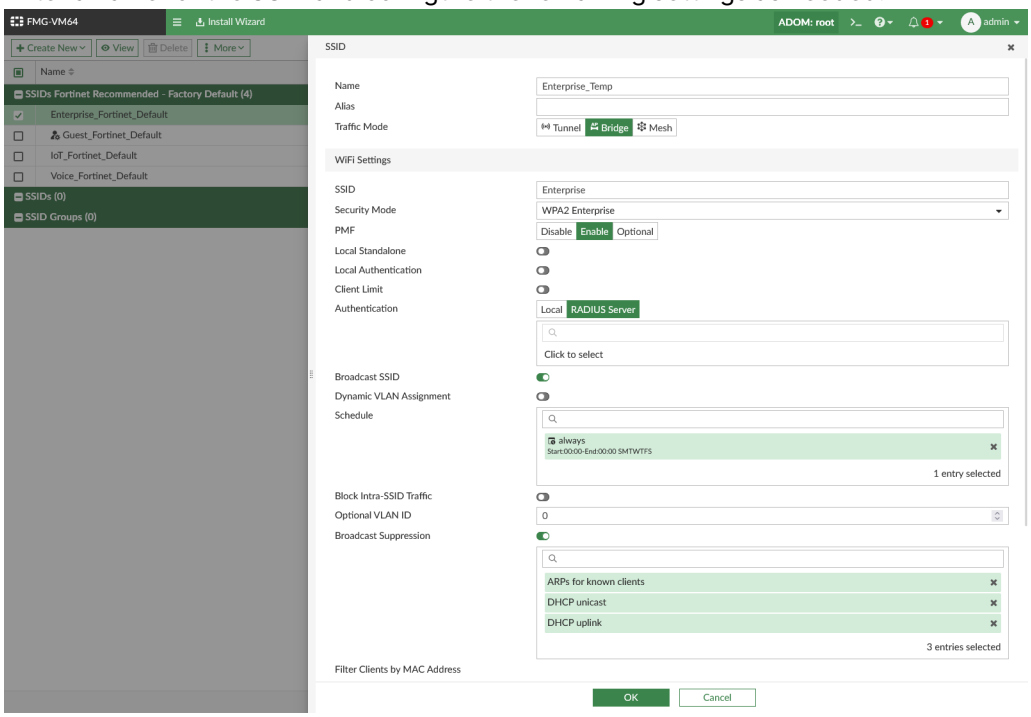
2. Right click on a recommended SSID and click *View* to view its details.



3. Right-click on a recommended SSID and click *Activate*.



4. Enter a name for the SSID and configure the remaining settings as needed.

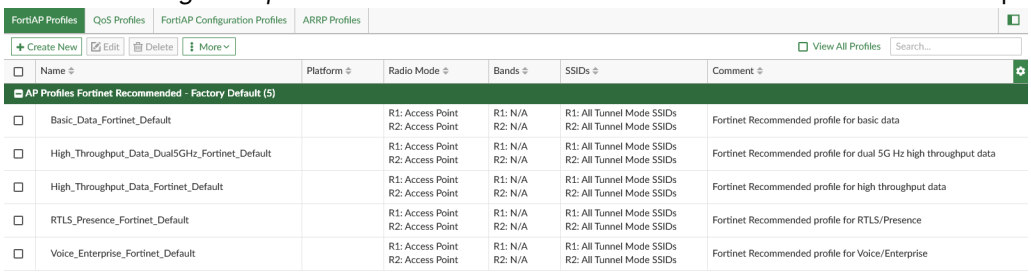


5. Assign the SSID to an AP profile, and then assign the AP profile to a FortiAP.

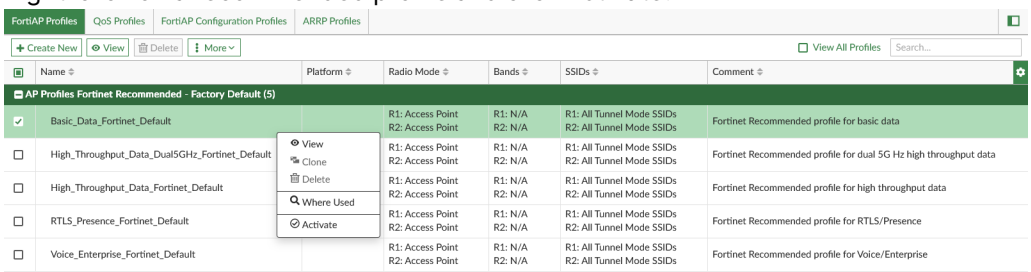
Fortinet recommended FortiAP profiles

To use Fortinet recommended FortiAP profiles:

1. Go to *AP Manager* > *Operation Profiles* > *FortiAP Profiles* to view the default FortiAP profiles.



2. Right click on a recommended AP profile and click *View* to view its details.
3. Right-click on a recommended profile and click *Activate*.



4. Select the platform type for the profile.

5. Enter a name for the AP profile and configure the remaining settings if required.

WiFi profiles and settings for per-device management

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

The following steps provide an overview of using per-device access point management:

1. Enable per-device management. See Enabling FortiAP per-device management on page 649.
2. Configure profiles for each managed access point. See Creating profiles on page 649.
3. Install changes to managed access points. See Installing changes to FortiAP devices on page 592.

Enabling FortiAP per-device management

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

To enable access point per-device management:

1. Go to *System Settings* > *ADOMs*.
2. Double-click the ADOM to open it for editing.
3. Beside *Central Management*, clear the *FortiAP* checkbox, and click *OK*.
   Central management is disabled, and per-device management is enabled for *AP Manager*.

Creating profiles

To create profiles:

1. Go to *AP Manager* > *Managed FortiAPs*.
2. Select a device from the list.
3. Go to the *Operation Profiles* > *FortiAP Profiles* tab.
4. In the toolbar, click *Create New*. The *Create New FortiAP Profile* pane opens.
5. Configure the profile settings, and click *OK*. The changes are saved to the FortiGate database.

VPN Manager

Use the *VPN Manager* pane to enable and use central VPN management. You can view and configure IPsec VPN and SSL-VPN settings that you can install to one or more devices.

After you use *VPN Manager* to configure VPN for FortiGates in the ADOM, it is not recommended to move the FortiGate devices to another ADOMs because the VPN settings are for the specific ADOM.



Additional configuration options and short-cuts are available using the right-click content menu. Right-click the mouse on different parts of the navigation panes on the GUI page to access these context menus.

The *VPN Manager* pane includes the following in the tree menu:

IPsec VPN Communities	Displays all of defined IPsec VPN communities and associated devices for the selected ADOM. You can create, monitor, and manage VPN settings. See IPsec VPN Communities on page 666
IPsec VPN Map	Displays an IPsec VPN map by topology view or traffic view. See Using Map View on page 683.
SSL-VPN Setting	View and manage SSL VPN settings. See SSL VPN settings on page 685.
SSL VPN Portals	View and create SSL VPN portal profiles. See SSL VPN portals on page 687
SSL VPN Monitor	View the SSL VPN monitor. See SSL VPN monitor on page 694

Overview

When central VPN management is enabled, you can use the *VPN Manager* pane to configure IPsec VPN settings that you can install to one or more devices. The settings are stored as objects in the objects database. You can then select the objects in policies for policy packages on the *Policy & Objects* pane. You install the IPsec VPN settings to one or more devices by installing the policy package to the devices.



You must enable central VPN management to access the settings on the *VPN Manager > IPsec VPN Communities* pane. However, you can access the settings on the *SSL-VPN* panes without enabling central VPN management. See Enabling central VPN management on page 651.

You can also configure VPN settings directly on a FortiGate by using *Device Manager*, and the configuration is stored in the device database. When you create a VPN configuration by using *VPN Manager*, FortiManager copies the VPN configuration from the objects database to the device database before installing the configuration to FortiGates. In addition, FortiManager checks for differences between the configuration in the

device database and the configuration on FortiGate. If any differences are found, FortiManager only installs the configuration differences to FortiGate. This process helps avoid conflicts.



If you are using both *Device Manager* and *VPN Manager* to configure VPN settings, you should avoid using *Device Manager* to modify the settings created by *VPN Manager*, because when installing a policy package again, the settings from *VPN Manager* will override the previous changes to those settings from *Device Manager*. *Device Manager* should only be used to create or modify VPN configurations that are not created by *VPN Manager*.

To create IPsec VPN settings:

1. Enable central VPN management. See Enabling central VPN management on page 651.
2. Create a VPN community, sometimes called a VPN topology. See Creating IPsec VPN communities on page 667.
3. Create a managed gateway. See Creating managed gateways on page 676.

To create SSL-VPN settings:

1. Create custom profiles. See Creating SSL VPN portal profiles on page 688.
   Alternately, you can skip this step, and use the default portal profiles.
2. Add an SSL VPN to a device, and select a portal profile. See Creating SSL VPNs on page 685.

To install VPN objects to devices:

1. Plan the VPN security policies. See VPN security policies on page 695.
2. In a policy package, create VPN security policies, and select the VPN settings. See Creating policies on page 429.
3. Edit the installation targets for the policy package to add all of the devices onto which you want to install the policy defined VPN settings. See Policy package installation targets on page 422.
4. Install the policy package to the devices. See Install a policy package on page 419.

Enabling central VPN management

You can enable centralized VPN management from the *VPN Manager > IPsec VPN* pane.

You can also enable centralized VPN management by editing an ADOM. When ADOMs are disabled, you can enable centralized VPN management by using the *Dashboard* pane.

Regardless of how you enable centralized VPN management, you use the *VPN Manager* module for centralized VPN management.

To enable central VPN management:

1. Go to *VPN Manager > IPsec VPN Communities*
   The VPN management status pane includes a message indicating that centralized VPN management is

currently disabled.

2. Select *Enable*.

To enable central VPN management for an ADOM:

1. Ensure that you are in the correct ADOM.
2. Go to *System Settings* > *ADOMs*.
3. Right-click an ADOM, and select *Edit*.
4. In the *Central Management* field, select the *VPN* checkbox.
5. Click *OK*. Centralized VPN management is enabled for the ADOM.

To enable central VPN management when ADOMs are disabled:

1. Go to *Dashboard*.
2. In the *System Information* widget, in the *VPN Management Mode* field, select *Change VPN Management Mode*. The *Change VPN Management Mode* dialog box is displayed.
3. Click *OK*.

DDNS support

When Dynamic DNS (DDNS) is enabled on FortiGates, VPN Manager supports DDNS. First VPN Manager searches for the interface IP for IPsec Phase2. If no IP is found, then VPN Manager searches for DDNS.

You can use FortiManager and the CLI Configurations menu to enable DDNS on each FortiGate device. The CLI Configurations menu is available in the Device Manager pane. See Device DB - CLI Configurations on page 227.

With the CLI Configurations menu, you can use the `config system ddns` command to enable DDNS on a per-device basis. The selected monitoring interface must be the interface that supports your tunnel, for example:

```
config system ddns
   edit 1
      set ddns-server FortiGuardDDNS
      set ddns-domain "<HOST1>.fortiddns.com"
      set monitor-interface "port14"
   next
end
```

You can also use the CLI Configurations menu to configure DDNS on multiple FortiGate interfaces. Once configured, you can use FortiManager to view all the DDNS entries, but you cannot edit the entries.

Following is an example of how to configure DDNS on multiple FortiGates by using the CLI Configurations menu:

```
config system ddns
   edit 1
      set ddns-server FortiGuardDDNS
      set ddns-domain "<HOST1>.fortiddns.com"
      set use-public-ip enable
      set monitor-interface "wan"
   next
   edit 2
      set ddns-server FortiGuardDDNS
```

```
        set ddns-domain "<HOST2>.fortiddns.com"
        set use-public-ip disable
        set monitor-interface "wwan"
    next
end
```

Multiple DDNS entries are useful when using SDWAN and multiple broadband links.

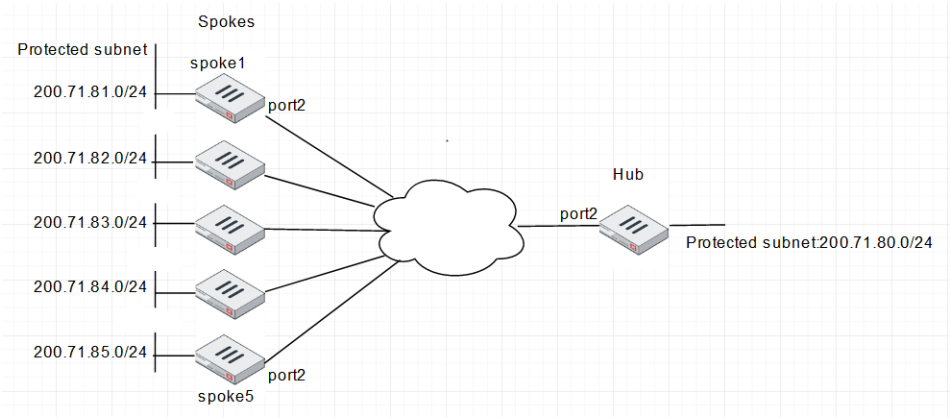
VPN Setup Wizard supports device groups

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 Creating device groups on page 654.
2. Create protected subnet firewall addresses for hub and spoke devices. See Creating protected subnet firewall addresses on page 654.
3. Create a VPN community. See Creating VPN communities on page 656.
4. Add spoke FortiGate units to the VPN community. See Adding spoke FortiGate units to the VPN community on page 657.
5. Add the hub FortiGate units to the VPN community. See Adding the hub FortiGate unit to the VPN community on page 659.
   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 662

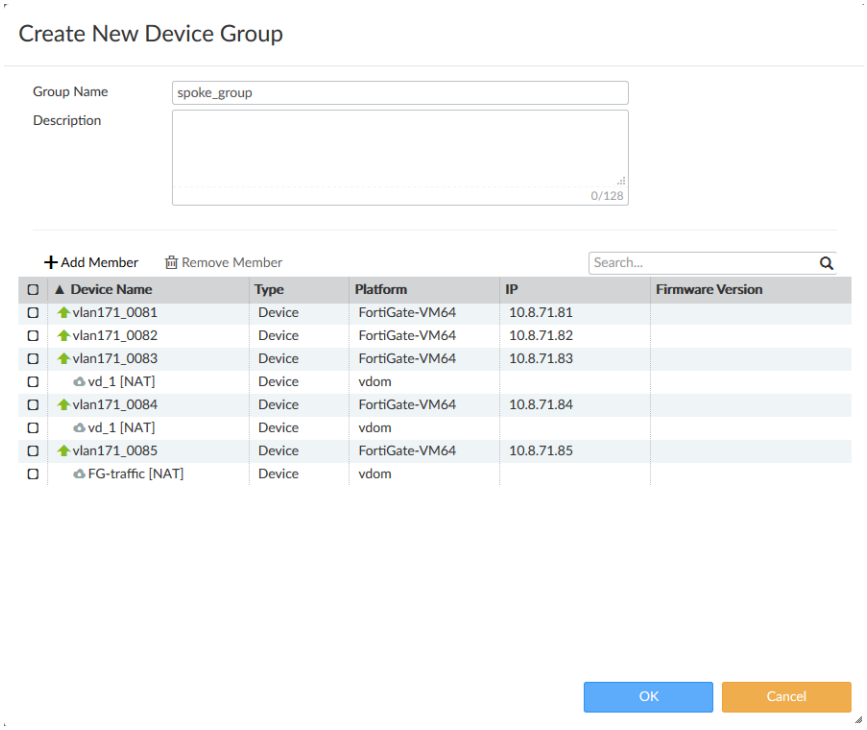
This topic also covers how to:

- Remove a spoke member from a VPN community. See Removing a spoke member from a VPN community on page 663
- Add a spoke member to a VPN community. See Adding a spoke member to a VPN community on page 665

Creating device groups

To create device groups:

1. Go to *Device Manager* > *Device & Groups*.
2. From the *Device Group* menu, select *Create New Group*.
   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.



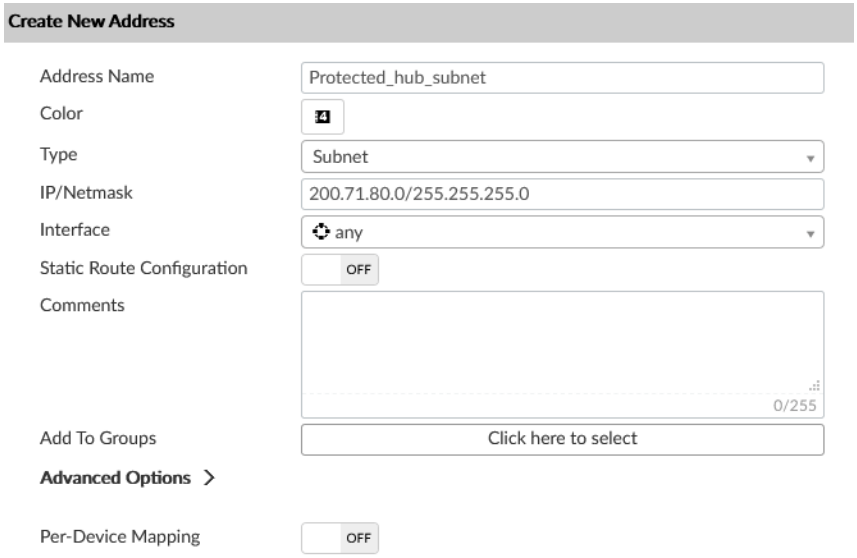
5. Click *OK* to save the group.

Creating protected subnet firewall addresses

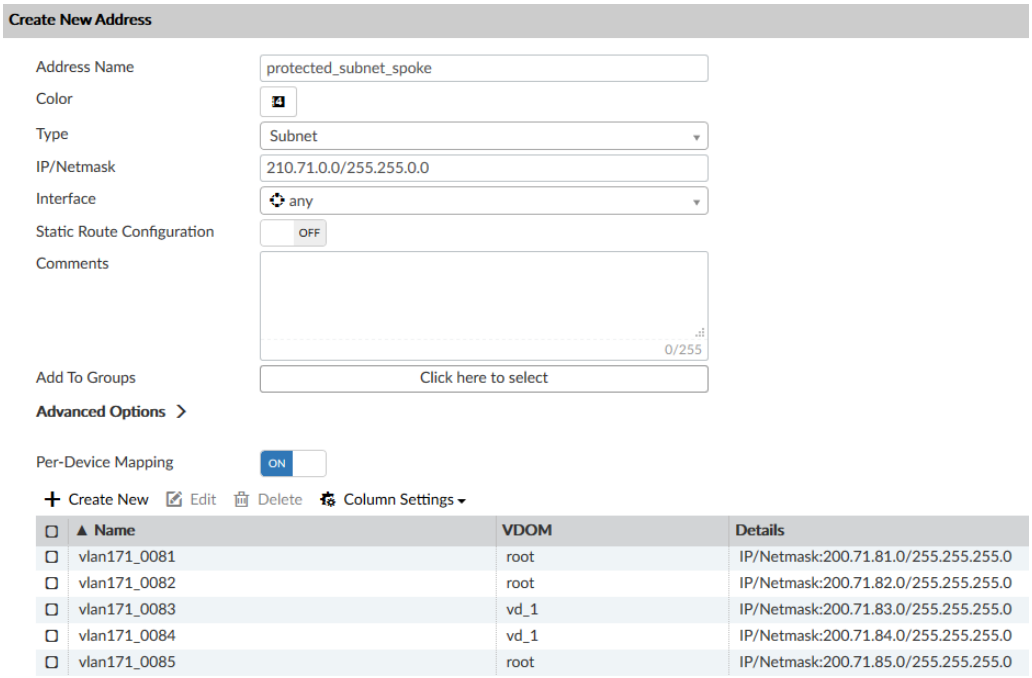
Create protected subnet firewall addresses for hub and spoke devices. VPN Manager can use the protected subnet firewall address to create static routes on FortiGate units to allow traffic destined for the remote protected network to pass through the VPN tunnel.

To create protected subnet firewall addresses:

1. Go to *Policy & Objects* > *Firewall Objects* > *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*.



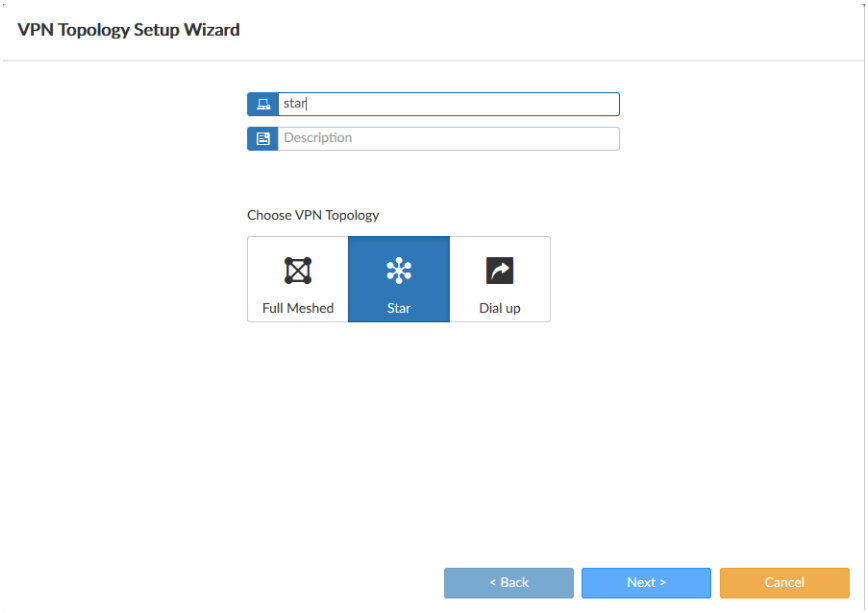
4. From the *Create New* menu, select *Address*.
   The *Create New Address* pane opens.
5. Create a protected subnet firewall address with per-device mapping for spoke FortiGate units, and click *OK*.



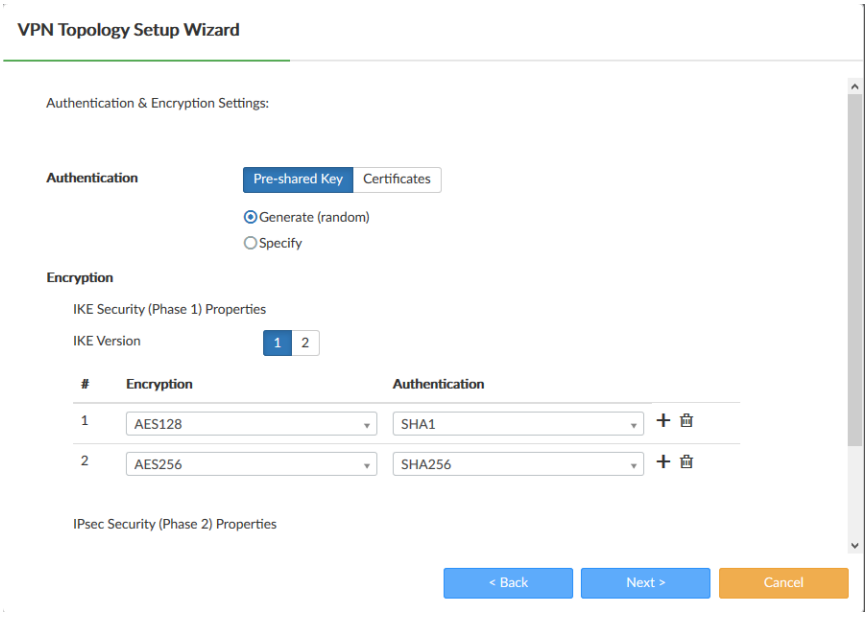
Creating VPN communities

To create a VPN community:

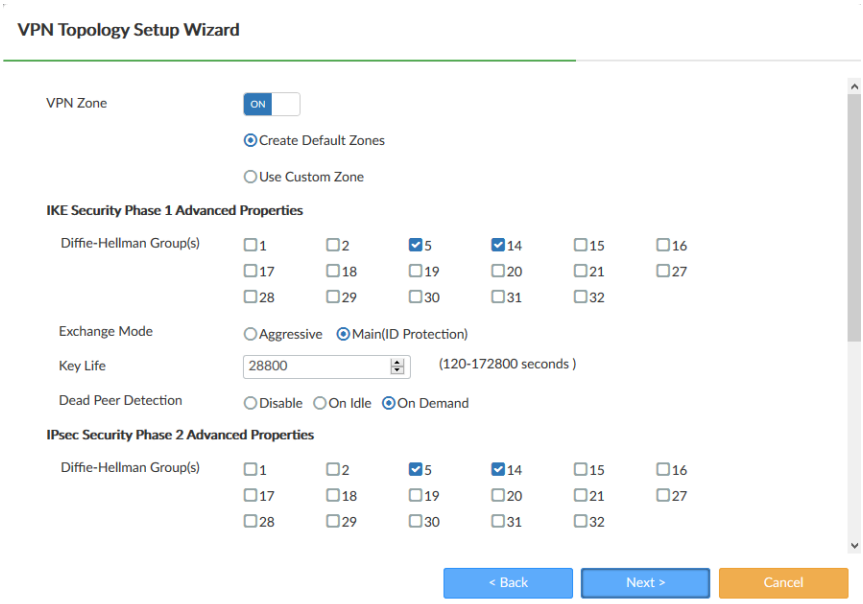
1. Go to *VPN Manager > IPsec VPN Communities*, and click *Create New*. The *VPN Topology Setup Wizard* opens.
2. In the *Name* box, type a name, such as *star*.
3. Under *Choose VPN Topology*, select *Star*, and click *Next*.



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



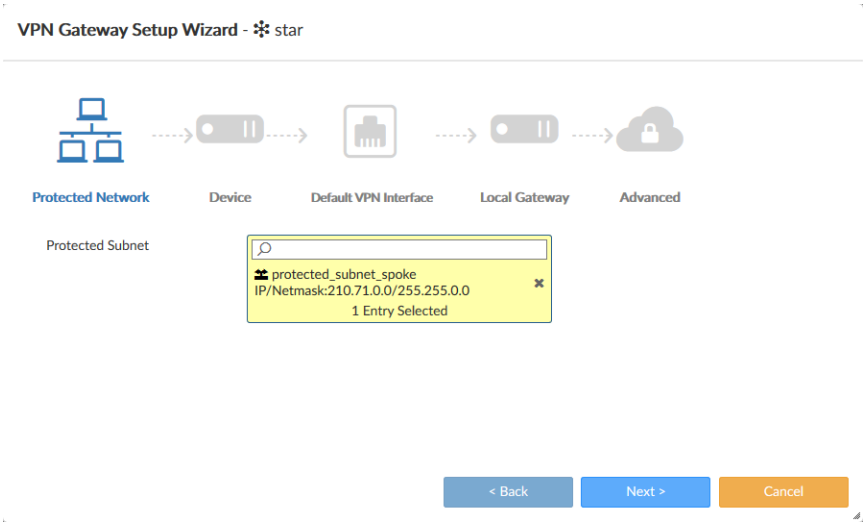
5. Configure VPN Phase 1 and Phase 2 settings, and click *Next*.



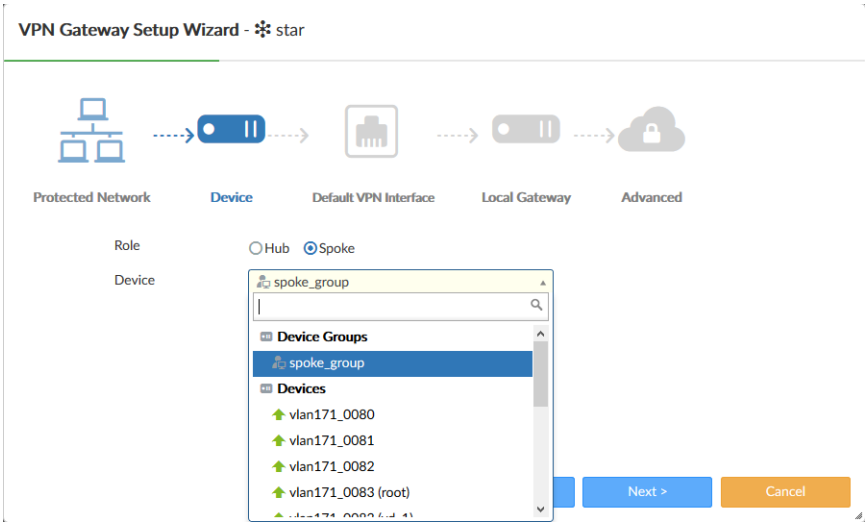
Adding spoke FortiGate units to the VPN community

To add spoke FortiGate units to the VPN community:

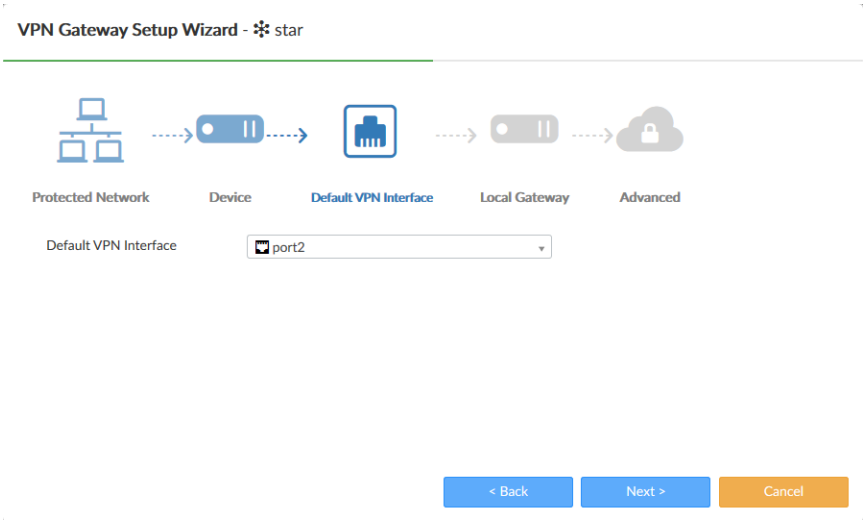
1. Go to *VPN Manager* > *IPsec VPN Communities*, and click the community that you created.
   The community opens in the content pane.
2. Click *Create New* > *Managed Gateway*.
   The *VPN Gateway Setup Wizard* opens for the community.
3. Set the *Protected Network* options, and then click *Next*: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



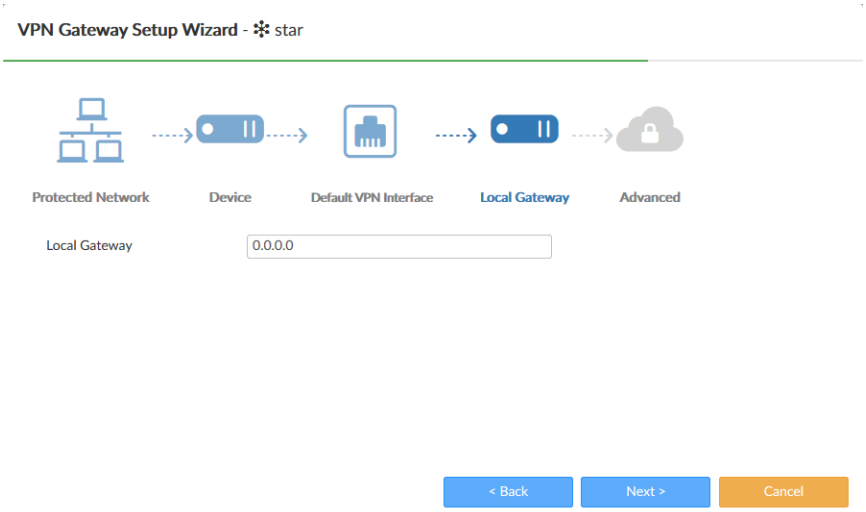
4. Set the *Device* options, and then click *Next*:
   a. Beside *Role*, select *Spoke*.
   b. Beside *Device*, select the device group you created named *spoke_group*.



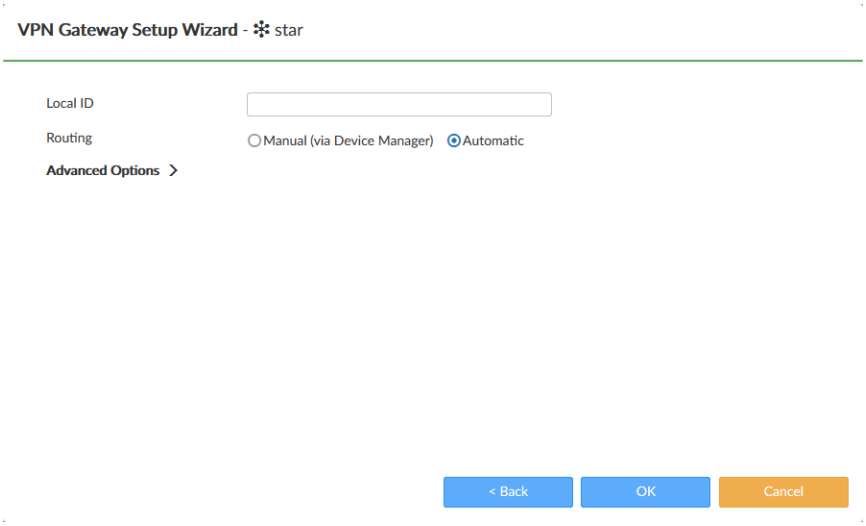
5. Set the *Default VPN Interface* options, and click *Next*.
   a. Beside *Default VPN Interface*, select the interface for spokes, which is often the internet-facing interface.



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



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

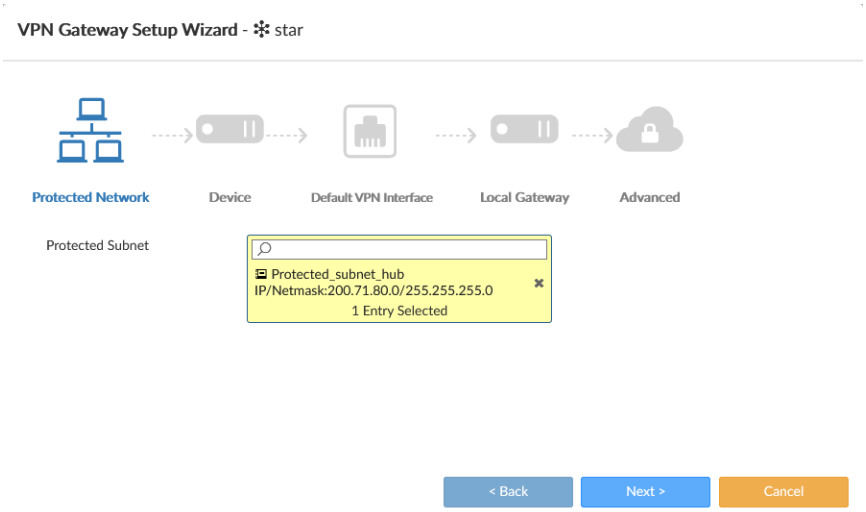


Adding the hub FortiGate unit to the VPN community

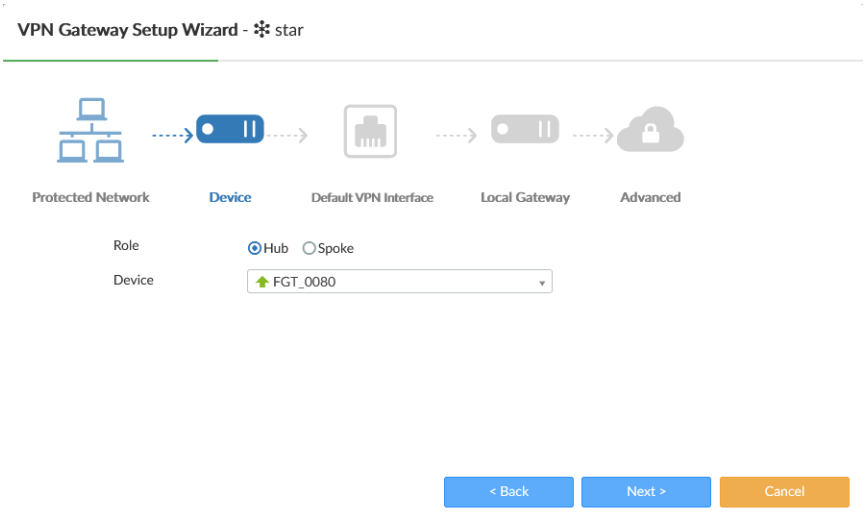
To add a hub FortiGate unit to the VPN community:

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

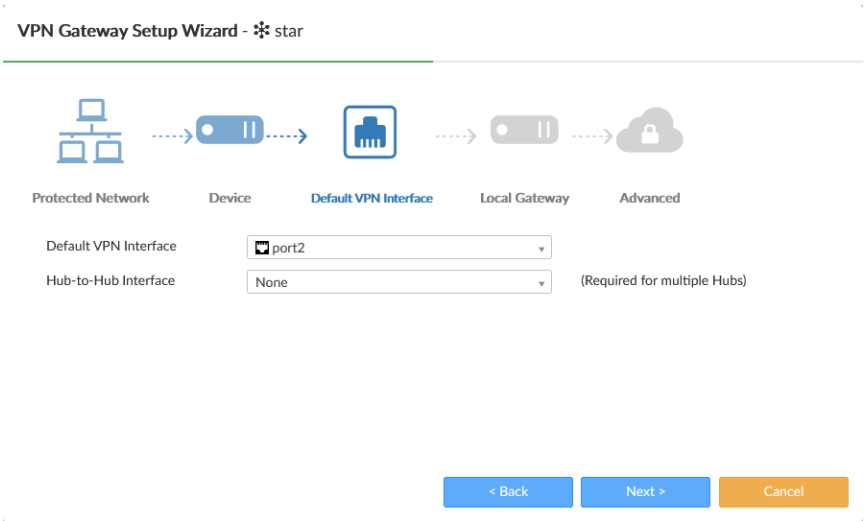
3. Set the *Protected Network* options, and then click *Next*:
   a. Beside *Protected Subnet*, click *Click here to select*, and select the protected subnet.



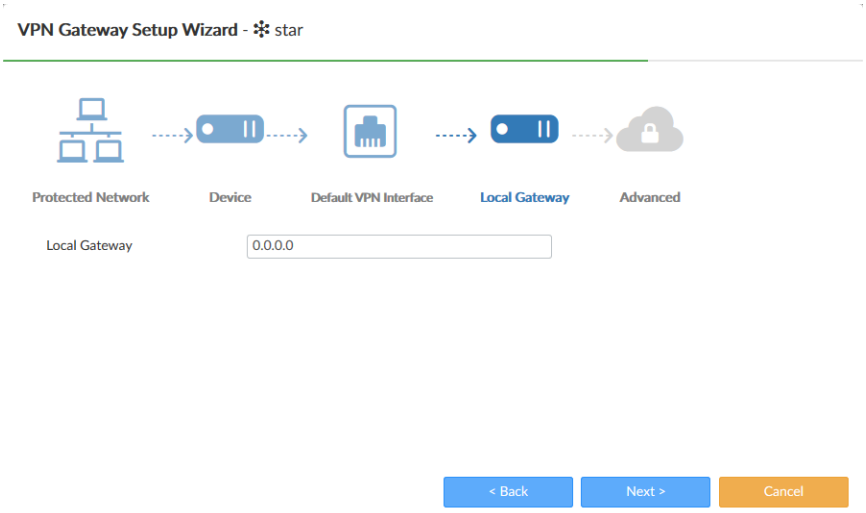
4. Set the *Device* options, and then click *Next*:
   a. Beside *Role*, select *Hub*.
   b. Beside *Device*, select the device for the hub.



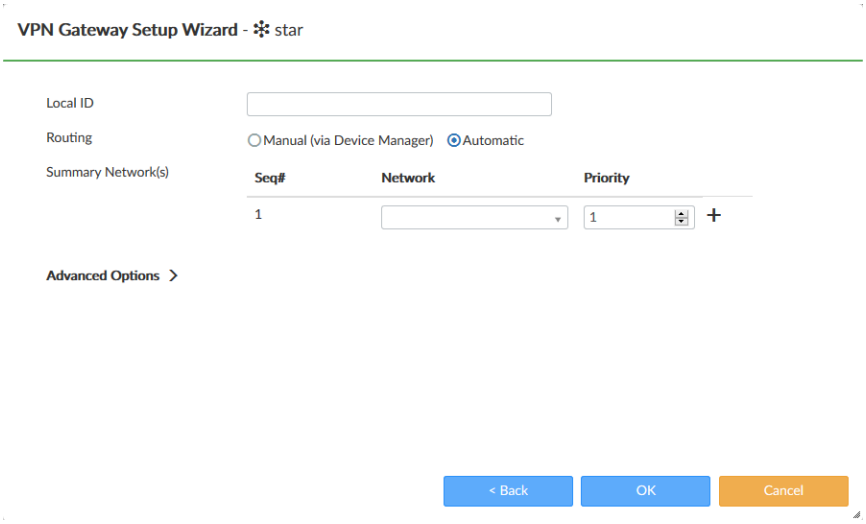
5. Set the *Default VPN Interface* options, and click *Next*.
   a. Beside *Default VPN Interface*, select the interface for the hub, which is often the internet-facing interface.



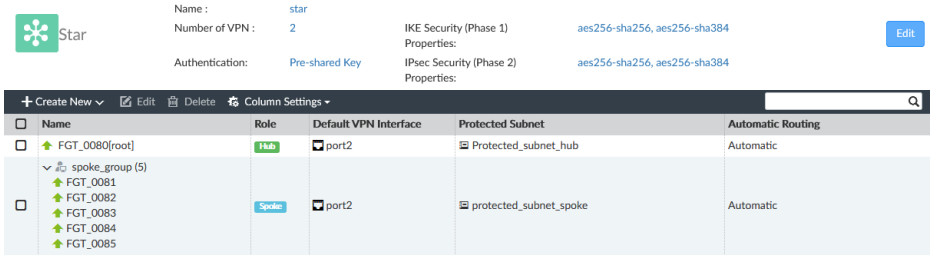
6. Set the *Local Gateway* options, and click *Next*.
   a. Beside *Local Gateway*, type the IP address for the gateway.



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



The hub and spoke are created.

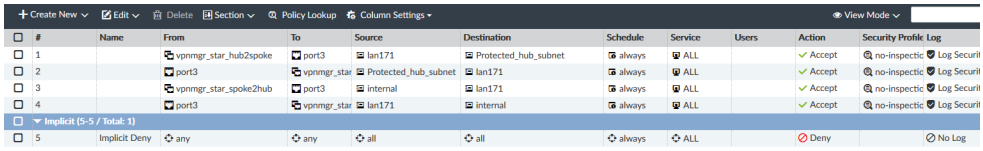


Installing firewall policies to hub and spoke devices

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

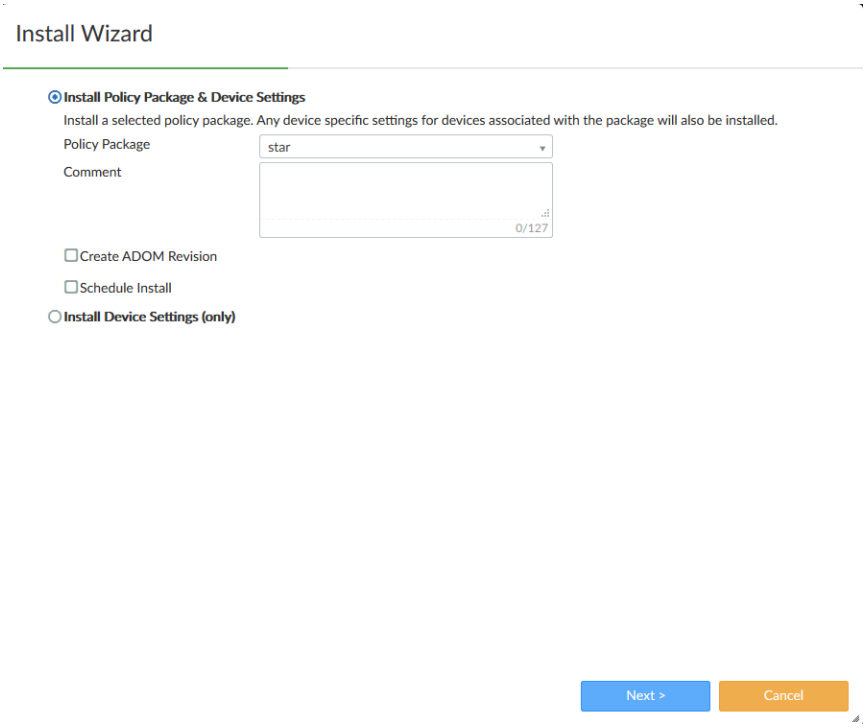
To install configurations to hub and spoke devices:

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



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

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



5. Complete the wizard to install the configurations.

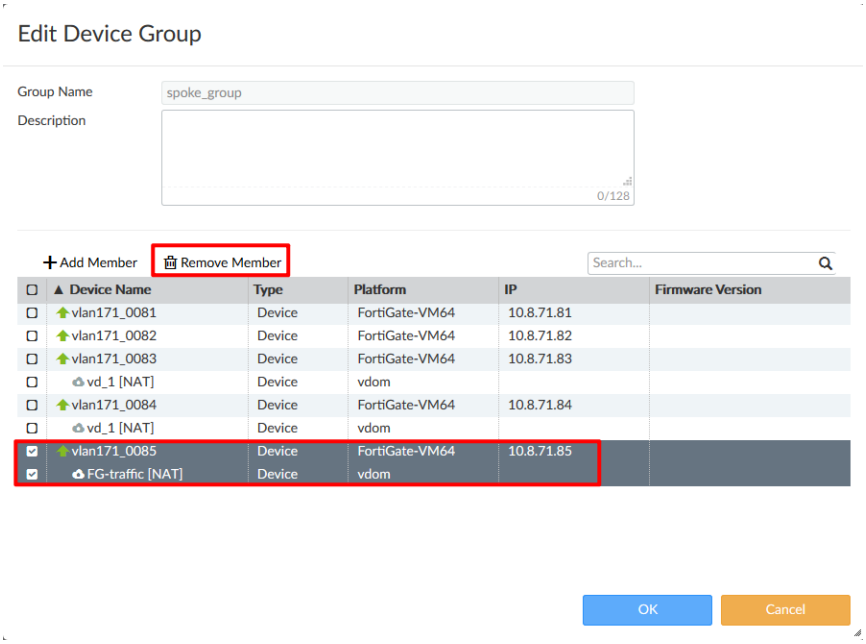
Removing a spoke member from a VPN community

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:

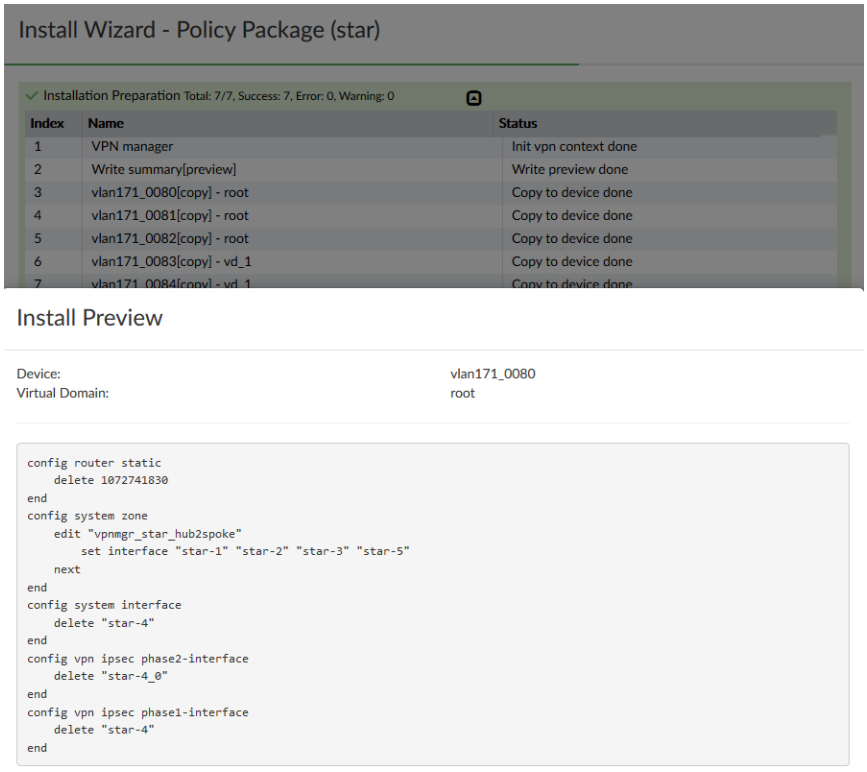
1. Remove the device from the device group:
   a. Go to *Device Manager* > *Device & Groups*.
   b. In the tree menu, right-click the group name, and select *Edit Group*.
      The *Edit Device Group* dialog box opens.

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

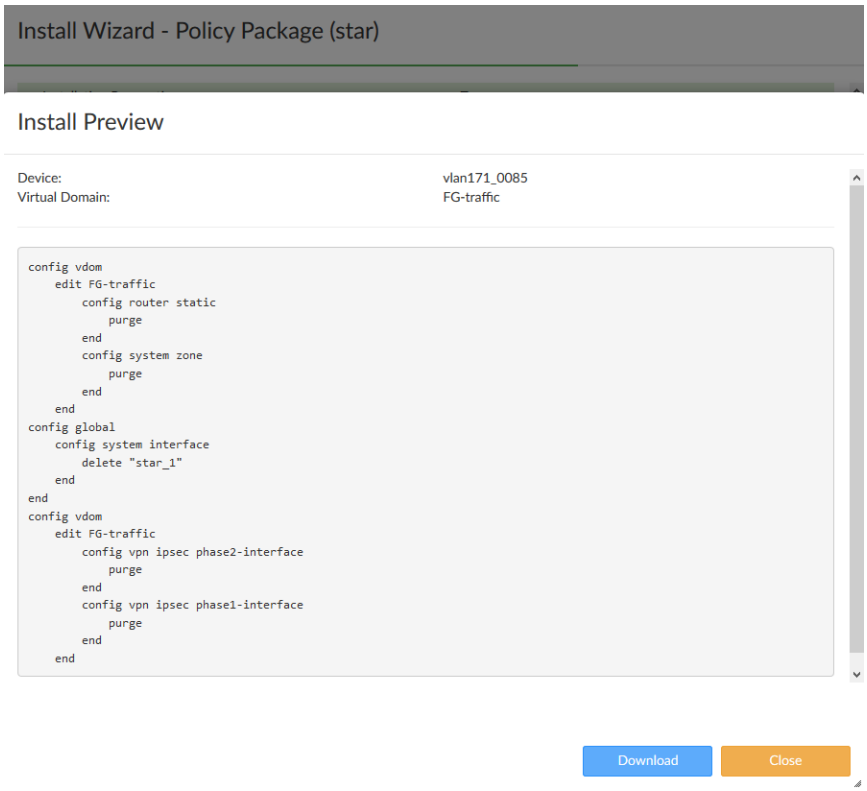


d. Click *OK* to save the changes.

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.



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

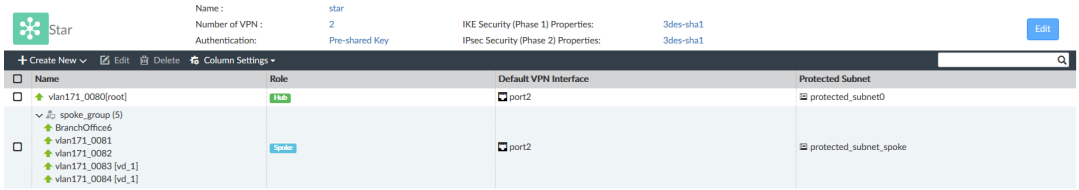


Adding a spoke member to a VPN community

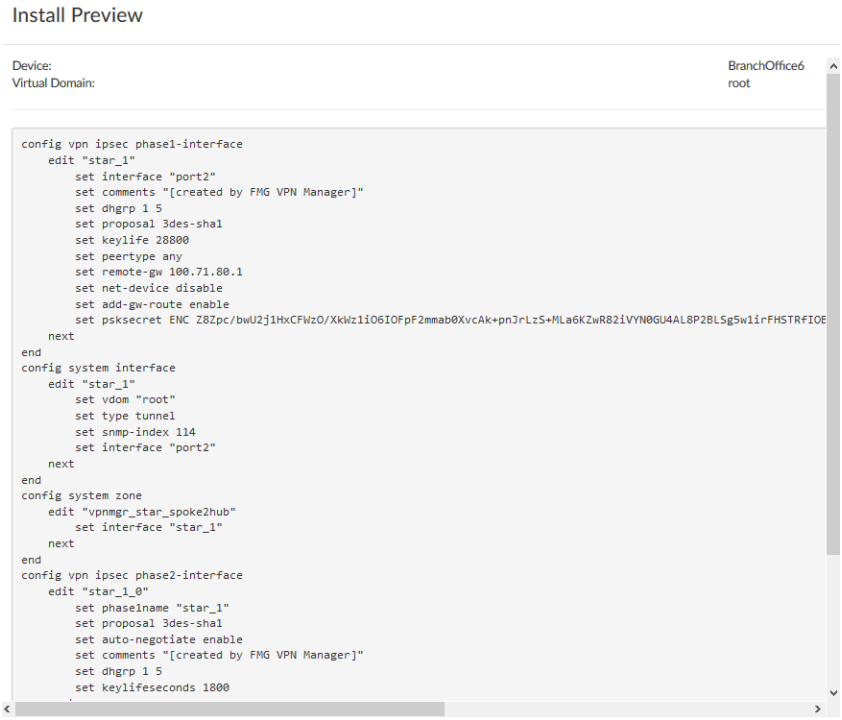
You can add a spoke member to a VPN community by adding the device to the device group, and then installing the configuration change to the FortiGates.

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*.



IPsec VPN

IPsec VPN includes the following topics:

- IPsec VPN Communities on page 666
- IPsec VPN gateways on page 676
- Using Map View on page 683
- Monitoring IPsec VPN tunnels on page 684

IPsec VPN Communities

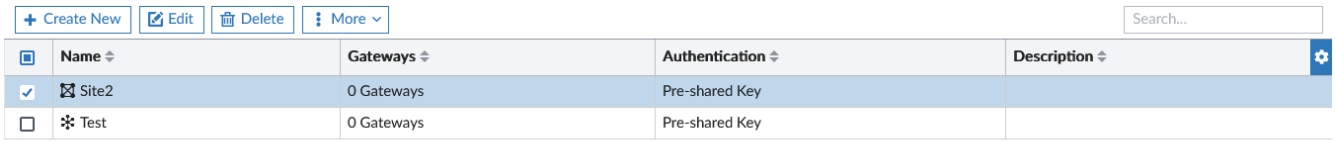
In the *VPN Management > IPsec VPN Communities* pane, you can create and monitor full-meshed, star, and dial-up IPsec VPN communities. IPsec VPN communities are also sometimes called VPN topologies.

Select *All Communities* from the dropdown in the toolbar to view the community list or select a specific community for the details page for that community.



Managing IPsec VPN communities

Go to *VPN Manager > IPsec VPN > VPN Communities*.



The following options are available:

Install Wizard	Launch the Install Wizard to install IPsec VPN settings to devices.
Create New	Create a new VPN community. See Creating IPsec VPN communities on page 667
Edit	Edit the selected VPN community. See Editing an IPsec VPN community on page 675.
Clone	Clone the selected VPN community.
Delete	Delete the selected VPN community or communities. See Deleting VPN communities on page 675.
Column Settings	Configure which columns are displayed, or click *Reset to Default* to reset the display to the default columns.
Search	Enter a search term to search the communities list.
Configure Gateways	Go to the gateway list for the community. This option is only available from the right-click menu. See IPsec VPN gateways on page 676.
Add Managed Gateway	Start the *VPN Gateway Setup Wizard*. This option is only available from the right-click menu. See Creating managed gateways on page 676.

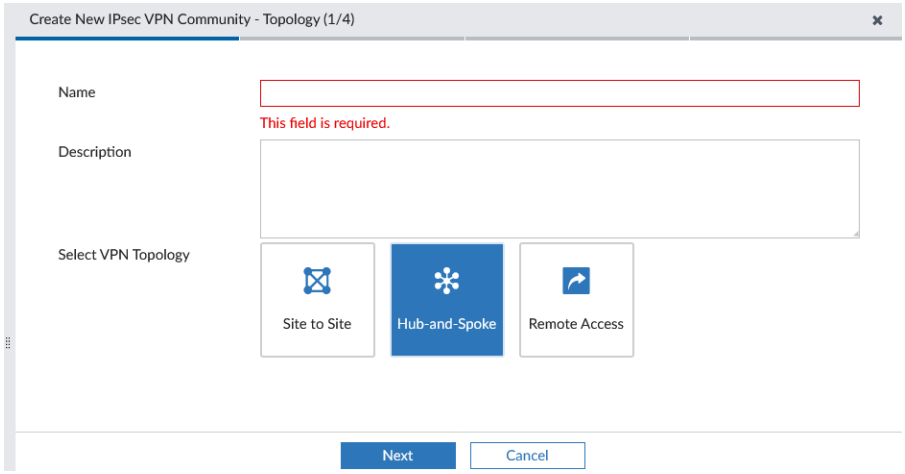
Creating IPsec VPN communities

You can create one or more IPsec VPN communities. An IPsec VPN community is also sometimes called a VPN topology. A *VPN Topology Setup Wizard* is available to help you set up topologies.

After you create the IPsec VPN community, you can create the VPN gateway. See IPsec VPN gateways on page 676.

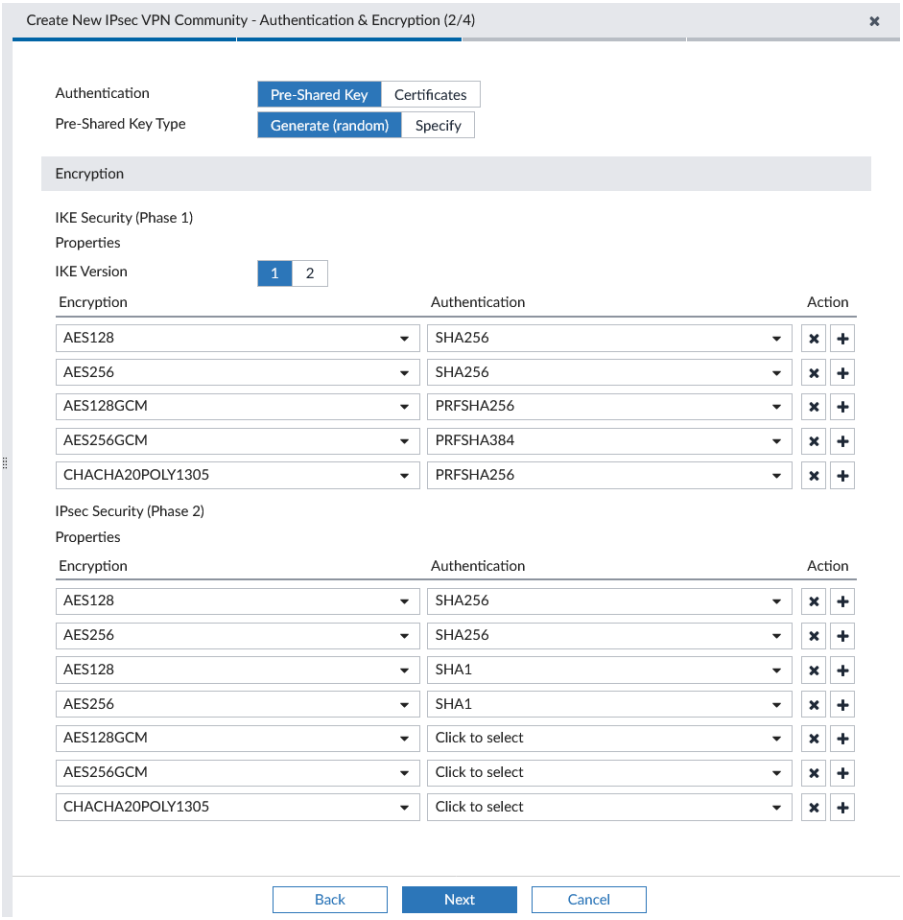
To create a new IPsec VPN community:

1. Go to *VPN Manager > IPsec VPN Communities* and click the *All Communities*.
2. Click *Create New* in the content pane toolbar.
   The *VPN Topology Setup Wizard* is displayed.



3. Enter a name for the topology in the *Name* field.
4. Optionally, enter a brief description of the topology in the *Description* field.
5. Choose a topology type: *Full Meshed*, *Star*, or *Dial up*.
   - *Full Meshed*: Each gateway has a tunnel to every other gateway.
   - *Star*: Each gateway has one tunnel to a central hub gateway.
   - *Dial up*: Some gateways, often mobile users, have dynamic IP addresses and contact the gateway to establish a tunnel.

6. Click *Next*.



7. Configure the *Authentication* and *Encryption* information for the topology
8. Click *Next*.
9. Configure the *VPN Zone*, *IKE Security Phase 1 Advanced Properties*, *IPsec Security Phase 2 Advanced Properties*, and *Advanced Options*.
10. Click *Next*.
11. Review the topology information on the *Summary* page, then click *OK* to create the topology.
    After you have created the VPN topology, you can create managed and external gateways for the topology.



For descriptions of the options in the wizard, see VPN community settings on page 669.

VPN community settings

The following table describes the options available in the *VPN Topology Setup Wizard* and on the *Edit VPN Community* page.

Name	Type a name for the VPN topology.

Description	Type an optional description.
Choose VPN Topology	Choose a topology type. Select one of: • *Full Meshed*: Each gateway has a tunnel to every other gateway. • *Star*: Each gateway has one tunnel to a central hub gateway. • *Dial up*: Some gateways, often mobile users, have dynamic IP addresses and contact the gateway to establish a tunnel.
Authentication	Select *Certificates* or *Pre-shared Key*. When you select *Pre-shared Key*, FortiGate implements the Encapsulated Security Payload (ESP) protocol. Internet Key Exchange (IKE) is performed automatically based on pre-shared keys or X.509 digital certificates.
Certificates	If you selected *Certificates*, select a certificate template. Fortinet provides several default certificate templates. You can also create certificate templates on the *Device Manager* > *Provisioning Templates* > *Certificate Templates* pane.
Pre-shared Key	If you selected *Pre-shared Key*, select *Generate* or *Specify*. When you select *Specify*, type the pre-shared key that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. You must define the same key at the remote peer or client. The key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters. Alternatively, you can select to generate a random pre-shared key.
Encryption	Define the IKE Profile. Configure IKE Phase 1 and IKE Phase 2 settings.
IKE Security (Phase 1) Properties	Define the Phase 1 proposal settings.
IKE Version	Select IKE version 1 or 2 (default = 2). For more information about IKE v2, refer to RFC 4306.
Encryption Authentication	Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select at least one combination. The remote peer or client must be configured to use at least one of the proposals that you define. Select one of the following symmetric-key encryption algorithms: • 3DES: Triple-DES, in which plain text is encrypted three times by three keys. • AES128: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key. • AES128GCM: AES128 Galois/Counter Mode (GCM).

	• AES192: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key. • AES256: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key. • AES256GCM • ARIA128: A 128-bit block size that uses a 128-bit key. • ARIA192: A 128-bit block size that uses a 192- bit key. • ARIA256: A 128-bit block size that uses a 256-bit key. • CHACHA20POLY1305: Arbitrary length, 96-bit nonce, and 256-bit key. • DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • SEED: A 16-round Feistel network with 128-bit blocks and a 128-bit key. Select either of the following authentication message digests to check the authenticity of messages during phase 1 negotiations: • MD5: Message Digest 5, the hash algorithm developed by RSA Data Security. • SHA1: Secure Hash Algorithm 1, which produces a 160-bit message digest. • SHA256: Secure Hash Algorithm 2, which produces a 256-bit message digest. • SHA384: Secure Hash Algorithm 3, which produces a 384-bit message digest. • SHA512: Secure Hash Algorithm 3, which produces a 512-bit message digest. Note: If the encryption is GCM or CHACHA20POLY1305, the authentication options are PRFSHA1, PRFSHA256, PRFSHA384, and PRFSHA512. To specify more combinations, use the *Add* button beside any of the table rows.
Network Overlay	When network overlay is enabled, FOS allows the creation of VPN IPsec Phase 1 interfaces with the same remote gateway and interface. You can specify the VPN gateway network ID in the *Network Overlay ID* field. This setting is only available if the IKE version is set to 2.
IPsec Security (Phase 2) Properties	Define the Phase 2 proposal settings. When you define phase 2 parameters, you can choose any set of phase 1 parameters to set up a secure connection for the tunnel and authenticate the remote peer. Auto Key configuration applies to both tunnel-mode and interface-mode VPNs.
Encryption Authentication	Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required.

	You need to select at least one combination. The remote peer or client must be configured to use at least one of the proposals that you define. It is invalid to set both Encryption and Authentication to NULL. Select one of the following symmetric-key encryption algorithms: • 3DES: Triple-DES, in which plain text is encrypted three times by three keys. • AES128: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key. • AES128GCM: AES128 Galois/Counter Mode (GCM). • AES192: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key. • AES256: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key. • AES256GCM • ARIA128: A 128-bit block size that uses a 128-bit key. • ARIA192: A 128-bit block size that uses a 192- bit key. • ARIA256: A 128-bit block size that uses a 256-bit key. • CHACHA20POLY1305: Arbitrary length, 96-bit nonce, and 256-bit key. • DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • NULL: Do not use an encryption algorithm. • SEED: A 16-round Feistel network with 128-bit blocks and a 128-bit key. Select either of the following authentication message digests to check the authenticity of messages during phase 1 negotiations: • NULL: Do not use a message digest. • MD5: Message Digest 5, the hash algorithm developed by RSA Data Security. • SHA1: Secure Hash Algorithm 1, which produces a 160-bit message digest. • SHA256: Secure Hash Algorithm 2, which produces a 256-bit message digest. • SHA384: Secure Hash Algorithm 3, which produces a 384-bit message digest. • SHA512: Secure Hash Algorithm 3, which produces a 512-bit message digest. Note: If the encryption is GCM or CHACHA20POLY1305, no authentication options can be selected. To specify more combinations, use the Add button beside any of the table rows.
VPN Zone	Select to create VPN zones. When enabled, you can select to create default or custom zones. When disabled, no VPN zones are created.
Create Default Zones	Select to have default zones created for you.

Use Custom Zone	Select to choose what zones to create.
IKE Security Phase 1 Advanced Properties	
Diffie Hellman Group(s)	Select one or more of the following Diffie-Hellman (DH) groups: *1*, *2*, *5*, *14*, *15*, *16*, *17*, *18*, *19*, *20*, *21*, *27*, *28*, *29*, *30*, *31*. At least one of the DH group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations. Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode.
Exchange Mode	Select either *Aggressive* or *Main (ID Protection)*. The FortiGate unit and the remote peer or dialup client exchange phase 1 parameters in either *Main (ID Protection)* or *Aggressive* mode. This choice does not apply if you use IKE version 2, which is available only for route-based configurations. • In Main mode, the Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information • In Aggressive mode, the Phase 1 parameters are exchanged in single message with authentication information that is not encrypted. Although Main mode is more secure, you must select Aggressive mode if there is more than one dialup Phase 1 configuration for the interface IP address, and the remote VPN peer or client is authenticated using an identifier local ID). Descriptions of the peer options in this guide indicate whether Main or Aggressive mode is required.
Key Life	Type the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The keylife can be from 120 to 172800 seconds.
Dead Peer Detection	Select this checkbox to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required. You can use this option to receive notification whenever a tunnel goes up or down, or to keep the tunnel connection open when no traffic is being generated inside the tunnel. For example, in scenarios where a dialup client or dynamic DNS peer connects from an IP address that changes periodically, traffic may be suspended while the IP address changes.
IPsec Security Phase 2 Advanced Properties	
Diffie Hellman Group(s)	Select one or more of the following Diffie-Hellman (DH) groups: *1*, *2*, *5*, *14*, *15*, *16*, *17*, *18*, *19*, *20*, *21*, *27*, *28*, *29*, *30*, *31*. At least one of the DH group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations.

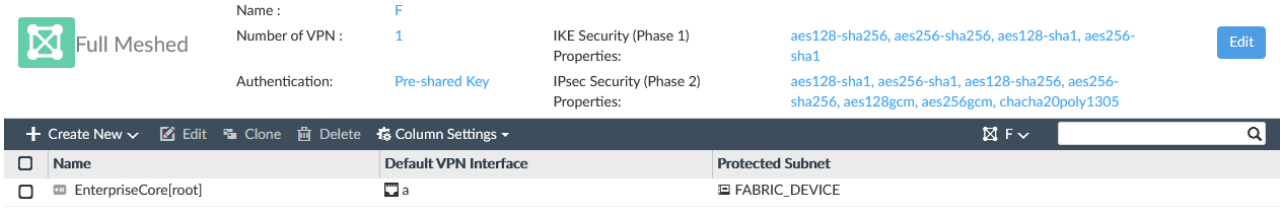
		Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode.
	Replay detection	Select to enable or disable replay detection. Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel.
	Perfect forward secrecy (PFS)	Select to enable or disable perfect forward secrecy (PFS). Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.
	Key Life	Select the PFS key life. Select *Second*, *Kbytes*, or *Both* from the dropdown list and type the value in the text field.
	Autokey Keep Alive	Select to enable or disable autokey keep alive. The phase 2 SA has a fixed duration. If there is traffic on the VPN as the SA nears expiry, a new SA is negotiated and the VPN switches to the new SA without interruption. If there is no traffic, the SA expires and the VPN tunnel goes down. A new SA will not be generated until there is traffic. The Autokey Keep Alive option ensures that a new SA is negotiated even if there is no traffic so that the VPN tunnel stays up.
	Auto-Negotiate	Select to enable or disable auto-negotiation.
NAT Traversal		Select the checkbox if a NAT device exists between the local FortiGate unit and the VPN peer or client. The local FortiGate unit and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared) to connect reliably.
Keep-alive Frequency		If NAT traversal is enabled or forced, type a keep-alive frequency setting (10-900 seconds).
Advanced-Options		For more information on advanced options, see the *FortiOS CLI Reference*.
fcc-enforcement		Enable or disable FCC enforcement.
inter-vdom		Enable or disable the inter-vdom setting.
loccalid-type		Select the local ID type from the dropdown list. Select one of: • *address*: IP Address • *asn1dn*: ASN.1 Distinguished Name • *auto*: Select type automatically • *fqdn*: Fully Qualified Domain name • *keyid*: Key Identifier ID • *user-fqdn*: User Fully Qualified Domain Name
negotiate-timeout		Enter the negotiation timeout value. The default is 30 seconds.
npu-offload		Enable (default) or disable offloading of VPN session to a network processing unit (NPU).

View IPsec VPN community details

The VPN community information pane includes a quick status bar showing the community settings and the list of gateways in the community. Gateways can also be managed from this pane. See IPsec VPN gateways on page 676 for information.

To view IPsec VPN community details:

1. Go to *VPN Manager > IPsec VPN Communities* and select a community.
   The community information pane opens.



2. Select *All Communities* from the dropdown to return to the VPN community list.

Editing an IPsec VPN community

To edit a VPN community, you must be logged in as an administrator with sufficient privileges. The community name and topology cannot be edited.

To edit IPsec VPN communities:

1. Go to *VPN Manager > IPsec VPN Communities*.
2. Do one of the following
   - Right-click on a community, and select *Edit* from the menu.
   - Select a community, and click *Edit* in the toolbar.

   The *Edit IPsec VPN Community* page is displayed.
3. Edit the settings as required, and then select *OK* to apply the changes.



For descriptions of the settings, see VPN community settings on page 669.

Deleting VPN communities

To delete a VPN community or communities, you must be logged in as an administrator with sufficient privileges.

To delete VPN communities:

1. Go to *VPN Manager > IPsec VPN Communities*.
2. Do one of the following:
   - Select a community then click *Delete* from the menu.
   - Right-click on a community then click *Delete* in the toolbar.
3. Select *OK* in the confirmation box to delete the VPN community or communities.

IPsec VPN gateways

A VPN gateway functions as one end of a VPN tunnel. It receives incoming IPsec packets, decrypts the encapsulated data packets, then passes the data packets to the local network. It also encrypts, encapsulates, and sends the IPsec data packets to the gateway at the other end of the VPN tunnel.

The IP address of a VPN gateway is usually the IP address of the network interface that connects to the Internet. You can also define a secondary IP address for the interface, and use that address as the local VPN gateway address, so that your existing setup is not affected by the VPN settings.

Once you have created the IPsec VPN topology, you can create managed and external gateways.

Managing VPN gateways

Go to *VPN Manager > IPsec VPN Communities*, then right-click a community to configure or add managed gateways for the selected community.

When *Configure Gateways* is selected for a community from the right-click menu, the following options are available.

Create New	Create a new managed or external gateway. See Creating managed gateways on page 676 and Creating external gateways on page 681 for more information.
Edit	Edit the selected gateway. See Editing an IPsec VPN gateway on page 682.
Delete	Delete the selected gateway or gateways. See Deleting VPN gateways on page 682.
Column Settings	Configure which columns are displayed, or click *Reset to Default* to reset the display to the default columns.
Search	Enter a search term to search the gateway list.
More	Select *More > Clone* to clone a gateway.

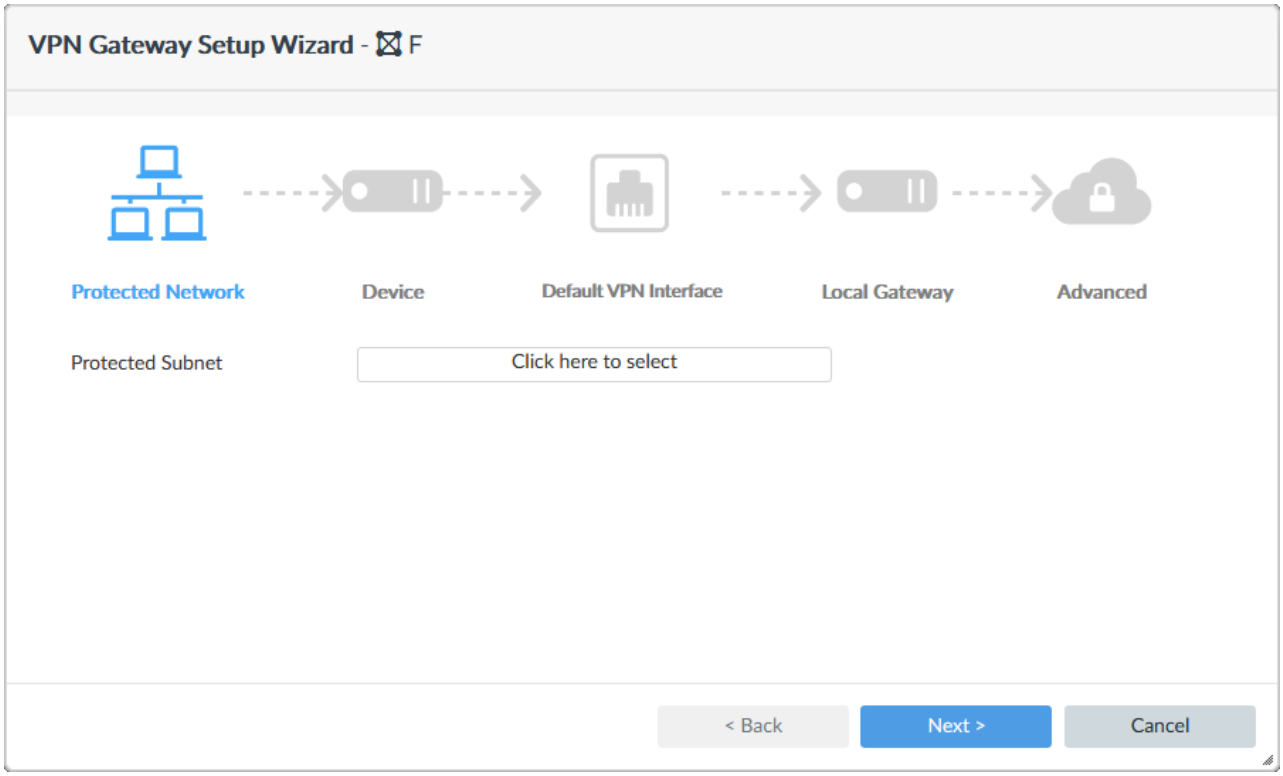
Creating managed gateways

The settings available when creating a managed gateway depend on the VPN topology type, and how the gateway is configured.

Managed gateways are managed by FortiManager in the current ADOM. Devices in a different ADOM can be treated as external gateways. VPN configuration must be handled manually by the administrator in that ADOM. See Creating external gateways on page 681.

To create a managed gateway:

1. Go to *VPN Manager > IPsec VPN Communities*.
2. Right-click a community, and click *Add Managed Gateway*.
   The *VPN Gateway Setup Wizard* opens.



3. Proceed through the five pages of the wizard, filling in the following values as required, then click *OK* to create the managed gateway.

Protected Subnet	Select a protected subnet from the drop-down list.
Role	Select the role of this gateway: *Hub* or *Spoke*. This option is only available for star and dial up VPN topologies.
Device	Select a *Device* or *Device Group* from the drop-down list.
Default VPN Interface	Select the interface to use for this gateway from the drop-down list.
Hub-to-Hub Interface	Select the interface to use for hub to hub communication. This is required if there are multiple hubs. This option is only available for star and dial up topologies with the role set to *Hub*.
Local Gateway	Enter the local gateway IP address.

Local ID	Enter a local ID.
Routing	Select the routing method: *Manual (via Device Manager)*, or *Automatic*.
Summary Network(s)	Select the network from the dropdown list and select the priority. Click the add icon to add more entries. This option is only available for star and dial up topologies with the role set to *Hub*.
Peer Type	Select one of the following: • *Accept any peer ID* • *Accept this peer ID*: Enter the peer ID in the text field • *Accept a dialup group*: Select a group from the drop-down list • *Accept peer*: Select a peer from the dropdown list • *Accept peer group*: Select a peer group from the drop-down list A Local ID is an alphanumeric value assigned in the Phase 1 configuration. The local ID of a peer is called a Peer ID. The Local ID or peer ID can be used to uniquely identify one end of a VPN tunnel, enabling a more secure connection. If you have multiple VPN tunnels negotiating, this ensures the proper remote and local ends connect. When you configure the ID on your end, it is your local ID. When the remote end connects to you, they see it as your peer ID. If you are debugging a VPN connection, the local ID is part of the VPN negotiations. You can use it to help troubleshoot connection problems. The default configuration is to accept all local IDs (peer IDs). If your local ID is set, the remote end of the tunnel must be configured to accept your ID. This option is only available for dial up topologies.
XAUTH Type	Select the XAUTH type: *Disable*, *PAP Server*, *CHAP Server*, or *AUTO Server*. This option is only available for dial up topologies.
User Group	Select the authentication user group from the dropdown list. This field is available when *XAUTH Type* is set to *PAP Server*, *CHAP Server*, or *AUTO Server*. When the FortiGate unit is configured as an XAuth server, enter the user group to authenticate remote VPN peers. The user group can contain local users, LDAP servers, and RADIUS servers. The user group must be added to the FortiGate configuration before the group name can be cross referenced.
Enable IKE Configuration Method ("mode config")	Select to enable or disable IKE configuration method. This option is only available for dial up topologies.
Enable IP Assignment	Select to enable or disable IP assignment. This option is only available for dial up topologies. When the role is set to *Hub*, this option is only available when *Enable IKE Configuration Method* is on.

	IP Assignment Mode	Select the IP assignment mode: *Range* or *User Group*. This option is only available for dial up topologies with the role set to *Hub* and *Enable IP Assignment* turned on.
	IP Assignment Type	Select the IP assignment type: *IP* or *Subnet*. This option is only available for dial up topologies with the role set to *Hub* and *Enable IP Assignment* turned on.
	IPv4 Start IP	Enter the IPv4 start IP address. This option is only available for dial up topologies with the role set to *Hub* and *Enable IP Assignment* turned on.
	IPv4 End IP	Enter the IPv4 end IP address. This option is only available for dial up topologies with the role set to *Hub* and *Enable IP Assignment* turned on.
	IPv4 Netmask	Enter the IPv4 netmask. This option is only available for dial up topologies with the role set to *Hub* and *Enable IP Assignment* turned on.
Add Route		Select to enable or disable adding a route for this gateway. This option is only available for dial up topologies.
DNS Server #1 to #3		Enter the DNS server IP addresses to provide IKE Configuration Method to clients. This option is only available for dial up topologies with the role set to *Hub* and either *Enable IKE Configuration Method* turned on, or *DNS Service* is set to *Specify*.
WINS Server #1 and #2		Enter the WINS server IP addresses to provide IKE Configuration Method to clients. This option is only available for dial up topologies with the role set to *Hub* and *Enable IKE Configuration Method* turned on.
IPv4 Split include		Select the address or address group from the dropdown list. This option is only available for dial up topologies with the role set to *Hub* and *Enable IKE Configuration Method* turned on.
Exclusive IP Range		Enter the start and end IP addresses of the exclusive IP address range. Click the add icon to add more entries. This option is only available for dial up topologies with the role set to *Hub* and either *Enable IKE Configuration Method* and *Enable IP Assignment* turned on, or *Enable IKE Configuration Method* turned off.
DHCP Server		Select to enable or disable DHCP server. This option is only available for dial up topologies with the role set to *Hub* and *Enable IKE Configuration Method* is off.
Default Gateway		Enter the default gateway IP address. This option is only available for dial up topologies with the role set to *Hub* and *Enable IKE Configuration Method* turned off.

DNS Service	Select *Use System DNS setting* to use the system's DNS settings, or *Specify* to specify DNS servers #1 to #3. This option is only available for dial up topologies with the role set to *Hub* and *Enable IKE Configuration Method* turned off.
Netmask	Enter the netmask. This option is only available for dial up topologies with the role set to *Hub* and *Enable IKE Configuration Method* turned off.
IPsec Lease Hold	Enter the IPsec lease hold time. This option is only available for dial up topologies with the role set to *Hub* and *Enable IKE Configuration Method* turned off.
Auto-Configuration	Select to enable or disable automatic configuration. This option is only available for dial up topologies with the role set to *Hub* and *Enable IKE Configuration Method* turned off.
DHCP Server IP Range	Enter the start and end IP addresses of the DHCP server range. Click the add icon to add more entries. This option is only available for dial up topologies with the role set to *Hub* and *Enable IKE Configuration Method* turned off.
Advanced Options	
authpasswd	Enter the XAuth client password for the FortiGate.
authusr	Enter the XAuth client user name for the FortiGate.
banner	Enter the banner value. Specify the message to send to IKE Configuration Method clients. Some clients display this message to users.
dns-mode	Select the DNS mode from the dropdown list: • *auto*: Assign DNS servers in the following order: **a.** Servers assigned to interfaces by DHCP **b.** Per-VDOM assigned DNS servers **c.** Global DNS servers • *manual*: Use the DNS servers specified in *DNS Server #1 to #3*.
domain	Enter the domain value.
public-ip	Enter the public IP address. Use this field to configure a VPN with dynamic interfaces. The value is the dynamically assigned PPPoE address that remains static and does not change over time.
route-overlap	Select the route overlap method from the dropdown list: *allow*, *use-new*, or *use-old*.
spoke-zone	Select a spoke zone from the dropdown list.
unity-support	Enable or disable unity support.

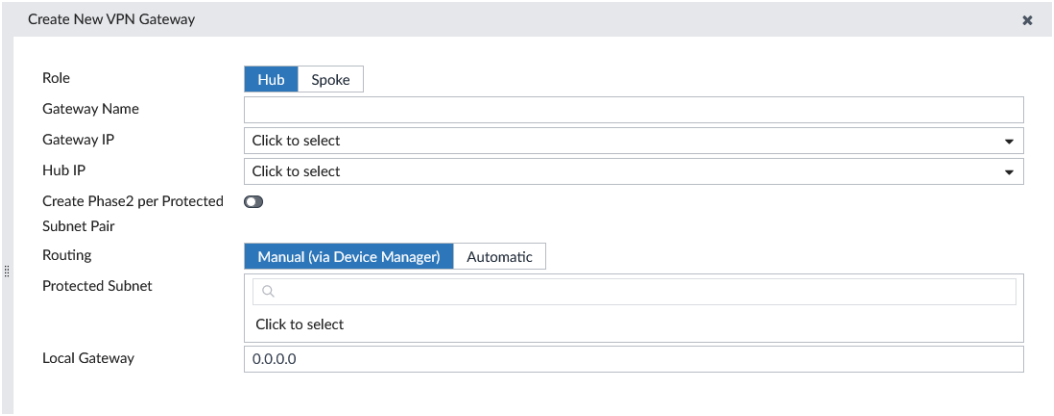
	vpn-interface-priority	Set the VPN gateway interface priority. The default value is 1.
	vpn-zone	Select a VPN zone from the dropdown list.

Creating external gateways

External gateways are not managed by the FortiManager device.

To create an external gateway:

1. Go to *VPN Manager > IPsec VPN Communities*.
2. Right-click a community, and click *Configure Gateways*.
3. Click *Create New > External Gateway*.



4.
5. Configure the following settings, then click *OK* to create the external gateway:

Role	Select either *HUB* or *Spoke*. This option is only available for star and dial up VPN topologies.
Gateway Name	Enter the gateway name.
Gateway IP	Select the gateway IP address from the dropdown list.
Hub IP	Select the hub IP address from the dropdown list. This option is only available for star and dial up topologies with the role set to *Hub*.
Create Phase2 per Protected Subnet Pair	Toggle the switch to *On* to create a phase2 per protected subnet pair.
Routing	Select the routing method: *Manual (via Device Manager*, or *Automatic*. This option is only available for full meshed and star topologies.
Peer Type	Select one of the following: • *Accept any peer ID* • *Accept this peer ID*: Enter the peer ID in the text field • *Accept a dialup group*: Select a group from the dropdown list

	A Local ID is an alphanumeric value assigned in the Phase 1 configuration. The local ID of a peer is called a Peer ID. The Local ID or peer ID can be used to uniquely identify one end of a VPN tunnel, enabling a more secure connection. If you have multiple VPN tunnels negotiating, this ensures the proper remote and local ends connect. When you configure the ID on your end, it is your local ID. When the remote end connects to you, they see it as your peer ID. If you are debugging a VPN connection, the local ID is part of the VPN negotiations. You can use it to help troubleshoot connection problems. The default configuration is to accept all local IDs (peer IDs). If your local ID is set, the remote end of the tunnel must be configured to accept your ID. This option is only available for dial up topologies.
Protected Subnet	Select a protected subnet from the list. You can add multiple subnets.
Local Gateway	Enter the local gateway IP address.

Editing an IPsec VPN gateway

To edit a VPN gateway, you must be logged in as an administrator with sufficient privileges. The gateway role and device (if applicable) cannot be edited.

To edit IPsec VPN communities:

1. Go to *VPN Manager > IPsec VPN Communities*.
2. Right-click on a community, and click *Configure Gateways*.
3. Select *Edit* from the menu, or select the gateway then click *Edit* in the toolbar. The *Edit VPN Gateway* pane opens.
4. Edit the settings as required, and then select *OK* to apply the changes.

Deleting VPN gateways

To delete a VPN gateway or gateways, you must be logged in as an administrator with sufficient privileges.

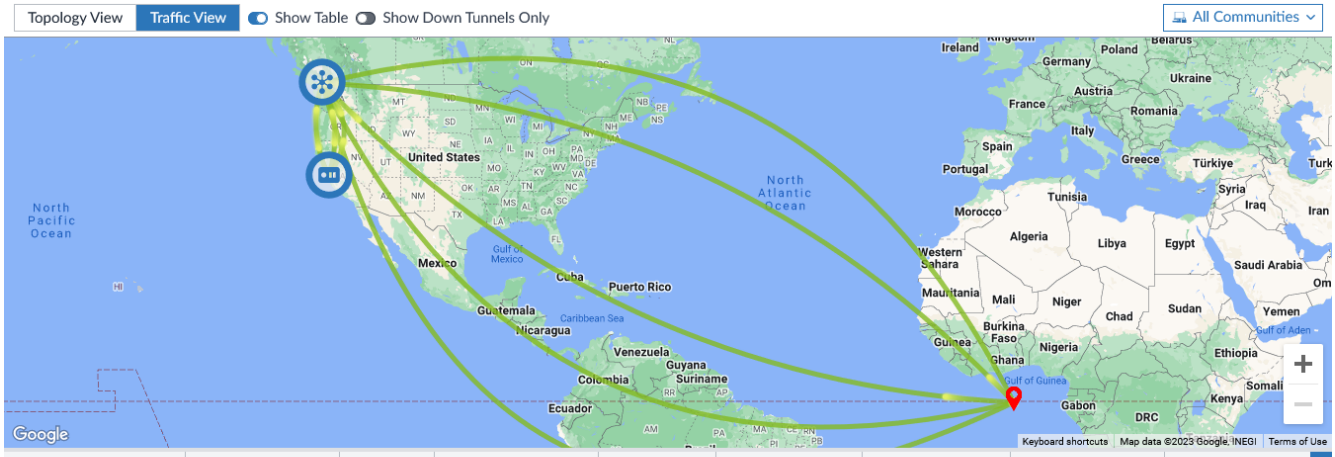
To delete VPN gateways:

1. Go to *VPN Manager > IPsec VPN Communities*.
2. Right-click on a community, and click *Configure Gateways*.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the gateway or gateways.

Using Map View

The *IPsec VPN Map* pane shows IPsec VPN connections on an interactive world map (Google Maps). Select a specific community from the tree menu to show only that community's tunnels.

Hovering the cursor over a connection will highlight the connection and show the gateway, ADOM, and city names for each end of the tunnel.



Device	Name	Type	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Branch_Office_01[root]	To-HQ-A	automatic	10.100.64.101		809.0 MB	116.4 MB	To-HQ-A	To-HQ-A
Branch_Office_01[root]	To-HQ-B	automatic	10.100.65.101		74.1 MB	245.0 MB	To-HQ-B	To-HQ-B
Branch_Office_01[root]	To-HQ-MPLS	automatic	192.168.0.1		60.8 MB	70.5 MB	To-HQ-MPLS	To-HQ-MPLS
fduncan-tech72[root]	Branch-HQ-A_0	dialup	10.100.67.5	10.100.67.5	116.4 MB	809.0 MB	Branch-HQ-A_0	Branch-HQ-A
fduncan-tech72[root]	Branch-HQ-A_1	dialup	10.100.68.5	10.100.68.5	107.0 MB	726.3 MB	Branch-HQ-A_1	Branch-HQ-A
fduncan-tech72[root]	Branch-HQ-B_0	dialup	10.100.67.13	10.100.67.13	245.0 MB	74.1 MB	Branch-HQ-B_0	Branch-HQ-B
fduncan-tech72[root]	Branch-HQ-B_1	dialup	10.100.68.13	10.100.68.13	51.9 MB	46.3 MB	Branch-HQ-B_1	Branch-HQ-B
fduncan-tech72[root]	HQ-MPLS_0	dialup	192.168.0.14	192.168.0.14	70.5 MB	60.8 MB	HQ-MPLS_0	HQ-MPLS
fduncan-tech72[root]	HQ-MPLS_1	dialup	192.168.1.14	192.168.1.14	221.3 MB	82.3 MB	HQ-MPLS_1	HQ-MPLS

The following options are available:

Topology View	The topology view shows the configured VPN gateways. See IPsec VPN gateways on page 676.
Traffic View	The traffic view shows network traffic through the tunnels between protected subnets.
Show Table	Select to show the connection table on the bottom of the pane. In the topology view, this option is only available when a specific community is selected. • The topology table shows the VPN gateway list and toolbar, with a column added for location. See Managing VPN gateways on page 676 for information. • The traffic table shows the same information and options as the *Monitor* tab. See Monitoring IPsec VPN tunnels on page 684 for information.

	 You can filter the VPN monitor table view. For example, you can use the greater than (>) or less than (<) signs on the incoming/outgoing bandwidth columns.
Show Tunnel Down Only	Select to show only tunnels that are currently down. This option is only available on the traffic view.
Refresh	Click to refresh the map view, or click the down arrow and select a refresh rate from the dropdown menu.



If necessary, the location of a device can be manually configured when editing the device; see Editing device information on page 153.

Monitoring IPsec VPN tunnels

Go to *VPN Manager > IPsec VPN Communities*, right-click a community and click *Monitor*.

To bring tunnels up or down:

1. Go to *VPN Manager > IPsec VPN Communities*.
2. Right-click on a community and select *Monitor*.
3. Find and select the tunnel or tunnels that you need to bring up or down in the list.
4. Click *Bring Tunnel Up* or *Bring Tunnel Down* from the toolbar or right-click menu
5. Select *OK* in the confirmation dialog box to apply the change.

SSL VPN

You can use the *VPN Manager > SSL-VPN* pane to create and monitor Secure Sockets Layer (SSL) VPNs. You can also create and manage SSL VPN portal profiles.

SSL VPN includes the following topics:

- SSL VPN settings on page 685
- SSL VPN portals on page 687
- SSL VPN monitor on page 694

SSL VPN settings

Go to *VPN Manager > SSL VPN Settings* to manage SSL VPN settings.

The following options are available:

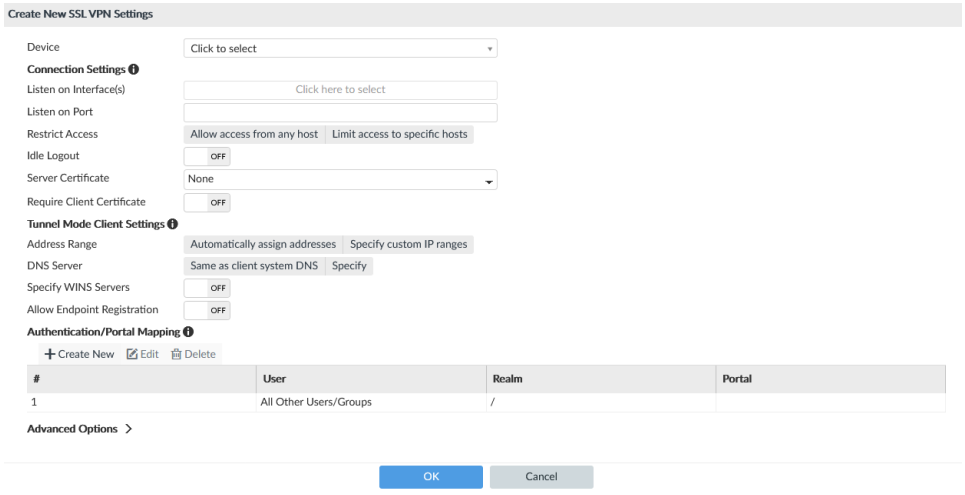
Install Wizard	Launch the *Install Wizard* to install SSL VPN settings to devices.
Create New	Create a new SSL VPN with the *Create SSL VPN Settings* pane. See Creating SSL VPNs on page 685.
Edit	Edit the selected VPN. This option is also available from the right-click menu. See Editing SSL VPNs on page 687.
Delete	Delete the selected VPN or VPNs. This option is also available from the right-click menu. See Deleting SSL VPNs on page 687.
Column Settings	Configure which columns are displayed, or click *Reset to Default* to reset the display to the default columns.
Search	Enter a search term to search the VPN list.

Creating SSL VPNs

To create SSL VPNs, you must be logged in as an administrator with sufficient privileges. Multiple VPNs can be created.

To add SSL-VPN:

1. Go to *VPN Manager > SSL-VPN Settings*.
2. Click *Create New* in the content toolbar. The *Create SSL VPN Settings* pane is displayed.



3. Configure the following settings, then click *OK* to create the VPN.

Device	Select a FortiGate device or VDOM.

Connection Settings		Specify the connection settings.
	Listen on Interface(s)	Define the interface the FortiGate will use to listen for SSL VPN tunnel requests. This is generally your external interface.
	Listen on Port	Enter the port number for HTTPS access.
	Restrict Access	Allow access from any hosts, or limit access to specific hosts. If limiting access, select the hosts that have access in the *Hosts* field.
	Idle Logout	Select to enable idle timeout. When enabled, enter the amount of time that the connection can remain inactive before timing out in the*Inactive For* field, in seconds(10 - 28800, default = 300). This setting applies to the SSL VPN session. The interface does not time out when web application sessions or tunnels are up.
	Server Certificate	Select the signed server certificate to use for authentication. Alternately, select a certificate template that is configured to use the FortiManager CA. See Certificate templates on page 354.
	Require Client Certificate	Select to use group certificates for authenticating remote clients. When the remote client initiates a connection, the FortiGate unit prompts the client for its client-side certificate as part of the authentication process. For information on using PKI to provide client certificate authentication, see the Authentication Guide.
Tunnel Mode Client Settings		Specify tunnel mode client settings. These settings determine how tunnel mode clients are assigned IP addresses.
	Address Range	Either automatically assign address, or specify custom IP ranges.
	DNS Server	Select to use the same DNS as the client system, or to specify DNS servers. Enter up to two DNS servers to be provided for the use of clients.
	Specify WINS Servers	Select to specify WINS servers. Enter up to two WINS servers to be provided for the use of clients.
	Allow Endpoint Registration	Select to allow endpoint registration.
Authentication/Portal Mapping		Select the users and groups that can access the tunnel. **Note**: the default portal cannot be empty.
	Create New	Create a new authentication/portal mapping entry. Select the *Users*, *Groups*, *Realm*, and *Portal*, then click *OK*.
	Edit	Edit the selected mapping.
	Delete	Delete the selected mapping or mappings.
Advanced Options		Configure advanced SSL VPN options. For information, see the *FortiOS CLI Reference*.

Editing SSL VPNs

To edit an SSL VPN, you must be logged in as an administrator with sufficient privileges. The device cannot be edited.

To edit an SSL VPN:

1. Go to *VPN Manager > SSL-VPN Settings*.
2. Double-click on a VPN, right-click on a VPN and then select *Edit* from the menu, or select the VPN then click *Edit* in the toolbar. The *Edit SSL VPN Settings* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

Deleting SSL VPNs

To delete an SSL VPN or VPNs, you must be logged in as an administrator with sufficient privileges.

To delete SSL VPNs:

1. Go to *VPN Manager > SSL-VPN Settings*.
2. Select the VPN or VPNs you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the selected VPN or VPNs.

SSL VPN portals

The SSL VPN portal enables remote users to access internal network resources through a secure channel using a web browser. FortiGate administrators can configure login privileges for system users as well as the network resources that are available to the users.

There are three pre-defined default portal profiles:

- Full-access
- Tunnel-access
- Web-access

Each portal type includes similar configuration options. You can also create custom portal profiles.

To manage portal profiles, go to *VPN Manager > SSL VPN Portals*.



The following options are available:

Create New	Create a new portal profile.
Edit	Edit the selected profile.

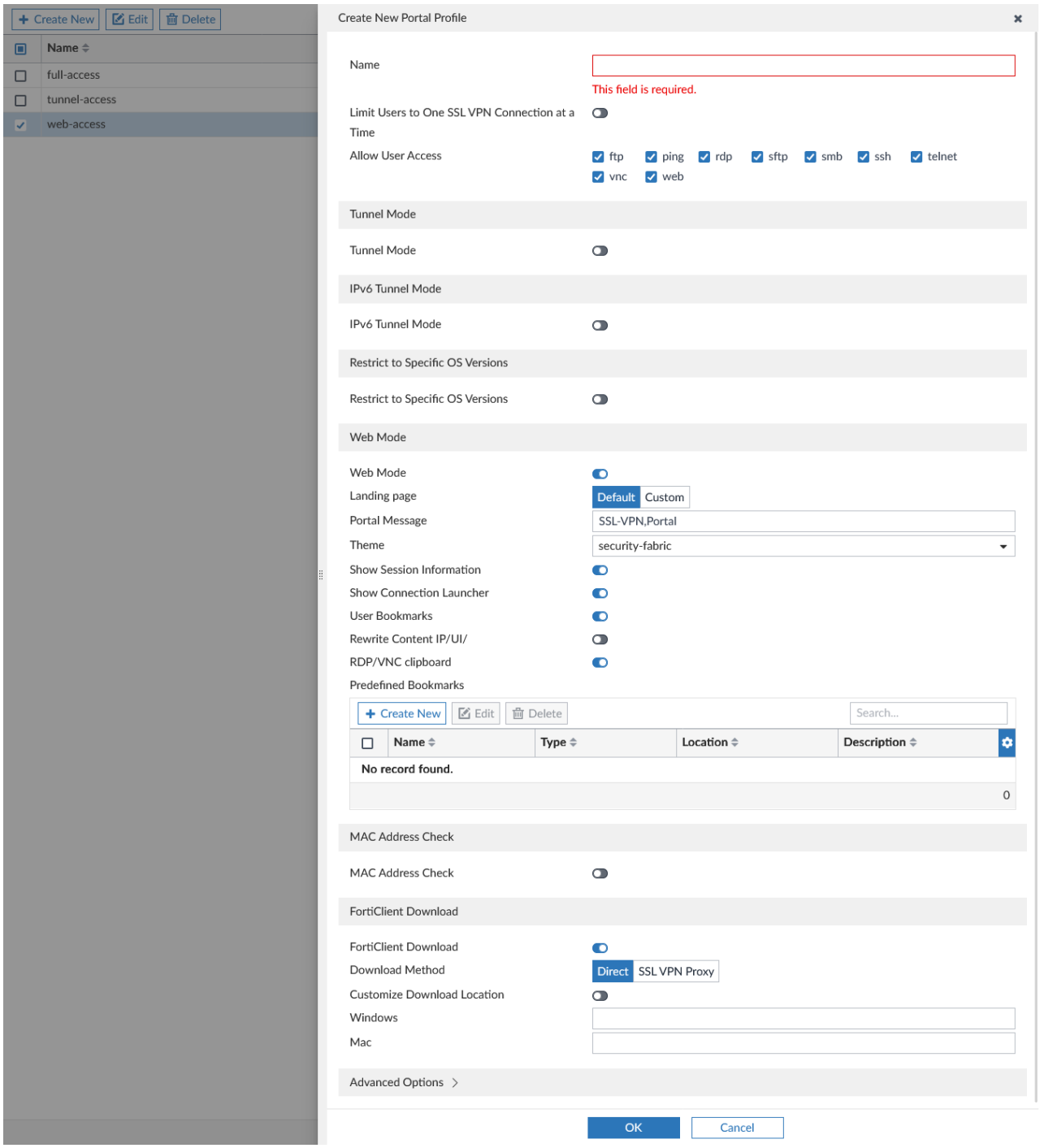
Delete	Delete the selected profile or profiles.
Column Settings	Adjust the visible columns.
Search	Enter a search term to search the portal profile list.

Creating SSL VPN portal profiles

To create SSL VPN portal profiles, you must be logged in as an administrator with sufficient privileges. Multiple profiles can be created.

To create portal profiles:

1. Go to *VPN Manager > SSL VPN Portals*.
2. Click *Create New* in the toolbar. The *Create New Portal Profile* pane is displayed.



3. Configure the following settings, then select *OK* to create the profile.

Name	Enter a name for the portal.

Limit Users to One SSL VPN Connection at a Time	Set the SSL VPN tunnel so that each user can only be logged in to the tunnel one time per user log in. Once they are logged in to the portal, they cannot go to another system and log in with the same credentials until they log out of the first connection.
Tunnel Mode	Select to configure and enable tunnel mode access. These settings determine how tunnel mode clients are assigned IPv4 addresses.
Split Tunneling	Select one of the following options: • *Disabled*: All client traffic will be directed over the SSL-VPN tunnel. • *Enable Based on Policy Destination*: Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel. • *Enabled for Trusted Destinations*: Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.
Routing Address Override	If you enable split tunneling, you are required to set the address that your corporate network is using. Traffic intended for the routing address will not be split from the tunnel.
Source IP Pools	Select an IPv4 pool for users to acquire an IP address when connecting to the portal. There is always a default pool available if you do not create your own.
IPv6 Tunnel Mode	Select to configure and enable tunnel mode access. These settings determine how tunnel mode clients are assigned IPv6 addresses.
Split Tunneling	Select one of the following options: • *Disabled*: All client traffic will be directed over the SSL-VPN tunnel. • *Enable Based on Policy Destination*: Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel. • *Enabled for Trusted Destinations*: Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.
IPv6 Routing Address Override	If you enable split tunneling, you are required to set the address that your corporate network is using. Traffic intended for the routing address will not be split from the tunnel.
Source IPv6 Pools	Select an IPv6 pool for users to acquire an IP address when connecting to the portal. There is always a default pool available if you do not create your own.
Tunnel Mode Client Options	These options affect how the FortiClient application behaves when connected to the FortiGate VPN tunnel. When enabled, a checkbox for the corresponding option appears on the VPN log in screen in FortiClient, and is disabled by default.
Allow client to save password	The user's password is stored on the user’s computer and will automatically populate each time they connect to the VPN.

Allow client to connect automatically	When the FortiClient application is launched, for example after a reboot or system start up, FortiClient will automatically attempt to connect to the VPN tunnel.
Allow client to keep connections alive	The FortiClient connection will not shut down. When not selected, during periods of inactivity, FortiClient will attempt to stay connected every three minutes for a maximum of 10 minutes.
Restrict to Specific OS Versions	Enable to restrict to the specified OS versions.
Web Mode	Select to enable web mode access.
Landing page	Select Default or Custom. When Custom is selected, you can specify the landing page *URL* and *Logout URL*.
Portal Message	The text header that appears on the top of the web portal.
Theme	A color styling specifically for the web portal: *blue*, *green*, *mariner*, *melongene*, or *red*.
Show Session Information	Display the *Session Information* widget on the portal page. The widget displays the log in name of the user, the amount of time the user has been logged in, and the inbound and outbound traffic statistics.
Show Connection Launcher	Display the *Connection Launcher* widget on the portal page. Use the widget to connect to an internal network resource without adding a bookmark to the bookmark list. You select the type of resource and specify the URL or IP address of the host computer.
Show Login History	Include user log in history on the web portal, then specify the number of history entries.
User Bookmarks	Include bookmarks on the web portal. Bookmarks are used as links to internal network resources. When a bookmark is selected from a bookmark list, a pop-up window opens with the web page. VNC and RDP require a browser plugin. FTP and Samba replace the bookmarks page with an HTML file-browser.
Pre-Defined Bookmarks	The list of predefined bookmarks. Click *Create New* to add a bookmark. See Predefined bookmarks on page 692 for information.
Enable FortiClient Download	Select to enable FortiClient downloads.
Download Method	Select the method to use for downloading FortiClient from the SSL VPN portal. Choose between *Direct* and *SSL-VPN Proxy*. This option is only available when *Enable FortiClient Download* is *On*.
Customize Download Location	Select to specify a custom location to use for downloading FortiClient. You can specify a location for FortiClient (Windows) and FortiClient (Mac). Type the URL in the *Windows* box and/or *Mac* box. This option is only available when *Enable FortiClient Download* is *On*.
Advanced Options	Configure advanced options. For information, see the *FortiOS CLI Reference*.

Predefined bookmarks

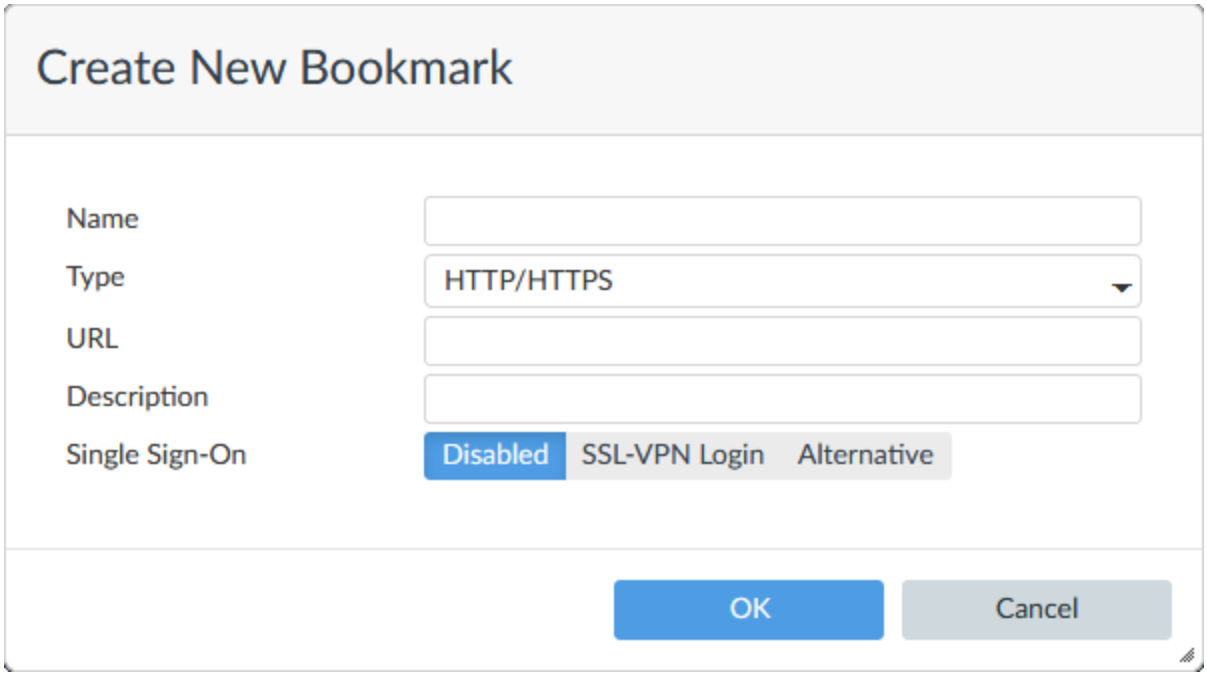
Bookmarks are used as links to specific resources on the network. When a bookmark is selected from a bookmark list, a window opens with the requested web page. RDP and VNC open a window that requires a browser plug-in. FTP replaces the bookmark page with an HTML file-browser.

A web bookmark can include log in credentials to automatically log the SSL VPN user into the web site. When the administrator configures bookmarks, the web site credentials must be the same as the user's SSL VPN credentials. Users configuring their own bookmarks can specify alternative credentials for the web site.

Predefined bookmarks can be added to portal profiles when creating or editing a profile.

To create a predefined bookmark:

1. Go to *VPN Manager > SSL VPN Portals*.
2. Edit an existing profile, or create a new profile. See Editing portal profiles on page 694 or Creating SSL VPN portal profiles on page 688.
3. Click *Create New* in the *Predefined Bookmarks* field. *Enable Web Mode* must be selected for this field to be available. The *Create New Bookmark* dialog box opens. The available options will vary depending on the selected type.



4. Configure the following settings, then select *OK* to create the bookmark.

Name	Enter a name for the bookmark.
Type	Select the bookmark type: *CITRIX*, *FTP*, *HTTP/HTTPS*, *Port Forward*, *RDP*, *SMB*, *SSH*, *Telnet*, or *VNC*.
URL	Enter the bookmark URL. This option is only available when *Type* is *Citrix*, or *HTTP/HTTPS*.
Folder	Enter the bookmark folder.

	This option is only available when *Type* is *FTP* or *SMB*.
Host	Enter the host name. This option is only available when *Type* is *Port Forward*, *RDP*, *SSH*, *TELNET*, or *VNC*.
Remote Port	Enter the remote port. This option is only available when *Type* is *Port Forward*.
Listening Port	Enter the listening port. This option is only available when *Type* is *Port Forward*.
Show Status Window	Enable to show the status window. This option is only available when *Type* is *Port Forward*.
Port	Enter the port number. This option is only available when *Type* is *RDP* or *VNC*.
Username	Enter the user name. This option is only available when *Type* is *RDP*.
Password	Enter the password. This option is only available when *Type* is *RDP* or *VNC*.
Keyboard Layout	Select the keyboard layout: *German (QWERTZ)*, *English (US)*, *Unknown*, *French (AZERTY)*, *Italian*, or *Swedish*. This option is only available when *Type* is *RDP*.
Security	Select the security type: *Allow the server to choose the type of security*, *Network Level Authentication*, *Standard RDP encryption*, or *TLS encryption*. This option is only available when *Type* is *RDP*.
Description	Optionally, enter a description of the bookmark.
Single Sign-on	Select the SSO setting for links that require authentication: *Disabled*, *Automatic*, or *Static*. If *Static* is selected, click the add icon, then enter the *Name* and *Value* to add SSO Form Data. Multiple fields can be added. Click *Remove* to remove a field. When including a link using SSO use the entire URL, not just the IP address. This option is only available when *Type* is *Citrix*, *FTP*, *HTTP/HTTPS*, *RDP*, or *SMB*. The *Static* option is only available when *Type* is *Citrix*, *HTTP/HTTPS*, or *RDP*.

To edit a bookmark:

1. Go to *VPN Manager > SSL VPN Portals*.
2. Edit and existing profile, or create a new profile. See Editing portal profiles on page 694 or Creating SSL VPN portal profiles on page 688.

3. Click the *Edit* icon in the bookmark row. The *Bookmark* dialog box opens.
4. Edit the bookmark as required, then click *OK* to apply your changes.

To delete a bookmark:

1. Go to *VPN Manager > SSL VPN Portals*.
2. Edit and existing profile, or create a new profile. See Editing portal profiles on page 694 or Creating SSL VPN portal profiles on page 688.
3. Click the *Delete* icon in the bookmark row.

Editing portal profiles

To edit a portal profile, you must be logged in as an administrator with sufficient privileges. The device cannot be edited.

To edit a portal profile:

1. Go to *VPN Manager > SSL VPN Portals*.
2. Double-click on a profile, right-click on a profile and then select *Edit* from the menu, or select the profile then click *Edit* in the toolbar. The *Edit Portal Profile* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

Deleting portal profiles

To delete a portal profile or profiles, you must be logged in as an administrator with sufficient privileges.

To delete portal profiles:

1. Go to *VPN Manager > SSL VPN Portals*.
2. Select the profile or profiles you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the selected profile or profiles.

SSL VPN monitor

SSL VPNs can be monitored by going to *VPN Manager > SSL VPN Monitor*.

The following information is shown:

Device	The device or VDOM name.
User	The user name.
Remote Host	The remote host.
Last Login	The time of the last log in.

Active Connections	The number of active connections on the VPN.

VPN security policies

Once you have defined the IP source and destination addresses, the phase 1 authentication parameters, and the phase 2 parameters, you must define the VPN security policies.

FortiGate unit VPNs can be policy-based or route-based. There is little difference between the two types. In both cases, you specify phase 1 and phase 2 settings. However there is a difference in implementation. A route-based VPN creates a virtual IPsec network interface that applies encryption or decryption as needed to any traffic that it carries. That is why route-based VPNs are also known as interface-based VPNs. A policy-based VPN is implemented through a special security policy that applies the encryption you specified in the phase 1 and phase 2 settings.

An IPsec security policy enables the transmission and reception of encrypted packets, specifies the permitted direction of VPN traffic, and selects the VPN tunnel. In most cases, only a single policy is needed to control both inbound and outbound IP traffic through a VPN tunnel.

For a route-based VPN, you create two security policies between the virtual IPsec interface and the interface that connects to the private network. In one policy, the virtual interface is the source. In the other policy, the virtual interface is the destination. The *Action* for both policies is *Accept*. This creates bidirectional policies that ensure traffic will flow in both directions over the VPN.

For a policy-based VPN, one security policy enables communication in both directions. You must select *IPSEC* as the *Action* and then select the VPN tunnel dynamic object you have mapped to the phase 1 settings. You can then enable inbound and outbound traffic as needed within that policy, or create multiple policies of this type to handle different types of traffic differently. For example HTTPS traffic may not require the same level of scanning as FTP traffic.

Defining policy addresses

A VPN tunnel has two end points. These end points may be VPN peers, such as two FortiGate gateways. Encrypted packets are transmitted between the end points. At each end of the VPN tunnel, a VPN peer intercepts encrypted packets, decrypts the packets, and forwards the decrypted IP packets to the intended destination.

You need to define firewall addresses for the private networks behind each peer. You will use these addresses as the source or destination address depending on the security policy.

In general:

- In a gateway-to-gateway, hub-and-spoke, dynamic DNS, redundant-tunnel, or transparent configuration, you need to define a policy address for the private IP address of the network behind the remote VPN peer.
- In a peer-to-peer configuration, you need to define a policy address for the private IP address of a server or host behind the remote VPN peer.

Defining security policies

Security policies allow IP traffic to pass between interfaces on a FortiGate unit. You can limit communication to particular traffic by specifying source and destination addresses. Then only traffic from those addresses will be allowed.

Policy-based and route-based VPNs require different security policies.

A policy-based VPN requires an IPsec security policy. You specify the interface to the private network, the interface to the remote peer and the VPN tunnel. A single policy can enable traffic inbound, outbound, or in both directions.

A route-based VPN requires an *Accept* security policy for each direction. As source and destination interfaces, you specify the interface to the private network and the virtual IPsec interface of the VPN. The IPsec interface is the destination interface for the outbound policy and the source interface for the inbound policy. One security policy must be configured for each direction of each VPN interface.

If the security policy that grants the VPN connection is limited to certain services, DHCP must be included, otherwise the client will not be able to retrieve a lease from the FortiGate's (IPsec) DHCP server because the DHCP request (coming out of the tunnel) will be blocked.

Before you define the IPsec policy, you must:

- Define the IP source and destination addresses.
- Specify the phase 1 authentication parameters.
- Specify the phase 2 parameters.
- Create a VPN Tunnel dynamic object (policy-based VPNs only).

You must define at least one IPsec policy for each VPN tunnel. If the same remote server or client requires access to more than one network behind a local FortiGate unit, the FortiGate unit must be configured with an IPsec policy for each network. Multiple policies may be required to configure redundant connections to a remote destination or control access to different services at different times.

To ensure a secure connection, the FortiGate unit must evaluate IPSEC policies before ACCEPT and DENY security policies. Because the FortiGate unit reads policies starting at the top of the list, you must move all IPsec policies to the top of the list. When you define multiple IPsec policies for the same tunnel, you must reorder the IPsec policies that apply to the tunnel so that specific constraints can be evaluated before general constraints.

When you define a route-based VPN, you create a virtual IPsec interface on the physical interface that connects to the remote peer. You create ordinary Accept security policies to enable traffic between the IPsec interface and the interface that connects to the private network. This makes configuration simpler than for policy-based VPNs, which require IPsec security policies.

See Managing policies on page 427 for information on creating policies on your FortiManager.

Fabric View

The *Fabric View* module enables you to view Security Fabric Ratings of configurations for FortiGate Security Fabric groups as well as create fabric connectors. The *Fabric View* tab is available in version 6.0 ADOMs and later.

This section contains the following topics:

- Security Fabric Topology on page 697
- Physical Topology on page 698
- Logical Topology on page 699
- Filter Topology Views on page 700
- Search Topology Views on page 701
- Security Rating on page 701
- Fabric Connectors on page 705

Security Fabric Topology

You can see the Security Fabric topology in the FortiManager GUI, in the *Fabric View* menu. You can choose the Physical Topology or Logical Topology views. In both topology views, you can hover over device icons and use filtering and sorting options to see more information about devices and your organization's network. Go to *Fabric View* and select the Fabric group to see the whole topology for that Fabric group.

Upstream

The *Upstream* dropdown in the Physical and Logical Topology views allows you to receive destination data from the following options in the drop-down menu: *Internet*, *Owner*, *IP Address*, and *Country/Region*. These options are available in the Physical Topology and the Logical Topology view, when you select Device Traffic in the menu in the top right corner.

When you set the upstream to *Owner*, the destination hosts are simplified to a donut chart. This chart shows the percentage division between Internal hosts (with private IP addresses) and Internet hosts. To see which color represents each host, hover over either color. To zoom in on the total number of hosts, click on the donut graph.

Switch stacking

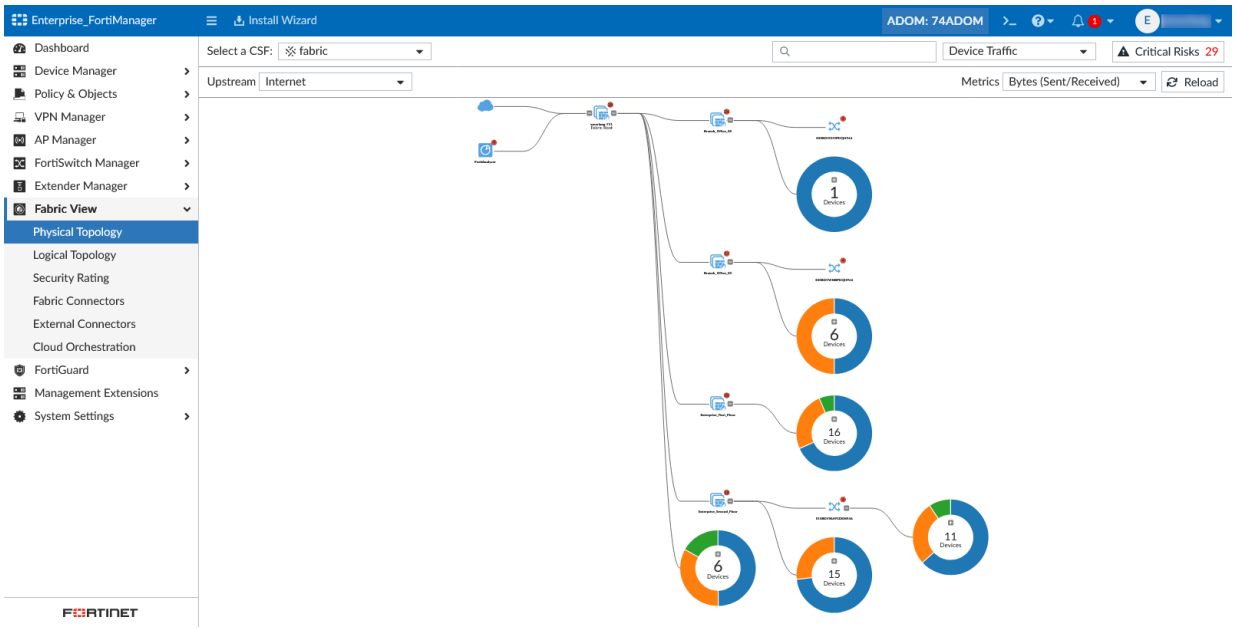
FortiAP and FortiSwitch links are enhanced in the Security Fabric's Logical and Topological views to show Link Aggregation Groups for the Inter-switch Link (ISL-LAG). This makes it easier to identify which links are physical links and which links are ISL-LAG. To quickly understand connectivity when you look at multiple link connections, ISL-LAG is identified with a thicker single line. To identify ISL-LAG groups with more than two links, you can also look at the port endpoint circles as references.

Physical Topology

The physical topology view shows the devices in the Security Fabric and the devices they are connected to. You can also select whether or not to view access layer devices in this topology. To see the physical topology, in FortiManager GUI, select *Fabric View* > *Physical Topology*.

From the dropdown list beside the search bar, select one of the following views:

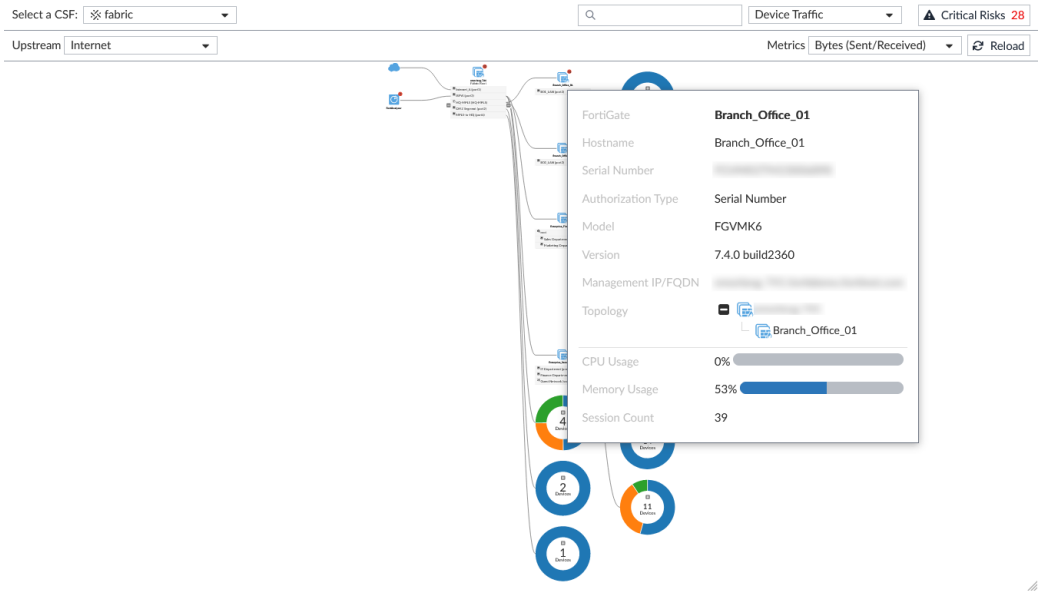
- *Device Traffic*: organize devices by traffic.
- *Device Count*: organize devices by the number of devices connected to it.
- *Device Operating System*: organize devices by operating system.
- *Device Hardware Vendor*: organize devices by hardware vendor.
- *Risk*: only include devices that have endpoints with medium, high, or critical risk values of the specified type: All, Compromised Host, Vulnerability, or Threat Score.
- *No Devices*: do not show endpoints.



The physical topology view displays your network as a chart of interconnected devices. These devices are grouped based on the upstream device they are connected to. You can click a device in the topology to view additional information.

The following fields are displayed in when viewing device information:

- *FortiGate*: hostname, serial number, model, version, and management IP.
- *FortiAnalyzer*: hostname, version, IP address, and model.
- *FortiSwitch*: label, serial number, and version.
- *Device*: name, IP address, hostname, MAC, interfaces, online interfaces, hardware type, hardware vendor, OS, and user.

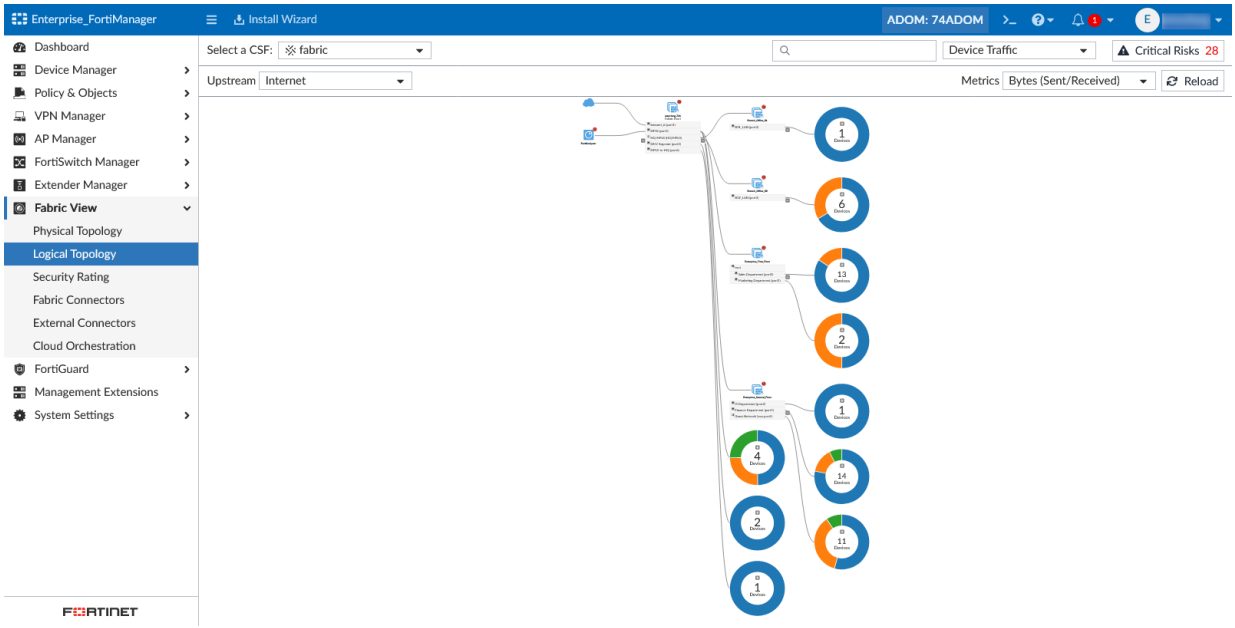


Security Fabric Rating recommendations are also shown in the topology, beside the icon of the device the recommendations apply to. Click the icon to view the rating report.

Logical Topology

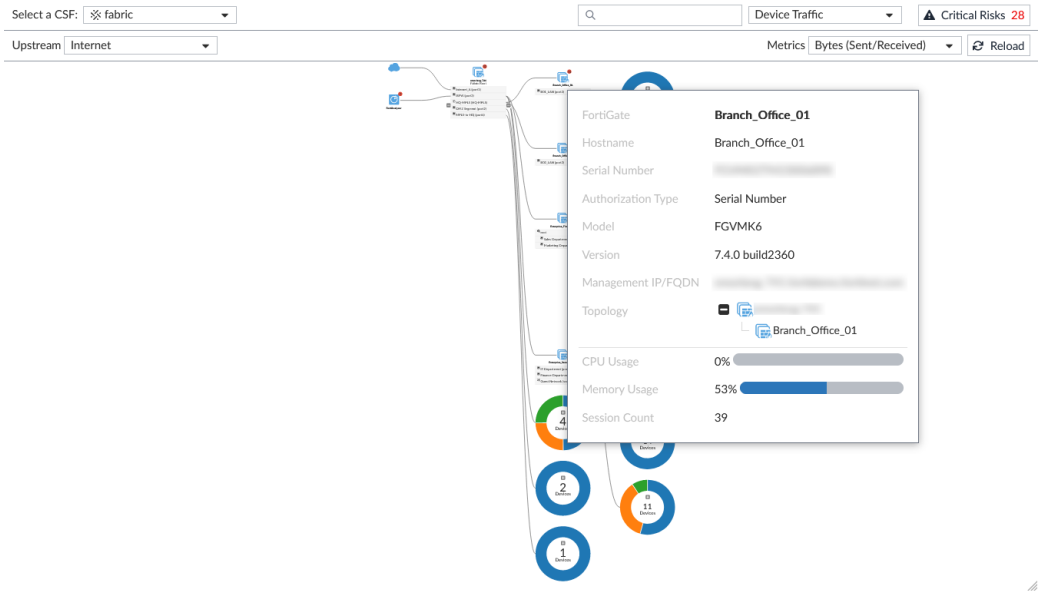
The Logical Topology view is similar to the Physical Topology view, but it shows the network interfaces, logical or physical, that are used to connect devices in the Security Fabric.

To see the Logical Topology, in FortiManager GUI, select *Fabric View* > *Logical Topology*.



The Logical Topology view displays your network as a chart of network connection endpoints. These devices are grouped based on the upstream device interface they are connected to.

You can hover over the icon for each device to see information, such as serial number, hostname, and firmware version. You can also see each FortiGate interface that has upstream and downstream devices connected to it.



Security Fabric Rating recommendations are also shown in the topology, beside the icon of the device the recommendations apply to.

Filter Topology Views

You can use filters to narrow down the data on the topology views to find specific information.

To filter the topology views by device or vulnerability:

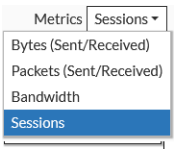
In the dropdown menu to the right of the *Search* field, select one of the following:



- Device Traffic
- Device Count
- Device Operating System
- Device Hardware Vendor
- Risk
- No Devices

To filter the topology views by metrics:

To sort the topology by metrics, in the *Metrics* dropdown menu, select one of the following:



- Bytes (Sent/Received)
- Packets (Sent/Received)
- Bandwidth
- Sessions

Search Topology Views

The search bar, located above the Physical and Logical Topology views, can help you easily find what you're looking for in the network topology and quickly resolve security issues. The search highlights devices that match your search criteria, and grays out devices that don't match.

- For *FortiGate* you can search for device information including IP address, model, serial number, and version.
- For *FortiAnalyzer* you can search for device information including IP address, version, and model.
- For *FortiSwitch* you can search by serial number.
- For *Other Devices*, you can search by IP address, hostname, and MAC address.

Security Rating

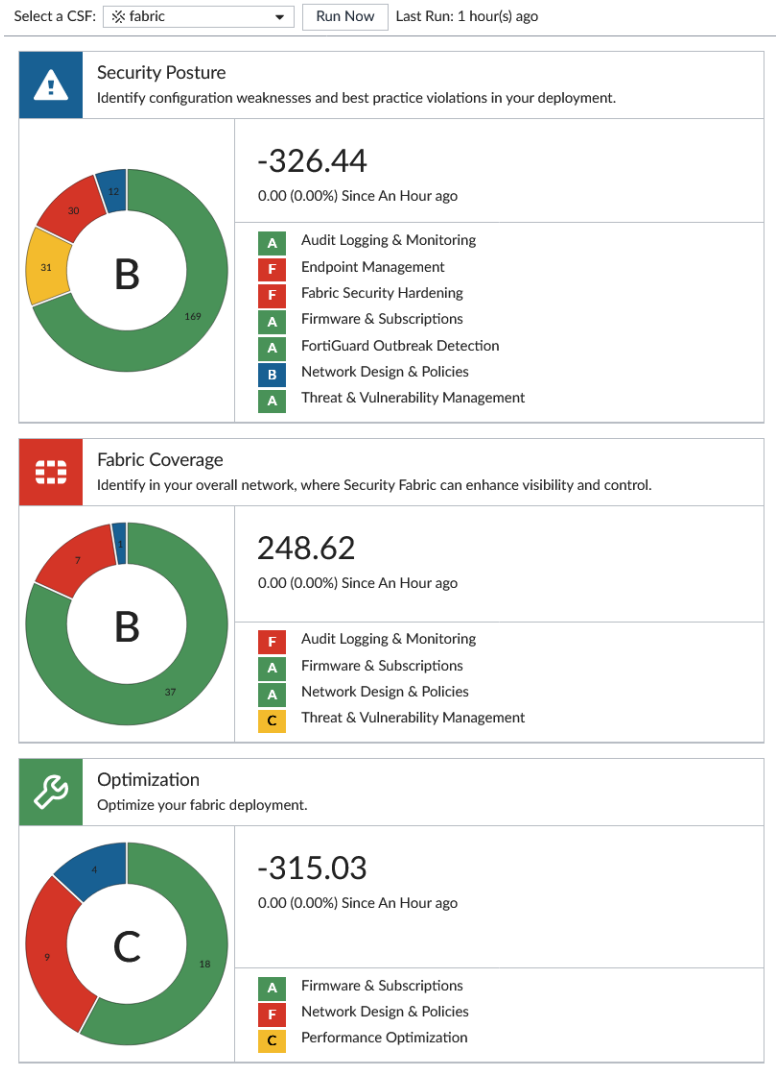
The *Fabric View > Security Rating* pane displays Security Fabric Ratings of configurations for FortiGate Security Fabric groups or a single FortiGate device (version 7.0 and later).

The security rating on FortiManager is based on the security rating reports from FortiGate. If security rating reports are unavailable from FortiGate devices, the report on FortiManager will not include its data.

You can view the results for multiple FortiGate Security Fabric groups by choosing a group in the *Select a CSF* dropdown menu.

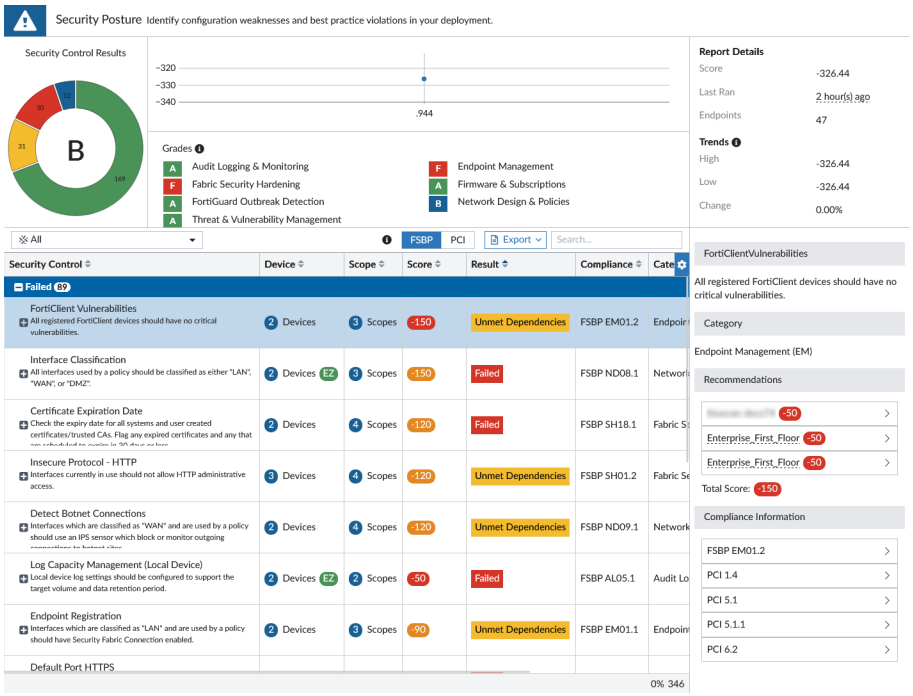
Click *Run Now* to run the Security Rating report at any time directly from FortiManager.

The *Security Rating* pane is separated into three major scorecards: *Security Posture*, *Fabric Coverage*, and *Optimization*, which provide an executive summary of the three largest areas of security focus in the Security Fabric.



The scorecards show an overall letter grade and breakdown of the performance in sub-categories. Clicking a scorecard drills down to a detailed report of itemized results and compliance recommendations. The point score represents the net score for all passed and failed items in that area.

The report includes the security controls that were tested against, linking to specific FSBP or PCI compliance policies. Click the *FSBP* and *PCI* buttons to reference the corresponding standard. Users can search or filter the report results.



To exit the detailed report view, click the scorecard title to return to the summary view.

For more information about security ratings, and details about each of the checks that are performed, go to Security Best Practices & Security Rating Feature.

Security rating licenses are required to run security rating checks across all the devices in the Security Fabric. It also allows ratings scores to be submitted to and received from FortiGuard for ranking networks by percentile.

See https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/security-rating.html for information.

Viewing Security Fabric Ratings

The *Security Rating* summary is displayed when FortiManager is managing FortiGate units that have Security Fabric enabled and are part of a Security Fabric group.

You can view Security Fabric Ratings of configurations for all FortiGate units in a Security Fabric Group or for individual FortiGate units in a Security Fabric group.

To run and view the Security Ratings check:

1. Ensure you are in an ADOM which includes a Security Fabric group.
2. Go to *Fabric View* > *Security Rating*.
3. Select the Security Fabric group from the *Select a CSF* dropdown menu, and click *Run Now* in the toolbar.

- Security Fabric Rating results are displayed in the content pane for the selected Security Fabric group.
- Click one of the scorecards, for example *Security Posture*, to view the detailed report.
  - In the detailed report view, you can view results by expanding the *Failed*, *Exempt*, and *Passed* categories.
  - In the detailed report view, select *All* to view results for all devices in the group, or select individual Fabric devices or device categories to filter results by the selection.

Security Fabric score

The Security Fabric score is calculated when a security rating check is run, based on the severity level of the checks that are passed or failed. A higher scores represents a more secure network. Points are added for passed checks and removed for failed checks.

Severity level	Weight (points)
Critical	50
High	25
Medium	10
Low	5

To calculate the number of points awarded to a device for a passed check, the following equation is used:

$$\text{score} = \frac{\text{<severity level weight>}}{\text{<\# of FortiGates>}} \times \text{<secure FortiGate multiplier>}$$

The secure FortiGate multiplier is determined using logarithms and the number of FortiGate devices in the Security Fabric.

For example, if there are four FortiGate devices in the Security Fabric that all pass the compatible firmware check, the score for each FortiGate device is calculated with the following equation:

$$\frac{50}{4} \times 1.292 = 16.15 \text{ points}$$

All of the FortiGate devices in the Security Fabric must pass the check in order to receive the points. If any one of the FortiGate devices fails a check, the devices that passed are not awarded any points. For the device that failed the check, the following equation is used to calculated the number of points that are lost:

$$\text{score} = \text{<severity level weight>} \times \text{<secure FortiGate multiplier>}$$

For example, if the check finds two critical FortiClient vulnerabilities, the score is calculated with the following equation:

$$-50 \times 2 = -100 \text{ points}$$

Scores are not affected by checks that do not apply to your network. For example, if there are no FortiAP devices in the Security Fabric, no points will be added or subtracted for the FortiAP firmware version check.

Fabric Connectors

You can use FortiManager to create the following types of fabric connectors:

- Core Network Security on page 705

Core Network Security

You can use the *Fabric Connectors* tab to create the following types of core network security fabric connectors:

- Creating FortiClient EMS connectors on page 705

Creating FortiClient EMS connectors

You can configure a FortiClient EMS connector on FortiManager to retrieve or generate EMS tag addresses from a FortiClient EMS or FortiClient EMS Cloud server.

When a FortiClient EMS connector is configured, FortiManager automatically registers the FortiGate on FortiClient EMS, allowing FortiGate to retrieve dynamic object details from FortiClient EMS. Once the FortiClient EMS connector has been created, you can configure a ZTNA server and use the security posture tags in policies. See Zero Trust Network Access (ZTNA) objects on page 572 and Configuring a ZTNA server on page 574.



Importing the FortiClient EMS configuration from FortiGate is not supported

You cannot import FortiGate's FortiClient EMS configuration into FortiManager. When an install is performed from FortiManager, the FortiClient EMS connectors configured on FortiManager are installed to the target FortiGate, replacing all existing device-level configurations. When adding a FortiGate to FortiManager with pre-existing connection to FortiClient EMS, you must manually configure a FortiClient EMS connector on FortiManager with matching settings before performing an install.

Fields that support metadata variables are identified with the following magnifying glass icon . See ADOM-level metadata variables on page 557..



FortiClient EMS connectors can also be configured from *Policy & Objects* > *Security Fabric* > *Endpoint/Identity*.



In order for the FortiClient EMS connector to import dynamic object details from FortiClient EMS, FortiClient EMS and FortiOS must be on version 7.0.3 or later.

To create a FortiClient EMS connector:

1. Go to *Fabric View* > *Fabric* > *Fabric Connectors*.
2. Select one of the five available FortiClient EMS connectors, and click *Edit*.
3. Fill in the EMS server details, and click *OK*.

Name	Enter a name for the FortiClient EMS connector.
Status	Set the status of the connector to enabled.
Type	Select *FortiClient EMS*.
IP/Domain name	Enter the IP or domain name for the FortiClient EMS.
HTTPS port	Enter the HTTPS port for the FortiClient EMS.
User Name	Enter the FortiClient EMS administrator user name.
Password	Enter the FortiClient EMS administrator password.
EMS Threat Feed	Toggle ON to allow FortiManager to pull FortiClient malware hash from FortiClient EMS.
Synchronize firewall addresses	Toggle ON to automatically create and synchronize firewall addresses for all EMS tags.
Multi Site	Enable to retrieve EMS tags with site information when multiple sites are configured on FortiClient EMS.
Advanced Options	Click to open and configure advanced options for the FortiClient EMS connector. The `source-ip` field supports metadata variables. See ADOM-level metadata variables on page 557.

4. Click *OK* to create the connector.
5. After the connector has been authenticated, FortiManager will retrieve tags and the certificate-fingerprint from the EMS server. FortiManager will *not* appear on the FortiClient EMS server under Fabric Devices.

To create a FortiClient EMS Cloud connector:

1. Go to *Fabric View* > *Fabric* > *Fabric Connectors*.
2. Select one of the five available FortiClient EMS connectors, and click *Edit*.
3. Fill in the EMS Cloud server details, and click *OK*.

Name	Enter a name for the FortiClient EMS connector.
Status	Set the status of the connector to enabled.
Type	Select *FortiClient EMS Cloud*.  FortiManager can only connect to the FortiClient EMS Cloud that is registered to the same FortiCloud account.

EMS Threat Feed	Toggle ON to allow FortiManager to pull FortiClient malware hash from FortiClient EMS.
Synchronize firewall addresses	Toggle ON to automatically create and synchronize firewall addresses for all EMS tags.
Multi Site	Enable to retrieve EMS tags with site information when multiple sites are configured on FortiClient EMS.
Advanced Options	Click to open and configure advanced options for the FortiClient EMS Cloud connector. The `source-ip` field supports metadata variables. See ADOM-level metadata variables on page 557.

4. Click *OK* to create the connector.
5. Once the connector is configured, FortiManager will appear on the EMS Cloud server under *Administration > Fabric Devices*, and you must authorize it before FortiManager is able to retrieve the EMS tags.

To manually import and view tags from the EMS server:

1. Go to *Fabric View > Fabric > Fabric Connectors*, and edit the configured FortiClient EMS connector.
2. Click *Apply & Refresh*.
   Any changes on the EMS server are dynamically populated on the FortiManager.
3. Go to *Policy & Objects > Firewall Objects > Security Posture Tag*.
   You can see imported IP and MAC tags available on the page. See Viewing security posture tags on page 572.

To use security posture tags imported from the EMS server in a policy:

1. Configure the proxy policy and object settings on FortiManager as required. See Create a new proxy policy on page 471.
2. Install the ZTNA policy to FortiGate using the *Device Manager* Install Wizard.
   While performing the installation to FortiGate, FortiManager also installs the digital fingerprint from the EMS server, removing the requirement to authorize the FortiGate on the EMS server.
3. Confirm that FortiGate is authorized on the EMS server:
   a. Log in on the FortiGate, and go to *Security Fabric > Fabric Connectors > FortiClient EMS*.
   b. Confirm the server details installed on the FortiGate are correct and that the status displays as *Connected*.

External Connectors

You can use FortiManager to create the following types of external connectors:

- Public and private SDN
- Threat Feeds
- Endpoint/Identity



You can create multiple fabric connectors of the same type in FortiManager.

Public and private SDN

Fabric connectors to SDNs provide integration and orchestration of Fortinet products with SDN solutions. Fabric Connectors ensure that any changes in the SDN environment are automatically updated in your network. There is no need to manually reconfigure addresses and policies whenever changes to the cloud environment occur.

SDN Connectors can be configured on FortiManager to create dynamic firewall address objects that can be installed to managed FortiGate devices.

You can use the *Fabric > External Connectors* pane to create public and private SDN fabric connectors for the following products:

- Public SDN
  - Creating AWS fabric connectors on page 711
  - Using FortiManager as a SDN proxy for AWS connectors on page 741
  - Creating Microsoft Azure fabric connectors on page 713
  - Creating Google Cloud Platform connector on page 735
  - Creating Oracle Cloud Infrastructure (OCI) connector on page 723
  - Creating AliCloud Service connector on page 733
  - Creating IBM Cloud connector on page 737
- Private SDN
  - Creating Kubernetes connector on page 731
  - Creating VMWare ESXi connector on page 725
  - Creating VMware NSX fabric connectors on page 715
  - Creating OpenStack (Horizon) connector on page 721
  - Creating ACI fabric connectors on page 708
  - Creating Nuage fabric connectors on page 717
  - Create Nutanix fabric connectors on page 719

Once an SDN connector has been created, you can import address names from the products to the fabric connectors to automatically create dynamic firewall address objects that you can use in policies. Alternatively, you can manually create dynamic firewall address objects.

- Importing address names to fabric connectors on page 739
- Configuring dynamic firewall addresses for fabric connectors on page 740

Creating ACI fabric connectors

With FortiManager, you can create a fabric connector for Application Centric Infrastructure (ACI), and then import address names from ACI to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate either with the Fortinet SDN Connector or directly with ACI and dynamically populate the objects with IP addresses.



The Cisco ACI fabric connector supports IPv4 and IPv6 addresses.

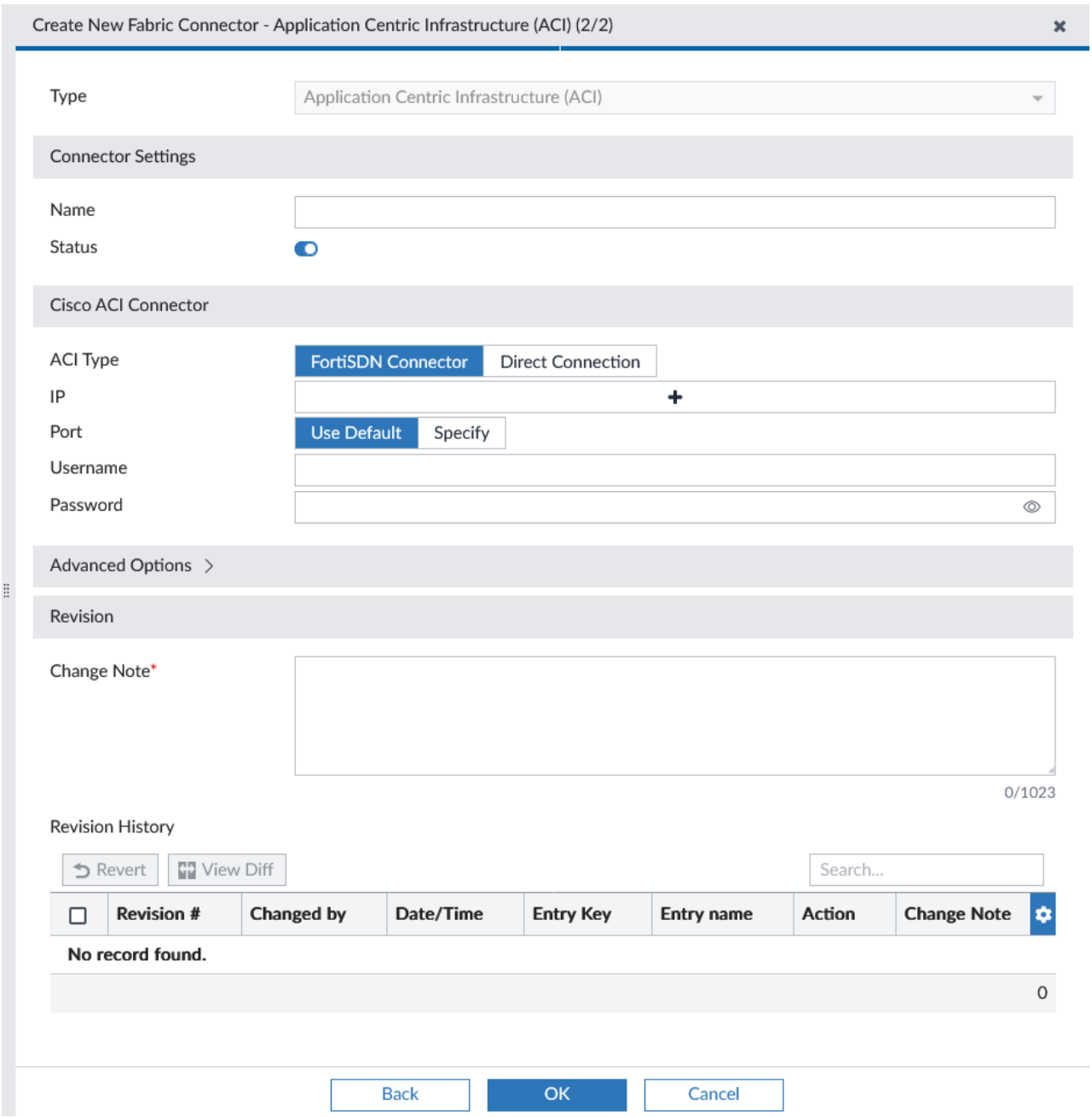
When you create a fabric connector for ACI, you are specifying how FortiGate can communicate with ACI.

Requirements:

- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with Application Centric Infrastructure (ACI).

To create a fabric connector object for ACI:

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.
2. Under *Private SDN*, select *Application Centric Infrastructure*. The *Application Centric Infrastructure* screen is displayed.



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

Type	Displays *Application Centric Infrastructure (ACI)*.
Name	Type a name for the fabric connector object.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.
ACI Type	Select the *FortiSDN Connector* or *Direct Connection*.
IP	Type the IP address.

Port	Identify the port used for Fortinet SDN Connector. Perform one of the following options: • Click *Use Default* to use the default port. • Click *Specify* and type the port number.
User Name	Type the user name for Fortinet SDN Connector.
Password	Type the password for Fortinet SDN Connector.

4. Click *OK* to save the connector.

To complete the fabric connector setup:

1. Import address names or manually create the dynamic firewall address for the SDN connector. See Importing address names to fabric connectors on page 739 and Configuring dynamic firewall addresses for fabric connectors on page 740.
   You can import SDN objects by filter or by endpoint group (EPG).
2. In the policy package in which you will be creating the new policy, create a firewall policy and include the dynamic firewall address objects for the SDN connector. See Create a new firewall policy on page 435.
3. Install the policy package to FortiGate. See Install a policy package on page 419.
   FortiGate communicates with the SDN to dynamically populate the firewall address objects with IP addresses.

Creating AWS fabric connectors

With FortiManager, you can create a fabric connector for Amazon Web Services (AWS), and then import address names from AWS to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate with AWS and dynamically populate the objects with IP addresses.

When you create a fabric connector for AWS, you are specifying how FortiGate can communicate directly with AWS.

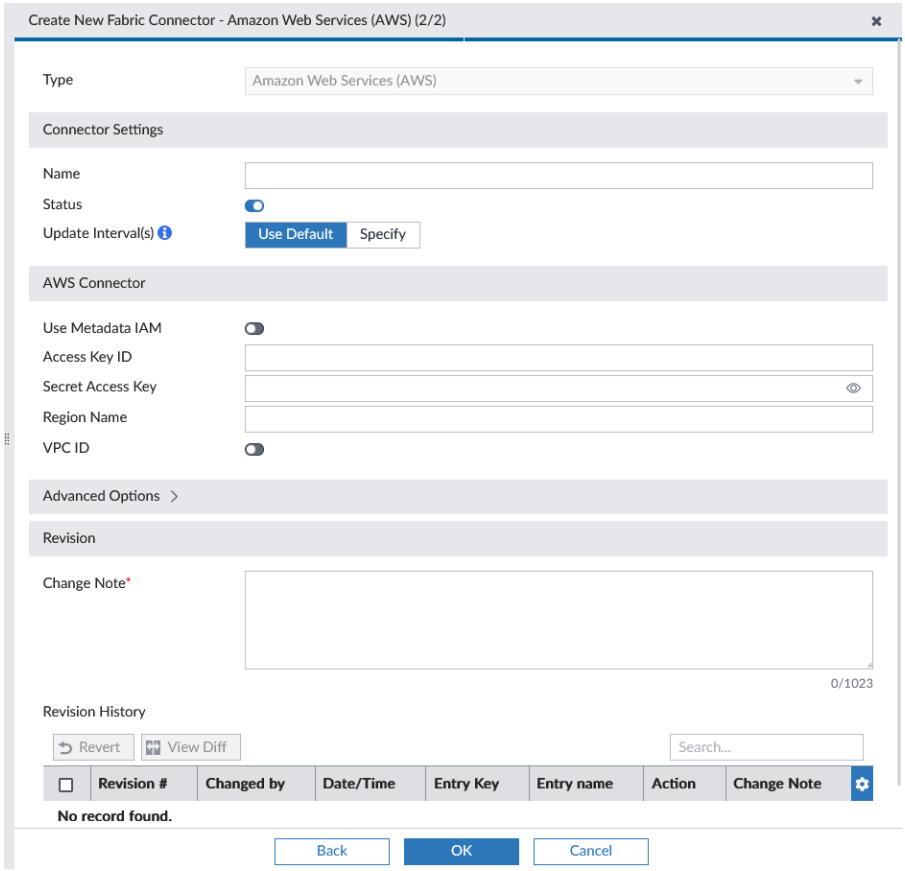
Requirements:

- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with AWS.

To create a fabric connector object for AWS:

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.

2. Under *Public SDN*, select *Amazon Web Services*. The *Amazon Web Services* screen is displayed.



3. Configure the following options, and then click *OK*:

Type	Displays *Amazon Web Services (AWS)*.
Name	Type a name for the fabric connector object.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.
Update Interval (s)	Specify how often in seconds that the dynamic firewall objects should be updated.
Access Key ID	Type the access key ID from AWS.
Secret Access key	Type the secret access key from AWS.
Region Name	Type the region name from AWS.
VPC ID	Type the AWS VPC ID.

4. Click *OK* to save the connector.

To complete the fabric connector setup:

1. Import address names or manually create the dynamic firewall address for the SDN connector. See Importing address names to fabric connectors on page 739 and Configuring dynamic firewall addresses for fabric connectors on page 740.

2. In the policy package in which you will be creating the new policy, create a firewall policy and include the dynamic firewall address objects for the SDN connector. See Create a new firewall policy on page 435.
3. Install the policy package to FortiGate. See Install a policy package on page 419.
   FortiGate communicates with the SDN to dynamically populate the firewall address objects with IP addresses.

Creating Microsoft Azure fabric connectors

With FortiManager, you can create a fabric connector for Microsoft Azure, and then import address names from Microsoft Azure to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate with Microsoft Azure and dynamically populate the objects with IP addresses.

When you create a fabric connector for Microsoft Azure, you are specifying how FortiGate can communicate directly with Microsoft Azure.



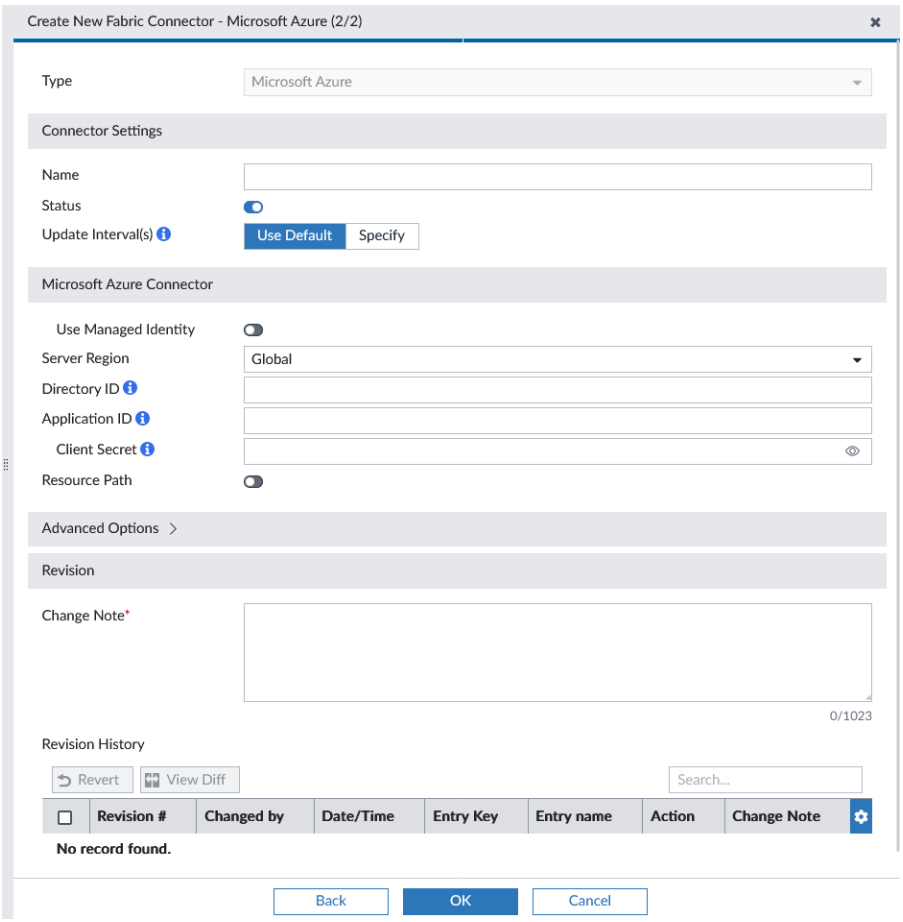
GraphQL is used to consolidate the number of queries required to read the Azure environment. The introduction of GraphQL helps avoid hitting Azure-throttling limits and facilitates scaling of SDN connector queries on large deployments.

Requirements:

- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with Microsoft Azure.

To create a fabric connector object for Microsoft Azure:

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.
2. Under *Public SDN*, select *Microsoft Azure*. The *Microsoft Azure* screen is displayed.



3. Configure the following options, and then click *OK*:

Type	Displays *Microsoft Azure*.
Name	Type a name for the fabric connector object.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.
Update Interval (s)	Specify how often in seconds that the dynamic firewall objects should be updated.
Server Region	Select an Azure region.
Directory ID	Enter the directory ID for your Azure AD tenant with Azure AD.
Application ID	Enter the application ID for your Azure application with Azure AD.
Client Secret	Enter the application secret created for your Azure application with Azure AD.
Resource Path	Optionally, enable the resource path to configure the *Subscribiption ID* and *Resource Group*.

4. Click *OK* to save the connector.

To complete the fabric connector setup:

1. Import address names or manually create the dynamic firewall address for the SDN connector. See Importing address names to fabric connectors on page 739 and Configuring dynamic firewall addresses for fabric connectors on page 740.
2. In the policy package in which you will be creating the new policy, create a firewall policy and include the dynamic firewall address objects for the SDN connector. See Create a new firewall policy on page 435.
3. Install the policy package to FortiGate. See Install a policy package on page 419.
   FortiGate communicates with the SDN to dynamically populate the firewall address objects with IP addresses.

Creating VMware NSX fabric connectors

With FortiManager, you can create a fabric connector for VMware NSX, and then import address names from VMware NSX to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate with VMware NSX and dynamically populate the objects with IP addresses.

When you create a fabric connector for VMware NSX, you are specifying how FortiGate can communicate directly with VMware NSX.

If ADOMs are enabled, you can create one fabric connector per ADOM.

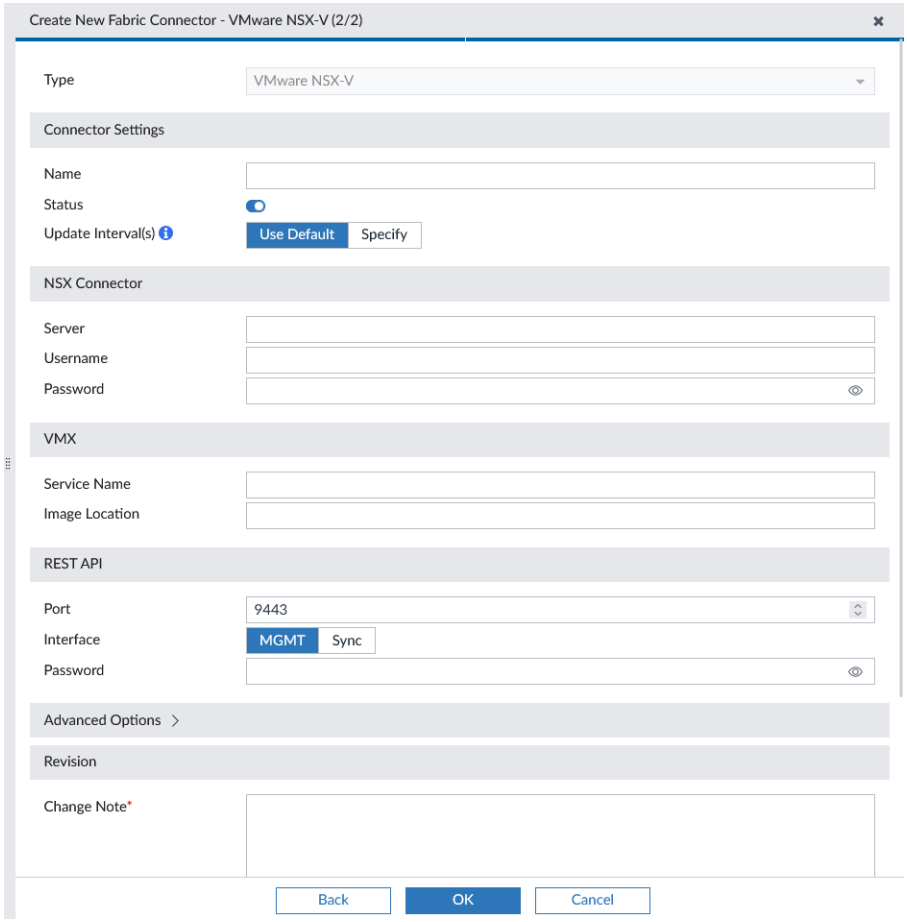
Requirements:

- FortiGate unit or FortiGate VMX Service Manager is managed by FortiManager.
- The managed FortiGate or FortiGate VMX Service Manager is configured to work with VMware NSX .
- IPv4 virtual wire pair policy
  FortiGate or FortiGate VMX Service Manager requires the use of an IPv4 virtual wire pair policy.

To create a fabric connector object for NSX:

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.

2. Under *Private SDN*, select *VMware NSX-V*. The *VMware NSX-V* screen is displayed.



3. Configure the following options, and then click *OK*:

Type	Displays *VMware NSX*.
Name	Type a name for the fabric connector object.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.
Update Interval (s)	Specify how often in seconds that the dynamic firewall objects should be updated.
Server	Type the IP address for VMware NSX.
Username	Type the username for VMware NSX.
Password	Type the password for VMware NSX.
VMX	The VMX options identify settings used by the FortiGate VMX Service Manager to communicate with the REST API for NSX Manager.
Service Name	Type the name of the FortiGate VMX service defined on NSX Manager.
Image Location	Type the location of the FortiGate VMX deployment template used by NSX Manager to deploy the FortiGate VMX service.

REST API	The REST API options specify how the FortiGate VMX Service Manager communicates with the REST API for NSX Manager.
Port	Type the port used by the FortiGate VMX Service Manager to communicate with NSX Manager.
Interface	Select the interface used by the FortiGate VMX Service Manager to communicate with NSX Manager. Choose between *MGMT* and *Sync*.
Password	Type the password that FortiGate VMX Service Manager uses with the REST API to communicate with NSX Manager. **Note**: This is not the admin password for FortiGate VMX Service Manager.

4. Click *OK* to save the connector.

To complete the fabric connector setup:

1. Import address names or manually create the dynamic firewall address for the SDN connector. See Importing address names to fabric connectors on page 739 and Configuring dynamic firewall addresses for fabric connectors on page 740.
2. Create a virtual wire pair. See Creating virtual wire pairs on page 550.
3. In the policy package in which you will be creating the new policy, create a firewall policy and include the dynamic firewall address objects for the SDN connector. See Create a new firewall policy on page 435.
4. Install the policy package to FortiGate. See Install a policy package on page 419.
   FortiGate communicates with the SDN to dynamically populate the firewall address objects with IP addresses.

Creating Nuage fabric connectors

With FortiManager, you can create a fabric connector for Nuage Virtualized Service Platform, and then import address names from Nuage to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate with Nuage Virtualized Service Platform and dynamically populate the objects with IP addresses.

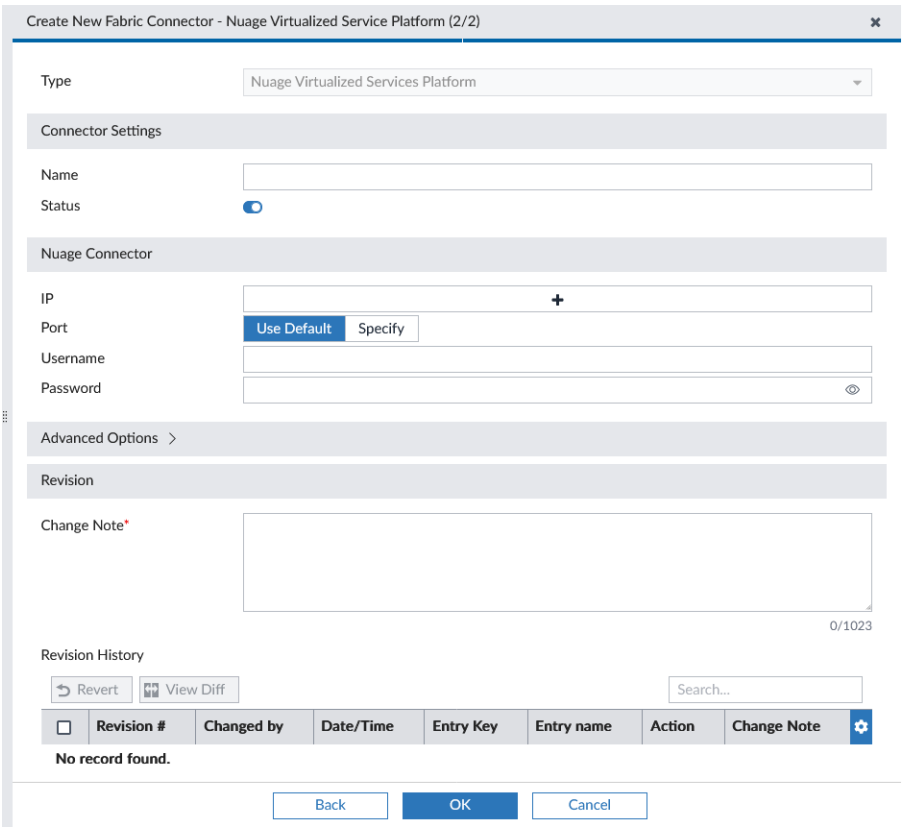
When you create a fabric connector for Nuage Virtualized Service Platform, you are specifying how FortiGate can communicate directly with Nuage.

Requirements:

- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with Nuage Virtualized Service Platform.

To create a fabric connector object for Nuage:

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.
2. Under *Private SDN*, select *Nuage Virtualized Service Platform*. The *Nuage Virtualized Service Platform* screen is displayed.



3. Configure the following options, and then click *OK*:

Type	Displays *Nuage Virtualized Services Platform*.
Name	Type a name for the fabric connector object.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.
IP	Type the IP address.
Port	Perform one of the following options: • Click *Use Default* to use the default port. • Click *Specify* and type the port number.
User Name	Type the Nuage user name.
Password	Type the Nuage password.

4. Click *OK* to save the connector.

To complete the fabric connector setup:

1. Import address names or manually create the dynamic firewall address for the SDN connector. See Importing address names to fabric connectors on page 739 and Configuring dynamic firewall addresses for fabric connectors on page 740.
2. In the policy package in which you will be creating the new policy, create a firewall policy and include the dynamic firewall address objects for the SDN connector. See Create a new firewall policy on page 435.

3. Install the policy package to FortiGate. See Install a policy package on page 419.
   FortiGate communicates with the SDN to dynamically populate the firewall address objects with IP addresses.

Create Nutanix fabric connectors

You can create Nutanix fabric connectors in FortiManager, and then import address names from Nutanix to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate with Nutanix and dynamically populate the objects with IP addresses.

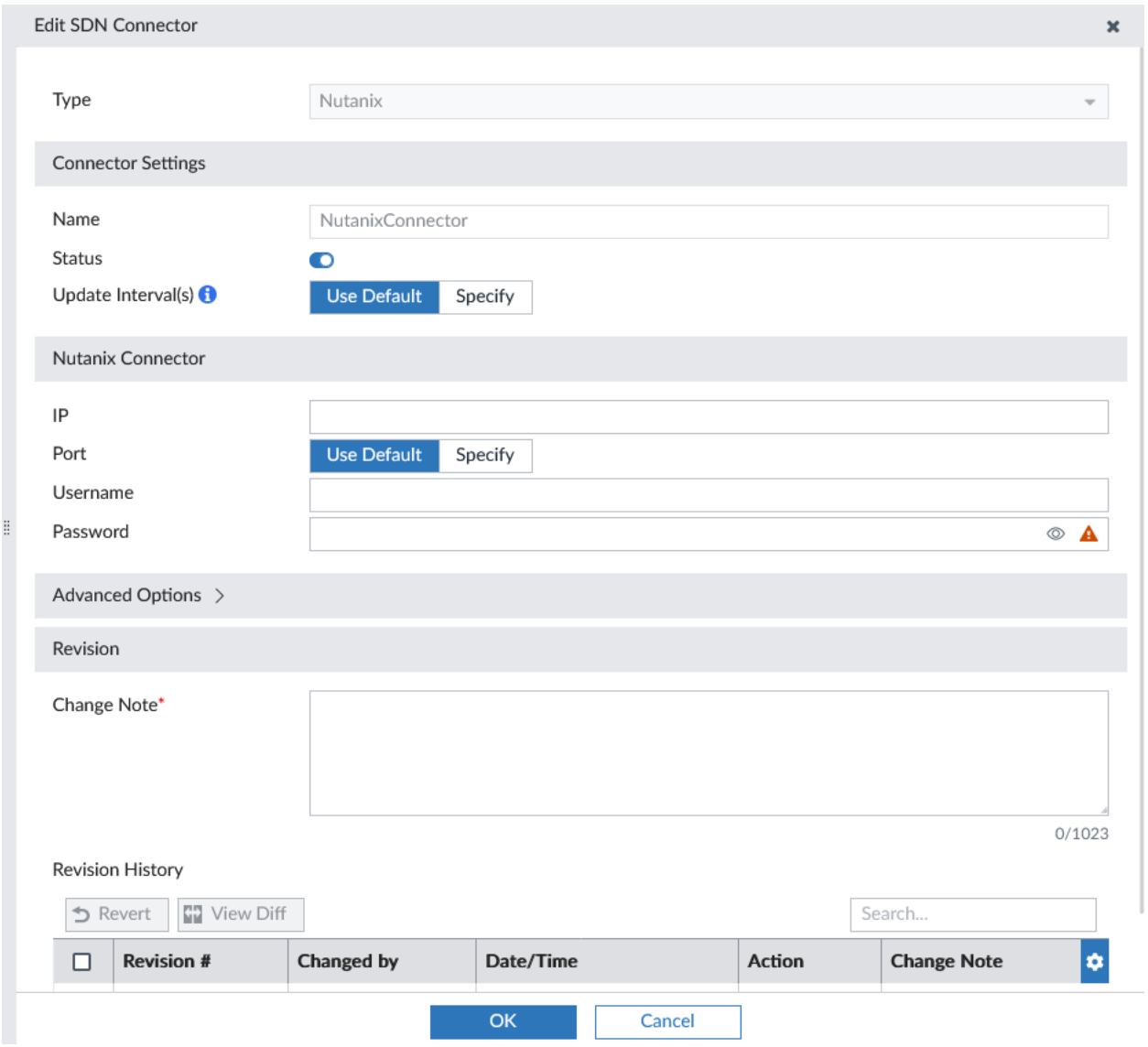
When you create a fabric connector for Nutanix, you are specifying how FortiGate can communicate with Nutanix.

Requirements:

- FortiManager version 7.0 ADOM or later
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with Nutanix.
- Supported with ISE 3.1.0 and 3.2.0.

To create a Nutanix fabric connector:

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.
2. Under *Private SDN*, select *Nutanix*. The *Nutanix* screen is displayed.



3. Configure the following options, and then click *OK*.

Type	Displays *Nutanix*.
Name	Enter a name for the connector.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.
Update Interval(s)	Specify how often in seconds that the dynamic firewall objects should be updated.
IP	Type the IP address for Nutanix.
Port	Select *Use Default* or *Specify* and enter the desired port.
Username	Enter the Nutanix account username.

Password	Enter your Nutanix account password.
Advanced Options	Click to expand and see advanced options.

4. Click *OK* to save the connector.

To complete the fabric connector setup:

1. Import address names or manually create the dynamic firewall address for the SDN connector. See Importing address names to fabric connectors on page 739 and Configuring dynamic firewall addresses for fabric connectors on page 740.
2. In the policy package in which you will be creating the new policy, create a firewall policy and include the dynamic firewall address objects for the SDN connector. See Create a new firewall policy on page 435.
3. Install the policy package to FortiGate. See Install a policy package on page 419.

   FortiGate communicates with the SDN to dynamically populate the firewall address objects with IP addresses.

Creating OpenStack (Horizon) connector

With FortiManager, you can create a fabric connector for Horizon (OpenStack), and then import address names from Horizon (OpenStack) to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate with Horizon (OpenStack) and dynamically populate the objects with IP addresses.

When you create a fabric connector for Horizon (OpenStack), you are specifying how FortiGate can communicate with Horizon (OpenStack).

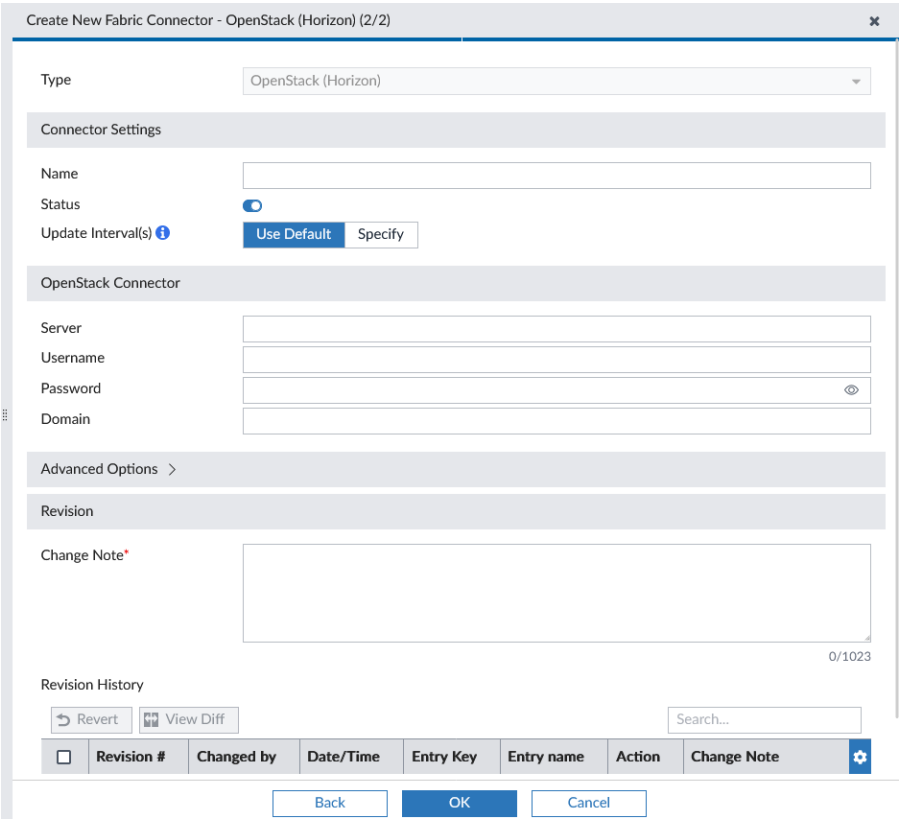
Requirements:

- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with Horizon (OpenStack).

To create a fabric connector object for Horizon (OpenStack):

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.

2. Under *Private SDN*, select *OpenStack*. The *OpenStack (Horizon)* screen is displayed.



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

Type	Displays OpenStack (Horizon).
Name	Type a name for the fabric connector object.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.
Update Interval (s)	Select one of the following options: • Click *Use Default* to use the default interval. • Click *Specify* and specify the interval.
Server	Type the IP address for the server.
User Name	Type the OpenStack Connector administrator user name.
Password	Type the OpenStack Connector administrator password.
Domain	Type the OpenStack Connector Domain.

4. Click *OK* to save the connector.

To complete the fabric connector setup:

1. Import address names or manually create the dynamic firewall address for the SDN connector. See Importing address names to fabric connectors on page 739 and Configuring dynamic firewall addresses for fabric connectors on page 740.

2. In the policy package in which you will be creating the new policy, create a firewall policy and include the dynamic firewall address objects for the SDN connector. See Create a new firewall policy on page 435.
3. Install the policy package to FortiGate. See Install a policy package on page 419.
   FortiGate communicates with the SDN to dynamically populate the firewall address objects with IP addresses.

Creating Oracle Cloud Infrastructure (OCI) connector

With FortiManager, you can create a fabric connector for Oracle Cloud Infrastructure (OCI), and then import address names from OCI to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate with OCI and dynamically populate the objects with IP addresses.

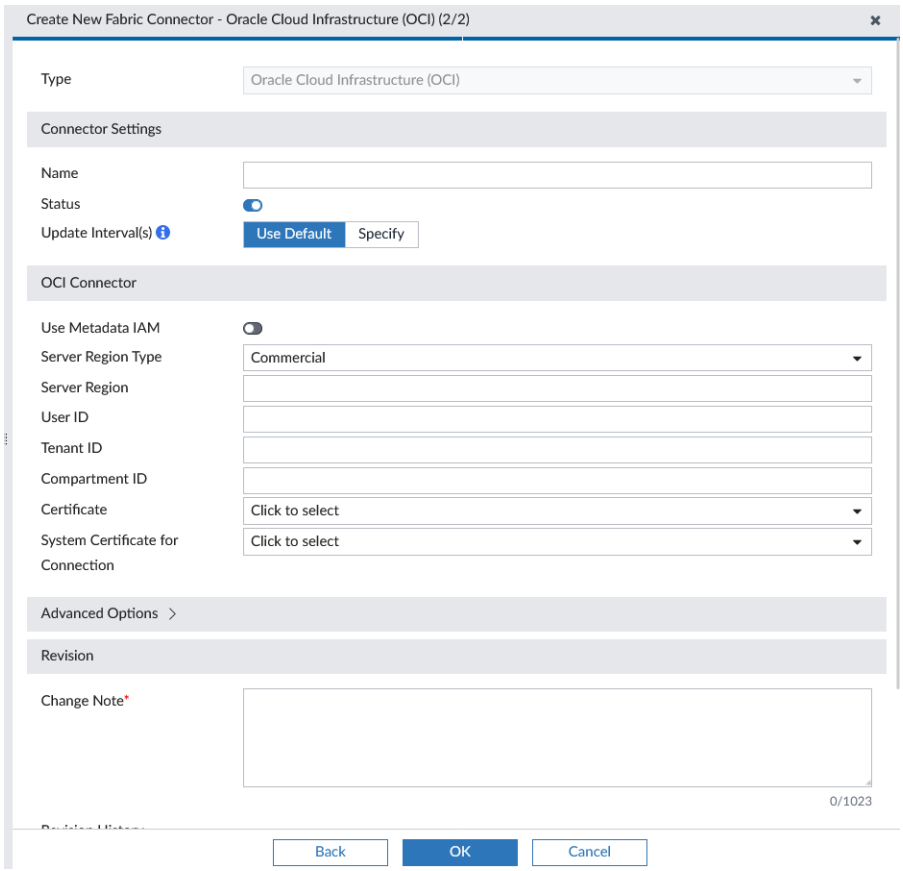
When you create a fabric connector for OCI. you are specifying how FortiGate can communicate with OCI.

Requirements:

- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with OCI.

To create a fabric connector object for Oracle (OCI):

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.
2. Under *Public SDN*, select *Oracle Cloud Infrastructure*. The *Oracle Cloud Infrastructure (OCI)* screen is displayed.



3. Configure the following options, and then click *OK*:

Type	Displays Oracle Cloud Infrastructure (OCI).
Name	Type a name for the fabric connector object.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.
Update Interval (s)	Select one of the following options: • Click *Use Default* to use the default interval. • Click *Specify* and specify the interval.
Server Region	Select the OCI Server Region from the drop-down.
User ID	Type the OCI User ID.
Tenant ID	Type the OCI Tenant ID.
Compartment ID	Type the OCI Compartment ID.
Certificate	Select the OCI Certificate from the drop-down.
System Certificate for Connection	Select the system certificate for the connection.

4. Click *OK* to save the connector.

To complete the fabric connector setup:

1. Import address names or manually create the dynamic firewall address for the SDN connector. See Importing address names to fabric connectors on page 739 and Configuring dynamic firewall addresses for fabric connectors on page 740.
2. In the policy package in which you will be creating the new policy, create a firewall policy and include the dynamic firewall address objects for the SDN connector. See Create a new firewall policy on page 435.
3. Install the policy package to FortiGate. See Install a policy package on page 419.
   FortiGate communicates with the SDN to dynamically populate the firewall address objects with IP addresses.

Creating VMWare ESXi connector

With FortiManager, you can create a VMWare ESXi fabric connector to import address names and objects from VMWare ESXi and vCenter servers that can be used create dynamic objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate with VMWare ESXi and dynamically populate the dynamic address objects.

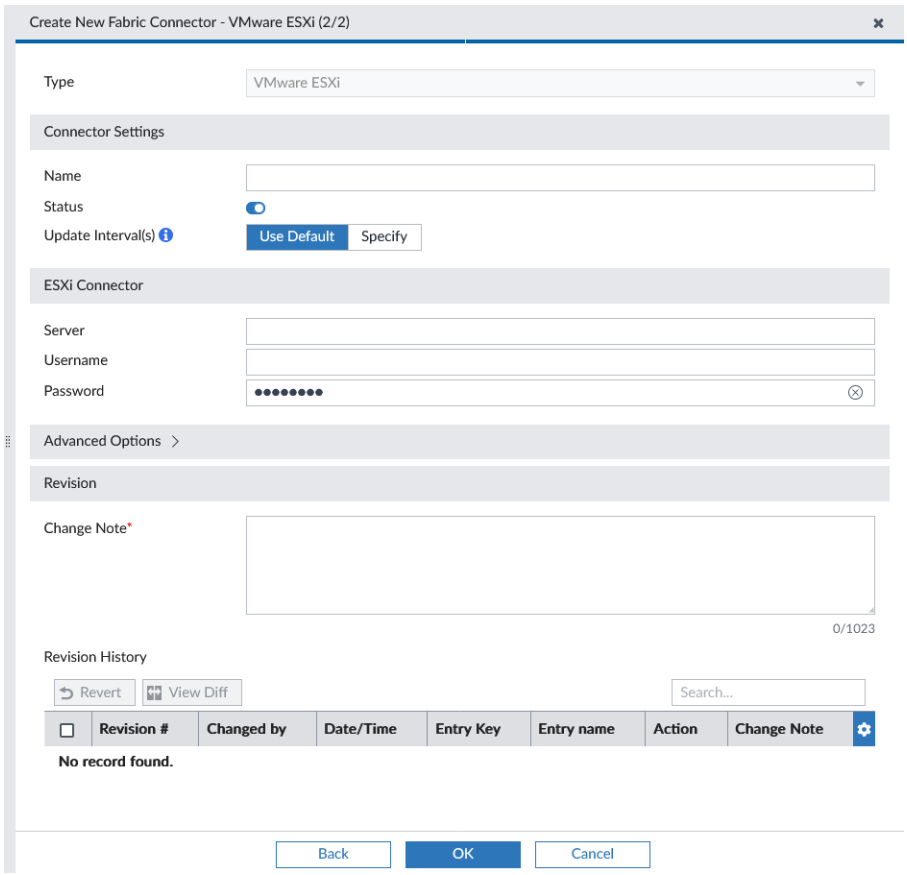
When you create a fabric connector for VMWare ESXi, you are specifying how FortiGate can communicate directly with VMWare ESXi/vCenter.

Requirements:

- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with VMWare ESXi/vCenter.

To create a VMWare ESXi fabric connector:

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.
2. Under *Private SDN*, select *VMWare ESXi*. The *VMWare ESXi* screen is displayed.



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

Type		Displays VMWare ESXi.
Connector Settings		
	Name	Type a name for the fabric connector object.
	Update Interval (s)	Select one of the following options: • Click *Use Default* to use the default interval. • Click *Specify* and specify the interval.
	Verify Certificate	Toggle *On* to enable certificate verification.
ESXi Connector		
	Server	Type the IP address for VMWare ESXi/vCenter.
	User Name	Type the VMWare ESXi/vCenter user name.
	Password	Type the VMWare ESXi/vCenter password.

4. Click *OK* to save the connector.

To complete the fabric connector setup:

1. Import address names/objects or manually create the dynamic firewall address for the SDN connector. See Importing address names to fabric connectors on page 739 and Configuring dynamic firewall addresses for

fabric connectors on page 740.

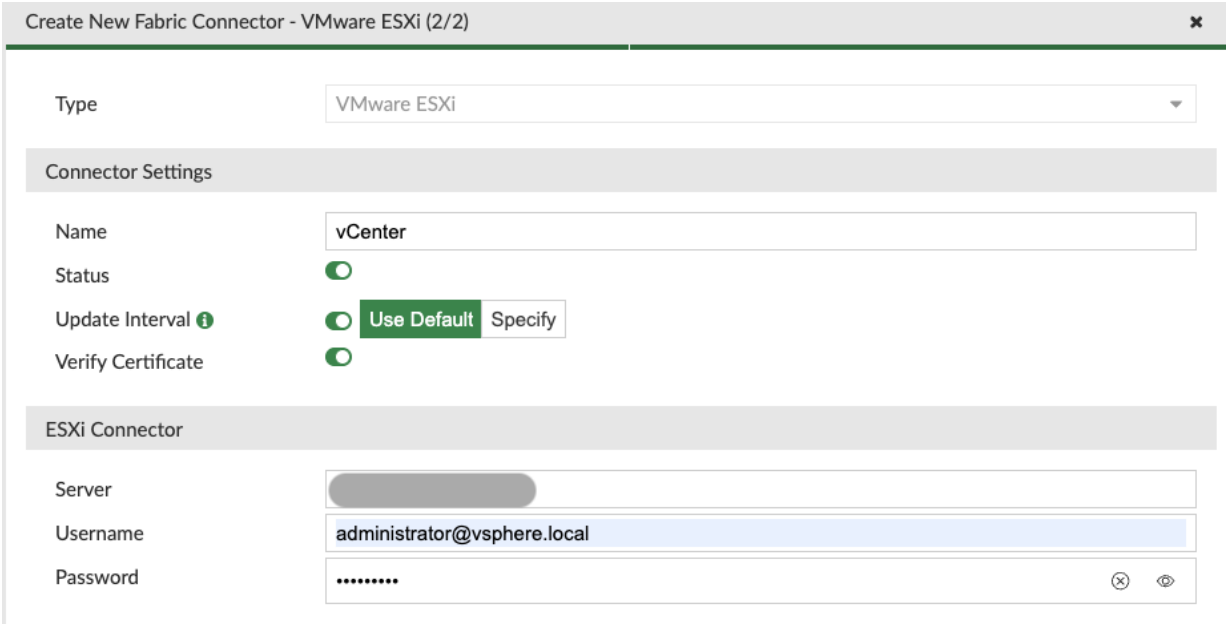
2. In the policy package in which you will be creating the new policy, create a firewall policy and include the dynamic objects for the SDN connector. See Create a new firewall policy on page 435.
3. Install the policy package to FortiGate. See Install a policy package on page 419.

   FortiGate communicates with the SDN to dynamically populate the firewall addresses/objects with IP addresses.

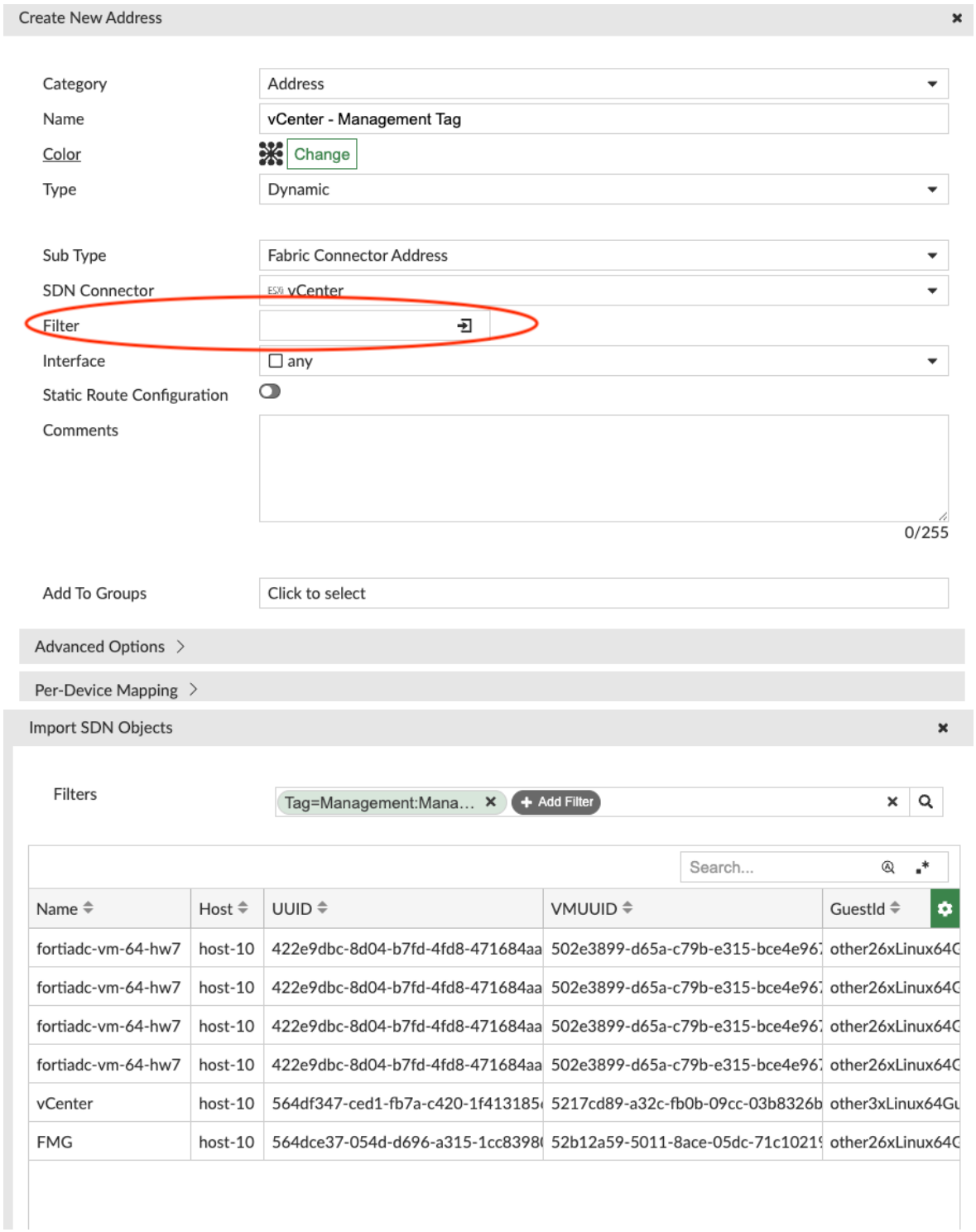
Example: Creating firewall policies using vCenter tags

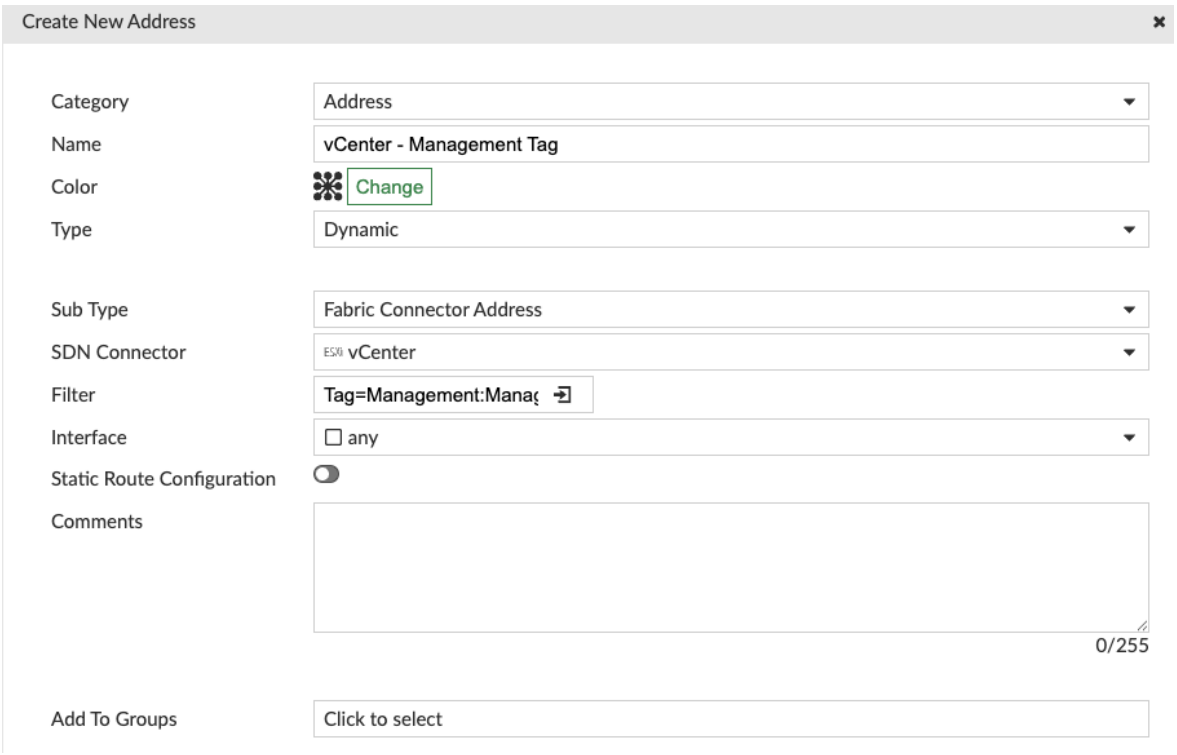
One use case for the FortiManager VMware ESXi connector is to leverage vCenter tags used to identify and classify virtual machines for use in firewall policies.

1. On FortiManager, go to *Fabric View* > *External Connectors*, and create a new *VMware ESXi* connector.
2. Configure the connector to point to the vCenter server:
   - **Server**: Enter the IP address for the vCenter server.
   - **Username/Password**: vCenter credentials.

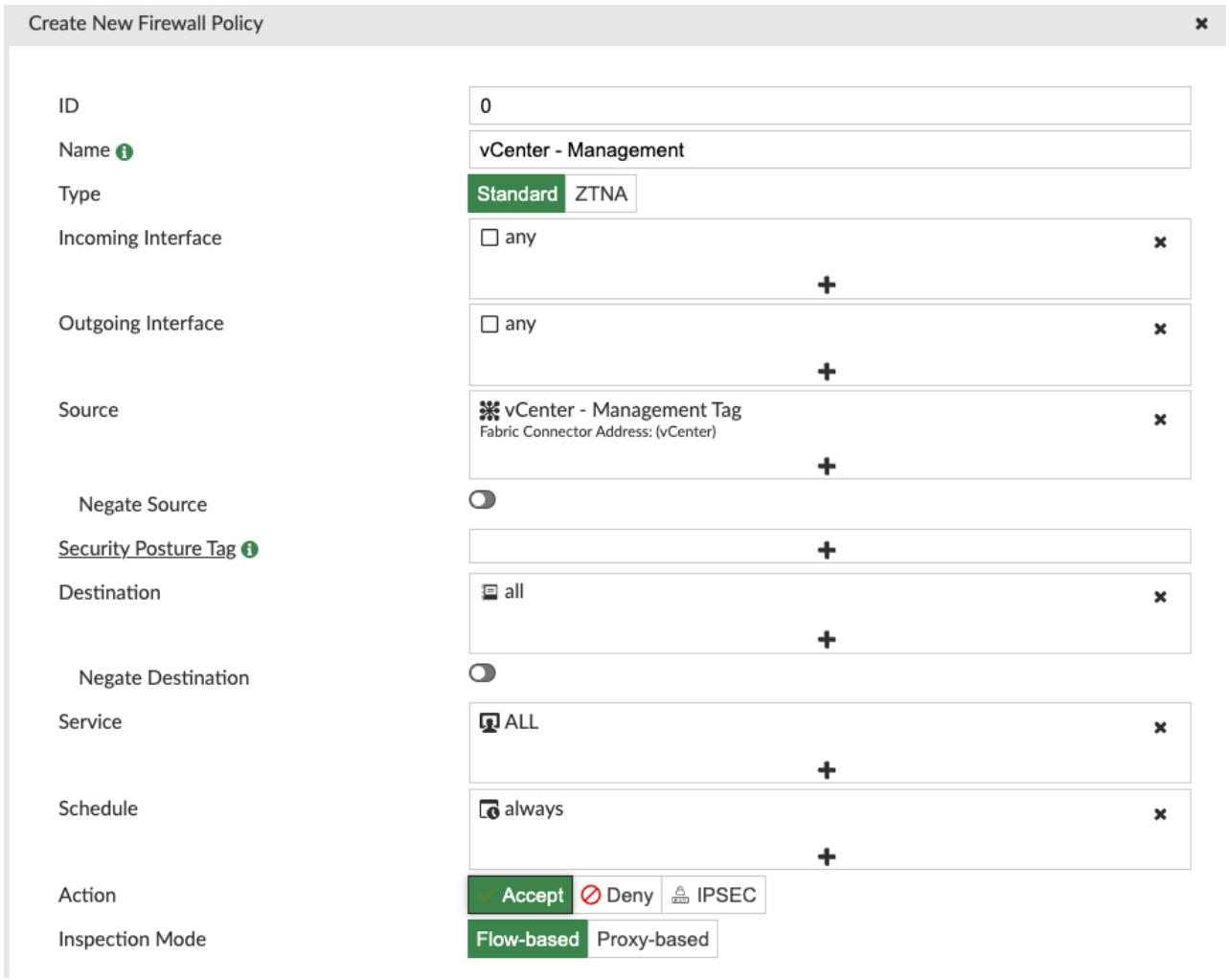


3. Create a dynamic firewall object based on the vCenter tag. This object will dynamically resolve to all VMs in the vCenter with the specified tag.
   a. Go to *Policy & Objects* > *Firewall Objects* and click *Create New* > *Address*.
   b. Configure the following, and then save the dynamic address object:
      - **Type**: *Dynamic*.
      - **Sub Type**: *Fabric Connector Address*.
      - **SDN Connector**: Select the previously configured VMWare ESXi connector.
      - **Filter**: Click the entry field and then enter your desired vCenter tag.

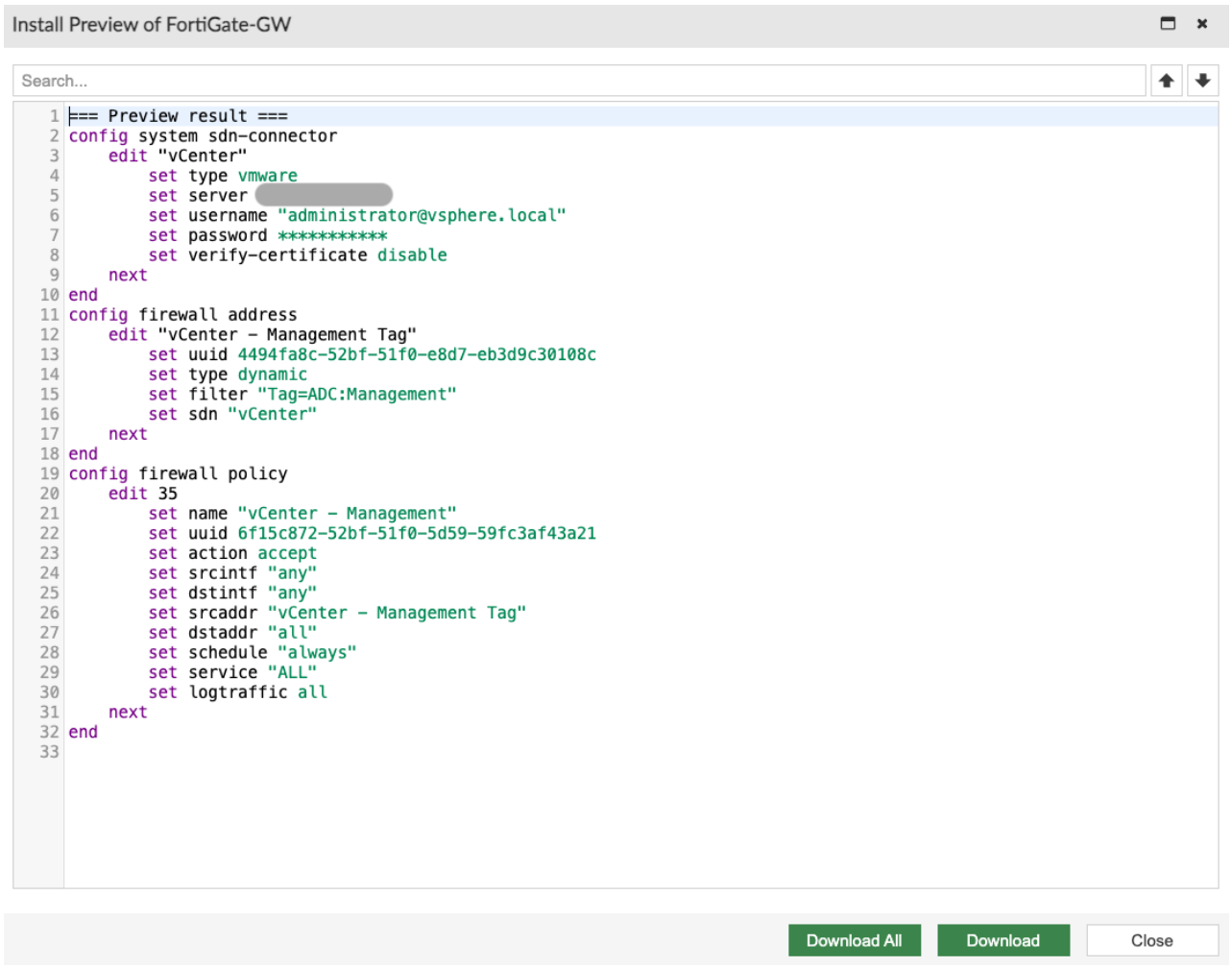

Create New Address
Category
Address
Name
vCenter - Management Tag
Color
Change
Type
Dynamic
Sub Type
Fabric Connector Address
SDN Connector
vCenter
Filter
Interface
any
Static Route Configuration
Comments
0/255
Add To Groups
Click to select
Advanced Options
Per-Device Mapping
Import SDN Objects
Filters
Tag=Management:Mana...
Add Filter
Search...
Name
Host
UUID
VMUUID
GuestId
fortiadc-vm-64-hw7 host-10 422e9dbc-8d04-b7fd-4fd8-471684aa 502e3899-d65a-c79b-e315-bce4e967 other26xLinux64C
fortiadc-vm-64-hw7 host-10 422e9dbc-8d04-b7fd-4fd8-471684aa 502e3899-d65a-c79b-e315-bce4e967 other26xLinux64C
fortiadc-vm-64-hw7 host-10 422e9dbc-8d04-b7fd-4fd8-471684aa 502e3899-d65a-c79b-e315-bce4e967 other26xLinux64C
fortiadc-vm-64-hw7 host-10 422e9dbc-8d04-b7fd-4fd8-471684aa 502e3899-d65a-c79b-e315-bce4e967 other26xLinux64C
vCenter host-10 564df347-ced1-fb7a-c420-1f413185 5217cd89-a32c-fb0b-09cc-03b8326b other3xLinux64Gu
FMG host-10 564dce37-054d-d696-a315-1cc8398 52b12a59-5011-8ace-05dc-71c1021 other26xLinux64C



4. Create a Firewall Policy that includes the dynamic firewall object.



5. Install the policy to FortiGate(s).
   The SDN Connector and firewall addresses required to support tags matching are created on the FortiGate.
   The FortiGate maintains a connection to vCenter, allowing dynamic addresses associated with the vCenter server to update automatically.



Creating Kubernetes connector

With FortiManager, you can create a fabric connector for Kubernetes, and then import address names from Kubernetes to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate with Kubernetes and dynamically populate the objects with IP addresses.

When you create a fabric connector for Kubernetes, you are specifying how FortiGate can communicate directly with Kubernetes.

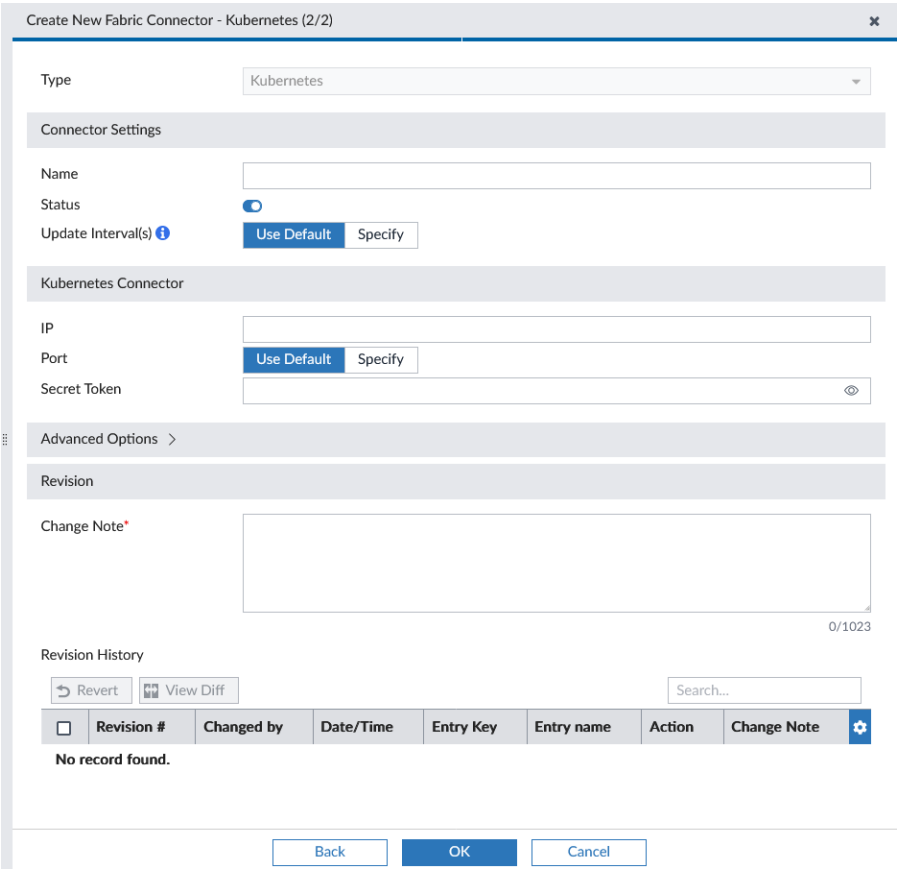
Requirements:

- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with Kubernetes.

To create a fabric connector object for Kubernetes:

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.

2. Under *Private SDN*, select *Kubernetes*. The *Kubernetes* screen is displayed.



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

Type	Displays Kubernetes.
Name	Type a name for the fabric connector object.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.
Update Interval (s)	Select one of the following options: • Click *Use Default* to use the default interval. • Click *Specify* and specify the interval.
IP	Type the IP address for Kubernetes.
Port	Select one of the following options: • Click *Use Default* to use the default port. • Click *Specify* and specify the port.
Secret Token	Specify a secret token.

4. Click *OK* to save the connector.

To complete the fabric connector setup:

1. Import address names or manually create the dynamic firewall address for the SDN connector. See Importing address names to fabric connectors on page 739 and Configuring dynamic firewall addresses for fabric connectors on page 740.
2. In the policy package in which you will be creating the new policy, create a firewall policy and include the dynamic firewall address objects for the SDN connector. See Create a new firewall policy on page 435.
3. Install the policy package to FortiGate. See Install a policy package on page 419.
   FortiGate communicates with the SDN to dynamically populate the firewall address objects with IP addresses.



Kubernetes Service must be enabled on the server side for AWS, Azure, OCI and, GCP for Kubernetes to function for the particular cloud platform. Once the service is enabled, Kubernetes can be configured for the particular cloud platform on FortiManager.

Creating AliCloud Service connector

With FortiManager, you can create a fabric connector for AliCloud Service, and then import address names from AliCloud Service to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate with AliCloud Service and dynamically populate the objects with IP addresses.

When you create a fabric connector for AliCloud Service, you are specifying how FortiGate can communicate directly with AliCloud Service.

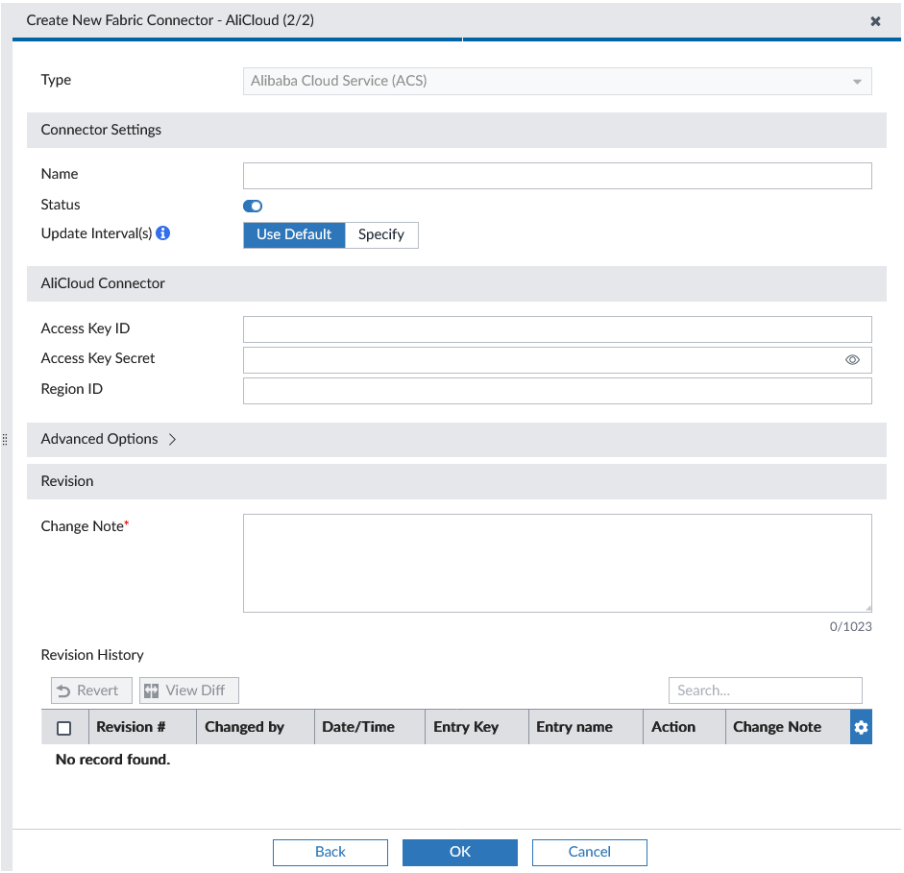
Requirements:

- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with AliCloud Service.

To create a fabric connector object for Alibaba Cloud Service:

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.

2. Under *Public SDN*, select *AliCloud*. The *Alibaba Cloud* screen is displayed.



3. Configure the following options, and then click *OK*:

Type	Displays Alibaba Cloud Service (ACS).
Name	Type a name for the fabric connector object.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.
Update Interval (s)	Select one of the following options: • Click *Use Default* to use the default interval. • Click *Specify* and specify the interval.
AccessKey ID	Specify the AccessKey ID for AliCloud.
AccessKey Secret	Specify the AccessKey Secret for AliCloud.
Region ID	Specify the Region ID.

4. Click *OK* to save the connector.

To complete the fabric connector setup:

1. Import address names or manually create the dynamic firewall address for the SDN connector. See Importing address names to fabric connectors on page 739 and Configuring dynamic firewall addresses for fabric connectors on page 740.

2. In the policy package in which you will be creating the new policy, create a firewall policy and include the dynamic firewall address objects for the SDN connector. See Create a new firewall policy on page 435.
3. Install the policy package to FortiGate. See Install a policy package on page 419.
   FortiGate communicates with the SDN to dynamically populate the firewall address objects with IP addresses.

Creating Google Cloud Platform connector

With FortiManager, you can create a fabric connector for Google Cloud Platform (GCP), and then import address names from GCP to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate with GCP and dynamically populate the objects with IP addresses.

When you create a fabric connector for GCP, you are specifying how FortiGate can communicate directly with GCP.

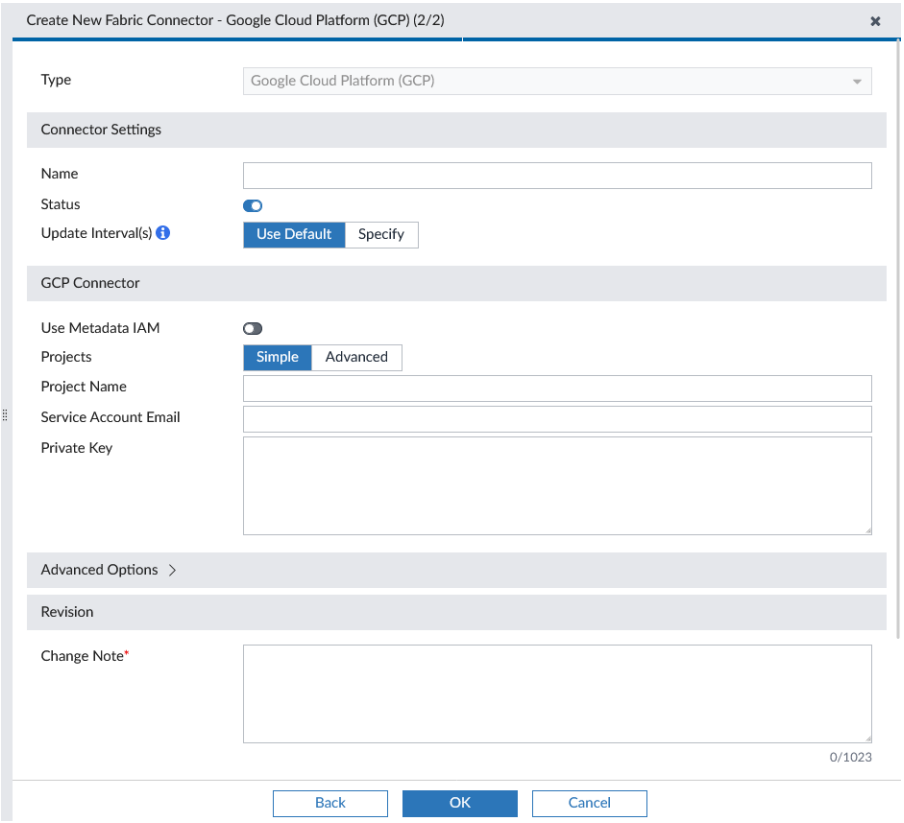
Requirements:

- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with Google Cloud Platform.

To create a fabric connector object for Google Cloud Platform:

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.

2. Under *Public SDN*, select *Google Cloud Platform*. The *Google Cloud Platform* screen is displayed.



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

Type	Displays Google Cloud Platform (GCP).
Name	Type a name for the fabric connector object.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.
Update Interval (s)	Select one of the following options: • Click *Use Default* to use the default interval. • Click *Specify* and specify the interval.
Projects	Select *Simple* or *Advanced*. When *Advanced* is selected, you can add *GCP Projects*.
Project Name	Specify the Project Name for the GCP.
Service Account Email	Specify the Service Account Email for GCP.
Private Key	Specify the Private Key.

4. Click *OK* to save the connector.

To complete the fabric connector setup:

1. Import address names or manually create the dynamic firewall address for the SDN connector. See Importing address names to fabric connectors on page 739 and Configuring dynamic firewall addresses for

fabric connectors on page 740.

2. In the policy package in which you will be creating the new policy, create a firewall policy and include the dynamic firewall address objects for the SDN connector. See Create a new firewall policy on page 435.
3. Install the policy package to FortiGate. See Install a policy package on page 419.
   FortiGate communicates with the SDN to dynamically populate the firewall address objects with IP addresses.

Creating IBM Cloud connector

With FortiManager, you can create a fabric connector for IBM Cloud, and then import address names from IBM Cloud to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate with IBM Cloud and dynamically populate the objects with IP addresses.

When you create a fabric connector for IBM Cloud, you are specifying how FortiGate can communicate directly with IBM Cloud.

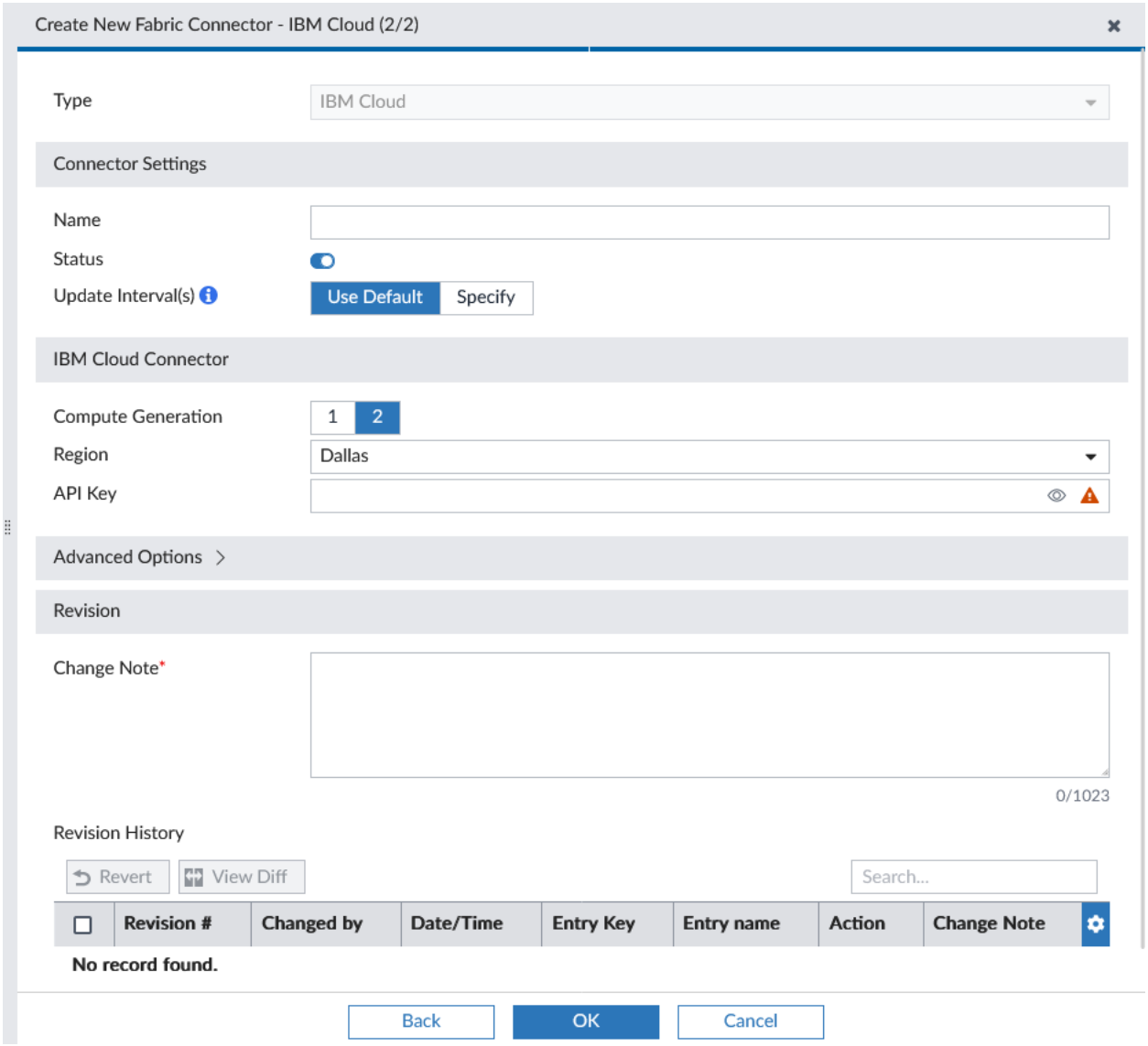
Requirements:

- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with IBM Cloud.

To create an IBM Cloud fabric connector:

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.

2. Under *Private SDN*, select *IBM Cloud*. The *IBM Cloud* screen is displayed.



3. Configure the following options, and then click *OK*.

Type	Displays *IBM Cloud*.
Name	Enter a name for the connector.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.
Update Interval(s)	Specify how often in seconds that the dynamic firewall objects should be updated.
Compute Generation	Specify the IBM Cloud computer generation.
Region	Select your IBM Cloud region from the dropdown list.
API Key	Enter your IBM Cloud API key.

4. Click *OK* to save the connector.

To complete the fabric connector setup:

1. Import address names or create a dynamic firewall address for the IBM Cloud connector.
   See Importing address names to fabric connectors on page 739 and Configuring dynamic firewall addresses for fabric connectors on page 740.
2. In the policy package in which you will be creating the new policy, create a firewall policy and include the dynamic firewall address objects for IBM Cloud. See Create a new firewall policy on page 435.
3. Install the policy package to FortiGate. See Install a policy package on page 419.
   FortiGate communicates with IBM Cloud to dynamically populate the firewall address objects with IP addresses.

Importing address names to fabric connectors

After you configure a fabric connector, you can import address names from products, such as ACI, to the fabric connector, and dynamic firewall address objects are automatically created.

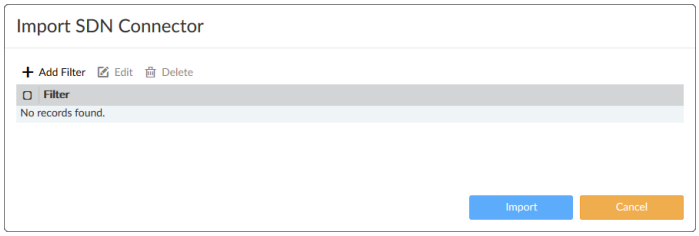
When you are importing address names, you must add filters to display the correct instances before importing address names.



You can manually create dynamic firewall address objects for SDN fabric connectors. See Configuring dynamic firewall addresses for fabric connectors on page 740.

To import address names for SDN connectors:

1. Go to *Policy & Objects* > *Security Fabric* > *SDN Connectors*.
2. In the content pane, right-click the fabric connector, and select *Import*.
   The *Import SDN Connector* dialog box is displayed.



3. If your connect supports both IPv4 and IPv6, you can select the *Address Type*.
4. Create a filter to select the correct instances:
   a. Click *Add Filter*.
      The *Filter Generator* dialog box is displayed.



b. Click *Add Filter*, and select a filter. A filtered list of instances is displayed.
c. Click *OK*. The *Import SDN Connector* dialog box is displayed, and it contains the filter. You can add additional filters, or edit and delete filters.
d. (Optional) Repeat this procedure to add additional filters.

5. Select the filters, and click *Import*.

   The address names are imported and converted to dynamic firewall address objects that are displayed on the *Firewall Objects* > *Addresses* pane. The name of the dynamic firewall address uses the following naming convention: `<SDN Type>-<random identifier>`. Use the *Details* column and the instance ID to identify the object.

Import by endpoint groups

You can import SDN objects from ACI connectors by endpoint group (EGP). In order to import SDN objects from ACI connectors by EPG, you must have configured your ACI connector with the *Type: Direct Connection*. See Creating ACI fabric connectors on page 708.

To import by endpoint groups (EPGs) for ACI connectors:

1. Go to *Policy & Objects* > *Security Fabric* > *SDN Connector*
2. In the content pane, right-click the ACI fabric connector under Private SDN Connector, and select *Import*. The *Import SDN Connector* dialog box is displayed.
3. Once the import function has loaded all of the objects, you can choose the *Import Mode*. Select *By EPG* to import SDN objects by endpoint group.
4. You can create address objects from *Policy & Objects* > *Firewall Objects* and use the address in a Policy Package, similar to other SDN connectors.

Configuring dynamic firewall addresses for fabric connectors

You can create dynamic firewall objects that can be dynamically populated when FortiGate communicates with the SDN platform.

To configure dynamic firewall addresses using SDN connectors:

1. Go to *Policy & Objects* > *Firewall Objects*.
2. In the content pane, click *Create New* and select *Address*.
3. Configure the firewall address settings for your chosen fabric connector:

Category	Select *Address*.
Name	Type a name for the firewall address object.
Type	Select *Dynamic*.
Sub Type	Select *Fabric Connector Address*.
SDN Connector	Select the fabric connector.

4. Configure the remaining settings as needed, and click *OK*.

To configure dynamic IPv6 firewall addresses using SDN connectors:

1. Go to *Policy & Objects > Firewall Objects*.
2. In the content pane, click *Create New* and select *Address*.
3. Configure the IPv6 firewall address settings for your chosen fabric connector:

Category	Select *IPv6 Address*.
Name	Type a name for the firewall address object.
Type	Select *IPv6 Fabric Connector Address*.
SDN	Select a fabric connector that supports IPv6 addresses. For example, Cisco ACI.

4. Configure the remaining settings as required, and click *OK*.

Configuring virtual wire pairs

Before you create a virtual wire pair policy, you must create a virtual wire pair.

To configure virtual wire pairs:

1. Go to *Policy & Objects > Object Configurations*.
2. In the tree menu, go to *Normalized Interface > Virtual Wire Pair*.
3. In the content pane, click *Create New*.
4. Complete the following options, and click *OK*.

Name	Type a name for the virtual wire pair.
Interface Members	Select two interface members.
Wildcard VLAN	Toggle *ON* to enable wildcard VLANs for the virtual wire pair. When enabled, all VLAN-tagged traffic can pass through the virtual wire pair, if allowed by the virtual wire pair firewall policies. Toggle *OFF* to disable wildcard VLANs for the virtual wire pair.

Using FortiManager as a SDN proxy for AWS connectors

Each FortiGate configured with an AWS fabric connector makes a separate connection request to the AWS server. Having a high volume of devices may result in many simultaneous connections to AWS. For example, having 100 FortiGate devices with AWS connectors results in 100 separate connections to the AWS server.

To improve efficiency and security in these cases, FortiManager can be configured to work as a proxy between the FortiGate devices and AWS. When configured as a proxy, FortiManager will make all requests to the AWS server. The FortiGate devices do not need to be managed by FortiManager to use it as a proxy.

This setting can only be configured in the CLI.

When using FortiManager as a proxy to AWS, you must have an admin user on FortiManager with read-write permissions for JSON API Access. It is recommended that you also increase the login-max setting in *Advanced Options* to allow for the maximum number of logins (256) for the user since this FortiManager will receive login requests from each FortiGate when making requests to the AWS server.

To configure FortiManager as proxy to AWS:

1. On each FortiGate, configure the SDN-Proxy object.

```
config system sdn-proxy
   edit <sdn-proxy name>
      set type fortimanager
      set server <FortiManager address>
      set username <username>
      set password <password>
next
```

2. On each FortiGate, configure the SDN connector to use the FortiManager proxy object.

```
config system sdn-connector
   edit <connector name>
      set proxy <sdn-proxy name>
      set use-metadata-iam disable
      set access-key <access>
      set secret-key <secret>
      set region <region>
   next
end
```

On FortiManager, you can manage the sdnproxy daemon with the following commands:

- **Restart the sdnproxy daemon**: `diagnose test application sdnproxyd <interger>`
- **Show debug logs**: `diagnose debug application sdnproxy <debug level (0 - 8)>`

Using FortiManager as a SDN proxy for GCP connectors

Each FortiGate configured with a GCP fabric connector makes a separate connection request to the GCP server. Having a high volume of devices may result in many simultaneous connections to GCP. For example, having 100 FortiGate devices with GCP connectors results in 100 separate connections to the GCP server.

To improve efficiency and security in these cases, FortiManager can be configured to work as a proxy between the FortiGate devices and GCP. When configured as a proxy, FortiManager will make all requests to the GCP server. The FortiGate devices do not need to be managed by FortiManager to use it as a proxy.

This setting can only be configured in the CLI.

When using FortiManager as a proxy to GCP, you must have an admin user on FortiManager with read-write permissions for JSON API Access. It is recommended that you also increase the login-max setting in *Advanced Options* to allow for the maximum number of logins (256) for the user since this FortiManager will receive login requests from each FortiGate when making requests to the GCP server.

To configure FortiManager as a proxy to GCP:

1. On each FortiGate, configure the SDN-Proxy object.
```
config system sdn-proxy
   edit <sdn-proxy name>
      set type fortimanager
      set server <FortiManager address>
      set username <username>
      set password <password>
next
```
2. On each FortiGate, configure the SDN connector to use the FortiManager proxy object.
```
config system sdn-connector
   edit <connector name>
      set proxy <sdn-proxy name>
      set use-metadata-iam disable
      set access-key <access>
      set secret-key <secret>
      set region <region>
   next
end
```

On FortiManager, you can manage the sdnproxy daemon with the following commands:

- **Restart the sdnproxy daemon**: `diagnose test application sdnproxyd <interger>`
- **Show debug logs**: `diagnose debug application sdnproxy <debug level (0 - 8)>`

Using FortiManager as a SDN proxy for Azure connectors

Each FortiGate configured with an Azure fabric connector makes a separate connection request to the Azure server. Having a high volume of devices may result in many simultaneous connections to Azure. For example, having 100 FortiGate devices with Azure connectors results in 100 separate connections to the Azure server.

To improve efficiency and security in these cases, FortiManager can be configured to work as a proxy between the FortiGate devices and Azure . When configured as a proxy, FortiManager will make all requests to the Azure server. The FortiGate devices do not need to be managed by FortiManager to use it as a proxy.

This setting can only be configured in the CLI.



When using FortiManager as a proxy to Azure, you must have an admin user on FortiManager with read-write permissions for JSON API Access. It is recommended that you also increase the login-max setting in Advanced Options to allow for the maximum number of logins (256) for the user since this FortiManager will receive login requests from each FortiGate when making requests to the Azure server.

To configure FortiManager as a proxy to Azure:

1. On each FortiGate, configure the SDN-Proxy object.
```
config system sdn-proxy
   edit <sdn-proxy name>
      set type fortimanager
      set server <FortiManager address>
      set username <username>
      set password <password>
```

```
next
```

2. On each FortiGate, configure the SDN connector to use the FortiManager proxy object.

```
config system sdn-connector
   edit <connector name>
      set proxy <sdn-proxy name>
      set use-metadata-iam disable
      set access-key <access>
      set secret-key <secret>
      set region <region>
   next
end
```

On FortiManager, you can manage the sdnproxy daemon with the following commands:

- **Restart the sdnproxy daemon**: `diagnose test application sdnproxyd <interger>`
- **Show debug logs**: `diagnose debug application sdnproxy <debug level (0 - 8)>`

Threat Feeds

You can use the *Fabric View* > *External Connectors* pane to create the following types of threat feed connectors:

- FortiGuard Category Threat Feed
- IP Address Threat Feed
- Domain Name Threat Feed
- Malware Hash Threat Feed
- MAC Address Threat Feed

Threat feed connectors dynamically import an external block list. The block list is a text file that contains a list of either addresses or domains and resides on an HTTP server. You use block lists to deny access to source or destination IP addresses in web filter and DNS filter profiles, SSL inspection exemptions, and as sources or destinations in proxy policies.

This section contains the following topic:

- Creating threat feed connectors on page 744

Creating threat feed connectors

You can create threat feed connectors for FortiGuard categories, firewall IP addresses, domain names, and malware hashes.

To create threat feed connectors:

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.
2. Under *Threat Feeds*, select *FortiGuard Category*, *IP Address*, *Domain Name*, or *Malware Hash*, and click *Next*.
3. Configure the following options, and then click *OK*:

Name	Type a name for the fabric connector object.
URI of external resource	Type the link to an external text file. The path must start with `http://`, `https://`, or `fmg://`, for example, `http://example.com/url`.  When using FortiManager hosted resources (`fmg://`) you must configure the resource file as FortiManager external resource first. See External resources on page 810.
HTTP Basic Authentication	Toggle *On* to enable basic HTTP authentication, and type a username and password. Toggle *Off* to disable basic HTTP authentication.
Category ID	Type the category ID. The ID is between 192 and 221. Available only when *Type* displays *Domain List*.
Refresh Rate	The time in minutes to refresh the external resource.
Comments	(Optional) Type comments about the connector.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.
Update Method	Select the update method: • *External Feed*: The threat feed will periodically fetch entries from the URI using HTTP or HTTPS. • *Push API*: The threat feed receives entry updates from webhook requests to the FortiGate REST API.

Endpoint/Identity

You can use the *Fabric > External Connectors* pane to create the following types of Endpoint/Identity connectors:

- Poll Active Directory Server
- Fortinet Single Sign-On (FSSO) Agent
- RADIUS Single Sign-On Agent
- User pxGrid
- User ClearPass
- VMware NSX-T
- VMware vCenter
- Symantec Endpoint Protection
- Exchange Server
- JSON API Connector

SSO connectors integrate single sign-on (SSO) authentication in networks. SSO allows users to enter their credentials once and have those credentials reused when they access other network resources through FortiGate.

This section contains the following topics:

- Creating Active Directory connectors on page 746
- Creating FSSO connectors on page 746
- Creating RADIUS connectors on page 747
- Creating Cisco pxGrid connectors on page 748
- Creating ClearPass connectors on page 755
- Creating VMware NSX-T connectors on page 769
- Creating VMware vCenter connectors on page 776
- Creating JSON API connectors on page 780

Creating Active Directory connectors

You can create SSO/identity connectors for Active Directory servers. This connector configures polling of Active Directory servers for FSSO.

To create Active Directory connectors:

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.
2. Under *Endpoint/Identity*, select *Poll Active Directory Server*.
3. Configure the following options, and click *OK*:

Server Name/IP	Type the name or IP address for the Active Directory server.
Local User	Type the user name required to log into the Active Directory server.
Password	Type the password required to log into the Active Directory server.
Enable Polling	Toggle *On* to enable polling of the Active Directory server. Toggle *OFF* to disable this feature.
LDAP Server	Select the LDAP server name from the list. The LDAP server name is used in LDAP connection strings.

Creating FSSO connectors

You can create SSO/identity connectors for Fortinet single sign-on (FSSO) agents.

FSSO is the authentication protocol by which users can transparently authenticate to FortiGate, FortiClient EMS, FortiAuthenticator, and FortiCache devices.

To create FSSO connectors:

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.
2. Under *Endpoint/Identity*, select *Fortinet Single Sign-on Agent*.

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

Name	Type a name for the connector object.
Type	Select the FSSO connector type as either *Active Directory / FortiAuthenticator* or *FortiNAC*.
FSSO Agent	Complete the *IP/Name*, *Password*, and *Port* options for each unit that will act as an SSO agent.
User Group Source	Specify whether to get FSSO groups from a *Collector Agents*, *Via FortiGate*, or *Local*.
User Groups	Displays imported FSSO groups from the selected source. This field is only displayed when the *User Group Source* is *Collector Agents* or *Via FortiGate*.
LDAP Server	Select the LDAP server. You can create a new LDAP server by clicking the add icon, or choose an existing LDAP server from the dropdown list. This field is only displayed when the *User Group Source* is *Local*.
Proactively Retrieve from LDAP	(Optional) Toggle this field *On* to proactively retrieve from the LDAP server.
Select LDAP Groups	Select the LDAP groups by choosing *Remote Server* or *Manually Specify*. When *Manually Specify* is selected, you can add each LDAP group in the *Group Name* field. This field is only displayed when the *User Group Source* is *Local*.
SSL	(Optional) Toggle this field *On* to enable SSL encryption. When enabled, the *SSL Trusted Certificate* field is displayed where you can specify the SSL certificate.
Per-Device Mapping	(Optional) Toggle *On* to set per-device mappings between FortiGate units and FSSO agents, and then create the mappings. Toggle *OFF* to disable this feature.
Advanced Options	Expand to view and configure advanced options for Fortinet single sign-on agents. For details, see the *FortiOS CLI Reference*.



When you have an FSSO polling server configured on the FortiManager fabric connector, FortiManager will import and install all *fsso-polling* objects to managed FortiGate devices in the ADOM, including to devices that do not have references to the polling objects in their policies. *user adgrp* objects are also imported and installed if any *fsso-polling* objects are copied.

Creating RADIUS connectors

You can create an SSO/identity connector for RADIUS single sign-on (RSSO) agents. Only one RADIUS connector can exist at one time.

To create RADIUS connectors:

1. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.
2. Under *Endpoint/Identity*, select *RADIUS Single Sign-On Agent*.
3. Configure the following options, and click *OK*:

Name	Type the name of the RADIUS SSO agent.
Use RADIUS Shared Secret	Toggle *On* to enable the use of a RADIUS shared secret between collector agent and RADIUS server, and then enter the shared secret. Toggle *OFF* to disable this feature.
Send RADIUS Responses	Toggle *On* to send RADIUS response packets after receiving start and stop records. Toggle *OFF* to disable this feature.
Advanced Options	Expand to view and configure advanced options for RADIUS single sign-on agents. For details, see the *FortiOS CLI Reference*.

Creating Cisco pxGrid connectors

Cisco pxGrid for FortiManager centralizes the updates from pxGrid for all FortiGate devices, and leverages the efficient FSSO protocol to apply dynamic policy updates to FortiGate.

FortiManager supports ISE distributed deployment including up to two PAN/MnT nodes and up to four Pxgrid nodes.

You can create multiple Cisco pxGrid connectors per ADOM.

Requirements:

- FortiManager version 6.0 ADOM or later.
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with Cisco pxGrid.
- The Cisco ISE server is configured, and the certificate is downloaded.
- pxGrid version 2.0 and ISE version 3.4.

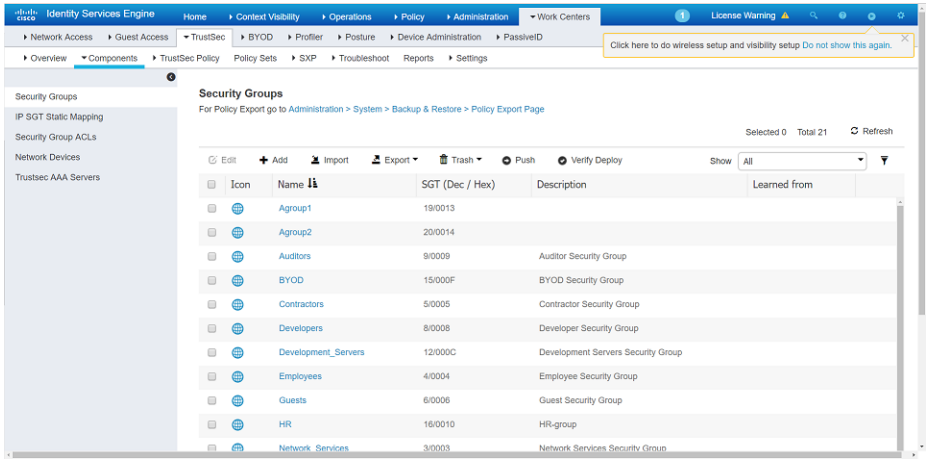


When the pxGrid connector is created, FortiManager will only process events with state "`Started`" or "`Disconnected`". All other Session Statuses possible on ISE, such as "`Authenticated`", are ignored by FortiManager.

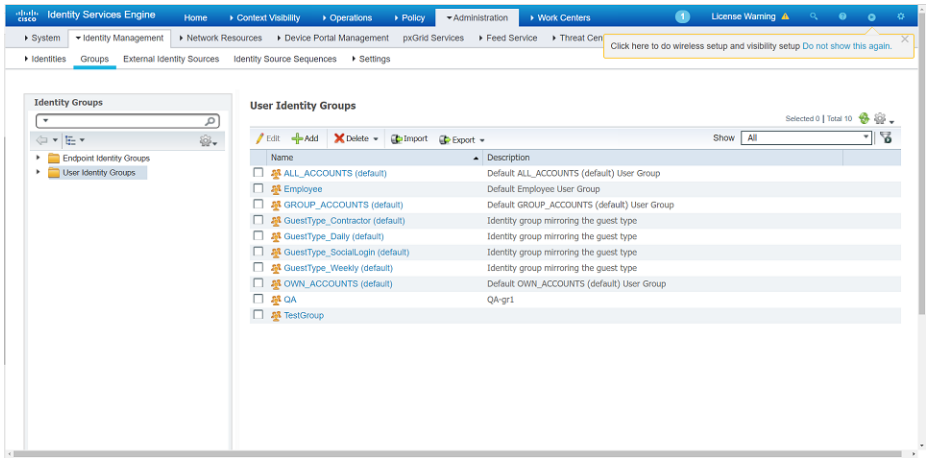
Additionally, a Security Group must be defined. See steps below. Users with null a Security Group are ignored by FortiManager.

To configure Cisco ISE server:

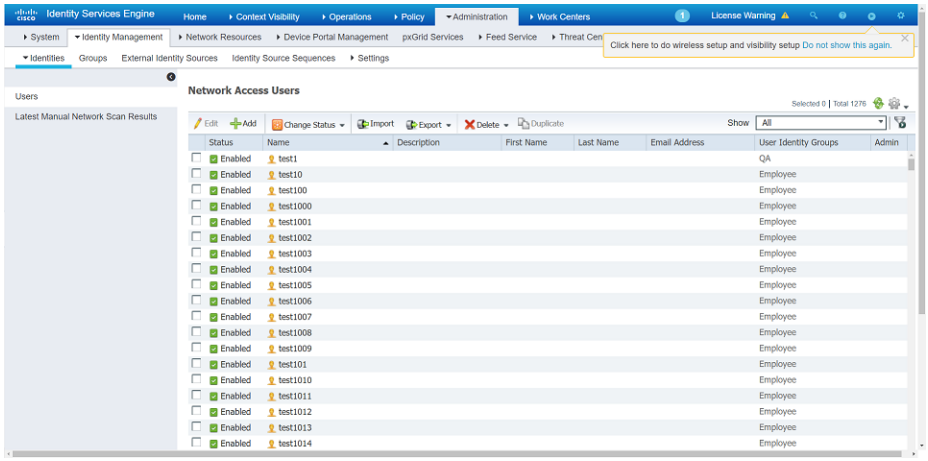
1. Create a Security Group: Go to *ISE > Work Centers > TrustSec > Components > Security Groups*. Click *Add*.



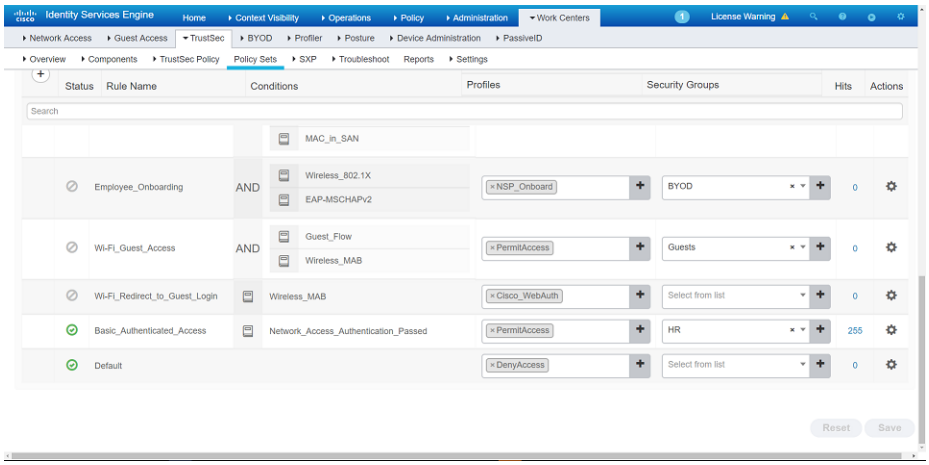
2. Create a User Identity Group: Go to *ISE > Administration > Identity Management > Groups > User Identity Groups*. Click *Add*.



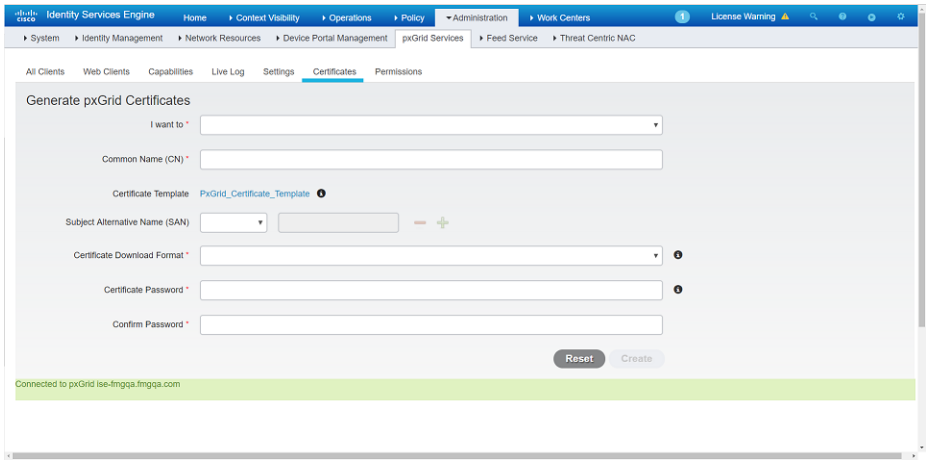
3. Create a user and add it to User Identity Group: Go to *ISE > Administration > Identity Management > Identities*. Click *Add*.



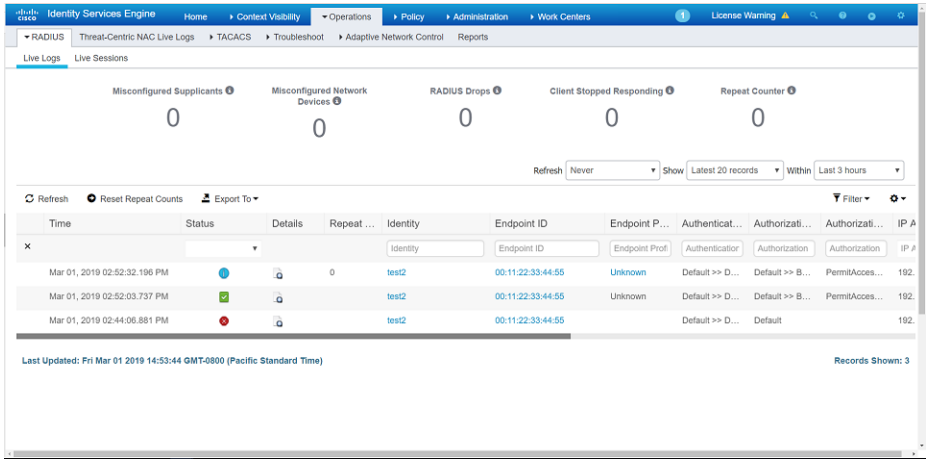
4. Match the Security Group with User Identity Group in the policy: Go to *ISE > Work Centers >TrustSec > Components > Policy Sets*. Right-click and go to *Authorization policy > Basic_Authenticatied _Access* and click *Edit* to match the Security Group with the User Identity Group.



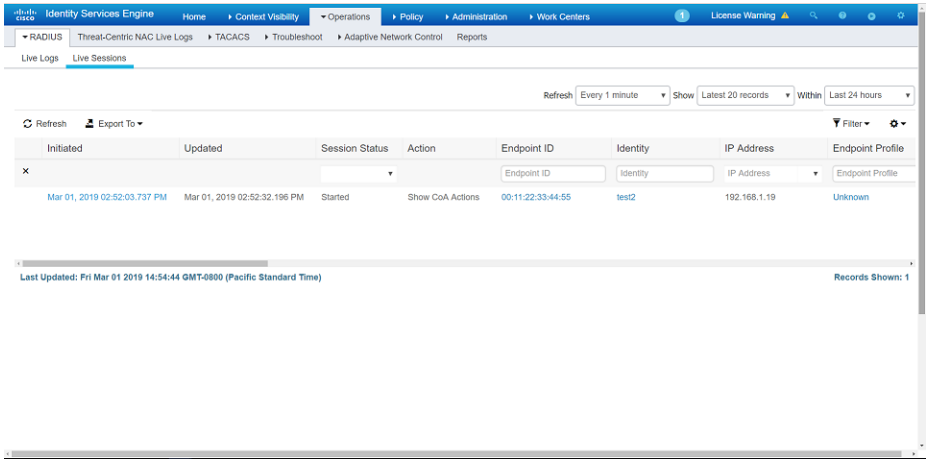
5. Generate the pxGrid certificate and download it to the local computer: Go to *ISE > Administration > pxGrid Services > Certificate* and select *Generate pxGrid Certificates*.



6. See log for current users: Go to *ISE > Operations > RADIUS > Live Logs*.

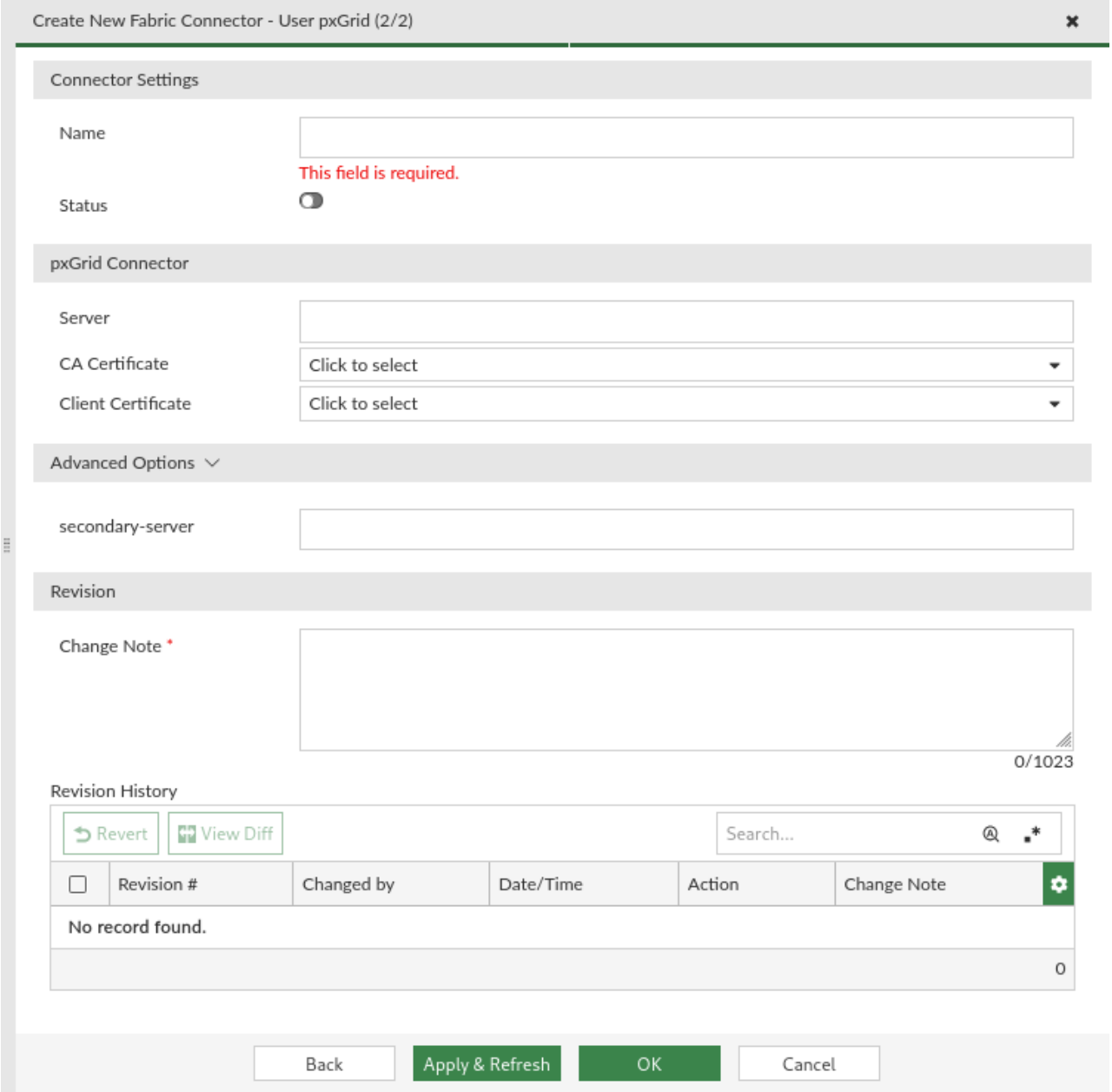


7. See live sessions of current users: Go to *ISE > Operations > RADIUS > Live Sessions*.



To configure FortiManager:

1. Go to *System Settings > Certificates*, and click *Create New/Import > Certificate*. Import the downloaded certificate.
2. Go to *Fabric View > External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.
3. Under *Endpoint/Identity*, select *User pxGrid*.
4. Configure the following options, and click *OK* to create the User pxGrid connector:



Name	Type a name for the fabric connector object.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.
Server	Type the IP address or FQDN of the primary MnT node for Cisco ISE server.
CA Certificate	Select the imported CA Certificate.
Client Certificate	Select the imported Client Certificate.
Advanced Options	Expand to view advanced options.

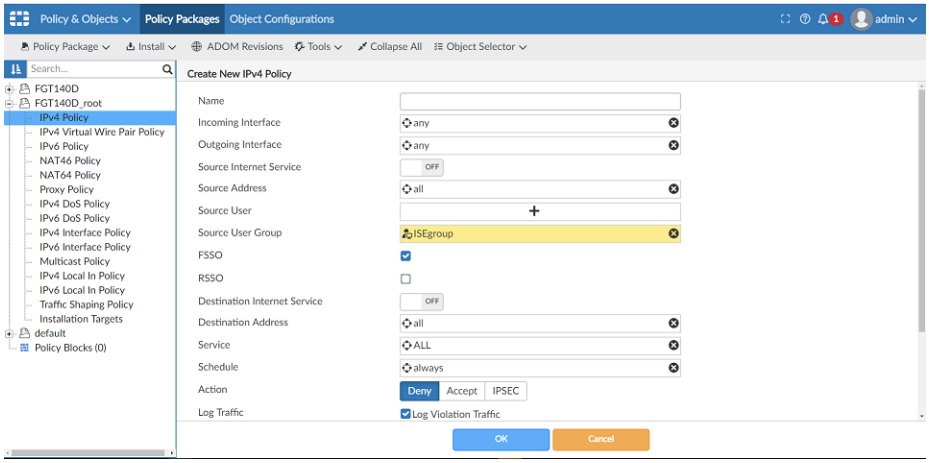
secondary-server	(Optional) Type the IP address or FQDN of the secondary MnT node for Cisco ISE server. FortiManager will try to connect to the IP address specified as the *Server* first, and if it fails, will attempt to connect to this secondary server. FortiManager supports ISE distributed deployment including up to two PAN/MnT nodes and up to four Pxgrid nodes.

You must approve the pending FortiManager in Cisco ISE by going to *Administrator > pxGrid Services > Clients* and selecting and approving the FortiManager.

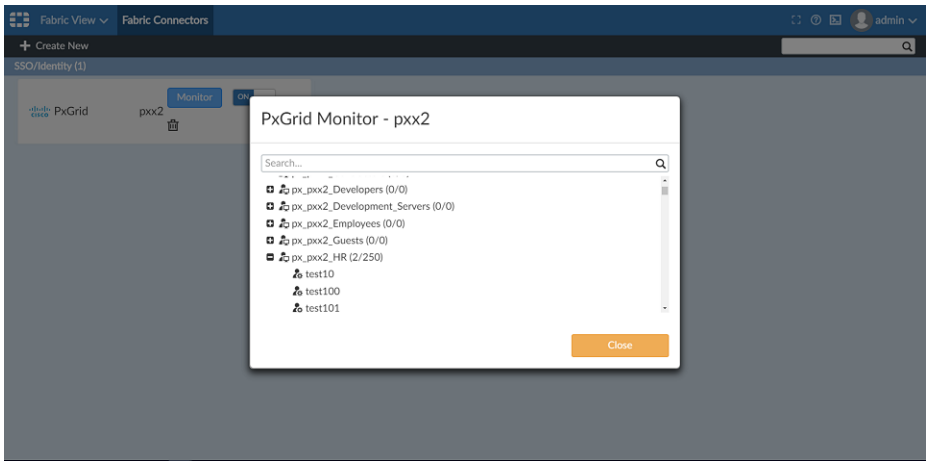
You can enable *Automatically Approve New Accounts* in *Administrator > pxGrid Services > Settings* to automatically approve new certificate-based accounts but you must manually approve any existing FortiManager devices that are pending approval before the feature can be enabled.

For more information about client approval, see the Cisco ISE documentation.

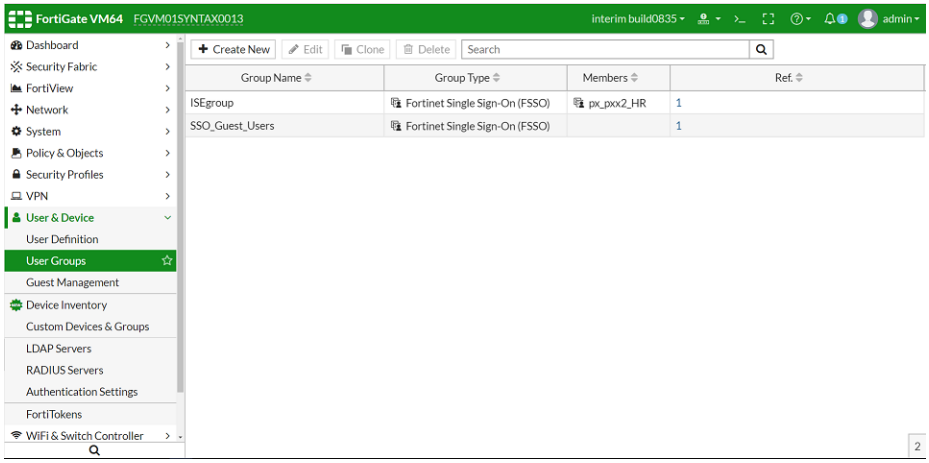
5. Go to *Policy & Objects > Security Fabric > Endpoint/Identity*.
6. Ensure the *Status* of the connector is enabled, then select the connector and click *Import*. The pxGrid connector is imported.
7. Click *Close* to close the import dialog.
8. Go to *Policy & Objects > User & Authentication > User Groups* and create a new group. Set the type as *FSSO/Cisco TrustSec*, and select *pxGrid* user as a member.
9. Create a policy with the *ISEgroup* user group and install the policy to FortiGate.



10. Go to *Fabric View > External Connectors*. Click *Monitor* to see the users currently logged in.



11. Log on to FortiGate to view the ISE user group.



12. On the FortiGate command line, use the `diagnose debug authd fsso` list to monitor the current user list.

CLI for FortiManager and FortiGate

Command line interface for FortiManager:

```
config system connector
 set
fsso-refresh-interval FSSO refresh interval (60 - 1800 seconds).
fsso-sess-timeout FSSO session timeout (30 - 600 seconds).
px-svr-timeout pxGrid server timeout (30 - 600 seconds).
```

Realtime monitor debug to watch server connection:

```
diag debug application connector 255
```

Show retrieved Active Directory group:

```
diag system print connector (adom name) (user group name)
```

Command line interface for FortiGate:

```
diag debug authd fsso server-status
diag debug authd fsso list-------> show connected users
```

```
----FSSO logons----
IP: 192.168.1.19 User: test2 Groups: px_fc1_security_grp1 Workstation: MemberOf: fscs1
IP: 192.168.1.20 User: test2 Groups: px_fc1_security_grp1 Workstation: MemberOf: fscs1
Total number of logons listed: 2, filtered: 0
----end of FSSO logons----
diag debug authd fsso refresh-logon
diag debug authd fsso refresh-group
```

Creating ClearPass connectors

ClearPass Policy Manager (CCPM) is a network access system that can send information about authenticated users to third party systems, such as a FortiGate or FortiManager. ClearPass connector for FortiManager centralizes updates from ClearPass for all FortiGate devices and leverages the efficient FSSO protocol to apply dynamic policy updates to FortiGate.

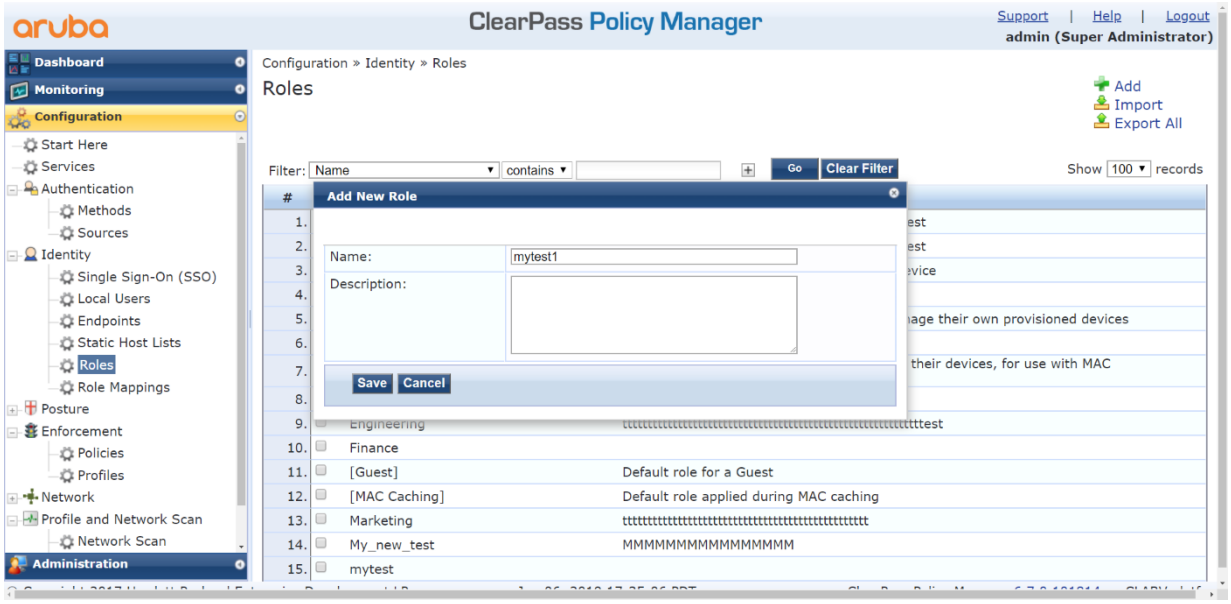
You can create multiple ClearPass connectors per ADOM.

Requirements:

- FortiManager version 6.0 or later ADOM
- FortiGate is managed by FortiManager and configured to work with ClearPass
- JSON API is exposed, allowing ClearPass to call it

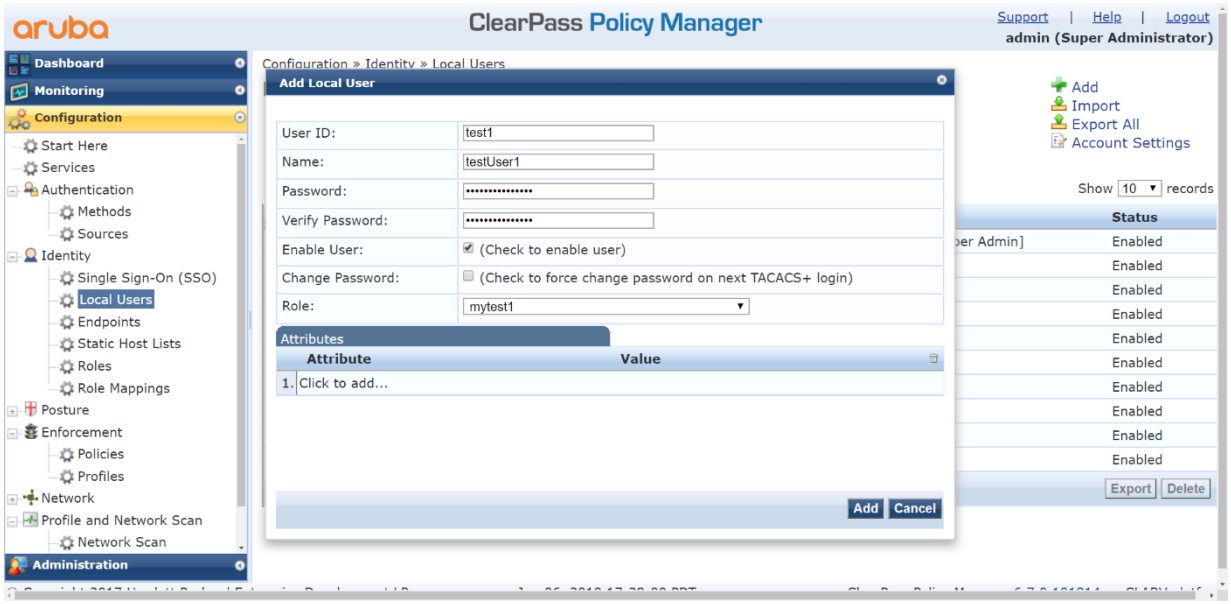
To configure ClearPass:

1. Log in to *ClearPass Policy Manager*.
2. Create roles:
   a. Go to *Configuration > Identity > Roles*.
   b. Click *Add*.
   c. For the name, enter *mytest1*.
   FortiManager will get this group as an Active Directory group.
   The *Description* field is optional.



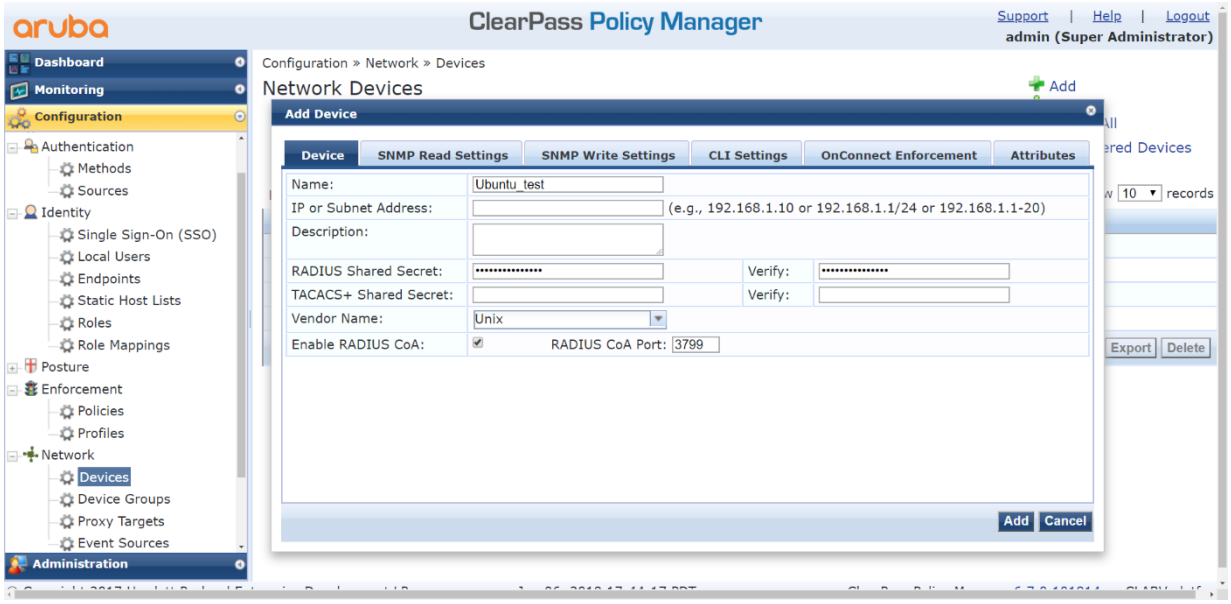
d. Click *Save*.

3. Create local users:
   a. Go to *Configuration* > *Identity* > *Local Users*.
   b. Click *Add*.
   c. Configure the following:
   - Set *User ID* to *test1*.
   - Set *Name* to *testUser1*.
   - Set *Password* to *qa1234*.
   - Select *Enable*.
   - Set *Role* to *mytest1*.



d. Click *Add*.

4. Add an Ubuntu simulator:
   a. Go to *Configuration* > *Network* > *Devices*.
   b. Click *Add*.
   c. Configure the following settings:
   - Set *Name* to *Ubuntu_test*.
   - Set *IP or Subnet Address* to *10.3.113.61*.
   - Set *RADIUS Shared Secret* to *qa1234*.
   - Set *Vendor Name* to *Unix*.



d. Click *Add*.

5. Configure FortiManager to get packets from ClearPass:

a. Add FortiManager as the Endpoint Context Server:

i. Go to *Administration > External Servers > Endpoint Context Servers*.

ii. Click *Add*.

iii. Configure the following:

- Set *Server Type* to *Generic HTTP*.
- Set *Server Name* to *10.3.113.57* (the FortiManager IP address).
- Set *Authentication Method* to *Basic*.
- Set *Username* to *admin* (the administrator on FortiManager).

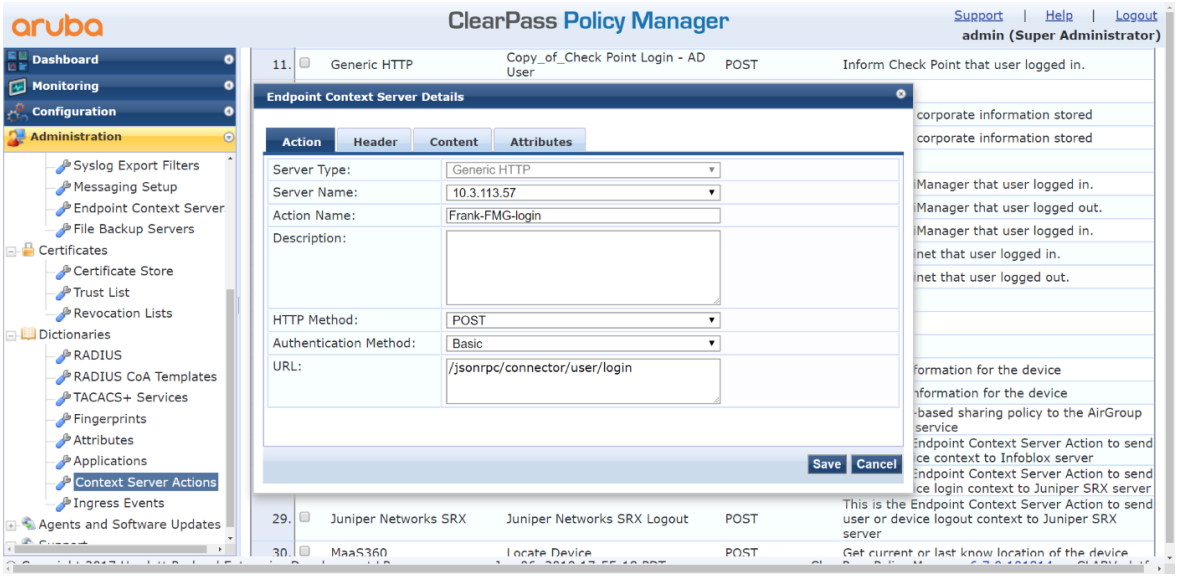
b. Create Endpoint Context Server Login action for FortiManager:

i. Go to *Administration > Dictionaries > Context Server Actions*

ii. Click *Add*.

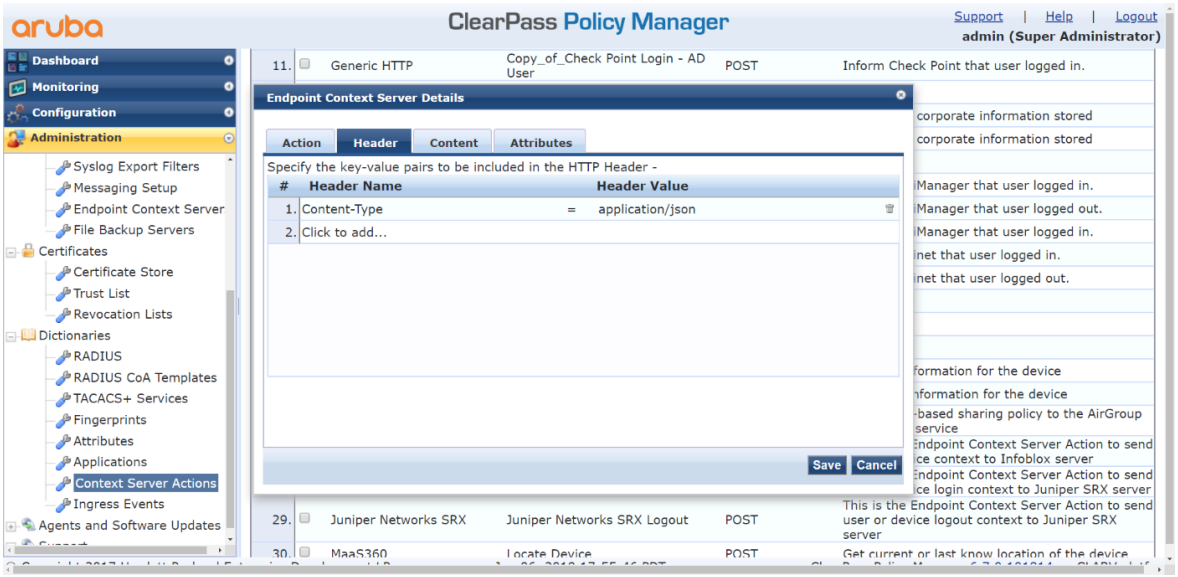
iii. On the *Action* tab, configure the following:

- Set *Server Type* to *Generic HTTP*.
- Set *Server Name* to *10.3.113.57* (the FortiManager IP address).
- Set *Action Name* to *Frank-FMG-login*.
- Set *Description* to *Inform FortiManager that the user logged on*.
- Set *HTTP Method* to *POST*.
- Set *Authentication Method* to *Basic*.
- Set *URL* to */jsonrpc/connector/user/login*



iv. On the *Header* tab, configure the following:

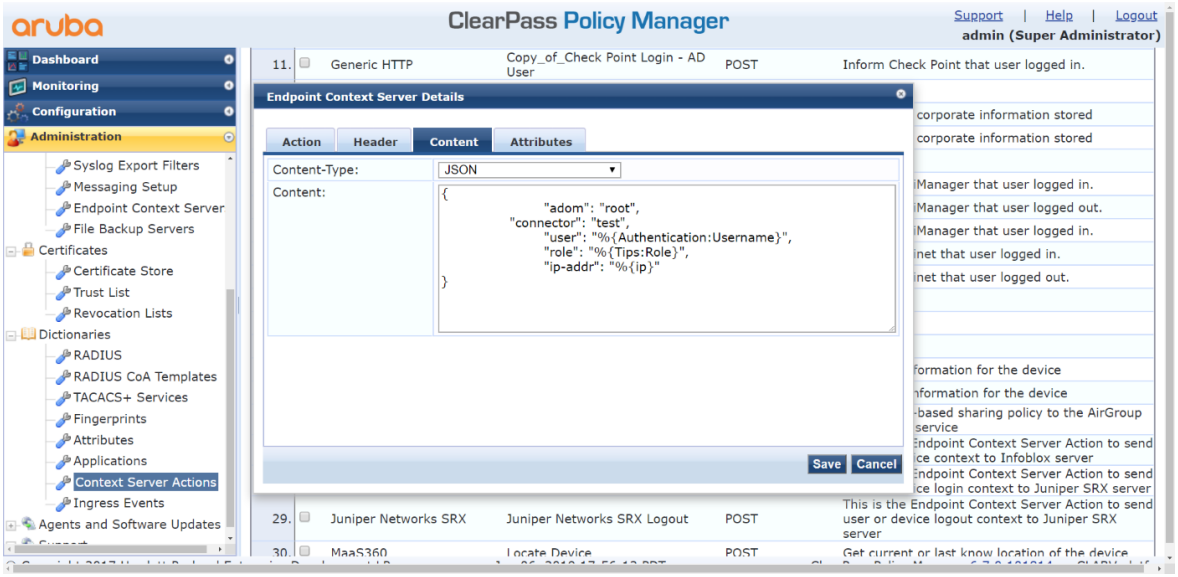
- Set *Header Name* to *Content-Type*.
- Set *Header Value* to *application/json*.



v. On the *Content* tab, configure the following:

- Set *Content-Type* to *JSON*.
- Set *Content* to:

```
{
    "adom": "root",
    "connector": "test", <--------the connector name created on FortiManager
    "user": "%{Authentication:Username}",
    "role": "%{Tips:Role}",
    "ip-addr": "%{ip}"
}
```



vi. Click *Save*.

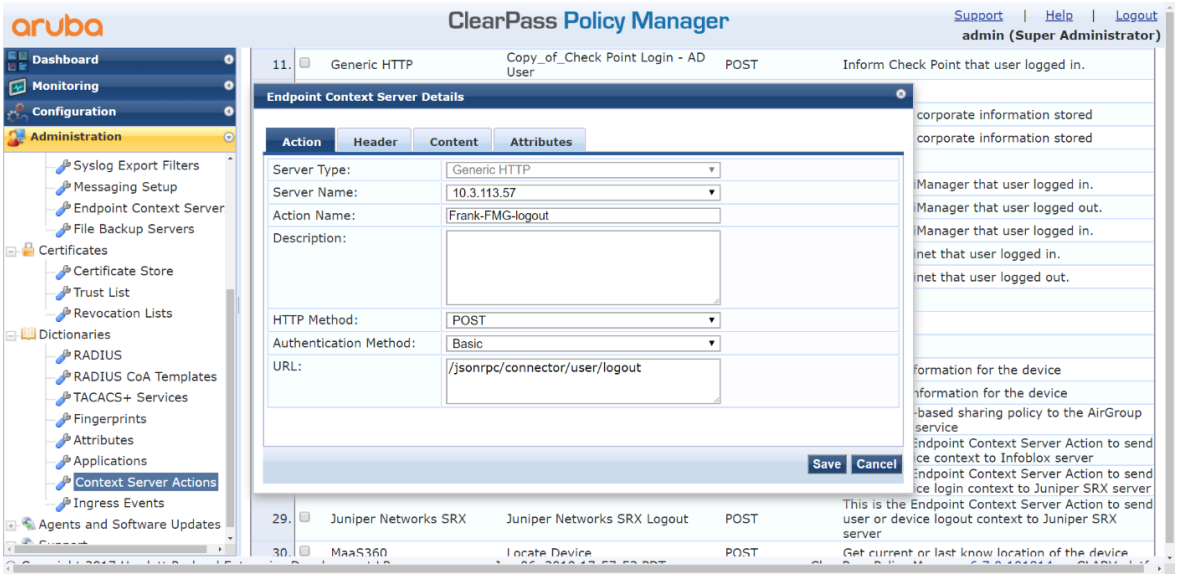
c. Create Endpoint Context Server Logout action for FortiManager:

i. Go to *Administration > Dictionaries > Context Server Actions*

ii. Click *Add*.

iii. On the *Action* tab, configure the following:

- Set *Server Type* to *Generic HTTP*.
- Set *Server Name* to *10.3.113.57* (the FortiManager IP address).
- Set *Action Name* to *Frank-FMG-logout*.
- Set *Description* to *Inform FortiManager that the user logged out*.
- Set *HTTP Method* to *POST*.
- Set *Authentication Method* to *Basic*.
- Set *URL* to */jsonrpc/connector/user/logout*



iv. On the *Header* tab, configure the following:

- Set *Header Name* to *Content-Type*.
- Set *Header Value* to *application/json*.

v. On the *Content* tab, configure the following:

- Set *Content-Type* to *JSON*.
- Set *Content* to:

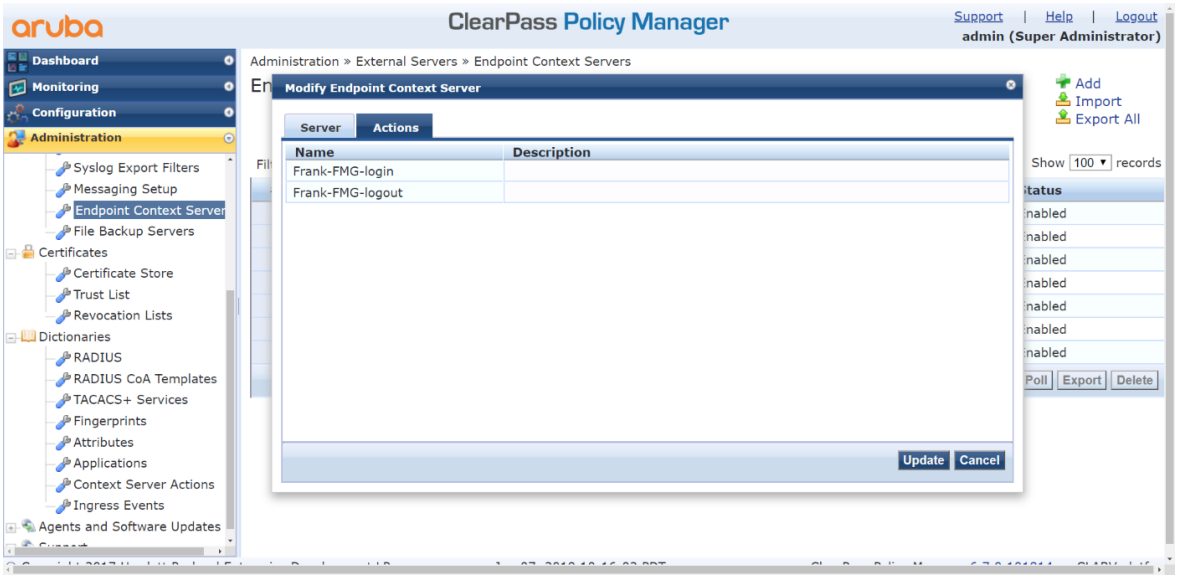
```
{
    "adom": "root",
    "connector": "test",
    "user": "%{Authentication:Username}",
    "role": "%{Tips:Role}",
    "ip-addr": "%{ip}"
}
```

vi. Click *Save*.

d. Check that the actions are added to the server:

i. Go to *Administration > External Servers > Endpoint Context Servers > 10.3.113.57 > Actions*.

ii. Locate the two just created actions.



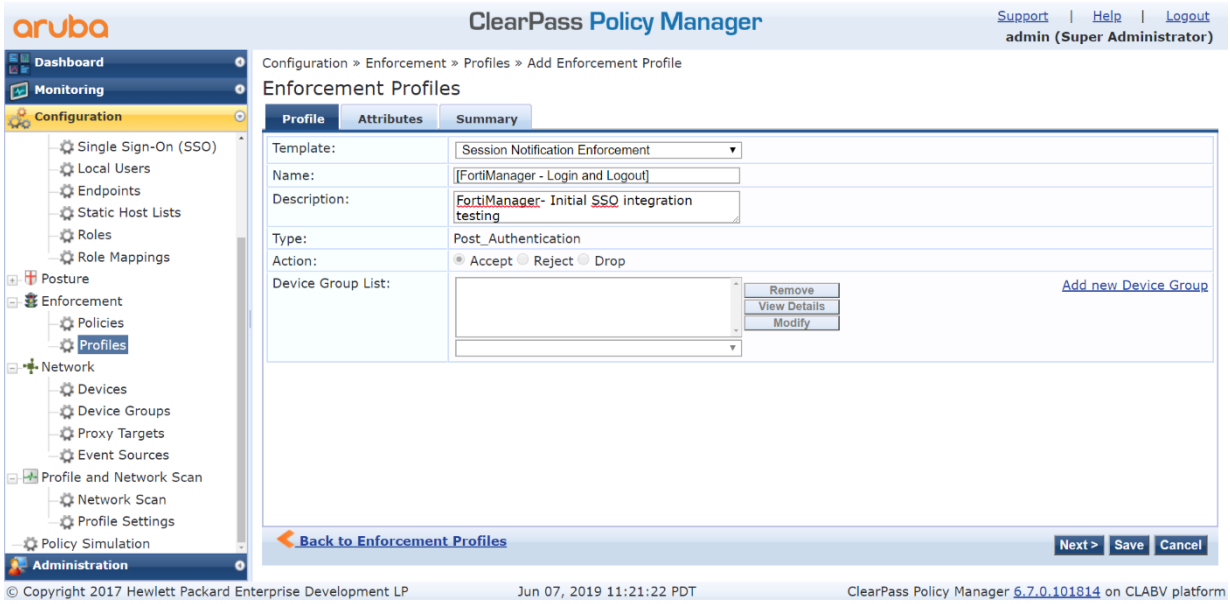
6. Create a profile:

a. Go to *Configuration > Enforcement > Profiles*.

b. Click *Add*.

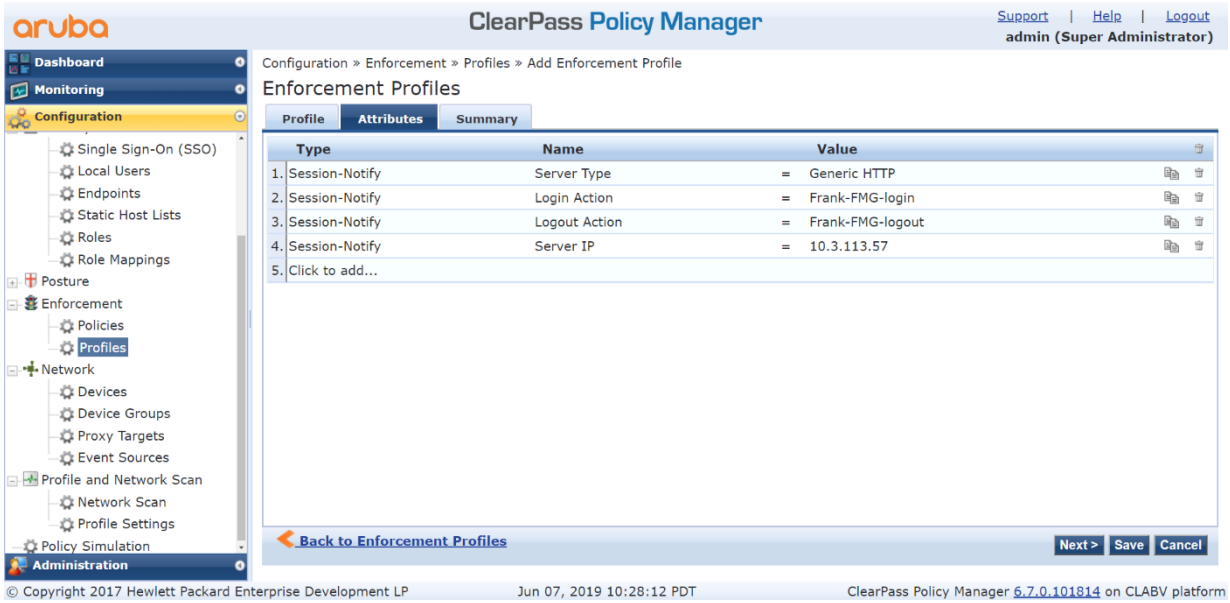
c. On the *Profile* tab, configure the following:

- Set *Template* to *Session Notification Management*.
- Set *Name* to *FortiManager Login and Logout*.
- Set *Description* to *FortiManager - Initial SSO integration testing*.
- Set *Type* to *Post_Authentication*.



d. On the *Attributes* tab, configure the following attributes:

Type	Name	Value
Session-Notify	Server Type	Generic HTTP
Session-Notify	Login Action	Frank-FMG-login
Session-Notify	Logout Action	Frank-FMG-logout
Session-Notify	Server IP	10.3.113.57



e. Click *Save*.

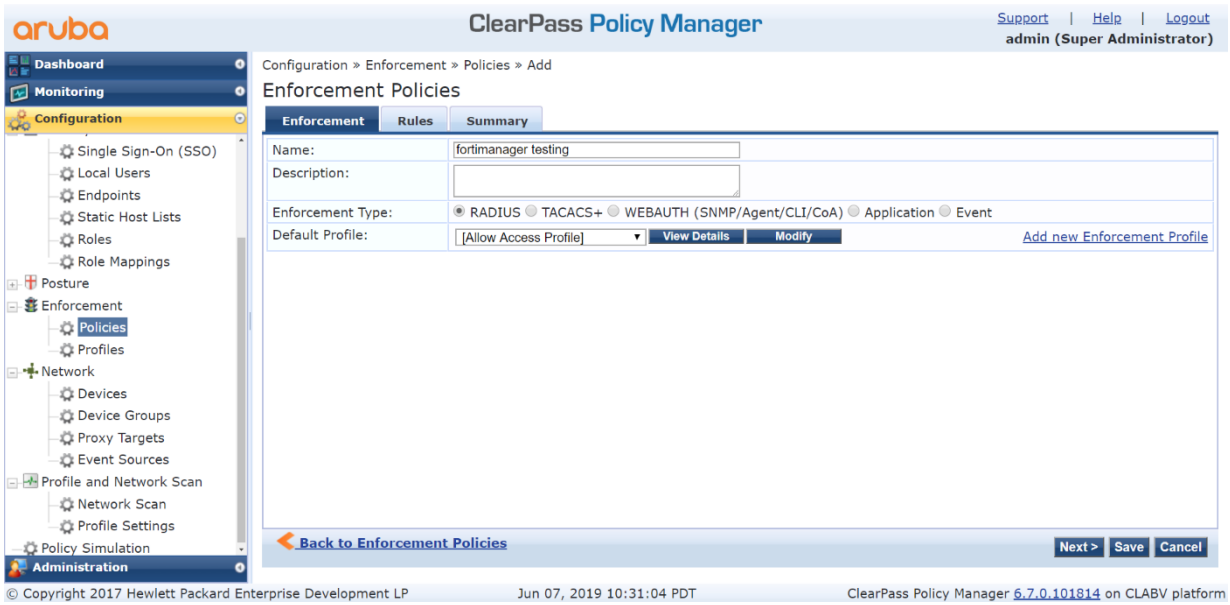
7. Create a policy:

a. Go to *Configuration* > *Enforcement* > *Policies*.

b. Click *Add*.

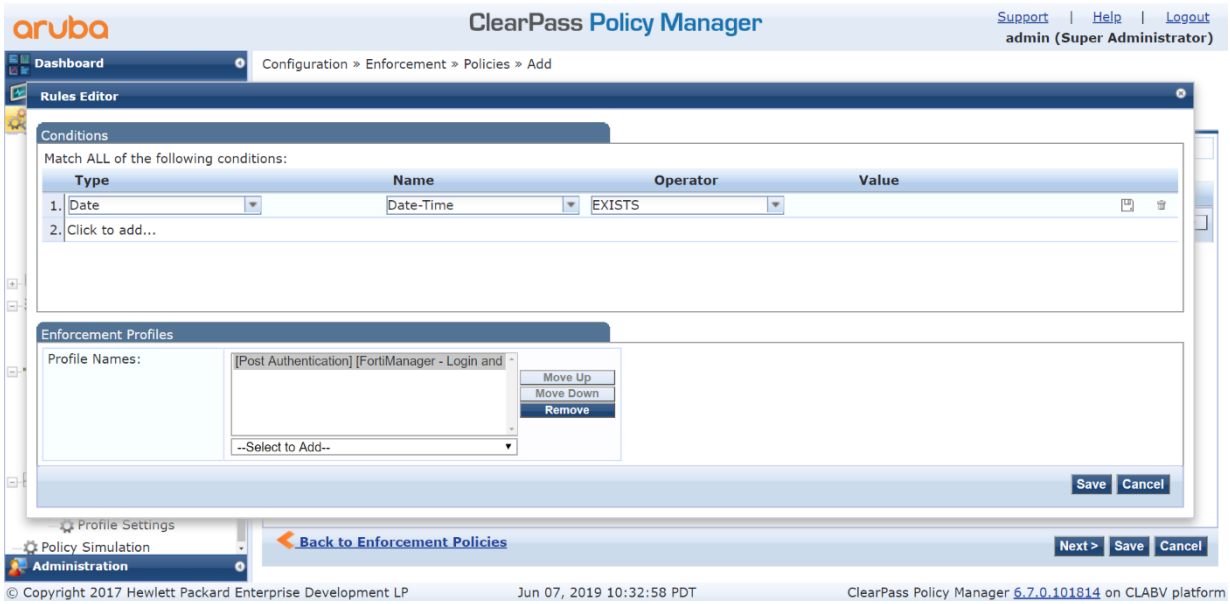
c. On the *Enforcement* tab, configure the following:

- Set *Name* to *FortiManager testing*.
- Set *Enforcement Type* to *RADIUS*.
- Set *Default Profile* to *Allow Access Profile*.



d. On the *Rules* tab, configure the following:

- Set *Type* to *Date*.
- Set *Name* to *Date-Time*.
- Set *Operation* to *EXISTS*.
- Set *Profile Names* to *[Post Authentication][FortiManager - Login and Logout]*.



e. Click *Save*.

8. Create services:
   a. Go to *Configuration* > *Services*.
   b. Click *Add*.
   c. On the *Service* tab, configure the following:
      - Set *Name* to *API Test Access OAuth2 API User Access*.
      - Set *Description* to *Authentication service for API access using OAuth2*.
      - Set *Type* to *Aruba Application Authentication*.
      - Set *Status* to *Enabled*.



   d. On the *Authentication* tab, set *Authentication Sources* to:

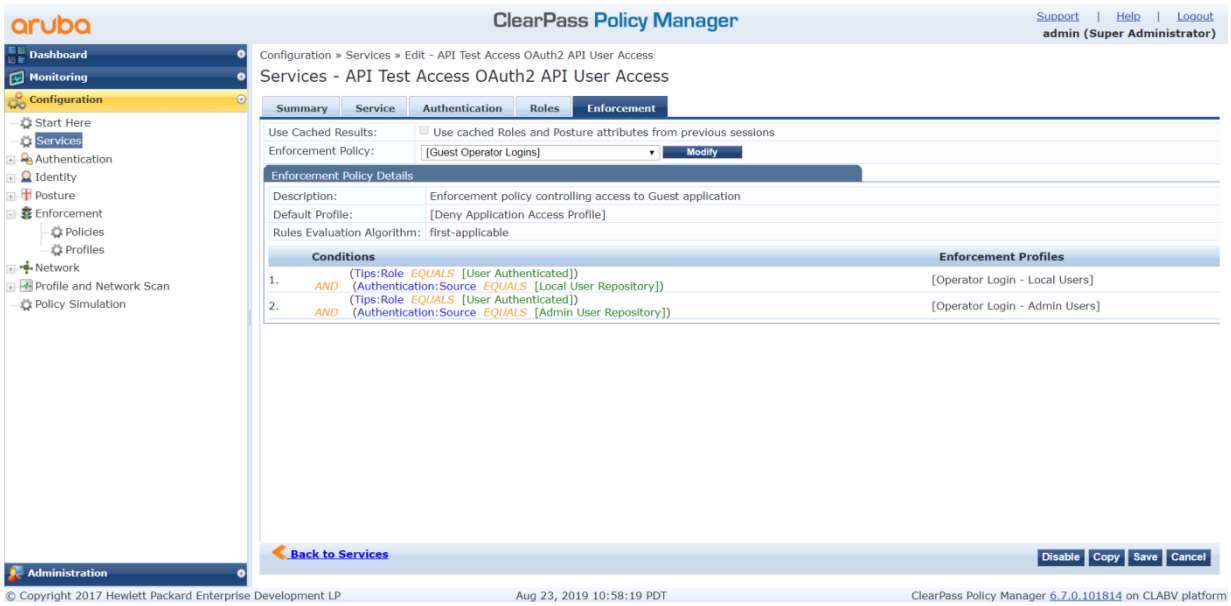
```
[Local User Repository] [Local SQL DB]
[Admin User Repository] [Local SQL DB]
```



   e. On the *Enforcement* tab, configure the following:

- Set *Enforcement Policy* to *[Guest Operator Logins]*.
- Set *Description* to *Enforcement policy controlling access to Guest application*.
- Set *Default Profile* to *[Deny Application Access Profile]*.
- Set *Rules Evaluation Algorithm* to *first-applicable*.
- Create the following two conditions:

	Conditions	Enforcement Profiles
1.	(Tips:Role EQUALS [User Authenticated]) *AND* (Authentication:Source EQUALS [Local User Repository])	[Operator Login - Local Users]
2.	(Tips:Role EQUALS [User Authenticated]) *AND* (Authentication:Source EQUALS [Admin User Repository])	[Operator Login - Admin Users]



f. Click *Save*.

g. Click *Add* again to add another service.

h. On the *Service* tab, configure the following:

- Set *Name* to *AuthN user for Fortimanager Testing*.
- Set *Description* to *Authorization service for AirGroup device access*.
- Set *Type* to *RADIUS Enforcement (Generic)*.
- Set *Status* to *Enabled*.
- Create the following service rule:

Type	Name	Operator	Value
Radius:IEFT	NAS-IP-Address	EQUALS	10.0.0.1

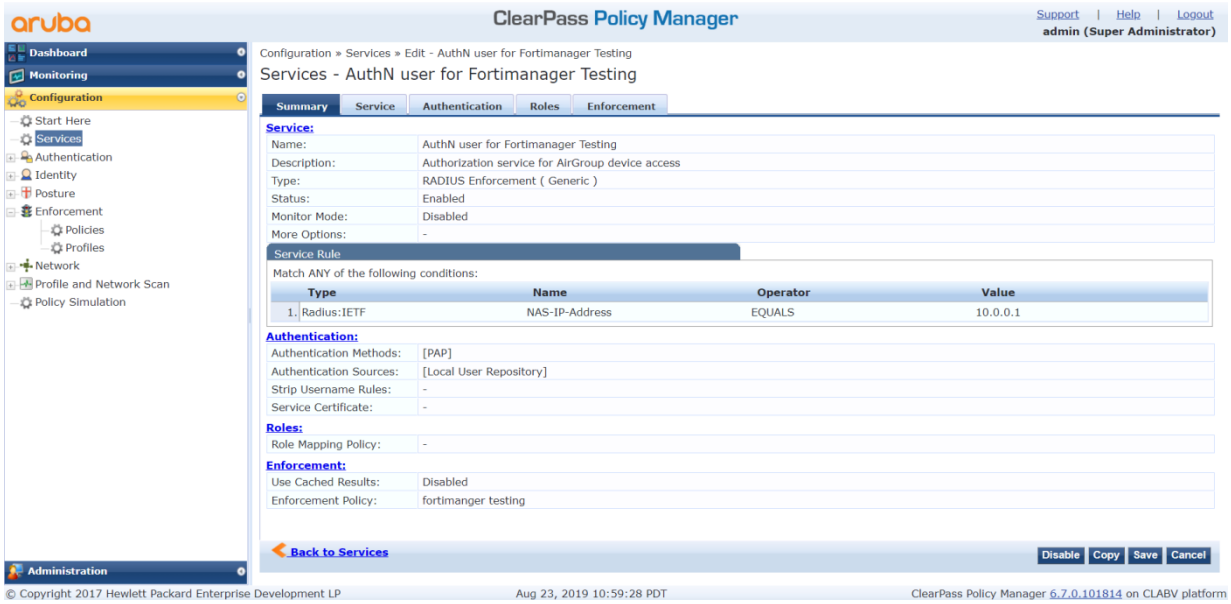
i. On the *Authentication* tab, configure the following:

- Set *Authentication Methods* to *[PAP]*.
- Set *Authentication Sources* to *[Local User Repository] [Local SQL DB]*.

j. On the *Enforcement* tab, configure the following:

- Set *Enforcement Policy* to *fortimanager testing* .
- Set *Default Profile* to *[AllowAccess Profile]*.
- Set *Rules Evaluation Algorithm* to *evaluate-all*.
- Create the following condition:

	Conditions	Enforcement Profiles
1.	(GuestUser:Company Name NOT_EQUALS ABCDE)	[FortiManager-login and Logout]



k. Click *Save*.

9. Configure the administrator the FortiManager fabric connector uses to access CPPM APIs:

a. Go to *Administration* > *Admin Users*.

b. Click *Add*.

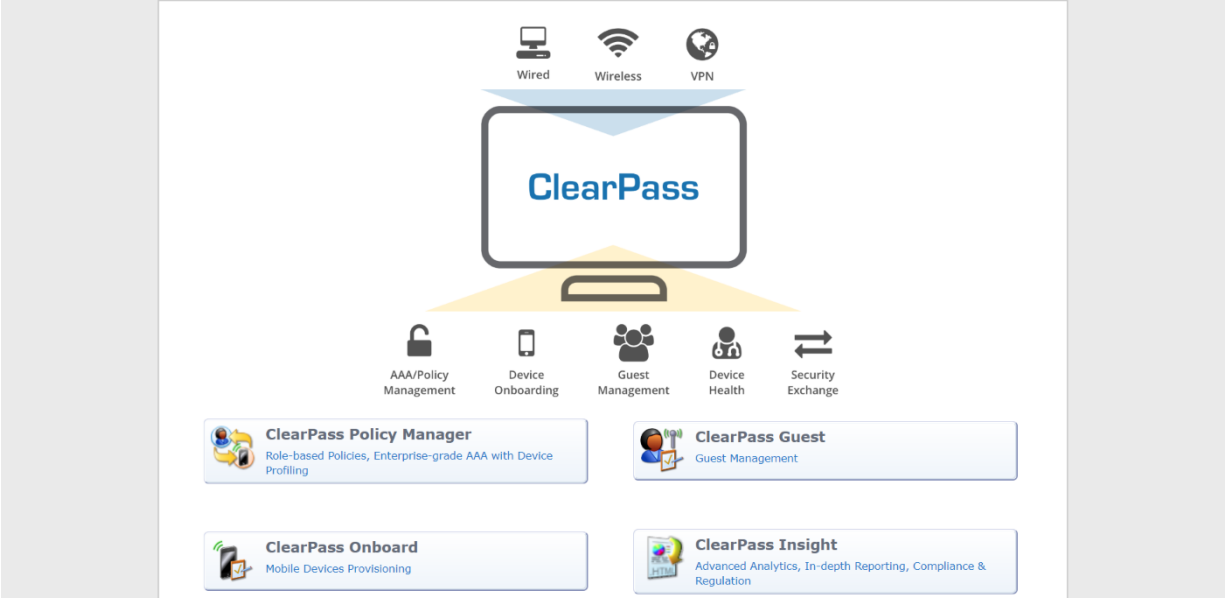
c. Configure the following:

- Set *User ID* to *admin*.
- Set *Name* to *admin*.
- Set *Password* to *qa987654*.
- In *Verify Password* enter the password again.
- Select *Enable User*.
- Set *Privilege Level* to *API Administrator*.

d. Click Save.

10. Create an API Client:

a. Log in to *ClearPass Guest*.

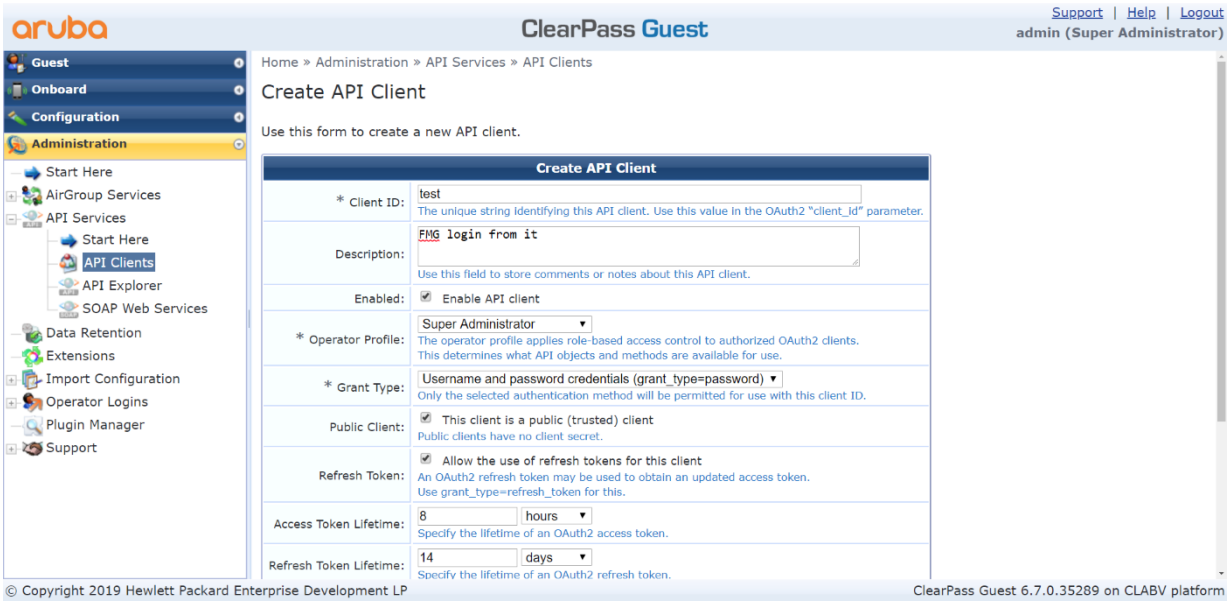


b. Go to *Administration > API Services > API Clients*.

c. Click *Create API Client*.

d. Configure the following:

- Set *Client ID* to *test*.
- Set *Desciption* to *FMG login from it*.
- Select *Enable API client*.
- Set *Operator Profile* to *Super Administrator*.
- Set *Grand Type* to *Username and password credentials (grant_type=password)*.
- In *Public Client* select *This client is public (trusted) client*.
- In *Refresh Token* select *Allow the use of refresh tokens for this client*.



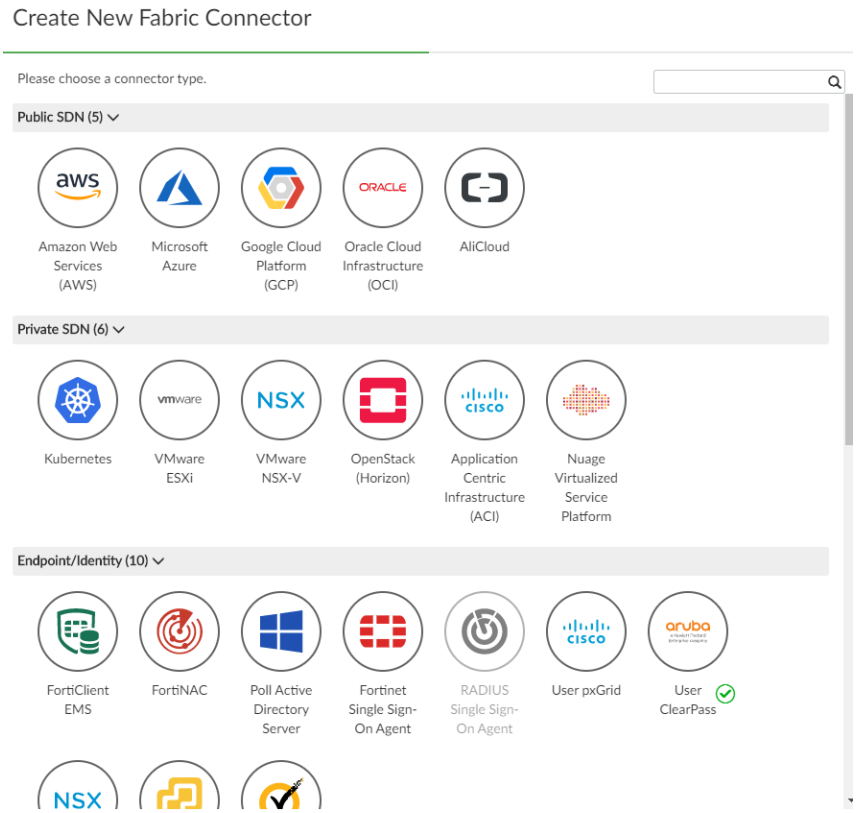
e. Click *Save*.

To configure FortiManager:

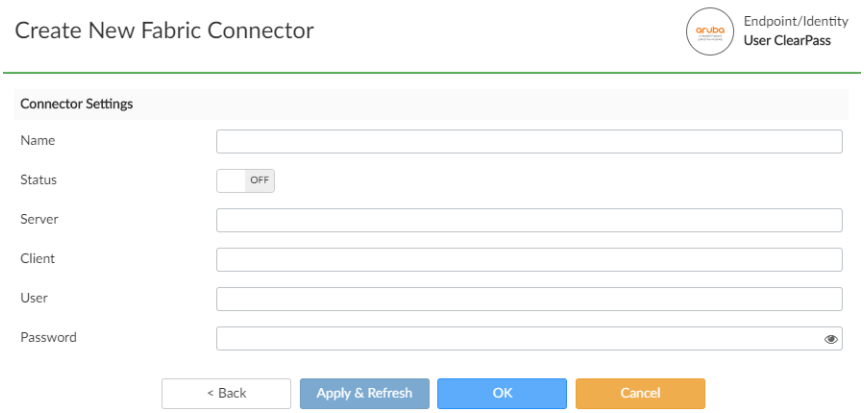
1. Log in to FortiManager.
2. Run the following CLI command:

```
config system admin user
    edit  admin
        set rpc-permit read-write
    next
end
```

3. Go to *Fabric View* > *External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.

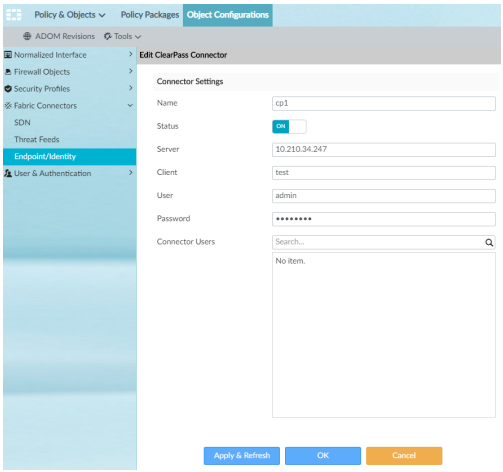


4. Under *Endpoint/Identity*, select *User ClearPass*.
5. Configure the following:
   - Set *Name* to *test*. This name must be same as the one used in the ClearPass actions.
   - Set *Status* to *On*.
   - Set *Server* to *10.3.113.102* (the ClearPass IP address).
   - Set *Client* to *test* (the previously created ClearPass API client).
   - Set *User* to *admin* (the ClearPass login name).
   - Set *Password* to *qa1234* (the ClearPass login password).

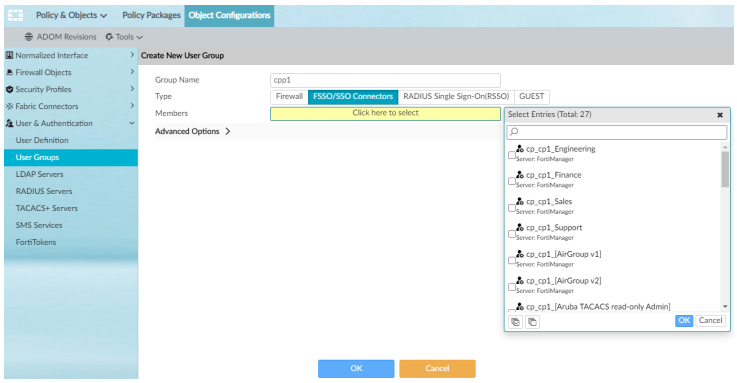


6. Click *OK*.
7. Get the role and user from ClearPass:
   a. Go to *Policy & Objects* > *Security Fabric* > *Endpoint/Identity*.
   b. Edit the ClearPass connector and click *Apply & Refresh*.

      FortiManager retrieves the roles and users from ClearPass. Users with green icons are currently logged in.



8. Install the address group from ClearPass to FortiGate:
   a. On the FortiManager, go to *Policy & Objects* > *User & Authentication* > *User Groups*.
   b. Click *Create New*.
   c. Configure the following:
      - Set *Group Name* to *cpp1*.
      - Set *Type* to *FSSO/SSO Connectors*.
      - Select *Members* as *ClearPass adgrp*.



9. Use the new user group in a policy to install it to FortiGate.
10. To check that the group was installed on the FortiGate:
    a. On the FortiGate, go to *User & Device* > *User Groups*. The group will be in the user group list.
    b. Edit the group to view its members.
    c. In the CLI console, enter the following:

```
# diagnose debug authd fsso list
----FSSO logons----
IP: 10.210.15.185  User: user1  Groups: cp_test_Finance  Workstation:  MemberOf: cpp1
Total number of logons listed: 1, filtered: 0
----end of FSSO logons----
```

Creating VMware NSX-T connectors

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 769
2. Creating a fabric connector for VMware NSX-T on page 770
3. Configure registered services on page 772
4. Configure the NSX-T Manager on page 773
5. Use the groups in a FortiManager policy on page 775

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. Select your Administrator account, and click *Edit*.
3. From the *JSON API Access* dropdown, select *Read-Write*, and click *OK*.
   The FortiManager will log you out to activate the settings.

Creating a fabric connector for VMware NSX-T

In FortiManager, create a fabric connector for VMware NSX-T.

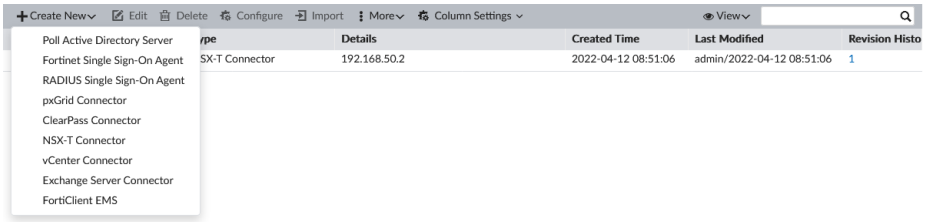
NSX-T connector configuration is not specific to the ADOM in which it is created. NSX-T connectors with the same IP address cannot be created in different ADOMs.

To configure an NSX-T connector on FortiManager:

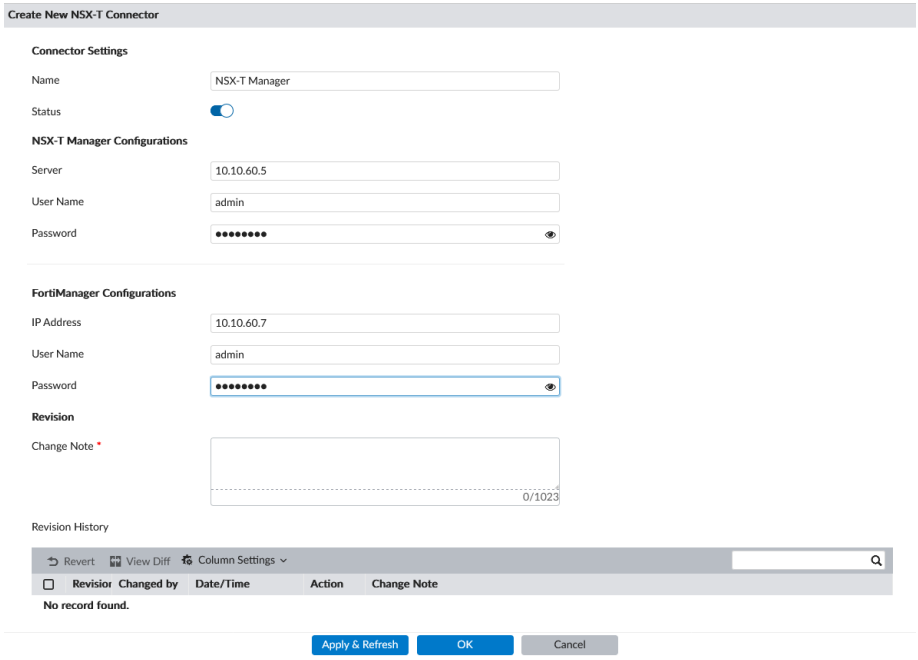
1. Log into FortiManager.
2. Go to *Policy & Objects* > *Security Fabric* > *Endpoint/Identity*.
3. Click *Create New* > *NSX-T Connector*.



NSX-T connectors can also be created from *Fabric View* > *Fabric* > *External Connectors* in FortiManager.



4. Configure the following parameters for the new NSX-T connector, and click *OK*.

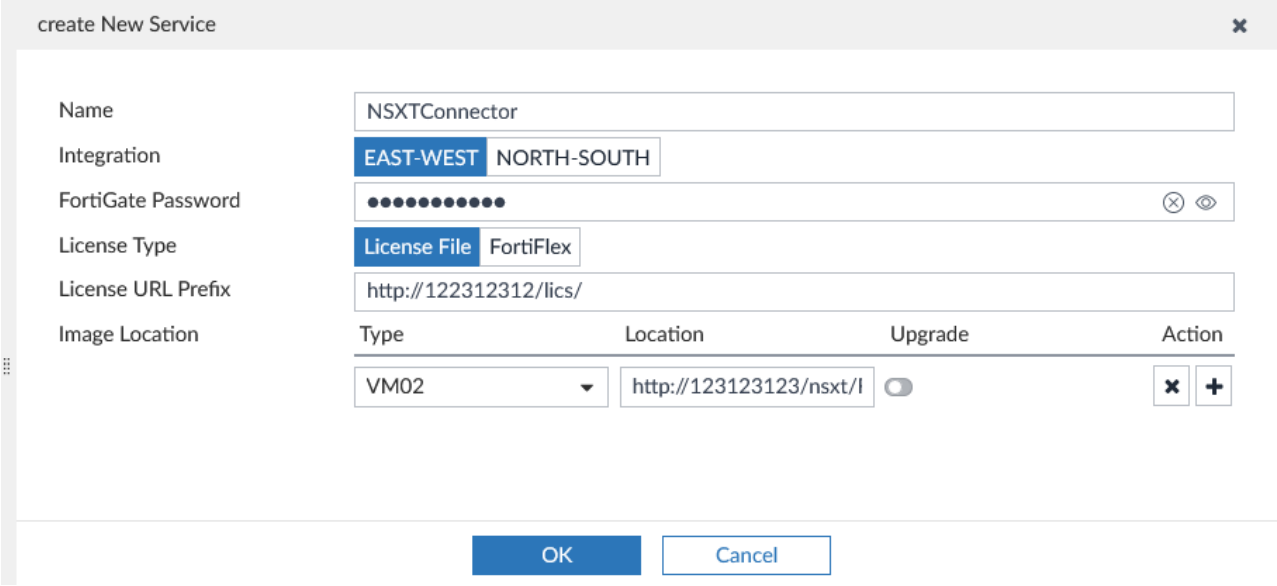


Name	Enter a name for the connector.
Status	Toggle the status to *ON* or *OFF*.
NSX-T Manager Configurations	
Server	Configure the server address for NSX-T Manager.
User Name	Enter your NSX-T username.
Password	Enter your NSX-T password.
FortiManager Configurations	
IP Address	Enter the IP or FQDN for FortiManager.
User Name	Your FortiManager administrator password.
	The user name under FortiManager configurations can be any other FortiManager local user with JSON API access set to read-write. This user will be used by the NSX-T Manager to perform the API calls to the FortiManager in order to dynamically update the VM groups objects.
Password	Your FortiManager administrator password.

Configure registered services

To configure a registered service:

1. Edit the previously configured NSX-T connector.
2. Under *Registered Service*, click *Add Service*.
   You also have the option to *Delete* or *Edit* previously configured registered services.



3.

Name	Enter the service name to register to NSX-T's partner service catalog.
Integration	Select the integration type as *East-West* or *North-South*.
FortiGate Password	Enter your FortiGate administrator password.
License Type	Select the license type as either *License File* or *FortiFlex*.
License File	When using a *License File*: 1. Enter the license URL prefix in *License URL Prefix*, for example: `http://x.x.x.x/lics/`. 2. Click the Add icon to add a new image location, and configure the following: • *Type*: Select the VM type, for example *VM01*. • *Location*: Enter the image location, for example: `http://x.x.x.x/FortiGate-VM64xCPU.nsxt.ovf`
FortiFlex	When using *FortiFlex*, select a previously configured FortiFlex Connector from which to obtain the license. See Creating FortiFlex connectors on page 779.

4. Click *OK*, and save the NSX-T connector.
5. In the NSX-T Manager, go to *System* > *Service Deployment* > *CATALOG* to confirm that the FortiGate-VM service was properly registered on NSX-T Manager.

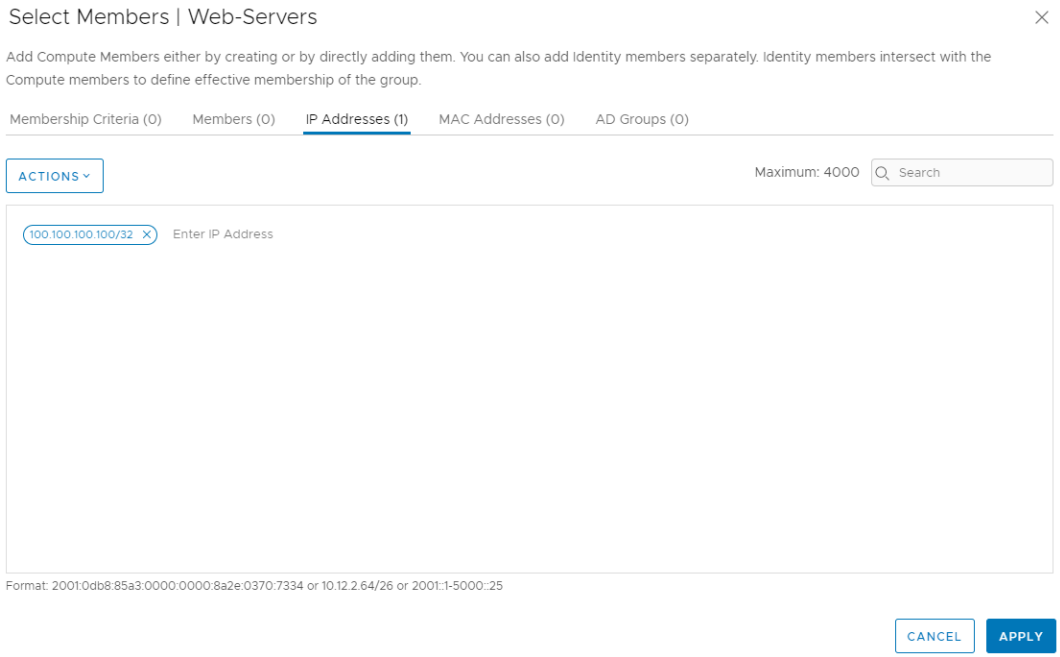
To edit a registered service:

1. Navigate to the NSX-T Connector in FortiManager.
2. Select the registered service, and click *Edit Service*.
3. Once *Edit Service* is selected, you can change the following information:
   - Password
   - License type
   - License URL (if license type is *License File*)
   - Image location of existing deployment specs
     When upgrading, make sure to mark the change as upgrade by enabling the *Upgrade* toggle. This marks the change on the NSX-T Manager. Once a deployment spec is set as *Upgrade*, users can upgrade a service deployment using the NSX-T Manager GUI.

Configure the NSX-T Manager

To configure NSX-T Manager:

1. In the NSX-T Manager, go to *Inventory* > *Groups*, and click *ADD GROUP*.
2. Enter a name, and click *Set Members*.
3. Select the *IP Addresses* tab, and add the IP addresses to add as members of this group.



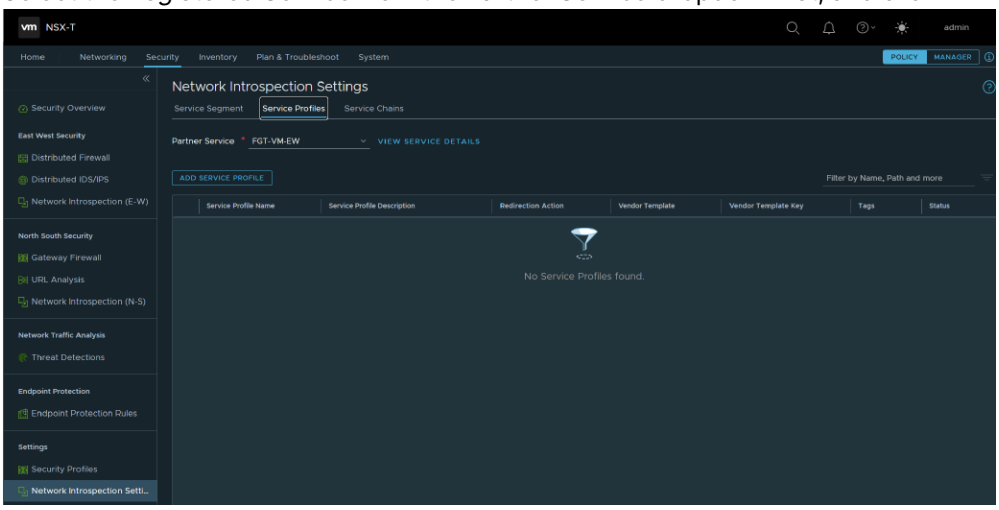
4. Save your changes, and repeat these steps until you have created all of the groups that you require.



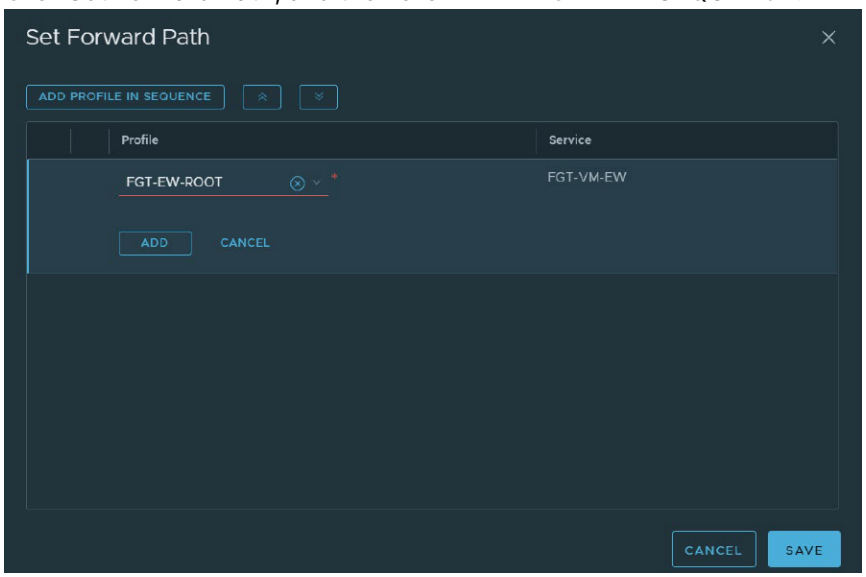
Group membership is what is used to determine dynamic NSX-T addresses in FortiManager. There are multiple criteria which can be defined on the NSX-T Manager to make a virtual machine part of that group.

5. Go to *Security* > *Network Introspection Settings* > *Service Profiles*.

6. Select the *Registered Service* from the *Partner Service* dropdown list, and click *ADD SERVICE PROFILE*.



7. Configure the following parameters, and click *Save*.
   a. *Name*: Enter a name.
   b. *Vendor Template*: Select the template listed in the dropdown.
8. Go to the *Service Chains* tab and click *ADD CHAIN*.
9. Configure the following parameters, and click *Save*.
   a. *Name*:Enter a name.
   b. *Service Segment*: Service-Segment.
10. Click *Set Forward Path*, and then click *ADD PROFILE IN SEQUENCE*.



11. Select the profile you just created, and click *ADD*.
12. Save your changes.
13. Go to *Service Chain Management* > *E-W Network Introspection* or *N-S Network Introspection*, and click on *Add Policy*.
14. Click on the policy name, and you can change it if required.

To create the redirection rule in NSX-T:

1. Select the policy you created in the previous step, and click *ADD RULE*.
2. Configure the parameters as follows:
   a. *Name*: Redir-Rule.
   b. *Source*: Any (Groups needs to be selected).
   c. *Destination*: Any (Groups needs to be selected).
   d. *Services*: Any.
   e. *Applied To*: DFW.
   f. *Action*: Redirect.

   This rule will redirect all traffic to the FortiGate instance. You can be more granular by selecting any combination of *Sources*, *Destinations*, *Services*, or *Applied To* for specific groups. If specific groups are selected, only they will be associated with the Service Manager and show up on FortiManager.
3. Click *PUBLISH* to apply the changes.



NSX-T currently only supports North-South Introspection once the service is deployed.

To deploy a North-South service on NSX-T Manager:

1. In the NSX-T Manager, go to *System > Service Deployment > Deployment*.
2. From the dropdown, select the newly registered service and select *Deploy*.
3. Fill in the details, and deploy the service.
4. Associate groups with the North-South service:
   a. Go to *Security > Service Chain Management > N-S Network Introspection*.
   b. In the policy, add the desired groups.
   c. The same groups will appear on FortiManager and be available for use.

Use the groups in a FortiManager policy

To use groups in a policy:

1. Go to *Policy & Objects > Security Fabric > Endpoint/Identity*.
2. Edit the NSXT-Manager object.
3. Scroll down and check that the objects with addresses appear. If there aren't any objects, select *Apply & Refresh*.
4. Click *Cancel*.



These groups and their members are automatically synchronized between FortiManager and NSX-T Manager. As soon as you add a VM/IP to a group that the Redir-Rule applies to on NSX-T Manager, it will be synchronized.

5. You can have the FortiManager create Firewall Addresses or create your own. Go to *Firewall Objects > Addresses*, and click *Create New > Address*.

6. Configure the parameters, and click *OK*.
   a. *Address Name*: Enter a name.
   b. *Type*: Dynamic.
   c. *Sub Type*: FSSO.
   d. *FSSO Group*: `nsx_NSXT-Manager_Default/groups/<group name>`

Migrating FortiGates that are part of the NSX-T connector to a new ADOM

Because the NSX-T configuration is not ADOM specific, migrating FortiGates to a different ADOM will not cause them to lose their configurations. The connector will continue to update IPs and address groups from the previously created policies for the FortiGates on the new ADOM.

It is recommended you import the Policy Package into the new ADOM after the migration is complete.

If you want to migrate the NSX-T connector to a new ADOM, you must follow these the process below.

To migrate the NSX-T connector to a new ADOM:

1. Delete the *Registered Services*.
2. Manually disable the connector by editing it in *Fabric Connectors* > *External Connectors* and clicking *Disable Server*.
3. Delete the connector.
4. Reconfigure the connector in the new ADOM.

Creating VMware vCenter connectors

You can create SDN connectors for VMware vCentre to allow FortiGate to retrieve dynamic addresses from VMware vCenter via FortiManager.

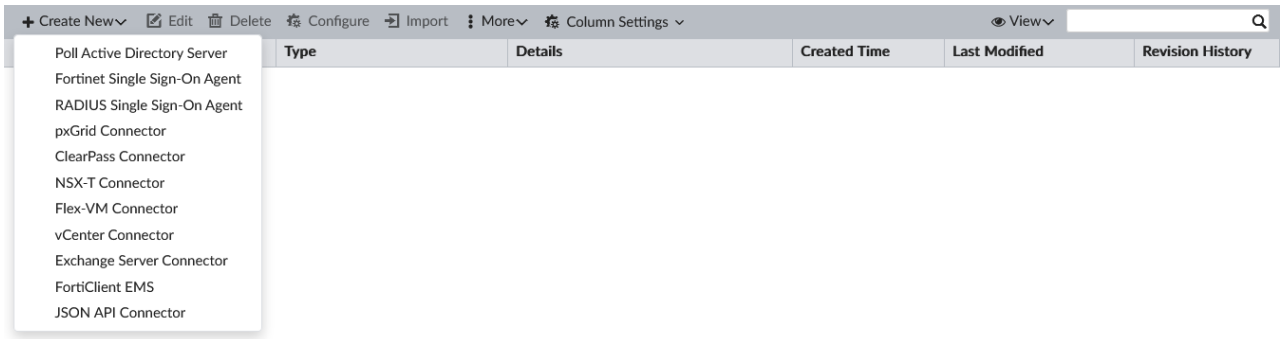
Following is an overview of how to configure an SDN connector for VMware vCenter:

1. Create an SDN connector for VMware vCenter. See Creating SDN connectors for VMware vCenter on page 776.
2. Create a dynamic address object that references the SDN connector for VMware vCenter. See Creating dynamic addresses on page 778.
3. Create a firewall policy. See Creating firewall policies on page 778.
4. Install the changes to FortiGate. See Installing changes to FortiGate on page 779.
   FortiGate can retrieve dynamic addresses from VMware vCenter via FortiManager.
   This example assumes that VMware vCenter is already set up.

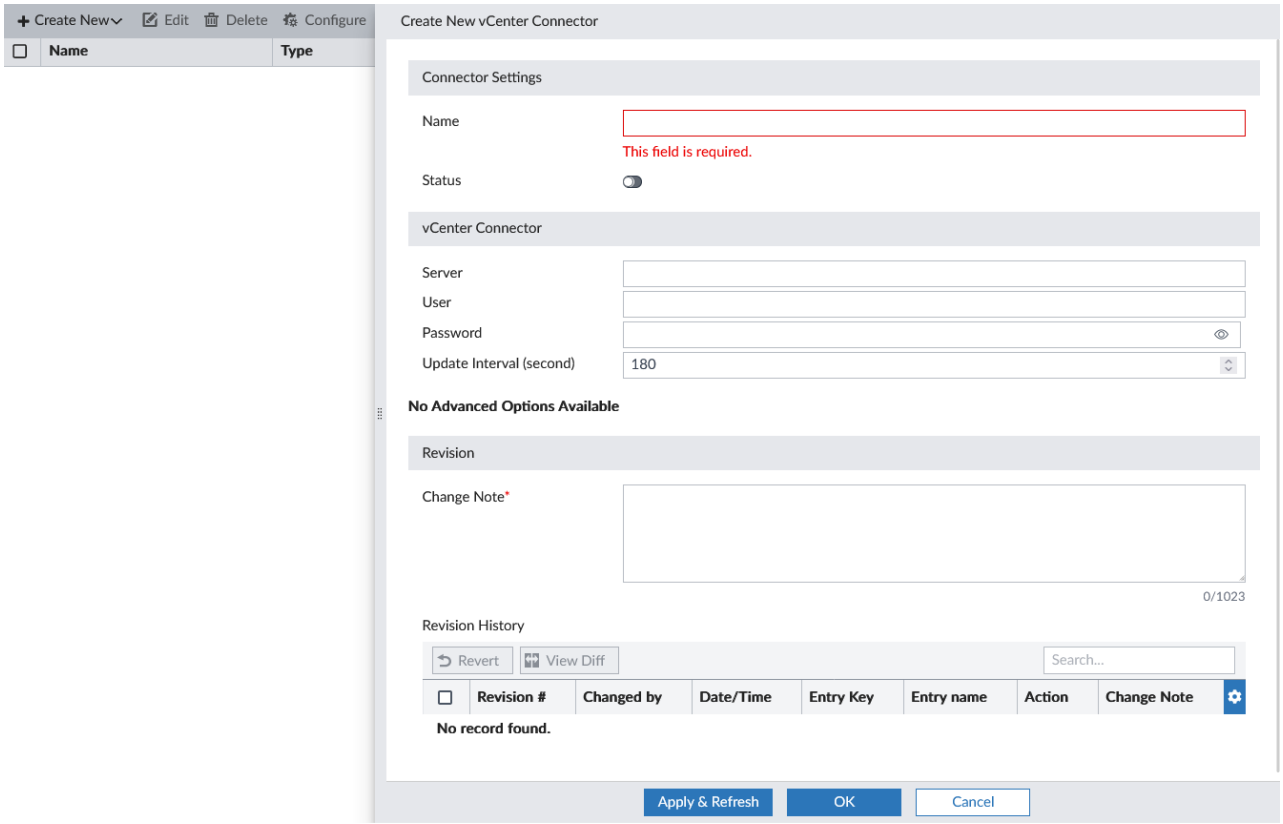
Creating SDN connectors for VMware vCenter

To create SDN connectors for VMware vCenter:

1. Go to *Policy & Objects* > *Security Fabric* > *Endpoint/Identity*.
2. Click *Create New* > *vCenter Connector*.
   The pane opens.



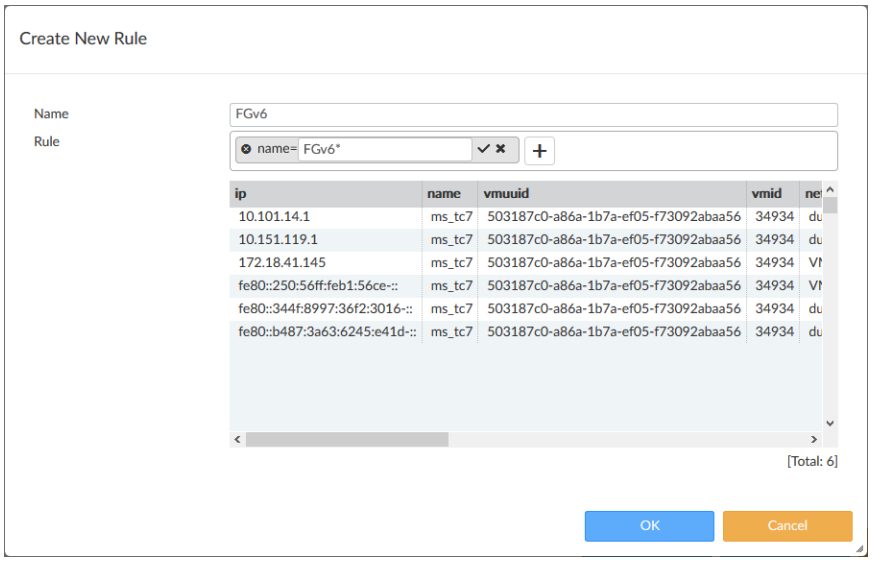
3. Complete the following options, and click *Apply & Refresh*:



The *Rule* section is displayed.

4. Under *Rule*, click *Create New*.

5. Complete the following options, and click *OK*.



FortiManager retrieves IP addresses from the VMware vCenter server.

Creating dynamic addresses

To create dynamic addresses:

1. Go to *Policy & Objects* > *Firewall Objects* > *Addresses*.
2. Click *Create New* > *Address*, or double-click an existing address object to open it for editing.
3. Complete the following options, and click *OK*.
   a. In the *Address Name* box, type a name.
   b. In the *Type* box, select *Dynamic*.
   c. Beside *Sub Type*, select *FSSO*.
   d. In the *FSSO Group* box, select the SDN connector that you created.
   e. Set the remaining objects as desired.

   The dynamic address is created.

Creating firewall policies

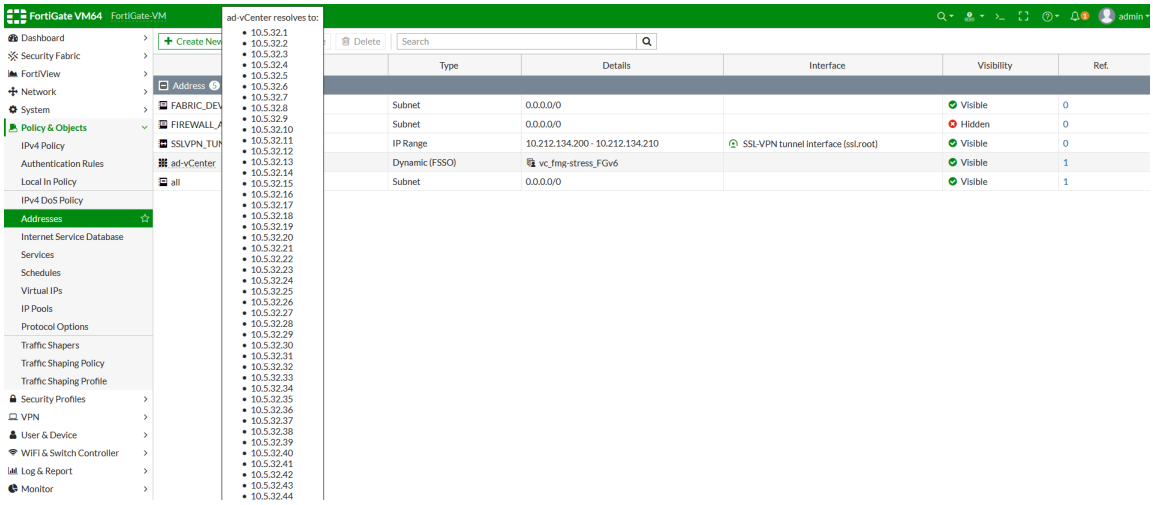
To create firewall policies:

1. Go to *Policy & Objects* > *Policy Packages*.
2. In the tree menu, click IPv4 Policy under the target FortiGate.
3. Click *Create New* , or double-click an existing policy to open it for editing.
4. Complete the options, and click *OK*.
   The policy package is created.

Installing changes to FortiGate

To install changes to FortiGate:

1. Go to *Policy & Objects* > *Policy Packages*.
2. In the tree menu, right-click *Installation Targets* under the target FortiGate, and select *Install Wizard*.
   The *Install Wizard* dialog box opens.
3. Select *Install Policy Package & Device Settings*.
4. In the *Policy Package* list, select the policy package, and click *Next*.
5. Complete the options, and click *Next*.
   The policy package is installed.
   FortiGate can retrieve dynamic addresses from VMware vCenter via FortiManager.



Creating FortiFlex connectors

You can configure a FortiFlex connector to allow FortiManager to assign licenses to managed FortiGate devices through the device manager. See Installing VM licenses on managed devices on page 159.

To create a FortiFlex connector:

1. Go to *Policy & Objects* > *Security Fabric* > *Endpoint/Identity*.
2. Click *Create New*, and select *FortiFlex Connector*.
   The Create New Fabric Connector - FortiFlex wizard opens.
3. Enter the following information:

Name	Enter a name for the FortiFlex connector.
Status	Toggle the slider on or off to enable or disable the connector.
API User	Enter the username for your FortiFlex API user.
API Password	Enter the password for your FortiFlex API user.
Program SN	Enter your FortiFlex program SN.

4. Click *OK* to save the connector.
   Once the connector has been created, it can be used to install VM licenses to managed FortiGate devices in the Device Manager.

Creating JSON API connectors

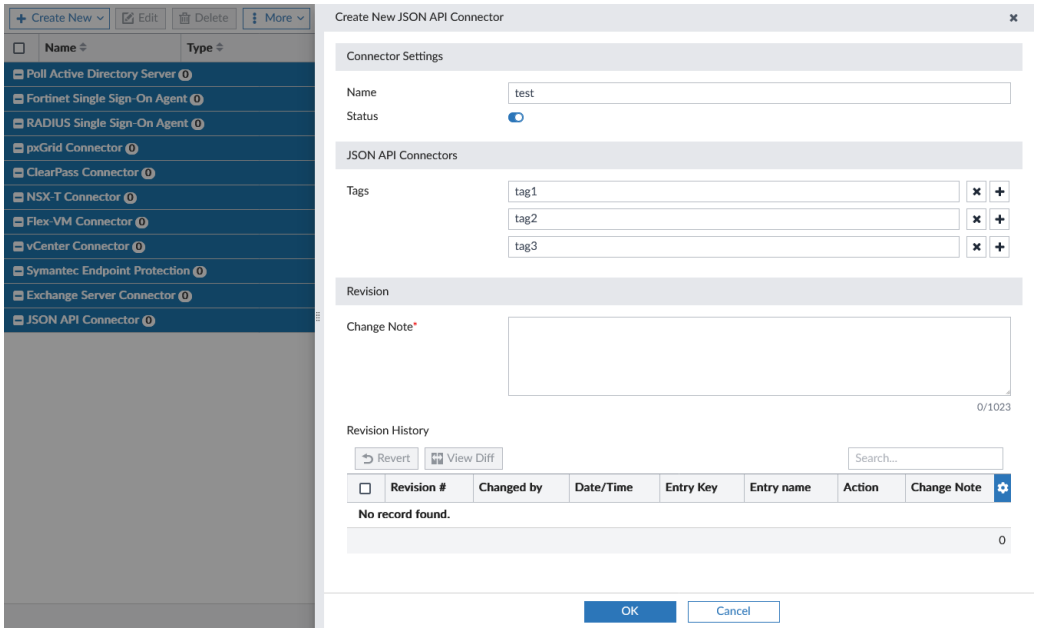
You can configure a JSON API connector to allow FortiManager to add users, get users and FSSO groups, and delete data.

To create a JSON API connector:

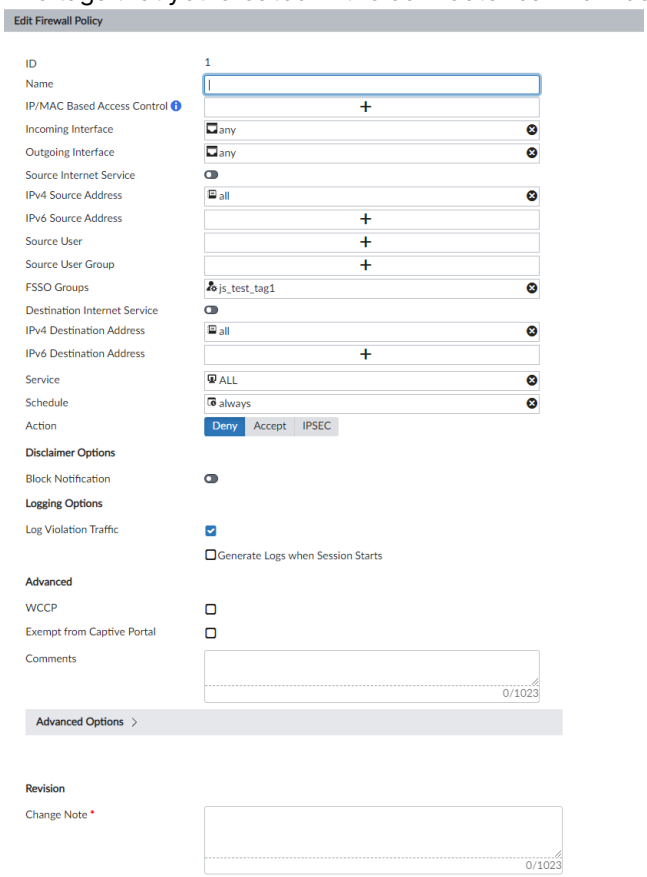
1. Go to *Fabric View* > *External Connectors* and click *Create New* > *JSON API connector*.
   You can also configure this connector at *Policy & Objects* > *Security Fabric* > *Endpoint/Identity*.
   Enter the following information:

Name	Enter a name for the JSON API connector.
Status	Toggle the slider on or off to enable or disable the connector.
Tags	Enter tags for the JSON API connector. You can add additional tags by clicking the plus icon beneath the text field.

2. Click *OK* to save the connector.



3. The tags that you created in the connector can now be used in a policy as the FSSO group (adgrp).



Once the policy with the FSSO group(s) are installed on a FortiGate, you can use the JSON API to operate the connector to add users, get FSSO groups, get users, or delete users.

Cloud Orchestration

FortiManager supports the ability to orchestrate the deployment of FortiGate autoscaling groups (ASG) on Amazon Web Services (AWS). This allows administrators to use FortiManager as a single-pane to deploy all resources required to implement FortiGate ASG in the public cloud.

You can deploy cloud orchestration on FortiManager for the following deployment types:

- FortiGate ASG on AWS for existing virtual private clouds.
- FortiGate ASG on AWS for new virtual private clouds.
- FortiGate ASG on AWS for new virtual private clouds with a transit gateway (TGW).

To deploy cloud orchestration with FortiManager:

1. Configure a cloud connector to connect to the AWS server. See Creating cloud connectors on page 782.
2. Configure a cloud deployment template to configure the VPC and FortiGate ASG settings. See Creating cloud deployment templates on page 783.

3. Create a new cloud orchestration and deploy it to the public cloud. See Deploying cloud orchestration on page 785.

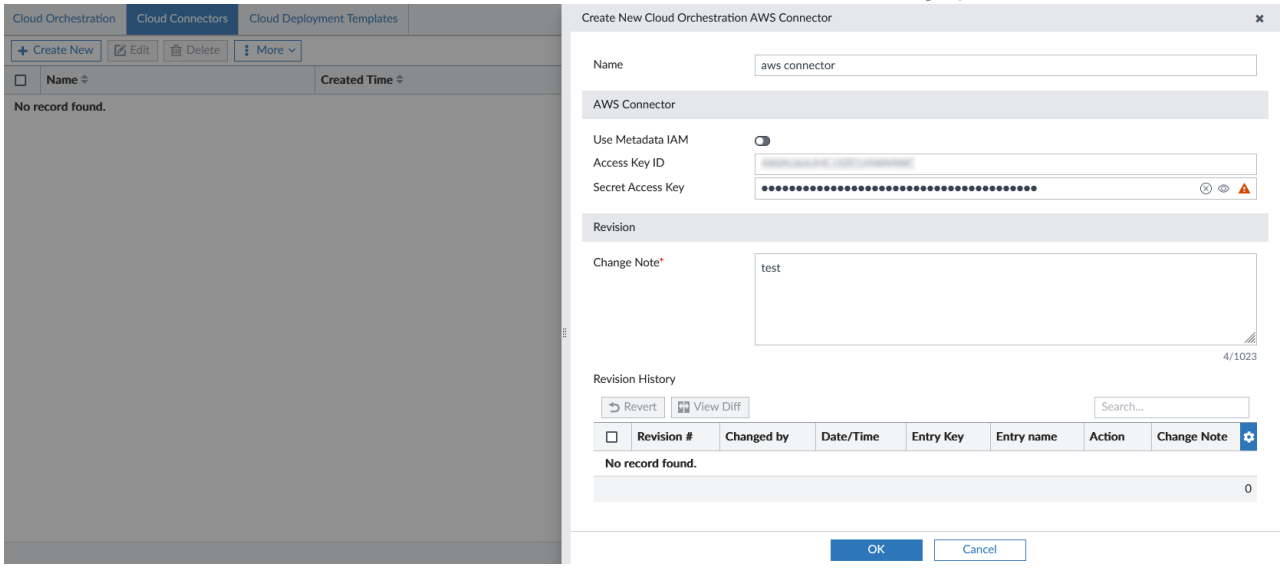
Once created, cloud connectors, deployment templates, and cloud orchestrations can be cloned, edited and deleted.

Creating cloud connectors

In order to use cloud orchestration with FortiManager, you must first configure a corresponding cloud orchestration connector to connect to the AWS server. After the cloud connector is created, you can select it from within a cloud orchestration configuration.

To create a cloud orchestration AWS connector:

1. Go to *Fabric View* > *Cloud Orchestration* > *Cloud Connectors*.
2. Click *Create New*. The *Create New Cloud Orchestration AWS Connector* dialog opens.



3. Configure the connector settings:

Name	Enter a name for the cloud orchestration connector.
Use Metadata IAM	When this setting is enabled, FortiManager will use the IAM information provided in metadata to access the cloud service, and you do not need to provide the *Access Key ID* or *Secret Access Key* for the cloud service. This setting is disabled by default.
Access Key ID	Enter your access key ID created from the AWS IAM console.
Secret Access Key	Enter your secret access key created from the AWS IAM console.

4. Click *OK* to save your configuration.

Creating cloud deployment templates

Cloud orchestration uses cloud deployment templates to specify the VPC and FortiGate ASG settings.

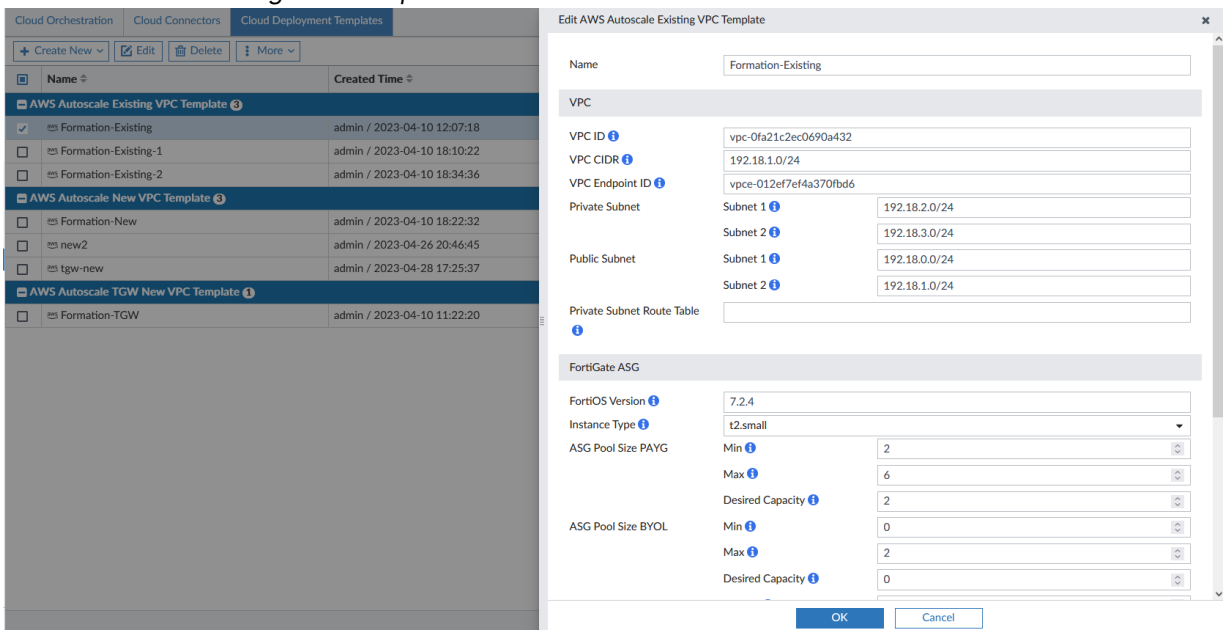
You can configure the following types of cloud deployment templates:

- AWS Autoscale Existing VPC Template.
- AWS Autoscale New VPC Template.
- AWS Autoscale TGW New VPC Template.

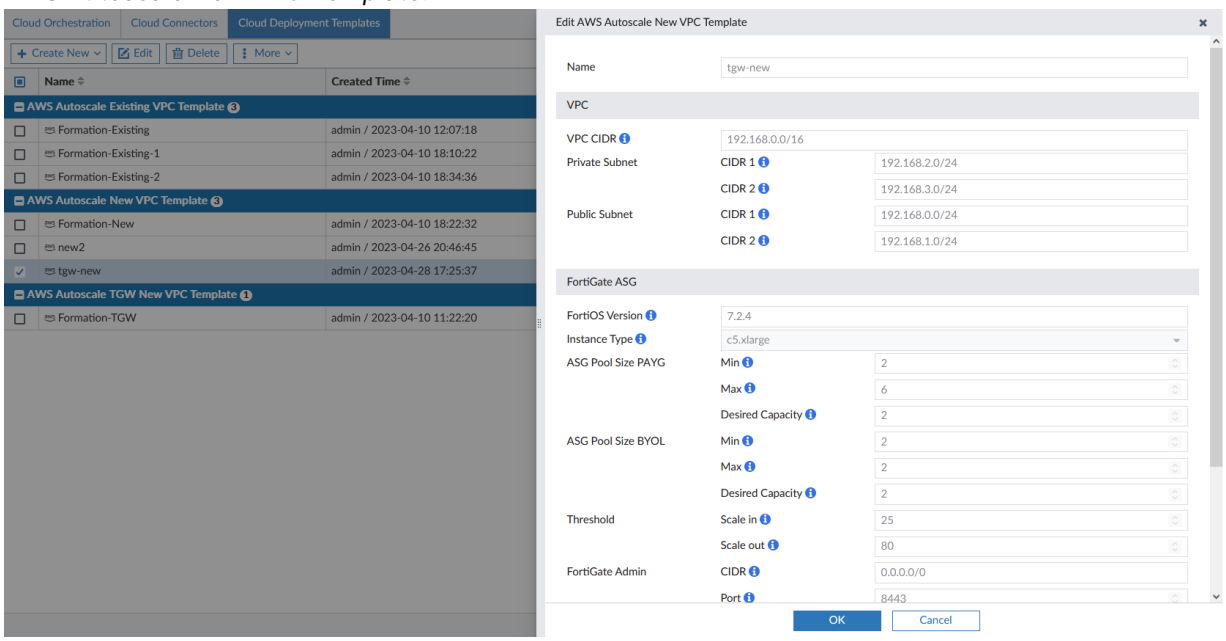
You can view a tooltip with information about each configurable setting in the GUI.

To create a cloud deployment template:

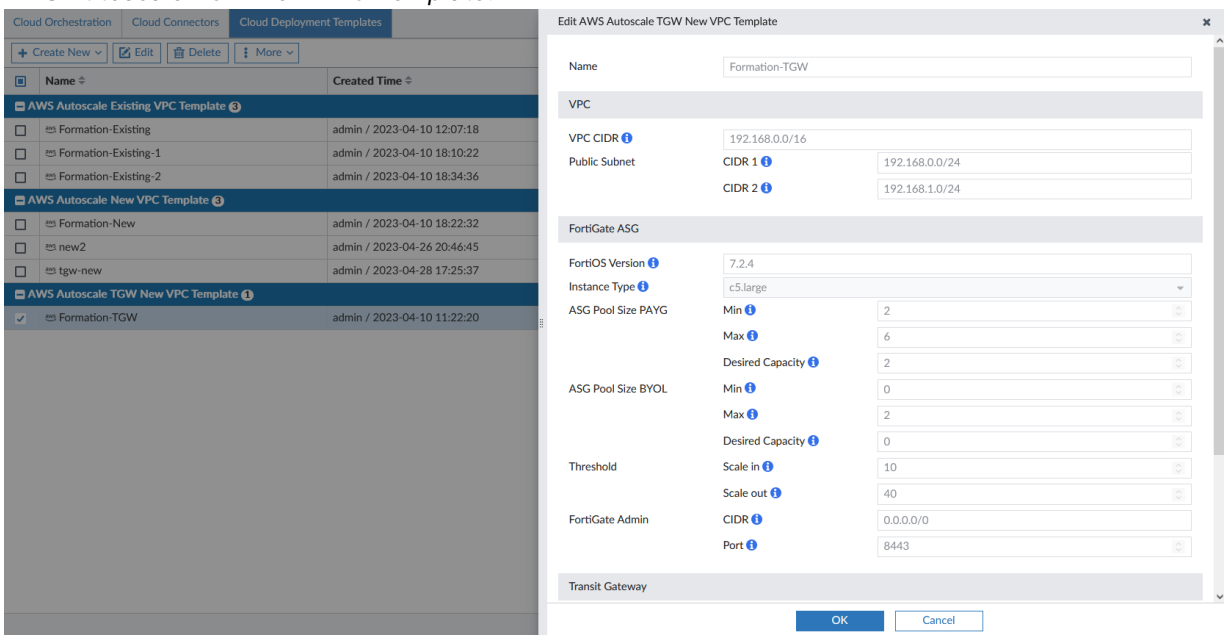
1. Go to *Fabric View* > *Cloud Orchestration* > *Cloud Deployment Templates*.
2. Click *Create New* and select a cloud deployment template. Settings vary depending on the template selected.
   You can configure the following types of templates:
   - *AWS Autoscale Existing VPC Template*.



- *AWS Autoscale New VPC Template.*



- *AWS Autoscale TGW New VPC Template.*



3. Enter a name for the template.
4. Configure the settings for your AWS VPC.
5. Configure the settings for your FortiGate ASG including the PAYG and/or BYOL pool size.
6. Optionally, provide an *Autoscale Notification Subscriber Email* to receive autoscale notifications. If provided, an email will be sent to the address to confirm the subscription.
7. Optionally, open the *Advanced Options* menu to see additional options including FortiAnalyzer integration options and advanced FortiGate ASG options.
   - When *FortiAnalyzer Integration Options* are enabled, cloud orchestrations using the template will deploy a FortiAnalyzer-VM on AWS in addition to the FortiGate ASG.

8. Click *OK* to save the template.

Upload BYOL licenses to the AWS bucket:

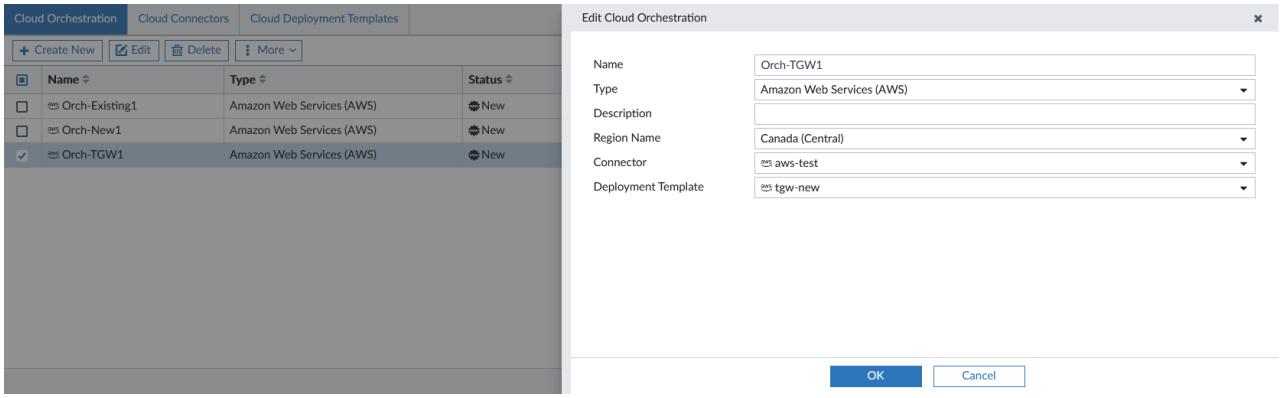
When configuring a cloud deployment template which includes any BYOL VMs, you must manually upload your BYOL license file(s) to AWS in the following location before deploying the cloud orchestration: *<S3Bucket>/assets/license-files/fortigate/* where *<S3Bucket>* is the default bucket created in each region, or the bucket specified in the Cloud Orchestration Template under *Advanced Options > Misc > S3 Bucket Name*.

Deploying cloud orchestration

Once you have configured a cloud connector to access the public cloud server and a deployment template to configure the deployment settings, you can create a cloud orchestration. Once the orchestration profile is created, you can deploy the cloud orchestration to the AWS public cloud to automatically create the FortiGate ASG and optional FortiAnalyzer-VM.

To configure cloud orchestration:

1. Go to *Fabric View > Cloud Orchestration*.
2. Click *Create New* to create a new cloud orchestration.



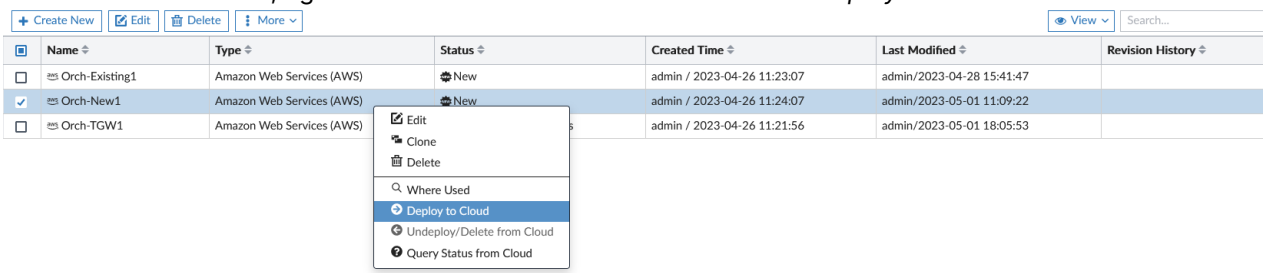
3. Enter the following information:

Name	Enter a name for the cloud orchestration.
Type	Select the cloud orchestration type.
Description	Optionally, enter a description.
Region Name	Select a region to deploy the cloud orchestration.
Connector	Choose a previously configured Cloud Orchestration Connector or click the plus icon to configure a new connector.
Deployment Template	Choose a previously configured Deployment Template or click the plus icon to configure a new template.

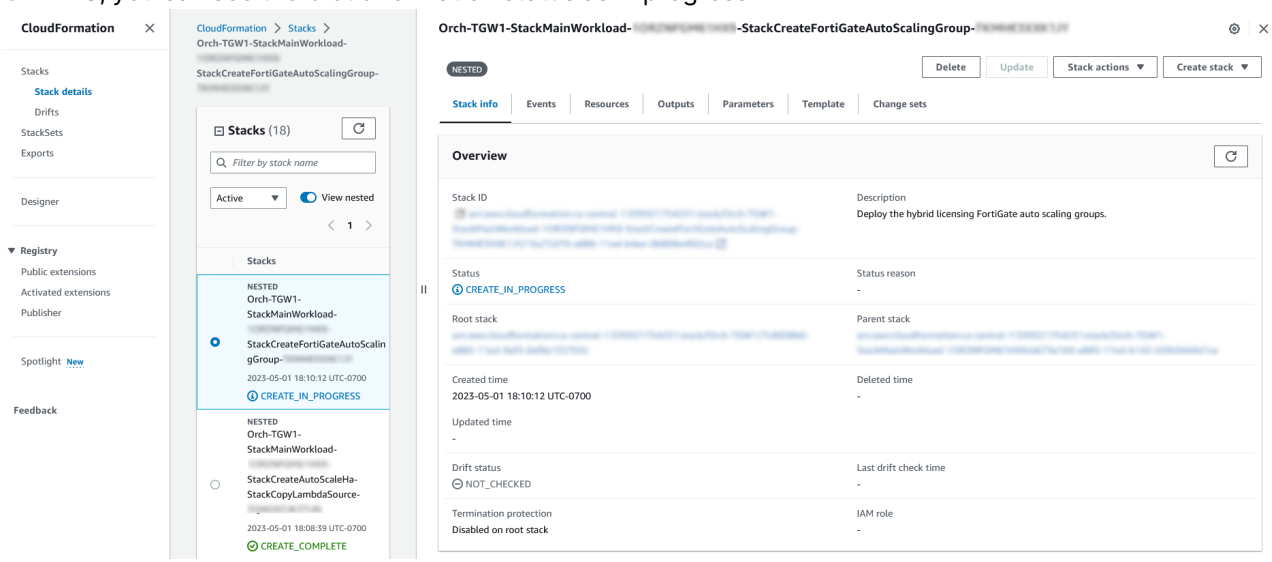
4. Click *OK* to save the cloud orchestration.
   The cloud orchestration appears in the table with a *Status* of *New*.

To deploy cloud orchestration:

1. In *Cloud Orchestration*, right-click on a cloud orchestration and click *Deploy to Cloud*.



2. On AWS, you can see the CloudFormation status as in progress.



3. Once the CloudFormation process is complete, you can see the cloud orchestration *Status* as *Deployed* on FortiManager.

To undeploy and delete a cloud orchestration from Cloud:

1. In *Cloud Orchestration*, right-click on a cloud orchestration and click *Undeploy/Delete from Cloud*.
   The cloud orchestration is undeployed in AWS CloudFormation.

The query the status from the cloud:

1. In *Cloud Orchestration*, right-click on a cloud orchestration and click *Query Status from Cloud*.
   The *Getting Status Information from Cloud* window opens.
2. The Status of the selected cloud orchestration is updated.

FortiGuard

The FortiGuard Distribution Network (FDN) provides FortiGuard services for your FortiManager system and its managed devices and FortiClient agents. The FDN is a world-wide network of FortiGuard Distribution Servers (FDS), which update the FortiGuard services on your FortiManager system on a regular basis so that your FortiManager system is protected against the latest threats.

The FortiGuard services available on the FortiManager system include:

- Antivirus and IPS engines and signatures
- Web filtering and email filtering rating databases and lookups
- Vulnerability scan and management support for FortiAnalyzer



FortiCare support contract required

In order to receive object updates from FortiGuard, FortiManager must have a valid FortiCare Elite or FortiCare Premium support contract.

To view and configure these services, go to *FortiGuard > Settings*. See Settings on page 812.



FortiManager-VM with a trial license does not support FortiGuard subscriptions and cannot act as a local FDS.



For information on current security threats, virus and spam sample submission, and FortiGuard service updates available through the FDN, including antivirus, IPS, web filtering, and email filtering, see the FortiGuard Center website, https://fortiguard.com.

This chapter contains the following topics:

- Using FortiManager as a local FDS on page 788
- Firmware revision management on page 789
- Device licenses on page 789
- Package management on page 791
- Query services on page 800
- Firmware images
- Settings
- Configuring devices to use the built-in FDS
- Configuring FortiGuard services
- Logging events related to FortiGuard services
- Restoring the URL or antispam database

Using FortiManager as a local FDS

In FortiGuard Management, you can configure the FortiManager system to act as a local FDS, or use a web proxy server to connect to the FDN.

FortiManager systems acting as a local FDS synchronize their FortiGuard service update packages with the FDN, then provide FortiGuard these updates and look up replies to your private network's FortiGate devices. The local FDS provides a faster connection, reducing Internet connection load and the time required to apply frequent updates, such as antivirus signatures, to many devices.

As an example, you might enable FortiGuard services to FortiGate devices on the built-in FDS, then specify the FortiManager system's IP address as the override server on your devices. Instead of burdening your Internet connection with all the devices downloading antivirus updates separately, the FortiManager system would use the Internet connection once to download the FortiGate antivirus package update, then redistribute the package to the devices.



FortiManager FDS updates available per platform

To see a list of which updates are available per platform when FortiManager is acting as a local FDS, see the FortiManager Release Notes.

Prerequisites for using FortiManager as a local FDS:

Before you can use your FortiManager system as a local FDS, you must:

- Register your devices with Fortinet Customer Service & Support and enable the FortiGuard service licenses. See your device documentation for more information on registering your products.
- FortiManager must have a valid FortiCare Elite or FortiCare Premium support contract.
- If the FortiManager system's Unregistered Device Options do not allow service to unauthorized devices, add your devices to the device list, or change the option to allow service to unauthorized devices. For more information, see the *FortiManager CLI Reference*.

  For information about FDN service connection attempt handling or adding devices, see Device Manager on page 88.
- Enable and configure the FortiManager system's built-in FDS. For more information, see Configuring network interfaces on page 902.
- Connect the FortiManager system to the FDN.

  The FortiManager system must retrieve service update packages from the FDN before it can redistribute them to devices and FortiClient agents on the device list. For more information, see Connecting the built-in FDS to the FDN on page 815.
- Configure each device or FortiClient endpoint to use the FortiManager system's built-in FDS as their override server. You can do this when adding a FortiGate system. For more information, see Add devices on page 91 and Configuring devices to use the built-in FDS.

Firmware revision management

FortiGuard Management also includes firmware revision management. To view and configure firmware options, go to *FortiGuard > Firmware Images*. You can download these images from the Customer Service & Support portal to install on your managed devices or on the FortiManager system.

See Firmware images on page 806.

Device licenses

On the *FortiGuard > Device Licenses* pane, you can view the status of all licenses for each managed device. This section includes the following topics:

- View licensing status on page 789

View licensing status

You can view license status for managed devices.

Following is a description of the icon states:

- Green: License OK
- Orange: License will expire soon
- Red: License has expired

To view the licensing status:

1. Go to *FortiGuard > Device Licenses*. This page displays the following columns of information:
   The following toolbar is displayed:

Refresh	Select the refresh icon to refresh the information displayed on this page.
Push Update	Push a license update to the selected device in the group.
Show License Expired Devices / Show All Devices	Toggle to hide and display only devices with an expired license.
Check License	Click to check expiry dates for licenses. The *Check License* dialog box is displayed. Select the FortiGuard license types that you want FortiManager to check expiry dates for and provide warnings when it is expired or approaching expiry date. The *FortiGuard Subscription* status is updated based on the selection in the Check License screen. If a license is expiring in 30 days, its license status is in orange (warning). If a license is expired already, the status is in red (error).

Export	Click to export the device list, device update details, and license details to an Excel, CSV, or PDF format. A file in the selected format is downloaded to the management computer.
Column Settings	Click to choose what columns to display on the *Device Licenses* page.
Search	Use the search field to find a specific device in the table.

The following columns of information are displayed:

Device Name	The device name or host name. You can change the order that devices are listed by clicking the column title.
Serial Number	The device serial number
Platform	The device type or platform.
ADOM	The name of the ADOM that contains the device. You can change the order that ADOMs are listed by clicking the column title.
Firmware Version	Displays the version of firmware installed on the device.
Support Contract	License status of the support contract. Hover over the license status to display expiration details about the following support contracts: hardware, firmware, enhanced support, and comprehensive support. License status can include: • N/A: No support contract • 24/7: Support contract level that provides support 24 hours per day and 7 days per week • 8/5: Support contract level
FortiGuard Subscription	Displays the license status of the FortiGuard subscription. The status reflects the worst license status of the individual components of the FortiGuard license. Hover over the license status to display details about the following components: IPS & Application Control, Antivirus, Web Filtering, and Email Filtering. License status can include: • All valid • Expires in <time> • Expired • Unknown
Service Status	License status of antivirus and IPS service. FortiManager calculates the status based on the FortiGate's last update request. Hover the mouse over the cell to display details about the service status. Licenses status can include: • Update Available • Up to Date • Expired • Unknown
Virtual Domains	Number of virtual domains. Click the cart icon to go to the Fortinet support site (https://support.fortinet.com)

Package management

When FortiManager is acting as a local FDS, antivirus and IPS signature packages are managed in *FortiGuard > Packages*. Packages received from FortiGuard and the service status of managed devices are listed in *Receive Status* and *Service Status*, respectively.

Receive status

To view packages received from FortiGuard, go to *FortiGuard > Packages > Receive Status*. This page lists received packages, grouped by platform.

The following information is displayed:

Refresh	Select to refresh the table.
Show Used Object Only	Clear to show all package information. Select to show only relevant package information.
Export	Select a package, and click *Export*. The package is compressed and downloaded to your management computer. You can import the package into another FortiManager.
Import	Click *Import* to select a package exported from another FortiManager and import it into this FortiManager.
Search	Use the search field to find a specific object in the table.
Package Name	The name of the package downloaded from FortiGuard.
Product	The name of the product supported by the package, such as FortiGate. Click the *Filter* icon to display the filter options. When a filter is active, the *Filter* icon is green. When the *Filter* icon is gray, no filter is applied.
Version	The package version. Click the *Filter* icon to display the filter options. When a filter is active, the *Filter* icon is green. When the *Filter* icon is gray, no filter is applied.
Service Entitlement	The name of the service entitlement that includes the package support.
Latest Version (Release Date/Time)	The package version.
Size	The size of the package.
To Be Deployed Version	The package version that is to be deployed. By default, the latest version is deployed. Select *Change* to change the version. When you export a package, only one version is exported. The *To Be Deployed Version* identifies what version is exported. See also Exporting packages example on page 795.
Update History	Click the icon to view the package update history.

Deployed version

To change the to be deployed version of a received packaged, click *Change* in the *To Be Deployed Version* column for the package.

The *Change Version* dialog box is displayed, allowing you to select an available version from the dropdown list.

Update history

When you click the *Update History* button for a package, the *Update History* pane is displayed for the package.

It shows the update times, the events that occurred, the statuses of the updates, and the versions downloaded.

Service status

To view service statuses, go to *FortiGuard > Packages > Service Status*. The service status information can be displayed by installed package name or by device name.

The following options are available in the toolbar:

Push Pending	Select the device or devices in the list, then click *Push Pending* in the toolbar to push pending updates to the device or devices.
Push All Pending	Select *Push All Pending* in the toolbar to push pending updates to all of the devices in the list.
Refresh	Select to refresh the list.
Column Settings	Select which fields are included in the service status table.
Display Options	Displays the available display options including *Show Pending Device Only* and *Group by ADOMs*. This option is only available while viewing service status *By Device*.
By ADOM	Displays the service status information for all devices in the selected ADOM (s). By default, this is set to *All ADOMs*. This option is only available while viewing service status *By Device*.
By Package	Displays the service status information by installed package name.
By Device	Displays the service status information by device name.
Search	Use the search field to find a specific device or package in the table.

Service status by Device

When you click the *By Device* button in the toolbar, the *Service Status* page displays a list of all the managed FortiGate devices, their last update time, and their status.

You can pushing pending updates to the devices, either individually or all at the same time. You can refresh the list by clicking *Refresh* in the toolbar.

Device	The device serial number or host name is displayed.

Status	The service update status. A device's status can be one of the following: • *Up to Date*: The latest package has been received by the FortiGate unit. • *Never Updated*: The FortiGate unit has never requested or received the package. • *Pending*: The FortiGate unit has an older version of the package due to an acceptable reason (such as the scheduled update time having not come yet). Hover the mouse over a pending icon to view the package to be installed. • *Problem*: The FortiGate unit missed the scheduled query, or did not correctly receive the latest package. • *Unknown*: The FortiGate unit's status is not currently known.
Last Update Time	The date and time of the last update.

Service status by Package

When you click the *By Package* button, the *Service Status* page shows a list of all the installed packages, the applicable firmware version, the package version, and the progress on package installation to devices. You can drill-down to view the installed device list.

The content pane displays the following information:

Installed Packages Name	The name of the installed package.
Applicable Firmware Version	The firmware version of the device for which the installed package is created.
Package Version	The version of the installed package.
Installed Devices	The package installation progress for the devices. Click the *<number> of <number>* link to view the installed device list.

To view the installed device list:

1. Go to *FortiGuard > Packages > Service Status*.
2. In the toolbar, click *By Package*.
   The list of installed packages is displayed.
3. In the *Installed Devices* column, click the *<number> of <number>* link for the installed package.
   Device details are displayed.

Device Name	The name of the device.
Current Version	The version of the package.
Status	The device update status.
Last Update Time	The time of the last package update.

4. Click the *Back* arrow to return to the previous page.

IoT packages

You can enable download of packages for the Internet of Things (IoT) service by using the CLI. Following is a summary of how FortiManager handles the IoT packages:

1. FortiManager downloads packages from FortiGuard.
2. FortiManager merges the downloaded packages into *Run Database*.
3. FortiManager provides the query service.



Downloads of IoT packages from FortiGuard to FortiManager are currently supported only when Anycast is enabled on FortiManager.



In FortiManager 7.4.1 and later, the IoT query services must be enabled separately using the FortiManager CLI.

See Enabling IoT query services on page 805.

Several databases are used for IoT packages. Use the `diagnose fmupdate fgd-dbver` command to view the following databases for IoT packages:

- `iots`: IoT single MAC database
  object ID: `00000000IOTS0000`
  Contains IoT info with entry of a single MAC. Considered a *delta* object because each version contains parts of data, and FortiManager merges all valid data, which is the same as the URL query service.
- `iotr`: IoT range MAC database
  object ID: `00000000IOTR0000`
  Contains IoT info with entry of a MAC range. Considered a *regular* object, and FortiManager uses only the latest version.
- `iotm`: IoT mapping database
  object ID: `00000000IOTR0000`
  Regular object used to map the info data to strings in tag-length-value (TLV) format.

To configure IoT package download:

1. Enable Anycast on FortiManager:
```
config fmupdate fds-setting
   set fortiguard-anycast enable
end
```
2. Enable the IoT query service:
```
config fmupdate service
   set query-iot enable
end
```
3. Configure downloading of IoT packages:
```
config fmupdate web-spam fgd-setting
   set iot-log nofilequery
   set iot-preload enable
   set restrict-iots-dbver <string>
end
```

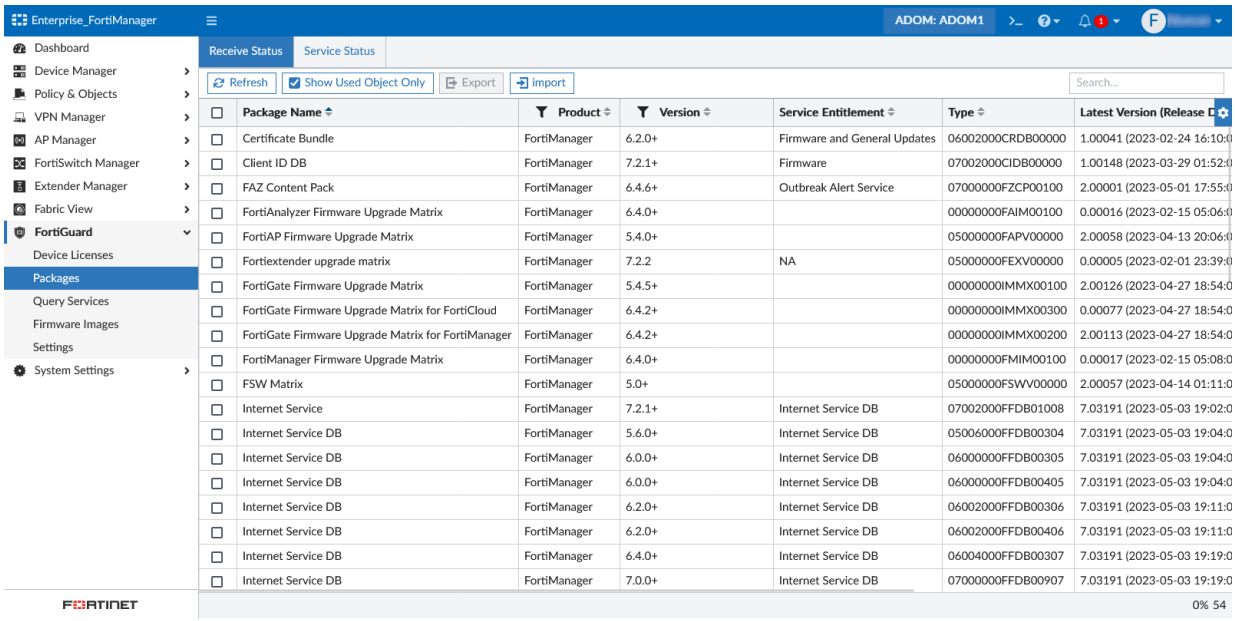
Exporting packages EXAMPLE

You can export one or more packages from FortiManager to a compressed file, so you can import the packages into another FortiManager. This is useful when you want to add packages to a FortiManager operating in a closed network.

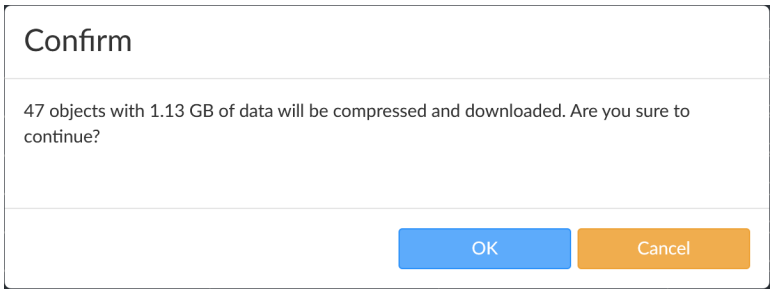
You can specify what version of the package to export.

To export packages:

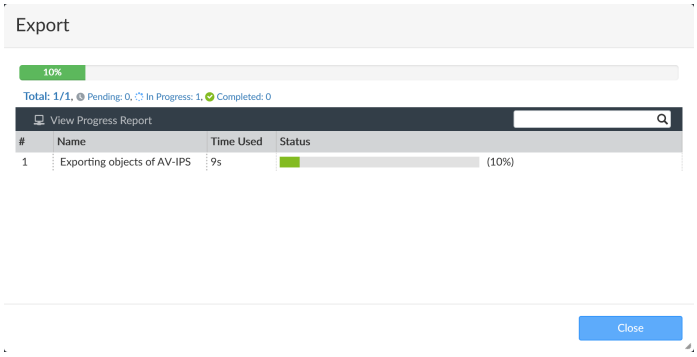
1. Go to *FortiGuard* > *Packages* > *Receive Status*.
2. In the *Search* box, type the name of the product, and press *Enter*.
   The search results are displayed.



3. Specify the version to export by using the *To Be Deployed* column.
   By default, the latest version is deployed, and the latest version is included in the export. However, you can specify a different version for deployment, and the specified version is included in the export.
   a. In the *To Be Deployed* column, click *Change*.
      The *Change Version* dialog box is displayed.
      image
   b. In the *Change to Version* box, select the version to deploy, and click *OK*.
      The *To Be Deployed* column displays the selected version.
4. Select one or more packages, and click *Export*.
   The *Confirm* dialog box is displayed.



5. Click *OK*.
   The progress of the process is displayed with the object is compressed and downloaded to your management computer.



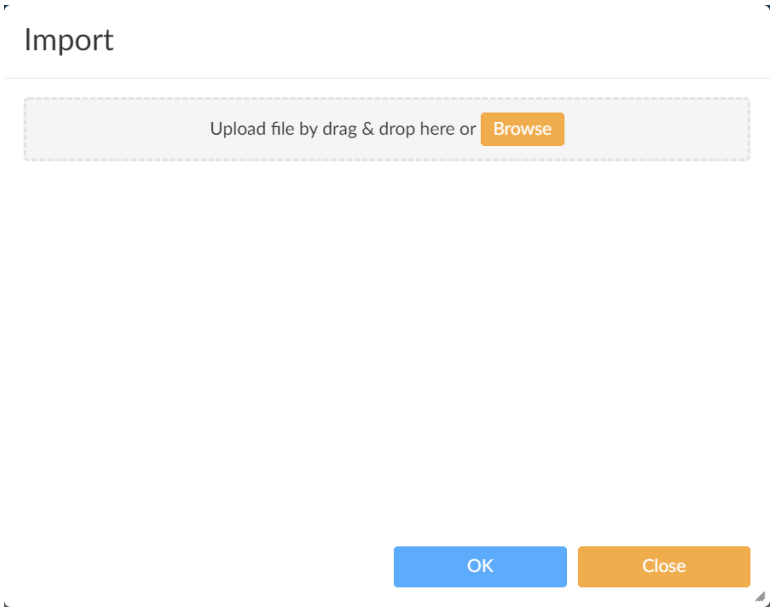
6. Click *Close* to close the dialog box.

Importing packages EXAMPLE

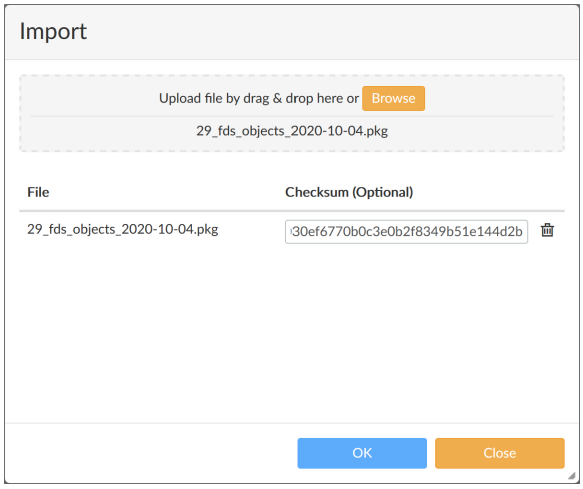
You can import packages that you exported from another FortiManager.

To import packages:

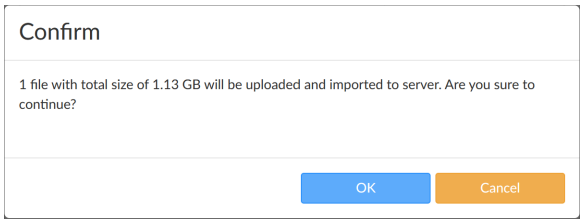
1. Go to *FortiGuard* > *Packages* > *Receive Status*.
2. Click *Import* box.
   The Import dialog box is displayed.



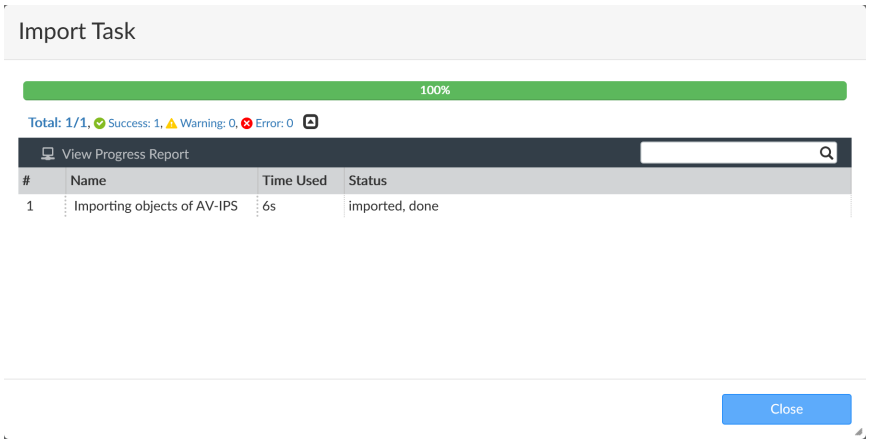
3. Drag and drop the exported package onto the dialog box.
   The dialog box updates.



4. Click *OK*.
   A confirmation dialog box is displayed.



5. Click *OK*.
   The progress of the process is displayed while the object is imported to FortiManager.



6. Click *Close*.

Manually specifying a package version to deploy

You can manually specify which version of a package is available for deployment on devices when FortiManager is acting as the FortiGuard server.

By default, FortiManager provides the latest object versions to FortiGate when it requests an update. FortiManager administrators can change this configuration by specifying a *To Be Deployed Version* of the package.

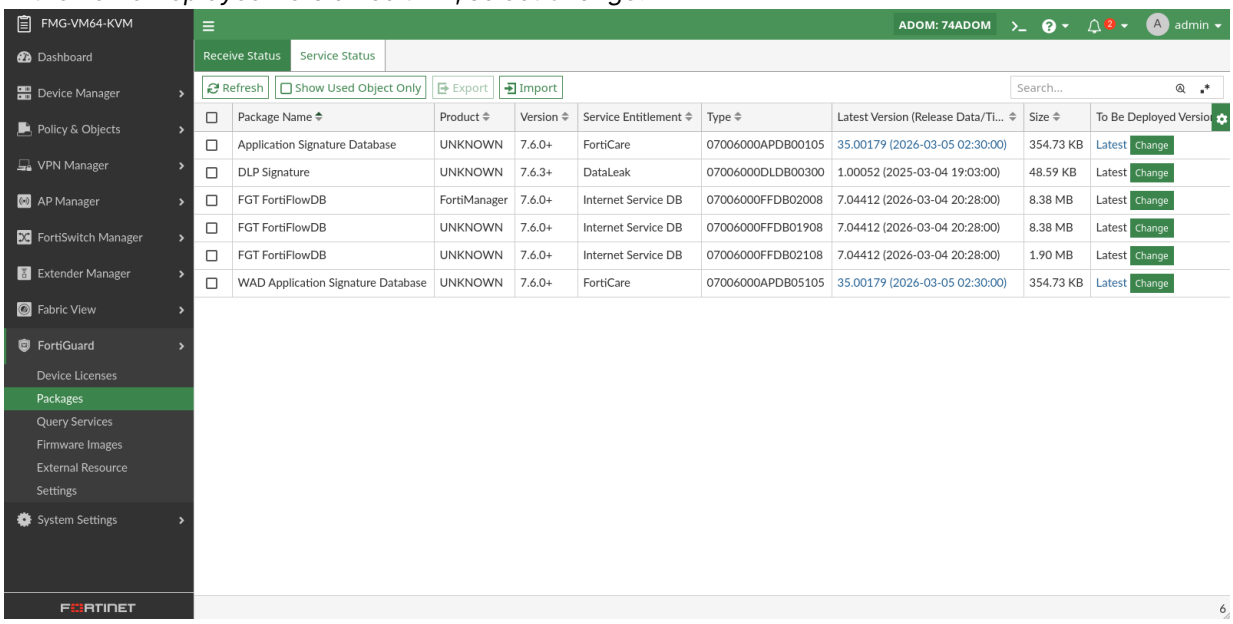
For example, administrators can search for application signature objects and set the *To Be Deployed Version* to be any previous version of the package. FortiManager will only provide that version to FortiGate instead of the latest version.

If the FortiGate device is already using a package version that is newer than the one selected, the FortiGate will remain on its current package version and will not be downgraded. FortiManager will not provide any package versions that are newer than the preferred version.

To choose the version of a package to be deployed:

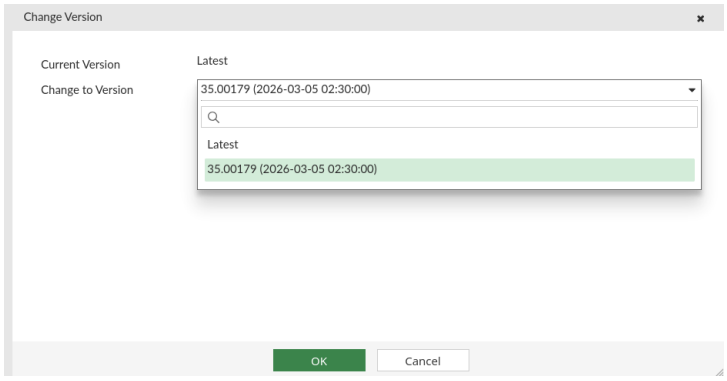
1. Go to *FortiGuard* > *Packages* > *Receive Status*.
2. Uncheck *Show Used Objects Only* and then search for the package (for example, application signature objects).

3. In the *To Be Deployed Version* column, select *Change*.



The *Change Version* window opens.

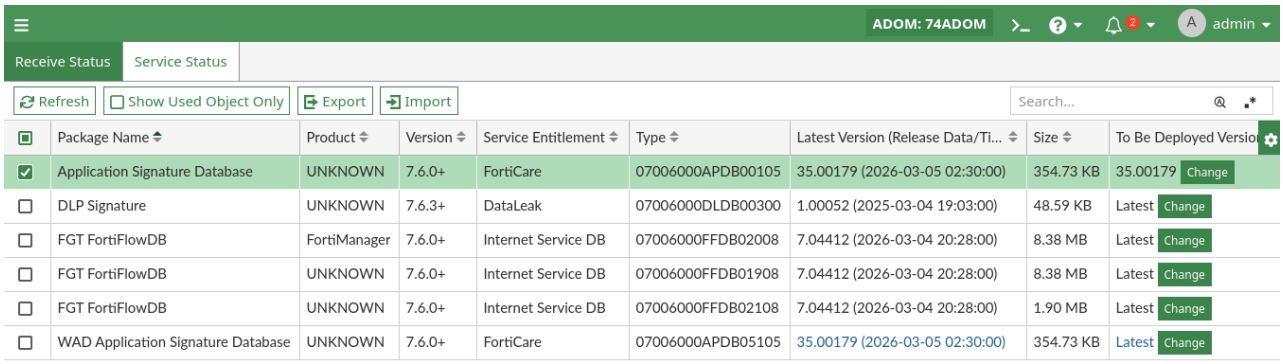
4. In the *Change to Version* field, select the desired version to be deployed. By default, this field is set to *Latest*.





By default, FortiManager retains a maximum of 20 object versions.

5. Click *OK* to save your selection. The selected version is displayed in the *To Be Deployed Version* column.



Query services

Query Services shows when managed devices query FortiManager acting as a local FDS. It displays when managed devices receive updates from the server, the update version, the size of the update, and the update history. It also has graphs showing the number of queries from all the managed FortiGate units made to FortiManager.

Receive status

The view the received packages, go to *FortiGuard > Query Services > Receive Status*.

The following information is displayed:

Refresh	Select to refresh the table.
Export	Select a package, and click *Export*. The package is compressed and downloaded to your management computer. You can import the package into another FortiManager.
Import	Click *Import* to select a package exported from another FortiManager and import it into this FortiManager.
Search	Use the search field to find a specific entry in the table.
History	The record of received packages.
Package Received	The name of the received package.
Latest Version (Release Date/Time)	The latest version of the received package.
Size	The size of the package.
Update History	Click to view the package update history.

Update history

When you click the *Update History* button for a package, the *Update History* pane is displayed for the package.

It shows the update times, the events that occurred, the statuses of the updates, and the versions downloaded.

Query status

Go to *FortiGuard > Query Services > Query Status* to view graphs that show:

- The number of queries made from all managed devices to the FortiManager unit over a user selected time period
- The top ten unrated sites
- The top ten devices for a user selected time period

The following information is displayed:

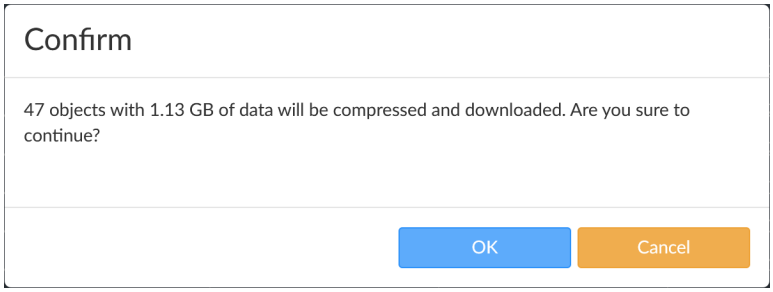
Top 10 Unrated Sites	Displays the top 10 unrated sites and the number of events. Hover the cursor over a row to see the exact number of queries.
Top 10 Devices	Displays the top 10 devices and number of sessions. Hover the cursor over a row to see the exact number of queries. Click a row to see a graph of the queries for that device.
Number of Queries	Displays the number of queries over a period of time.

Exporting web filter databases EXAMPLE

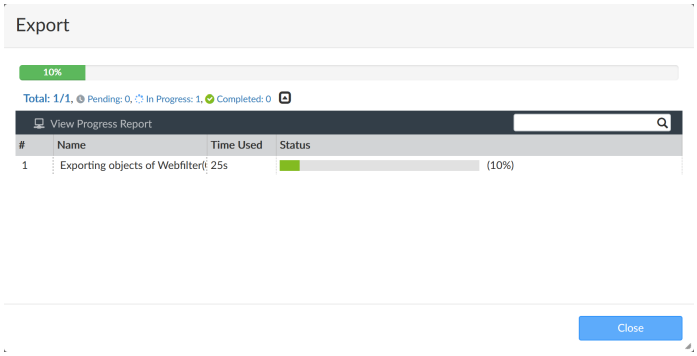
You can export one or more web filter databases from FortiManager to a compressed file, so you can import the web filter database into another FortiManager. This is useful when you want to add a web filter database to a FortiManager operating in a closed network.

To export web filter databases:

1. Go to *FortiGuard > Query Services > Receive Status*.
2. Select *Webfilter*, and click *Export*.
   The *Confirm* dialog box is displayed.



3. Click *OK*.
   The progress of the process is displayed while the object is compressed and downloaded to your management computer.



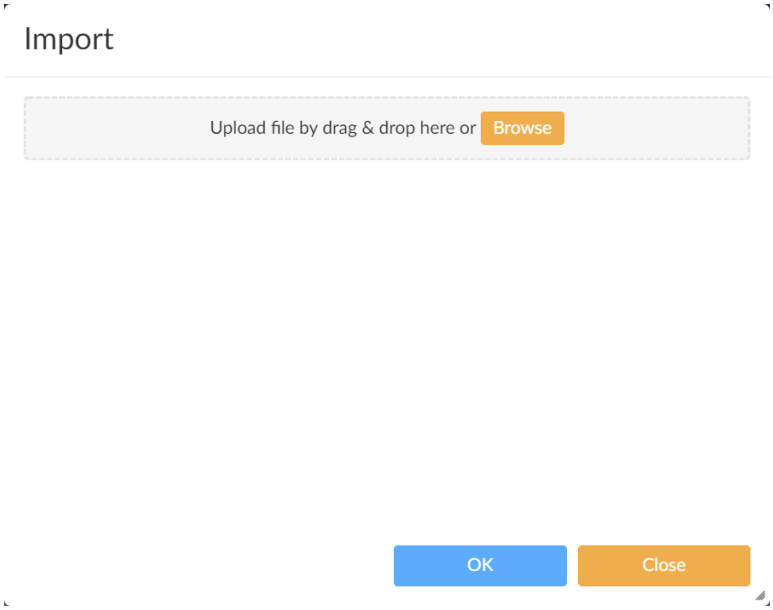
4. Click *Close* to close the dialog box.

Importing web filter databases EXAMPLE

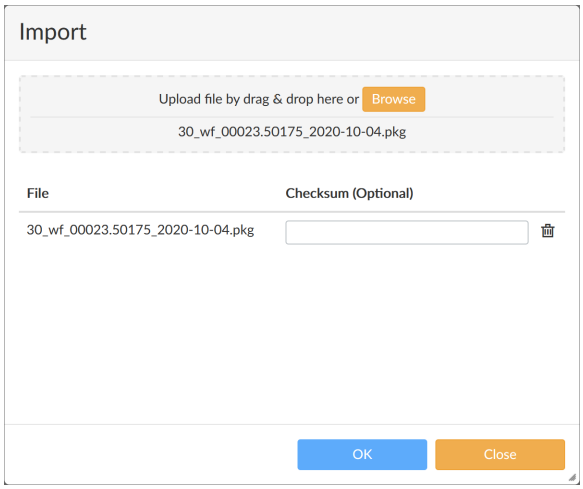
You can import web filter databases that you exported from another FortiManager.

To import web filter databases:

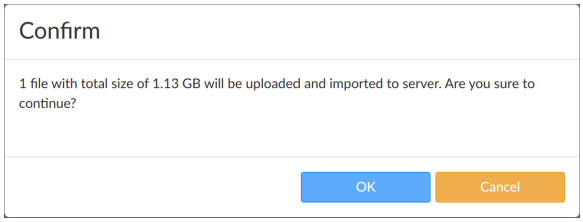
1. Go to *FortiGuard > Query Services > Receive Status*.
2. Click *Import* box.
   The Import dialog box is displayed.



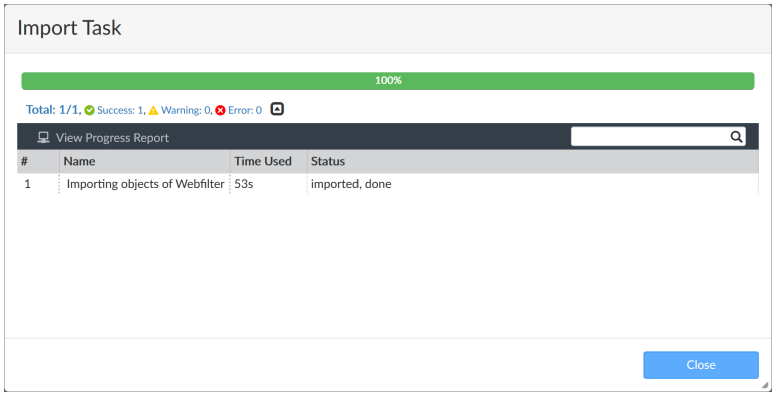
3. Drag and drop the exported package onto the dialog box.
   The dialog box updates.



4. Click *OK*.
   A confirmation dialog box is displayed.



5. Click *OK*.
   The progress of the process is displayed while the object is imported to FortiManager.

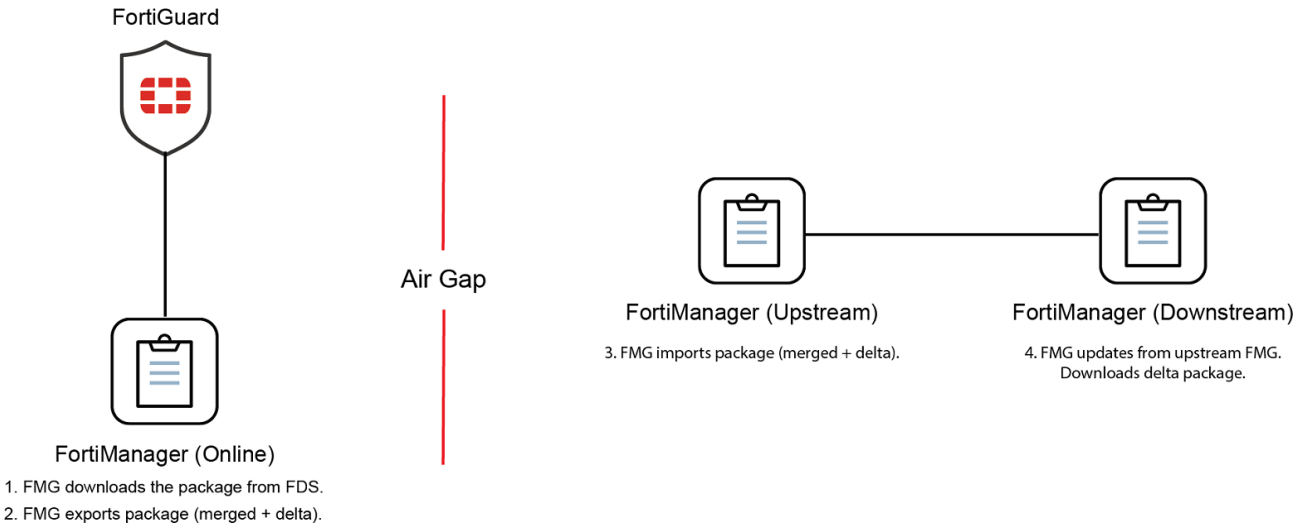


6. Click *Close*.

Providing delta updates to downstream FortiManagers in cascade mode

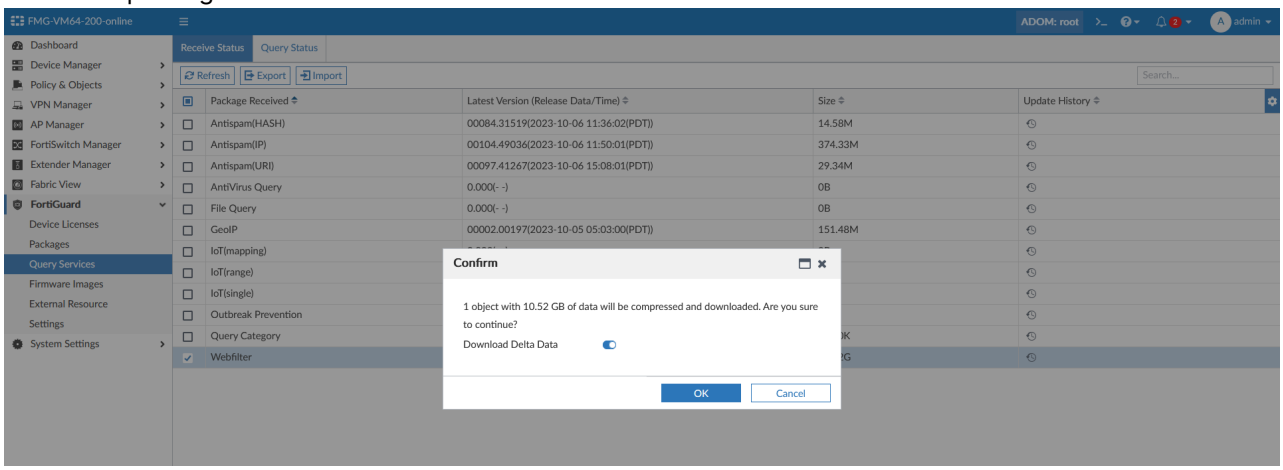
FortiManagers connected to FDS have the option to download delta packages from FortiGuard when exporting FortiGuard packages.

When the package is imported into the upstream FortiManager, the upstream FortiManager can provide the delta package update to downstream FortiManagers instead of the entire merged package, saving bandwidth.

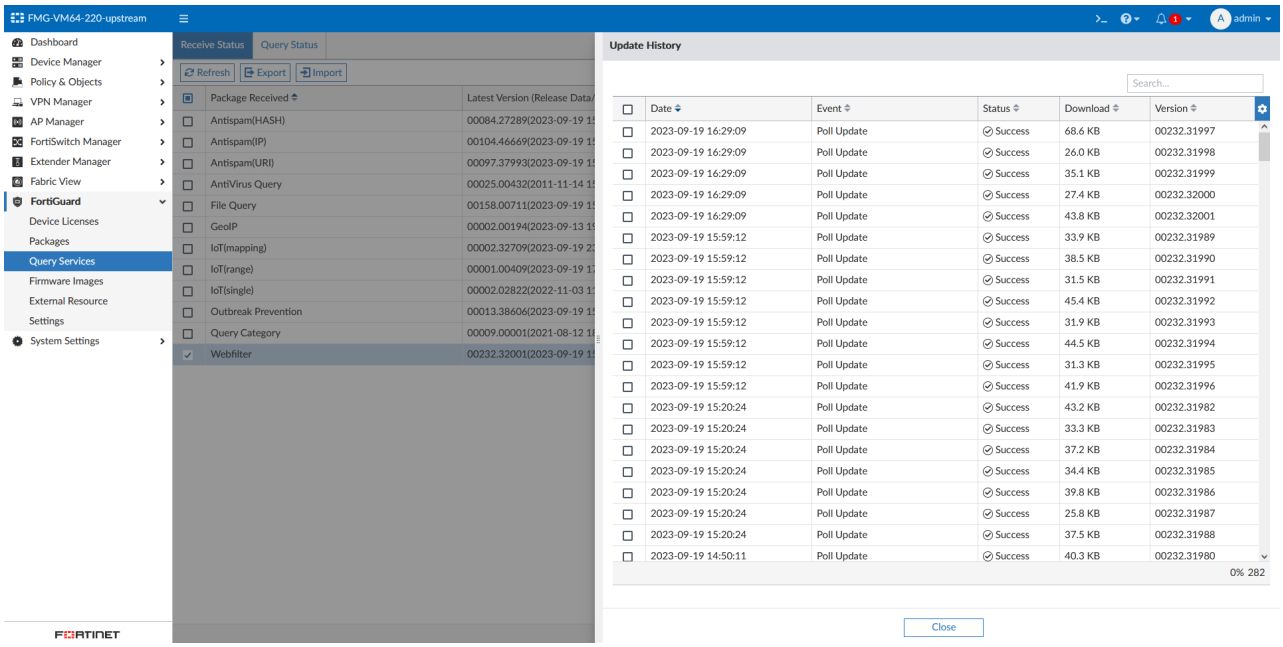


To provide delta updates to downstream FortiManager:

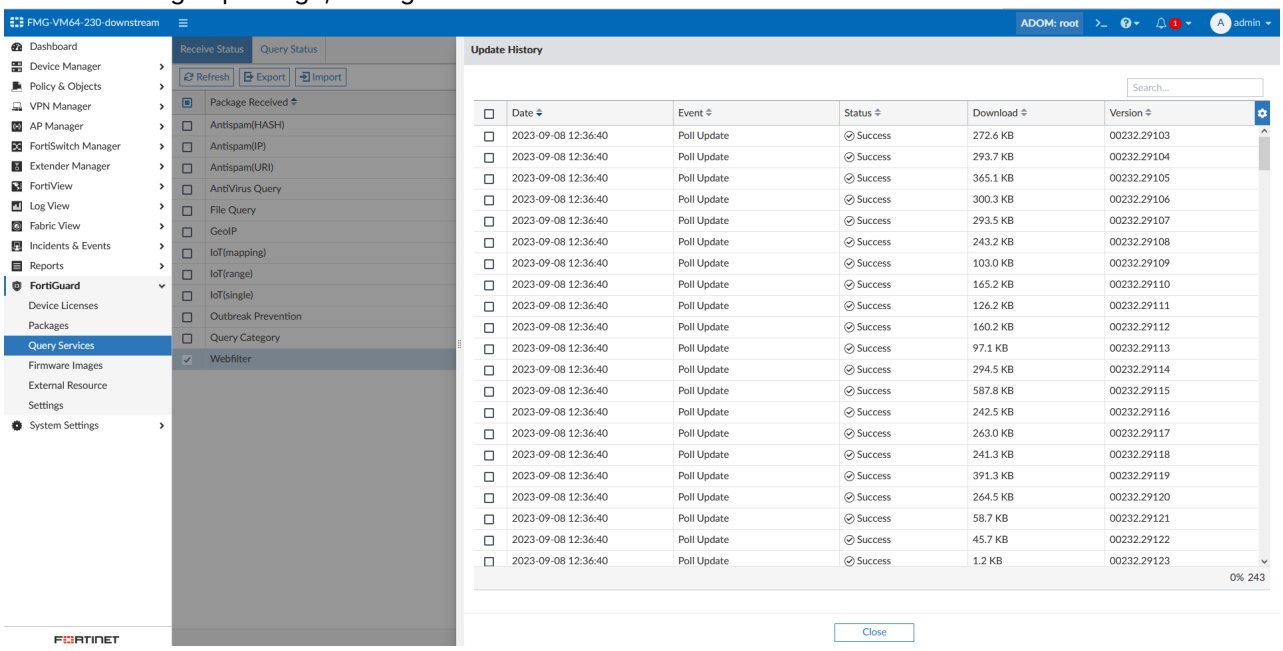
1. On the online FortiManager, go to *FortiGuard* > *Query Services* > *Receive Status*, and *Export* the FortiGuard package.
   A dialog appears with the option to enable or disable delta package downloads.
2. Enable the *Download Delta Data* toggle. When enabled, the merged FortiGuard package will be downloaded with delta packages.



3. On the upstream FortiManager, go to *FortiGuard* > *Query Services* > *Receive Status* and *Import* the package with the delta packages. The download history shows the imported delta packages.



4. The downstream FortiManager can pull delta packages from the upstream FortiManager instead of getting the entire merged package, saving bandwidth.



Enabling IoT query services

In FortiManager 7.4.1 and later, the IoT Query, IoT Vulnerability Query, and IoT Collection Query services must be enabled or disabled separately using the following FortiManager CLI commands:

Command	Description
`query-iot`	Enable/disable IOT query service (default = disable).
`query-iot-collection`	Enable/disable IOT collection query service (default = disable).
`query-iot-vulnerability`	Enable/disable IOT vulnerability query service (default = disable).

To enable the IoT query services:

1. Enter the FortiManager CLI.
2. Enable the required IoT query service(s):

```
config fmupdate service
   set query-iot {enable | disable}
   set query-iot-vulnerability {enable | disable}
   set query-iot-collection {enable | disable}
end
```

For more information, see the FortiManager CLI Reference.

Firmware images

Go to *FortiGuard > Firmware Images* to manage the firmware images stored on the FortiManager device. You can import firmware images for FortiGate, FortiAnalyzer, FortiManager, FortiAP, FortiExtender, FortiSwitch, and FortiProxy.

You can download only those images that are needed from the FDS systems, and customize which firmware images are available for deployment.



FortiGate devices must have a valid Firmware & General Updates (FMWR) contract in order for firmware updates to be performed through FortiManager. This applies to firmware images from FortiGuard and images that are manually uploaded to FortiManager.

When a FortiGate device is added to the FortiManager, a 24 hour grace period is provided in which firmware updates can be applied without a license to allow time for the FMWR contract information to synchronize from FortiCare. FortiManager expects the managed device to be on the same FortiCloud account, or have the device serial number added in FortiGuard's auth list.

The following information and settings are available:

Import Images	Select to open the firmware image import list.
Models	From the dropdown list, select *All* to show all the available models on the FortiGuard server, or select *Managed* to show only the models that are currently being managed by the FortiManager device.
Product	Select a managed product type from the dropdown list.

Search	Use the search field to find a specific entry in the table.
Seq.#	The sequence number.
Model	The device model number that the firmware is applicable to.
Latest Version (Release Date/Time)	The latest version of the firmware that is available.
Preferred Version	The firmware version that you would like to use on the device. Click *Change* to open the *Change Version* dialog box, then select the desired version from the dropdown list and select *OK* to change the preferred version.
Size	The size of the firmware image.
Status	The status of the image, that is, from where it is available.
Action Status	The status of the current action being taken.
Release Notes	A link to a copy of the release for the firmware image that has been downloaded.
Download/Delete	Download the firmware image from the FDS if it is available. If the firmware images has already been downloaded, then delete the firmware image from the FortiManager device.

For information about upgrading your FortiManager device, see the FortiManager Release Notes or contact Fortinet Customer Service & Support.

To import a firmware image:

1. Go to *FortiGuard > Firmware Images*, and click *Import Images* in the toolbar.
2. Select a device in the list, and click *Import* in the toolbar. The *Firmware Upload* dialog box, opens.
3. Click *Browse* to browse to the desired firmware image file, or drag and drop the file onto the dialog box.
4. Click *OK* to import the firmware image.



Firmware images can be downloaded from the Fortinet Customer Service & Support site at https://support.fortinet.com/ (support account required).

To delete firmware images:

1. Go to *FortiGuard > Firmware Images*, and click *Import Images* in the toolbar.
2. Select the firmware images you would like to delete.
3. Click *Delete* in the toolbar. A confirmation dialog box appears.
4. Click *OK* to delete the firmware images.

Download prioritization

When FortiManager is acting as a local FDS, you can prioritize downloads from FortiGuard to FortiManager by product and version and/or package.

Go to *FortiGuard > Download Prioritization* to enable download prioritization. The following settings are available:

Enable by Product	Toggle *ON* to enable download prioritization by product and version. See Product download prioritization on page 808.
Enable by Package	Toggle *ON* to enable download prioritization by package. See Package download prioritization on page 809.

Before you can specify a priority list, you must enable products and versions for prioritization.

Some products cannot be prioritized, such as FortiCache, FortiWeb, FortiDDoS, FortiProxy, and FortiNAC.

To enable products and versions for prioritization:

1. Go to *FortiGuard > Settings*.
2. Under *Enable AntiVirus and IPS Service*, select the versions for each product.
3. Click *Apply*.

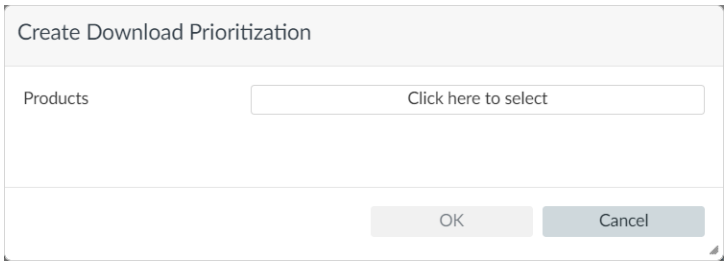
Product download prioritization

You can add products and versions to the download prioritization list, and then specify the download priority for the selected products and versions. Top priority is number 1.

When FortiManager downloads packages for products from FDN, it downloads packages based on the priority first, starting at priority number 1.

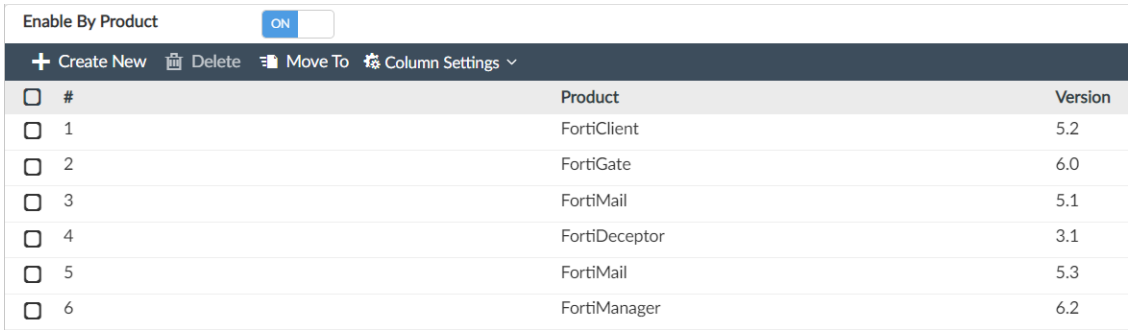
To enable product download prioritization:

1. Go to *FortiGuard > Download Prioritization*, and toggle *Enable by Product* to *ON*.
2. Add products to the priority list:
   a. In the toolbar, click *Create New*.
   The *Create Download Prioritization* dialog box is displayed.



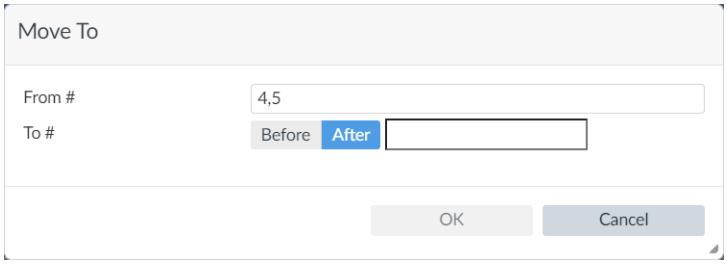
b. Beside *Products*, click the box, and select one or more products and versions, and click *OK*.
The selected products are displayed in the product list.

c. Click *OK*.
The products are displayed in the priority list.



3. Specify the download priority for products:

a. Select one or more products, and click *Move To*.
The *Move To* dialog box is displayed.



b. Beside *To #*, select *Before* or *After*, and click the box to use the up and down arrows to position the selected products in the priority list.

c. Click *OK*.
The products are moved, and the updated priority list is displayed.
You can remove products from the priority list. Select one or more products, and click *Delete*.

4. (Optional) Add packages to the priority list. See Package download prioritization on page 809.

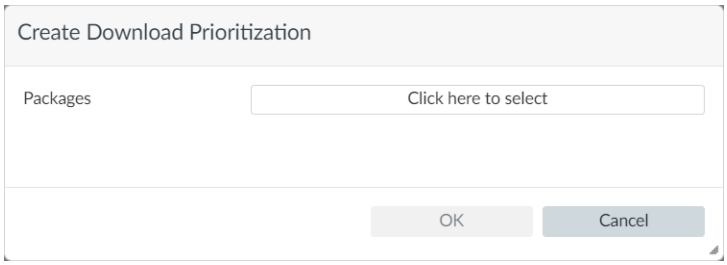
Package download prioritization

You can add packages the download prioritization list, and then specify the download priority for the selected packages. Top priority is number 1.

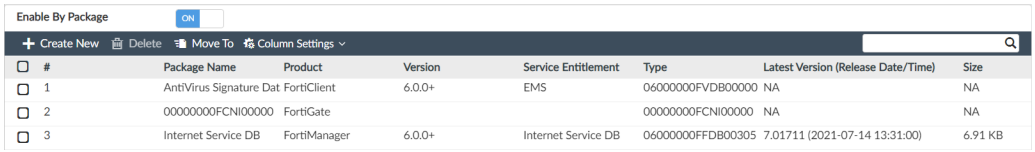
When FortiManager downloads packages from FortiGuard, it downloads packages based on the priority list, starting at priority number 1.

To enable package download prioritization:

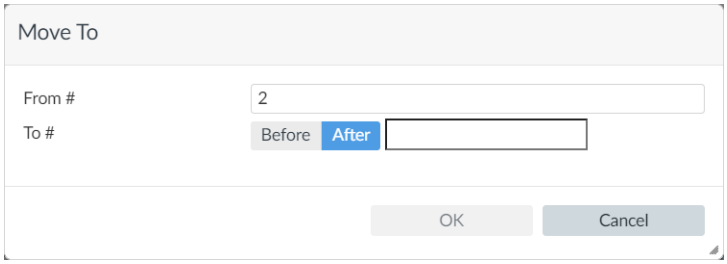
1. Go to *FortiGuard > Download Prioritization*, and toggle *Enable by Package* to *ON*.
2. Add packages to the priority list:
   a. In the toolbar, click *Create New*.
   The *Create Download Prioritization* dialog box is displayed.



   b. Beside *Packages*, click the box, and select one or more packages, and click *OK*.
   The selected packages are displayed in the packages list.
   c. Click *OK*.
   The packages are displayed in the priority list.



3. Specify the download priority for the packages:
   a. Select one or more packages, and click *Move To*.
   The *Move To* dialog box is displayed.



   b. Beside *To #*, select *Before* or *After*, and click the box to use the up and down arrows to position the selected packages in the priority list.
   c. Click *OK*.
   The packages are moved, and the updated priority list is displayed.
   You can remove packages from the priority list. Select one or more packages, and click *Delete*.
4. (Optional) Add products and versions to the priority list. See Product download prioritization on page 808.

External resources

FortiManager allows external resources to be uploaded in order to support FortiManager hosted resources for threat feeds.

After external resources are uploaded to FortiManager, they can be used in threat feeds using the following format as the URI of the resource: `fmg://<filename>.`

For example, if you have uploaded a resource called `exresource1.txt` to FortiManager, the URI would be `fmg://exresource1.txt`.

For more information on threat feeds, see Threat Feeds on page 744.

To upload an external resource to FortiManager:

1. Go to *FortiGuard > External Resource*.
2. Click *Import* in the toolbar.
3. Drag and drop a file into the selection window or browse to your file location.
4. Click *OK*. Uploaded files are displayed in the *External Resources* table and can be edited directly in the FortiManager GUI.

To edit external resource file content:

1. In the external resource file list, select a file and do one of the following:
   a. Click *Edit* in the toolbar.
   b. Right-click and select *Edit* from the context menu.
2. The content of the file is displayed and can be edited directly in the *Content* pane.
3. Click *OK* to save changes to the external resource.

To create a threat feed using a FortiManager hosted resource:

1. Go to *Policy & Objects > Security Fabric > Threat Feeds*.



If the *Threat Feeds* tab is not visible, it must first be enabled in *Tools > Feature Visibility*. You can also create Threat Feeds in *Fabric View > External Connectors*.

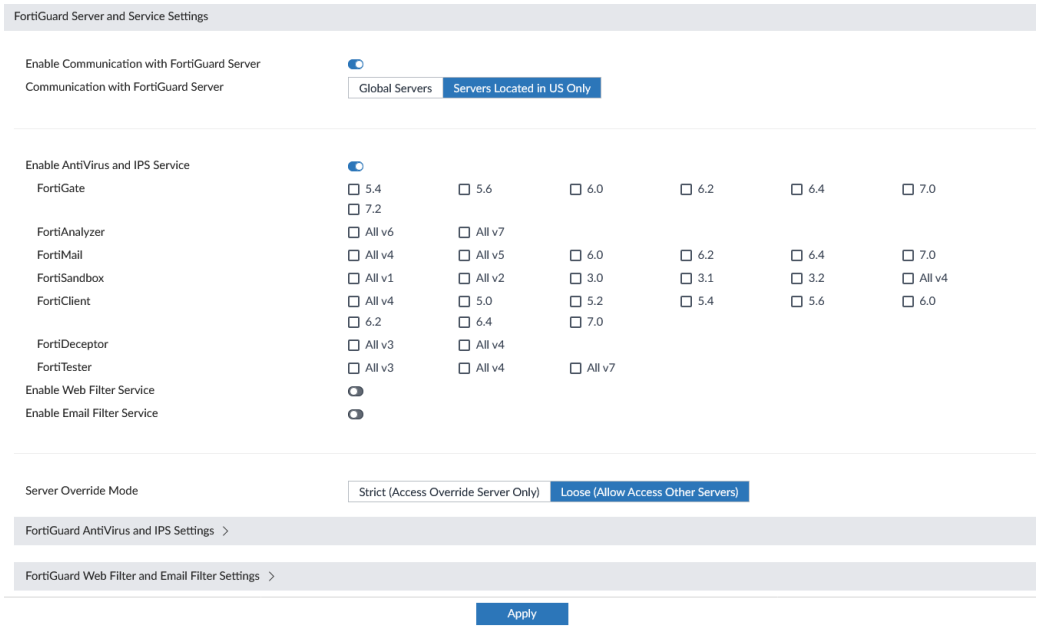
2. Create a new threat feed.
3. Select the threat feed type. For example, if the uploaded file is a list of IP addresses, you must select *Type > IP Address*.
4. In the *URI of External Resource* field, define the file using the following format: `fmg://filename`.
5. Once the threat feed is created, you can use it in a policy and install it to a device. In the example below, the threat feed is used in a DNS Filter in *Policy & Objects > Security Profiles > DNS Filter*. The DNS Filter is applied to a policy and installed to the managed FortiGate.
6. Details about the threat feed can be viewed on FortiGate.
   a. On FortiGate, go to *Security Fabric > External Connectors*. The content can be refreshed automatically or manually on this page.
   b. Click *View Entries* to see the content from the external resource.

Settings

FortiGuard > Settings provides a central location for configuring and enabling your FortiManager system's built-in FDS as an FDN override server.

By default, this option is enabled. After configuring FortiGuard and configuring your devices to use the FortiManager system as their FortiGuard server, you can view overall and per device statistics on FortiGuard service benefits.

To operate in a closed network, disable communication with the FortiGuard server. See Operating as an FDS in a closed network on page 816.

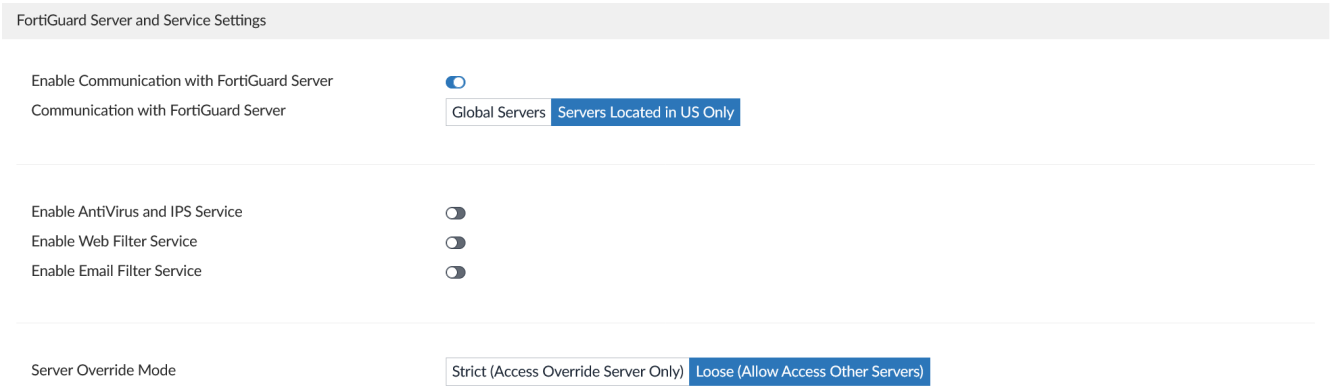


Enable Communication with FortiGuard Server	When toggled *OFF*, you must manually upload packages, databases, and licenses to your FortiManager. See Operating as an FDS in a closed network on page 816.
Communication with FortiGuard Server	Select *Servers Located in the US Only* to limit communication to FortiGuard servers located in the USA. Select *Global Servers* to communicate with servers anywhere.
Enable Antivirus and IPS Service	Toggle *ON* to enable antivirus and intrusion protection service. When on, select what versions of *FortiGate*, *FortiMail*, *FortiSandbox*, *FortiClient*, *FortiDeceptor*, and *FortiTester* to download updates for.
Enable Web Filter and Service	Toggle *ON* to enable web filter services. When uploaded to FortiManager, the Web Filter database version is displayed.
Enable Email Filter Service	Toggle *ON* to enable email filter services. When uploaded to FortiManager, the Email Filter databases versions are displayed.

Server Override Mode	Select *Strict (Access Override Server Only)* or *Loose (Allow Access Other Servers)* override mode.
FortiGuard Antivirus and IPS Settings	Configure antivirus and IPS settings. See FortiGuard antivirus and IPS settings on page 813.
FortiGuard Web Filter and Email Filter Settings	Configure web and email filter settings. See FortiGuard web and email filter settings on page 814.
Override FortiGuard Server (Local FortiManager)	Configure web and email filter settings. See Override FortiGuard server (Local FortiManager) on page 815.

FortiGuard antivirus and IPS settings

In this section you can enable settings for FortiGuard Antivirus and IPS settings.



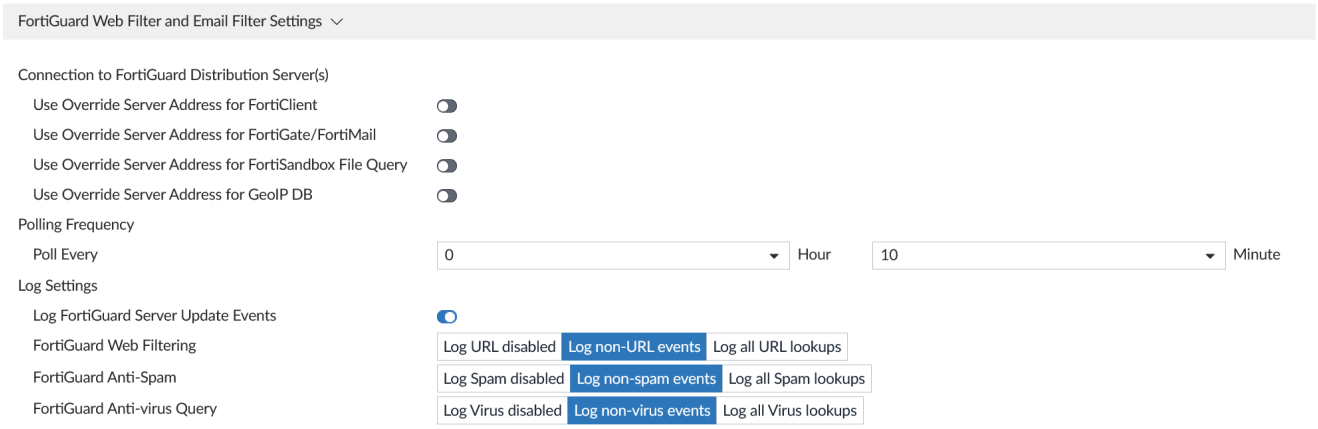
The following settings are available:

Use Override Server Address for FortiClient	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the add icon to add additional override servers, up to a maximum of ten. Select the delete icon to remove entries. To override the default server for updating FortiClient device's FortiGuard services, see Overriding default IP addresses and ports on page 833.
Use Override Server Address for FortiGate/FortiMail	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the add icon to add additional override servers, up to a maximum of ten. Select the delete icon to remove entries. To override the default server for updating FortiGate/FortiMail device's FortiGuard services, see Overriding default IP addresses and ports on page 833.
Allow Push Update	Configure to allow urgent or critical updates to be pushed directly to the FortiManager system when they become available on the FDN. The FortiManager system immediately downloads these updates. To enable push updates, see Enabling push updates on page 831.
Scheduled Regular Updates	Configure when packages are updated without manually initiating an update request. To schedule regular service updates, see Scheduling updates on page 833.

Advanced	Enables logging of service updates and entries. If either option is not turned on, you will not be able to view these entries and events when you select *View FDS and FortiGuard Download History*.

FortiGuard web and email filter settings

In this section you can enable settings for FortiGuard Web Filter and Email Filter.



The following settings are available:

Connection to FortiGuard Distribution Server(s)	Configure connections for overriding the default built-in FDS or web proxy server for web filter and email filter settings. To override an FDS server for web filter and email filter services, see Overriding default IP addresses and ports on page 833. To enable web filter and email filter service updates using a web proxy server, see Enabling updates through a web proxy on page 832.
Use Override Server Address for FortiClient	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the add icon to add additional override servers, up to a maximum of ten. Select the delete icon to remove entries.
Use Override Server Address for FortiGate/FortiMail	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the add icon to add additional override servers, up to a maximum of ten. Select the delete icon to remove entries. To override the default server for updating FortiGate device's FortiGuard services, see Overriding default IP addresses and ports on page 833.
Polling Frequency	Configure how often polling is done.
Log Settings	Configure logging of FortiGuard server update, web filtering, email filter, and antivirus query events. • *Log FortiGuard Server Update Events*: enable or disable • *FortiGuard Web Filtering*: Choose from *Log URL disabled*, *Log non-URL events*, and *Log all URL lookups*. • *FortiGuard Anti-spam*: Choose from *Log Spam disabled*, *Log non-spam*

	events, and *Log all Spam lookups*. • *FortiGuard Anti-virus Query*: Choose from *Log Virus disabled*, *Log non-virus events*, and *Log all Virus lookups*. To configure logging of FortiGuard web filtering and email filtering events, see Logging FortiGuard web or email filter events on page 836.

Override FortiGuard server (Local FortiManager)

Configure and enable alternate FortiManager FDS devices, rather than using the local FortiManager system. You can set up as many alternate FDS locations, and select what services are used. The following settings are available:

Additional number of Private FortiGuard Servers (Excluding This One)	Select the add icon to add a private FortiGuard server. Select the delete icon to remove entries. When adding a private server, you must type its IP address and time zone.
Enable Antivirus and IPS Update Service for Private Server	When one or more private FortiGuard servers are configured, update antivirus and IPS through this private server instead of using the default FDN. This option is available only when a private server has been configured.
Enable Web Filter and Email Filter Update Service for Private Server	When one or more private FortiGuard servers are configured, update the web filter and email filter through this private server instead of using the default FDN. This option is available only when a private server has been configured.
Allow FortiGates to Access Public FortiGuard Servers When Private Servers Unavailable	When one or more private FortiGuard servers are configured, managed FortiGate units will go to those private servers for FortiGuard updates. Enable this feature to allow those FortiGate units to then try to access the public FDN servers if the private servers are unreachable. This option is available only when a private server has been configured.

The FortiManager system's network interface settings can restrict which network interfaces provide FDN services. For more information, see Configuring network interfaces on page 902.

Connecting the built-in FDS to the FDN

When you enable the built-in FDS and initiate an update either manually or by a schedule, the FortiManager system attempts to connect to the FDN.

If all connection attempts to the server list fail, the connection status will be *Disconnected*.

If the connection status remains *Disconnected*, you may need to configure the FortiManager system's connection to the FDN by:

- overriding the default IP address and/or port
- configuring a connection through a web proxy.

After establishing a connection with the FDN, the built-in FDS can receive FortiGuard service update packages, such as antivirus engines and signatures or web filtering database updates, from the FDN.

To enable the built-in FDS:

1. Go to *FortiGuard* > *Settings*.
2. Enable the types of FDN services that you want to provide through your FortiManager system's built-in FDS. For more information, see Configuring FortiGuard services on page 830.
3. Click *Apply*.
   The built-in FDS attempts to connect to the FDN.



If the built-in FDS is unable to connect, you may need to enable the selected services on a network interface. For more information, see Configuring network interfaces on page 902.

If you still cannot connect to the FDN, check routes, DNS, and any intermediary firewalls or NAT devices for policies that block necessary FDN ports and protocols.

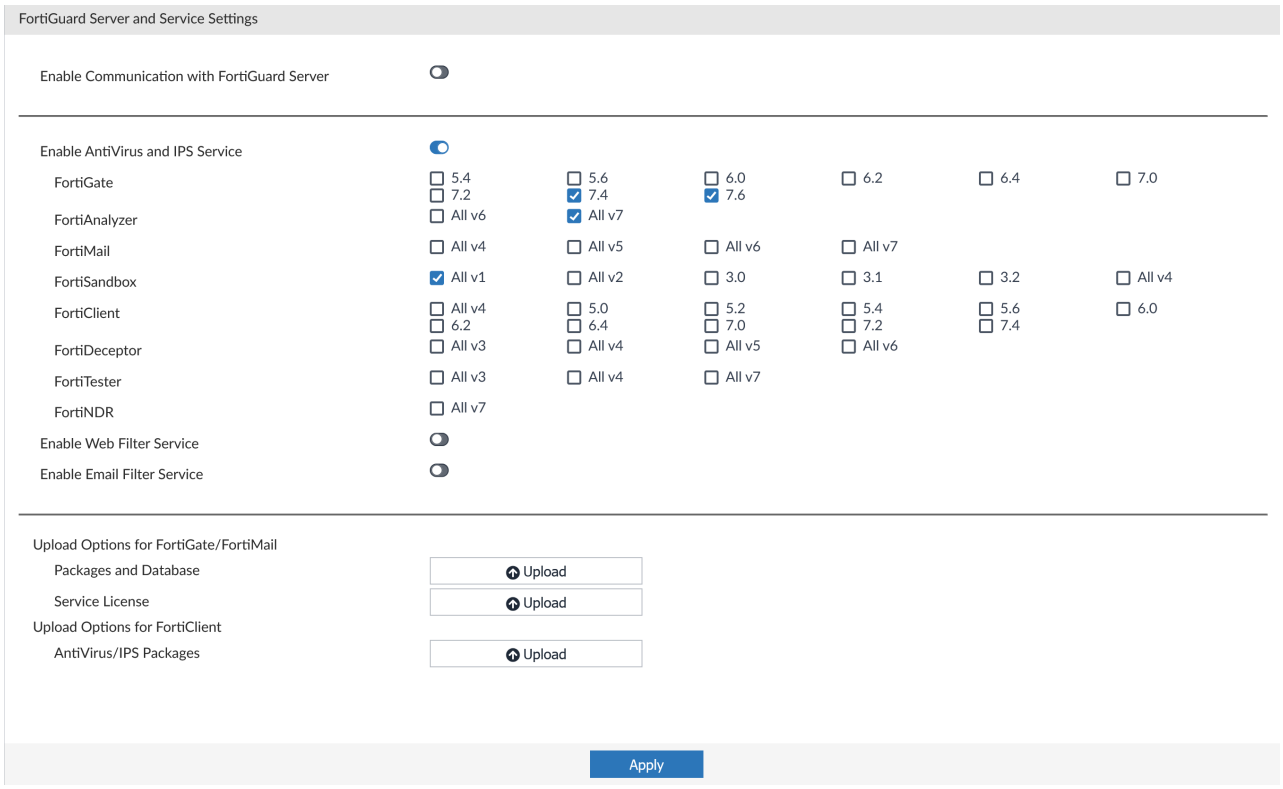
Operating as an FDS in a closed network

The FortiManager can be operated as a local FDS server when it is in a closed network with no internet connectivity.

Without a connection to a FortiGuard server, update packages and licenses must be manually downloaded from the Fortinet Support portal, and then uploaded to the FortiManager.

To use FortiManager as FDS in a closed network:

1. On FortiGate, enable the update services/profiles that you require.
2. On FortiManager, go to *FortiGuard* > *Settings* to configure FortiManager as a local FDS server:



Enable Communication with FortiGuard Servers	Toggle *OFF* to disable communication with the FortiGuard servers.
Enable Antivirus and IPS Service	Toggle *ON* to enable antivirus and intrusion protection service, and select what versions for each product to support.
Enable Web Filter Services	Toggle *ON* to enable web filter services. When uploaded to FortiManager, the Web Filter database is displayed.
Enable Email Filter Services	Toggle *ON* to enable email filter services. When uploaded to FortiManager, the Email Filter database is displayed.

3. Download the service update package(s) that are required by the FortiGate from the Fortinet Support portal.

FortiGate only downloads service updates from FortiManager for the services/profiles that it has enabled. For more information on available services, see *FortiGuard* in the FortiGate Administration Guide.

Importing metadata packages in closed network scenarios

When operating FortiManager as an FDS in a closed network, metadata packages (for example, *Signature Meta Data (IPS Slim)* packages) must be manually imported into the FortiManager. Some metadata packages are not available for download through FortiGuard.com; instead, they can be obtained by exporting them from an online FortiManager. See Exporting packages example on page 795.

4. Go to *FortiGuard > Settings* and upload the service update packages:

Upload Options for FortiGate/FortiMail (and FortiSOAR)	
Packages and Database	Select to upload antivirus and IPS packages, web filter databases, and email filter databases. Browse for the file you downloaded from the Fortinet Support portal on your management computer, or drag and drop the file onto the dialog box, and click *OK*.  As databases can be large, we recommend uploading them using the CLI. See Uploading packages with the CLI on page 818.
Service License	Select to import the FortiGate or FortiSOAR license. License files can be obtained from support by requesting your account entitlement for the device. See Requesting account entitlement files on page 823. Browse for the file you downloaded from the Fortinet Support portal on your management computer, or drag and drop the file onto the dialog box, and click *OK*.
Upload Options for FortiClient	
AntiVirus/IPS Packages	Select to upload the FortiClient AntiVirus/IPS packages. Browse for the file you downloaded from the Fortinet Support portal on your management computer, or drag and drop the file onto the dialog box, and click *OK*.

Uploading packages with the CLI

Packages and licenses can be uploaded using the CLI. This should be used when the packages being uploaded are large, like database packages.

To upload packages and license files using the CLI:

1. If not already done, disable communications with the FortiGuard server and enable a closed network with the following CLI commands:
   ```
   config fmupdate publicnetwork
      set status disable
   end
   ```
2. Upload an update package or license:
   a. Load the package or license file to an FTP, SCP, or TFTP server
   b. Run the following CLI command:
   ```
   execute fmupdate {ftp | scp | tftp} import <av-ips | fct-av | url | spam | file-query | license-fgt | license-fct | custom-url | domp> <remote_file> <ip> <port> <remote_path> <user> <password>
   ```

Licensing in an air-gap environment

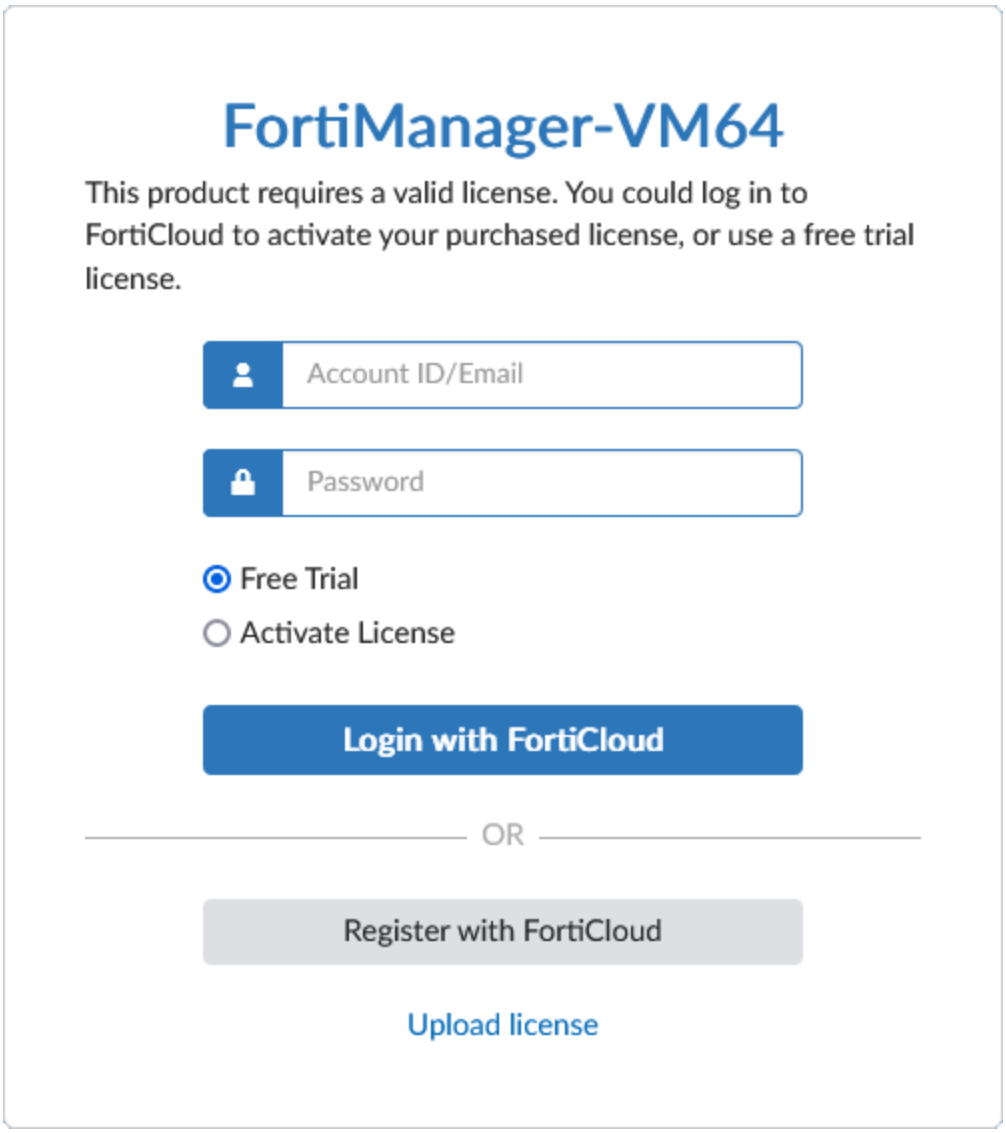
When performing the initial setup of FortiManager, you are required to register your FortiManager to FortiCare, which typically requires internet access. While operating in a closed network or air-gap environment, you must complete this step by uploading the entitlements file through the FortiManager GUI or CLI.



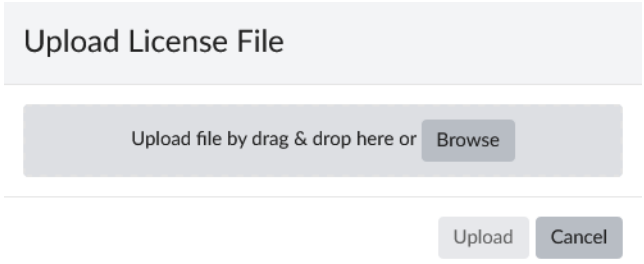
When internet access is restricted by a web proxy, you can establish a connection to FortiGuard for the FortiCare registration information or status by configuring a web proxy. See Enabling updates through a web proxy on page 832.

To register FortiManager in an air-gap environment:

1. In FortiManager, disable access to the public FortiGuard Distribution Servers (FDS) using the following CLI commands:
   ```
   config fmupdate publicnetwork
      set status disable
   end
   ```
2. Connect to the FortiManager GUI, and on the FortiManager login screen, click *Upload License*.

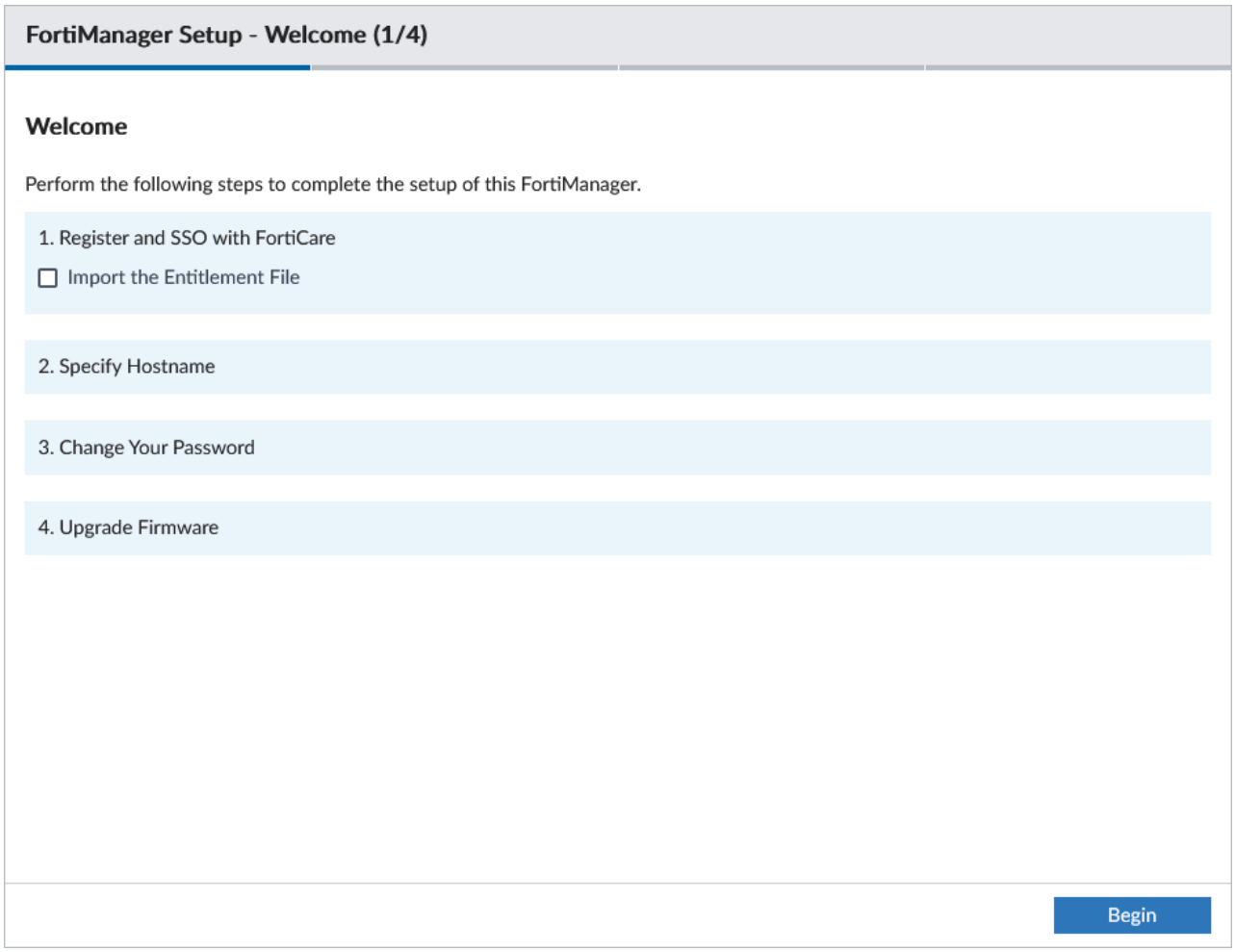


3. Click *Browse* to select your FortiManager license or drag-and-drop the license file, and click *Upload*.



The license file will be applied, and the FortiManager will be restarted in order to verify the license.

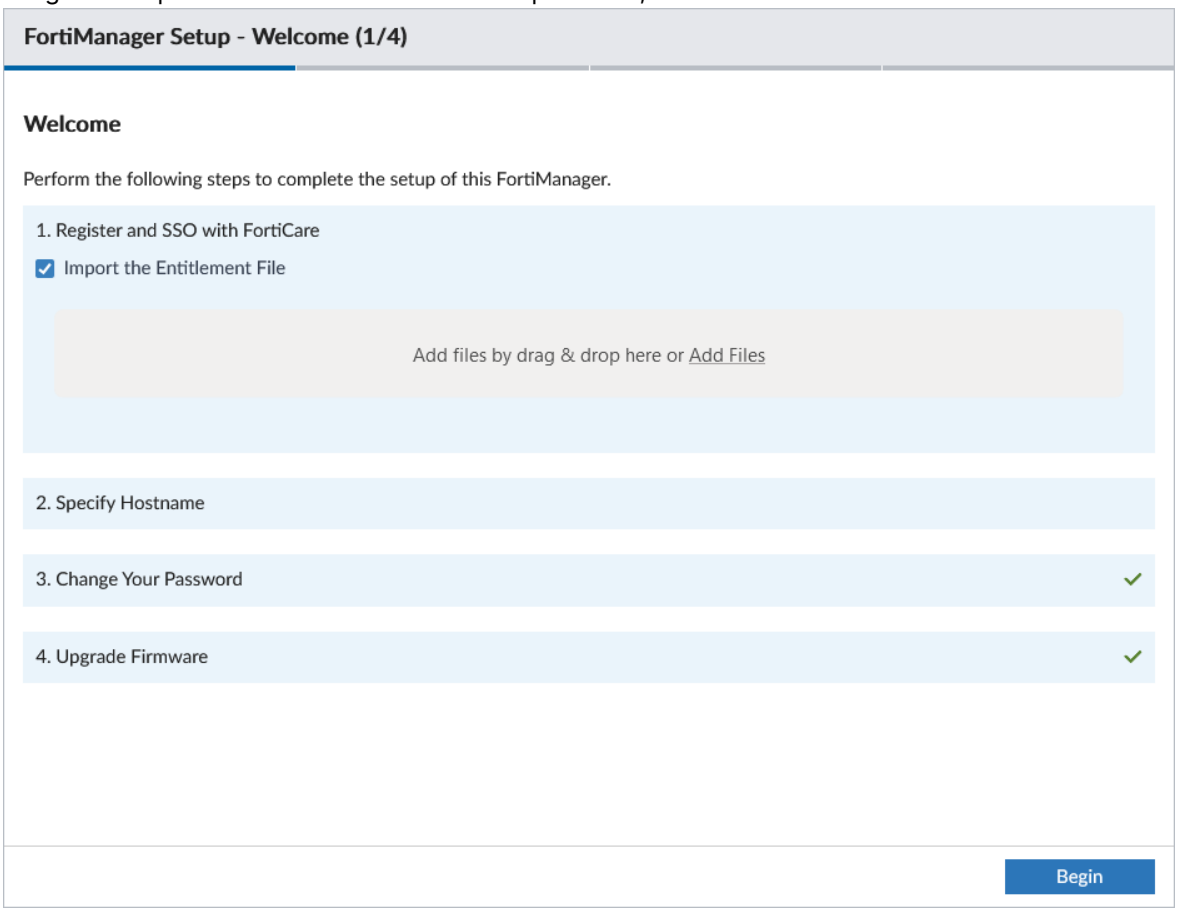
4. Sign in to FortiManager.
The FortiManager Setup Wizard is displayed.



In order to access your FortiManager, it must be registered to FortiCare in the FortiManager Setup Wizard.

5. On FortiCloud, create a ticket for your FortiManager entitlements file, and Fortinet Customer Service will provide you with the file.

6. You can upload your entitlement file either through the setup wizard or through the FortiManager CLI.
   a. *Onboarding wizard*:
      i. Select *Import the Entitlement File* in the FortiManager Setup wizard.
      ii. Drag and drop the entitlement file into the import area, or click *Add Files* to select the file location.



   b. *Command line interface*:
      i. Open the FortiManager CLI.
      ii. Upload the entitlement file using the following command.

```
execute fmupdate <ftp | scp | tftp> import license <filename> <server> <port>
      <directory> <username> <password>
```



The <port> variable is only required when connecting to a remote SCP host. The <directory>, <username>, and <password> variables are only required for logging into a FTP server or SCP host to download the file. For more information, see the FortiManager CLI Reference.

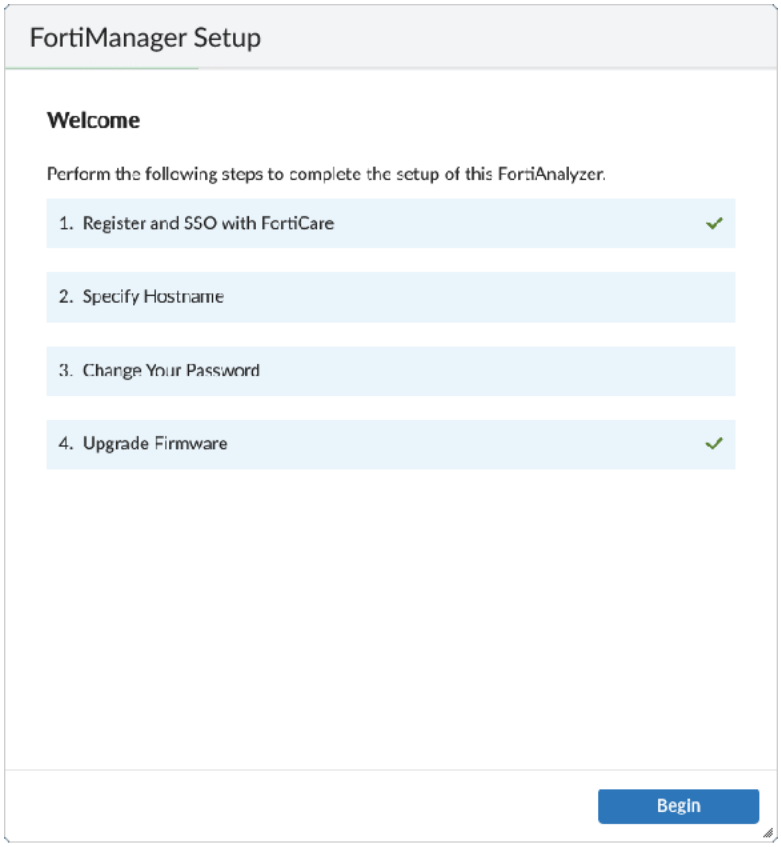
For example:

```
execute fmupdate ftp import license entitlement-file 172.10.1.10 /pub/place user1
      password1
This operation will replace the current package!
Do you want to continue? (y/n)y

Start getting file from FTP Server...
Transferred 0.001M of 0.001M in 0:00:00s (0.008M/s)
```

```
FTP transfer is successful.
Package installation is in process...
This could take some time.
Update successfully
```

7. The FortiManager Setup wizard will display that you are successfully registered with FortiCare.



Requesting account entitlement files

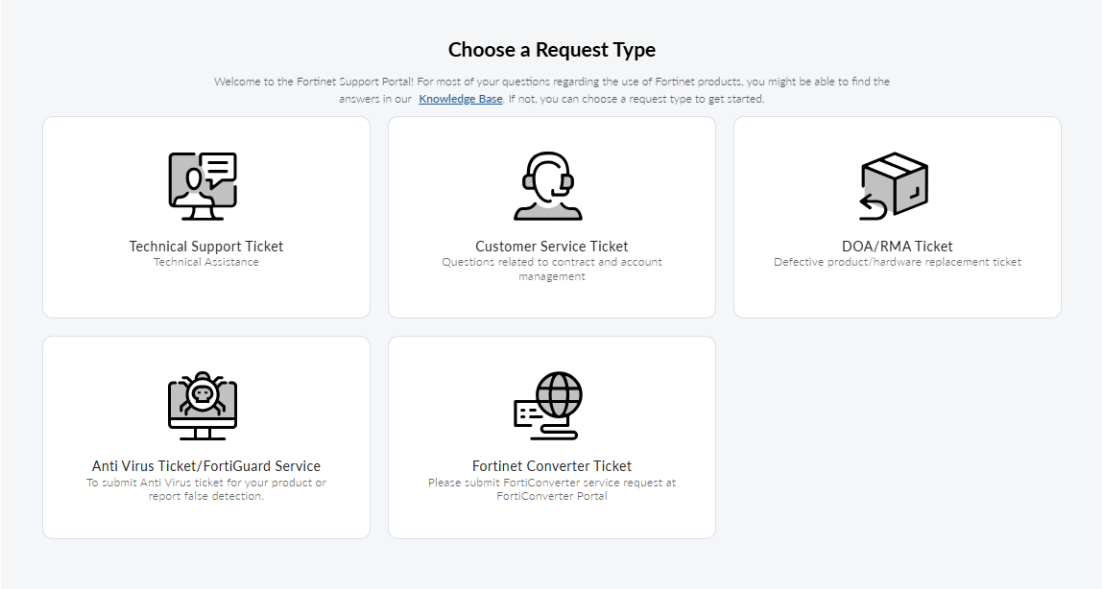
When FortiManager is operating in a closed network, you can request account entitlement files from Fortinet Customer Service & Support for devices, and then upload the files to the *FortiGuard* module. This allows devices in the closed network to check licenses.

For example, you can export an account entitlement file and then upload it to the FortiGuard panel. See Uploading account entitlement files on page 826.

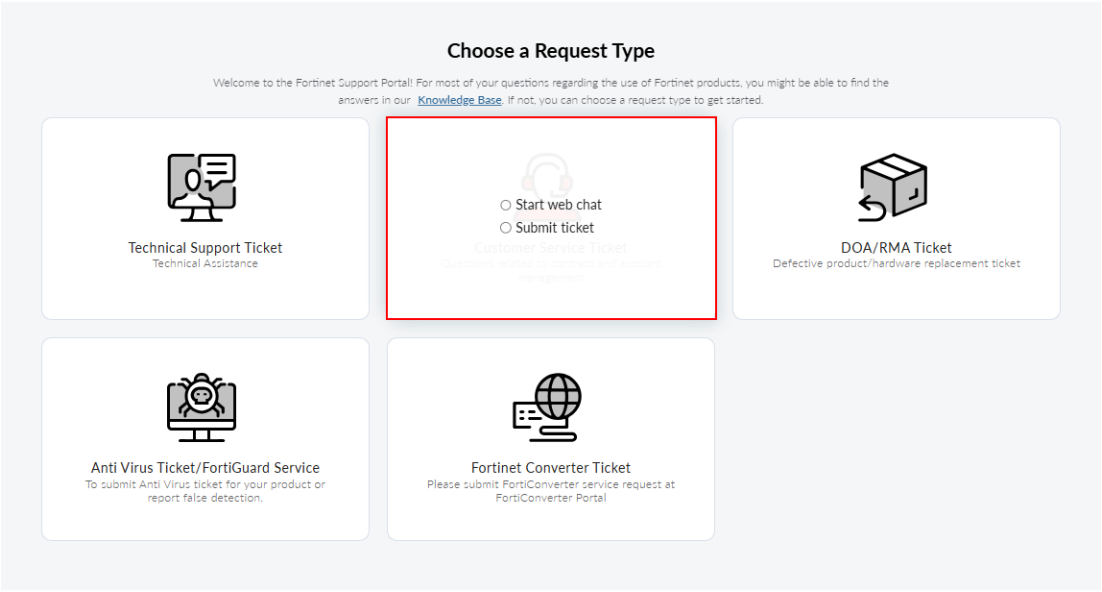
You can request access to your entitlement files from Fortinet Customer Service & Support by creating a support ticket.

To request account entitlement files:

1. Log in to the Fortinet Customer Service & Support site.
2. Go to *Support* > *Manage Tickets* > *Create Ticket*.
   The *Ticket Wizard* is displayed, starting at the *Choose a Request Type* page.

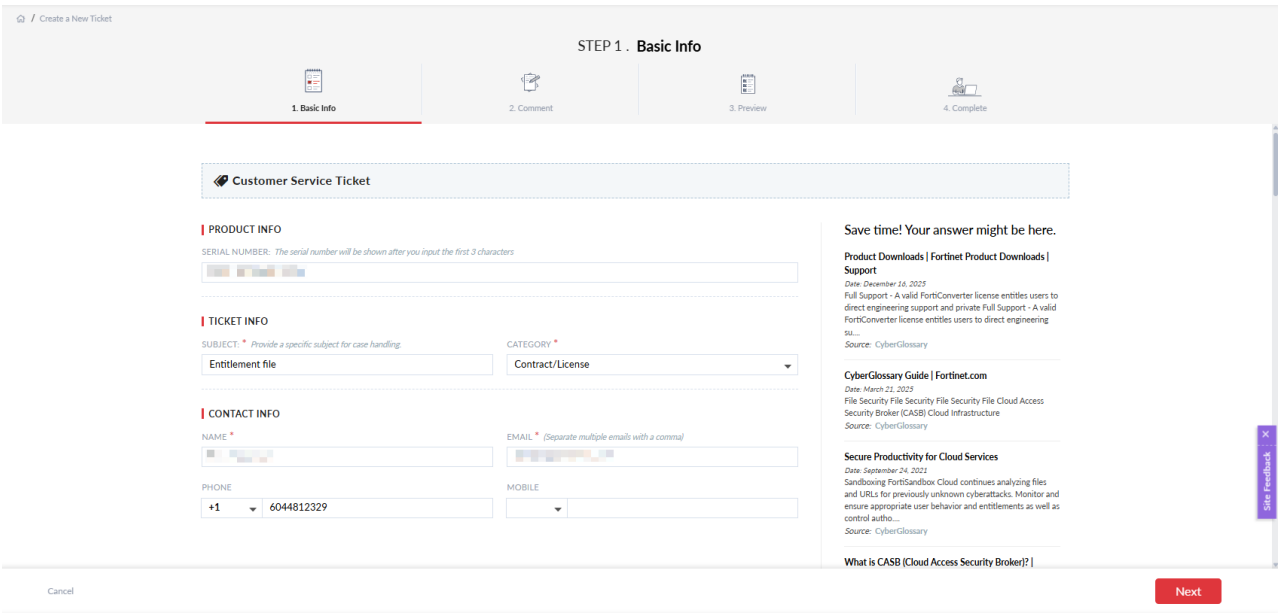


3. Hover your mouse over the *Customer Service Ticket* tile, and click *Submit Ticket*.



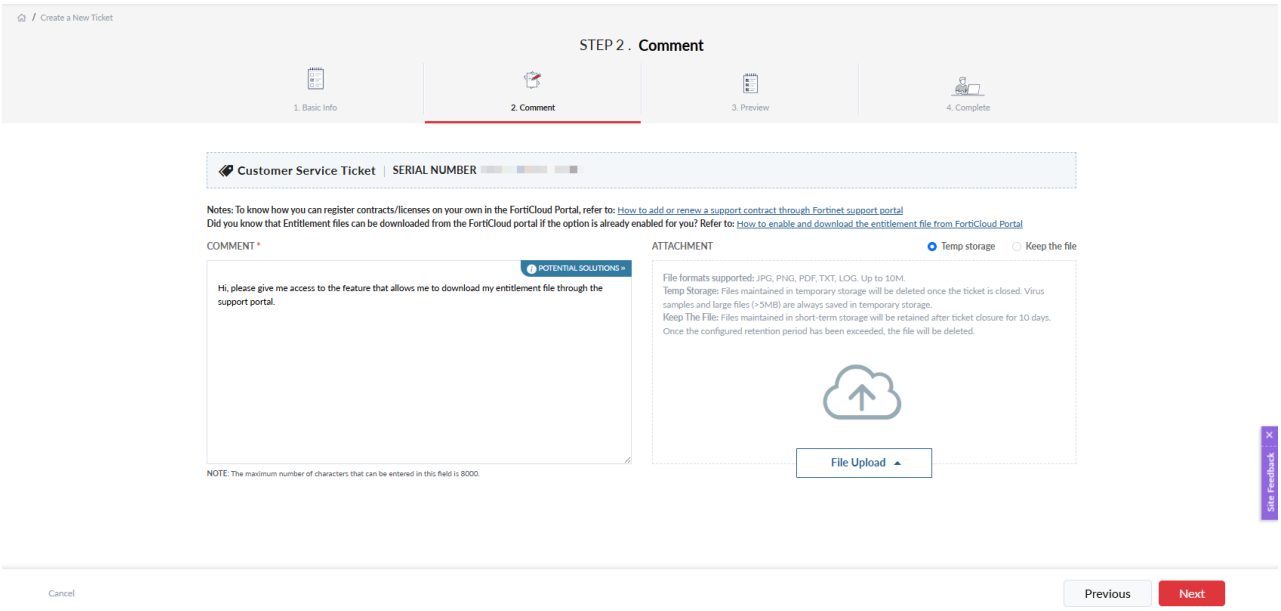
The wizard moves to the *STEP 1: Basic Info* page, where you can specify ticket information.

4. Complete the following information, and click *Next*.
   a. In the *Serial Number* box, add the serial number for the device for which you want an entitlement file.
   b. In the *Subject* box, type *Entitlement file*.
   c. In the *Category* list, select *Contract/License*.



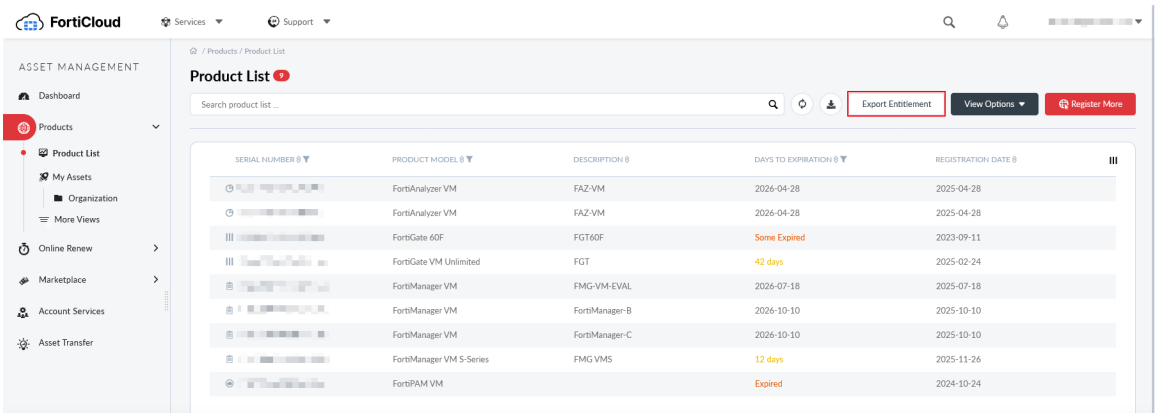
The wizard moves to the *STEP 2: Comment* page, where you can add a comment.

5. In the *Add Comment* box, request the entitlement access to the Entitlement File Download feature, and click *Next*.



The wizard moves to the *STEP 3: Preview* page, where you can review your request.

6. Review your request, and click *Confirm*.
7. Monitor your email to receive confirmation that the Entitlement File Download feature has been enabled for you in FortiCloud.
8. Sign in to FortiCloud and go to *Asset Management* > *Products* > *Product List*.
   A *Export Entitlement* option is displayed.
9. Click *Export Entitlement* and then *Continue*.

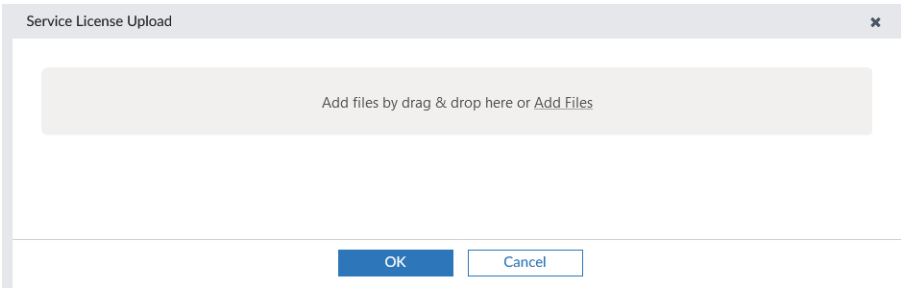


Uploading account entitlement files

After receiving an account entitlement file from Fortinet support, you can upload the file to the FortiGuard module when FortiManager is configured to operate in a closed network.

To upload account entitlement files:

1. Ensure that you received the account entitlement file from Fortinet support. See Requesting account entitlement files on page 823.
2. Ensure that FortiManager is configured to work in a closed network. See Operating as an FDS in a closed network on page 816.
3. Go to *FortiGuard* > *Settings*.
4. Ensure that *Enable Communication with FortiGuard Server* is toggled *OFF*.
5. Under *Upload Options for FortiGate/FortiMail*, click *Upload* beside *Service License*.
   Although the option is labeled for FortiGate or FortiMail, you can use this option for other types of devices, such as FortiSOAR.
   The *Service License Upload* dialog box is displayed.



6. Drop the account entitlement file on the dialog box, and click *OK*.
   The license information is uploaded.

Enabling FDN third-party SSL validation and Anycast support

You can enable Anycast to optimize the routing performance to FortiGuard servers. Relying on Fortinet DNS servers, FortiManager obtains a single IP address for the domain name of each FortiGuard service. BGP routing optimization is transparent to FortiManager. The domain name of each FortiGuard service is the common name in that service's certificate. The certificate is signed by a third-party intermediate CA. The FortiGuard server uses the Online Certificate Status Protocol (OCSP) stapling technique, enabling FortiManager to always validate the FortiGuard server certificate efficiently.

When Anycast is enabled, FortiManager only completes the TLS handshake with a FortiGuard server that provides a *good* OCSP status for its certificate. Any other status will result in a failed SSL connection. OCSP stapling is reflected on the signature interval (currently, 24 hours), and good means that the certificate is not revoked at that timestamp. The FortiGuard servers query the CA's OCSP responder every four hours and update its OCSP status. If the FortiGuard server is unable to reach the OCSP responder, it keeps the last known OCSP status for seven days. This cached OCSP status is immediately sent out when a client connection request is made, which optimizes the response time.

To enable Anycast support:

1. Enable Anycast support
```
config fmupdate fds-setting
(fds-setting)# set fortiguard-anycast enable
(fds-setting)# end
```
2. (Optional) Specify an authorized mirror server hosted by AWS for better performance.
```
config fmupdate fds-setting
(fds-setting)# set fortiguard-anycast-source {aws | fortinet}
(fds-setting)# end
```

Configuring devices to use the built-in FDS

After enabling and configuring the FortiManager system's built-in FDS, you can configure devices to use the built-in FDS by providing the FortiManager system's IP address and configured port as their override server.

Devices are not required to be authorized by FortiManager in *Device Manager* to use the built-in FDS for FortiGuard updates and services.

Some settings must be first configured on FortiManager before it can act as the FDS. After configuring FortiManager settings, the procedures for configuring devices to use the built-in FDS vary by device type. See the documentation available for your device for more information.

Prerequisite configuration of FortiManager:

- *FortiGate Updates* and/or *Web Filtering* must be enabled on the management interface used by devices connecting to FortiManager for FDS services. See *Service Access* in Configuring network interfaces on page 902.

- The types of FDN services that you want to provide through your FortiManager system's built-in FDS are enabled as needed in FortiGuard settings. See Connecting the built-in FDS to the FDN on page 815 and Settings on page 812.



If you are connecting a device to a FortiManager system's built-in FDS, some types of updates, such as antivirus engine updates, require you to enable SSH and HTTPS Administrative Access on the network interface which will receive push updates. See Network on page 901 for details.

FortiGuard Service Status

On FortiGate, the `include-default-servers` command controls whether the FortiGate can receive updates directly from the default FortiGuard servers.

In the managed FortiGate configuration, `include-defualt-servers` should be set to `disable` and the `server-address` should be set to the FortiManager IP address. This configuration ensures that the FortiGate will only receive updates from FortiManager, and that FortiManager will display the correct *Service Status* for the device.

When `include-default-servers` is `enabled`, the FortiGate update service list includes the production FDS server and FortiManager. If FortiGate receives an update from the FDS production server, FortiManager will not know that the FortiGate object's package version was updated, and FortiManager will not show the correct *Service Status*.

Related information:

- Using FortiManager as a local FortiGuard server in the FortiGate/FortiOS Administration Guide.
- Incoming Ports in the FortiManager Ports guide.
- Operating as an FDS in a closed network on page 816
- Connecting the built-in FDS to the FDN on page 815

Matching port settings

When configuring a device to override default FDN ports and IP addresses with that of a FortiManager system, the default port settings for the device's update or query requests may not match the listening port of the FortiManager system's built-in FDS. If this is the case, the device's requests will fail. To successfully connect them, you must match the devices' port settings with the FortiManager system's built-in FDS listening ports.

For example, the default port for FortiGuard antivirus and IPS update requests is TCP 443 on FortiOS v4.0 and higher, but the FortiManager system's built-in FDS listens for those requests on TCP 8890. In this case, the FortiGate unit's update requests would fail until you configure the unit to send requests on TCP 8890.

In some cases, the device may not be configurable; instead, you must configure the FortiManager system to listen on an alternate port.

For more information about what ports must be open, see the *FortiManager Ports*.

Handling connection attempts from unauthorized devices

The built-in FDS replies to FortiGuard update and query connections from devices authorized for central management by FortiManager. If the FortiManager is configured to allow connections from unauthorized devices, unauthorized devices can also connect.

For example, you might choose to manage a FortiGate unit's firmware and configuration locally (from its GUI), but use the FortiManager system when the FortiGate unit requests FortiGuard antivirus and IPS updates. In this case, the FortiManager system considers the FortiGate unit to be an unauthorized device, and must decide how to handle the connection attempt. The FortiManager system will handle the connection attempt based on how it is configured. Connection attempt handling is only configurable via the CLI.

To configure connection attempt handling:

1. From the toolbar, open the `CLI Console`, or connect to the FortiManager with terminal emulation software.
2. To configure the system to add unauthorized devices and allow service requests, enter the following command:
   ```
   config system admin setting
      set unreg_dev_opt add_allow_service
   end
   ```
3. To configure the system to add unauthorized devices but deny service requests, enter the following command:
   ```
   config system admin setting
      set unreg_dev_opt add_no_service
   end
   ```

For more information, see the *FortiManager CLI Reference*.

Configure a FortiManager without Internet connectivity to access a local FortiManager as FDS

By default, FortiManager connects to the public FDN to download security feature updates, including databases and engines for security feature updates such as Antivirus and IPS. Your FortiManager can be configured to use a second, local FortiManager for FDS updates.

To use a second FortiManager as the FDS in cascade mode:

1. Configure the upstream FortiManager that is connected to FDS.
   a. On the upstream FortiManager, enable *FortiGate Updates*, *FortiClient Updates*, and *Webfilter-Antispam* service access on the interface where the downstream FortiManager(s) will connect. For example, in the FortiManager CLI you can enter the following commands:

   ```
   edit "port1"
   ```

   ```
           set ip x.x.x.x 255.255.254.0
   ```

   ```
           set allowaccess ping https ssh snmp http webservice
   ```

```
        set serviceaccess fgtupdates fclupdates webfilter-antispam
        set type physical
next
```



In a closed network environment, the upstream FortiManager can be configured to operate as the local FDS by manually downloading package updates and licenses. See Operating as an FDS in a closed network on page 816.

2. Configure the downstream FortiManager.
   a. On the second FortiManager, go to *FortiGuard > Settings*.
   b. Ensure that *Communication with FortiGuard Server* is set to *Global Servers*.
   c. Under *FortiGuard Antivirus and IPS Settings*:
      i. Turn on *Use Override Server Address for FortiGate/FortiMail* and enter the IP address of the FortiManager unit being used as the FDS, and port number 8890.
      ii. If required, turn on *Use Override Server Address for FortiClient* and enter the IP address of the FortiManager unit being used as the FDS, and port number 8891.
   d. Under *FortiGuard Web Filter and Email Filter Settings*:
      i. Turn on *Use Override Server Address for FortiGate/FortiMail* and enter the IP address of the FortiManager unit being used as the FDS, and port number 8900.
      ii. If required, turn on *Use Override Server Address for FortiClient* and enter the IP address of the FortiManager unit being used as the FDS, and port number 8901.
   e. Click *Apply*.
   The FortiManager will use the second FortiManager unit as the FDS.

Configuring FortiGuard services

FortiGuard Management provides a central location for configuring how the FortiManager system accesses the FDN and FDS, including push updates. The following procedures explain how to configure FortiGuard services and configuring override and web proxy servers, if applicable.

If you need to host a custom URL list that are rated by the FortiGate unit, you can import a list using the CLI.

- Enabling push updates
- Enabling updates through a web proxy
- Overriding default IP addresses and ports
- Scheduling updates
- Accessing public FortiGuard web and email filter servers
- Preloading FortiGuard services on page 835

Enabling push updates

When an urgent or critical FortiGuard antivirus or IPS signature update becomes available, the FDN can push update notifications to the FortiManager system's built-in FDS. The FortiManager system then immediately downloads the update.

To use push updates, you must enable both the built-in FDS and push updates. Push update notifications will be ignored if the FortiManager system is not configured to receive them. If TCP port 443 downloads must occur through a web proxy, you must also configure the web proxy connection. See Enabling updates through a web proxy on page 832.

If push updates must occur through a firewall or NAT device, you may also need to override the default push IP address and port.

For example, overriding the push IP address can be useful when the FortiManager system has a private IP address, and push connections to a FortiManager system must traverse NAT. Normally, when push updates are enabled, the FortiManager system sends its IP address to the FDN; this IP address is used by the FDN as the destination for push messages; however, if the FortiManager system is on a private network, this IP address may be a private IP address, which is not routable from the FDN – causing push updates to fail.

To enable push through NAT, type a push IP address override, replacing the default IP address with an IP address of your choice, such as the NAT device's external or virtual IP address. This causes the FDN to send push packets to the override IP address, rather than the FortiManager system's private IP address. The NAT device can then forward the connection to the FortiManager system's private IP address.



The built-in FDS may not receive push updates if the external IP address of any intermediary NAT device is dynamic (such as an IP address from PPPoE or DHCP). When the NAT device's external IP address changes, the FortiManager system's push IP address configuration becomes out-of-date.

To enable push updates to the FortiManager system:

1. Go to *FortiGuard > Settings*.
2. Click the arrow to expand *FortiGuard Antivirus and IPS Settings*. See FortiGuard antivirus and IPS settings on page 813.
3. Toggle *ON* beside *Allow Push Update*.
4. If there is a NAT device or firewall between the FortiManager system and the FDN which denies push packets to the FortiManager system's IP address on UDP port 9443, type the IP Address and/or Port number on the NAT device which will forward push packets to the FortiManager system. The FortiManager system will notify the FDN to send push updates to this IP address and port number.
   - *IP Address* is the external or virtual IP address on the NAT device for which you will configure a static NAT or port forwarding.
   - *Port* is the external port on the NAT device for which you will configure port forwarding.
5. Click *Apply*.
6. If you performed step 4, also configure the device to direct that IP address and/or port to the FortiManager system.
   - If you entered a virtual IP address, configure the virtual IP address and port forwarding, and use static NAT mapping.

- If you entered a port number, configure port forwarding; the destination port must be UDP port 9443, the FortiManager system's listening port for updates.

To enable push through NAT in the CLI:

Enter the following commands:

```
config fmupdate fds-setting
   config push-override-to-client
      set status enable
      config announce-ip
         edit 1
            set ip <override IP that FortiGate uses to download updates from FortiManager>
            set port <port that FortiManager uses to send the update announcement>
         end
      end
   end
```

Enabling updates through a web proxy

If the FortiManager system's built-in FDS must connect to the FDN through a web (HTTP or HTTPS) proxy, you can specify the IP address and port of the proxy server.

If the proxy requires authentication, you can also specify a user name and password.

FortiManager can only have one proxy server configuration.

To enable updates to the FortiManager system through a proxy using the GUI:

1. Go to *System Settings* > *Advanced* > *Misc Settings*.
2. Enable *Use Web Proxy*.
3. Configure the following settings:

Proxy Mode	Select the proxy mode. FortiManager supports web proxy using *Tunnel* or *Proxy* mode: • Tunnel mode (default) uses port TCP/443. • Proxy mode uses port TCP/80.
Address	Enter the address and port of the proxy server. The default port is 1080.
User Name	If authentication is required by the proxy server, provide a user name.
Password	If authentication is required by the proxy server, provide a password.

4. Click *Apply*.

To enable updates to FortiManager through a proxy using the CLI:

Use the following command in the FortiManager CLI:

```
config system web-proxy
   set status enable
   set mode {proxy | tunnel} (default = tunnel)
   set address <string>
```

```
    set password <passwd>
    set port <integer>
    set username <string>
end
```

For more information about the variables, see the FortiManager CLI Reference.

Overriding default IP addresses and ports

The FortiManager device's built-in FDS connects to the FDN servers using default IP addresses and ports. You can override these defaults if you want to use a port or specific FDN server that differs from the default.

To override default IP addresses and ports:

1. Go to *FortiGuard > Settings*.
2. If you need to override the default IP address or port for synchronizing with available FortiGuard antivirus and IPS updates, click the arrow to expand *FortiGuard Antivirus and IPS Settings*, then toggle *ON* beside *Use Override Server Address for FortiGate/FortiMail* and/or *Use Override Server Address for FortiClient*.
3. If you need to override the FortiManager system's default IP address or port for synchronizing with available FortiGuard web and email filtering updates, click the arrow to expand *FortiGuard Web Filter and Email Filter Settings*, then toggle *ON* beside *Use Override Server Address for FortiGate/FortiMail* and/or *Use Override Server Address for FortiClient*.
4. Enter the IP address and/or port number.
5. Click *Apply*.
   If the FDN connection status remains disconnected, the FortiManager system is unable to connect with the configured override.

FDN port numbers and protocols

Both the built-in FDS and devices use certain protocols and ports to successfully request and receive updates from the FDN or override server. Any intermediary proxies or firewalls must allow these protocols and ports, or the connection will fail.

After connecting to the FDS, you can verify connection status on the FortiGuard Management page. For more information about connection status, see Connecting the built-in FDS to the FDN on page 815.

Scheduling updates

Keeping the built-in FDS up-to-date is important to provide current FortiGuard update packages and rating lookups to requesting devices. This is especially true as new viruses, malware, and spam sources pop-up frequently. By configuring a scheduled update, you are guaranteed to have a recent version of database updates.

A FortiManager system acting as an FDS synchronizes its local copies of FortiGuard update packages with the FDN when:

- you manually initiate an update request by selecting *Update Now*
- it is scheduled to poll or update its local copies of update packages
- if push updates are enabled, it receives an update notification from the FDN.

If the network is interrupted when the FortiManager system is downloading a large file, it downloads all files again when the network resumes.

To schedule antivirus and IPS updates:

1. Go to *FortiGuard > Settings*.
2. Click the arrow to expand *FortiGuard Antivirus and IPS Settings*; see FortiGuard antivirus and IPS settings on page 813.
3. In *Polling Frequency*, select the number of hours and minutes of the polling interval.
4. Click *Apply*.

To schedule Web Filtering and Email Filter polling:

1. Go to *FortiGuard > Settings*.
2. Click the arrow to expand *FortiGuard Web Filter and Email Filter Settings*.
3. In *Polling Frequency*, select the number of hours and minutes of the polling interval.
4. Click *Apply*.



If you have formatted your FortiManager system's hard disk, polling and lookups will fail until you restore the URL and email filter databases. For more information, see Restoring the URL or antispam database on page 837.

Accessing public FortiGuard web and email filter servers

You can configure FortiManager to allow the managed FortiGate units to access public FortiGuard web filter or email filter network servers in the event local FortiGuard web filter or email filter server URL lookups fail. You can specify private servers where the FortiGate units can send URL queries.

To access public FortiGuard web and email filter servers:

1. Go to *FortiGuard > Settings*.
2. Click the arrow beside *Override FortiGuard Server (Local FortiManager)*.
3. Click the add icon next to *Additional number of private FortiGuard servers (excluding this one)*. Select the delete icon to remove entries.
4. Type the *IP Address* for the server and select its *Time Zone*.
5. Repeat step 4 as often as required. You can include up to ten additional servers.
6. Select the additional options to set where the FDS updates come from, and if the managed FortiGate units can access these servers if the local FDS is not available.
   - Toggle *ON* beside *Enable Antivirus and IPS update Service for Private Server* if you want the FDS updates to come from a private server.

- Toggle *ON* beside *Enable Web Filter and Email Filter Service for Private Server* if you want the updates to come from a private server.
- Toggle *ON* beside *Allow FortiGates to Access Public FortiGuard Servers when Private Servers are Unavailable* if you want the updates to come from public servers in case the private servers are unavailable.

7. Click *Apply*.

Preloading FortiGuard services

To ensure that the hosted FortiGuard server can respond quickly to rating queries, and to preserve sufficient disk I/O and CPU resources for management functions, the enabled databases can be preloaded into RAM. Enabling preload results in a significantly higher memory requirement.

When preload is disabled, the rating services use less memory but rely heavily on disk I/O to serve requests. This can result in high I/O wait times, increased CPU usage, and degraded FortiManager performance.

Preload behavior can be controlled individually for each rating service using the following CLI commands:

```
   config fmupdate fgd-setting
   set
     as-preload --- Enable/disable preloading antispam database to memory (default = disable).
     av-preload --- Enable/disable preloading antivirus database to memory (default = disable).
     av2-preload -- Enable/disable preloading outbreak prevention database to memory (default =
disable).
     fq-preload --- Enable/disable preloading file query database to memory (default = disable).
     iot-preload -- Enable/disable preloading IoT database to memory (default = disable).
     iotv-preload - Enable/disable preloading IoT-Vulnerability database to memory (default =
disable).
     wf-preload --- Enable/disable preloading the web filter database into memory (default =
disable).
```

Even with all services enabled, it may not always be necessary to preload all databases into memory. This depends on the number of requests from the devices, the specifics of the inspected traffic, and the available storage IOPS.



Preload is enabled by default for WebFilter when memory exceeds 60GB.

Logging events related to FortiGuard services

You can log a variety of events related to FortiGuard services.



Logging events from the FortiManager system's built-in FDS requires that you also enable local event logging.

Logging FortiGuard antivirus and IPS updates

You can track FortiGuard antivirus and IPS updates to both the FortiManager system's built-in FDS and any authorized FortiGate or FortiMail devices that use the FortiManager system's FDS.

To log updates and histories to the built-in FDS:

1. Go to *FortiGuard > Settings*.
2. Click the arrow to expand *FortiGuard Antivirus and IPS Settings*; see FortiGuard antivirus and IPS settings on page 813.
3. Under the *Advanced* heading, toggle *ON* beside *Log Update Entries from FortiGuard Distribution Server*.
4. Click *Apply*.

To log updates to FortiGate devices:

1. Go to *FortiGuard > Settings*.
2. Click the arrow to expand *FortiGuard Antivirus and IPS Settings*.
3. Under the *Advanced* heading, toggle *ON* beside *Log Update Histories for Each FortiGate*.
4. Click *Apply*.

Logging FortiGuard web or email filter events

You can track FortiGuard web filtering and email filtering lookup and non-events occurring on any authorized FortiGate or FortiMail device that use FortiManager system's FDS.

Before you can view lookup and non-event records, you must enable logging for FortiGuard web filtering or email filter events.

To log rating queries:

1. Go to *FortiGuard > Settings*.
2. Click the arrow to expand *FortiGuard Web Filter and Email Filter Settings*.
3. Configure the log settings, the click *Apply*:

Log Settings	
Log FortiGuard Server Update Events	Enable or disable logging of FortiGuard server update events.
FortiGuard Web Filtering	
Log URL disabled	Disable URL logging.
Log non-URL events	Logs only non-URL events.
Log all URL lookups	Logs all URL lookups (queries) sent to the FortiManager system's built-in FDS by FortiGate devices.
FortiGuard Anti-spam	

Log Spam disabled	Disable spam logging.
Log non-spam events	Logs email rated as non-spam.
Log all Spam lookups	Logs all spam lookups (queries) sent to the FortiManager system's built-in FDS by FortiGate devices.
FortiGuard Anti-virus Query	
Log Virus disabled	Disable virus logging.
Log non-virus events	Logs only non-virus events.
Log all Virus lookups	Logs all virus queries sent to the FortiManager system's built-in FDS by FortiGate devices.

Restoring the URL or antispam database

Formatting the hard disk or partition on FortiManager 3000 units and higher deletes the URL and antispam databases required to provide FortiGuard email filter and web filtering services through the built-in FDS. The databases will re-initialize when the built-in FDS is next scheduled to synchronize them with FDN.

Before formatting the hard disk or partition, you can back up the URL and antispam database using the CLI, which encrypts the file. You can also back up licenses as well. The databases can be restored by importing them using the CLI. If you have created a custom URL database, you can also back up or restore this customized database (for FortiGate units).

FortiSwitch Manager

The *FortiSwitch Manager* pane allows you to manage FortiSwitch devices that are controlled by FortiGate devices that are managed by FortiManager. You can use *FortiSwitch Manager* for the following modes of management:

You can use *FortiSwitch Manager* for the following modes of management:

Central management of managed switches	When central management is enabled, you can view, create, edit, and import profiles. These profiles share a common database and can be applied to any device. Central management mode is recommended when you need to create common profiles to share between different FortiSwitch devices, for example in environments where you have many FortiSwitches and managing the settings for each device individually is not practical. Configuration of FortiSwitch settings is completed in the FortiSwitch Manager. When an install occurs, only necessary configurations (configurations that are directly referenced in a profile assigned to the FortiSwitch) are installed.
Per-device management of managed switches	When per-device management is enabled, you can change settings for each managed switch. All FortiSwitch devices are managed at the device level with no shared objects. Per-device management mode is recommended when you want to manage each FortiSwitch configuration individually. Configuration of FortiSwitch settings is completed in the FortiSwitch Manager. When an install occurs, all configurations for the FortiSwitch are synchronized to the managing FortiGate.

The panes available in the *FortiSwitch Manager* tree menu depend on whether you have central management or per-device management enabled.

When central management is enabled, the *FortiSwitch Manager* pane includes the following in the tree menu:

Managed FortiSwitches on page 839	Displays unauthorized and authorized FortiSwitch devices. You can view, authorize, and edit authorized switches, as well as apply templates to switches.
FortiSwitch Templates	View, create, and edit FortiSwitch templates, VLANs, security policies, and custom commands. Templates can also be imported.
FortiSwitch VLANs on page 865	Configure FortiSwitch VLANs.
FortiLink settings on page 876	Configure FortiLink settings templates.

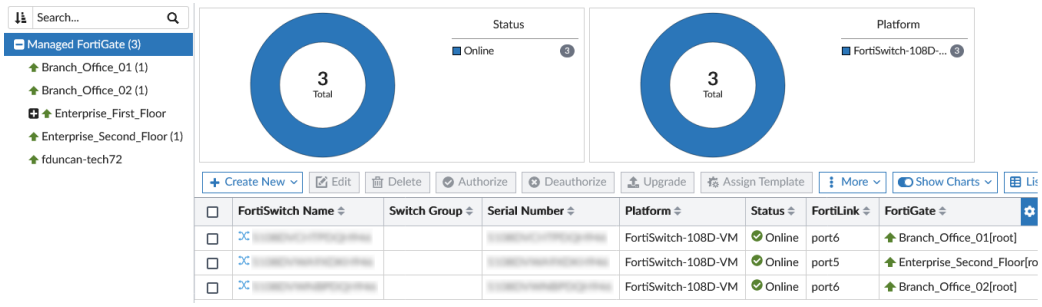
VDOM Settings	View and edit VDOM settings.
Port Policies	Configure FortiSwitch security and dynamic port policies. • FortiSwitch security policies on page 873 • FortiSwitch dynamic port policies on page 872
LLDP Profiles	Configure LLDP profiles. See Creating LLDP profiles on page 879.
QoS	Configure *QoS Policies*, *Egress Queue Policies*, *IP Precedence/DSCP*, and *802.1p*. See Creating QoS policies on page 880.
Custom commands on page 874	Create custom commands using the CLI.

When per-device management is enabled, the *FortiSwitch Manager* module includes the following in the tree menu:

Managed FortiSwitches on page 839	Displays unauthorized and authorized FortiSwitch devices. You can view, authorize, and edit authorized switches as well as configure ports for each managed switch. View, create, and edit *VLANs*, *Port Policies*, *NAC Policies*, *LLDP Policies*, *QoS*, and *Custom Commands*. Use the CLI to configure switches in the *CLI Configurations* tab.

Managed FortiSwitches

Go to *FortiSwitch Manager* > *Manged FortiSwitches* and select a FortiGate to access managed FortiSwitches. Managed switches are organized by their FortiGate controller.



Additional configuration options and short-cuts are available using the right-click content menu. Right-click on the mouse on different parts of the navigation panes on the GUI page to access these context menus.

If workspace or workflow is enabled, the ADOM must be locked before changes can be made. See Locking an ADOM on page 947.

This topic includes the following information:

- Quick status bar on page 840
- Authorizing and deauthorizing FortiSwitch devices on page 849
- Managing FortiSwitches on page 841
- Upgrading firmware for managed switches on page 849
- Using zero-touch deployment for FortiSwitch on page 850
- Creating a FortiSwitch group on page 851
- Installing changes to managed switches on page 852
- Diagnostics and tools on page 853
- Monitors on page 856

Quick status bar

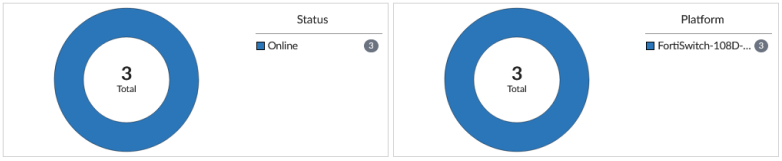
You can quickly view the status of devices on the *Managed Switches* pane by using the quick status bar, which contains the following information:

- Status Chart
- Platform Chart

Use the *Show Charts* dropdown and toggle to show or hide charts. From the dropdown, select or de-select the checkboxes for *Status* and *Platform* to show or hide the respective chart.

To use charts in the quick status bar:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *FortiSwitch Manager* > *Managed FortiSwitches*. The quick status bar is displayed above the content pane.

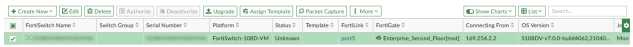


3. In the tree menu, select a FortiGate or *Managed FortiGate*. The devices for the group are displayed in the content pane, and the quick status bar updates.
4. Mouse over the charts to see more information about the data in a tooltip.
5. Click items in the legend to filter the devices displayed on the content pane. For example, if *Offline* is available in the legend, click *Offline* to display only devices that are currently offline.

   You can click multiple items in the legend to apply multiple filters. A filter icon appears next to the chart title when it is being used to filter the *Managed Switches* pane.
6. To remove the filters, click the chart title with the filter icon.

Managing FortiSwitches

FortiSwitch devices can be managed from the content pane below the quick status bar on the *FortiSwitch Manager > Managed FortiSwitches* pane when *Managed FortiSwitch* is selected.



The following options are available from the toolbar and right-click menu:

Create New	From the dropdown, add a FortiSwitch device using the model device wizard or add a new FortiSwitch group. For adding FortiSwitch devices, see Using zero-touch deployment for FortiSwitch on page 850. For adding FortiSwitch groups, see Creating a FortiSwitch group on page 851.
Edit	Edit the selected FortiSwitch.
Delete	Delete the selected FortiSwitch or ForiSwitches.
Authorize	Authorize a switch. See Authorizing and deauthorizing FortiSwitch devices on page 849.
Deauthorize	Deauthorize a switch. See Authorizing and deauthorizing FortiSwitch devices on page 849.
Upgrade	Upgrade the switch. The FortiSwitch must already be authorized. Before upgrading FortiSwitch, you can optionally go to *FortiGuard > Firmware Images > Product: FortiSwitch*, and click the download icon to manually download the firmware images.
Assign Template	Available when central management is enabled for *FortiSwitch Manager*. Assign a template to the FortiSwitch. Only applicable templates will be listed. See Assigning templates to FortiSwitch devices on page 877.
Packet Capture	Performs packet capture on the selected device. When performing packet capture, a filter can be created by clicking *Create New*, and then run by clicking *Start Capture*. You can also configure a schedule for the packet capture. See Configuring FortiSwitch packet captures on page 847.
More	Select *More* from the toolbar to view additional options. These options are also available from the right-click menu.
View Ports	Available when per-device management is enabled for *FortiSwitch Manager*. View and configure ports for the selected FortiSwitch. See Configuring a port on a single FortiSwitch on page 886.
Faceplates	View the faceplate monitor. See Monitors on page 856.

	Replace	Replace a FortiSwitch device. Selecting this option allows you to enter a new FortiSwitch Serial Number for the selected device. See Replacing switches on page 844.
	Restart	Restart the FortiSwitch.
	Refresh	Refresh the FortiSwitch list.
	Factory Reset	Reset the FortiSwitch to factory settings.
	Register	View the registration status and/or register the FortiSwitch to a FortiCloud account.
	Export to Excel/CSV	Export the selected device details to an Excel or CSV file. See Importing and exporting FortiSwitch devices on page 846.
	Import from CSV	Import FortiSwitches from an uploaded CSV file. See Importing and exporting FortiSwitch devices on page 846.
	Diagnostics and Tools	View additional diagnostic and tool information, including device summary and cable tests. See Diagnostics and tools on page 853. See Run a cable test on FortiSwitch ports from FortiManager on page 855.
LED Blink		Start LED blink on the selected FortiSwitch for the specified period of time. This option is only available in the right-click menu.
Show Charts		Toggle between hiding and showing the charts in the quick status bar. Click the dropdown to toggle a specific chart in the quick status bar. See Quick status bar on page 840.
List/Group/Topology		Use the dropdown to toggle between the following views: *List*: Display the individiual FortiSwitches in the list chart. This is the default. *Group*: Display the FortiSwitch groups in a list chart. *Topology*: Display the topology monitor. To return to the list view, click *Back to Managed Switches*. See Monitors on page 856
Search		Enter a search string into the search field to search the switch list. This option is only available in the toolbar.
Column Settings		Click to select which columns to display or select *Reset to Default* to display the default columns. This option is only available in the toolbar.

The following information is available in the content pane:

FortiSwitch Name	The name assigned to the switch.
Serial Number	The serial number of the switch.

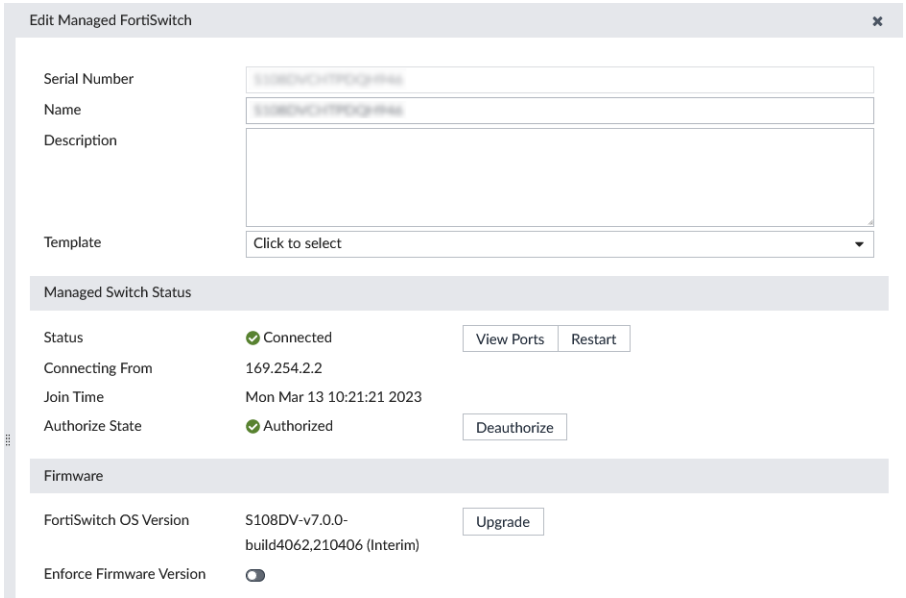
Platform	The FortiSwitch model.
Status	The online status of the switch.
FortiLink	The FortiLink of the switch.
FortiGate	The FortiGate that the FortiSwitch is connected to.
Connecting From	The IP address of the switch.
OS Version	The OS version on the switch.
Join Time	The date and time that the switch joined.
Comments	User entered comments.
Template	The FortiSwitch template assigned to the device, if any.

Editing switches

FortiSwitch devices can be edited from the *FortiSwitch Manager > Managed FortiSwitches* pane.

To edit FortiSwitch devices:

1. In the tree menu, select the FortiGate that contains the FortiSwitch device to be edited, or select *Managed FortiGate* to list all of the switches.
2. In the content pane, select the switch and click *Edit* from the toolbar, or right-click on the switch and select *Edit*. The *Edit Managed FortiSwitch* window opens.
   The following example is of *FortiSwitch Manager* with central management enabled.



3. Edit the following options, then click *Apply* to apply your changes.

Serial Number	The device's serial number. This field cannot be edited.

Name	The name of the FortiSwitch.
Description	A description of the FortiSwitch, such as its model.
Template	Available when central management is enabled for *FortiSwitch Manager*. Select the template that will be applied to the FortiSwitch from the dropdown list. Only applicable templates are available.
Custom Command Entry	Available when per-device management is enabled for *FortiSwitch Manager*. Click *Create New* to create a new custom command entry that will be applied to the FortiSwitch. See Creating custom commands on page 883.
Status	The status of the FortiSwitch, such as *Online*. Click *Restart* to restart the switch. Click *View Ports* to view the switches configured ports.
Connecting From	The IP address of the switch.
Join Time	The date and time that the switch joined.
Authorized State	The state of the AP, such as *Authorized*. If the switch is authorized, click *Deauthorize* to deauthorize the switch. If the switch is not authorized, click *Authorize* to authorize it. See Authorizing and deauthorizing FortiSwitch devices on page 849.
FortiSwitch OS Version	The OS version on the switch. Click *Upgrade* to upgrade the firmware to a newer version if you have one available.
Enforce Firmware Version	Toggle the switch to the *On* position to enable enforced firmware versioning.

Deleting switches

FortiSwitch devices can be deleted from the *FortiSwitch Manager > Managed FortiSwitches* pane.

To delete FortiSwitch devices:

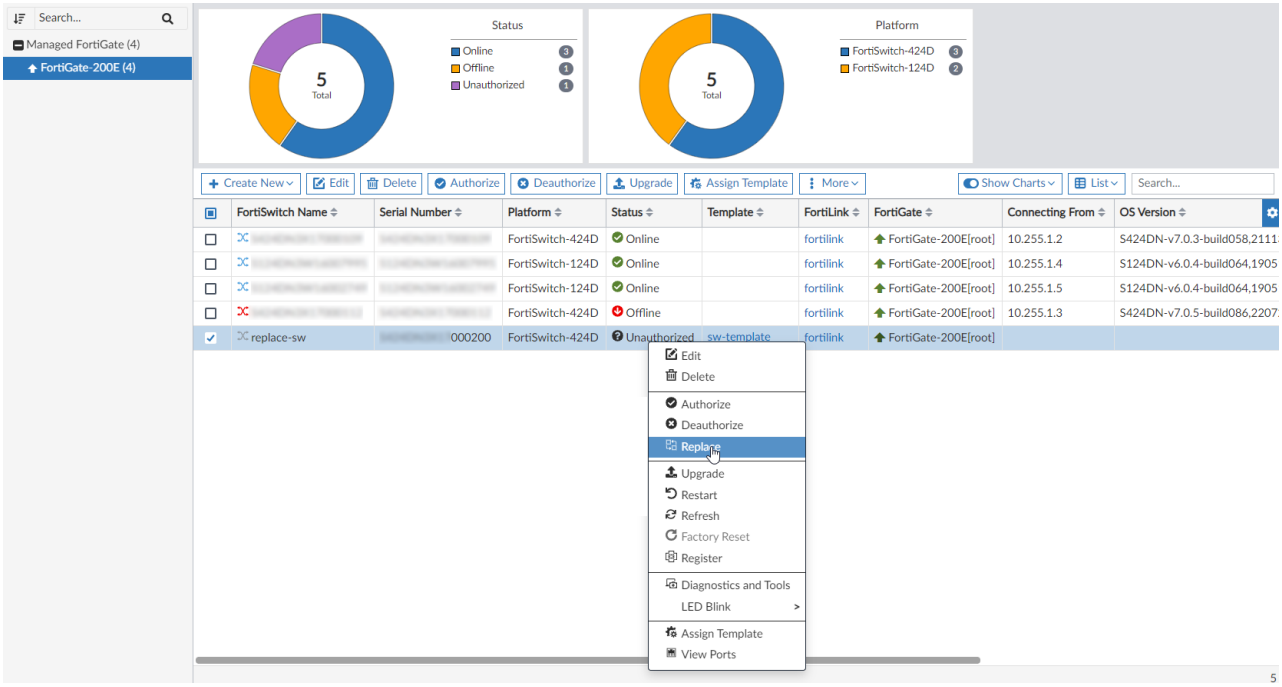
1. In the tree menu, select the FortiGate that contains the switch or switches to be deleted, or select *Managed FortiGate* to list all of the switches.
2. In the content pane, select the switch or switches, and click *Delete* from the toolbar, or right-click and select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the switch or switches.
4. Perform an install to apply the changes to the managed FortiGate. See Install wizard on page 180.

Replacing switches

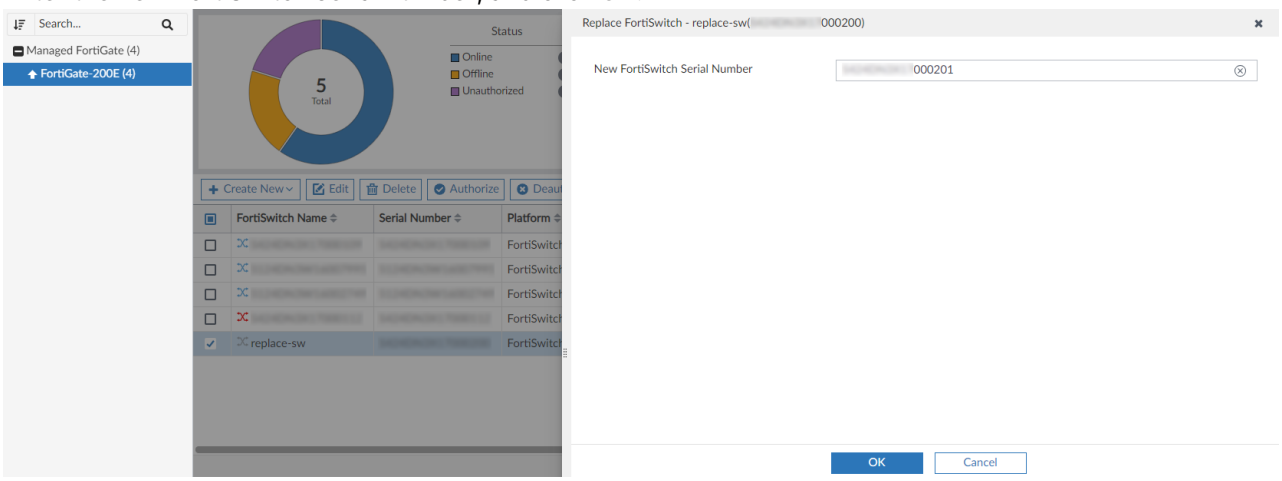
FortiSwitch devices can be replaced from the *FortiSwitch Manager > Managed FortiSwitches* pane.

To replace a FortiSwitch device:

1. Go to *FortiSwitch Manager* > *Managed FortiSwitches*, and select a managed FortiGate.
   To replace a FortiSwitch device, the FortiGate device must be online and the FortiSwitch must be *Deauthorized*.
2. Select FortiSwitch device and click *Deauthorize* in the toolbar or right-click menu.
3. Right-click on the FortiSwitch device and click *Replace*.

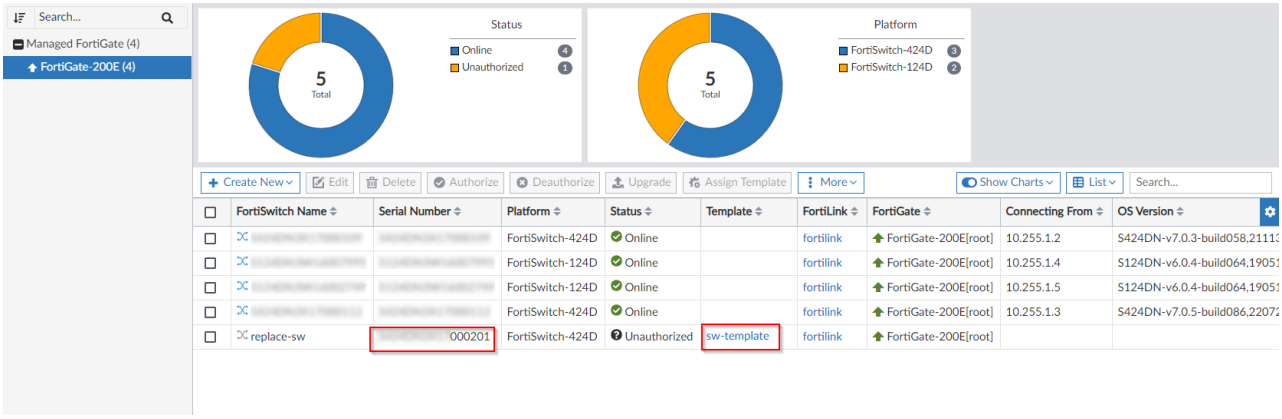


4. Enter the new FortiSwitch serial number, and click *OK*.



After the operation is complete, refresh the FortiSwitch list. The new FortiSwitch serial number is displayed

and the original template is kept.



5. Authorize the FortiSwitch, and the replacement is complete.

Importing and exporting FortiSwitch devices

To import FortiSwitch devices:

1. Configure a CSV file with the following fields as column headers, and enter the corresponding information for each FortiSwitch to be imported in the cells below:

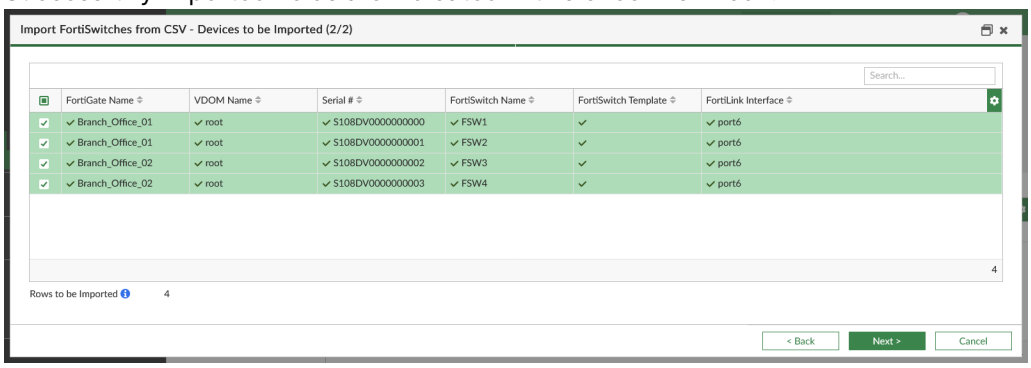
Header	Cell
FortiGate	The name of the FortiGate to which the FortiSwitch will be assigned.
FortiSwitch Name	The FortiSwitches name.
Serial Number	The FortiSwitches serial number
FortiLink	The FortiLink interface used to allow the FortiGate to manage the FortiSwitch.
Template	The template to be assigned to the FortiSwitch.
VDOM Name	(Optional) If VDOMs are enabled on the FortiGate, specify the VDOM to which the FortiSwitch will be assigned. If VDOMs are disabled, leave this field blank, and the default *root* VDOM will be applied automatically.

For example:

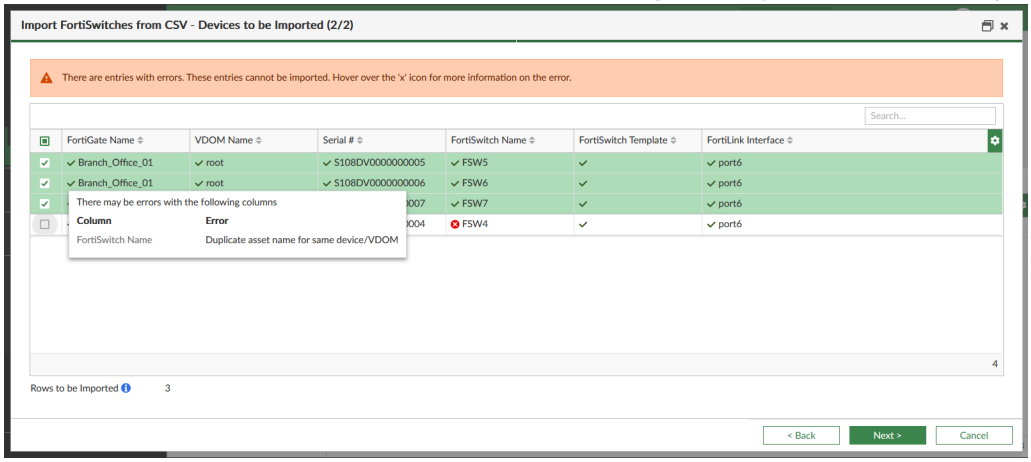
	A	B	C	D	E	F
1	FortiGate	FortiSwitch Name	Serial Number	FortiLink	Template	VDOM Name
2	Branch_Office_01	FSW1	S108DV0000000000	port6	FSW_Template	
3	Branch_Office_01	FSW2	S108DV0000000001	port6	FSW_Template	
4	Branch_Office_02	FSW3	S108DV0000000002	port6	FSW_Template	
5	Branch_Office_02	FSW4	S108DV0000000003	port6	FSW_Template	
6						
7						

2. Go to *FortiSwitch Manager* > *Managed FortiSwitches*, and select *More* > *Import from CSV* from the toolbar.
3. Browse to the CSV file location, or drag and drop the file into the *Upload* field. The results are displayed in the import results window.

- Successfully imported fields are indicated with a checkmark icon.



- Fields with errors are indicated with an error icon. Hover your mouse over the error icon or the FortiSwitch's check box to view details about the error. Fields can be directly edited from the import results window. FortiSwitches with errors will not be imported if you continue the import process.



4. Click *Next* to complete the import.

To export FortiSwitch devices:

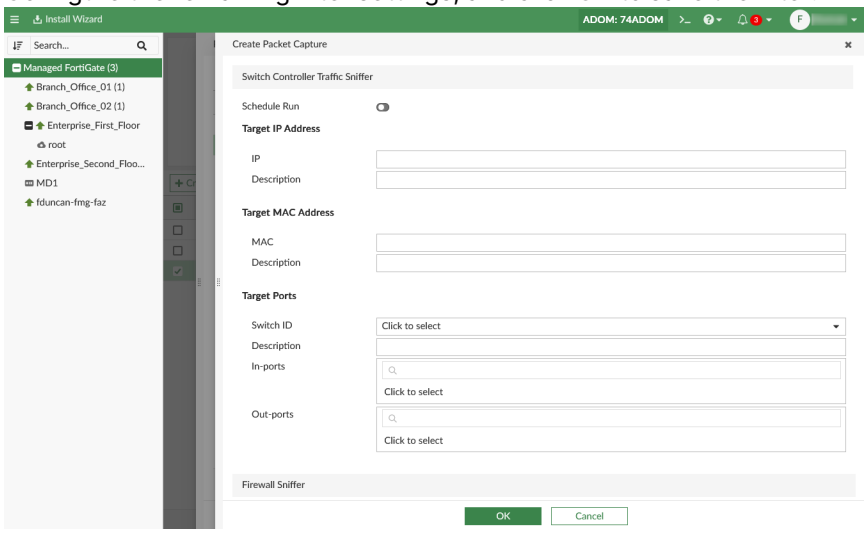
1. Go to *FortiSwitch Manager* > *Managed FortiSwitches*.
2. Select a FortiGate in the table to view its FortiSwitches or select *Managed FortiGate (#)* to view all FortiSwitch devices.
3. Open the *More* menu in the toolbar, and select one of the following options:
   - *Export to Excel*: The FortiSwitch information for the selected FortiGate(s) is exported to an Excel file
   - *Export to CSV*: Configure the following information and click *OK*:
     - *File Name*: Enter the name of the CSV file.
     - *Options*: Select *Export all columns* or *Export customized columns* only.
     - *Export All Devices*: In per-device mode only, enable this toggle to include all managed FortiGate's FortiSwitches in the CSV file.

Configuring FortiSwitch packet captures

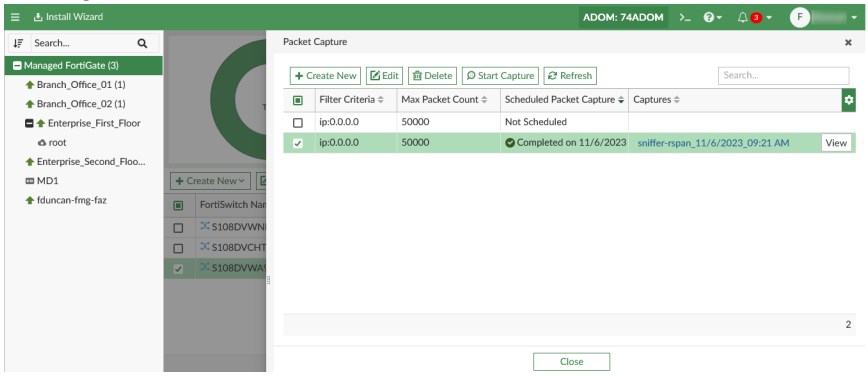
You can run or schedule a FortiSwitch packet capture on FortiManager.

To configure a FortiSwitch packet capture:

1. Go to *FortiSwitch Manager > Managed FortiSwitches*.
2. From the devices menu, select a FortiGate or choose *Managed FortiGate (#)*.
   The FortiSwitch devices for the selected FortiGate(s) are displayed in the table.
3. Select a FortiSwitch from the table, and click *Packet Capture* from the toolbar.
   The *Packet Capture* window is displayed.
4. Click *Create New* to create a new packet capture filter.
5. (Optional) Enable the *Schedule Run* setting to schedule the packet capture to run between the specified start and end time.
6. Configure the remaining filter settings, and click *OK* to save the filter.



7. You can view, edit, delete and run the configured filter in the Packet Capture window.
   - Select the packet capture filter, and click *Start Capture*. After the packet capture is run, you can download the results by clicking *Save as PCAP*.
   - If a schedule is configured, the schedule is displayed in the *Scheduled Packet Capture* field. You can download the results by clicking the capture in the *Captures* field, or see the results in FortiManager by clicking *View*.



Authorizing and deauthorizing FortiSwitch devices

FortiSwitch devices can be authorized and deauthorized from the *Managed FortiSwitches* pane, or from the *Edit Managed FortiSwitch* pane (see Editing switches on page 843).

To authorize FortiSwitch devices:

1. In the tree menu, select a FortiGate that contains the unauthorized FortiSwitch devices, or select *Managed FortiGate* to list all of the switches.
2. In the legend for the *Status* chart, click *Unauthorized*. The unauthorized FortiSwitch devices are displayed in the content pane.
3. Select the switches and either click *Authorize* in the toolbar, or right-click and select *Authorize*.
4. Select *OK* in the confirmation dialog box to authorize the selected devices.

To deauthorize FortiSwitch devices:

1. In the tree menu, select a FortiGate that contains the FortiSwitch devices to be deauthorized.
2. Select the FortiSwitch devices and either click *Deauthorize* in the toolbar, or right-click and select *Deauthorize*.
3. Select *OK* in the confirmation dialog box to deauthorize the selected devices.

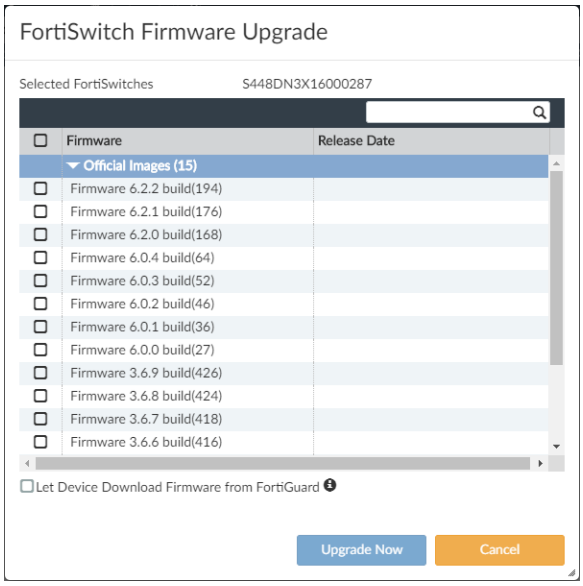
Upgrading firmware for managed switches

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

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

To upgrade firmware for managed switches:

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



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

Using zero-touch deployment for FortiSwitch

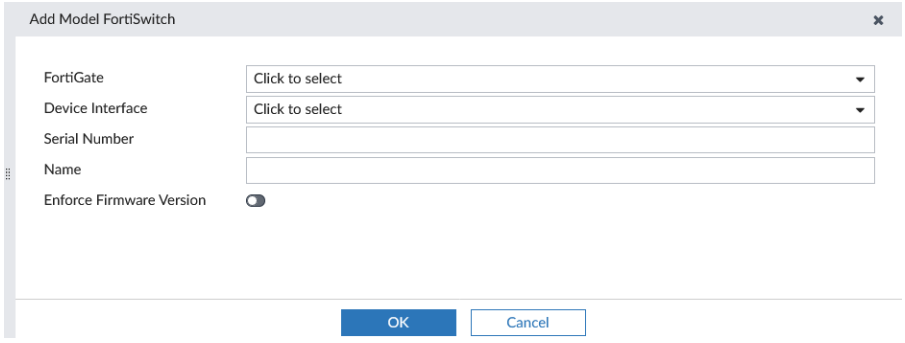
Configure FortiSwitch on FortiManager using its serial number and deploy FortiSwitch devices across the network using zero touch deployment. After configuring FortiSwitch on FortiManager, you can deploy remote FortiSwitch devices by just plugging them into remote FortiGate devices.

Requirements:

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

To enable zero touch deployment:

1. Go to *FortiSwitch Manager > Managed FortiSwitches*.
2. From the *Create New* dropdown, select *FortiSwitch*. The *Add Model FortiSwitch* pane is displayed.



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

FortiGate	Select the FortiGate device or VDOM from the drop-down.
Device Interface	Select the port where the FortiSwitch will be connected.
Serial Number	Specify the FortiSwitch serial number.
Name	Specify a name.
Enforce Firmware Version	Toggle *ON* to enforce a firmware version and select the firmware version from the drop-down menu. Toggle *OFF* to disable this feature.



Adding model devices using a wildcard SN

FortiSwitch model devices can be added using wildcard serial numbers. The wildcard SN format is: *PREFIX****000001*

- *PREFIX*: The first 6 digits of the device's serial number. The prefix must be valid.
- *******: The wildcard characters.
- *000001*: The valid characters.

For example: `S108DV****000001`.

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

4. Click *Close* to close the *Add Model FortiSwitch* pane.
5. Configure the switch.
   - For *FortiSwitch Manager* with central management enabled, see Assigning templates to FortiSwitch devices on page 877.
   - For FortiSwitch Manager with per-device management enabled, see Configuring a port on a single FortiSwitch on page 886.

   Because this is a model device, FortiManager saves the changes to the FortiGate database.
6. Connect FortiSwitch to FortiGate.
   The FortiSwitch settings are deployed to FortiSwitch. You can view the progress on the notification toolbar in FortiManager.



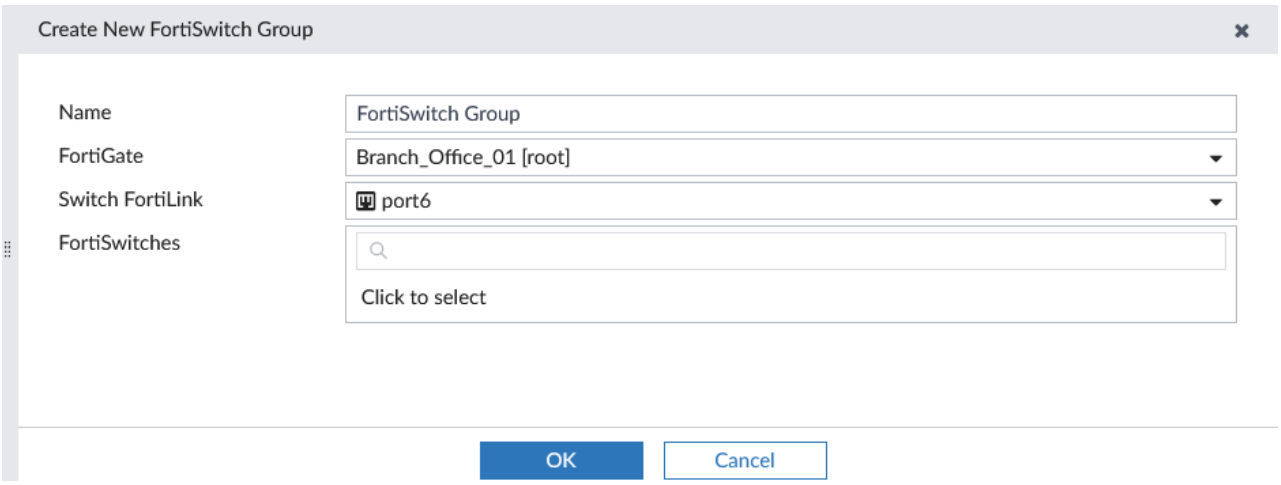
You can also use the Zero Touch Deployment process to deploy FortiGate devices. For more information, see Adding offline model devices on page 104.

Creating a FortiSwitch group

You can configure FortiSwitch groups to manage from the *Group* view in the *FortiSwitch Manager* pane.

To create a FortiSwitch group:

1. Go to *FortiSwitch Manager > Managed FortiSwitches*.
2. From the *Create New* dropdown, click *FortiSwitch Group*.
   The *Create New FortiSwitch Group* dialog displays.



3. Configure the following options:

Option	Description
Name	Enter a name for the FortiSwitch group.
FortiGate	Select the FortiGate device that controls the FortiSwitches.
Switch FortiLink	Select the port.
FortiSwitches	Select the FortiSwitches to add to the group.

4. To save the group, click *OK*.
The Group is now available in the *Group* view of *FortiSwitch Manager > Device & Groups*. From this view, you can *Authorize*, *Deauthorize*, *Upgrade*, or *Restart* all switches in the group at once. See Managing FortiSwitches on page 841

To edit a FortiSwitch group:

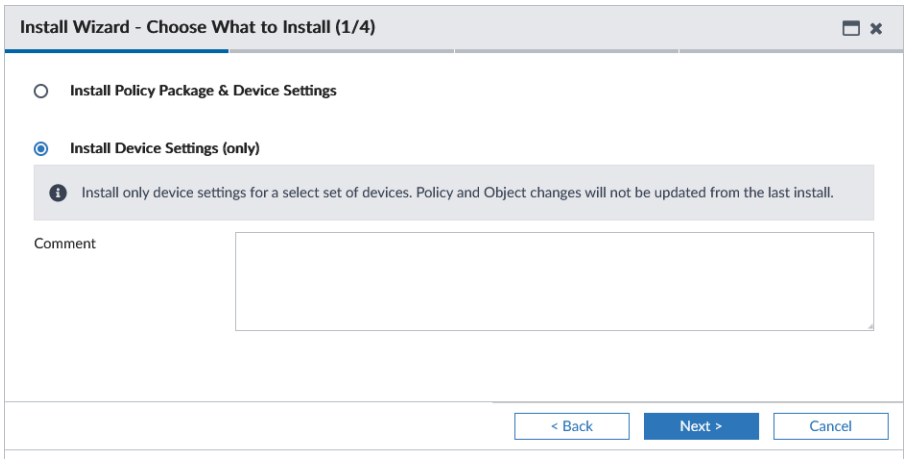
1. Go to *FortiSwitch Manager > Managed FortiSwitches*.
2. From the *List/View/Topology* dropdown, select *Group*.
3. Select the checkbox for the FortiSwitch group.
4. To edit the group, click *Edit*.
Alternatively, you can delete the group by clicking *Delete*.

Installing changes to managed switches

On the *FortiSwitch Manager* pane, you can use the *Install Wizard* to install changes to managed FortiSwitch devices. Alternately you can install changes when you install a configuration to the FortiGate that manages the switch.

To install changes to managed switches:

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



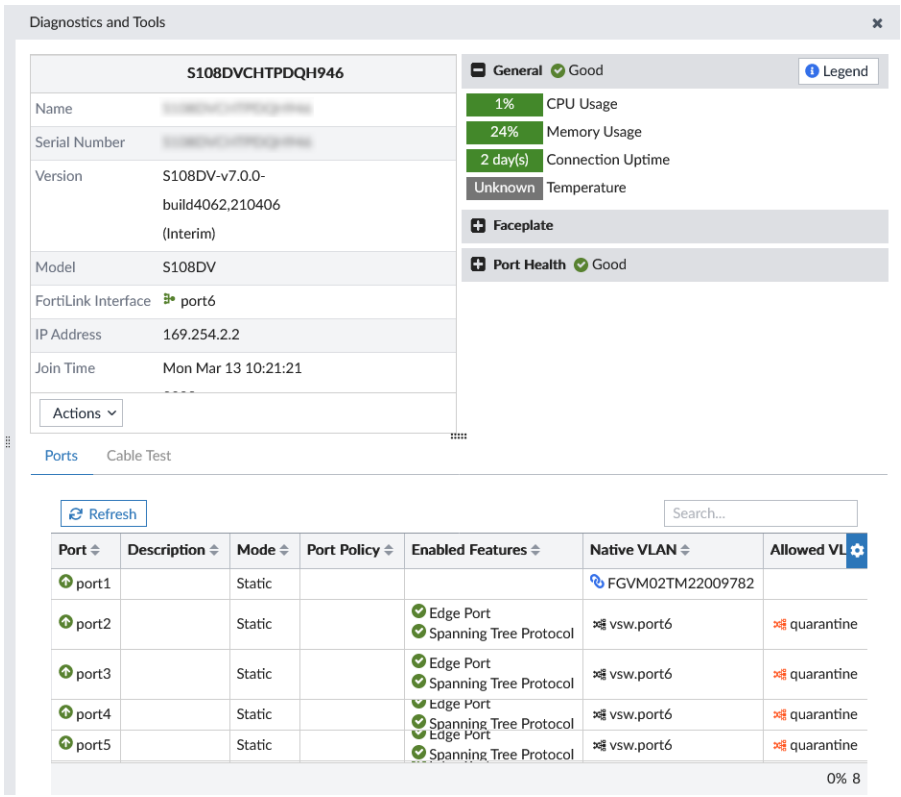
4. Select *Install Device Settings (only)*, and click *Next*.
   The *Device Settings only* pane is displayed.
5. Select the device, and click *Next*.
   The *Device Settings* pane is displayed.
6. (Optional) Click *Install Preview* to review the changes.
7. Click *Install*.

Diagnostics and tools

The *Diagnostics and Tools* form reports the general health of the FortiSwitch unit, displays details about the FortiSwitch unit, and allows you to run diagnostic tests.

You can perform the following tasks from the *Diagnostics and Tools* form:

- Authorize or deauthorize the FortiSwitch
- Upgrade the firmware running on the switch
- Restart the FortiSwitch unit
- Register the FortiSwitch unit
- Run a Cable Test
- Start and Stop an LED Blink
- Packet Capture: Packet capture is only available when traffic sniffing is configured for the device in the FortiGate's CLI. See Performing a packet capture on page 855.



To view the Diagnostics and Tools form:

1. Go to *FortiSwitch Manager > Managed FortiSwitches*
2. In the tree menu, select a FortiGate that contains the FortiSwitch you want to view and then select the unit in the FortiSwitch pane.
3. In the toolbar, click *More > Diagnostics and Tools*, or right-click the unit and select *Diagnostics and Tools*.

Making the LEDs blink

When you have multiple FortiSwitch units and need to locate a specific switch, you can flash all port LEDs on and off for a specified number of minutes.

To identify a specific FortiSwitch unit:

1. In the FortiSwitch pane, select the unit you want to identify.
2. Right-click the unit and select *LED Blink > Start* and then select *5 minutes*, *15 minutes*, *30 minutes*, or *60 minutes*. You can also start the LED Blink from the *Actions* menu in the *Diagnostics and Tools* form.
3. After you locate the FortiSwitch unit, click *LED Blink > Stop*.



For the 5xx switches, LED Blink flashes only the SFP port LEDs, instead of all the port LEDs.

Performing a packet capture

To perform a packet capture on managed FortiSwitch devices:

1. In the FortiGate CLI, configure the `switch-controller traffic-sniffer` setting.
   For example:
```
config switch-controller traffic-sniffer
   set mode rspan
   config target-mac
      edit 00:0c:29:1a:2b:3c
         set description "ABC123"
      next
   end
   config target-ip
      edit 192.168.11.11
         set description "ABC123IP"
      next
   end
   config target-port
      edit "S000DN4K15000050"
         set description "ABC123switch"
         set out-ports "port1"
      next
   end
```
2. Go to *Managed FortiSwitches*, select a FortiSwitch device, right-click and select *Diagnostics and Tools*. When the FortiSwitch is configured in `switch-controller traffic-sniffer`, the *Packet Capture* tab is displayed and can be selected.
3. Configure the *Max Number of Packets* and/or *Filters*, and click *Start Capture* to begin capturing packets.
4. Select *Graph*, *Headers* or *Packet Data* to view details of the packet.
5. When the packet capture stops, the captured packets can be saved as a .pcap file.

Run a cable test on FortiSwitch ports from FortiManager

You can trigger a FortiSwitch cable test from FortiManager.

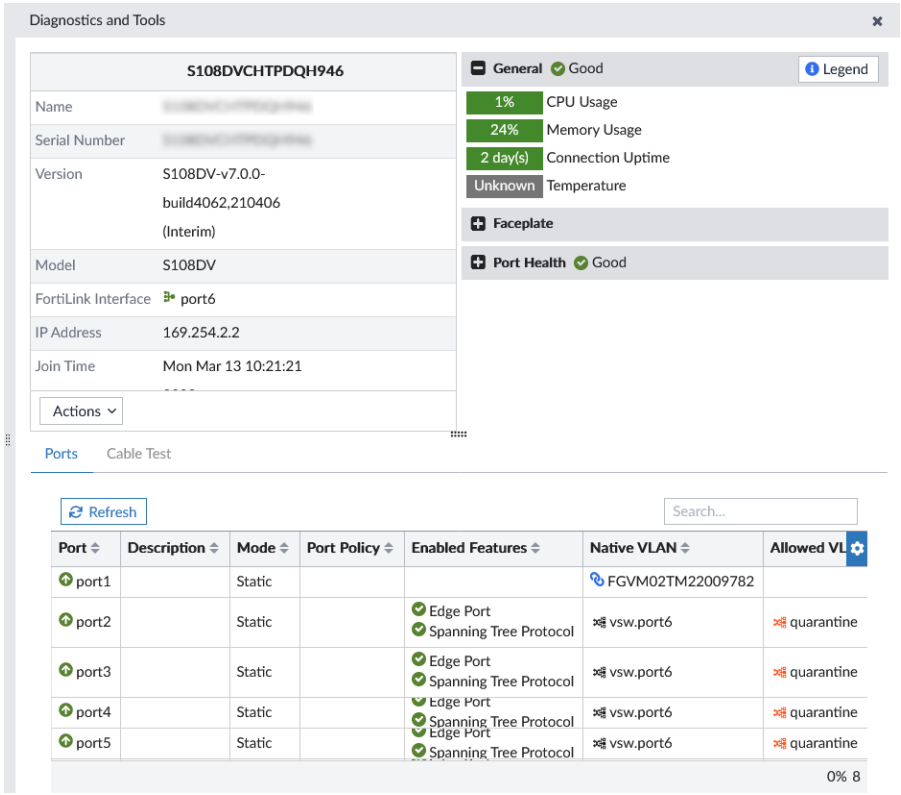


The FortiSwitch cable test is only available on ADOM 6.4 and later.

To perform a FortiSwitch cable test:

1. Go to *FortiSwitch Manager > Managed FortiSwitches*.
2. In the tree menu, select a FortiGate that contains the FortiSwitch and then select the unit in the FortiSwitch pane.
3. In the toolbar, click *More > Diagnositcs and Tools* from the toolbar, or right-click the FortiSwitch and select *Diagnositcs and Tools*. The *Diagnostics and Tools* form opens.

4. Click *Cable Test*.

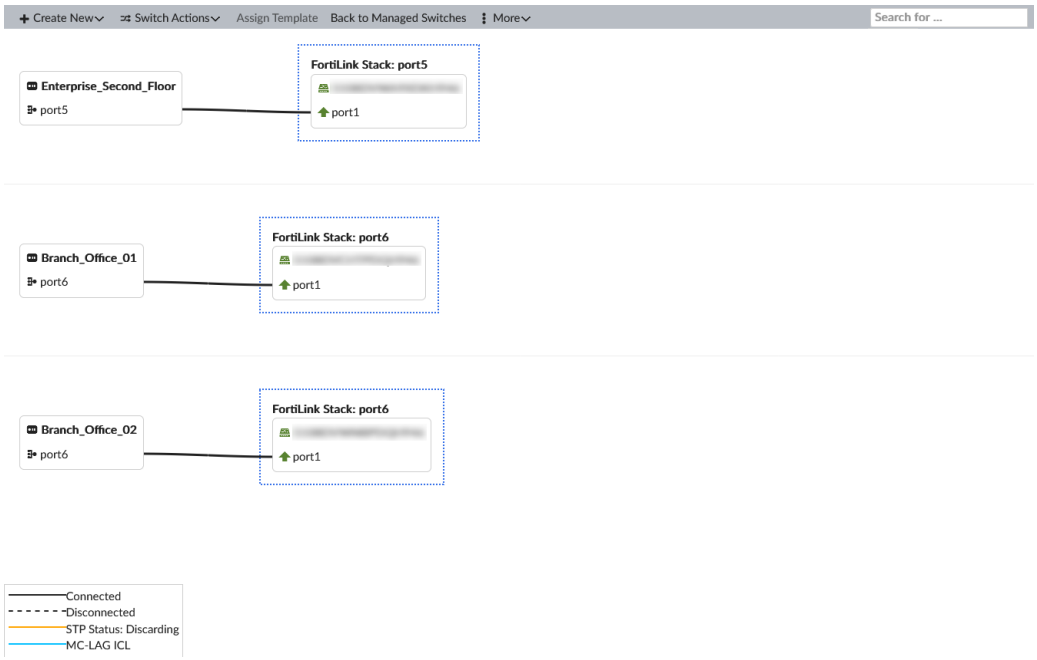


5. In the *Cable Test* pane, select the FortiSwitch ports you want to test, and click *Diagnose*. Once the cable test is run, the results are displayed

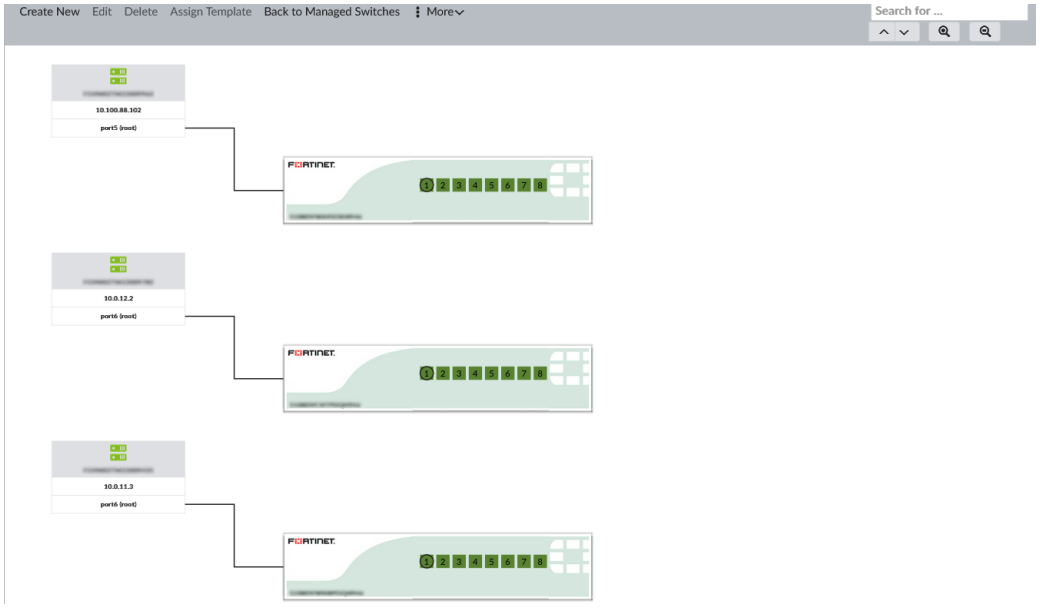
Monitors

The *FortiSwitch Manager > Managed FortiSwitches* pane includes both a graphical representation and a port status or faceplates view of the connected FortiSwitch devices. You can see a block-style topology view or a faceplates view similar to FortiOS for selected devices. This gives you the visibility of the managed FortiSwitch status, connection topology, and MC-LAG status among others.

Go to *FortiSwitch Manager > Managed FortiSwitches*. From the *List/Group/Topology* dropdown, select *Topology* to display a block-style topology representation of the connected FortiSwitch devices. Use the search box to find a specific device or filter the view, and hover over connections or ports to get more information.



Go to *FortiSwitch Manager > Managed FortiSwitches* and click *Faceplates* from the *More* menu in the toolbar to see a port status or faceplate view of the connected FortiSwitch devices. Use the search box to find a specific device or filter the view, and hover over connections or ports to get more information.



Hovering the cursor over a port group will open a pop-up showing the type of port in the group. Hovering the cursor over a port will open a pop-up showing information about the port, including:

Port	The port number.
FortiSwitch	The name of the FortiSwitch.

Peer Device	The device that this switch is connected to. The current port, as well as the port that it is connected to on the connected, and the connection between the two devices, will be highlighted. This item is only displayed when the port is connected to another FortiSwitch device.
Link	The state of the link, either *up* or *down*.
Native VLAN	The native VLAN of the port.
Speed	The speed of the port, such as *1000Mbps/Full Duplex*. The value is *0Mbps* if the link is down.
Bytes Sent	The total number of bytes sent by the port.
Bytes Received	The total number of bytes received by the port.

FortiSwitch central management

When central management is enabled, you can create templates for a variety of switch configurations, and assign templates to multiple managed switches. The following steps provide an overview of using centralized FortiSwitch management to configure and install templates:

1. Enable central management of switches. See Enabling FortiSwitch central management on page 858.
2. Create FortiSwitch VLANs. See FortiSwitch VLANs on page 865.
3. Create or import FortiSwitch templates. See FortiSwitch Templates on page 859.
4. Assign templates to FortiSwitch devices. See Assigning templates to FortiSwitch devices on page 877.
5. Install the templates to the devices. See Installing changes to managed switches on page 852.

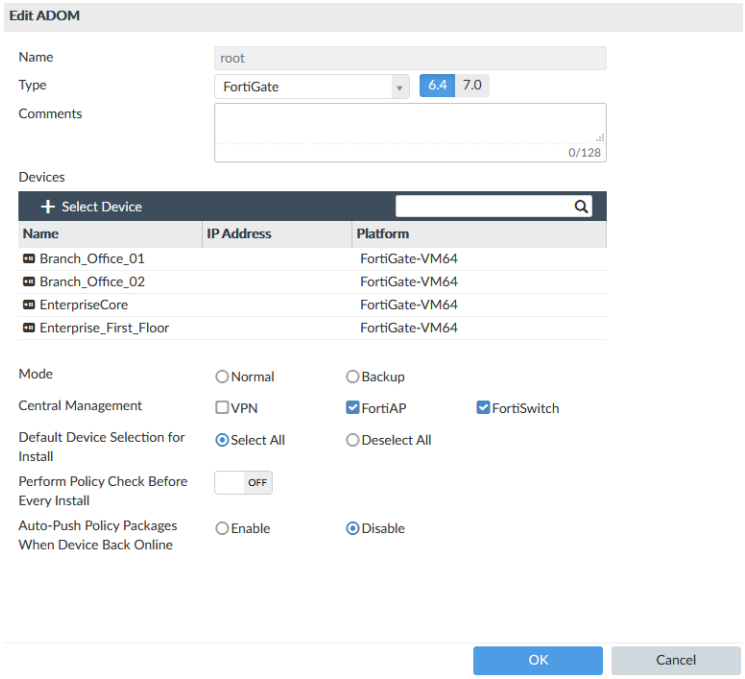
Enabling FortiSwitch central management

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

To enable central management:

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

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



Central management is enabled for FortiSwitch.

FortiSwitch Templates

The *FortiSwitch Manager* > *FortiSwitch Templates* pane is available when central management is enabled. You can use the *FortiSwitch Templates* pane to create and manage FortiSwitch templates, VLANs, security policies, LLDP profiles, QoS policies, and custom commands that can be assembled into templates, and then the template assigned to FortiSwitch devices.

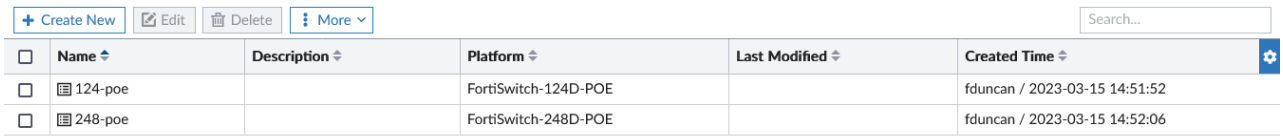
You can also import templates from FortiSwitch devices, and then apply the template to other FortiSwitch devices of the same model. See Importing AP profiles and FortiSwitch templates on page 179.

Accessing FortiSwitch templates

FortiSwitch templates define VLAN and PoE assignments for a FortiSwitch platform.

To view FortiSwitch templates:

1. Ensure that you are in the correct ADOM.
2. Go to *FortiSwitch Manager* > *FortiSwitch Templates*.



The following options are available in the toolbar and right-click menu:

Create New	Create a new FortiSwitch template. See Creating FortiSwitch templates on page 860.
Edit	Edit the selected template.
Clone	Create a copy of an existing template.
Delete	Delete the selected template or templates.
Where Used	View where the selected template is used.
Import	Import a FortiSwitch template. See Importing FortiSwitch templates on page 863.
Column Settings	Adjust the visible columns.
Search	Enter a search string into the search field to search the template list.

To edit a template:

1. Double-click a template name.
   Alternately you can right-click a template, and click *Edit* in the toolbar.
   The *Edit FortiSwitch Template* pane opens.
2. Edit the settings as required.
3. Click *OK* to apply your changes.

To delete templates:

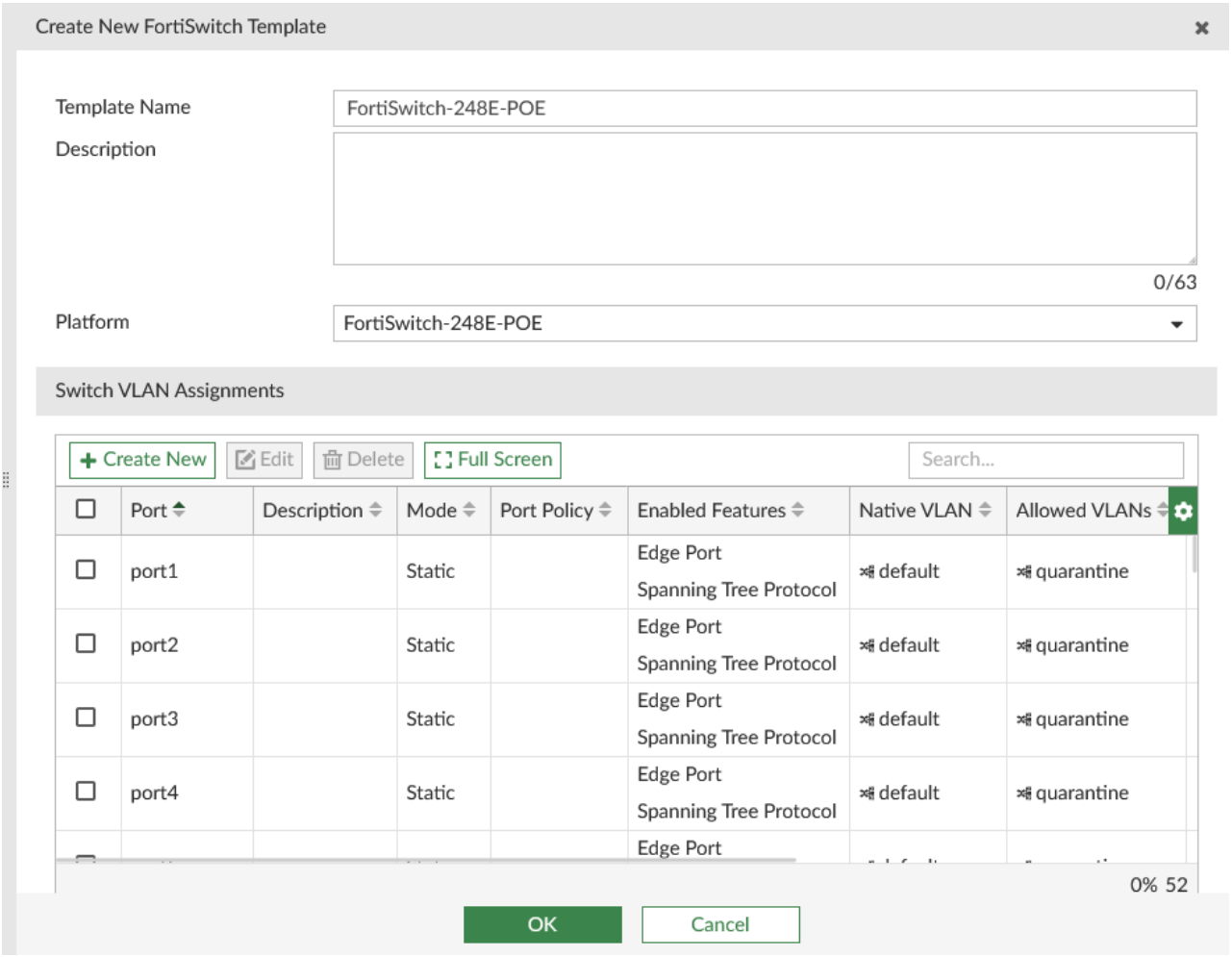
1. Select the template or templates that will be deleted.
2. Either click *Delete* from the toolbar, or right-click and select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the selected template or templates.

Creating FortiSwitch templates

When creating a new FortiSwitch template, the platform must be selected before configuring VLAN assignments.

To create a FortiSwitch template:

1. Go to *FortiSwitch Manager* > *FortiSwitch Templates*.
2. In the content pane, click *Create New* in the toolbar. The *Create New FortiSwitch Template* window opens.



3. Enter the following information, then click *OK* to create the new template.

Template Name	Type a name for the template.
Description	Optionally, enter a description.
Platforms	Select the platform that the template will apply to from the dropdown list.
Switch VLAN Assignments	Configure VLAN assignments. A platform must be selected before VLAN assignments can be configured. Right-clicking on a physical port or trunk group displays a context menu with options to edit, delete, and modify the selection(s). Using the context menu, you can also configure *Native VLAN*, *Allowed VLAN*, *Security Policy*, *QoS Policy*, and *LLDP profiles* while multiple ports are selected.

	Create	Create a physical port or trunk group. See Creating ports and trunk groups on page 862.
	Edit	Edit the selected port or trunk.
	Delete	Delete the selected ports or trunks.
	Column Settings	Select which columns are visible or hidden in the Switch VLAN Assignments table.
	Full Screen/Exit Full Screen	Click to enter/exit fullscreen mode for the VLAN assignment table.
Custom Command Entry		Create a new custom command entry. Enter a name, and select a previously configured custom command. See Custom commands on page 874. If a custom command has not yet been created, click the add icon in the *Custom Command* selection box to create one.

Creating ports and trunk groups

To create a physical port:

1. On the *Create New FortiSwitch Template* pane, click *Create* in the *Switch VLAN Assignments* toolbar. The *Add VLAN Assignment* dialog box opens.
2. Select *physical* as the type.
3. Configure the following settings:

4.

Port Name	Enter the name of the port.
Description	Optionally, enter a description.
Access Mode	Select the access mode from *dynamic*, *nac*, or *normal*.
Port Policy	Select the dynamic port policy from the available port policy objects. See FortiSwitch dynamic port policies on page 872. This setting is only available when the access mode is dynamic.
Native VLAN	Select the native VLAN from the available VLAN objects. See FortiSwitch VLANs on page 865. This setting is only available when the access mode is normal.
Allowed VLAN	Select the allowed VLAN from the available VLAN objects. See FortiSwitch VLANs on page 865.
Security Policy	Select the security policies from the available switch controller security policies. See Viewing FortiSwitch security policies on page 873.
LLDP Profile	Select an LLDP profile.
QoS Policy	Select a QoS policy.
DHCP Blocking	Enable or disable DHCP blocking for the port or trunk.

	If the port is in a trunk, then DHCP blocking can only be enabled for the trunk, and not the individual ports.
Loop Guard	Enable or disable Loop Guard for the port. Loop Guard cannot be applied to trunks, or ports that are in trunks.
STP	Enable or disable STP for the port or trunk. If the port is in a trunk, then STP can only be enabled for the trunk, and not the individual ports.
Edge Port	Enable or disable Edge Port for the port or trunk. If the port is in a trunk, then STP can only be enabled for the trunk, and not the individual ports.
STP BPDU Guard	Enable or disable STP BPDU Guard for the port or trunk. If the port is in a trunk, then STP BPDU Guard can only be enabled for the trunk, and not the individual ports.
STP Root Guard	Enable or disable STP Root Guard for the port or trunk. If the port is in a trunk, then STP Root Guard can only be enabled for the trunk, and not the individual ports.

5. Click *OK* to create the port.
Additional settings are available through the right-click context menu in the *Switch VLAN Assignments* table once the port has been created.

POE	Right-click to enable or disable PoE for the port where applicable.
IGMP Snooping	Right-click to enable or disable IGMP snooping. If the port is in a trunk, then IGMP snooping can only be enabled for the trunk, and not the individual ports.

To create a trunk group:

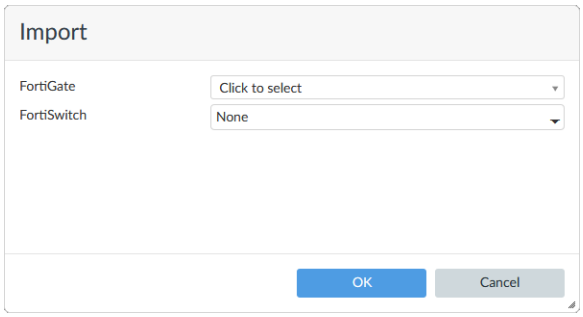
1. On the *Create New FortiSwitch Template* pane, click *Create* in the *Switch VLAN Assignments* toolbar. The *Add VLAN Assignment* dialog box opens.
2. Select *trunk* as the type.
3. Enter a name for the trunk group in the *Trunk Name* field.
4. In the *Members* field, select all the ports that will be in the group from the dropdown list.
5. Select the mode: *lacp-active* (active link aggregation), *lacp-passive* (passive link aggregation), or *static*.
6. Click *OK* to create the trunk group.

Importing FortiSwitch templates

FortiSwitch templates can be imported from connected devices, and then applied to other FortiSwitch devices of the same model.

To import a FortiSwitch template:

1. Go to *FortiSwitch Manager* > *FortiSwitch Template*.
2. In the content pane, click *More* > *Import* in the toolbar. The *Import* window opens.



3. Select a FortiGate from the dropdown list.
4. Select the FortiSwitch whose template will be imported from the dropdown list.
5. (Optional) Enter a name for the template in the *New Name* field.
6. Click *OK*.
   The template is imported from the device.

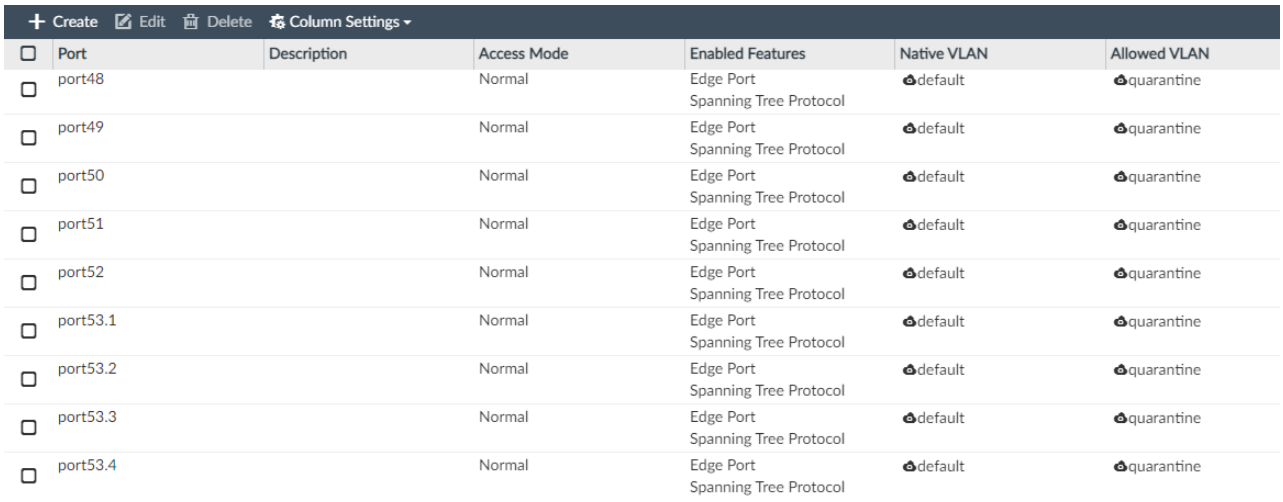
FortiSwitch templates can also be imported through the Device Manager. See Importing AP profiles and FortiSwitch templates on page 179.

FortiSwitch templates with split ports

FortiSwitch templates using split ports can be imported into FortiManager. Before adding the FortiSwitch to FortiGate, the administrator must enable split ports through `phy-mode` on the FortiSwitch. Once the FortiSwitch has been authorized on the FortiGate, the FortiGate can be added to FortiManager, and the template can be imported.

To import FortiSwitch templates with split ports:

1. On the FortiSwitch, enable split ports using `phy-mode`. See FortiSwitch documentation on the Fortinet Document Library.
2. Authorize the FortiSwitch device on FortiGate, and add the FortiGate device to FortiManager. See Add devices on page 91.
3. Import the FortiSwitch template using the *Import* feature in *FortiSwitch Manager* > *FortiSwitch Templates*. See Importing FortiSwitch templates on page 863.
4. Once the import is complete, edit the imported template.
   To view FortiSwitch split ports, select *View Ports* from the Managed Switches menu. The split port configuration is retained and is visible in the list of *Switch VLAN Assignments*. See Managing FortiSwitches on page 841.



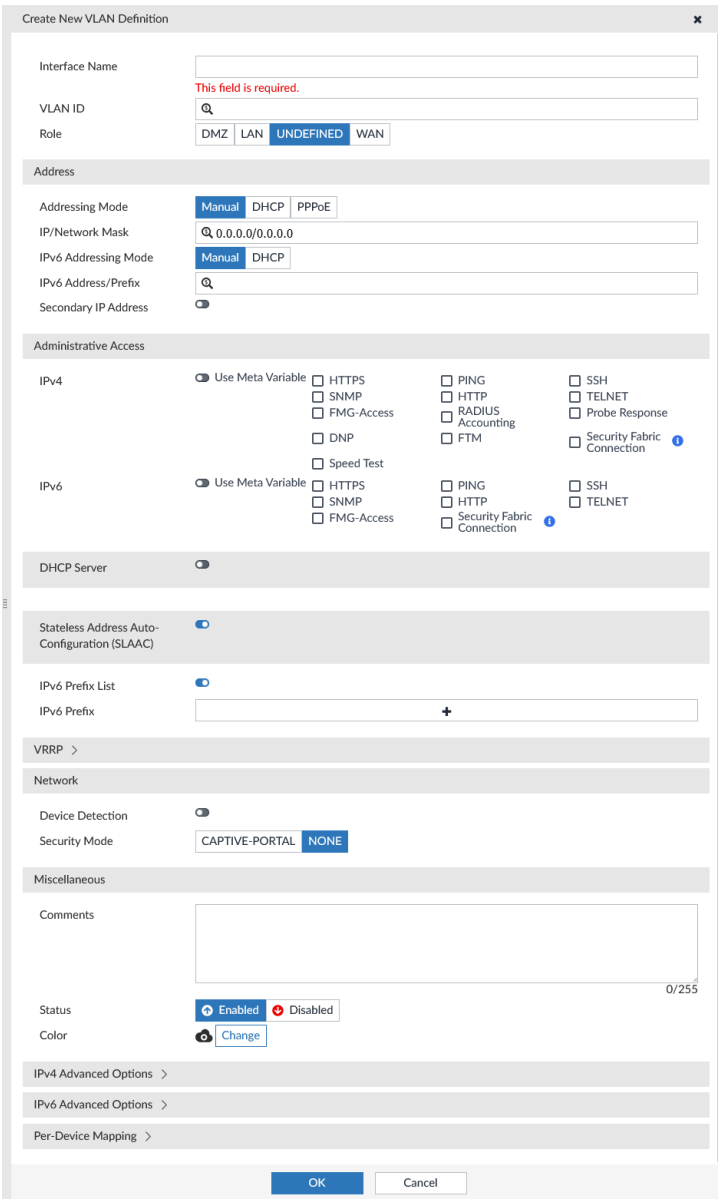
Port	Description	Access Mode	Enabled Features	Native VLAN	Allowed VLAN
port48		Normal	Edge Port Spanning Tree Protocol	default	quarantine
port49		Normal	Edge Port Spanning Tree Protocol	default	quarantine
port50		Normal	Edge Port Spanning Tree Protocol	default	quarantine
port51		Normal	Edge Port Spanning Tree Protocol	default	quarantine
port52		Normal	Edge Port Spanning Tree Protocol	default	quarantine
port53.1		Normal	Edge Port Spanning Tree Protocol	default	quarantine
port53.2		Normal	Edge Port Spanning Tree Protocol	default	quarantine
port53.3		Normal	Edge Port Spanning Tree Protocol	default	quarantine
port53.4		Normal	Edge Port Spanning Tree Protocol	default	quarantine

Administrators can edit the split ports, and changes can be installed to the FortiGate when the template is assigned to a managed FortiSwitch.
When per-device FortiSwitch management is enabled, users can edit split ports in the *Ports Configuration* page. See Configuring a port on a single FortiSwitch on page 886.

FortiSwitch VLANs

To create a FortiSwitch VLAN:

1. Go to *FortiSwitch Manager > FortiSwitch VLANs*.
2. In the content pane, click *Create New* in the toolbar. The *Create New VLAN Definition* window opens.



3. Enter the following information, then click *OK* to add the new VLAN.

Interface Name	Enter a name for the interface.
VLAN ID	Enter the VLAN ID
Role	Select the role for the interface: *DMZ*, *LAN*, *UNDEFINED*, or *WAN*.
Estimated Bandwidth	Enter the estimated upstream and downstream bandwidths. This option is only available when *Role* is *WAN*.
Address	
Addressing mode	The addressing mode.
IP/Network Mask	Enter the IP address and netmask.

IPv6 Addressing mode	Select the IPv6 addressing mode: *Manual* or *DHCP*.
IPv6 Address/Prefix	Enter the IPv6 address. This option is only available when *IPv6 Addressing mode* is *Manual*.
Secondary IP Address	Turn secondary IP addresses on or off. Add IP addresses to the table. See To add a secondary IP address: on page 871 for details. Addresses can also be edited and deleted as required.
Administrative Access	
IPv4	Select the allowed IPv4 administrative service protocols from: *CAPWAP*, *DNP*, *FGFM*,*FTM*,*HTTP*, *HTTPS*, *PING*, *PROBE-RESPONSE*, *RADIUS-ACCT*, *SNMP*, *SSH*, and *TELNET*. Toggle *Use Meta Variable* ON to alternatively use a metadata variable to define this field. See ADOM-level metadata variables on page 557.
IPv6	Select the allowed IPv6 administrative service protocols from: *CAPWAP*, *FGFM*, *HTTP*, *HTTPS*, *PING*, *SNMP*, *SSH*, and *TELNET*. Toggle *Use Meta Variable* ON to alternatively use a metadata variable to define this field. See ADOM-level metadata variables on page 557.
DHCP Server	Turn the DHCP server on or off.
DHCP Status	Set the DHCP status as *Enabled* or *Disabled*.
Address Range	Configure address ranges for DHCP. Click *Create* to create a new range. Ranges can also be edited and deleted as required. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
Netmask	Enter the netmask. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
Default Gateway	Configure the default gateway: *Same as Interface IP*, or *Specify*. If set to *Specify*, enter the gateway IP address in the field. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
DNS Server	Configure the DNS server: *Same as System DNS*, *Same as Interface IP*, or *Specify*. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.

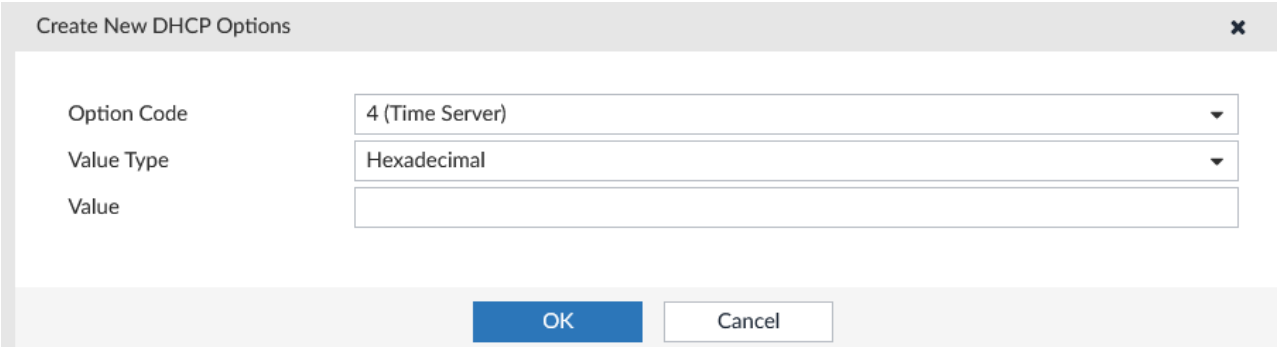
DNS Server 1 - 3		Enter the DNS server IP addresses. This option is only available when *DHCP Server* is *ON*, *Mode* is *Server*, and *DNS Server* is *Specify*.
Advanced		Expand advanced options
	Mode	Select the DHCP mode: *Server* or *Relay*. This option is only available when *DHCP Server* is *ON*.
	Type	Select the type: *Regular*, or *IPsec*. This option is only available when *DHCP Server* is *ON*.
	NTP Server	Configure the NTP server: *Local*, *Same as System NTP*, or *Specify*. If set to *Specify*, enter the NTP server IP address in the field. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
	Wireless Controllers	Configure wireless controllers: *Same as Interface IP* or *Specify*. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
	Timezone Option	Configure the timezone: *Disable*, *Same as System*, or *Specify*. If set to *Specify*, select the timezone from the dropdown list. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
	Next Bootstrap Server	Enter the IP address of the next bootstrap server. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
	TFTP Server(s)	Add TFTP server(s).
	Additional DHCP Options	In the *Lease Time* field, enter the lease time, in seconds. Default: 604800 seconds (7 days). Add DHCP options to the table. See To add additional DHCP options: on page 870 for details. Options can also be edited and deleted as required. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.
	IP Address Assignment Rules	Select the action to take with unknown MAC addresses or DHCP Relay Agent: *Assign IP*, *Block* or *Reserve IP*. Specify the match criteria. Add MAC address actions to the table. See To add a MAC address or DHCP Relay Agent reservation: on page 871 for details. Reservations can also be edited and deleted as required. This option is only available when *DHCP Server* is *ON* and *Mode* is *Server*.

Stateless Address Auto-Configuration (SLAAC)	Enable or disable stateless address auto-configuration (SLAAC).
IPv6 Prefix List	Enable to define an IPv6 Prefix.
VRRP	Configure VRRP settings for the VLAN template. Click *Create New* to create a new VRRP item.
Network	These options are only available when *Role* is *DMZ*, *LAN*, or *UNDEFINED*.
Device Detection	Turn device detection on or off.
Active Scanning	Turn active scanning on or off. This option is only available when *Device Detection* is on.
Security Mode	Select the security mode: *CAPTIVE-PORTAL*, or *NONE*.
Authentication Portal	Configure the authentication portal: *Local* or *External*. If *External* is selected, enter the portal in the field. This option is only available when *Security Mode* is *CAPTIVE-PORTAL*.
User Access	Select *Restricted to Groups* or *Allow All*. This option is only available when *Security Mode* is *CAPTIVE-PORTAL*.
User Groups	Select user groups from the available groups. This option is available when *Security Mode* is *CAPTIVE-PORTAL* and *User Access* is *Restricted to Groups*.
Exempt Sources	Select sources that are exempt from the available firewall addresses. This option is only available when *Security Mode* is *CAPTIVE-PORTAL*.
Exempt Destinations	Select destinations that are exempt from the available firewall addresses. This option is only available when *Security Mode* is *CAPTIVE-PORTAL*.
Exempt Services	Select services that are exempt from the available firewall services. This option is only available when *Security mode* is *CAPTIVE-PORTAL*.
Miscellaneous	
Comments	Optionally, enter comments.
Status	Select if the interface is *Enabled* or *Disabled*.
Color	Change the color of the interface to one of the 32 options.
IPv4 Advanced Options	Expand to view and configure advanced IPv4 options.

IPv6 Advanced Options	Expand to view and configure advanced IPv6 options.
Per-Device Mapping	Enable per-device mapping. Add mappings to the table. See To add per device mapping: on page 871 for details. Mappings can also be edited and deleted as required.

To add additional DHCP options:

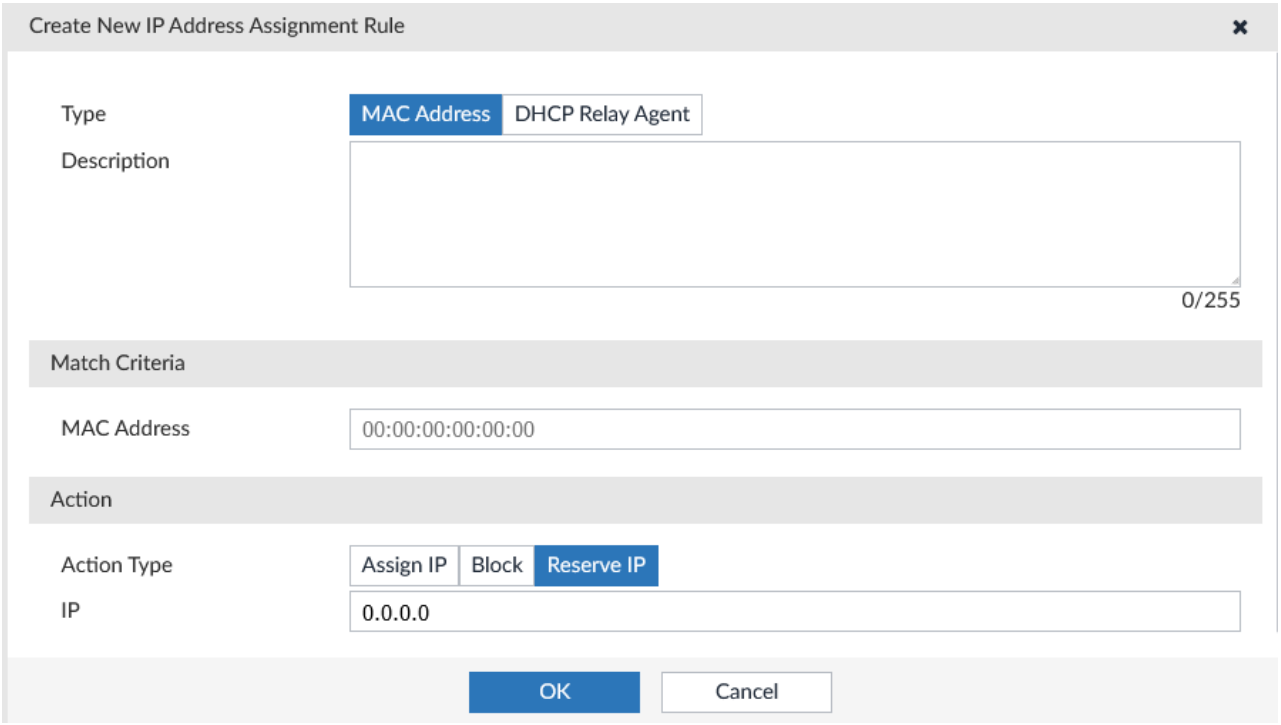
1. Enable the *DHCP Server* setting, and expand the *Advanced* drawer.
2. Click *Create New* in the *Additional DHCP Options* table toolbar. The *Additional DHCP Options* dialog box opens.



3. Enter the *Option Code*.
4. Select the *Value Type*: *Hexadecimal*, *String*, *IP*, or *FQDN*.
5. Enter the corresponding value.
6. Click *OK* to create the option.

To add a MAC address or DHCP Relay Agent reservation:

1. Enable the *DHCP Server* setting, and expand the *Advanced* drawer.



2. Click *Create New* in the *IP Address Assignment Rules* table toolbar. The *Create New IP Address Assignment Rule* dialog box opens.
3. Select the Type as either *MAC Address* or *DHCP Relay Agent*, and enter the corresponding *Match Criteria*.
4. Select the *Action Type* as *Assign IP*, *Block*, or *Reserve IP*. When selecting *Reserve IP*, specify the IP address.
5. Click *OK* to create the reservation.

To add a secondary IP address:

1. Enable the *Secondary IP Address* setting under *Address*.
2. Click *Create New* in the *Secondary IP address* table toolbar. A dialog box opens.
3. Enter the IP address and netmask in the *IP/Network Mask* field.
4. Select the allowed administrative service protocols from: *CAPWAP*, *DNP*, *FGFM*, *FTM*, *HTTP*, *HTTPS*, *PING*, *PROBE-RESPONSE*, *RADIUS-ACCT*, *SNMP*, *SSH*, and *TELNET*.
5. Click *OK* to add the address.

To add per device mapping:

1. Expand the *Per-Device Mapping* section.
2. Click *Create New* in the *Per-Device Mapping* table toolbar. The *Per-Device Mapping* dialog box opens.
3. Select the device to be mapped from the *Mapped Device* drop-down list.
4. Enter the VLAN ID.
5. Enter the mapped IP address and netmask in the *IP/Netmask* field.

6. If required, enable *Mapped DHCP Server* and configure the options (options are the same as when creating a new VLAN definition).
7. Configure the remaining settings as needed.
8. Click *OK* to add the device mapping.

FortiSwitch dynamic port policies

To create a FortiSwitch dynamic port policy:

1. Go to *FortiSwitch Manager* > *Port Policies* > *Dynamic Port Policies*.
2. Click *Create New*. The *Create New Dynamic Port Policy* pane opens.
3. Enter a name for the dynamic port policy.
4. In the *Policy Information* section, click *Create New*. The *Create New Dynamic Port Policy Rule* pane opens.
5. Enter the following information, and click *OK* to save the dynamic port policy rule.

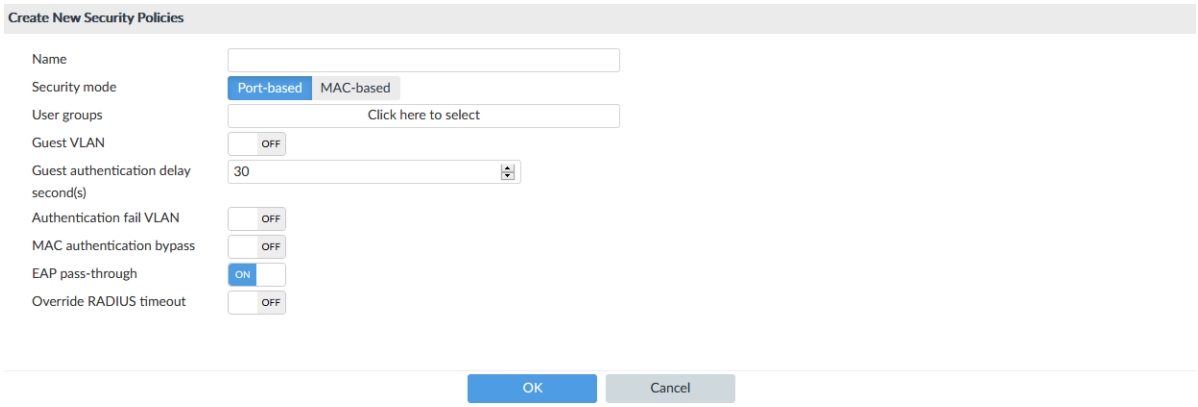
Name	Enter a unique name for the dynamic port policy rule.
Status	Set the rule to Enabled or Disabled.
Description	Optionally, enter a description for the rule.
Device Patterns	
MAC Address	Enable or disable matching a MAC address, then enter a MAC address.
Host	Enable or disable matching a host address, then enter a host address.
Hardware Vendor	Enable or disable matching a hardware vendor, then enter a hardware vendor name.
Device Family	Enable or disable matching a device family, then enter a device family name.
Type	Enable or disable matching a device type, then enter a device type.
Switch Controller Action	
LLDP Profile	Enable to select an LLDP profile for the switch controller action.
QoS Policy	Enable to select a QoS policy for the switch controller action.
802.1X Policy	Enable to select an 802.1X policy for the switch controller action.
VLAN Policy	Enable to select a QoS policy for the switch controller action.

6. Click OK to save the dynamic port policy.
The dynamic port policy can now be used in a FortiSwitch template. See Creating FortiSwitch templates on page 860.

FortiSwitch security policies

To create a FortiSwitch security policy:

1. Go to *FortiSwitch Manager* > *Port Policies* > *Security Policies*.
2. In the content pane, click *Create New* in the toolbar. The *Create New Security Policies* window opens.



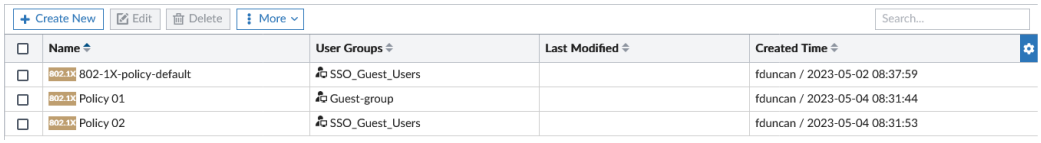
3. Enter the following information, then click *OK* to create the new security policy.

Name	Type a name for the template.
Security mode	Select the security mode, *Port-based* or *MAC-based*.
User groups	Select the user groups that the security policy will apply to.
Guest VLAN	Enable a guest VLAN, and select the VLAN from the available VLAN objects. See FortiSwitch VLANs on page 865.
Guest authentication delay second(s)	Set the guest authentication delay, in seconds (1 - 900, default = 30).
Authentication fail VLAN	Enable an authentication failure VLAN, and select the VLAN from the available VLAN objects. See FortiSwitch VLANs on page 865. This option is not available when *Security mode* is *MAC-based*.
MAC authentication bypass	Enable MAC Authentication Bypass (MAB).
EAP pass-through	Enable EAP pass-through.
Override RADIUS timeout	Enable overriding the RADIUS timeout.

Viewing FortiSwitch security policies

To view FortiSwitch security policies:

1. Ensure that you are in the correct ADOM.
2. Go to *FortiSwitch Manager* > *Port Policies* > *Security Policies*.
3.



The following options are available in the toolbar and right-click menu:

Create New	Create a new FortiSwitch security policy. See FortiSwitch security policies on page 873.
Edit	Edit the selected policy.
Clone	Create a copy of the selected security policy.
Delete	Delete the selected policy or policies.
Where Used	See where the security policy is being used.
Import	Import security policies from a managed FortiGate device.
Column Settings	Select which columns are hidden or displayed in the security policy table.
Search	Enter a search string into the search field to search the policy list.

To edit a security policy:

1. Either double-click a policy, right-click a policy and select *Edit*, or select a policy then click *Edit* in the toolbar. The *Edit Security Policies* pane opens. The name cannot be edited.
2. Edit the settings as required, then click *OK* to apply your changes.

To delete security policies:

1. Select the policy or policies that will be deleted.
2. Either click *Delete* from the toolbar, or right-click and select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the selected policy or policies.

To import security policies:

1. Click *Import* on the toolbar. The *Import* dialog box opens.
2. Select the FortiGate that the policies will be imported from in the drop-down list.
3. Select the policies that will be imported.
4. If only one policy is being imported, and its name is already used by a policy on the FortiManager, you can optionally enter a new name for the policy. If a new name is not entered, or if you are importing multiple policies, existing policies will be overwritten by imported policies.
5. Click *OK* in the confirmation dialog box to import the policies.

Custom commands

When creating or editing a new FortiSwitch template, you can include custom commands in the template. After the template has been assigned to the FortiSwitch, use the *Install Wizard* to install the custom command entry to the FortiGate.

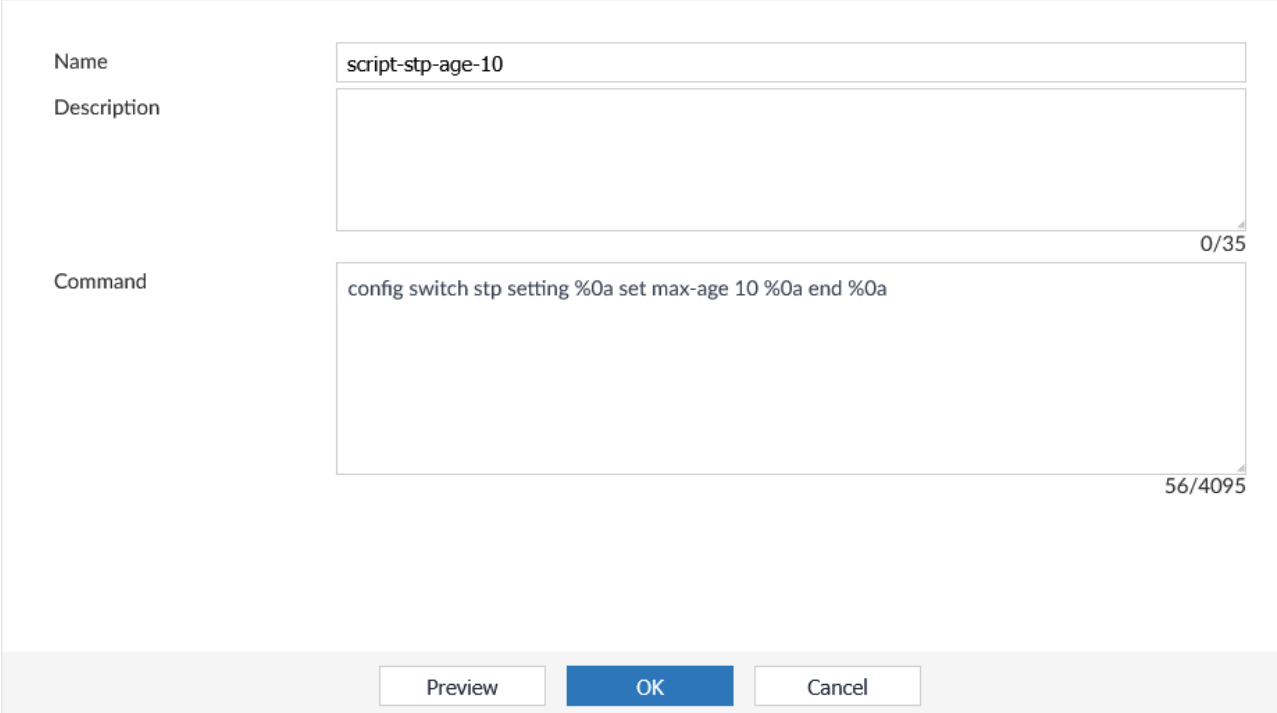
To create a custom command:

1. Go to *FortiSwitch Manager > Custom Commands*.
2. In the content pane, click *Create New* in the toolbar. The *Create New Custom Command* window opens.

3. Enter the following information, then click *OK* to create the new custom command.

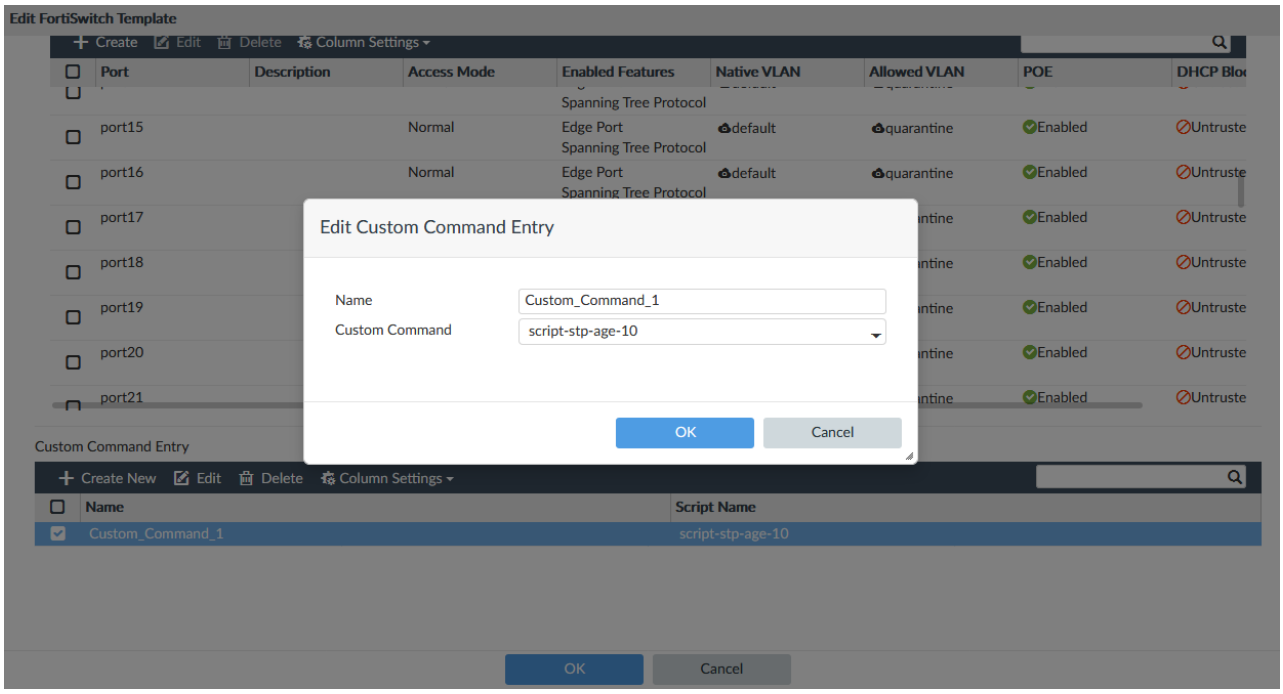
Name	Type a name for the custom command template.
Description	Optionally, type a description.
Command	Enter the CLI commands. Commands must be added on a single line. You can use `%0a` to indicate a return. For more information on custom FortiSwitch scripts, see the FortiLink Guide. Quotation marks cannot be used within the command.

Below is an example custom command.



You can now add the custom command to a FortiSwitch template.

4. Go to *FortiSwitch Manager* > *FortiSwitch Templates*, and edit an existing template or create a new one.
5. In the *Custom Command Entry* table, click *Create New*.
   The *Create New Custom Command Entry* dialog appears.
6. Enter a name for the command entry and select your previously configured custom command. Click *OK*, and save your changes to the FortiSwitch template.

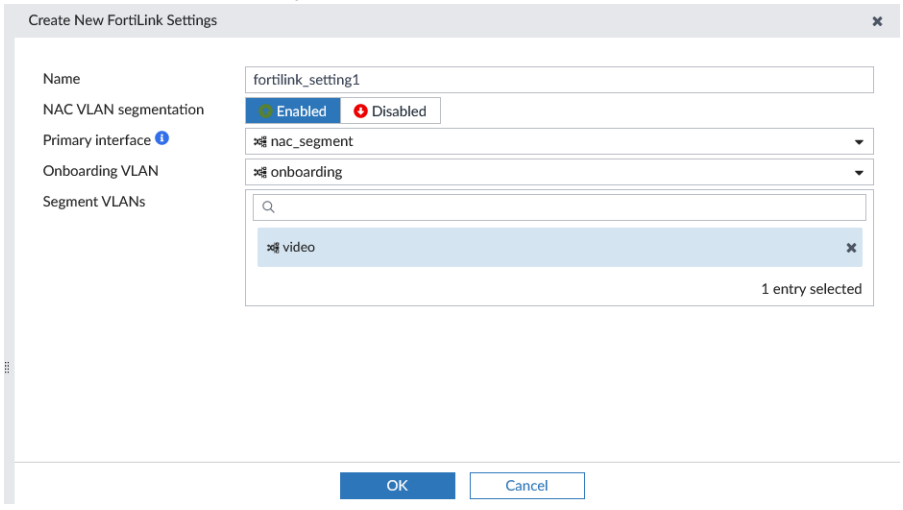


You can now install the custom command using the Install Wizard. See Installing changes to managed switches on page 852.

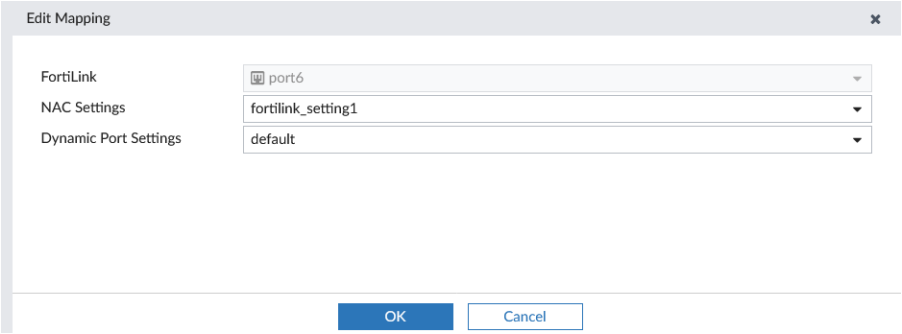
FortiLink settings

To create a new FortiLink Setting template:

1. Go to *FortiSwitch Manager* > *FortiLink Settings*, and click *Create New*.
2. Configure the details of the FortiLink Settings template including the *Name*, *NAC VLAN Segmentation*, *Primary Interface*, *Onboarding VLAN*, and *Segment VLANs*.
3. Click *OK* to save the template.



4. Go to *FortiSwitch Manager* > *FortiSwitch Profiles* > *VDOM Settings*, and edit a FortiGate's mapped FortiLink. Assign the *FortiLink Settings* template to a FortiGate in the *NAC Settings* field.



5. Install the FortiLink Settings template to FortiGate using the *Install Wizard*.

Assigning templates to FortiSwitch devices

When central management is enabled for *FortiSwitch Manager*, you can assign templates to switches. For more information about creating and managing FortiSwitch templates, see FortiSwitch Templates on page 859.

To assign a templates:

1. Go to *FortiSwitch Manager* > *Managed FortiSwitches*.
2. In the tree menu, select a FortiGate to list its managed switches, or select *Managed FortiGate* to list all switches.
   The list of managed FortiSwitch units is displayed in the content pane.
3. Use the quick status bar to filter the list of switches in the content pane and help locate the switch.
4. Select the switch, and click *Assign Template* from the toolbar.
5. Select a FortiSwitch template from the dropdown list, then click *OK* to assign it.
6. Install the changes. See Installing changes to managed switches on page 852.



Only templates that apply to the specific device model will be available for selection.



Templates can also be applied when editing a device. See Editing switches on page 843.

FortiSwitch per-device management

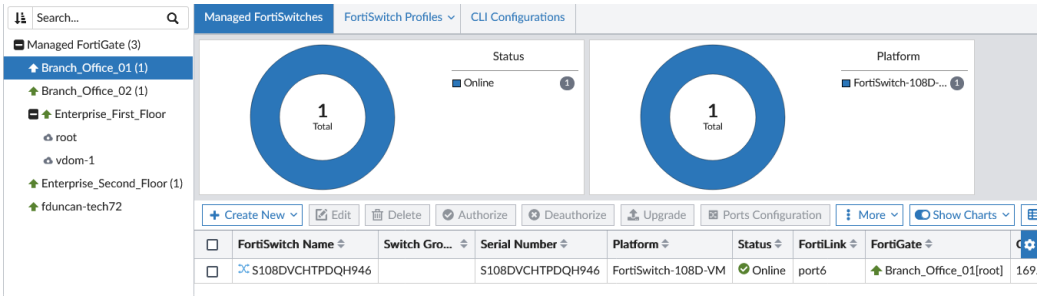
When per-device management is enabled, you can configure changes on each managed switch. The following steps provide an overview of using per-device FortiSwitch management:

1. Enable per-device management. See Enabling per-device management on page 878.
2. Configure policies and profiles for managed switches.
   You can configure VLANs, security policies, LLDP profiles, and QoS policies, and the changes are saved to the FortiGate database.
3. Configure ports for each managed switch.
   When you configure ports, you can assign the profiles and policies that you created. See Configuring a port on a single FortiSwitch on page 886.
4. Install changes to managed switches. See Installing changes to managed switches on page 852.

Enabling per-device management

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

To enable FortiSwitch per-device management:

1. Go to *System Settings* > *ADOMs*.
2. Double-click the ADOM to open it for editing.
3. Beside *Central Management*, clear the *FortiSwitch* checkbox, and click *OK*.
   Central management is disabled, and per-device management is enabled for FortiSwitch.
4. 

Creating VLANs

To create VLANs:

1. Go to *FortiSwitch Manager* > *Managed FortiSwitches*, and select *VLAN* from the tab.
2. In the tree menu, select a FortiGate.
3. Click *Create New*.
4. The *Create New VLAN Interface* pane opens.
5. Edit the options, and click *OK*.
   The changes are saved to the FortiGate database.

Creating NAC policies

To create NAC policies:

1. Go to *FortiSwitch Manager* > *Managed FortiSwitches*, and select *NAC Policy* from the tab.
2. In the tree menu, select a FortiGate.
   The NAC policies are displayed.
3. Click *Create New*.
   The *Create New NAC Policies* pane opens.
4. Set the options, and click *OK*. See Create a new NAC policy on page 496 for more information.

Creating security policies

To create security policies:

1. Go to *FortiSwitch Manager* > *Managed FortiSwitches*, and select *Security Policy* from the *Port Policies* tab.
2. In the tree menu, select a FortiGate.
   The security policies are displayed.
3. Click *Create New*.
   The *Create New Security Policies* pane opens.
4. Edit the options, and click *OK*.
   The changes are saved to the FortiGate database.

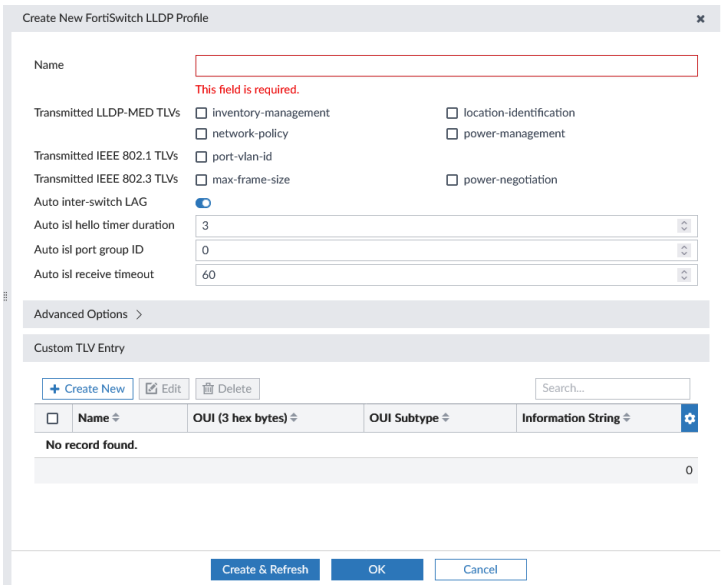
Creating LLDP profiles

To create LLDP profiles:

1. Go to *FortiSwitch Manager* > *Managed FortiSwitches*, and select *LLDP Profile* from the tab.
2. In the tree menu, select a FortiGate.
   The *VLAN* profiles are displayed.



3. Click *Create New*.
   The *Create New FortiSwitch LLDP Profiles* pane opens.



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

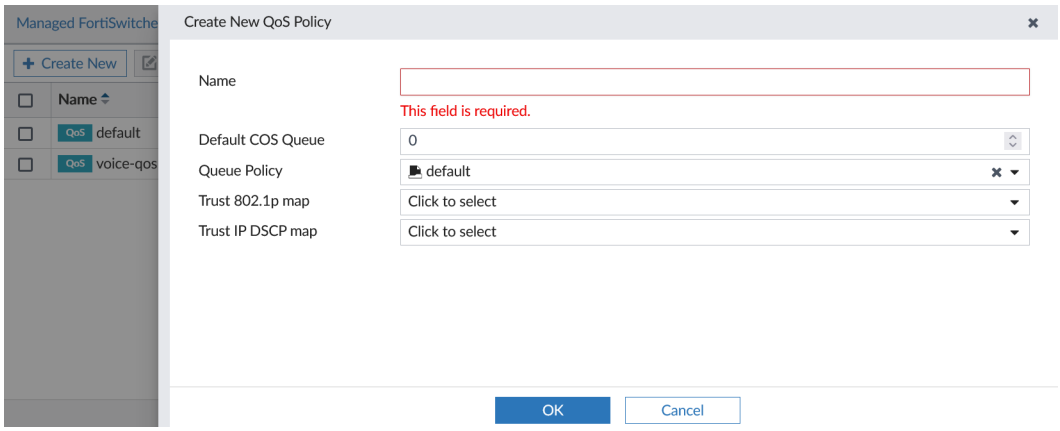
Creating QoS policies

You can set the following types of QoS policies for each managed switch:

- QoS policies
- QoS egress queue policies
- QoS IP precedence/DSCP policies
- QoS 802.1 policies

To create QoS policies:

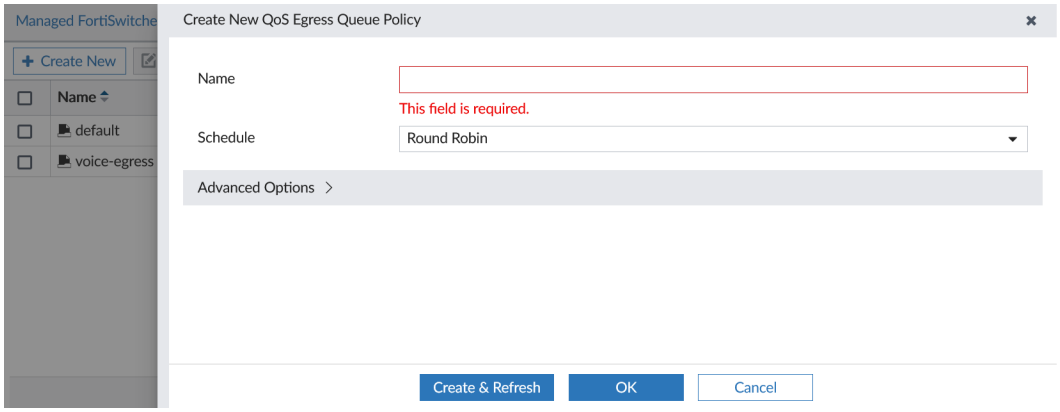
1. Go to *FortiSwitch Manager* > *Managed FortiSwitches*, and select *QoS Policies* from the *QoS* tab.
2. In the tree menu, select a FortiGate.
3. Click *Create New*.
   The *Create New QoS Policy* pane opens.



4. Set the options, and click *OK*.
   The changes are saved to the FortiGate database.

To create QoS egress queue policies:

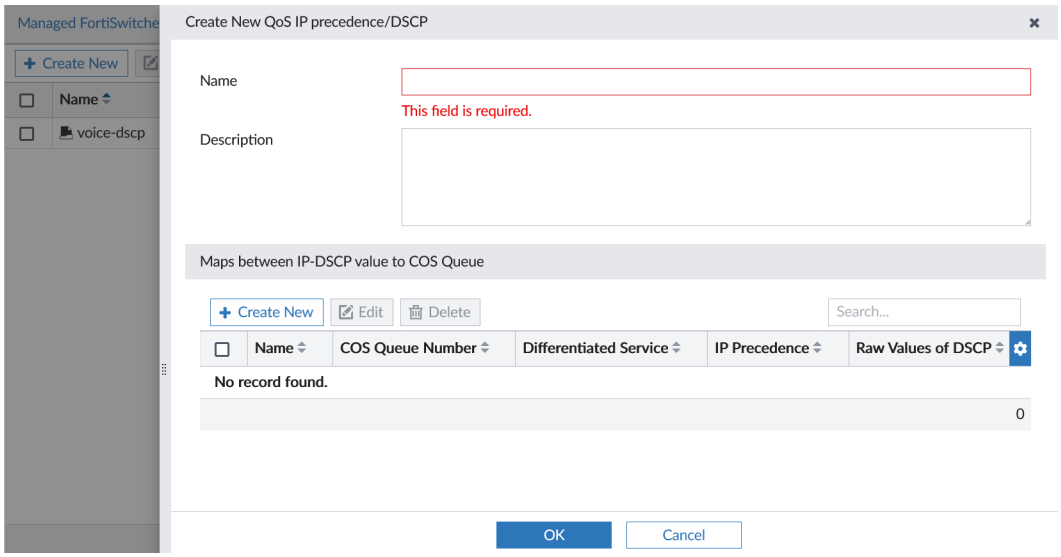
1. Go to *FortiSwitch Manager* > *Managed FortiSwitches*, and select *Egress Queue Policies* from the *QoS* tab.
2. In the tree menu, select a FortiGate.
   The QoS egress queued policies are displayed in the content pane.
3. Click *Create New*.
   The *Create New Egress Queue Policy* pane opens.



4. Set the options, and click *OK*.
   The changes are saved to the FortiGate database.

To create QoS IP precedence/DSCP policies:

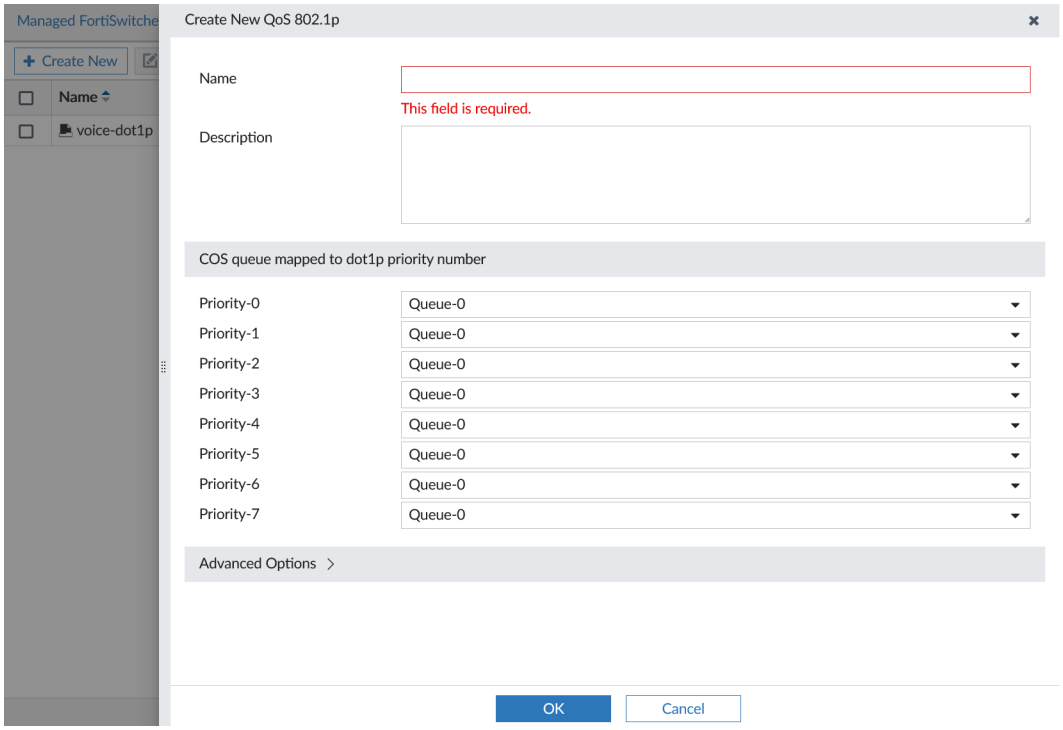
1. Go to *FortiSwitch Manager* > *Managed FortiSwitches*, and select *IP Precedence/DSCP* from the *QoS* tab.
2. In the tree menu, select a FortiGate.
   The QoS IP precedence/DSCP policies are displayed in the content pane.
3. Click *Create New*.
   The *Create New QoS IP precedence/DSCP* pane opens.



4. Set the options, and click *OK*.
   The changes are saved to the FortiGate database.

To create QoS 802.1p policies:

1. Go to *FortiSwitch Manager* > *Managed FortiSwitches*, and select *802.1P* from the *QoS* tab.
2. In the tree menu, select a FortiGate.
   The *QoS 802.1p* policies are displayed in the content pane.
3. Click *Create New*.
   The *Create New 802.1* pane opens.



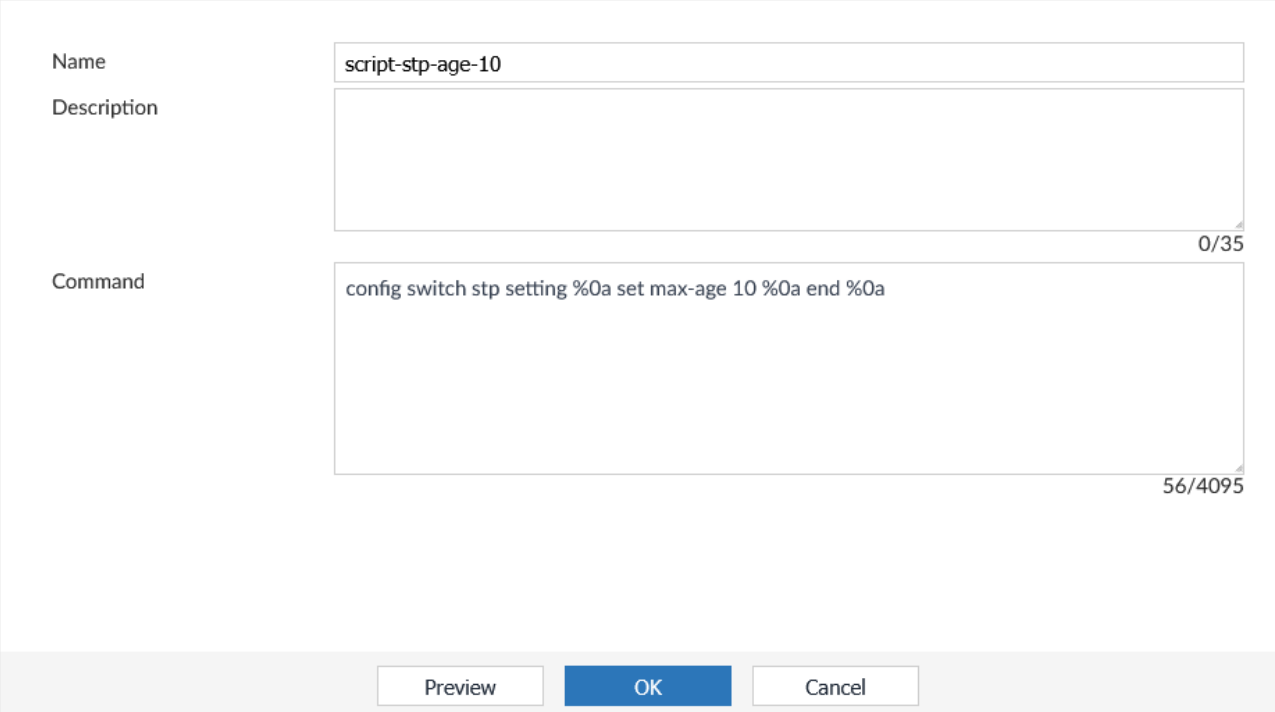
4. Set the options, and click *OK*.
   The changes are saved to the FortiGate database.

Creating custom commands

When per-device management is enabled, FortiSwitch custom commands can be created and edited in the *Custom Commands* tab. Once created, the custom command can be added to one or more managed FortiSwitch. Once selected, use the Install Wizard to deploy the changes to FortiGate.

To create a custom command:

1. Go to *FortiSwitch Manager > Managed FortiSwitches* and select the *Custom Commands* tab.
2. In the content pane, click *Create New* in the toolbar. The *Create New Custom Command* window opens.



3. Enter the following information, then click *OK* to create the new custom command.

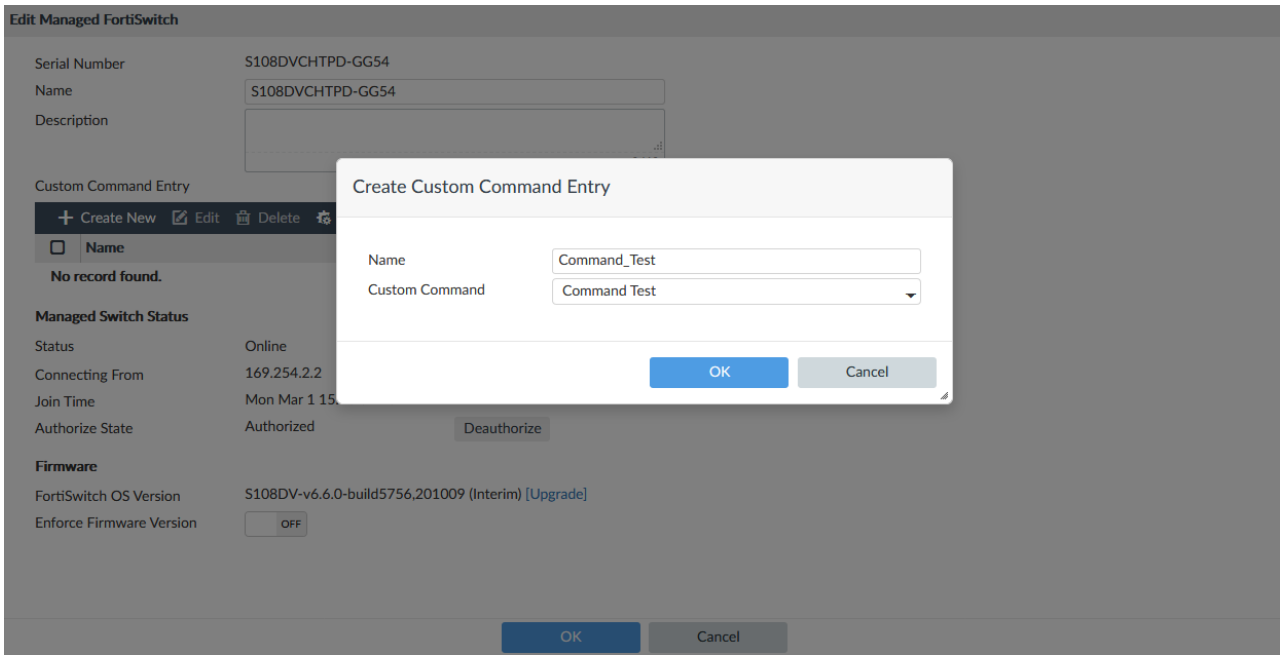
Name	Type a name for the custom command template.
Description	Optionally, type a description.
Command	Enter the CLI commands.

You can now add the custom command to one or more managed FortiSwitch device.

To add custom commands to a single FortiSwitch:

1. Go to *FortiSwitch Manager > Managed FortiSwitches* and select a FortiGate, then edit a managed FortiSwitch.
2. In the *Edit Manged FortiSwitch* pane, select *Create New* under *Custom Command Entry*.

3. Enter a name for the command entry and select your previously configured custom command. Click *OK*, and save your changes to the managed FortiSwitch.

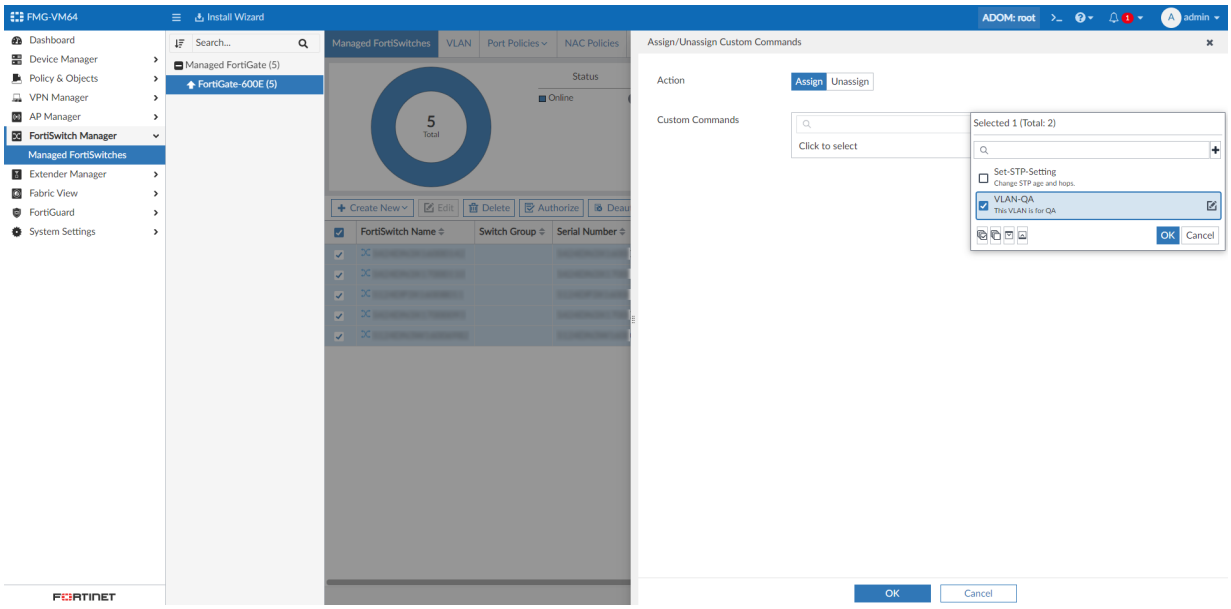


You can now install the custom command using the Install Wizard. See Installing changes to managed switches on page 852.

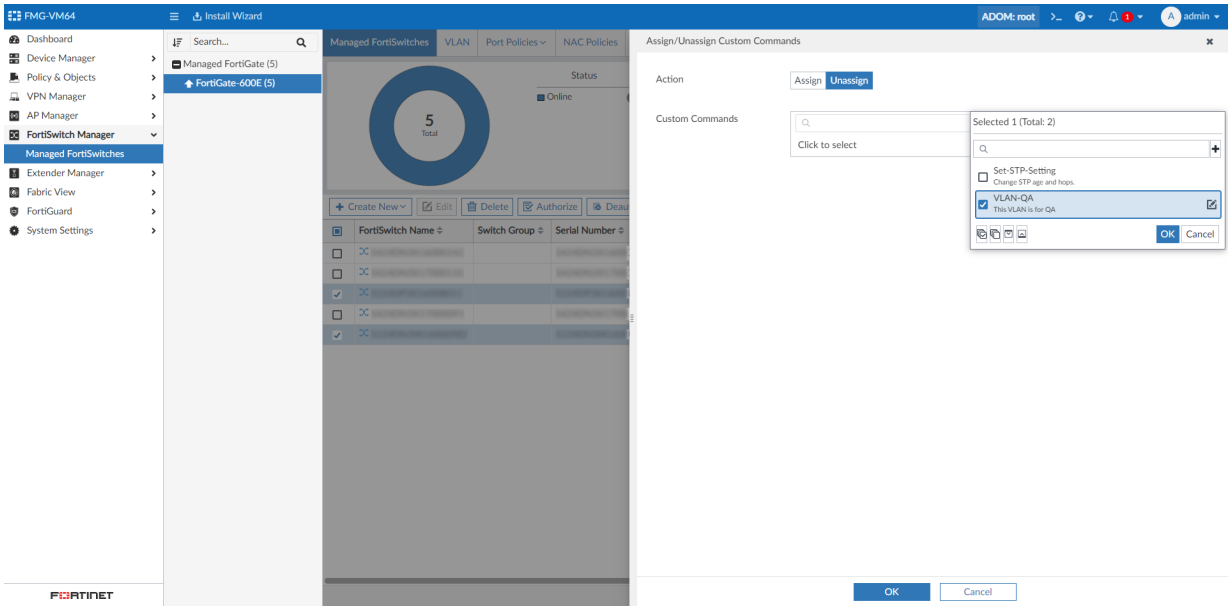
To assign or unassign custom commands on multiple FortiSwitches:

1. Go to *FortiSwitch Manager > Managed FortiSwitches* and select a FortiGate.
2. Select multiple FortiSwitch devices in the table.
3. Right-click and select *Assign/Unassign Custom Commands* from the context menu.
4. Assign custom commands:
   a. Select the *Assign* tab.
   b. In the *Custom Commands* field, select one or more commands to assign to the selected devices.

c. Click *OK*.



5. Unassign custom commands:
   a. Select the *Unassign* tab.
   a. In the *Custom Commands* field, select which commands to unassign from the selected devices.
   a. Click *OK*.



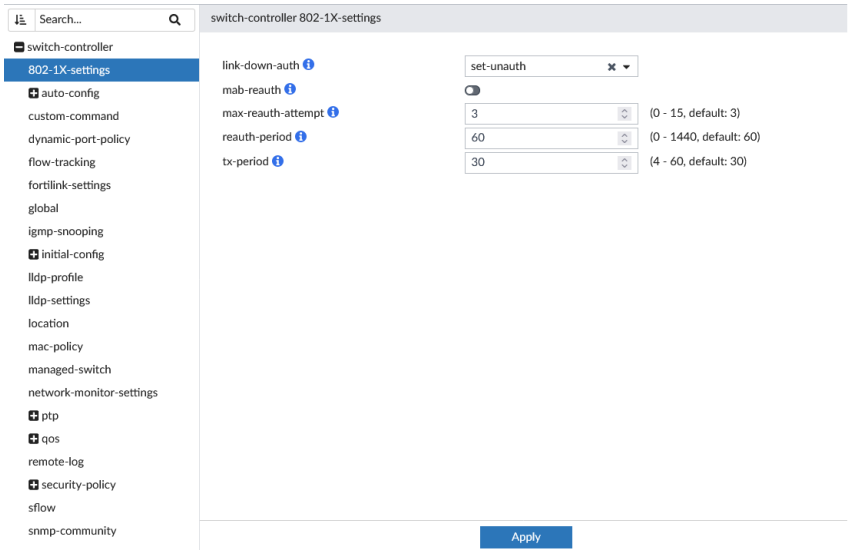
6. You can now install the changes using the Install Wizard. See Installing changes to managed switches on page 852.

CLI Configurations

You can use the CLI for per-device configuration to access settings that might not yet be available in the GUI.

To use the CLI:

1. Go to *FortiSwitch Manager* > *Managed FortiSwitches*, and select the *CLI Configurations* tab.
2. In the tree menu, select a FortiGate.
   The commands are displayed in the content pane.
3. Use the tree menu to navigate between the commands.
   The options display in the content pane.



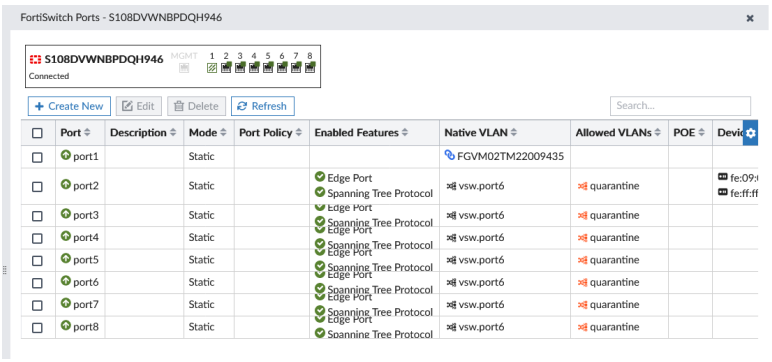
4. Set the options, and click *Apply*.
   The changes are saved to the FortiGate database.

Configuring a port on a single FortiSwitch

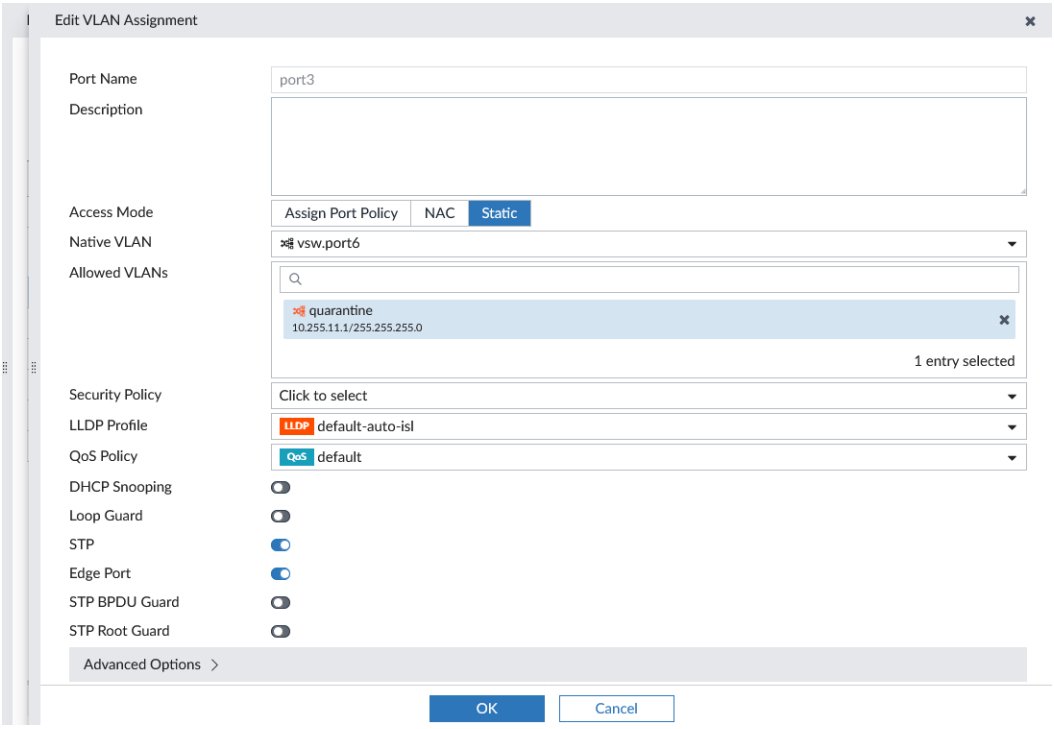
When per-device management is enabled, you can use the *FortiSwitch Manager* pane to configure ports for each managed switch.

To configure ports on a managed FortiSwitch:

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



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



5. Edit the options, and click *OK*.
   The changes are saved to the FortiGate database.

Right-click each port to modify POE, DHCP Blocking, IGMP Snooping, IGMP Snooping, STP, Loop Guard, Edge Port, STP BPDU Guard, and STP Root Guard directly from the context-menu.

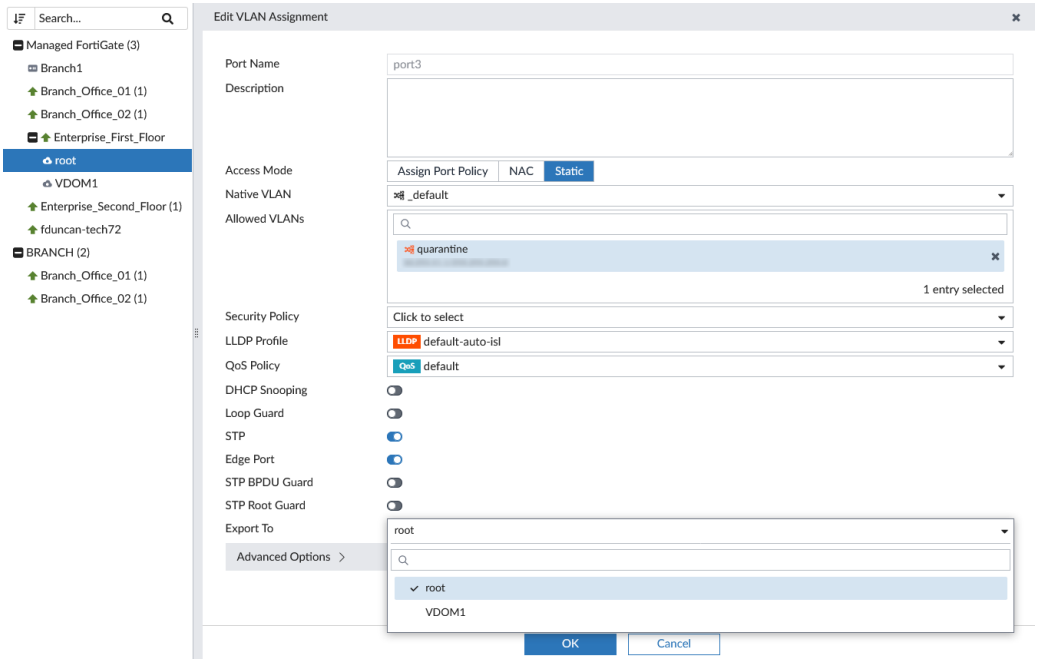
Exporting FortiSwitch ports to another VDOM

For FortiGate's with VDOM enabled, you can export FortiSwitch ports to another VDOM when operating in per-device management mode.

To export ports to another VDOM, *FortiSwitch Central Management* must be disabled in the ADOM, and a Multi-VDOM enabled FortiGate with assigned FortiSwitch must be added to FortiManager.

To export FortiSwitch ports to another VDOM:

1. Disable *FortiSwitch Central Management*. See Enabling per-device management on page 878.
2. Add a Multi-VDOM enabled FortiGate with assigned FortiSwitch to FortiManager.
3. Go to *FortiSwitch Manager > Managed FortiSwitches*, right-click on a FortiSwitch, and select *Ports Configuration*.
4. Edit a port to enter the *Edit VLAN Assignment* pane, and choose the new VDOM in the *Export To* field.



5. After the port is exported, users can edit the port's configuration in the chosen VDOM.
6. After the settings are configured, the changes can be installed to the FortiGate.

Extender Manager

The *Extender Manager* module allows you to manage connected FortiExtenders. You can use the Extender Manager to create custom templates, SIM profiles, and data plans for up to two modems.

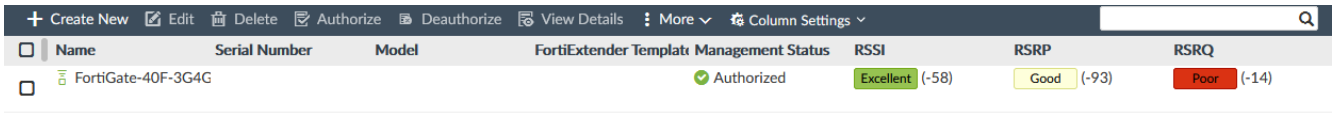
This section contains the following topics:

- Managed extenders on page 889
- Extender profiles on page 892
- Data plans on page 896

Managed extenders

Use the *Managed Extenders* pane to configure modems, associate data plans with a device, and authorize devices.

To view managed FortiExtender devices, go to *Extender Manager > Managed Extenders*.



LTE modems built into FortiGate 3G4G models will appear as managed devices in the tree menu. For example, *FortiGate-xxx-3G4G*.

To view the modem's RSSI score and connection details, select the device and click *View Details*.

The following information is displayed:

Name	The name of the FortiGate device that is managing the FortiExtender.
Serial Number	The serial number of the FortiExtender.
Model	The FortiExtender model.
FortiExtender Template	The FortiExtender template name.
Management Status	The FortiExtender management status, either *Authorized* or *Deauthorized*.
RSSI	The Received Signal Strength Indicator status, either *Excellent*, *Good*, or *Poor*.
RSRP	The Reference Signal Received Power status, either *Excellent*, *Good*, or *Poor*.

RSRQ	The Reference Signal Received Quality status, either *Excellent*, *Good*, or *Poor*.
SINR	The Signal-to-Interference-plus-Noise Ratio status, either *Excellent*, *Good*, or *Poor*.
Network	The FortiExtender network status and carrier name.
Data Usage	The current data usage.
ENSI IMEI	The FortiExtender electronic serial number (ESN) and international mobile equipment identity (IMEI).
Phone Number	The FortiExtender phone number.
IMSI	The FortiExtender international mobile subscriber identity (IMSI) number.
ICCID	The FortiExtender integrated circuit card identity (ICCID) number.
Temperature	The temperature information of FortiExtender. If temperature value is not available the value in the column will be empty.
Version	The FortiExtender firmware version.
IP	The FortiExtender IP address.

The right-click menu and toolbar options include:

Refresh	Select a FortiExtender in the list, right-click, and select *Refresh* in the menu to refresh the information displayed.
Edit	Select a FortiExtender in the list, right-click, and select *Edit* in the menu to edit the FortiExtender modem settings, PPP authentication, general, GSM/LTE, and CDMA settings.
View Details	Select a FortiExtender in the list, right-click, and select *View Details* in the menu to view the system status, modem status, and data usage.
Upgrade	Select a FortiExtender in the list, right-click, and select *Upgrade* in the menu to upgrade the FortiExtender firmware.
Authorize	Select a FortiExtender in the list, right-click, and select *Authorize* in the menu to authorize the unit for management.
Deauthorize	Select a FortiExtender in the list, right-click, and select *Deauthorize* in the menu to deauthorize the unit for management.
Restart	Select a FortiExtender in the list, right-click, and select *Restart* in the menu to restart the unit.
Export to Excel	Click to export the configuration as an Excel file.
Export to CSV	Click to export the configuration as a CSV file.

To install the configurations on a device, click *Install Wizard*.

Managing FortiExtender devices

You can use the Extender Manager to create new model devices, authorize devices, assign templates, and upgrade a device.

To create a new model device:

1. Go to *Extender Manager* > *Managed Extenders*.
2. In the toolbar, click *Create New*. The *Create New Model FortiExtender* dialog is displayed.
3. Configure the model device.

FortiGate	Click the dropdown and select a device from the list.
Serial Number	Enter the serial number for the FortiExtender.
Name	Enter the device name.
Mode	Select *LAN Extension* or *WAN Extension*.
FortiExtender Profile	Click the dropdown and select a template from the list.

4. Click *OK*.



Adding model devices using a wildcard SN

FortiExtender model devices can be added using wildcard serial numbers. The wildcard SN format is: *PREFIX************

- *PREFIX*: The first 6 digits of the device's serial number. The prefix must be valid.
- **********: The wildcard characters.

To edit a FortiExtender:

1. Go to *Extender Manager* > *Managed Extenders*.
2. In the *Managed Extenders* pane do one of the following:
   - Double-click a device to open it.
   - In the toolbar, click *Edit*.
   - Right-click a device, and select *Edit* from the menu.

   The *Edit FortiExtender* dialog is displayed.
3. Edit the device settings as required, and click OK.

To authorize a device:

1. Go to *Extender Manager* > *Managed Extenders*.
2. In the tree menu, click *Managed FortiGate*, and select a device in the list.
3. In the *Managed Extender* pane, select a device, and do one of the following.
   - In the toolbar, click *Authorize*.
   - Right-click the device, and select *Authorize* from the menu.
4. Click *OK*.

To deauthorize a device:

1. Go to *Extender Manager* > *Managed Extenders*.
2. In the tree menu, click *Managed FortiGate*, and select a device in the list.
3. In the Managed Extender pane, select a device, and do one of the following.
   - In the toolbar, click *Deauthorize*.
   - Right-click the device, and select *Deauthorize* from the menu.
4. Click *OK*.

To restart a device:

1. Go to *Extender Manager* > *Managed Extenders*.
2. In the tree menu, click *Managed FortiGate*, and select a device in the list.
3. In the *Managed Extender* pane, select a device, and do one of the following.
   - In the toolbar, click *Restart*.
   - Right-click the device, and select *Restart* from the menu.

   The *Execute Extender Action* dialog is displayed.
4. Click *OK*.

To upgrade a device:

1. Go to *Extender Manager* > *Managed Extenders*.
2. In the tree menu, click *Managed FortiGate*, and select a device from the list.
3. In the *Managed Extender* pane, select a device and do one of the following.
   - In the toolbar, click *Upgrade*.
   - Right-click the device, and select *Upgrade* from the menu.

   The *Upgrade Firmware* dialog is displayed.
4. Select the firmware and click *Upgrade Now*. The status bar is displayed.
5. Click *Close*.

Extender profiles

Extender Manager profiles allow you to configure a FortiExtender device settings remotely. To configure the device settings, create a SIM profile and dataplan and then assign them to a profile template. After the template is configured, you can assign it to a device.

This section contains the following topics:

- FortiExtender profiles on page 893
- Using Fortinet recommended extender profiles on page 894

FortiExtender profiles

You can create custom FortiExtender profiles, assign a profile to a device, and view where a profile is used.

To create a FortiExtender profile:

1. Go to *FortiExtender > Extender Profiles > FortiExtender Profile*.
2. In the toolbar click *Create New*. The *Create New FortiExtender Profile* page opens.
3. Configure the profile settings.

Name	Enter a name for the profile.	
Description	(Optional) Enter a description of the profile.	
Modem (1 & 2)	**Normalized Interface**	Select an interface from the dropdown list.
	SIM Profile	Select a profile from the dropdown list, or click *Add* to create new profile.
Dataplan	Select a dataplan from the list, or click *Add* to create new dataplan, and click *OK*.	

4. Under Modem 1, configure the details for the SIM.

Default SIM	Select the default SIM.
SIM1 PIN	Toggle ON to provide a PIN for SIM1.
SIM2 PIN	Toggle ON to provide a PIN for SIM2.
GPS	Toggle ON to enable GPS.
Advanced Options	View advanced options.

5. Configure the remaining settings as needed, and click *OK*.

To edit a FortiExtender profile:

1. In the tree menu, select a profile and do one of the following:
   - Double-click the profile to open it.
   - In the toolbar, click *Edit*.
   - Right-click the profile , and select *Edit* from the menu.

   The *Edit FortiExtender Profile* window opens.
2. Edit the profile details, and click *OK*.

To clone a FortiExtender profile:

1. Go to *FortiExtender > Extender Profiles > FortiExtender Profile*.
2. Select a profile.
3. In the toolbar, click *Clone*, or right-click the profile and select *Clone* from the menu. The *Clone FortiExtender Profile* window opens.

4. Edit the profile *Name* and settings as required.
5. Click *OK*.

To assign a FortiExtender profile to a device:

1. Go to *FortiExtender* > *Extender Profiles* > *FortiExtender Profile*.
2. Select a profile.
3. In the toolbar, click *Assign to Device*, or right-click the profile and select *Assign to Device* from the menu. The *Assign to Device* window opens.
4. Click the *FortiExtenders* field, and select a device(s) from the list.
5. Click *OK*.

To view where a FortiExtender profile is used:

1. Go to *FortiExtender* > *Extender Profiles* > *FortiExtender Profile*.
2. Select a profile.
3. In the toolbar, click *Where Used*, or right-click the profile and select *Where Used* from the menu. The *Where <profile_name> is used* window opens.
4. (Optional) Click *Edit* to edit the device.
5. (Optional) Click *View*, to view the device.
6. Click *Close*.

To import a FortiExtender profile:

1. Go to *FortiExtender* > *Extender Profiles* > *FortiExtender Profile*.
2. In the toolbar, click *Import*. The *Import FortiExtender Profile* window opens.
3. Configure the profile settings.

Devices	Select a device from the dropdown list.
Profile on Device	Choose a profile from the selected device.
New Profile Name	Enter a name for the new profile.

4. Click *OK*.

To delete a FortiExtender profile:

1. Go to *FortiExtender* > *Extender Profiles* > *FortiExtender Profile*.
2. Select a profile.
3. In the toolbar click *Delete*, or right-click the profile and select *Delete* from the menu. The *Confirm Delete* window opens.
4. Click *OK*.

Using Fortinet recommended extender profiles

FortiManager includes factory default extender profiles recommended by Fortinet.

The Fortinet recommended profiles are based on Fortinet security best practices, and they are created based on the most relevant network topologies Fortinet sees with customer implementation. The configuration is validated by Fortinet field engineers and security experts.

The following Fortinet recommended extender profile is available:

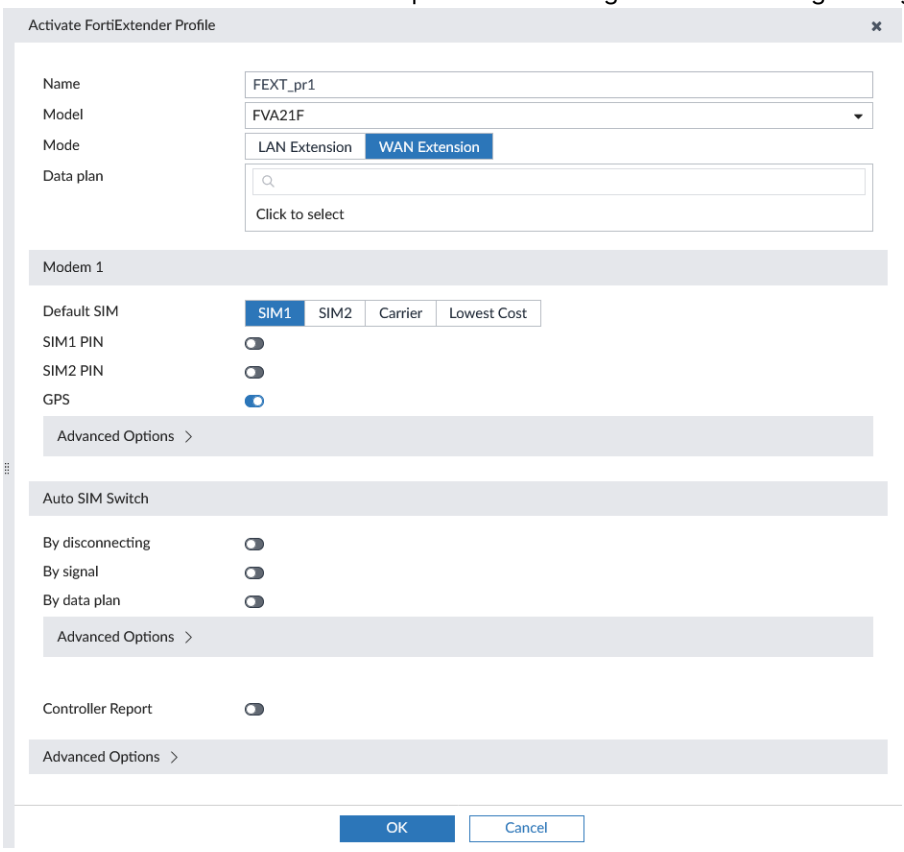
- *Fortinet_Default_FEXT_Profile*

You can use recommended profiles by activating them from the *Extender Manager > Extender Profiles* menu in FortiManager and then configuring them to meet your requirements.

To use Fortinet recommended extender profiles:

To use recommended FortiExtender templates:

1. The recommended Extender Profile is shown in *Extender Manager > Extender Profiles* on the *FortiExtender Profile* tab.
2. An extender profile can be created by activating the recommended FortiExtender profile.
   a. Right-click on the recommended FortiExtender profile and click *Activate*.
   b. Choose a model for the template.
   c. Enter a name for the FortiExtender profile and configure the remaining settings as needed.



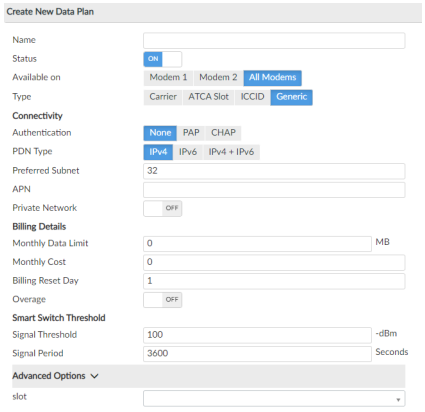
3. The created extender profile can be assigned to an extender, then the user can deploy the settings.
   a. Right-click on a managed FortiExtender and click *Assign Profiles*.
   b. Select the configured FortiExtender Profile, and click *OK*.

Data plans

The *Data Plan* pane allows you to create a new data plan profile and view where is plan is used.

To create a data plan:

1. Go to *Extender Manager* > *Data Plans*.
2. In the toolbar, click *Create New*. The *Create New Data Plan* dialog is displayed.
3. Enter a name and ensure the *Status* is enabled.
4. Configure the data plan settings.
   a. In the Name field, enter a name for the profile.
   b. For *Available on*, select a criterion (*Modem 1*, *Modem 2*, or *All Modems*).
   c. For *Type* select a criterion (*Carrier*, *ATCA Slot*, *ICCID*, or *Generic*).
   d. Configure the other settings as needed (*Connectivity*, *Billing Details*, and *Smart Switch Threshold*.

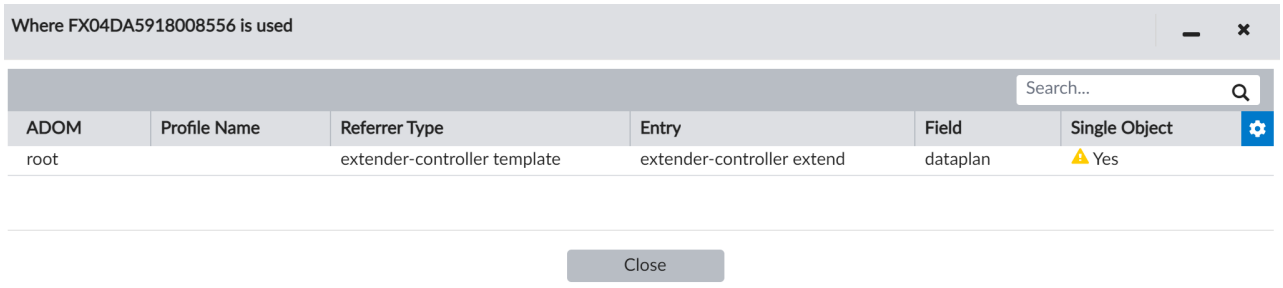


5. Click *OK*.

To install the data plan on a device, click *Install Wizard*.

To view where a data plan is used:

1. Go to *Extender Manager* > *Data Plans*.
2. Select a data plan in the list, and click *Where Used*. The *Where <data_plan_name> is used* window displays.



3. Click *Close*.

To clone a data plan:

1. Go to *Extender Manager* > *Data Plans*.
2. In the toolbar, click *Clone*, or right-click a profile and select *Clone* from the menu. The *Clone Data Plan* window opens.
3. Edit the Data Plan name and other settings as required.
4. Click *OK*.

To delete a data plan:

1. Go to *Extender Manager* > *Data Plans*.
2. In the toolbar, click *Delete*, or right-click a profile and select *Delete* from the menu. The *Confirm Deletion* dialog is displayed.
3. Click *OK*.

FortiExtender SSIDs

You can create, edit, clone, and delete FortiExtender SSIDs.

FortiExtender SSIDs are supported on supported FortiExtender models when used as a FortiGate LAN extension. This allows wireless clients behind a managed FortiExtender to access the internet, even when the FortiGate is in LAN extension mode.

FortiExtender SSIDs must be applied to a FortiExtender LAN extension profile to take affect.

See the FortiExtender documentation for more information.

To create a FortiExtender SSID:

1. Go to *Extender Manager* > *SSIDs*.
2. Click *Create New*.
3. Configure the following information:

Name	Enter a name for your SSID plan.
Type	Select a type from one of the following: • **Local SSID**: The SSIDs to be used by FortiExtender's local network. Connected devices may access the local network or internet, which are directly controlled by FortiExtender's firewall policies. Each radio can manage up to three local SSIDs simultaneously. • **LAN extension SSID**: The SSID to be used by the LAN extension network. All device traffic via this SSID will follow the IPsec tunnel to the FortiExtender's LAN extension controller FortiGate.
SSID	Enter an SSID name to be broadcasted.
Security	Configure security settings.

Security	Select a security type. • Open • WPA2-Personal • WPA-WPA2-Personal • WPA3-SAE • WPA3-SAE-Transition • WPA2-Enterprise • WPA3-Enterprise-only • WPA3-Enterprise-transition • WPA3-Enterprise-192-bit
Passphrase	Enter a password for the SSID.
Access Control	Configure access control settings.
Client Limit	Set the maximum number of clients that are allowed to connect to this SSID.
Broadcast SSID	Select if you want to broadcast the SSID.
IP/Netmask	For Local SSIDs only. Enter the FortiExtender IP address.
Address Range	For Local SSIDs only. Enter the FortiExtender IP address range.
Administrative Access	For Local SSIDs only. Select which types of administrative access you want to allow for the FortiExtender.
Advanced Options	(Optional) Configure advanced options.

4. Click *OK*.

To apply the FortiExtender SSID to a FortiExtender profile:

1. Go to *Extender Manager > Extender Profiles* and select or create a supported FortiExtender profile.
2. Ensure the profile *Mode* is set to *LAN Extension* and select a *Model* that supports WiFi.
3. In the *WiFi* section, configure the following:
   a. Select the radio band you want to use, *2.4 GHz WiFi Radio* or *5 GHz WiFi Radio*, and set the *Status* to *Enable*.
   b. In *LAN Extension SSID*, select a *LAN* type SSID.
   c. In *Local SSID*, select a *Local* type SSID.
4. When you are finished, click *OK*.

To edit a FortiExtender SSID:

1. Select the SSID and click *Edit* or *Edit in CLI*.
2. Edit the settings as required. The *Name* and *Type* cannot be edited.
3. Click *OK* to apply your changes.

To delete FortiExtender SSIDs:

1. Select the SSIDs to delete.
2. In the toolbar click *Delete*, or right-click and select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the selected SSIDs.

To clone an FortiExtender SSID:

1. Select an SSID.
2. In the toolbar click *Clone*, or right-click the SSID, and select *Clone*. The *Clone SSID* dialog box opens.
3. Edit the settings as required.
4. Click *OK*.

System Settings

System Settings allows you to manage system options for your FortiManager device.



Additional configuration options and short-cuts are available using the right-click menu. Right-click the mouse on different navigation panes on the GUI page to access these options.

This section contains the following topics:

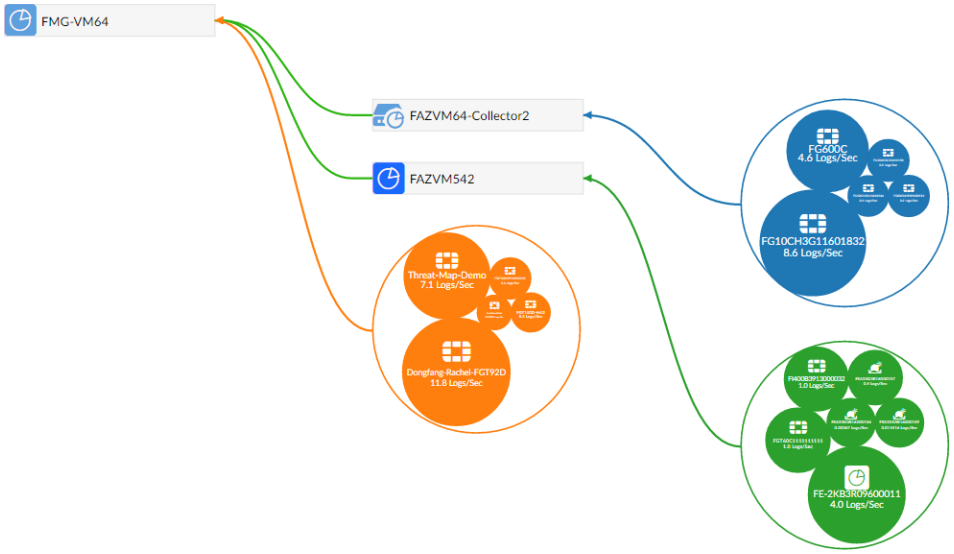
- Logging Topology on page 900
- Network on page 901
- RAID Management on page 918
- Administrative Domains (ADOMs) on page 924
- Certificates on page 955
- Event Log on page 961
- Task Monitor on page 963
- Mail Server on page 964
- Syslog Server on page 966
- Meta Fields on page 967
- Device logs on page 969
- Miscellaneous Settings on page 973

Logging Topology

The *System Settings* > *Advanced* > *Logging Topology* pane shows the physical topology of devices in the Security Fabric. Click, hold, and drag to adjust the view in the content pane, and double-click or use the scroll wheel to change the zoom.

The visualization can be filtered to show only FortiAnalyzer devices or all devices by device count or traffic.

Hovering the cursor over a device in the visualization will show information about the device, such as the IP address and device name. Right-click on a device and select *View Related Logs* to go to the *Log View* pane, filtered for that device.



This pane is only available when the FortiAnalyzer features are manually enabled. For more information, see FortiAnalyzer Features on page 41.

Network

The network settings are used to configure ports for the FortiManager unit. You should also specify what port and methods that an administrators can use to access the FortiManager unit. If required, static routes can be configured.

The default port for FortiManager units is port 1. It can be used to configure one IP address for the FortiManager unit, or multiple ports can be configured with multiple IP addresses for improved security.

You can configure administrative access in IPv4 or IPv6 and include settings for HTTPS, HTTP, PING, SSH, SNMP, and Web Service.

FortiManager supports SSHv2.

You can prevent unauthorized access to the GUI by creating administrator accounts with trusted hosts. With trusted hosts configured, the administrator can only log in to the GUI when working on a computer with the trusted host as defined in the administrator account. For more information, see Trusted hosts on page 976 and Managing administrator accounts on page 977.

Configuring network interfaces

Fortinet devices can be connected to any of the FortiManager unit's interfaces. The DNS servers must be on the networks to which the FortiManager unit connects, and should have two different IP addresses.

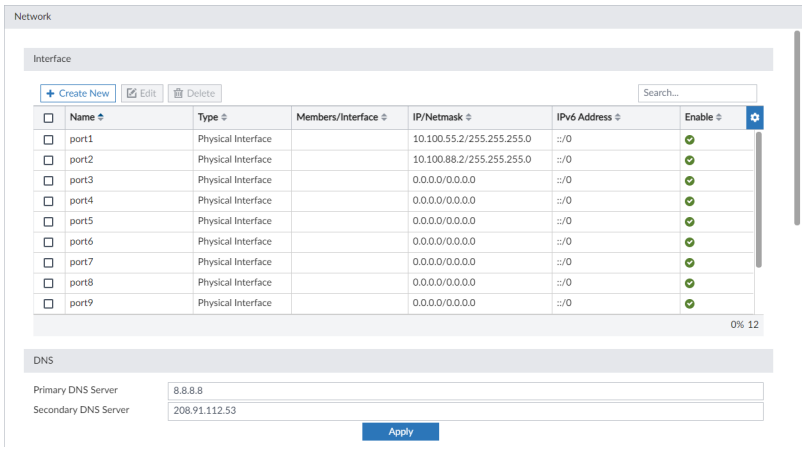
If the FortiManager unit is operating as part of an HA cluster, it is recommended to configure interfaces dedicated for the HA connection / synchronization. However, it is possible to use the same interfaces for both HA and device management. The HA interface will have */HA* appended to its name.

The following port configuration is recommended:

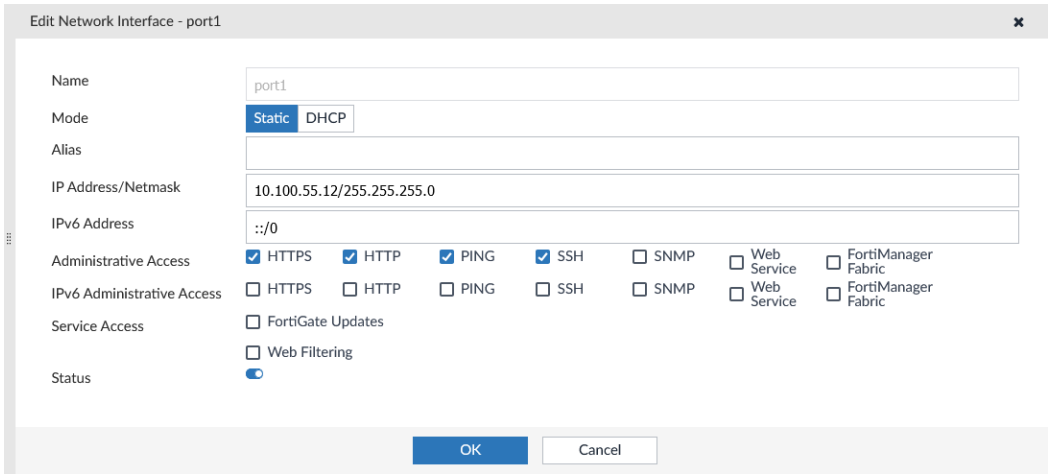
- Use port 1 for device log traffic, and disable unneeded services on it, such as SSH, Web Service, and so on.
- Use a second port for administrator access, and enable HTTPS, Web Service, and SSH for this port. Leave other services disabled.

To configure port 1:

1. Go to *System Settings* > *Network*.The *Interface* pane is displayed at the top of the page.



2. In the *Interface* pane, double-click *Port1*. The *Edit System Interface* pane is displayed.



3. Configure the following settings for *port1*, then click *OK* to apply your changes.

Name	Displays the name of the interface.

IP Address/Netmask	The IP address and netmask associated with this interface.
IPv6 Address	The IPv6 address associated with this interface.
Administrative Access	Select the allowed administrative service protocols from: HTTPS, HTTP, PING, SSH, SNMP, Web Service, and FortiManager Fabric.
IPv6 Administrative Access	Select the allowed IPv6 administrative service protocols from: HTTPS, HTTP, PING, SSH, SNMP, Web Service, and FortiManager Fabric.
Service Access	Select the Fortinet services that are allowed access on this interface. These include *FortiGate Updates* and *Web Filtering*. Service access is not enabled on any port by default. Specify the *Bind to IP Address:* • The IP address specified in *Bind to IP Address* address should be a unique address on the same subnet as the IP address of the interface. This IP address is used for update and rating requests to FortiManager over TCP/443. • FortiManager can only configure one interface with update and rating service using port 443.  When configuring FortiManager as a local FortiGuard server for FortiGate, you must use the *Bind to IP* addresses for the update and rating services over TCP/443. The *Bind to IP address* does not need to be configured for update services if the default port was not changed to TCP/443. See the FortiGate Admin Guide for more information.
Status	Select *Enable* or *Disable*.

4. Configure the DNS settings, and click *Apply*.

Primary DNS Server	The primary DNS server IP address.
Secondary DNS Server	The secondary DNS server IP address.

To configure additional ports:

1. Go to *System Settings* > *Network*. The *Interface* pane is displayed at the top of the page.
2. In the *Interface* pane, double-click on a port, right-click on a port then select *Edit* from the pop-up menu, or select a port then click *Edit* in the toolbar. The *Edit System Interface* pane is displayed.
3. Configure the settings as required.
4. Click *OK* to apply your changes.



The port name, default gateway, and DNS servers cannot be changed from the *Edit System Interface* pane. The port can be given an alias if needed.

Disabling ports

Ports can be disabled to prevent them from accepting network traffic

To disable a port:

1. Go to *System Settings* > *Network*. The *Interface* list is displayed.
2. Double-click on a port, right-click on a port then select *Edit* from the pop-up menu, or select a port then click *Edit* in the toolbar. The *Edit System Interface* pane is displayed.
3. In the *Status* field, click *Disable*
4. Click *OK* to disable the port.

Changing administrative access

Administrative access defines the protocols that can be used to connect to the FortiManager through an interface. The available options are: HTTPS, HTTP, PING, SSH, SNMP, Web Service, and FortiManager Fabric.

To change administrative access:

1. Go to *System Settings* > *Network* and click *All Interfaces*. The interface list opens.
2. Double-click on a port, right-click on a port then select *Edit* from the pop-up menu, or select a port then click *Edit* in the toolbar. The *Edit System Interface* pane is displayed.
3. Select one or more access protocols for the interface for *Administrative Access* and *IPv6 Administrator Access*, as required.
4. Click *OK* to apply your changes.

The following access protocols are available on FortiManager:

Protocol	Description when access is enabled
HTTPS `https`	Allows secure HTTPS connections to the FortiManager GUI through this interface.
HTTP `http`	Allows HTTP connections to the FortiManager GUI through this interface.
PING `ping`	The interface responds to pings. Use this setting to verify your installation and for testing.
SSH `ssh`	Allows SSH access through the interface.
SNMP `snmp`	Allows a remote SNMP manager to request SNMP information by connecting to this interface.
Web Service `webservice`	Allows FortiManager to be accessed by the XML API through the interface. The FortiManager XML API can be used to retrieve information about managed devices and perform actions such as modifying device configurations using the API.

Static routes

Static routes can be managed from the routing tables for IPv4 and IPv6 routes. The routing tables can be accessed by going to *System Settings* > *Network*.

To add a static route:

1. From the network routing table, click *Create New* in the toolbar. The *Create New Network Route* pane opens.
2. Select the *IP Type* as either IPv4 or IPv6.
3. Enter the destination IP address and netmask, or IPv6 prefix, and gateway in the requisite fields.
4. Select the network interface that connects to the gateway from the dropdown list. Ports, aggregate links, and VLANs are available.
5. Click *OK* to create the new static route.

To edit a static route:

1. From the network routing table: double-click on a route, right-click on a route then select *Edit* from the pop-up menu, or select a route then click *Edit* in the toolbar. The *Edit Network Route* pane opens.
2. Edit the configuration as required. The route ID cannot be changed.
3. Click *OK* to apply your changes.

To delete a static route or routes:

1. From the newtork routing table, right-click on a route then select *Delete* from the pop-up menu, or select a route or routes then click *Delete* in the toolbar.
2. Click *OK* in the confirmation dialog box to delete the selected route or routes.

Packet capture

Packets can be captured on configured interfaces by going to *System* > *Network* > *Packet Capture*.

The following information is available:

Interface	The name of the configured interface for which packets can be captured. For information on configuring an interface, see Configuring network interfaces on page 902.
Filter Criteria	The values used to filter the packet.
# Packets	The number of packets.
Maximum Packet Count	The maximum number of packets that can be captured on a sniffer.
Progress	The status of the packet capture process.
Actions	Allows you to start and stop the capturing process, and download the most recently captured packets.

To start capturing packets on an interface, select the *Start capturing* button in the *Actions* column for that interface. The *Progress* column changes to *Running*, and the *Stop capturing* and *Download* buttons become available in the *Actions* column.

To add a packet sniffer:

1. From the *Packet Capture* table, click *Create New* in the toolbar. The *Create New Sniffer* pane opens.
2. Configure the following options:

Interface	The interface name (non-changeable).
Max. Packets to Save	Enter the maximum number of packets to capture, between 1-10000. The default is 4000 packets.
Include IPv6 Packets	Select to include IPv6 packets when capturing packets.
Include Non-IP Packets	Select to include non-IP packets when capturing packets.
Enable Filters	You can filter the packet by *Host(s)*, *Port(s)*, *VLAN(s)*, and *Protocol*.

3. Click *OK*.

To download captured packets:

1. In the *Actions* column, click the *Download* button for the interface whose captured packets you want to download.
   If no packets have been captured for that interface, click the *Start capturing* button.
2. When prompted, save the packet file (*sniffer_[interface].pcap*) to your management computer.
   The file can then be opened using packet analyzer software.

To edit a packet sniffer:

1. From the *Packet Capture* table, click *Edit* in the toolbar. The *Edit Sniffer* pane opens.
2. Configure the packet sniffer options
3. Click *OK*.

Aggregate links

Link aggregation enables you to bind two or more physical interfaces together to form an aggregated (combined) link. This new link has the bandwidth of all the links combined. If a link in the group fails, traffic is transferred automatically to the remaining interfaces.

To configure aggregate links:

1. Go to *System Settings* > *Network*.
2. In the *Interface* toolbar, click *Create New*. The *Create New Interface* page is displayed.
3. In the *Name* field, enter a name for the interface.
4. In the *Type* field, select *Aggregate*.

5. In the *Members* field, select the ports you want to include in the aggregate.
6. In the *IP Addess/Netmask* field, enter the IP address for the aggregate link.
7. In the *Administrative Access* field, select the access protocol.
8. In the *IPv6 Administrative Access* area, select the access protocol.
9. Set the *LACP Speed* to *Slow* or *Fast*.
10. In the *Minimum Links Up* field, enter the number of aggregated ports that must be up.



You must enter a minimum value of *2* for the aggregate links to work.

11. Set *Minimum Links Down* to *Operational* or *Administrative*.
12. In the *Links up Delay*, set the number of milliseconds to wait before considering the link is up.
13. Click *OK*.

To enable the interface with the GUI:

1. Go to *System Settings* > *Network*.
2. In the *Interface* pane, double-click the aggregate interface to edit it. The *Edit System Interface* window opens.
3. Set the *Status* to *Enable*.

To enable the interface with the CLI:

```
# config system interface
(interface)# edit Aggregation1
(Aggregation1)# set status up
(Aggregation1)# end
```

VLAN interfaces

You can configure a VLAN interface in FortiManager by going to *System Settings* > *Network*.

To configure a VLAN interface:

1. Go to *System Settings* > *Network*.
2. In the *Interface* toolbar, click *Create New*. The *Create New Network Interface* page is displayed.
3. In the *Name* field, enter a name for the VLAN.
4. In the *Type* field, select *VLAN*.
5. In the *VLAN ID* field, enter a VLAN ID. You can use a range between 1 and 4094.
6. In the *Interface* field, select the interface to which the VLAN will be bound.
7. In the *Protocol* field, select either *IEEE 802.1Q*. or *IEEE 802.1AD*.
8. In the *IP Address/Netmask* field, enter the IP address for the VLAN.
9. Optionally, add an *IPv6 Address*.
10. In the *Administrative Access* field, select the access protocol.

11. Optionally, configure the *IPv6 Administrative Access*.
12. In the *Service Access* field, select which services can be accessed in this VLAN.
13. In the *Status* field, select the VLAN status.
14. Click *OK*.
15. If required, you can create a static route with the VLAN interface. See Static routes on page 905.

SNMP

Enable the SNMP agent on the FortiManager device so it can send traps to and receive queries from the computer that is designated as its SNMP manager. This allows for monitoring the FortiManager with an SNMP manager.

SNMP has two parts - the SNMP agent that is sending traps, and the SNMP manager that monitors those traps. The SNMP communities on monitored FortiGate devices are hard coded and configured by the FortiManager system - they are not user configurable.

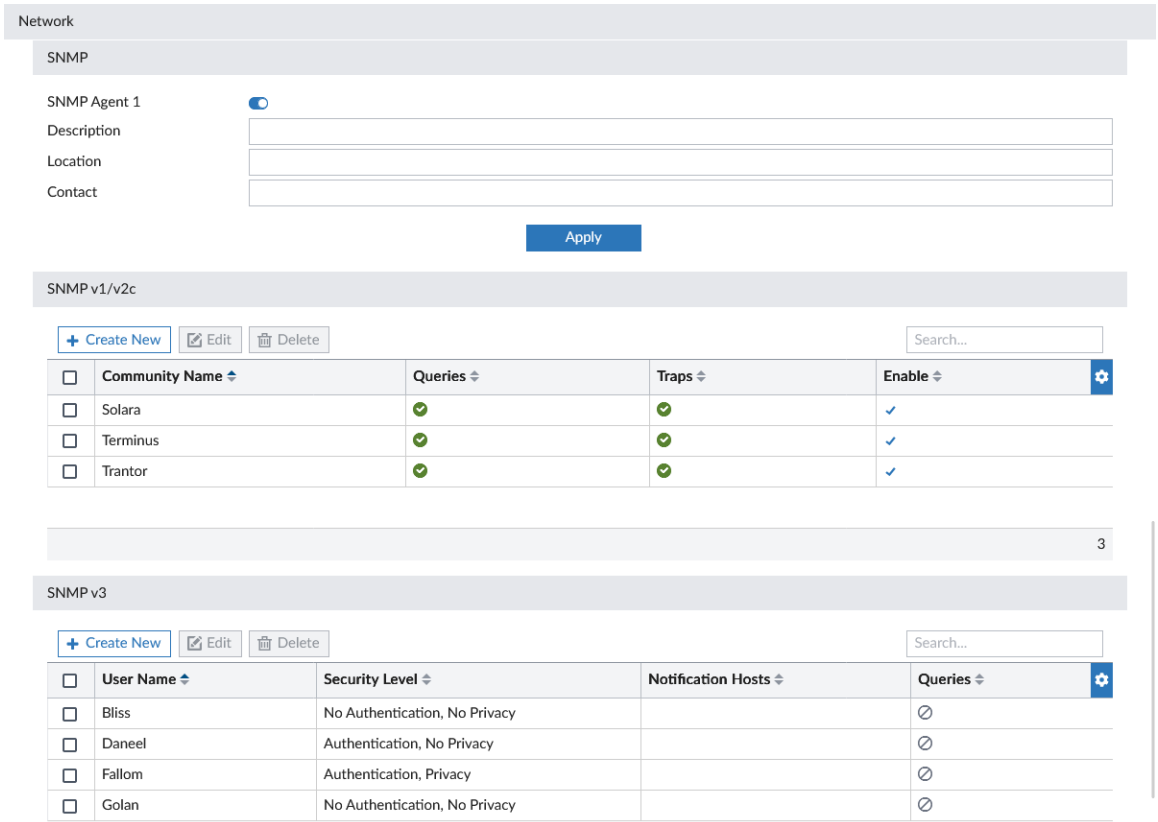
The FortiManager SNMP implementation is read-only — SNMP v1, v2c, and v3 compliant SNMP manager applications, such as those on your local computer, have read-only access to FortiManager system information and can receive FortiManager system traps.

SNMP agent

The SNMP agent sends SNMP traps originating on the FortiManager system to an external monitoring SNMP manager defined in a SNMP community. Typically an SNMP manager is an application on a local computer that can read the SNMP traps and generate reports or graphs from them.

The SNMP manager can monitor the FortiManager system to determine if it is operating properly, or if there are any critical events occurring. The description, location, and contact information for this FortiManager system will be part of the information an SNMP manager will have — this information is useful if the SNMP manager is monitoring many devices, and it will enable faster responses when the FortiManager system requires attention.

Go to *System Settings* > *Network* and scroll to the *SNMP* section to configure the SNMP agent.



The following information and options are available:

SNMP Agent	Select to enable the SNMP agent. When this is enabled, it sends FortiManager SNMP traps.
Description	Optionally, type a description of this FortiManager system to help uniquely identify this unit.
Location	Optionally, type the location of this FortiManager system to help find it in the event it requires attention.
Contact	Optionally, type the contact information for the person in charge of this FortiManager system.
SNMP v1/2c	The list of SNMP v1/v2c communities added to the FortiManager configuration.
Create New	Select *Create New* to add a new SNMP community. If SNMP agent is not selected, this control will not be visible. For more information, see SNMP v1/v2c communities on page 910.
Edit	Edit the selected SNMP community.
Delete	Delete the selected SNMP community or communities.
Community Name	The name of the SNMP community.

	Queries	The status of SNMP queries for each SNMP community. The enabled icon indicates that at least one query is enabled. The disabled icon indicates that all queries are disabled.
	Traps	The status of SNMP traps for each SNMP community. The enabled icon indicates that at least one trap is enabled. The disabled icon indicates that all traps are disabled.
	Enable	Enable or disable the SNMP community.
SNMP v3		The list of SNMPv3 users added to the configuration.
	Create New	Select *Create New* to add a new SNMP user. If SNMP agent is not selected, this control will not be visible. For more information, see SNMP v3 users on page 913.
	Edit	Edit the selected SNMP user.
	Delete	Delete the selected SNMP user or users.
	User Name	The user name for the SNMPv3 user.
	Security Level	The security level assigned to the SNMPv3 user.
	Notification Hosts	The notification host or hosts assigned to the SNMPv3 user.
	Queries	The status of SNMP queries for each SNMP user. The enabled icon indicates queries are enabled. The disabled icon indicates they are disabled.

SNMP v1/v2c communities

An SNMP community is a grouping of equipment for network administration purposes. You must configure your FortiManager to belong to at least one SNMP community so that community's SNMP managers can query the FortiManager system information and receive SNMP traps from it.



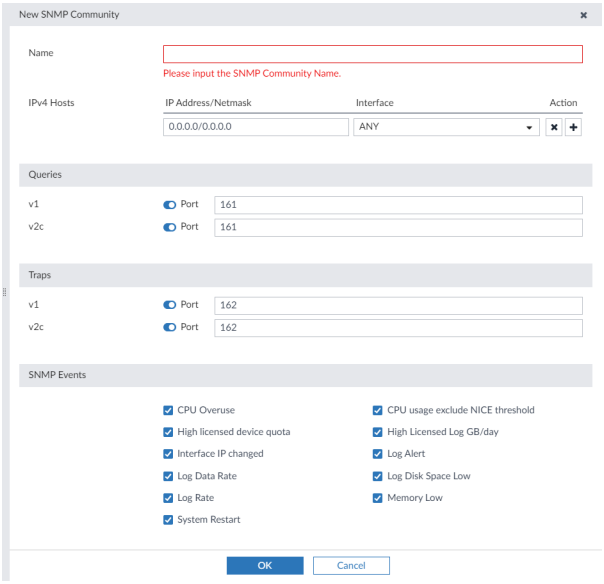
These SNMP communities do not refer to the FortiGate devices the FortiManager system is managing.

Each community can have a different configuration for SNMP traps and can be configured to monitor different events. You can add the IP addresses of up to eight hosts to each community. Hosts can receive SNMP device traps and information.

To create a new SNMP community:

1. Go to *System Settings* > *Network*.
2. In the *SNMP* section, ensure the SNMP agent is enabled.

3. In the *SNMP v1/v2c* section, click *Create New* in the toolbar. The *New SNMP Community* pane opens.



4. Configure the following options, then click *OK* to create the community.

Name		Enter a name to identify the SNMP community. This name cannot be edited later.
Hosts		The list of hosts that can use the settings in this SNMP community to monitor the FortiManager system. When you create a new SNMP community, there are no host entries. Select *Add* to create a new entry that broadcasts the SNMP traps and information to the network connected to the specified interface.
	IP Address/Netmask	Enter the IP address and netmask of an SNMP manager. By default, the IP address is 0.0.0.0 so that any SNMP manager can use this SNMP community. Hosts configured with a /31 or larger subnet can poll SNMP but will not be sent any SNMP traps. To ensure traps are sent, configure the host with a /32 subnet (for example, `10.1.1.1/32` or `10.1.1.1/255.255.255.255`)
	Interface	Select the interface that connects to the network where this SNMP manager is located from the dropdown list. This must be done if the SNMP manager is on the Internet or behind a router.
	Delete	Click the delete icon to remove this SNMP manager entry.
	Add	Select to add another entry to the Hosts list. Up to eight SNMP manager entries can be added for a single community.

Queries	Enter the port number (161 by default) the FortiManager system uses to send v1 and v2c queries to the FortiManager in this community. Enable queries for each SNMP version that the FortiManager system uses.
Traps	Enter the Remote port number (162 by default) the FortiManager system uses to send v1 and v2c traps to the FortiManager in this community. Enable traps for each SNMP version that the FortiManager system uses.
SNMP Event	Enable the events that will cause SNMP traps to be sent to the community. • *Interface IP changed* • *Log disk space low* • *CPU Overuse* • *Memory Low* • *System Restart* • *CPU usage exclude NICE threshold* • *HA Failover* • *RAID Event* (only available for devices that support RAID) • *Power Supply Failed* (only available on supported hardware devices) • *Fan Speed Out of Range* • *Temperature Out of Range* • *Voltage Out of Range* FortiAnalyzer feature set SNMP events: • *High licensed device quota* • *High licensed log GB/day* • *Log Alert* • *Log Rate* • *Data Rate*

To edit an SNMP community:

1. Go to *System Settings > Network*.
2. In the *SNMP v1/v2c* section, double-click on a community, right-click on a community then select *Edit*, or select a community then click *Edit* in the toolbar. The *Edit SNMP Community* pane opens.
3. Edit the settings as required, then click *OK* to apply your changes.

To delete an SNMP community or communities:

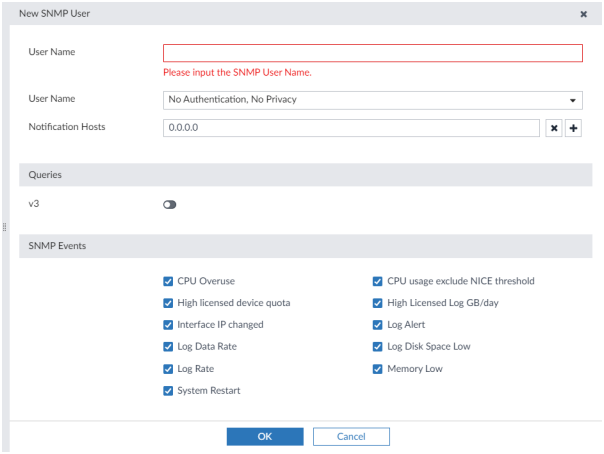
1. Go to *System Settings > Network*.
2. In the *SNMP v1/v2c* section, select the community or communities you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected community or communities.

SNMP v3 users

The FortiManager SNMP v3 implementation includes support for queries, traps, authentication, and privacy. SNMP v3 users can be created, edited, and deleted as required.

To create a new SNMP user:

1. Go to *System Settings* > *Network*.
2. In the *SNMP* section, ensure the SNMP agent is enabled.
3. In the *SNMP v3* section, click *Create New* in the toolbar. The *New SNMP User* pane opens.



4. Configure the following options, then click *OK* to create the community.

User Name	The name of the SNMP v3 user.
Security Level	The security level of the user. Select one of the following: • *No Authentication, No Privacy* • *Authentication, No Privacy*: Select the *Authentication Algorithm* (SHA1, MD5) and enter the password. • *Authentication, Privacy*: Select the *Authentication Algorithm* (SHA1, MD5), the *Private Algorithm* (AES, DES), and enter the passwords.
Queries	Select to enable queries then enter the port number. The default port is 161.
Notification Hosts	The IP address or addresses of the host. Click the add icon to add multiple IP addresses.

SNMP Event	Enable the events that will cause SNMP traps to be sent to the SNMP manager. • *Interface IP changed* • *Log disk space low* • *CPU Overuse* • *Memory Low* • *System Restart* • *CPU usage exclude NICE threshold* • *HA Failover* • *RAID Event* (only available for devices that support RAID) • *Power Supply Failed* (only available on supported hardware devices) • *Fan Speed Out of Range* • *Temperature Out of Range* • *Voltage Out of Range* FortiAnalyzer feature set SNMP events: • *High licensed device quota* • *High licensed log GB/day* • *Log Alert* • *Log Rate* • *Data Rate*

To edit an SNMP user:

1. Go to *System Settings > Network*.
2. In the *SNMP v3* section, double-click on a user, right-click on a user then select *Edit*, or select a user then click *Edit* in the toolbar. The *Edit SNMP User* pane opens.
3. Edit the settings as required, then click *OK* to apply your changes.

To delete an SNMP user or users:

1. Go to *System Settings > Network*.
2. In the *SNMP v3* section, select the user or users you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected user or users.

To configure the SNMPv3 trap remote port:

You can configure the SNMPv3 trap remote port using the FortiManager CLI:

```
config system snmp user
   edit <name>
      set notify-port <integer>(default = 162)
   end
end
```

SNMP MIBs

The Fortinet and FortiManager MIBs, along with the two RFC MIBs, can be obtained from Customer Service & Support (https://support.fortinet.com). You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.mib* MIB file in the firmware image file folder. The *FORTINET-CORE-MIB.mib* file is located in the main FortiManager 5.00 file folder.

RFC support for SNMP v3 includes Architecture for SNMP Frameworks (RFC 3411), and partial support of User-based Security Model (RFC 3414).

To be able to communicate with the SNMP agent, you must include all of these MIBs into your SNMP manager. Generally your SNMP manager will be an application on your local computer. Your SNMP manager might already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet and FortiManager proprietary MIBs to this database.



Not all MIBs and OIDs are supported on all devices. For example, some models do not include temperature sensors; thus, they will not support the related MIBs/OIDs.

MIB file name or RFC	Description
FORTINET-CORE-MIB.mib	The proprietary Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor Fortinet unit configuration settings and receive traps from the Fortinet SNMP agent.
FORTINET-FORTIMANAGER-MIB.mib	The proprietary FortiManager MIB includes system information and trap information for FortiManager units.
RFC-1213 (MIB II)	The Fortinet SNMP agent supports MIB II groups with the following exceptions. • No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10). • Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all Fortinet traffic activity. More accurate information can be obtained from the information reported by the Fortinet MIB.
RFC-2665 (Ethernet-like MIB)	The Fortinet SNMP agent supports Ethernet-like MIB information with the following exception. No support for the dot3Tests and dot3Errors groups.

SNMP traps

Fortinet devices share SNMP traps, but each type of device also has traps specific to that device type. For example FortiManager units have FortiManager specific SNMP traps. To receive Fortinet device SNMP traps, you must load and compile the FORTINET-CORE-MIB into your SNMP manager.

Traps sent include the trap message as well as the unit serial number (fnSysSerial) and host name (sysName). The Trap Message column includes the message that is included with the trap, as well as the SNMP MIB field name to help locate the information about the trap.

Event	Trap Name	Description
HA Failover `ha_switch`	fmTrapHASwitch	FortiManager HA cluster has been re-arranged. A new master has been selected and asserted.
High Licensed Log GB/day `lic-gbday`	fmTrapLicGbDayThreshold	Indicates that the used log has exceeded the licensed GB/Day.
Log Alert `log-alert`	fmTrapLogAlert	Trap is sent when a log based alert has been triggered. Alert description included in trap.

CPU usage exclude NICE threshold
`cpu-high-exclude-nice`
	fmTrapCpuThresholdExcludeNice	Indicates that the CPU usage excluding nice processes has exceeded the threshold.
		This threshold can be set in the CLI using the following commands:
		`config system snmp sysinfo`
		`set trap-cpu-high-exclude-nice-threshold <percentage value>`
		`end`

High licensed device quota `lic-dev-quota`	fmTrapLicDevQuotaThreshold	Indicates that the used device quota has exceeded the licensed device quota.
Log Data Rate `log-data-rate`	fmTrapLogDataRateThreshold	Indicates that the incoming log data rate has exceeded the threshold. The peak data rate is calculated using the peak log rate x 512 bytes (average log size).
Log Rate `log-rate`	fmTrapLogRateThreshold	Indicates that the incoming log rate has exceeded the threshold. To determine the peak log rate, use the following CLI command: `get system loglimits`
System Restart `sys_reboot`	fmTrapPowerStateChange	Trap is sent when there is a change in the status of the power supply, if present.

CPU Overuse
`cpu_high`
	fnTrapCpuThreshold	Indicates that the CPU usage has exceeded the configured threshold.
		This threshold can be set in the CLI using the following commands:
		`config system snmp sysinfo`
		`set trap-high-cpu-threshold <percentage value>`
		`end`

Memory Low `mem_low`	fnTrapMemThreshold	Indicates memory usage has exceeded the configured threshold.

Event	Trap Name	Description

		This threshold can be set in the CLI using the following commands:
		`config system snmp sysinfo`
		`set trap-low-memory-threshold <percentage value>`
		`end`

Log Disk Space Low `disk_low`	fnTrapLogDiskThreshold	Log disk usage has exceeded the configured threshold. Only available on devices with log disks.
Interface IP changed `intf_ip_chg`	fnTrapIpChange	Indicates that the IP address of the specified interface has been changed. The trap message includes the name of the interface, the new IP address and the serial number of the Fortinet unit. You can use this trap to track interface IP address changes for interfaces with dynamic IP addresses set using DHCP or PPPoE.

Fortinet & FortiManager MIB fields

The Fortinet MIB contains fields reporting current Fortinet unit status information. The below tables list the names of the MIB fields and describe the status information available for each one. You can view more details about the information available from all Fortinet MIB fields by compiling the `fortinet.3.00.mib` file into your SNMP manager and browsing the Fortinet MIB fields.

System MIB fields:

MIB field	Description
fnSysSerial	Fortinet unit serial number.

Administrator accounts:

MIB field	Description	
fnAdminNumber	The number of administrators on the Fortinet unit.	
fnAdminTable	Table of administrators.	
	fnAdminIndex	Administrator account index number.
	fnAdminName	The user name of the administrator account.
	fnAdminAddr	An address of a trusted host or subnet from which this administrator account can be used.
	fnAdminMask	The netmask for fnAdminAddr.

Custom messages:

MIB field	Description
fnMessages	The number of custom messages on the Fortinet unit.

MIB fields and traps

MIB field	Description
fmModel	A table of all FortiManager models.
fmTrapHASwitch	The FortiManager HA cluster has been re-arranged. A new primary has been selected and asserted.

RAID Management

RAID helps to divide data storage over multiple disks, providing increased data reliability. For FortiManager devices containing multiple hard disks, you can configure the RAID array for capacity, performance, and/or availability.



The *RAID Management* tree menu is only available on FortiManager devices that support RAID.

Supported RAID levels

FortiManager units with multiple hard drives can support the following RAID levels:



See the FortiManager datasheet to determine your devices supported RAID levels.

Linear RAID

A Linear RAID array combines all hard disks into one large virtual disk. The total space available in this option is the capacity of all disks used. There is very little performance change when using this RAID format. If any of the drives fails, the entire set of drives is unusable until the faulty drive is replaced. All data will be lost.

RAID 0

A RAID 0 array is also referred to as striping. The FortiManager unit writes information evenly across all hard disks. The total space available is that of all the disks in the RAID array. There is no redundancy available. If any single drive fails, the data on that drive cannot be recovered. This RAID level is beneficial because it provides better performance, since the FortiManager unit can distribute disk writing across multiple disks.

- Minimum number of drives: 2
- Data protection: No protection



RAID 0 is not recommended for mission critical environments as it is not fault-tolerant.

RAID 1

A RAID 1 array is also referred to as mirroring. The FortiManager unit writes information to one hard disk, and writes a copy (a mirror image) of all information to all other hard disks. The total disk space available is that of only one hard disk, as the others are solely used for mirroring. This provides redundant data storage with no single point of failure. Should any of the hard disks fail, there are backup hard disks available.

- Minimum number of drives: 2
- Data protection: Single-drive failure



One write or two reads are possible per mirrored pair. RAID 1 offers redundancy of data. A re-build is not required in the event of a drive failure. This is the simplest RAID storage design with the highest disk overhead.

RAID 1s

A RAID 1 with hot spare array uses one of the hard disks as a hot spare (a stand-by disk for the RAID). If a hard disk fails, within a minute of the failure the hot spare is substituted for the failed drive, integrating it into the RAID array and rebuilding the RAID's data. When you replace the failed hard disk, the new hard disk is used as the new hot spare. The total disk space available is the total number of disks minus two.

RAID 5

A RAID 5 array employs striping with a parity check. Similar to RAID 0, the FortiManager unit writes information evenly across all drives but additional parity blocks are written on the same stripes. The parity block is staggered for each stripe. The total disk space is the total number of disks in the array, minus one disk for parity storage. For example, with four hard disks, the total capacity available is actually the total for three hard disks. RAID 5 performance is typically better with reading than with writing, although performance is degraded when one disk has failed or is missing. With RAID 5, one disk can fail without the loss of data. If a drive fails, it can be replaced and the FortiManager unit will restore the data on the new disk by using reference information from the parity volume.

- Minimum number of drives: 3
- Data protection: Single-drive failure

RAID 5s

A RAID 5 with hot spare array uses one of the hard disks as a hot spare (a stand-by disk for the RAID). If a hard disk fails, within a minute of the failure, the hot spare is substituted for the failed drive, integrating it into the RAID array, and rebuilding the RAID's data. When you replace the failed hard disk, the new hard disk is used as the new hot spare. The total disk space available is the total number of disks minus two.

RAID 6

A RAID 6 array is the same as a RAID 5 array with an additional parity block. It uses block-level striping with two parity blocks distributed across all member disks.

- Minimum number of drives: 4
- Data protection: Up to two disk failures.

RAID 6s

A RAID 6 with hot spare array is the same as a RAID 5 with hot spare array with an additional parity block.

RAID 10

RAID 10 (or 1+0), includes nested RAID levels 1 and 0, or a stripe (RAID 0) of mirrors (RAID 1). The total disk space available is the total number of disks in the array (a minimum of 4) divided by 2, for example:

- 2 RAID 1 arrays of two disks each,
- 3 RAID 1 arrays of two disks each,
- 6 RAID1 arrays of two disks each.

One drive from a RAID 1 array can fail without the loss of data; however, should the other drive in the RAID 1 array fail, all data will be lost. In this situation, it is important to replace a failed drive as quickly as possible.

- Minimum number of drives: 4
- Data protection: Up to two disk failures in each sub-array.



Alternative to RAID 1 when additional performance is required.

RAID 50

RAID 50 (or 5+0) includes nested RAID levels 5 and 0, or a stripe (RAID 0) and stripe with parity (RAID 5). The total disk space available is the total number of disks minus the number of RAID 5 sub-arrays. RAID 50 provides increased performance and also ensures no data loss for the same reasons as RAID 5. One drive in each RAID 5 array can fail without the loss of data.

- Minimum number of drives: 6
- Data protection: Up to one disk failure in each sub-array.



Higher fault tolerance than RAID 5 and higher efficiency than RAID 0.



RAID 50 is only available on models with 9 or more disks. By default, two groups are used unless otherwise configured via the CLI. Use the `diagnose system raid status` CLI command to view your current RAID level, status, size, groups, and hard disk drive information.

RAID 60

A RAID 60 (6+ 0) array combines the straight, block-level striping of RAID 0 with the distributed double parity of RAID 6.

- Minimum number of drives: 8
- Data protection: Up to two disk failures in each sub-array.



High read data transaction rate, medium write data transaction rate, and slightly lower performance than RAID 50.

Configuring the RAID level



Changing the RAID level will delete all data.

To configure the RAID level:

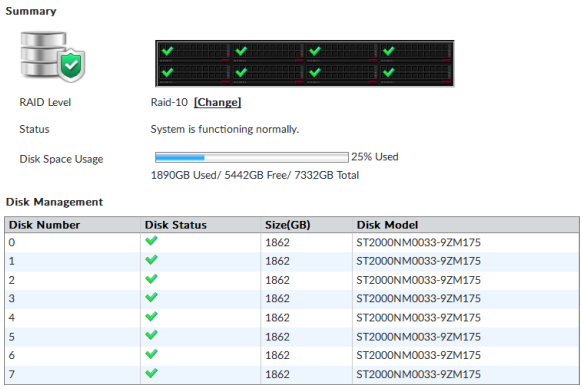
1. Go to *System Settings* > *RAID Management*.
2. Click *Change* in the *RAID Level* field. The *RAID Settings* dialog box is displayed.
3. From the *RAID Level* list, select a new RAID level, then click *OK*.
   The FortiManager unit reboots. Depending on the selected RAID level, it may take a significant amount of time to generate the RAID array.

Monitoring RAID status

To view the RAID status, go to *System Settings* > *RAID Management*. The RAID Management pane displays the RAID level, status, and disk space usage. It also shows the status, size, and model of each disk in the RAID array.



The *Alert Message Console* widget, located in *Dashboard*, provides detailed information about RAID array failures. For more information see Alert Messages Console widget on page 82.



Summary		Shows summary information about the RAID array.
	Graphic	Displays the position and status of each disk in the RAID array. Hover the cursor over each disk to view details.
	RAID Level	Displays the selected RAID level. Click *Change* to change the selected RAID level. When you change the RAID settings, all data is deleted.
	Status	Displays the overall status of the RAID array.
	Disk Space Usage	Displays the total size of the disk space, how much disk space is used, and how much disk space is free.
Disk Management		Shows information about each disk in the RAID array.
	Disk Number	Identifies the disk number for each disk.
	Disk Status	Displays the status of each disk in the RAID array. • *Ready*: The hard drive is functioning normally. • *Rebuilding*: The FortiManager unit is writing data to a newly added hard drive in order to restore the hard drive to an optimal state. The FortiManager unit is not fully fault tolerant until rebuilding is complete. • *Initializing*: The FortiManager unit is writing to all the hard drives in the device in order to make the array fault tolerant. • *Verifying*: The FortiManager unit is ensuring that the parity data of a redundant drive is valid. • *Degraded*: The hard drive is no longer being used by the RAID controller. • *Inoperable*: One or more drives are missing from the FortiManager unit. The drive is no longer available to the operating system. Data on an inoperable drive cannot be accessed.
	Size (GB)	Displays the size, in GB, of each disk.
	Disk Model	Displays the model number of each disk.

Checking RAID from command line

Use command line to check if your device uses hardware or software RAID.

To check RAID type from the command line:

1. Select the *CLI Console* from the GUI banner.
2. Type the command `diagnose system raid status` and press *Enter*.
3. The following information is shown in the output:
   - Mega RAID - this output shows that the device uses hardware RAID.
   - Software RAID - this output shows that the device uses software RAID.

Sample command line output showing hardware RAID:

```
[Product_Name_Model] # diagnose system raid status
   Mega RAID: <-- this is hardware RAID
   RAID Level: Raid-50
   RAID Status: OK
   RAID Size: 11175GB
   Groups: 2

[Product_Name_Model] # diagnose system raid status
   Software RAID: <-- this is software RAID
   RAID Level: Raid-50
   RAID Status: OK
   RAID Size: 11175GB
   Groups: 2
```

Swapping hard disks

If a hard disk on a FortiManager unit fails, it must be replaced. On FortiManager devices that support hardware RAID, the hard disk can be replaced while the unit is still running - known as hot swapping. On FortiManager units with software RAID, the device must be shutdown prior to exchanging the hard disk.

To identify which hard disk failed, read the relevant log message in the *Alert Message Console* widget. See Alert Messages Console widget on page 82.



Electrostatic discharge (ESD) can damage FortiManager equipment. Only perform the procedures described in this document from an ESD workstation. If no such station is available, you can provide some ESD protection by wearing an anti-static wrist or ankle strap and attaching it to an ESD connector or to a metal part of a FortiManager chassis.



When replacing a hard disk, you need to first verify that the new disk is the same size as those supplied by Fortinet and has at least the same capacity as the old one in the FortiManager unit. Installing a smaller hard disk will affect the RAID setup and may cause data loss. Due to possible differences in sector layout between disks, the only way to guarantee that two disks have the same size is to use the same brand and model.

The size provided by the hard drive manufacturer for a given disk model is only an approximation. The exact size is determined by the number of sectors present on the disk.

To hot swap a hard disk on a device that supports hardware RAID:

1. Remove the faulty hard disk.
2. Install a new disk.
   The FortiManager unit automatically adds the new disk to the current RAID array. The status appears on the console. The *RAID Management* pane displays a green checkmark icon for all disks and the *RAID Status* area displays the progress of the RAID re-synchronization/rebuild.

Adding hard disks

Some FortiManager units have space to add more hard disks to increase your storage capacity.



Fortinet recommends you use the same disks as those supplied by Fortinet. Disks of other brands will not be supported by Fortinet. For information on purchasing extra hard disks, contact your Fortinet reseller.

To add more hard disks:

1. Obtain the same disks as those supplied by Fortinet.
2. Back up the log data on the FortiManager unit.
   You can also migrate the data to another FortiManager unit, if you have one. Data migration reduces system down time and the risk of data loss.
3. Install the disks in the FortiManager unit.
   If your unit supports hot swapping, you can do so while the unit is running. Otherwise the unit must be shut down first. See Unit Operation widget on page 82 for information.
4. Configure the RAID level. See Configuring the RAID level on page 921.
5. If you backed up the log data, restore it.

Administrative Domains (ADOMs)

Administrative domains (ADOMs) enable administrators to manage only those devices that they are specifically assigned, based on the ADOMs to which they have access. When the ADOM mode is advanced, FortiGate devices with multiple VDOMs can be divided among multiple ADOMs.

Administrator accounts can be tied to one or more ADOMs, or denied access to specific ADOMs. When a particular administrator logs in, they see only those devices or VDOMs that have been enabled for their account. Super user administrator accounts, such as the `admin` account, can see and maintain all ADOMs and the devices within them.

When FortiAnalyzer features are enabled, each ADOM specifies how long to store and how much disk space to use for its logs. You can monitor disk utilization for each ADOM and adjust storage settings for logs as needed.

The maximum number of ADOMs you can add depends on the FortiManager system model. Please refer to the FortiManager data sheet for more information.

By default, ADOMs are disabled. Enabling and configuring ADOMs can only be done by administrators with the *Super_User* profile. See Administrators on page 976.



Non-FortiGate devices, except for FortiAnalyzer devices, are automatically located in specific ADOMs for their device type. They cannot be moved to other ADOMs.

One FortiAnalyzer device can be added to each ADOM. For more information, see Add FortiAnalyzer or FortiAnalyzer BigData on page 134.

Root ADOM

The *root ADOM* type is *FortiGate*.When ADOMs are disabled, only the root ADOM is visible. When ADOMs are enabled, other default ADOMs are visible too.

Unauthorized devices display in the root ADOM.

See also Default device type ADOMs on page 925.

Default device type ADOMs

When ADOMs are enabled, FortiManager includes default ADOMs for specific types of devices. When you add one or more of these devices to FortiManager, the devices are automatically added to the appropriate ADOM, and the ADOM becomes selectable. When a default ADOM contains no devices, the ADOM is not selectable.

For example, when you add a FortiClient EMS device to the FortiManager, the FortiClient EMS device is automatically added to the default FortiClient ADOM. After the FortiClient ADOM contains a FortiClient EMS device, the FortiClient ADOM is selectable when you log into FortiManager or when you switch between ADOMs.

You can view all of the ADOMs, including default ADOMs without devices, on the *System Settings > ADOMs* pane.

ADOM types

When ADOMs are enabled, you can create ADOMs and select a type. The type of ADOM determines what types of devices you can add to the ADOM. FortiManager supports the following types of ADOMs:

Fabric	You can add FortiGate and other types of devices from a Security Fabric to an ADOM with *Fabric* type selected.
FortiGate	You can add only FortiGate devices to an ADOM with *FortiGate* type selected.
FortiCarrier	You can add only FortiCarrier devices to an ADOM with *FortiCarrier* type selected.
FortiFirewall	You can add only FortiFirewall devices to an ADOM with *FortiFirewall* type selected.

FortiFirewallCarrier	You can add only FortiFirewall Carrier devices to an ADOM with *FortiFirewallCarrier* type selected.
FortiProxy	You can only add FortiProxy devices to an ADOM with *FortiProxy* type selected. See FortiProxy ADOMs on page 926.

See Creating ADOMs on page 934.

FortiProxy ADOMs

You can create FortiProxy ADOMs to centrally manage FortiProxy devices using FortiManager. See Creating ADOMs on page 934.

The following FortiManager modules are available in FortiProxy ADOMs:

FortiManager Module	Features available in FortiProxy ADOM
Device Manager on page 88	Use the *Device Manager* pane to create device configuration changes and install device and policy package configuration changes to managed devices. You can also monitor managed FortiProxy devices from the *Device Manger* pane. Using the device database, you can configure managed FortiProxy devices. For more information, see Device Manager on page 88.
Policy & Objects on page 407	Configure policies and objects for FortiProxy devices, including: • Create a new FortiProxy firewall policy on page 498 • Create a new FortiProxy proxy auto-configuration (PAC) policy on page 500 • FortiProxy content analysis objects on page 575 For more information, see Policy & Objects on page 407.
VPN Manager on page 650	Use the *VPN Manager* pane to enable and use central VPN management. You can view and configure IPsec VPN and SSL-VPN settings that you can install to one or more devices. For more information, see VPN Manager on page 650.
Fabric View on page 697	The *Fabric View* module enables you to view and create fabric connectors. For more information, see Fabric View on page 697.
FortiGuard on page 787	View and manage FortiGuard services for FortiProxy devices. For more information, see FortiGuard on page 787.
System Settings on page 900	Configure FortiManager system settings. For more information, see System Settings on page 900.



FortiProxy ADOMs cannot be upgraded or downgraded.

If another FortiProxy ADOM version is required, you can move your FortiProxy device(s) into another FortiProxy ADOM created on the selected version.

Organizing devices into ADOMs

You can organize devices into ADOMs to allow you to better manage these devices. Devices can be organized by whatever method you deem appropriate, for example:

- Firmware version: group all devices with the same firmware version into an ADOM.
- Geographic regions: group all devices for a specific geographic region into an ADOM, and devices for a different region into another ADOM.
- Administrative users: group devices into separate ADOMs based for specific administrators responsible for the group of devices.
- Customers: group all devices for one customer into an ADOM, and devices for another customer into another ADOM.

Enabling and disabling the ADOM feature

By default, ADOMs are disabled. Enabling and configuring ADOMs can only be done by super user administrators.

When ADOMs are enabled, the *Device Manager*, *Policy & Objects*, *AP Manager*, and *VPN Manager* panes are displayed per ADOM. If FortiAnalyzer features are enabled, the *FortiView*, *Log View*, *Incidents & Events*, and *Reports* panes are also displayed per ADOM. You select the ADOM you need to work in when you log into the FortiManager unit. Switching between ADOMs on page 37.



ADOMs must be enabled to support FortiMail and FortiWeb logging and reporting. When a FortiMail or FortiWeb device is authorized, the device is added to the respective default ADOM and is visible in the left-hand tree menu.



FortiGate and FortiCarrier devices cannot be grouped into the same ADOM. FortiCarrier devices are added to a specific default FortiCarrier ADOM.

To enable the ADOM feature:

1. Log in to the FortiManager as a super user administrator.
2. Go to *Dashboard*.
3. In the *System Information* widget, toggle the *Administrative Domain* switch to *ON*.
   You will be automatically logged out of the FortiManager and returned to the log in screen.

To disable the ADOM feature:

1. Remove all the devices from all non-root ADOMs. That is, add all devices to the root ADOM.
2. Delete all non-root ADOMs. See Deleting ADOMs on page 938.
   Only after removing all the non-root ADOMs can ADOMs be disabled.
3. Go to *Dashboard*.
4. In the *System Information* widget, toggle the *Administrative Domain* switch to *OFF*.

You will be automatically logged out of the FortiManager and returned to the log in screen.



The ADOMs feature cannot be disabled if ADOMs are still configured and have managed devices in them.

ADOM device modes

ADOM deployment can have two device modes: *Normal* (default) and *Advanced*.

- In *Normal* mode, you cannot assign different FortiGate VDOMs to different ADOMs. The FortiGate unit can only be added to a single ADOM.
- In *Advanced* mode, you can assign a VDOM from a single device to a different ADOM. This allows you to analyze data for individual VDOMs, but will result in more complicated management scenarios. It is recommended only for advanced users.



FortiManager does not support splitting FortiGate VDOMs between multiple ADOMs in different ADOM modes (normal/backup).

To change from *Advanced* mode back to *Normal* mode, you must ensure no FortiGate VDOMs are assigned to an ADOM.

To change the ADOM device mode:

1. Go to *System Settings* > *Advanced* > *Advanced Settings*.
2. In the ADOM Mode field, select either *Normal* or *Advanced*.
3. Select *Apply* to apply your changes.



While in *Workspace* mode with *Advanced* ADOM mode enabled, changes made to a managed device's database in the *Device Manager* are automatically saved and applied, and the *Save* button is not selectable.

ADOM modes

When creating an ADOM, the mode can be set to *Normal* or *Backup*.

Normal mode ADOMs

When creating an ADOM in normal mode, the ADOM is considered *Read/Write*, where you are able to make changes to the ADOM and managed devices from the FortiManager. FortiGate units in the ADOM will query their own configuration every 5 seconds. If there has been a configuration change, the FortiGate unit will send a diff revision on the change to the FortiManager using the FGFM protocol.

Backup mode ADOMs

Backup mode ADOMs are used to store the configurations of managed devices.

In backup mode, you cannot push new configuration changes from FortiManager to managed devices directly. Instead, changes are made using scripts run on the managed device, or through the device's GUI or CLI directly.

When adding a device to a backup ADOM, the device's configuration is automatically stored in the FortiManager device database, and revisions are sent to the FortiManager when the following specific conditions are met:

- Configuration change and session timeout
- Configuration change and log out
- Configuration change and reboot
- Manual configuration backup from the managed device

You can monitor and review the revision history for managed devices, and you can push existing revisions to managed devices.

Optionally, you can also import a device's objects (for example, firewall addresses) into the FortiManager's ADOM database, which allows these objects to be stored and shared with other managed devices. See Importing objects to backup ADOMs on page 930.

In backup mode, scripting is still allowed for pushing scripts directly to FortiGate units.



Enable fcp-cfg-service for backup mode ADOMs

In order to perform configuration backups from the CLI of a FortiGate device that is in a backup mode ADOM, you must first enable "`fcp-cfg-service`" using the following command on the FortiManager:

```
config system global
   set fcp-cfg-service enable
end
```

Creating backup ADOMs

You can create an ADOM with backup mode enabled, and then add devices to the ADOM.

When an ADOM is in backup mode, the following panes are available:

- *Dashboard*
- *Device Manager*
- *Policy & Objects*
- *FortiView*
- *Fabric View*
- *FortiGuard*
- *System Settings*

To create backup ADOMs:

1. Go to *System Settings* > *ADOMs*, and click *Create New*.
2. Set the following options, and click *OK*:

Name	Type a name for the ADOM.
Type	Select the type of device and ADOM version.
Devices	Select a device. Alternately, you can add a device to the ADOM later by using the *Add Device* wizard.
Mode	Select *Backup*.

The ADOM in backup mode is created.

Importing objects to backup ADOMs

You can use the *Add Device* wizard to add FortiGate devices to an ADOM in backup mode.

After the FortiGate device is added, its entire configuration (including objects and policies) is available in FortiManager's device database.

The wizard then offers the option to import the configuration from the device. However, in an ADOM operating in backup mode, only objects are imported from the device configuration. Policies are not. Objects imported this way are stored in the ADOM database and can be shared with other managed devices within the same ADOM.

Alternatively, you can import objects from an existing (already added) device at any time, for example, if you want to share specific objects with other managed devices. Objects imported using this method are also stored in the ADOM database and can be shared with other devices in the same ADOM.

Objects must be manually imported into the FortiManager backup ADOM. They are not automatically synchronized to FortiManager when they are created, edited or deleted on the FortiGate.

Objects created on FortiManager can also be imported into the FortiGate. See Managing synchronization of FortiManager objects on FortiGate on page 931.

Importing FortiGate objects

To import FortiGate objects to the ADOM database when adding devices:

1. Go to *Device Manager* > *Device & Groups*, and click *Add Device*.
2. Follow the *Add Device* wizard, until the *Import Now* button is displayed.
3. Click *Import Now* to import firewall address and service objects to the ADOM database.
4. Go to the *Policy & Objects* pane to view the objects.
   You can also create, edit, and delete objects.

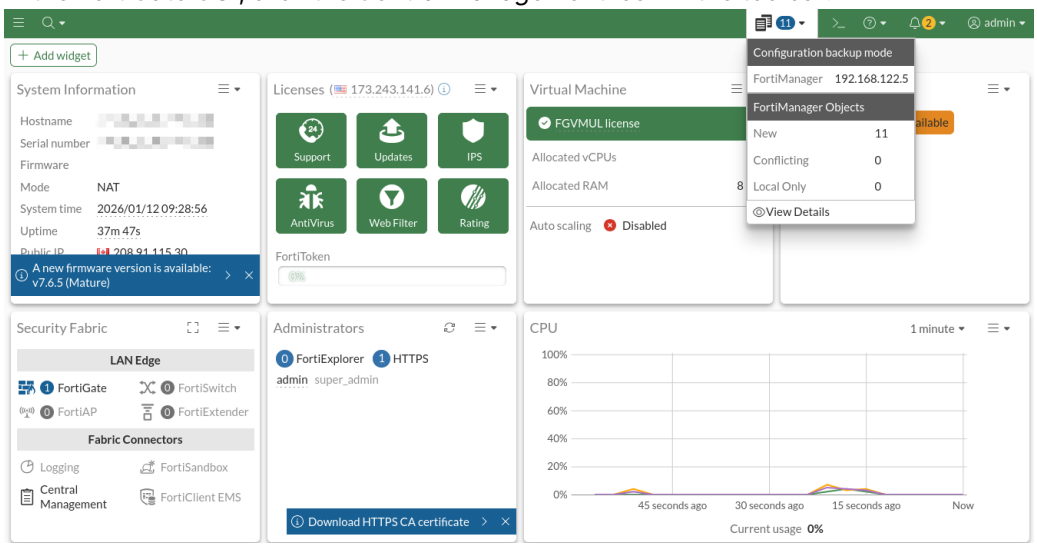
To import FortiGate objects to the ADOM database after adding devices:

1. Go to *Device Manager* > *Device & Groups*.
2. Select a device and click *Import Configuration*.
   The objects are imported into the ADOM database.
3. Go to the *Policy & Objects* pane to view the objects.
   You can also create, edit, and delete objects.

Managing synchronization of FortiManager objects on FortiGate

To manage synchronization of FortiManager objects on FortiGate:

1. In the FortiGate GUI, click the *Central Management* icon in the toolbar.



2. Click *View Details* to view the FortiManager Backup Objects Table.
The table displays information about objects by status:

New	Objects stored on the FortiManager backup ADOM that are not available locally. To import new objects to the local FortiGate, select them and click *Import* or *Import All*.
Conflicting	Local and FortiManager objects that are in conflict. To view a comparison of the objects, click *View Properties*. To replace a local object with the FortiManager object, select the object and click *Update*.
Local Only	Local objects that have not been imported to the FortiManager backup ADOM. To import local objects to FortiManager, use the FortiManager Import Configuration wizard. See Importing FortiGate objects on page 930.

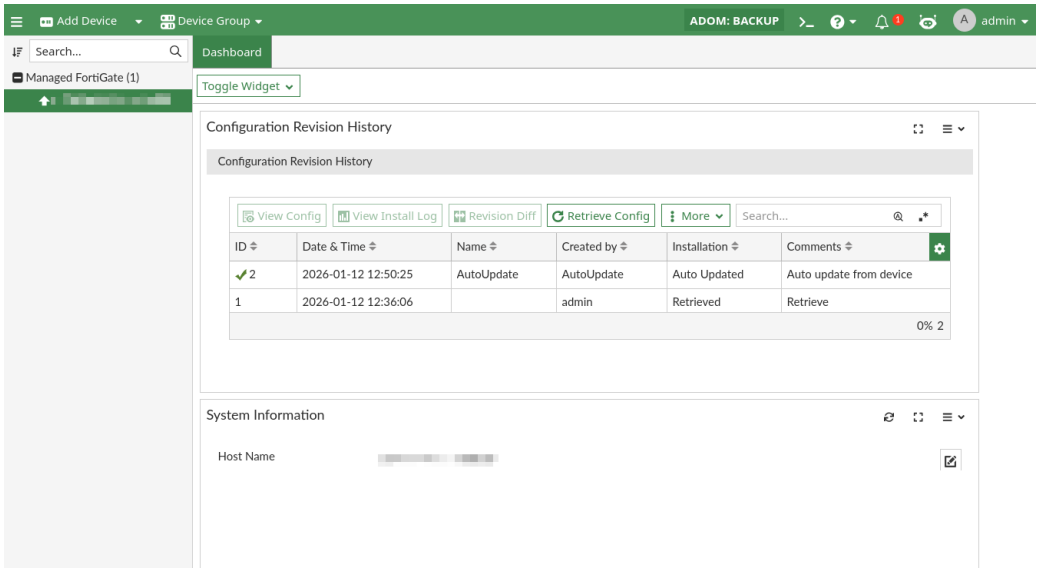
Viewing read-only polices in backup ADOMs

When an ADOM is in backup mode, you can view information about read-only policies

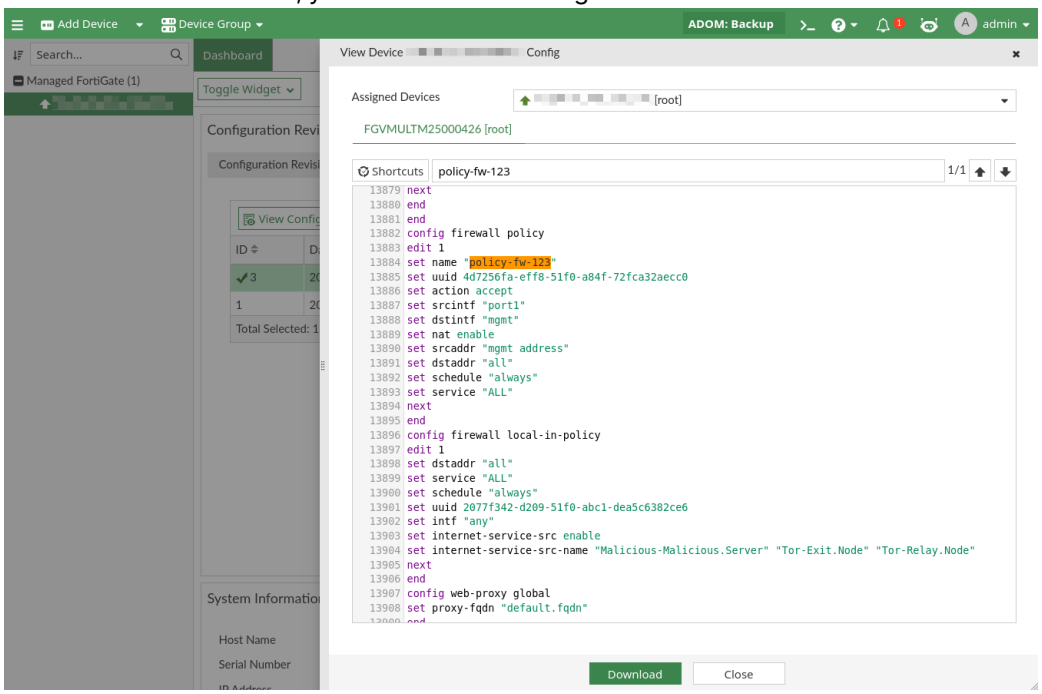
To view read-only polices:

1. Ensure you are in an ADOM with backup mode enabled.
2. Go to *Device Manager* > *Device & Groups*.
3. In the tree menu, select the device group, for example, *Managed Devices*. The list of devices display in the content pane and in the bottom tree menu.
4. In the bottom tree menu, select a device. The *System dashboard* is displayed.

For a description of the widgets, see Device DB - Dashboard on page 199.



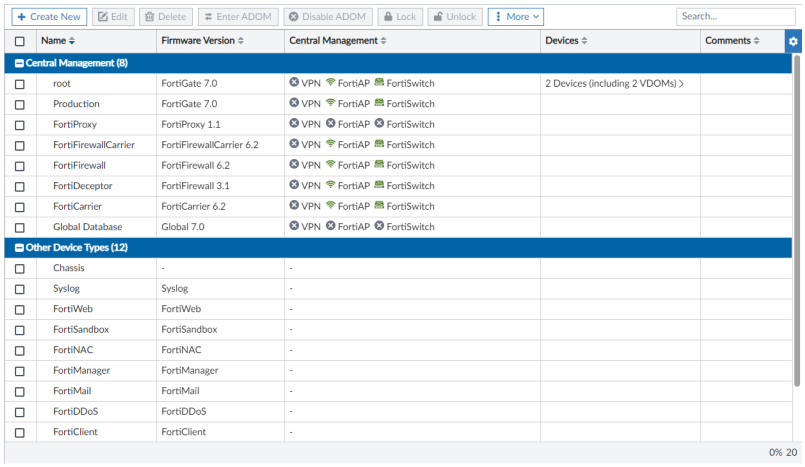
5. In the dashboard toolbar, you can view the configuration for the current revision to view policy information.



Managing ADOMs

The ADOMs feature must be enabled before ADOMs can be created or configured. See Enabling and disabling the ADOM feature on page 927.

To create and manage ADOMs, go to *System Settings* > *ADOMs*.



Create New	Create a new ADOM. See Creating ADOMs on page 934.
Edit	Edit the selected ADOM. This option is also available from the right-click menu. See Editing an ADOM on page 938.
Delete	Delete the selected ADOM or ADOMs. You cannot delete default ADOMs. This option is also available from the right-click menu. See Deleting ADOMs on page 938.
Enter ADOM	Switch to the selected ADOM. This option is also available from the right-click menu.
Disable ADOM	Disable the selected ADOM. This option is also available from the right-click menu.
More	Select *Expand Devices* to expand all of the ADOMs to show the devices in each ADOM. Select *Collapse Devices* to collapses the device lists. Select *ADOM Health Check* to generate a report that identifies whether any ADOMs contain problematic devices. See Checking ADOM health on page 939. Select an ADOM, and click *Clone* to make a copy of the ADOM. Devices are not cloned to the new ADOM. Select an ADOM, and click *Upgrade* to upgrade the ADOM. See also ADOM versions on page 941. Some of these options are also available from the right-click menu.
Search	Enter a search term to search the ADOM list.
Name	The name of the ADOM. ADOMs are listed in the following groups: *Security Fabric*, *Central Management*, *Backup Mode* (if there are any backup mode ADOMs), and *Other Device Types*. A group can be collapsed or expanded by clicking the triangle next to its name.

Firmware Version	The firmware version of the ADOM. Devices in the ADOM should have the same firmware version. See ADOM versions on page 941 for more information.
Central Management	Whether or not central management for VPN, FortiAP, or FortiSwitch is enabled for the ADOM.
Devices	The number of devices and VDOMs that the ADOM contains. The device list can be expanded or by clicking the triangle.

Creating ADOMs

ADOMs must be enabled, and you must be logged in as a super user administrator to create a new ADOM.

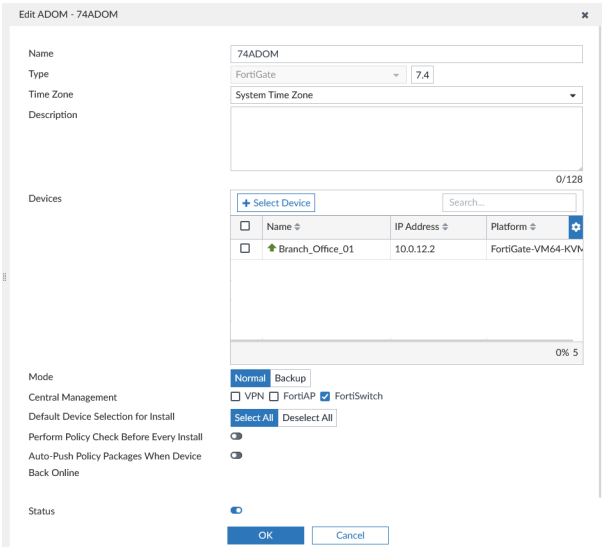
Consider the following when creating ADOMs:

- The maximum number of ADOMs that can be created depends on the FortiManager model. For more information, see the FortiManager data sheet at https://www.fortinet.com/products/management/fortimanager.html.
- You must use an administrator account that is assigned the *Super_User* administrative profile.
- You can add a device to only one ADOM. You cannot add a device to multiple ADOMs.
- You cannot add FortiGate and FortiCarrier devices to the same ADOM. FortiCarrier devices are added to a specific, default FortiCarrier ADOM.
- You can add one or more VDOMs from a FortiGate device to one ADOM. If you want to add individual VDOMs from a FortiGate device to different ADOMs, you must first enable advanced device mode. See ADOM device modes on page 928.
- When FortiAnalyzer features are enabled, you can configure how an ADOM handles log files from its devices. For example, you can configure how much disk space an ADOM can use for logs, and then monitor how much of the allotted disk space is used. You can also specify how long to keep logs indexed in the SQL database and how long to keep logs stored in a compressed format.

To create an ADOM:

1. Ensure that ADOMs are enabled. See Enabling and disabling the ADOM feature on page 927.
2. Go to *System Settings* > *ADOMs*.

3. Click *Create New* in the toolbar. The *Create New ADOM* pane is displayed.



4. Configure the following settings, then click *OK* to create the ADOM.

Name	Type a name that allows you to distinguish this ADOM from your other ADOMs. ADOM names must be unique.
Type	Select *Fabric*, *FortiCarrier*, *FortiFirewall*, *FortiFirewall Carrier*, *FortiGate*, or *FortiProxy* from the dropdown menu. The ADOM type cannot be edited. Other device types are added to their respective default ADOM when authorized for central management with FortiManager.
Time Zone	Select the time zone for the ADOM. The selected time zone is used by all modules in the ADOM (for example, *Policy & Objects* and *System Settings*) except in the *Event Log* which uses the system time zone regardless of the selected ADOM. When FortiAnalyzer features are enabled, this time zone will be used when displaying data in *Log View* and *FortiView*. When FortiManager is managing a FortiAnalyzer, each FortiAnalyzer ADOM synchronizes its time zone from the corresponding FortiManager ADOM. The *Default* time zone is the time zone set for the FortiManager. For more information, see Configuring the system time on page 65.
Version	Select the version of the devices in the ADOM. The ADOM version cannot be edited.
Devices	Add a device or devices with the selected versions to the ADOM. The search field can be used to find specific devices. See Assigning devices to an ADOM on page 937.
Mode	Select *Normal* mode if you want to manage and configure the connected devices from the FortiManager GUI. Select *Backup* mode if you want to backup the configurations to the FortiManager, but configure each device locally. See ADOM modes on page 928 for more information.

Central Management	Select the *VPN* checkbox to enable central VPN management. Select the *FortiAP* checkbox to enable central FortiAP management. This checkbox is selected by default. Select the *FortiSwitch* checkbox to enable central FortiSwitch management. This option is only available when the *Mode* is *Normal*.
Default Device Selection for Install	Select either *Select All* or *Deselect All*. This option is only available when the *Mode* is *Normal*.
Perform Policy Check Before Every Install	Turn *On* to perform a policy consistency check before every install. Only added or modified policies are checked. See Perform a policy consistency check on page 424.
Action When Conflicts Occur During Policy Check	Select an action to take when a conflict occurs during the automatic policy consistency check , either *Continue Installation* or *Stop Installation*.
Auto-Push Policy Packages When Device Back Online	Automatically push policy package updates to currently offline managed devices when the devices come back online.
Data Policy	Specify how long to keep logs in the indexed and compressed states. This section is only available when FortiAnalyzer features are enabled. See FortiAnalyzer Features on page 41.
Keep Logs for Analytics	Specify how long to keep logs in the indexed state. During the indexed state, logs are indexed in the SQL database for the specified amount of time. Information about the logs can be viewed in the *FortiView*, *Incidents & Events*, and *Reports* modules. After the specified length of time expires, Analytics logs are automatically purged from the SQL database.
Keep Logs for Archive	Specify how long to keep logs in the compressed state. During the compressed state, logs are stored in a compressed format on the FortiManager unit. When logs are in the compressed state, information about the log messages cannot be viewed in the *FortiView*, *Incidents & Events*, or *Reports* modules. After the specified length of time expires, Archive logs are automatically deleted from the FortiManager unit.
Disk Utilization	Specify how much disk space to use for logs. This section is only available when FortiAnalyzer features are enabled. See FortiAnalyzer Features on page 41.
Maximum Allowed	Specify the maximum amount of FortiManager disk space to use for logs, and select the unit of measure. The total available space on the FortiManager unit is shown.
Analytics : Archive	Specify the percentage of the allotted space to use for Analytics and Archive logs.

		Analytics logs require more space than Archive logs. For example, a setting of 70% and 30% indicates that 70% of the allotted disk space will be used for Analytics logs, and 30% of the allotted space will be used for Archive logs. Select the *Modify* checkbox to change the setting.
	Alert and Delete When Usage Reaches	Specify at what data usage percentage an alert messages will be generated and logs will be automatically deleted. The oldest Archive log files or Analytics database tables are deleted first.

Assigning devices to an ADOM

To assign devices to an ADOM you must be logged in as a super user administrator. Devices cannot be assigned to multiple ADOMs.

To assign devices to an ADOM:

1. Go to *System Settings* > *ADOMs*.
2. Double-click on an ADOM, right-click on an ADOM and then select the *Edit* from the menu, or select the ADOM then click *Edit* in the toolbar. The *Edit ADOM* pane opens.
3. Click *Select Device*. The *Select Device* list opens on the right side of the screen.
4. Select the devices that you want to add to the ADOM. Only devices with the same version as the ADOM can be added. The selected devices are displayed in the *Devices* list.
   If the ADOM mode is *Advanced* you can add separate VDOMs to the ADOM as well as units.
5. When done selecting devices, click *Close* to close the *Select Device* list.
6. Click *OK*.
   The selected devices are removed from their previous ADOM and added to this one.

Assigning VDOMs to an ADOM

To assign VDOMs to an ADOM you must be logged in as a super user administrator and the ADOM mode must be *Advanced* (see ADOM device modes on page 928). VDOMs cannot be assigned to multiple ADOMs.

To assign VDOMs to an ADOM:

1. Go to *System Settings* > *ADOMs*.
2. Double-click on an ADOM, right-click on an ADOM and then select the *Edit* from the menu, or select the ADOM then click *Edit* in the toolbar. The *Edit ADOM* pane opens.
3. Click *Select Device*. The *Select Device* list opens on the right side of the screen.
4. Select the VDOMs that you want to add to the ADOM. Only VDOMs on devices with the same version as the ADOM can be added. The selected VDOMs are displayed in the *Devices* list.
5. When done selecting VDOMs, click *Close* to close the *Select Device* list.
6. Click *OK*.
   The selected VDOMs are removed from their previous ADOM and added to this one.

Assigning administrators to an ADOM

Super user administrators can create other administrators and either assign ADOMs to their account or exclude them from specific ADOMs, constraining them to configurations and data that apply only to devices in the ADOMs they can access.



By default, when ADOMs are enabled, existing administrator accounts other than *admin* are assigned to the *root* domain, which contains all devices in the device list. For more information about creating other ADOMs, see Creating ADOMs on page 934.

To assign an administrator to specific ADOMs:

1. Log in as a super user administrator. Other types of administrators cannot configure administrator accounts when ADOMs are enabled.
2. Go to *System Settings > Administrators*.
3. Double-click on an administrator, right-click on an administrator and then select the *Edit* from the menu, or select the administrator then click *Edit* in the toolbar. The *Edit Administrator* pane opens.
4. Edit the *Administrative Domain* field as required, either assigning or excluding specific ADOMs.
5. Select *OK* to apply your changes.



The *admin* administrator account cannot be restricted to specific ADOMs.

Editing an ADOM

To edit an ADOM you must be logged in as a super user administrator. The ADOM type and version cannot be edited. For the default ADOMs, the name cannot be edited.

To edit an ADOM:

1. Go to *System Settings > ADOMs*.
2. Double-click on an ADOM, right-click on an ADOM and then select *Edit* from the menu, or select the ADOM then click *Edit* in the toolbar. The *Edit ADOM* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

Deleting ADOMs

To delete an ADOM, you must be logged in as a super-user administrator (see Administrator profiles on page 1010), such as the *admin* administrator.

Prior to deleting an ADOM:

- All devices must be removed from the ADOM. Devices can be moved to another ADOM, or to the root ADOM. See Assigning devices to an ADOM on page 937.

To delete an ADOM:

1. Go to *System Settings* > *ADOMs*.
2. Ensure that the ADOM or ADOMs being deleted have no devices in them.
3. Select the ADOM or ADOMs you need to delete.
4. Click *Delete* in the toolbar, or right-click and select *Delete*.
5. Click *OK* in the confirmation box to delete the ADOM or ADOMs.
6. If there are users or policy packages referring to the ADOM, they are displayed in the *ADOM References Detected* dialog. Click *Delete Anyway* to delete the ADOM or ADOMs. The references to the ADOMs are also deleted.

Default ADOMs cannot be deleted.

Checking ADOM health

From the *System Settings* > *ADOMs* pane, you can check the status of all devices in all ADOMs. You can check the status of the following criteria for all devices in all ADOMs:

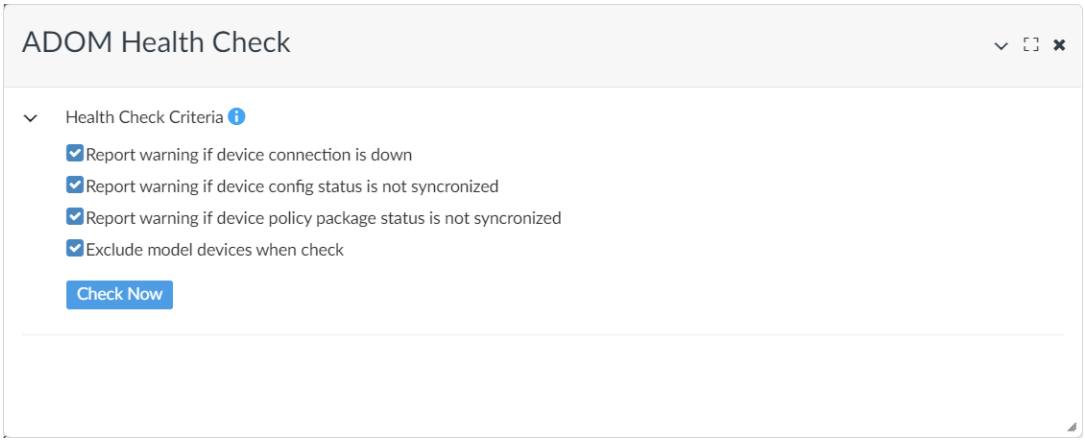
- Device connection is down.
- Device configuration status is not synchronized.
- Device policy package status is not synchronized.

You can also choose whether to exclude model devices from the health check.

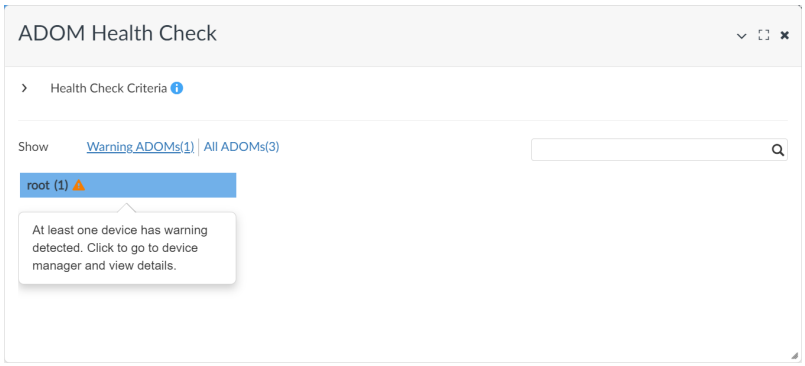
When the health check status is displayed, you can view what ADOMs contain problematic devices, and go directly to the *Device Manager* pane in the ADOM with problematic devices. You can also return to the *ADOM Health Check* dialog box, and continue checking ADOM statuses.

To check ADOM health:

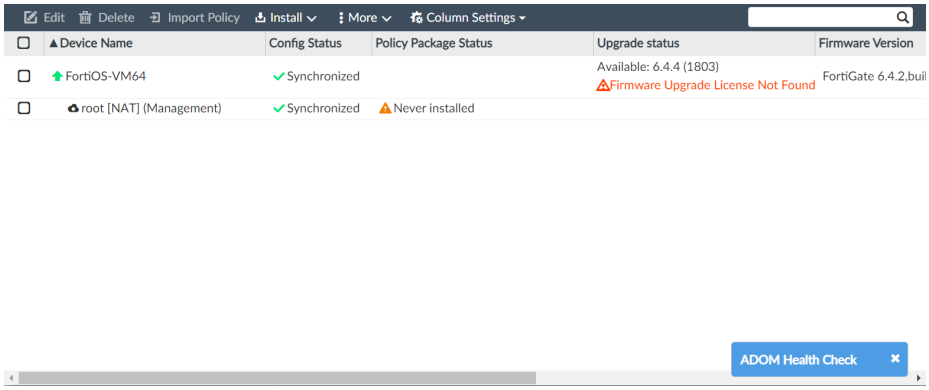
1. Go to *System Settings* > *ADOMs*.
2. From the *More* menu, select *ADOM Health Check*. The *ADOM Health Check* dialog box is displayed.



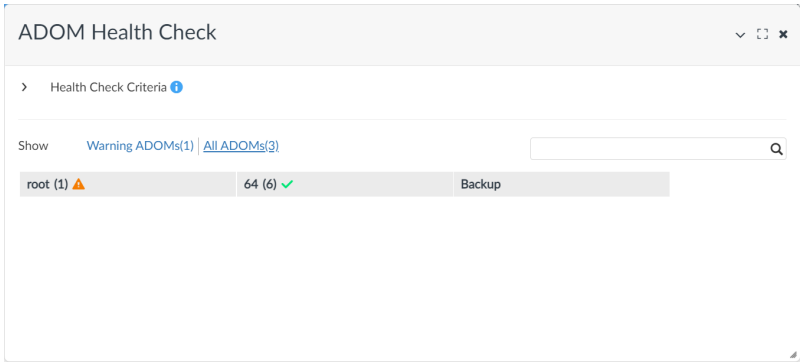
3. In the *Health Check Criteria* section, select what items to check, and click *Check Now*.
   The results of the check are displayed. In the following example, *Warning ADOMs <number>* is selected, and the list of ADOMs with warnings are displayed. The *root* ADOM has a warning.



4. Under *Warning ADOMs <number>*, click the ADOM name to display the *Device Manager* pane, and view details about the warning.
   The *Device Manager* pane is displayed for the ADOM with the warning. The *ADOM Health Check* button remains at the bottom of the pane.



5. At the bottom-right of the *Device Manager* pane, click the *ADOM Health Check* button to return to the *ADOM Health Check* dialog box, and continue checking ADOMs.
   The *ADOM Health Check* dialog box is displayed.
6. Click *All ADOMs <number>*.
   A summary of all ADOMs is displayed. In the following example, a warning status (orange triangle) displays beside the *root* ADOM, and a synchronized status (green checkmark) displays beside the *64* ADOM.



7. Click the *x* on the top-right corner to close the dialog box.

ADOM versions

Each ADOM created on FortiManager has its own version. The version of an ADOM refers to the specific FortiOS version that the ADOM's central database is aligned with. For example, a version 7.4 ADOM uses FortiOS 7.4 syntax, and its Policy & Objects are based on FortiOS 7.4.

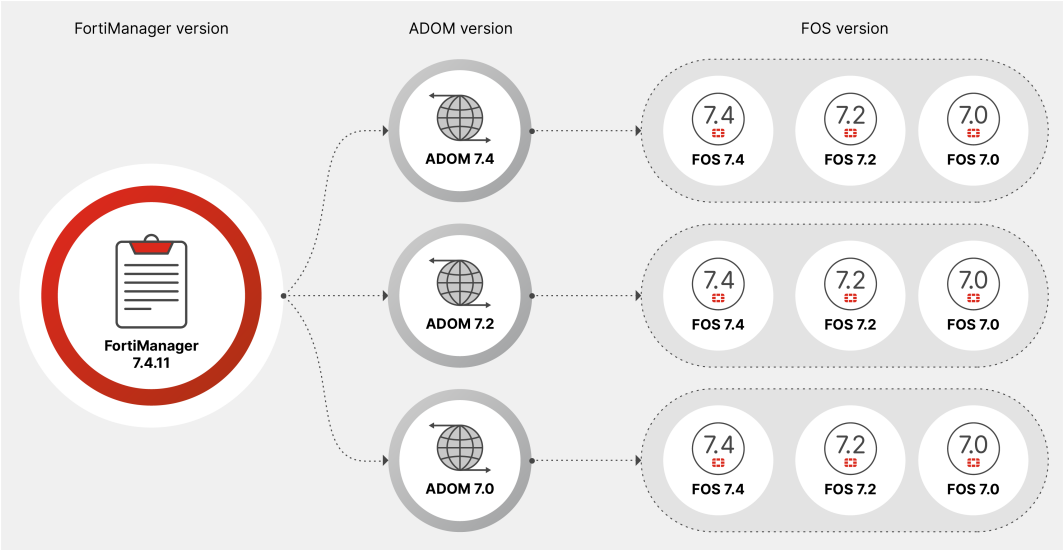
The ADOM version defines the features, configuration options, and policies that are available within that ADOM:

Firmware compatibility	The ADOM version aligns with a specific FortiOS firmware version (for example, 7.0, 7.2, and 7.4), ensuring that devices running a compatible FortiOS version can be managed within that ADOM. This is important because different FortiOS versions may have different features, commands, or configurations, so the ADOM version must match to enable proper management.
FortiOS feature set	Each FortiOS version may introduce new features, security policies, or configuration settings. By setting the ADOM to a specific version, you define the feature set available to that ADOM, limiting the options to those compatible with the selected FortiOS version.
Version control	Using versioned ADOMs allows for consistent policy and configuration management across devices within the same ADOM, ensuring they all operate within the same FortiOS environment.
FortiOS device allocation	Only devices running a FortiOS version compatible with the ADOM's version can be assigned to that ADOM, helping avoid misconfigurations or conflicts. See FortiOS version support by ADOM version on page 943.
ADOM version upgrades	ADOMs can be upgraded to support newer FortiOS versions, allowing you to adopt the latest features and improvements as devices in that ADOM are upgraded. When planning upgrades, it's essential to ensure that the FortiManager version supports the desired ADOM versions and that those ADOM versions are compatible with the FortiOS versions on your devices. See Upgrading an ADOM on page 948 and Understanding the relationships between versions on page 943.

Managing devices on different firmware versions

Some ADOM versions can also manage FortiGate devices that are on earlier or later firmware versions. For example, in 7.4.11, the 7.4 ADOM can also manage FortiGate devices on firmware versions 7.2.x and 7.0.x.

Fig 1: Supported FortiOS versions for each FortiManager 7.4.11 ADOM version



When the ADOM is managing devices on earlier or later firmware versions, it does not include the exact FortiOS syntax for those versions, and instead uses a “downgrade” and “upgrade” mechanism to adapt to different versions of FortiOS syntax as needed.

For example:

Configuration upgrade	If you install policies to a device with a higher FortiOS version than the ADOM version, FortiManager will leverage its upgrade capability. Automatic upgrade of CLI syntax is handled as follows: **1.** New CLI syntax that exists in the higher FortiGate version but not in the ADOM's version is not used. **2.** Modified CLI syntax is upgraded to the higher version's CLI syntax and used. **3.** Deleted CLI syntax is not installed to the higher version FortiGate.
Configuration downgrade	If you install policies to a device with a lower FortiOS version, FortiManager will leverage its downgrade capability. Automatic downgrade of CLI syntax is handled as follows: **1.** New CLI syntax that does not exist in the previous version is discarded during downgrade and isn't used. **2.** Modified CLI syntax is reverted to the previous version's CLI syntax and used. **3.** Deleted CLI syntax is converted to the previous version's CLI syntax and uses the default values from that version.

The upgrade and downgrade process is performed on a best-effort basis. If FortiManager supports the necessary downgrade or upgrade capabilities for the target FortiOS versions, then the ADOM can manage devices with those versions. See FortiOS version support by ADOM version on page 943.



While some ADOM versions can manage multiple FortiOS versions, it's generally recommended to minimize version discrepancies to avoid potential compatibility issues.

It is not recommended to permanently leave devices on earlier or later firmware versions within the ADOM due to the restrictions the ADOM may have by not sharing the exact FortiOS syntax. For example, you cannot use features from higher firmware version, such as templates that reference syntax from the higher version.

FortiOS version support by ADOM version

The table below outlines the FortiOS versions that can be managed by each ADOM version in FortiManager 7.4.11, including the ability to install and import configurations to and from FortiGate devices on that version.

ADOM version support can change between each release as additional support is added so it is recommended that you view the table below for **your specific FortiManager version** to see the firmware versions that are supported by each ADOM version.

Supported ADOM versions in FortiManager7.4.11:

FortiOS Version	ADOM Versions					
	ADOM 7.4		ADOM 7.2		ADOM 7.0	
	Install	Import	Install	Import	Install	Import
7.4.x	✓	✓	✓	✓	✓	✓
7.2.x	✓	✓	✓	✓	✓	✓
7.0.x	✓	✓	✓	✓	✓	✓



The versions that each ADOM is able to support is also based on the FortiManager firmware version's overall compatibility with other products.

- For example, in FortiManager 7.2.8 the 7.0 ADOM can include devices on FortiOS 6.4.x.
- In FortiManager 7.4.11, the 7.0 ADOM **can not** include FortiOS 6.4.x devices because FortiManager 7.4.11 firmware is not compatible with FortiOS 6.4.x.

For information on devices supported by your FortiManager firmware version, see the FortiManager Release Notes.



New ADOM versions introduced to FortiManager will initially only support FortiOS on matching firmware versions. Additional upgrade/downgrade configuration support is typically added within one or two patch versions.

Understanding the relationships between versions

When using ADOMs in FortiManager, there are three different versions to be aware of:

1. **FortiManager version**: This is the software version of the FortiManager system itself, which determines the overall capabilities and the range of ADOM versions available.
2. **ADOM version**: An ADOM in FortiManager is a logical partition that allows for the separate management of devices and policies. Each ADOM is assigned to a specific version, which aligns with a particular FortiOS syntax version. This alignment ensures that the features and configurations within the ADOM are compatible with the devices it manages.
3. **FortiOS version**: This is the firmware version running on Fortinet devices, such as FortiGate firewalls. The FortiOS version dictates the features and configurations available on the device.

By understanding the way these versions interact, you can effectively manage your Fortinet environment, ensuring compatibility and optimal performance across the FortiManager, ADOMs, and FortiOS versions.

Relationship between FortiManager and ADOM versions:

- A single FortiManager instance can support multiple ADOMs, each potentially set to different versions.
- The range of ADOM versions that FortiManager can support depends on its own version. For example, FortiManager 7.4.11 can support ADOM versions 7.4, 7.2 and 7.0.

Relationship between ADOM and FortiGate versions:

- An ADOM's version determines which FortiOS versions it can manage. For instance, in FortiManager 7.4.11 an ADOM set to version 7.4 can manage devices running FortiOS 7.4, 7.2, and 7.0.
- This compatibility ensures that configurations and policies within the ADOM are appropriate for the device's firmware.

Global database version

When deploying global policies using the Global Database ADOM, it is essential to consider both the Global ADOM version and the corresponding local ADOM version to ensure compatibility and successful policy installation.

1. Global Database ADOM version

- The Global Database ADOM version determines the FortiOS syntax that is used when creating policies and objects in the ADOM. For example, if the Global Database ADOM version is 7.4, then policies and objects created in the ADOM use FortiOS 7.4 syntax.
- The Global Database ADOM version also determines the local ADOM versions that can be selected for assignment. See Assigning a global policy package to an ADOM on page 955.

2. Local ADOM version

- Once a global policy package has been assigned to an ADOM, the local ADOM handles the installation of the policy package to managed devices.
- The local ADOM version controls what FortiOS versions the global policy package can be installed on. The local ADOM includes a configuration upgrade/downgrade mechanism so that the global policy package can be installed on FortiOS devices that are on higher or lower firmware versions. To see what FortiOS versions are supported by each local ADOM version and for more information on configuration upgrade/downgrades, see ADOM versions on page 941.

Global Database and local ADOM compatibility

The following table identifies the local ADOM versions that can be selected for assignment in FortiManager 7.4.11:

Global Database ADOM version	Assignable local ADOM versions
7.4	7.4, 7.2, 7.0
7.2	7.4, 7.2, 7.0
7.0	7.4, 7.2, 7.0

Example

1. A global policy package is created in the Global Database ADOM on version 7.2. The global policy package uses FortiOS 7.2 syntax.
2. The global policy package is assigned to a local ADOM using version 7.0.
3. The local ADOM contains FortiOS devices on version 7.4, 7.2 and 7.0 because these versions are all supported by the local ADOM version.
4. The administrator performs an install to these FortiGate devices from the local ADOM, and the global policy package is installed by the local ADOM.
   - When the global policy package is installed to the FOS 7.4 devices, the local ADOM upgrades the syntax.
   - When the global policy package is installed to the FOS 7.0 devices, the local ADOM downgrades the syntax.
   - When the global policy package is installed to the FOS 7.2 devices, no syntax upgrade or downgrade is required.

Upgrading Global Database ADOMs



The global database ADOM should only be upgraded after all the ADOMs that are using a global policy package have been upgraded to a supported version. See ADOM versions on page 941.

To upgrade the global database ADOM:

1. Go to *System Settings* > *ADOMs*.
2. Select *Global Database* then click *More* > *Upgrade* in the toolbar, or right-click *Global Database* and select *Upgrade*.

   If the ADOM has already been upgraded to the latest version, this option will not be available.
3. Click *OK* in the *Upgrade ADOM* dialog box.
4. After the upgrade finishes, click *Close* to close the dialog box.

To edit the global database version:

1. Go to *System Settings* > *ADOMs*.
2. Select *Global Database* then click *Edit* in the toolbar, or right-click *Global Database* and select *Edit*. The *Edit Global Database* window opens.
3. Select the version.
4. Click *OK* to save the setting.
5. A confirmation dialog box will be displayed. Click *OK* to continue.

Concurrent ADOM access

Concurrent ADOM access is controlled by enabling or disabling the workspace function. Concurrent access is enabled by default. To prevent multiple administrators from making changes to the FortiManager database at the same time and causing conflicts, the workspace function must be enabled.

When workspace mode is enabled, concurrent ADOM access is disabled. An administrator must lock the ADOM before they can make device-level changes to it, and only one administrator can hold the lock at a time, while other administrators have read-only access. Optionally, ADOM lock override can be enabled, allowing an administrator to unlock an ADOM that is locked by another administrator. See Locking an ADOM on page 947

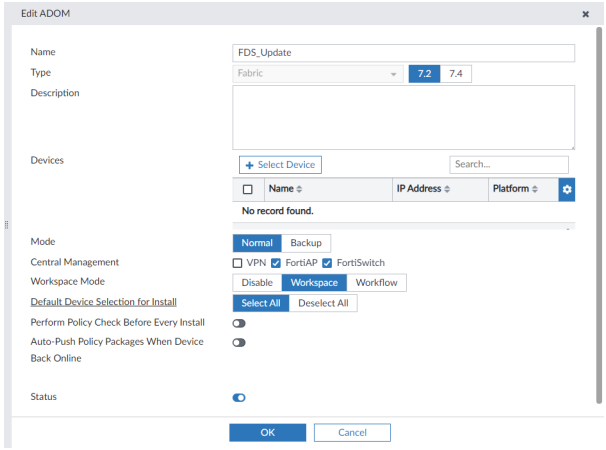
When workspace is disabled, concurrent ADOM access is enabled, and multiple administrators can log in and make changes to the same ADOM at the same time.



Workspace mode can be applied per ADOM or on all ADOMS. See Enable workspace mode on page 1019.

To enable workspace mode, and disable concurrent ADOM access:

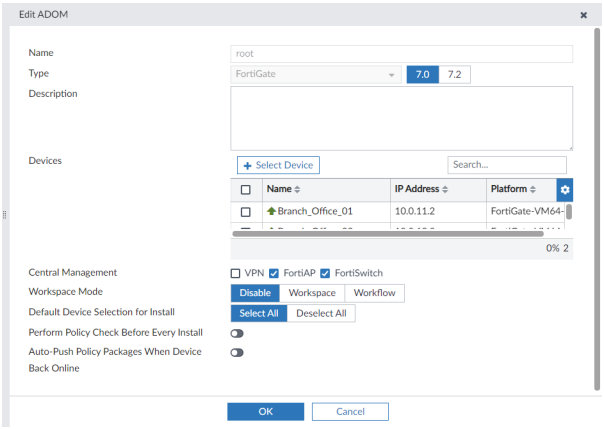
1. Go to *Systems Settings* > *ADOMs*.
2. Double-click an ADOM, or right-click the ADOM and select *Edit*. The *Edit ADOM* page is displayed.
3. In the *Workspace Mode* area, click *Workspace*.



4. Click *OK*. Concurrent mode is disabled.

To disable workspace mode, and enable concurrent ADOM access:

1. Go to *Systems Settings* > *ADOMs*.
2. Double-click an ADOM, or right-click the ADOM and select *Edit*. The *Edit ADOM* page is displayed.
3. In the *Workspace Mode* area, click *Disable*.



4. Click *OK*. Concurrent mode is enabled.

After changing the workflow mode, your session will end and you will be required to log back in to the FortiManager.

To enable workspace mode, and disable concurrent ADOM access:

```
config system global
   set workspace-mode normal
end
```

Concurrent ADOM access is disabled.

To disable workspace mode, and enable concurrent ADOM access in the CLI:

```
config system global
   set workspace-mode disabled
   Warning: disabling workspaces may cause some logged in users to lose their unsaved data. Do you
         want to continue? (y/n) y
end
```

Locking an ADOM

If workspace is enabled, you must lock an ADOM prior to making changes in Policy & Objects, AP Manager, VPN Manager, FortiSwitch Manager, and Extender Manager, as well as performing any device-level changes to a device, such as upgrading firmware for a device.

When using the FortiManager API, the ADOM does not need to be locked in order to perform device-level changes.

Policy packages, policies, objects, and devices can be individually locked. See:

- Locking a policy package on page 1024
- Lock an individual policy on page 1025
- Lock an individual object on page 1026
- Locking a device on page 1023

In the GUI, the padlock icon shown next to the ADOM name on the banner and in the *All ADOMs* list will turn green when you lock an ADOM. If it is red, it means that another administrator has locked the ADOM.

When an ADOM is locked, other administrators are unable to make changes in that ADOM until you either unlock the ADOM, or log out of the FortiManager. Optionally, ADOM lock override can be enabled, allowing an administrator to unlock an ADOM that has been locked by another administrator and discard all of their unsaved changes.

For more information about locking an ADOM, see Locking an ADOM on page 1022.

Upgrading an ADOM

To upgrade an ADOM, you must be logged in as a super user administrator.

Before upgrading your ADOM, it is recommended to backup your configuration and/or take a VM snapshot so that you can roll back changes if required.
See Creating a snapshot of VM instances and Backing up the system on page 71.

To upgrade an ADOM:

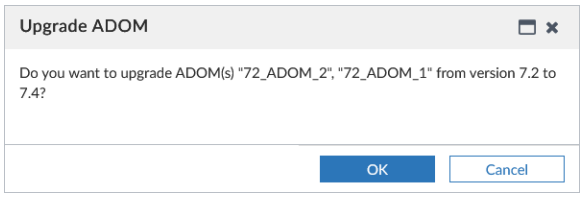
1. Go to *System Settings* > *ADOMs*.
2. Select an ADOM, and then select *More* > *Upgrade* from the toolbar.
   If the ADOM has already been upgraded to the latest version, this option will not be available.
3. Select *OK* in the confirmation dialog box to upgrade the device.

Upgrading multiple ADOMs

Multiple ADOMs of the same version can be upgraded at the same time in FortiManager. For example you can simultaneously update multiple 7.2 ADOMs to 7.4 but cannot upgrade a 6.4 and 7.2 ADOM at the same time.

To upgrade multiple ADOMs at the same time:

1. Go to *System Settings* > *ADOMs*.
2. Select multiple ADOMs of the same version in the ADOM table and do one of the following:
   a. Right-click on a selected device in the table and select *Upgrade*.
   b. Select *More* > *Upgrade* in the toolbar.
3. Select *OK* in the confirmation dialog box to upgrade the devices.



Verifying ADOM upgrade readiness

An ADOM upgrade readiness tool is available in FortiManager that can be used to check for potential issues that would prevent an ADOM's version from being upgraded. For example, you can perform a check on a 7.4 ADOM to determine if it is ready to be upgraded to ADOM version 7.6.

Each FortiManager ADOM version is aligned with a particular FortiOS syntax version. For example, the 7.6 ADOM aligns with FortiOS 7.6. syntax. The ADOM upgrade readiness tool checks if devices in the ADOM(s) have any missing or invalid configurations that are not compatible with the new FortiOS syntax version. For more information on ADOM versions, see ADOM versions on page 941

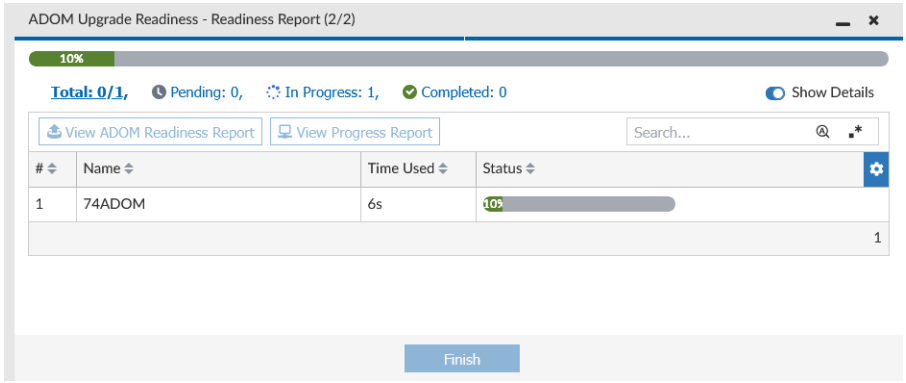
After performing the check, a report is generated that identifies any discovered issues. This report can be exported as a CSV or PDF. The ADOM readiness cannot automatically fix invalid values in ADOMs.

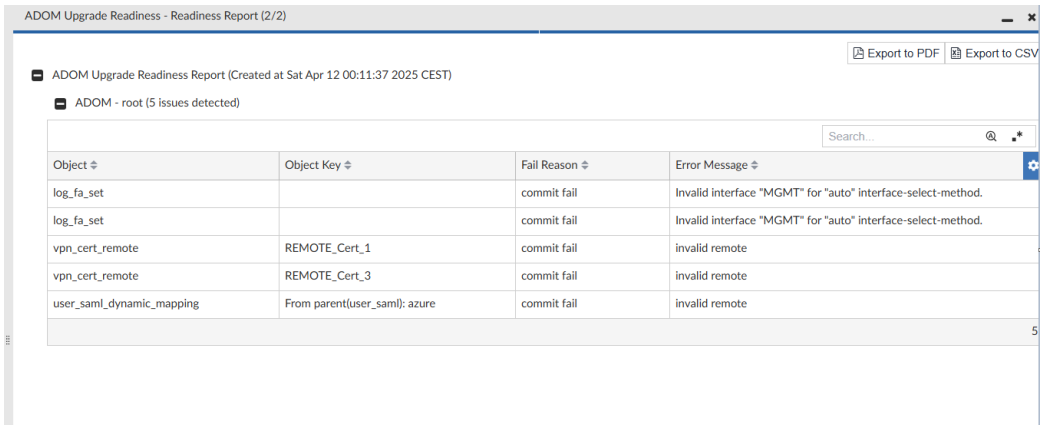
When there are no issues detected, the report will indicate that the ADOM is ready to be upgraded, and you can proceed with the upgrade. See Upgrading an ADOM on page 948.

To check an ADOM's upgrade readiness:

1. Go to *System Settings > ADOMs*.
2. In the ADOMs table, select one or more ADOMs on the same version.

   For example, you can test two 7.4 ADOMs simultaneously, but you cannot test a 7.2 and 7.4 ADOM together.
3. In the toolbar, select *More > ADOM Upgrade Readiness*.
4. Optionally, change which ADOMs will be checked by adding or removing them in the *Select ADOMs* selector.
5. Click *Next* to begin the upgrade readiness check.





FortiManager will generate an upgrade readiness report and display any detected issues. If there are no detected issues, the report will indicate that the ADOM is ready to upgrade.

6. Optionally, click *Export to PDF* or *Export to CSV* to export the report into the selected format.
7. Click *Finish*.

Using mixed versions in ADOMs

FortiManager is able to manage devices on mixed firmware versions in an ADOM. See ADOM versions on page 941.

Global Database

The Global Database contains object configurations, policy packages, and header and footer sensor configuration for IPS.

To configure Global Database components:

1. Change the ADOM to *Global Database*.
2. Configure the following Global Database components:
   - **Policy Packages**: *Policy Packages* contain packages created with objects. You can also define firewall and traffic shaping header and footer policies. For more information, see Creating policy packages on page 954.
   - **Header/Footer IPS**: *Header/Footer IPS* allows you to configure header and footer sensors for use in IPS policies. For more information, see Header/Footer IPS on page 951.
   - **Object Configurations**: You can view or create objects from the *Normalized Interface*, *Firewall Objects*, *Security Profiles*, *User & Authentication*, *Security Fabric*, *Advanced*, and *Scripts* menus. For more information, see Creating object configurations on page 950.

Creating object configurations

You can create new object configurations before including them in policy packages. Alternatively, you can also create policy packages using existing object configurations.

To create objects in Global Database:

1. Change the ADOM to *Global Database*.
2. Go to *Policy & Objects*, and select your object type from the tree menu.
3. Click *Create New* to create new objects.
4. Click *OK* after creating the objects.
5. (Optional) Additional object configuration options can be enabled in *Tools* > *Feature Visibility*.

FortiGate global objects

FortiManager supports FortiGate global objects. FortiGate global objects are identified with the prefix "*g-*".

When a FortiGate configuration using FortiGate global objects is imported into FortiManager, the global objects are added to the FortiManager as ADOM-level objects.

If FortiGate global objects (g-) are referenced in a FortiManager policy package, they are installed to the FortiGate Global VDOM and are usable in other VDOMs.

Below is a list of FortiGate global objects supported by FortiManager:

- system replacemsg-group
- system external-resource
- webfilter profile
- firewall wildcard-fqdn custom
- ips sensor
- sctp-filter profile
- application list
- dlp data-type
- dlp dictionary
- dlp sensor
- dlp profile
- webfilter search-engine
- antivirus profile
- file-filter profile
- wireless-controller utm-profile
- firewall ssh local-key
- firewall ssh local-ca
- threat feeds

For more information, see the FortiGate Administration Guide.

Header/Footer IPS

You can create new IPS headers and footers for use in Intrusion Prevention object configuration. When a IPS header/footer is created and assigned to an ADOM, all new and existing Intrusion Prevention objects in that ADOM will include the header and footer.

The Header/Footer IPS table includes the following features in the toolbar:

Create New	Create a new IPS header/footer.
Edit	Edit an existing IPS header/footer.
Delete	Delete an existing IPS header/footer.
ADOM Assignments	Specify to which ADOM(s) an IPS header/footer can be assigned.
Assign/Un-assign	Assign the IPS header/footer to one or more ADOMs. ADOMs will not appear in the *Assign/Un-assign* list unless they have first been specified using *ADOM Assignment*. When the IPS header/footer is assigned to an ADOM, all new and existing Intrusion Prevention objects within this ADOM are updated to include the IPS headers and footers.
Column Settings	Configure which columns are displayed in the Header/Footer IPS table.

To create an IPS header or footer sensor:

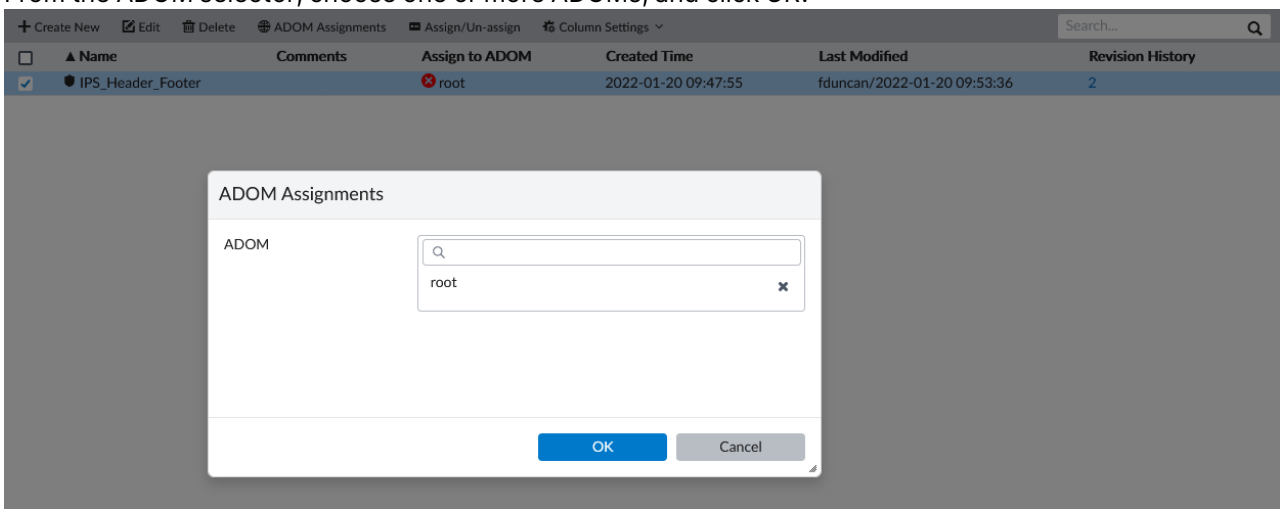
1. Change the ADOM to *Global Database*.
2. Click *Header/Footer IPS* from the navigation menu, and click *Create New*. The *Create New Header/Footer IPS Sensor* page is displayed.
3. Configure the IPS header/footer, and click *OK*. The following settings are available:

Name	Enter a name.
Comments	Optionally, enter comments about the IPS header/footer.
IPS Signatures and Filters	Click *Create new*, and select *Header IPS* or *Footer IPS* to create new IPS signatures and filters.
Filters	When creating filters, the following settings are available: *Action (Allow, Monitor, Block, Reset, Default, Quarantine)*, *Packet Logging*, *Status*, and *Filter*. Click the edit filter icon to create a new filter. For information on hold-time and CVE filter options, see Intrusion prevention hold-time and CVE filtering on page 999.
Signatures	When selecting signatures, the following settings are available: *Action (Allow, Monitor, Block, Reset, Default, Quarantine)*, *Packet Logging*, *Status*, *Rate-based Setting*, *Exempt IPs*, and *Signatures*. Click *Add Signature* to select a new signature.
Revision	Enter a change note for any changes made to the IPS header/footer sensor. Previous changes are displayed under *Revision History*.

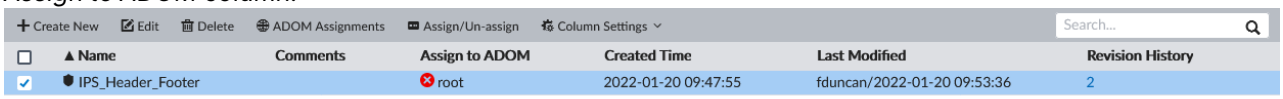
To assign an IPS header/footer to an ADOM:

1. Change the ADOM to *Global Database*.
2. Click *Header/Footer IPS* from the navigation menu, and click *ADOM Assignments*.
   ADOM Assignments determines to which ADOM(s) an IPS header/footer can be assigned.

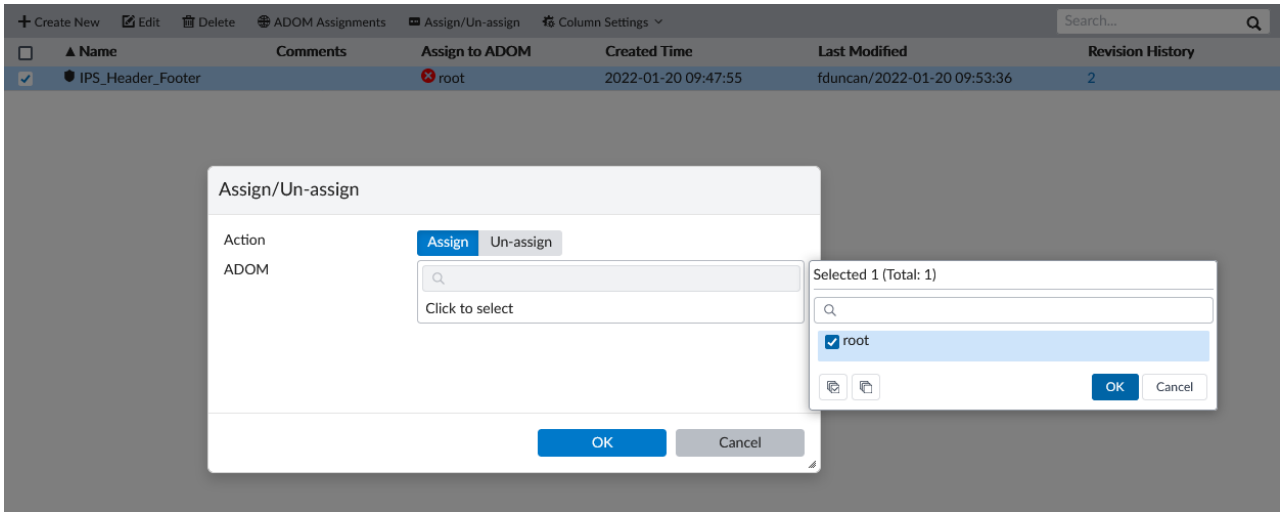
3. From the ADOM selector, choose one or more ADOMs, and click *OK*.



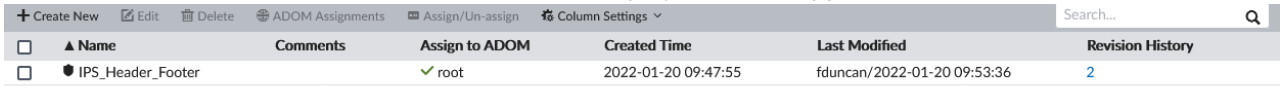
In the Header/Footer IPS table, the header/footer displays that it is not yet applied to the ADOM(s) in the *Assign to ADOM* column.



4. Click *Assign/Un-assign* in the toolbar, select the ADOM where the IPS header/footer will be assigned, and click *OK*.

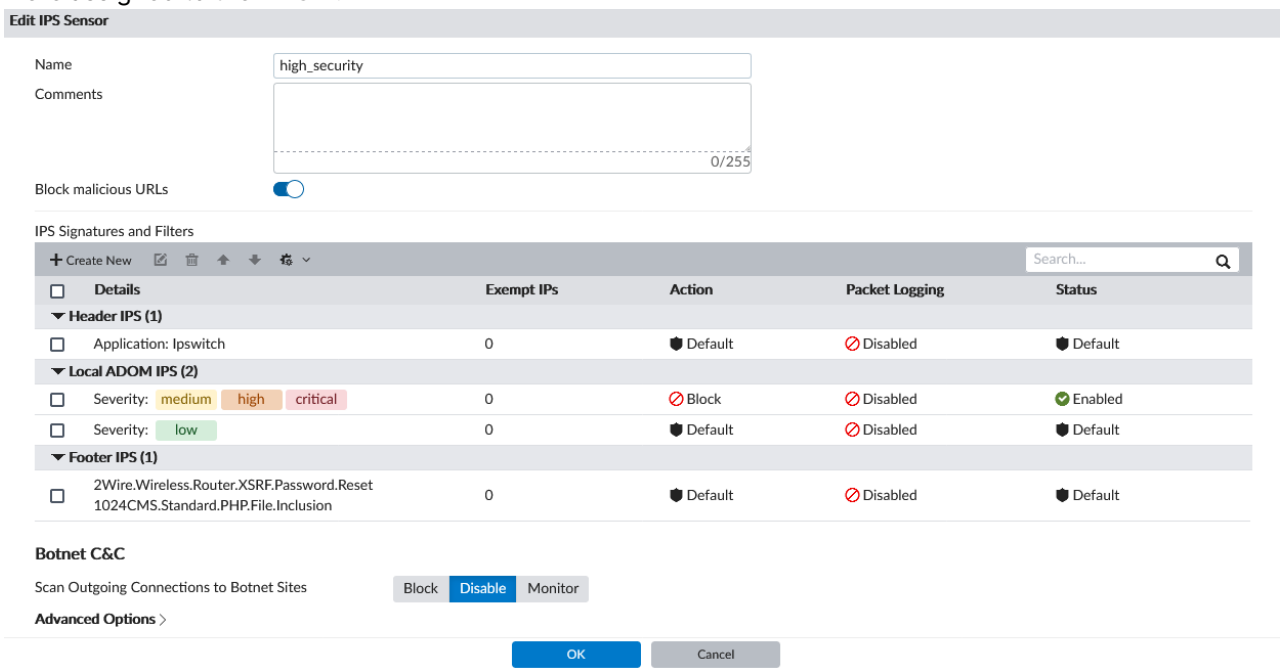


In the Header/Footer IPS table, the header/footer displays that it is applied to the selected ADOM.



5. Navigate to the ADOM where the IPS header/footer was installed, and go to *Policy & Objects* > *Security Profiles* > *Intrusion Prevention*.
All new and existing Intrusion Prevention objects within this ADOM include the IPS headers and footers that

were assigned to the ADOM.



To un-assign a global IPS header and footer from an ADOM:

1. Change the ADOM to *Global Database*.
2. Click *Header/Footer IPS* from the navigation menu, and select the IPS header/footer that you want to un-assign.
3. Click *Assign/Un-assign* in the toolbar, and select the Un-assign tab in the dialog window that appears.
4. Select the ADOMs to be un-assigned from the ADOM, and click *OK*.

Creating policy packages

Create a policy package with selected objects.



The use of local Policy Blocks simplifies the process for upgrading your ADOMs and can be considered as an alternative to Global Policy Packages. For more information, see Using Policy Blocks versus Global Policy Packages on page 525.



NGFW policy mode is not supported for global policy packages.

To create a policy package:

1. Change the ADOM to *Global Database*.
2. Click *Policy Packages*.
3. Select *Policy Package* > *New Package*.
4. Specify a name for the policy package in the *Name* field.
5. Select the folder where the policy package is to be saved. Click OK.
6. Click the newly created policy package.
7. Go to Firewall Header Policy and click Create New.
8. Configure the Firewall Header Policy and click *OK*. For more information, see Creating policies on page 429.
9. Go to Firewall Footer Policy and click Create New.
10. Configure the Firewall Footer Policy and click *OK*. For more information, see Creating policies on page 429.



Importing configs with global policies

When re-importing a managed device's configuration, global policies and objects that are installed on the device will not be re-imported, and the following error will be displayed: *The global header/footer policies will not be imported*. Global policy and objects can not be retrieved from a managed device.

When a global policy package is unassigned from a device, you must perform an install to the target device to remove the global policies and objects.

Assigning a global policy package to an ADOM

Once a global policy package is created, you can assign it to an ADOM or to specific policy packages within an ADOM. This allows the administrator for the ADOM to deploy the policy package to all devices within the ADOM.

See Assign a global policy package on page 417.

Installing policy packages on devices

You can install all policy packages which have been modified by the global policy package assignment.

See Installing policy packages and device settings on page 180

Certificates

The FortiManager generates a certificate request based on the information you entered to identify the FortiManager unit. After you generate a certificate request, you can download the request to a management computer and then forward the request to a CA.

Local certificates are issued for a specific server, or website. Generally they are very specific, and often for an internal enterprise network.

CA root certificates are similar to local certificates, however they apply to a broader range of addresses or to an entire company.

The CRL is a list of certificates that have been revoked and are no longer usable. This list includes expired, stolen, or otherwise compromised certificates. If your certificate is on this list, it will not be accepted. CRLs are maintained by the CA that issues the certificates and include the date and time when the next CRL will be issued, as well as a sequence number to help ensure you have the most current versions.

Local certificates

The FortiManager unit generates a certificate request based on the information you enter to identify the FortiManager unit. After you generate a certificate request, you can download the request to a computer that has management access to the FortiManager unit and then forward the request to a CA.

The certificate window also enables you to export certificates for authentication, importing, and viewing.

The FortiManager has one default local certificate: *Fortinet_Local*.

You can manage local certificates from the *System Settings > Certificates* page. Some options are available in the toolbar and some are also available in the right-click menu.

Creating a local certificate

To create a certificate request:

1. Go to *System Settings > Certificates*.
2. Click *Create New/Import > Generate CSR* in the toolbar. The *Generate Certificate Signing Request* pane opens.
3. Enter the following information as required, then click *OK* to save the certificate request:

Certificate Name		The name of the certificate.
Subject Information		Select the ID type from the dropdown list: • *Host IP*: Select if the unit has a static IP address. Enter the public IP address of the unit in the *Host IP* field. • *Domain Name*: Select if the unit has a dynamic IP address and subscribes to a dynamic DNS service. Enter the domain name of the unit in the *Domain Name* field. • *Email*: Select to use an email address. Enter the email address in the *Email Address* field.
Optional Information		
	Organization Unit (OU)	The name of the department. You can enter a series of OUs up to a maximum of 5. To add or remove an OU, use the plus (+) or minus (-) icons.
	Organization (O)	Legal name of the company or organization.
	Locality (L)	Name of the city or town where the device is installed.

	State/Province (ST)	Name of the state or province where the FortiGate unit is installed.
	Country (C)	Select the country where the unit is installed from the dropdown list.
	E-mail Address (EA)	Contact email address.
	Subject Alternative Name	Optionally, enter one or more alternative names for which the certificate is also valid. Separate names with a comma. A name can be: • e-mail address • IP address • URI • DNS name (alternatives to the Common Name) • directory name (alternatives to the Distinguished Name) You must precede the name with the name type. Examples: • IP:1.1.1.1 • email:test@fortinet.com • email:my@other.address • URI:http://my.url.here/
Key Type		The key type can be *RSA* or *Elliptic Curve*.
Key Size		Select the key size from the dropdown list: *512 Bit*, *1024 Bit*, *1536 Bit*, or *2048 Bit*. This option is only available when the key type is *RSA*.
Curve Name		Select the curve name from the dropdown list: *secp256r1* (default), *secp384r1*, or *secp521r1*. This option is only available when the key type is *Elliptic Curve*.
Enrollment Method		The enrollment method is set to *File Based*.

Importing local certificates

To import a local certificate:

1. Go to *System Settings* > *Certificates*.
2. Click *Create New/Import* > *Local Certificate* in the toolbar.
3. Enter the following information as required, then click *OK* to import the local certificate:

Type	Select the certificate type from the dropdown list: *Local Certificate*, *PKCS #12 Certificate*, or *Certificate*.
Certificate File	Click *Browse...* and locate the certificate file on the management computer, or drag and drop the file onto the dialog box.
Key File	Click *Browse...* and locate the key file on the management computer, or drag and drop the file onto the dialog box. This option is only available when *Type* is *Certificate*.

Password	Enter the certificate password. This option is only available when *Type* is *PKCS #12 Certificate* or *Certificate*.
Certificate Name	Enter the certificate name. This option is only available when *Type* is *PKCS #12 Certificate* or *Certificate*.

Deleting local certificates

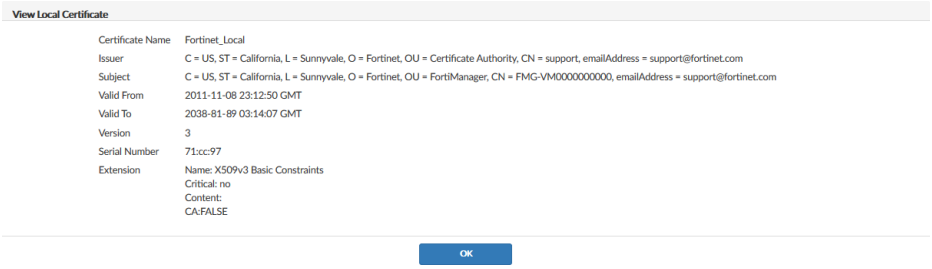
To delete a local certificate or certificates:

1. Go to *System Settings* > *Certificates*.
2. Select the certificate or certificates you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected certificate or certificates.

Viewing details of local certificates

To view details of a local certificate:

1. Go to *System Settings* > *Certificates*.
2. Select the certificates that you would like to see details about, then click *View Certificate Detail* in the toolbar or right-click menu. The *View Local Certificate* page opens.



3. Click *OK* to return to the local certificates list.

Downloading local certificates

To download a local certificate:

1. Go to *System Settings* > *Certificates*.
2. Select the certificate that you need to download.
3. Click *Download* in the toolbar, or right-click and select *Download*, and save the certificate to the management computer.



When an object is added to a policy package and assigned to an ADOM, the object is available in all devices that are part of the ADOM. If the object is renamed on a device locally, FortiManager automatically syncs the renamed object to the ADOM.

CA certificates

The FortiManager has one default CA certificate, *Fortinet_CA*. In this sub-menu you can delete, import, view, and download certificates.

Importing CA certificates

To import a CA certificate:

1. Go to *System Settings* > *Certificates*.
2. Click *Create New/Import* > *CA Certificate* in the toolbar.
3. Click *Browse...* and locate the certificate file on the management computer, or drag and drop the file onto the dialog box.
4. Click *OK* to import the certificate.

Viewing CA certificate details

To view a CA certificate's details:

1. Go to *System Settings* > *Certificates*.
2. Select the certificates you need to see details about.
3. Click *View Certificate Detail* in the toolbar, or right-click and select *View Certificate Detail*. The *View CA Certificate* page opens.
4. Click *OK* to return to the CA certificates list.

Downloading CA certificates

To download a CA certificate:

1. Go to *System Settings* > *Certificates*.
2. Select the certificate you need to download.
3. Click *Download* in the toolbar, or right-click and select *Download*, and save the certificate to the management computer.

Deleting CA certificates

To delete a CA certificate or certificates:

1. Go to *System Settings* > *Certificates*.
2. Select the certificate or certificates you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected certificate or certificates.



The *Fortinet_CA* certificate cannot be deleted.

Certificate revocation lists

When you apply for a signed personal or group certificate to install on remote clients, you can obtain the corresponding root certificate and Certificate Revocation List (CRL) from the issuing CA.

The CRL is a list of certificates that have been revoked and are no longer usable. This list includes expired, stolen, or otherwise compromised certificates. If your certificate is on this list, it will not be accepted. CRLs are maintained by the CA that issues the certificates and includes the date and time when the next CRL will be issued as well as a sequence number to help ensure you have the most current version of the CRL.

When you receive the signed personal or group certificate, install the signed certificate on the remote client(s) according to the browser documentation. Install the corresponding root certificate (and CRL) from the issuing CA on the FortiManager unit according to the procedures given below.

Importing a CRL

To import a CRL:

1. Go to *System Settings* > *Certificates*.
2. Click *Create New/Import* > *CRL* in the toolbar.
3. Click *Browse...* and locate the CRL file on the management computer, or drag and drop the file onto the dialog box.
4. Click *OK* to import the CRL.

Viewing a CRL

To view a CRL:

1. Go to *System Settings* > *Certificates*.
2. Select the CRL you need to see details about.
3. Click *View Certificate Detail* in the toolbar, or right-click and select *View Certificate Detail*. The *Result* page opens.
4. Click *OK* to return to the CRL list.

Deleting a CRL

To delete a CRL or CRLs:

1. Go to *System Settings* > *Certificates*.
2. Select the CRL or CRLs you need to delete.

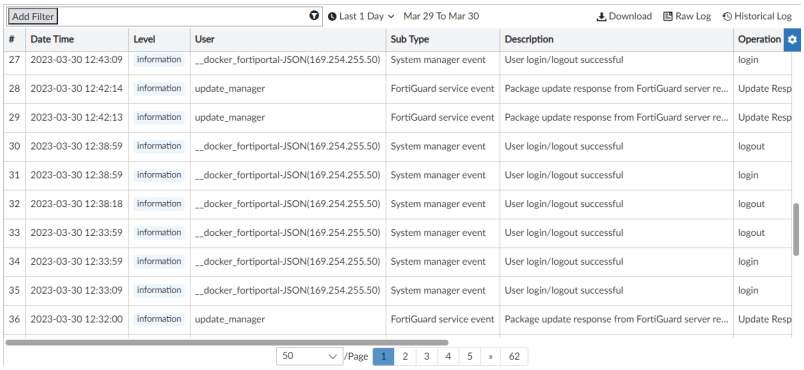
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected CRL or CRLs.

Event Log

The *Event Log* pane provides an audit log of actions made by users on FortiManager. It allows you to view log messages that are stored in memory or on the internal hard disk drive. You can use filters to search the messages and download the messages to the management computer.

See the *FortiManager Log Message Reference*, available from the Fortinet Document Library, for more information about the log messages.

Go to *System Settings* > *Event Log* to view the local log list.



The following options are available:

Last...	Select the amount of time to show from the available options, or select a custom time span or any time.
Add Filter	Filter the event log list based on the log level, user, sub type, or message. See Event log filtering on page 962.
Download	Download the event logs in either CSV or the normal format to the management computer.
Raw Log / Formatted Log	Click on *Raw Log* to view the logs in their raw state. Click *Formatted Log* to view them in the formatted into a table.
Historical Log	Click to view the historical logs list.
Back	Click the back icon to return to the regular view from the historical view.
View	View the selected log file. This option is also available from the right-click menu, or by double-clicking on the log file. This option is only available when viewing historical event logs.
Delete	Delete the selected log file. This option is also available from the right-click menu. This option is only available when viewing historical event logs.

Clear	Clear the selected file of logs. This option is also available from the right-click menu. This option is only available when viewing historical event logs.
Type	Select the type from the dropdown list: • Event Log • FDS Upload Log: Select the device from the dropdown list. • FDS Download Log: Select the service (FDS or FCT) from the *Service* dropdown list, select the event type (*All Event*, *Push Update*, *Poll Update*, or *Manual Update*) from the Event dropdown list, and then click *Go* to browse the logs. This option is only available when viewing historical logs.
Search	Enter a search term to search the historical logs. This option is only available when viewing historical event logs.
Pagination	Browse the pages of logs and adjust the number of logs that are shown per page.

The following information is shown:

#	The log number.
Date/Time	The date and time that the log file was generated.
Level	The severity level of the message. For a description of severity levels, see the Log Message Reference.
User	The user that the log message relates to.
Sub Type	The event log subtype. For a description of the subtypes for event logs, see the Log Message Reference.
Description	A description of the event.
Operation	The change or operation that triggered the event.
Performed On	Entity affected by the change or operation. For example, when you log out of the FortiManager GUI, the operation is performed on the local FortiManager GUI.
Changes	Details of the change.
Message	Log message details. A *Session ID* is added to each log message. The *username* of the administrator is added to log messages wherever applicable for better traceability.

Event log filtering

The event log can be filtered using the *Add Filter* box in the toolbar.

To filter event log results using the toolbar:

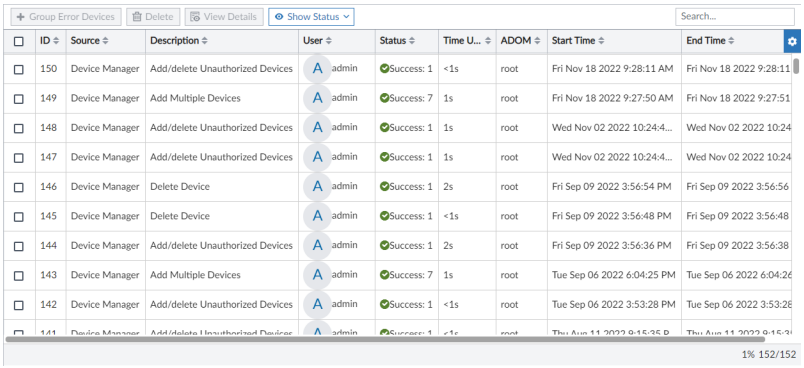
1. Specify filters in the *Add Filter* box.
   - **Filter mode**: Click in the *Add Filter* box, select a filter from the dropdown list, then type a value.
   - **Text Mode**: Click the *Switch to Text Mode* icon at the right end of the *Add Filter* box to switch to text mode. In this mode, you can type in the whole search criteria.
     Click the *Switch to Filter Mode* icon to return to filter mode.
2. Click *Go* to apply the filter.

Task Monitor

Use the task monitor to view the status of the tasks you have performed.

Go to *System Settings* > *Task Monitor* to view the task monitor. The task list size can also be configured; see Miscellaneous Settings on page 973.

To filter the information in the monitor, enter a text string in the search field.



The following options are available:

Group Error Devices	Create a group of the failed devices, allowing for re-installations to be done only on the failed devices.
Delete	Remove the selected task or tasks from the list. This changes to *Cancel Running Task(s)* when *View* is *Running*.
View Task Detail	View the task *Index*, *Name*, *Status*, *Time Used*, and *History*, in a new window. Click the icons in the *History* column to view the following information: • History • Promotion of device in FortiManager with autolink • Upgrade remote device firmware • Retrieve remote device configuration • Installation of device templates • Installation of policy packages • Execution of additional scripts

	To filter the information in the task details, enter a text string in the search field. This can be useful when troubleshooting warnings and errors.
Show Status	Select which tasks to view from the dropdown list, based on their status. The available options are: *All*, *Pending*, *Running*, *Canceling*, *Canceled* , *Done*, *Error*, *Aborting*, *Aborted*, and *Warning*.
Column Settings	Select the columns you want to display from the dropdown.

The following information is available:

ID	The identification number for a task.
Source	The platform from where the task is performed.
Description	The nature of the task. Double-click the task to display the specific actions taken under this task.
User	The user or users who performed the tasks.
Status	The status of the task: • *Success*: Completed with success. • *Error*: Completed without success. • *Canceled*: User canceled the task. • *Canceling*: User is canceling the task. • *Aborted*: The FortiManager system stopped performing this task. • *Aborting*: The FortiManager system is stopping performing this task. • *Running*: Being processed. In this status, a percentage bar appears in the Status column. • *Pending* • *Warning*
Time Used	The number of seconds to complete the task.
ADOM	The ADOM associated with the task.
Start Time	The time that the task was started.
End Time	The time that the task was completed.

Mail Server

A mail server allows the FortiManager to sent email messages, such as notifications when reports are run or specific events occur. Mail servers can be added, edited, deleted, and tested.

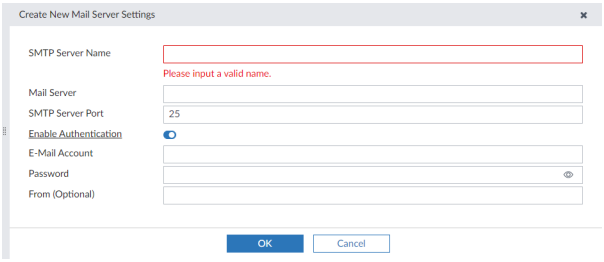
Go to System *Settings* > *Advanced* > *Mail Server* to configure SMTP mail server settings.



If an existing mail server is in use, the delete icon is removed and the mail server entry cannot be deleted.

To add a mail server:

1. Go to *System Settings* > *Advanced* > *Mail Server*.
2. Click *Create New* in the toolbar. The *Create New Mail Server Settings* pane opens.



3. Configure the following settings and then select *OK* to create the mail server.

SMTP Server Name	Enter a name for the SMTP server.
Mail Server	Enter the mail server information.
SMTP Server Port	Enter the SMTP server port number. The default port is 25.
Enable Authentication	Enable or disable authentication.
Email Account	Enter an email account. This option is only accessible when authentication is enabled.
Password	Enter the email account password. This option is only accessible when authentication is enabled.
From (Optional)	Optionally, set the default username for sending.

To edit a mail server:

1. Go to *System Settings* > *Advanced* > *Mail Server*.
2. Double-click on a server, right-click on a server and then select *Edit* from the menu, or select a server then click *Edit* in the toolbar. The *Edit Mail Server Settings* pane opens.
3. Edit the settings as required, and then click *OK* to apply the changes.

To test the mail server:

1. Go to *System Settings* > *Advanced* > *Mail Server*.
2. Select the server you need to test.
3. Click *Test* from the toolbar, or right-click and select *Test*.
4. Type the email address you would like to send a test email to and click *OK*. A confirmation or failure message will be displayed.
5. Click *OK* to close the confirmation dialog box.

To delete a mail server or servers:

1. Go to *System Settings* > *Advanced* > *Mail Server*.
2. Select the server or servers you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.

4. Click *OK* in the confirmation box to delete the server.

Syslog Server

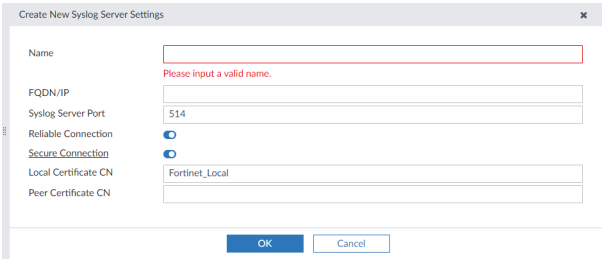
Go to *System Settings* > *Advanced* > *Syslog Server* to configure syslog server settings. Syslog servers can be added, edited, deleted, and tested.

After adding a syslog server, you must also enable FortiManager to send local logs to the syslog server. See Send local logs to syslog server on page 967.

If an existing syslog server is in use, the delete icon is removed and the server entry cannot be deleted.

To add a syslog server:

1. Go to *System Settings* > *Advanced* > *Syslog Server*.
2. Click *Create New* in the toolbar. The *Create New Syslog Server Settings* pane opens.



3. Configure the following settings and then select *OK* to create the syslog server.

Name	Enter a name for the syslog server.
IP address (or FQDN)	Enter the IP address or FQDN of the syslog server. FortiManager supports IPv4 and IPv6 addresses.
Syslog Server Port	Enter the syslog server port number. The default port is 514.
Reliable Connection	Enable or disable a reliable connection with the syslog server. The default is *disable*.
Secure Connection	Enable/disable connection secured by TLS/SSL. The default is *disable*. This option is only available when *Reliable Connection* is enabled.
Local Certificate CN	Enter one of the available local certificates used for secure connection: *Fortinet_Local* or *Fortinet_Local2*. The default is *Fortinet_Local*. This option is only available when *Secure Connection* is enabled.
Peer Certificate CN	Enter the certificate common name of syslog server. Null means no certificate CN for the syslog server. This option is only available when *Secure Connection* is enabled.

To edit a syslog server:

1. Go to *System Settings* > *Advanced* > *Syslog Server*.
2. Double-click on a server, right-click on a server and then select *Edit* from the menu, or select a server then click *Edit* in the toolbar. The *Edit Syslog Server Settings* pane opens.
3. Edit the settings as required, and then click *OK* to apply the changes.

To test the syslog server:

1. Go to *System Settings* > *Advanced* > *Syslog Server*.
2. Select the server you need to test.
3. Click *Test* from the toolbar, or right-click and select *Test*.
   A confirmation or failure message will be displayed.

To delete a syslog server or servers:

1. Go to *System Settings* > *Advanced* > *Syslog Server*.
2. Select the server or servers you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation box to delete the server or servers.

Send local logs to syslog server

After adding a syslog server to FortiManager, the next step is to enable FortiManager to send local logs to the syslog server. See Syslog Server on page 966.

You can only enable these settings by using the CLI.

```
config system locallog syslogd setting
   set severity information
   set status enable
   set syslog-name <syslog server name>
end
```

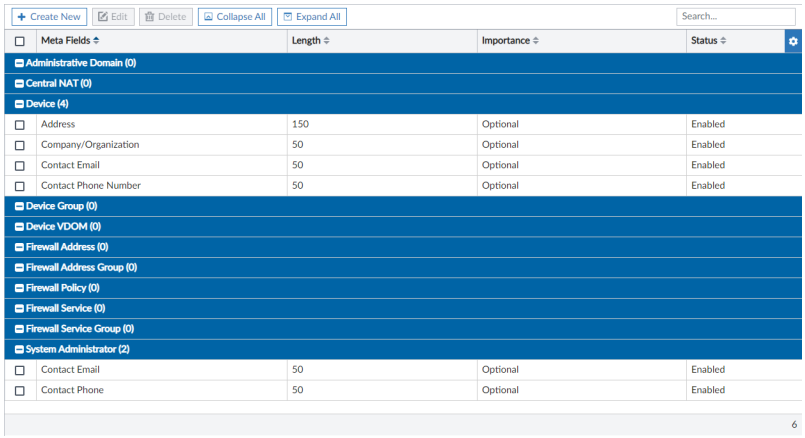
Meta Fields

Meta fields allow administrators to add additional attributes to objects and administrators. You can make meta fields required or optional.

When meta fields are required, administrators must supply additional information when they create an associated object. For example, if you create a required meta field for a device object, administrators must define a value for that meta field for all devices.

Go to *System Settings* > *Advanced* > *Meta Fields* to configure meta fields. Meta fields can be added, edited, and deleted.

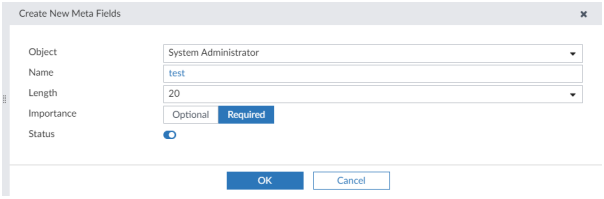
Meta fields cannot be used as variables in scripts or provisioning templates. Instead, you can use ADOM-level metadata variables which can be created in *Policy & Objects*. See ADOM-level metadata variables on page 557.



Select *Expand All* or *Collapse All* from the toolbar or right-click menu to view all or none of the meta fields under each object.

To create a new meta field:

1. Go to *System Settings* > *Advanced* > *Meta Fields*.
2. Click *Create New* in the toolbar. The *Create New Meta Field* pane opens.



3. From the *Object* field, select an object.
   Some objects also allow you to define a value for the meta field for each device.

Object	The object this metadata field applies to: *Administrative Domain*, *Central NAT*, *Device*, *Device Group*, *Device VDOM*, *Firewall Address*, *Firewall Address Group*, *Firewall Policy*, *Firewall Service*, *Firewall Service Group*, or *System Administrator*.

4. Configure the following settings:

Name	Enter the label to use for the field. When you type the name, a variable name is automatically created.
Length	Select the maximum number of characters allowed for the field from the dropdown list: *20*, *50*, or *255*.
Importance	Select *Required* to make the field compulsory; otherwise, select *Optional*.

Status	Disable/enable the field. The default selection is *Enabled*. This field is only available for non-firewall objects.

5. Click *OK*.
   The meta field is created.

To edit a meta field:

1. Go to *System Settings* > *Advanced* > *Meta Fields*.
2. Double-click on a field, right-click on a field and then select *Edit* from the menu, or select a field then click *Edit* in the toolbar. The *Edit Meta Fields* pane opens.
3. Edit the settings as required, and then click *OK* to apply the changes.



The *Object* and *Name* fields cannot be edited.

To delete a meta field or fields:

1. Go to *System Settings* > *Advanced* > *Meta Fields*.
2. Select the field or fields you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation box to delete the field or fields.



The default meta fields cannot be deleted.

Device logs

The FortiManager allows you to log system events to disk. You can control device log file size and the use of the FortiManager unit's disk space by configuring log rolling and scheduled uploads to a server.

As the FortiManager unit receives new log items, it performs the following tasks:

- Verifies whether the log file has exceeded its file size limit.
- Checks to see if it is time to roll the log file if the file size is not exceeded.

When a current log file (`tlog.log`) reaches its maximum size, or reaches the scheduled time, the FortiManager unit rolls the active log file by renaming the file. The file name will be in the form of `xlog.N.log` (for example, `tlog.1252929496.log`), where `x` is a letter indicating the log type and `N` is a unique number corresponding to the time the first log entry was received. The file modification time will match the time when the last log was received in the log file.

Once the current log file is rolled into a numbered log file, it will not be changed. New logs will be stored in the new current log called `tlog.log`. If log uploading is enabled, once logs are uploaded to the remote server or downloaded via the GUI, they are in the following format:

```
FG3K6A3406600001-tlog.1252929496.log-2017-09-29-08-03-54.zst
```

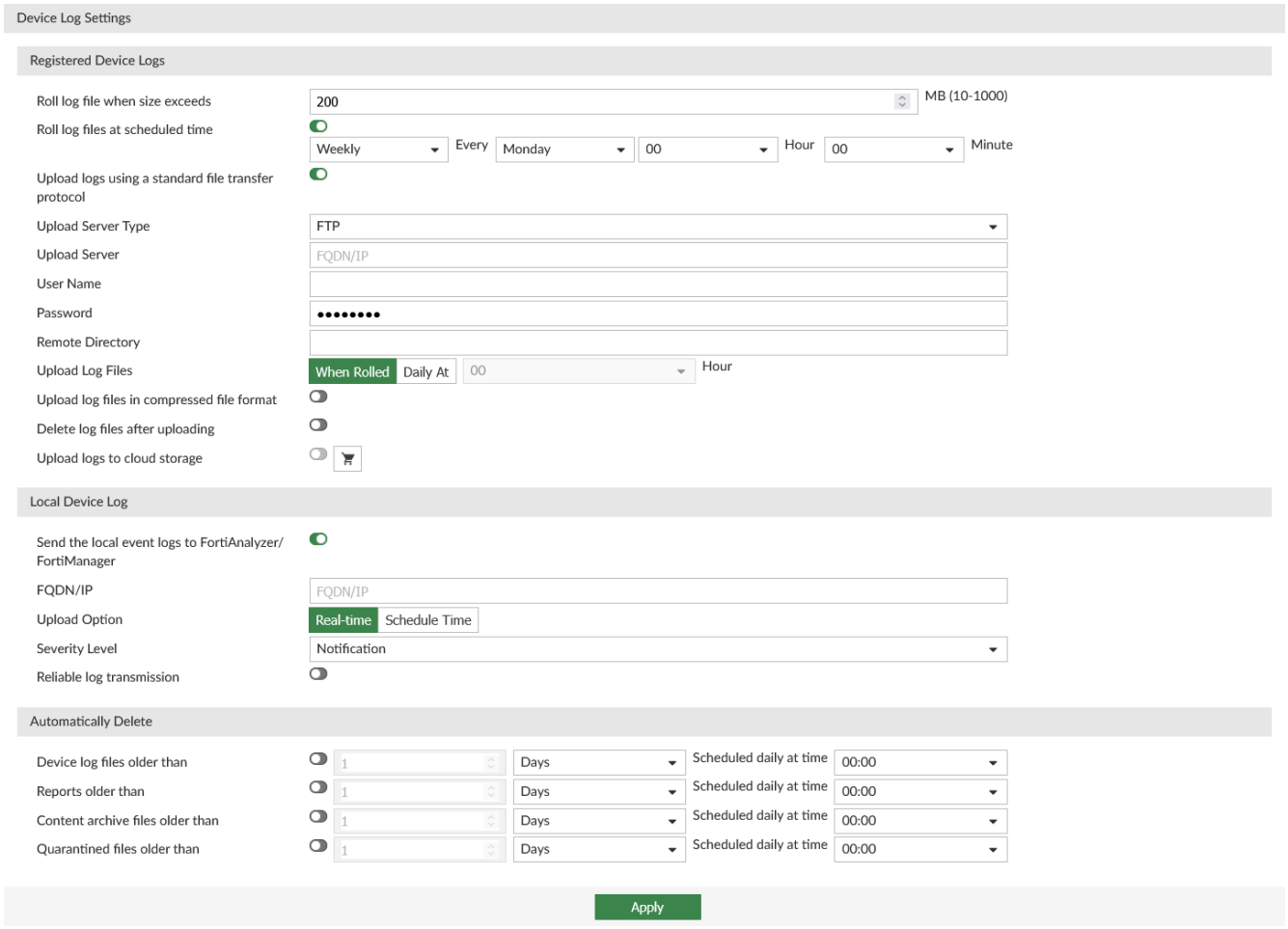
If you have enabled log uploading, you can choose to automatically delete the rolled log file after uploading, thereby freeing the amount of disk space used by rolled log files. If the log upload fails, such as when the FTP server is unavailable, the logs are uploaded during the next scheduled upload.

Log rolling and uploading can be enabled and configured using the GUI or CLI.

This pane is only available when the FortiAnalyzer features are manually enabled. For more information, see FortiAnalyzer Features on page 41.

Configuring rolling and uploading of logs using the GUI

Go to *System Settings* > *Advanced* > *Device Log Setting* to configure device log settings.



Configure the following settings, and then select *Apply*:

Registered Device Logs	
Roll log file when size exceeds	Enter the log file size, from 10 to 500MB. Default: 200MB.
Roll log files at scheduled time	Select to roll logs daily or weekly. • *Daily*: select the hour and minute value in the dropdown lists. • *Weekly*: select the day, hour, and minute value in the dropdown lists.
Upload logs using a standard file transfer protocol	Select to upload logs and configure the following settings.
Upload Server Type	Select one of *FTP*, *SFTP*, or *SCP*.
Upload Server IP	Enter the IP address of the upload server.
User Name	Enter the username used to connect to the upload server.
Password	Enter the password used to connect to the upload server.
Remote Directory	Enter the remote directory on the upload server where the log will be uploaded.
Upload Log Files	Select to upload log files when they are rolled according to settings selected under *Roll Logs*, or daily at a specific hour.
Upload rolled files in compressed file format	Select to compress the logs before uploading. This will result in smaller logs and faster upload times.
Delete files after uploading	Select to remove device log files from the FortiManager system after they have been uploaded to the Upload Server.
Local Device Log	
Send the local event logs to FortiAnalyzer / FortiManager	Select to send local event logs to another FortiAnalyzer or FortiManager device.
IP Address	Enter the IP address of the FortiAnalyzer or FortiManager.
Upload Option	Select to upload logs in real time or at a scheduled time. When selecting a scheduled time, you can specify the hour and minute to upload logs each day.
Severity Level	Select the minimum log severity level from the dropdown list. This option is only available when *Upload Option* is *Realtime*.
Reliable log transmission	Select to use reliable log transmission.
Secure connection	Select to use a secure connection for log transmission. This option is only available when *Reliable log transmission* is selected.
Peer Certificate CN	Enter the certificate common name of syslog server. Null means no certificate CN for the syslog server.

	This option is only available when *Reliable log transmission* is enabled.
Automatically Delete	
	In the following settings, the time period you select determines how often the item is checked. If you select *Months*, then the item is checked once per month. If you select *Weeks*, then the item is checked once per week, and so on. For example, if you specify *Device log files older than 3 Months*, then on July 1, the logs for April, May, and June are kept and the logs for March and older are deleted.
Device log files older than	Select to enable automatic deletion of compressed log files. Enter a value in the text field, select the time period (*Days*, *Weeks*, or *Months*), and choose a time of day.
Reports older than	Select to enable automatic deletion of reports of data from compressed log files. Enter a value in the text field, select the time period, and choose a time of day.
Content archive files older than	Select to enable automatic deletion of IPS and DP archives from Archive logs. Enter a value in the text field, select the time period, and choose a time of day.
Quarantined files older than	Select to enable automatic deletion of compressed log files of quarantined files. Enter a value in the text field, select the time period, and choose a time of day.

Configuring rolling and uploading of logs using the CLI

Log rolling and uploading can be enabled and configured using the CLI. For more information, see the *FortiManager CLI Reference*.

Enable or disable log file uploads

Use the following CLI commands to enable or disable log file uploads.

To enable log uploads:

```
config system log settings
   config rolling-regular
      set upload enable
   end
```

To disable log uploads:

```
config system log settings
   config rolling-regular
      set upload disable
   end
```

Roll logs when they reach a specific size

Use the following CLI commands to specify the size, in MB, at which a log file is rolled.

To roll logs when they reach a specific size:

```
config system log settings
   config rolling-regular
      set file-size <integer>
   end
```

Roll logs on a schedule

Use the following CLI commands to configure rolling logs on a set schedule, or never.

To disable log rolling:

```
config system log settings
   config rolling-regular
      set when none
   end
```

To enable daily log rolling:

```
config system log settings
   config rolling-regular
      set upload enable
      set when daily
      set hour <integer>
      set min <integer>
   end
```

To enable weekly log rolling:

```
config system log settings
   config rolling-regular
      set when weekly
      set days {mon | tue | wed | thu | fri | sat | sun}
      set hour <integer>
      set min <integer>
   end
```

Miscellaneous Settings

Go to *System Settings* > *Advanced* > *Misc Settings* to view and configure advanced settings and download WSDL files.

Configure the following settings and then select *Apply*:

Offline Mode	Enabling *Offline Mode* shuts down the protocol used to communicate with managed devices. This allows you to configure, or troubleshoot, the FortiManager without affecting managed devices.The FortiManager cannot automatically connect to a FortiGate if offline mode is enabled.
ADOM Mode	Select the ADOM mode, either *Normal* or *Advanced*. Advanced mode will allow you to assign a VDOM from a single device to a different ADOM, but will result in more complicated management scenarios. It is recommended only for advanced users.  Advanced ADOM mode cannot be enabled when a remote FortiAnalyzer is being managed by FortiManager.
Download WSDL file	Select the required WSDL functions then click the *Download* button to download the WSDL file to your management computer. When selecting *Legacy Operations*, no other options can be selected. Web services is a standards-based, platform independent, access method for other hardware and software APIs. The file itself defines the format of commands the FortiManager will accept as well as the responses to expect. Using the WSDL file, third-party or custom applications can communicate with the FortiManager unit and operate it or retrieve information, just as an administrator can from the GUI or CLI.
Chassis Management	Enable chassis management, then enter the chassis update interval, from 4 to 1440 minutes. Default: 15 minutes.
Configuration Changes Received from FortiGate	Select to either automatically accept changes (default) or to prompt the administrator to accept the changes.
Task List Size	Set a limit on the size of the task list. Default: 2000.
Verify Installation	Configure settings for installation verification. When FortiManager performs install verification, it compares the install script pushed to the target FortiGate with the post-install configuration returned by the FortiGate.

Disable	Installation verification is disabled.
Enable	Verification is always performed during the installation process (default).
Optimal	Verification is only performed when command errors are returned by the target FortiGate while the FortiManager is pushing the install script. If the FortiGate accepts the configuration without errors, verification does not occur. This setting is only available through the CLI.

	To configure installation verification through the CLI:
	
	`config system dm`
	`  set verify-install {disable | enable | optimal}`
	`end`

Allow Install Interface Policy Only	Select to manage and install only interface based policies, instead of all device and policy configuration.
Display Device/Group tree view in Device Manager	Enable to display devices and groups within a single tree menu and include *Add Device* and *Install Wizard* commands in the right-click menu.
Display Policy & Objects in Dual Pane	Enable to display both the *Policy Packages* and *Object Configurations* tabs on a single pane in the *Policy & Objects* module. See Feature visibility on page 413.
Use Web Proxy	If the FortiManager system's built-in FDS must connect to the FDN through a web (HTTP or HTTPS) proxy, you can specify the IP address and port of the proxy server. See Enabling updates through a web proxy on page 832.

Administrators

The *System Settings* administrator menus enable you to configure administrator accounts, access profiles, remote authentication servers, and adjust global administrative settings for the FortiManager unit.

Administrator accounts are used to control access to the FortiManager unit. Local and remote authentication is supported, as well as two-factor authentication. Administrator profiles define different types of administrators and the level of access they have to the FortiManager unit, as well as its authorized devices.

If you use ServiceNow apps for FortiManager, we recommend creating an account to use for integration with the app. This account does not need to be a Super_User account and you don't need to set trusted hosts for this account.

Global administration settings, such as the GUI language and password policies, can be configured on the *Admin Settings* pane. See Global administration settings on page 1051 for more information.

In workflow mode, approval matrices can be create and managed on the *Approval Matrix* pane. See Workflow approval on page 1029 for more information.

This section contains the following topics:

- Trusted hosts on page 976
- Monitoring administrators on page 977
- Disconnecting administrators on page 977
- Managing administrator accounts on page 977
- Administrator profiles on page 1010
- Authentication on page 1037
- Global administration settings on page 1051
- Multi-factor authentication on page 1060

Trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative permissions. In addition to knowing the password, an administrator must connect only through the subnet or subnets you specify. You can even restrict an administrator to a single IP address if you define only one trusted host IP address with a netmask of 255.255.255.255.

When you set trusted hosts for all administrators, the FortiManager unit does not respond to administrative access attempts and cannot be pinged from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply to both the GUI and to the CLI when accessed through SSH. CLI access through the console connector is not affected.



If you set trusted hosts and want to use the Console Access feature of the GUI, you must also set 127.0.0.1/255.255.255.255 as a trusted host.

Monitoring administrators

The *Admin Session List* lets you view a list of administrators currently logged in to the FortiManager unit.

To view logged in administrators:

1. Go to *Dashboard*.
2. In the *System Information* widget, in the *Current Administrators* field, click the *Current Session List* button.
   The *Admin Session List* opens in the widget.
   The following information is available:

User Name	The name of the administrator account. Your session is indicated by *(current)*.
IP Address	The IP address where the administrator is logging in from. This field also displays the logon type (GUI, jsconsole, or SSH).
Start Time	The date and time the administrator logged in.
Time Out (mins)	The maximum duration of the session in minutes (1 to 480 minutes).

Disconnecting administrators

Administrators can be disconnected from the FortiManager unit from the *Admin Session List*.

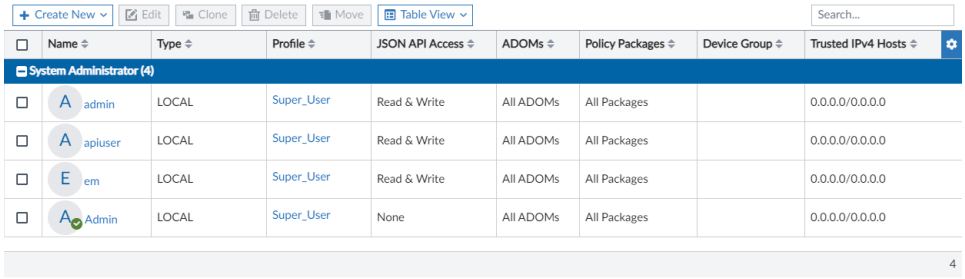
To disconnect administrators:

1. Go to *Dashboard*.
2. In the *System Information* widget, in the *Current Administrators* field, click the *Current Session List* button.
   The *Admin Session List* opens in the widget.
3. Select the administrator or administrators you need to disconnect.
4. Click *Delete* in the toolbar, or right-click and select *Delete*.
   The selected administrators will be automatically disconnected from the FortiManager device.

Managing administrator accounts

Go to *System Settings* > *Administrators* to view the list of administrators and manage administrator accounts.

Only administrators with the *Super_User* profile can see the complete administrators list. If you do not have certain viewing permissions, you will not see the administrator list. When ADOMs are enabled, administrators can only access the ADOMs they have permission to access.



The following options are available:

Create New	Create a new administrator. See Creating administrators on page 979.
Edit	Edit the selected administrator. See Editing administrators on page 984.
Clone	Clone the selected administrator.
Move	Move the adminstrator to a different sequence in the table.
Delete	Delete the selected administrator or administrators. See Deleting administrators on page 985.
Table View/Tile View	Change the view of the administrator list. Table view shows a list of the administrators in a table format. Tile view shows a separate card for each administrator in a grid pattern.
Column Settings	Change the displayed columns.
Search	Search the administrators.
Change Password	Change the selected administrator's password. This option is only available from the right-click menu. See Editing administrators on page 984.

The following columns are available:

#	The sequence number.
Name	The name the administrator uses to log in.
Type	The user type, as well as if the administrator uses a wildcard.
Profile	The profile applied to the administrator. See Administrator profiles on page 1010 If a profile is applied per-ADOM for the administrator, they are listed as *ADOM:profile*.
JSON API Access	The administrators read/write privileges for JSON API.
ADOMs	The ADOMs the administrator has access to or is excluded from.
Policy Packages	The policy packages the administrator can access.

Comments	Comments about the administrator account. This column is hidden by default.
Trusted IPv4 Hosts	The IPv4 trusted host(s) associated with the administrator. See Trusted hosts on page 976.
Trusted IPv6 Hosts	The IPv6 trusted host(s) associated with the administrator. See Trusted hosts on page 976. This column is hidden by default.
Contact Email	The contact email associated with the administrator. This column is hidden by default.
Contact Phone	The contact phone number associated with the administrator. This column is hidden by default.

Creating administrators

To create a new administrator account, you must be logged in as a super user administrator.

You need the following information to create an account:

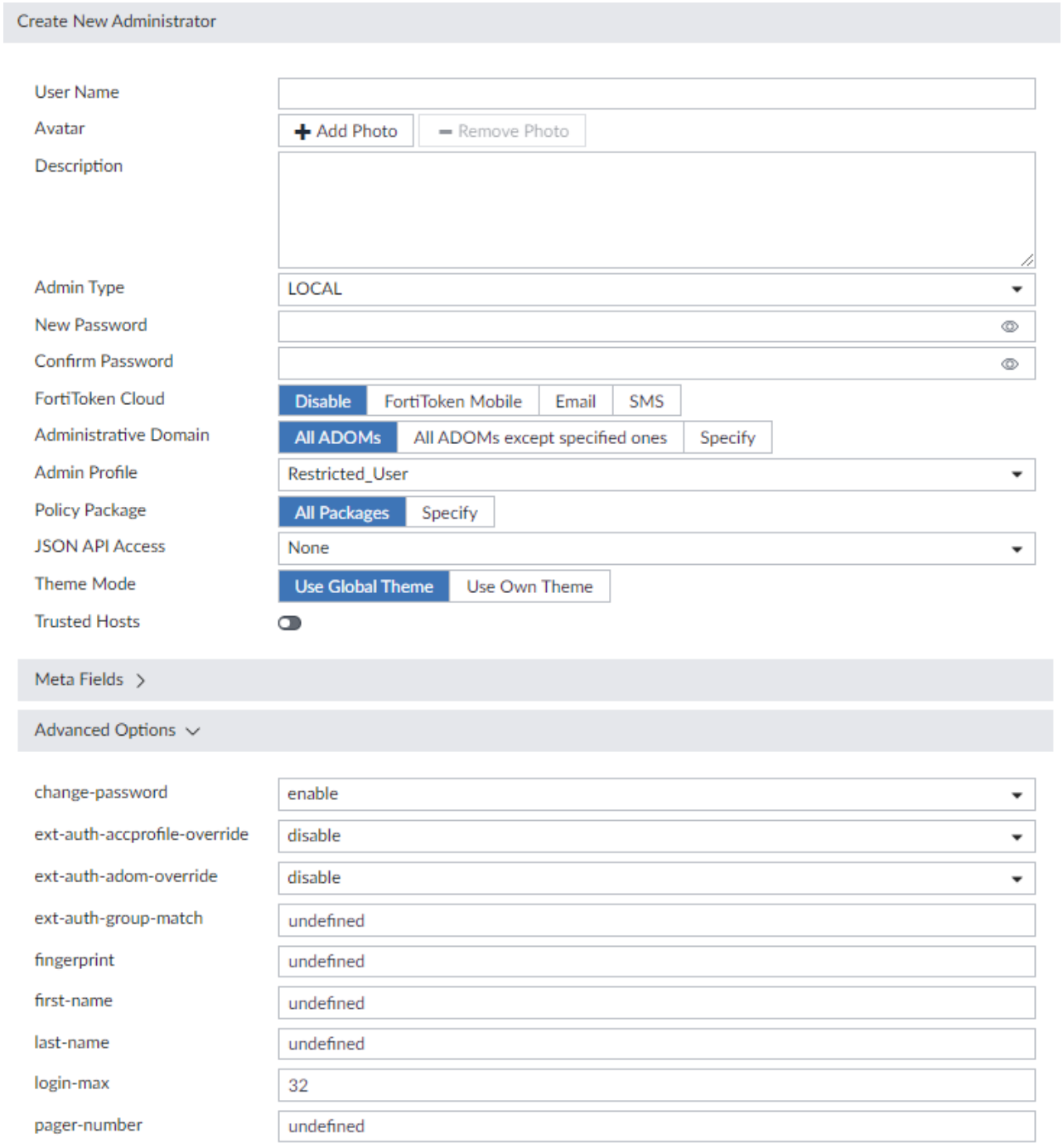
- Which authentication method the administrator will use to log in to the FortiManager unit. Local, remote, and Public Key Infrastructure (PKI) authentication methods are supported.
- What administrator profile the account will be assigned, or what system privileges the account requires.
- If ADOMs are enabled, which ADOMs the administrator will require access to.
- If using trusted hosts, the trusted host addresses and network masks.



For remote or PKI authentication, the authentication must be configured before you create the administrator. See Authentication on page 1037 for details.

To create a new administrator:

1. Go to *System Settings* > *Administrators*.
2. In the toolbar, click *Create New* > *Administrator* to display the *Create New Administrator* pane.



3. Configure the following settings, and then click *OK* to create the new administrator.

User Name	Enter the name of the administrator will use to log in.

Avatar	Apply a custom image to the administrator. Click *Add Photo* to select an image already loaded to the FortiManager, or to load an new image from the management computer. If no image is selected, the avatar will use the first letter of the user name.
Comments	Optionally, enter a description of the administrator, such as their role, location, or the reason for their account.
Admin Type	Select the type of authentication the administrator will use when logging into the FortiManager unit. One of: *LOCAL*, *RADIUS*, *LDAP*, *TACACS+*, *PKI*, *Group*, or *SSO*. See Authentication on page 1037 for more information.
Server or Group	Select the RADIUS server, LDAP server, TACACS+ server, or group, as required. The server must be configured prior to creating the new administrator. This option is not available if the *Admin Type* is *LOCAL* or *PKI*.
Match all users on remote server	Select this option to automatically add all users from a LDAP server specified in *Admin>Remote Authentication Server*. All users specified in the *Distinguished Name* field in the LDAP server will be added as FortiManager users with the selected Admin Profile. Select this option when the *Admin Type* is *SSO* to create one SAML SSO wildcard admin user to match all users on the identity provider (IdP) server. This FortiManager must be configured as a service provider (SP), added to the IdP, and have the same user profile and ADOM names as the IdP. If this is done, the user is assigned the same profile and ADOMs when logging in as an SSO user on this SP. See SAML admin authentication on page 1046. If this option is not selected, the *User Name* specified must exactly match the LDAP user specified on the LDAP server. This option is not available if the *Admin Type* is *LOCAL* or *PKI*.
Subject	Enter a comment for the PKI administrator. This option is only available if the *Admin Type* is *PKI*.
CA	Select the CA certificate from the dropdown list. This option is only available if the *Admin Type* is *PKI*.
Required two-factor authentication	Select to enable two-factor authentication. This option is only available if the *Admin Type* is *PKI*.
New Password	Enter the password. This option is not available if *Match all users on remote server* is selected. If the *Admin Type* is *PKI*, this option is only available when *Require two-factor authentication* is selected. If the *Admin Type* is *RADIUS*, *LDAP*, or *TACACS+*, the password is only used when the remote server is unreachable.

Confirm Password	Enter the password again to confirm it. This option is not available if *Match all users on remote server* is selected. If the *Admin Type* is *PKI*, this option is only available when *Require two-factor authentication* is selected.
Force this administrator to change password upon next log on.	Force the administrator to change their password the next time that they log in to the FortiManager. This option is only available if *Password Policy* is enabled in *Admin Settings*. See Password policy on page 1054.
FortiToken Cloud	Enable or disable multi-factor authentication with FortiToken Cloud, then select the token delivery method from the following options: • *FortiToken Mobile*: Use the FortiToken Mobile app to get tokens. The administrator is sent an email with a link to activate their token in the FortiToken Mobile app on their mobile device. • *Email*: Receive the token by email. • *SMS*: Receive the token by SMS message. This option is not available if Admin Type is set to *PKI* or *SSO*. For more information, see Multi-factor authentication with FortiToken Cloud on page 1064
Administrative Domain	Choose the ADOMs this administrator will be able to access. • *All ADOMs*: The administrator can access all the ADOMs. • *All ADOMs except specified ones*: The administrator cannot access the selected ADOMs. • *Specify*: The administrator can access the selected ADOMs. Specifying the ADOM shows the *Specify Device Group to Access* check box. Select the *Specify Device Group to Access* check box and select the Device Group this administrator is allowed to access. The newly created administrator will only be able to access the devices within the Device Group and sub-groups. If the *Admin Profile* is *Super_User*, then this setting is *All ADOMs*. This field is available only if ADOMs are enabled. See Administrative Domains (ADOMs) on page 924.
Admin Profile	Select an administrator profile from the list. The profile selected determines the administrator's access to the FortiManager unit's features. See Administrator profiles on page 1010. If the *Administrative Domain* is *Specify*, you can select *Single* or *Per-ADOM*. • *Single* (default): Select one admin profile to apply for all ADOMs the administrator can access. • *Per-ADOM*: Select a admin profile for each ADOM that the administrator can access. The administrator's access to the FortiManager's features will vary by ADOM according to the profiles selected.
Policy Package	Choose the policy packages this administrator will have access to.

	• *All Packages*: The administrator can access all the packages. • *Specify*: The administrator can access the selected packages or package folder. If you specify a policy package folder, the administrator can access the policy packages in the selected folder and all sub-folders. This option is only available when the *Admin Profile* is not a *Restricted Admin* profile. See Restricted administrators on page 989.
JSON API Access	Select the permission for JSON API Access. Select *Read-Write*, *Read*, or None. The default is *None*.
Web Filter Profile	Select the web filter profiles that the restricted administrator will be able to edit. This option is only available when the *Admin Profile* is set to a *Restricted Admin* profile. Security profiles can be configured by going to *Policy & Objects* > *Object Configuration*. See Managing objects and dynamic objects on page 532.
IPS Sensor	Select the IPS profiles that the restricted administrator will be able to edit. This option is only available when the *Admin Profile* is set to a *Restricted Admin* profile. Security profiles can be configured by going to *Policy & Objects* > *Object Configuration*. See Managing objects and dynamic objects on page 532.
Application Sensor	Select the application control profiles that the restricted administrator will be able to edit. This option is only available when the *Admin Profile* is set to a *Restricted Admin* profile. Security profiles can be configured by going to *Policy & Objects* > *Object Configuration*. See Managing objects and dynamic objects on page 532.
Trusted Hosts	Optionally, turn on trusted hosts, then enter their IP addresses and netmasks. Up to ten IPv4 and ten IPv6 hosts can be added. See Trusted hosts on page 976 for more information.
Theme Mode	Select *Use Global Theme* to apply a theme to all administrator accounts. Select *Use Own Theme* to allow administrators to select their own theme.
Meta Fields	Optionally, enter the new administrator's email address and phone number. The email address is also used for workflow session approval notifications, if enabled. See Workflow mode on page 1026.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced options, see the *FortiManager CLI Reference*.

Advanced options

Option	Description	Default
change-password	Enable or Disable changing password.	disable
ext-auth-accprofile-override	Enable or Disable overriding the account profile by administrators configured on a Remote Authentication Server.	disable
ext-auth-adom-override	Enable or Disable overriding the ADOM by administrators configured on a Remote Authentication Server. This will also override the *Admin Profile* configured for each ADOM.	disable
ext-auth-group-match	Specify the group configured on a Remote Authentication Server.	-
fingerprint	Specify the user certificate fingerprint based on MD5, SHA-1, or SHA-256 hash function. This option is only available if the *Admin Type* is *PKI*.	-
first-name	Specify the first name.	-
last-name	Specify the last name.	-
mobile-number	Specify the mobile number.	-
pager-number	Specify the pager number.	-
restrict-access	Enable or Disable restricted access.	disable

Editing administrators

To edit an administrator, you must be logged in as a super user administrator. The administrator's name cannot be edited. An administrator's password can be changed using the right-click menu, if the password is not a wildcard.

To edit an administrator:

1. Go to *System Settings > Administrators*.
2. Double-click on an administrator, right-click on an administrator and then select *Edit* from the menu, or select the administrator then click *Edit* in the toolbar. The *Edit Administrator* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

To change an administrator's password:

1. Go to *System Settings > Administrators*.
2. Right-click on an administrator and select *Change Password* from the menu. The *Change Password* dialog box opens.
3. If you are editing the *admin* administrator's password, enter the old password in the *Old Password* field.
4. Enter the new password for the administrator in the *New Password* and *Confirm Password* fields.
5. Select *OK* to change the administrator's password.



The current administrator's password can also be changed from the admin menu in the GUI banner. See GUI overview on page 33 for information.

Deleting administrators

To delete an administrator or administrators, you must be logged in as a super user administrator.



You cannot delete an administrator that is currently logged in to the device.



The *admin* administrator can only be deleted using the CLI.

To delete an administrator or administrators:

1. Go to *System Settings* > *Administrators*.
2. Select the administrator or administrators you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the administrator or administrators.

To delete an administrator using the CLI:

1. Open a CLI console and enter the following command:

```
config system admin user
   delete <username>
end
```

Override administrator attributes from profiles

FortiManager administrator accounts can be configured to use the *RPC Permit (JSON API Access)* and *Trusted Hosts* attributes that are defined by an administrator profile.

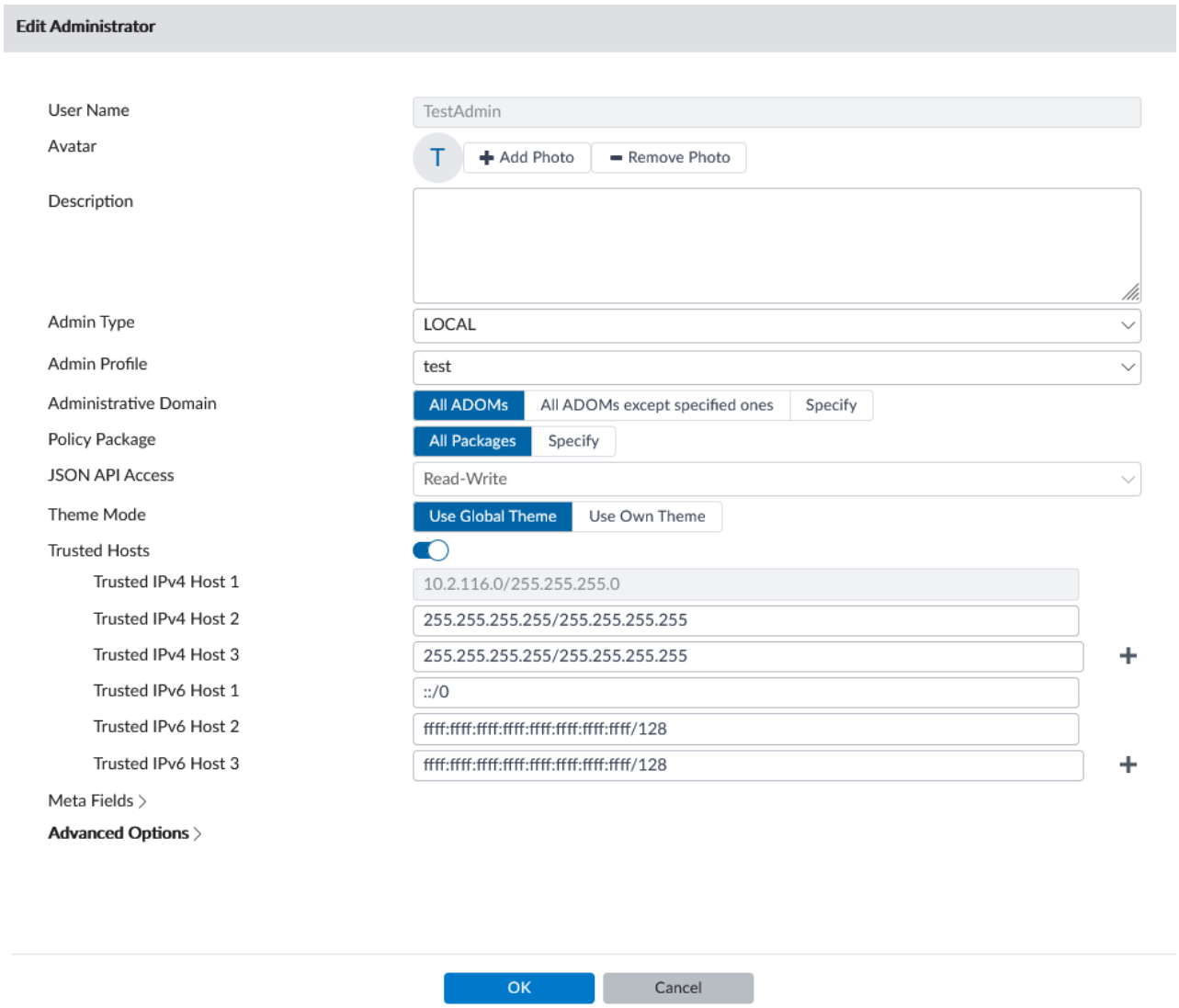
When an administrator has been configured to use the attributes from the profile, the attributes can no longer be changed by editing the administrator account.

This feature can only be configured from the FortiManager CLI.

For more information, see the FortiManager CLI Reference Guide on the Fortinet Document Library.

To use RPC Permit and Trusted Host administrator attributes from a profile:

1. Go to *System Settings* > *Administrators*, and create or edit an admin user.
2. In *Admin Profile* dropdown, select an administrator profile, and click *OK*.
3. Configure the settings for the `rpc-permit` and/or `trusthost1` attributes in the admin profile.
   Enter the following commands in the FortiManager CLI:
   ```
   config system admin profile
      edit <profile name>
         set rpc-permit {none | read | read-write}
         set trusthost1 <ip & netmask>
      end
   ```
4. Configure the admin user to use the `from-profile` option for the `rpc-permit` and/or `trusthost1` attributes.
   Enter the following commands in the FortiManager CLI:
   ```
   config system admin user
      edit <admin user>
         set rpc-permit from-profile
         set trusthost1 from-profile
   end
   ```
5. In the FortiManager GUI, go to *System Settings* > *Administrators* and view the administrator account. The attributes that were configured to use the `from-profile` setting can no longer be edited and display the settings defined in the administrator profile.



Creating administrators for the FortiManager API

In order to use the FortiManager JSON API, you must first create an administrator.

The type of administrator required depends on if you will be using a predefined API key or session-based authentication.

- **Predefined API key**: A REST API Admin is used to generate a permanent API key, which means the same user account will always share the same session and you do not need to use the login/logout endpoints. Because of this benefit, predefined API keys are useful for simplifying automation workflows.
- **Session-based authentication**: A regular FortiManager administrator with JSON API access is used with the login operation in order to get a session ID that is used in API requests.

Both types of administrators also require that you assign an *Admin Profile* with the appropriate permissions to complete the desired operations.

For more information on using the FortiManager JSON API, see the Fortinet Developer Network (FNDN).

To create REST API administrator with a predefined API key:

1. Go to *System Settings > Administrators*.
2. Click the *Create New* dropdown and choose *REST API Admin*.
3. Configure the following required information:

User Name	Enter a username.
Admin Profile	Select an admin profile that provides appropriate permissions required to complete the operations needed using the API.
JSON API Access	Select *Read* or *Read-Write* access, depending on your need.
PKI Group	(Optional) Certificate matching is supported as an extra layer of security. Both the client certificate and token must match to be granted access to the API.
CORS Allow Origin	(Optional) Cross Origin Resource Sharing (CORS) allows third-party web apps to make API requests to the FortiManager using the token.
Trusted Hosts	At least one trusted host must be configured. This trusted host should align with the IP range where the API requests will originate from.

4. Configure any remaining settings as required, such as additional role-based access control settings to restrict the administrator to specific ADOMs, policy packages, or policy blocks.
5. Click *OK* to create the REST API Admin.
   An API key is automatically generated for the REST API Admin. The API key is permanent and only shown once.
6. Copy the API key. The generated API key can be used in the request header using the bearer authentication scheme.
7. Optionally, you can generate a new API key by editing the REST API Admin and clicking *Regenerate API Key*.

To create an administrator for session-based authentication:

1. Go to *System Settings > Administrators*.
2. Click the *Create New* dropdown and choose *Administrator*.
3. Configure the following required information:

User Name	Enter a username.
New Password/Confirm Password	Enter a password.
Admin Profile	Select an admin profile that provides appropriate permissions required to complete the operations needed using the API.
JSON API Access	Select *Read* or *Read-Write* access, depending on your need.

4. Configure any remaining settings as required, such as additional role-based access control settings to restrict the administrator to specific ADOMs, policy packages, or policy blocks.
5. Click *OK* to create the administrator.

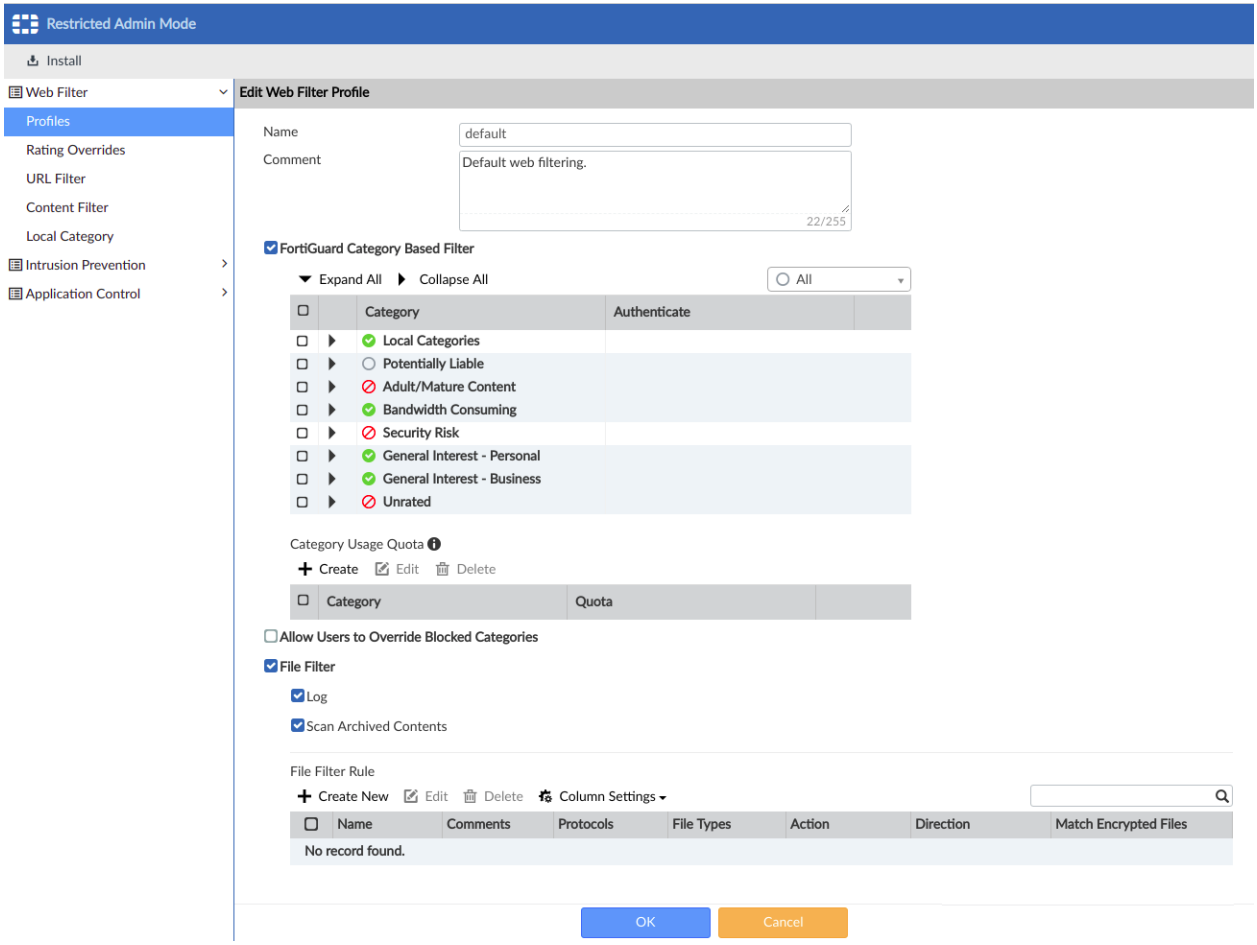
The username and password of this administrator will be used for the `login` operation on FortiManager which will generate a session ID which is used in API requests.

Restricted administrators

Restricted administrator accounts are used to delegate management of Web Filter, IPS, and Application Control profiles, and then install those objects to their assigned ADOM.

Workspace mode is supported for restricted administrators. See Workspace mode for restricted administrators on page 1009.

When a restricted administrators logs in to the FortiManager, they enter the *Restricted Admin Mode*. This mode consists of a simplified GUI where they can make changes to the profiles that they have access to, and then install those changes using the *Install* command in the toolbar, to their designated ADOM.



To create a restricted administrator:

1. Create an administrator profile with the *Type* set to *Restricted Admin* and the required permissions selected. See Creating administrator profiles on page 1015.
2. Create a new administrator and select the restricted administrator profile for the *Admin Profile*, then select the specific ADOMs and profiles that the administrator can manage. See Creating administrators on page 979



Starting in FortiManager 7.0.3, you can select multiple ADOMs with restricted administrator profiles when creating or editing an administrator account.



Restricted administrators can create new custom signatures for Intrusion Prevention and Application Control.

See Intrusion prevention restricted administrator on page 993 and Application control restricted administrator on page 1006.

Web Filter restricted administrator

Web filtering restricts or controls user access to web resources.

To create a profile:

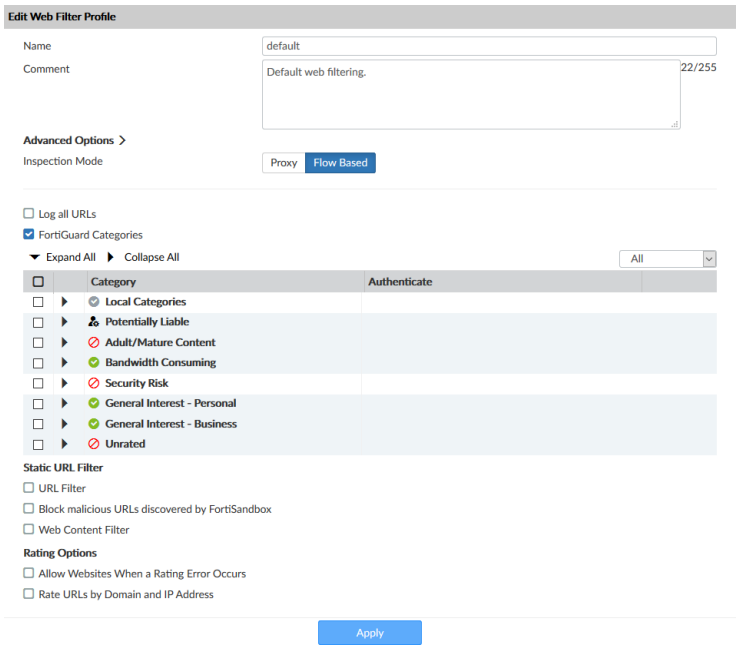
1. Log in as a Restricted Administrator.
2. In the tree menu, select *Web Filter*, and then select a profile category.
3. In the toolbar, click *Create New*.
4. Configure the profile settings, and click *OK*.



To clone an existing profile, right-click the profile in the content pane, and select *Clone*.

To edit a profile:

1. Log in as a Restricted Administrator.
2. In the tree menu, select *Web Filter*, and then select a profile category.
3. In the content pane select a profile and take one of the following actions:
   - In the toolbar, click *Edit*.
   - Right-click the profile, and select *Edit*.
4. Edit the settings, and click *OK*.



Name	The profile name.
Comment	Optionally, enter a description of the profile.
Advanced Options	Configure advanced options, including: • *https-replacemsg*: enable/disable • *replacemsg-group*: select a group from the list • *web-filter-activex-log*: enable/disable • *web-filter-command-block-log*: enable/disable • *web-filter-cookie-removal-log*: enable/disable • *web-filter-js-log*: enable/disable • *web-filter-jscript-log*: enable/disable • *web-filter-referer-log*: enable/disable • *web-filter-unknown-log*: enable/disable • *web-filter-vbs-log*: enable/disable • *wisp*: enable/disable • *wisp-algorithm*: *auto-learning*, *primary-secondary*, or *round-robin*
Inspection Mode	Select *Proxy* or *Flow Based*.
Log all URLs	Select to log all URLs.
FortiGuard Categories	Select FortiGuard categories. Right-click on a category to change the action: *Allow*, *Block*, *Warning*, *Monitor*, *Authenticate*, or, if available, *Disable*. Use the filter drop-down menu to filter the categories shown in the table based on the action.
Allow Users to override blocked categories	Select to allow users to override blocked categories. This option is only available if *Inspection Mode* is *Proxy*.

Override Permit	Select the override permits: *bannedword-override*, *contenttype-check-override*, *fortiguard-wf-override*, and *urlfilter-override*.
Groups that can override	Select groups that can override blocked categories.
Profile can switch to	Select profiles that the user can switch to.
Switch applies to	Select what the switch applies to: *ask*, *browser*, *ip*, *user*, or *user-group*.
Switch Duration	Select the switch duration, either *ask* or *constant*.
Duration	Enter the duration of the switch. This option is only available if *Switch Duration* is *constant*.
Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex	Select to enforce *Safe Search*. This option is only available if *Inspection Mode* is *Proxy*.
Log all search keywords	Select to log all search keywords. This option is only available if *Inspection Mode* is *Proxy*.
Block Invalid URLs	Select to block invalid URLs. This option is only available if *Inspection Mode* is *Proxy*.
URL Filter	Select to enable URL filters. Select URL filters from the dropdown list, and/or create and manage filters in the table.
Block malicious URLs discovered by FortiSandbox	Select to block URLs that FortiSandbox deems malicious.
Web Content Filter	Select to apply web content filters. Click *Add* to add filters to the table. Edit and delete filters as required.
Allow Websites When a Rating Error Occurs	Select to allow access to websites if a rating error occurs.
Rate URLs by Domain and IP Address	Select to rate URLs by both their domain and IP address.
Block HTTP Redirects by Rating	Select to block HTTP redirects based on the site's rating. This option is only available if *Inspection Mode* is *Proxy*.
Rate Images by URL (Blocked images will be replaced with blanks)	Select to rate images based on the URL. This option is only available if *Inspection Mode* is *Proxy*.
Restrict Google account usage to specific domains	Select to restrict Google account usage to specific domains. Click *Add* to add the domains to the table. This option is only available if *Inspection Mode* is *Proxy*.
Provide Details for Blocked HTTP 4xx and 5xx Errors	Select to receive details about blocked HTTP errors. This option is only available if *Inspection Mode* is *Proxy*.

HTTP POST Action: Block	Select to set the HTTP POST action to block. This option is only available if *Inspection Mode* is *Proxy*.
Remove Java Applet Filter	Select to remove the Java applet filter. This option is only available if *Inspection Mode* is *Proxy*.
Remove ActiveX Filter	Select to remove the ActiveX filter. This option is only available if *Inspection Mode* is *Proxy*.
Remove Cookie Filter	Select to remove the cookie filter. This option is only available if *Inspection Mode* is *Proxy*.

To view where a profile is being used:

1. Log in as a restricted administrator.
2. In the tree menu, select *Profiles*.
3. In the content pane, select a profile from the list, and click *Where Used* in the *More* dropdown menu. The dialog window displays the ADOM and policy package/block where the package is currently being used.
4. (Optional) Select a policy in the list, and click *View* to display the policy details.

Intrusion prevention restricted administrator

An Intrusion Prevention System (IPS) can be used to detect and block network-based attacks. In FortiManager, a restricted administrator profile can be created to allow an administrator to configure IPS settings without interfering with FortiManager's networking capabilities and functions.

Restricted administrators can create new profiles and signatures, add signatures and filters to a profile, and define the action (Allow, Monitor, Block, Reset, Default, Quarantine) that will occur for detected signatures. They are also able to view IPS diagnostics, FortiGuard package status, licenses and services, and create IPS templates.

Restricted administrator profiles can be used when migrating from a standalone IPS system to give the IPS administrator granular control over what IPS profiles and signatures to deploy.

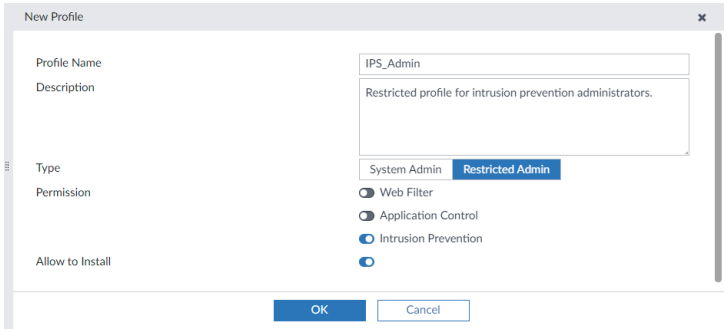
Optionally, restricted administrator profiles can be configured with permissions to install changes to managed FortiGate devices. See Installing profiles as a restricted administrator on page 1008.

For firewall administrators, read-write access to IPS related objects can be configured in each administrator profile using the CLI. For more information, see `ips-objects` in Permissions on page 1011.

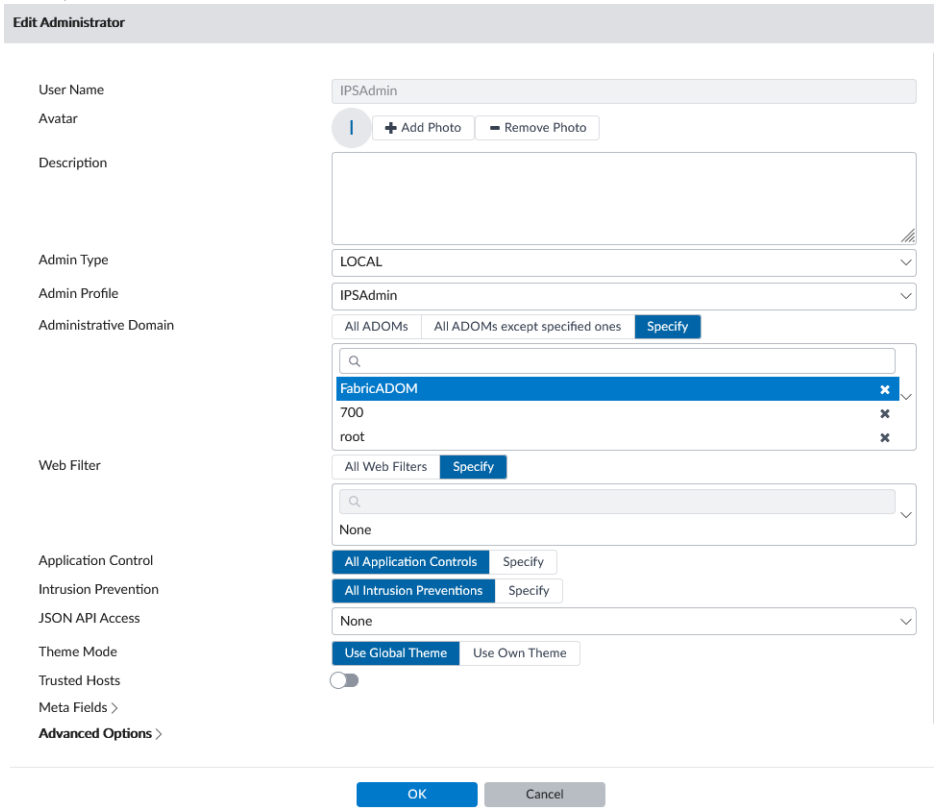
To create an IPS restricted administrator:

1. Go to *System Settings* > *Admin Profiles*, and create an administrator profile with the *Type* set to *Restricted Admin* and the permissions set as *Intrusion Prevention*. See Creating administrator profiles on page 1015.

2. Optionally, toggle *Allow to Install* if you want this administrator to be able to install changes to FortiGate devices.



3. Go to *System Settings* > *Administrators*, and create a new administrator.
4. Select the restricted IPS profile for the *Admin Profile*, then select the ADOMs and *Intrusion Prevention* profiles that the administrator can manage. See Creating administrators on page 979.
   You can select *All ADOMs*, *All ADOMs except specified ones*, or *Specify* to select ADOMs that the restricted admin is able to access. Restricted administrators can only view and install changes to devices included in the specified ADOMs.





For more information about restricted administrator profiles, see Restricted administrators on page 989.

To configure IPS settings as a restricted administrator, see:

- Intrusion prevention profiles on page 995
- Intrusion prevention signatures on page 998
- Intrusion prevention diagnostics on page 998
- Intrusion prevention hold-time and CVE filtering on page 999
- Intrusion prevention FortiGuard packages on page 1000
- Intrusion prevention licenses and services on page 1001
- Intrusion prevention templates on page 1002
- Intrusion prevention global headers and footers on page 1003
- IPS administration permissions on page 1004

Intrusion prevention profiles

Intrusion prevention profiles can be used to manage IPS filters and signatures, block malicious URLs, and configure Botnet C&C scanning.

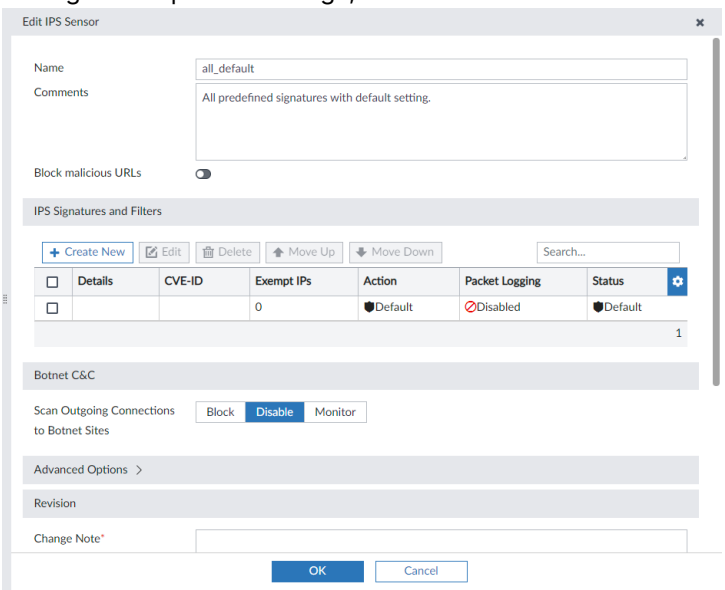
Profiles can be installed to the FortiGate devices included in ADOMs that are assigned to the restricted administrator account. The administrator can select which devices to install changes to, giving them the ability to test signatures and filters on a subset of devices before installing the changes to all managed devices.

You can see where each profile in the Profile table is being used by enabling *Used* in the *Column Settings*.

Intrusion prevention profiles include the revision history of changes made to the profile. Using the revision history you can compare two previous versions of the profile, and if needed, revert to a previous revision.

To create a IPS profile:

1. Log in as a restricted administrator.
2. In the tree menu, select *Intrusion Prevention* > *Profiles*.
3. In the toolbar, click *Create New*.
4. Configure the profile settings, and click *OK*.



Name	The profile name.
Comment	Optionally, enter a description of the profile.
IPS Signatures and Filters	Click *Create New* and select the *Type* as either *Filter* or *Signature* to add IPS signatures and filters to the table. The table list can be filtered to simplify adding them. You can quickly edit an existing signature or filter by double-clicking it in the list.
Filters	When creating filters, the following settings are available: *Action (Allow, Monitor, Block, Reset, Default, Quarantine)*, *Packet Logging*, *Status*, and *Filter*. Click the edit filter icon to create a new filter. For information on hold-time and CVE filter options, see Intrusion prevention hold-time and CVE filtering on page 999.
Signatures	When selecting signatures, the following settings are available: *Action (Allow, Monitor, Block, Reset, Default, Quarantine)*, *Packet Logging*, *Status*, *Rate-based Setting*, *Exempt IPs*, and *Signatures*. Click *Add Signature* to select a new signature. As a restricted administrator, custom IPS signatures can be created by navigating to *Intrusion Prevention > IPS Signatures* in the tree menu. See Intrusion prevention signatures on page 998.
Botnet C&C	Enable Botnet C&C to scan outgoing connections to botnet sites. Botnet C&C can be set to *Block*, *Disable*, or *Monitor*.
Advanced Options	Enable or disable extended logging.
Revision	Enter a change note that includes details about the change made to the IPS profile.
Revision History	View the revision history for this profile. Select *View Diff* in the toolbar to compare two versions in revision history. Select *Revert* in the toolbar to revert to a previous version based on revision history.



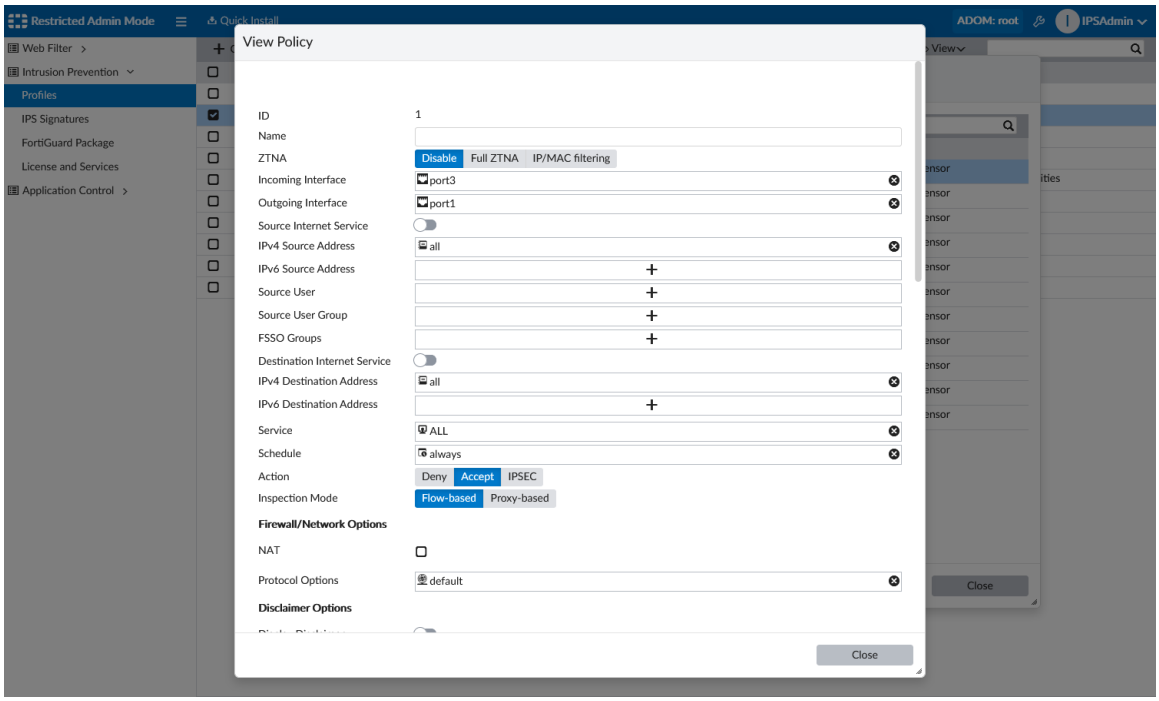
To clone an existing profile, right-click the profile in the content pane, and select *Clone*.

To edit a IPS profile:

1. Log in as a restricted administrator.
2. In the tree menu, select *Intrusion Prevention > Profiles*.
3. In the content pane, select a profile, and take one of the following actions:
   - In the toolbar, click *Edit*.
   - Right-click the profile, and select *Edit*.
4. Edit the settings, and click *OK*.

To view where a profile is being used:

1. Log in as a restricted administrator.
2. In the tree menu, select *Profiles*.
3. In the content pane, select a profile from the list, and click *Where Used* in the *More* dropdown menu.
   The dialog window displays the ADOM and policy package/block where the package is currently being used.
4. (Optional) Select a policy in the list, and click *View* to display the policy details.



To revert a profile to a previous version:

1. Log in as a restricted administrator.
2. In the tree menu, select *Intrusion Prevention* > *Profiles*.
3. In the content pane, edit the profile that you want to revert from the list.
   Past changes made to this profile are listed in a table under *Revision History*.
4. Select a saved revision from the table and click *Revert*, and click *OK* in the window confirming that you want to revert the profile.

To view IPS profile usages:

1. Log in as a restricted administrator.
2. In the tree menu, select *Intrusion Prevention* > *Profiles*.
3. In the toolbar, select *More* > *IPS Profile Usages*.
   The IPS Profile Usages window displays the status (synced or modified) and timestamps for each IPS sensor installed on managed devices.
4. When an IPS sensor has been modified, you can click *Show Diff* in the status column to view modifications made to the IPS profile that are not installed to the device.

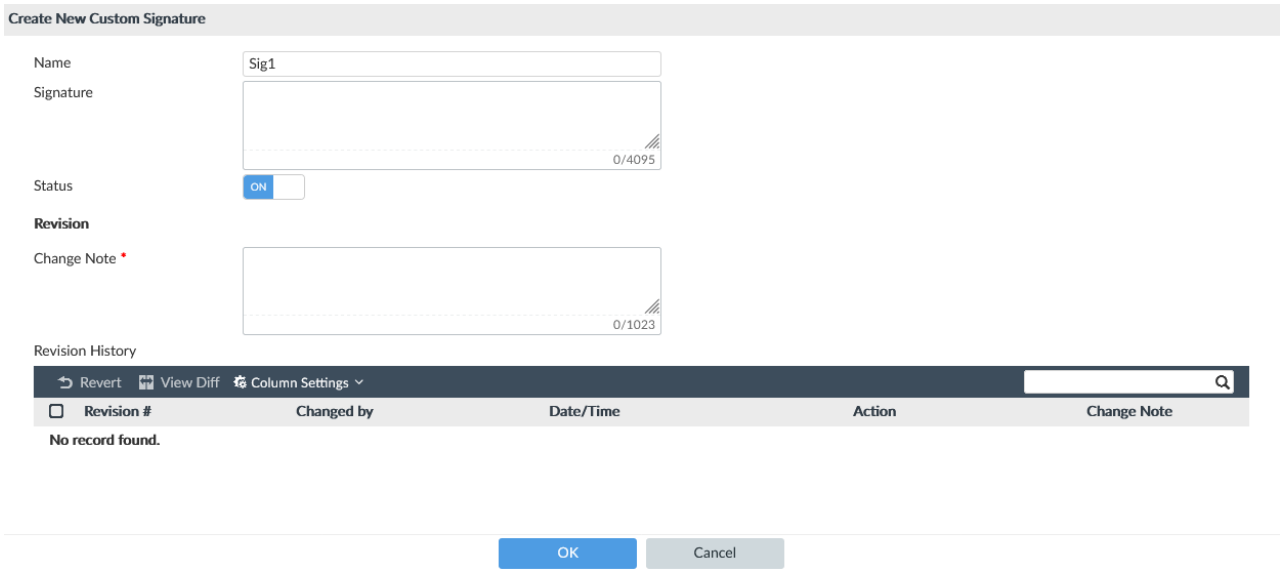
Intrusion prevention signatures

As a restricted administrator, you can view and create IPS signatures by going to *Intrusion Prevention > IP Signatures* in the FortiManager tree menu.

Configured IPS signatures can be added to an IPS profile and installed to devices.

To create a custom signatures as a restricted administrator:

1. Log on as a restricted administrator.
2. Go to *Intrusion Prevention > IPS Signatures*.
3. Click *Create New*. The *Create New Custom Signature* screen appears.

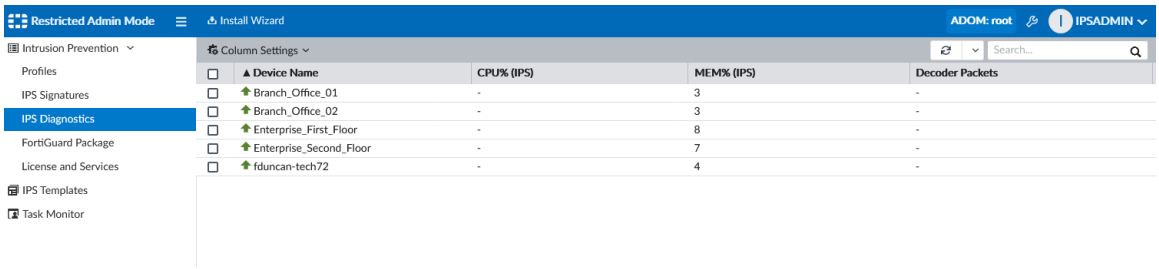


4. Specify the values for the following and click *OK*.
   - Name - specify a name for the custom signature.
   - Signature - add a custom signature.
   - Status - toggle the status to ON.

For additional information on managing IPS signatures and viewing signature details, see Intrusion prevention signatures on page 569 in Policy & Objects.

Intrusion prevention diagnostics

IPS Diagnostics are available to IPS restricted administrators in *Intrusion Prevention > IPS Diagnostics*. The IPS Diagnostics page displays a list of devices in the ADOM with the following information:



Device Name	The name of the FortiGate device.
CPU% (IPS)	The CPU used by IPS processes as a percentage for the device.
MEM% (IPS)	The memory used by IPS processes as a percentage for the device.
Decoder Packets	The number of transmitted decoder packets.
Session Packets	The number of transmitted sesion packets.
Protocol Packets	The number of transmitted protocol packets.
Application Packets	The number of transmitted application packets.

Intrusion prevention hold-time and CVE filtering

IPS signature filter options include hold-time and CVE pattern.

IPS signature hold-time

The hold-time option allows you to set the amount of time that signatures are held after a FortiGuard IPS signature update per VDOM. During the holding period, the signature's mode is *monitor*. The new signatures are enabled after the hold-time to avoid false positives.

The hold-time can be from 0 days and 0 hours (default) up to 7 days, in the format ##d##h.



This setting is configured for each FortiGate device and *cannot* be configured by restricted administrators.

For more information on configuring hold-time, see Intrusion prevention filtering options on page 567 in Policy & Objects.

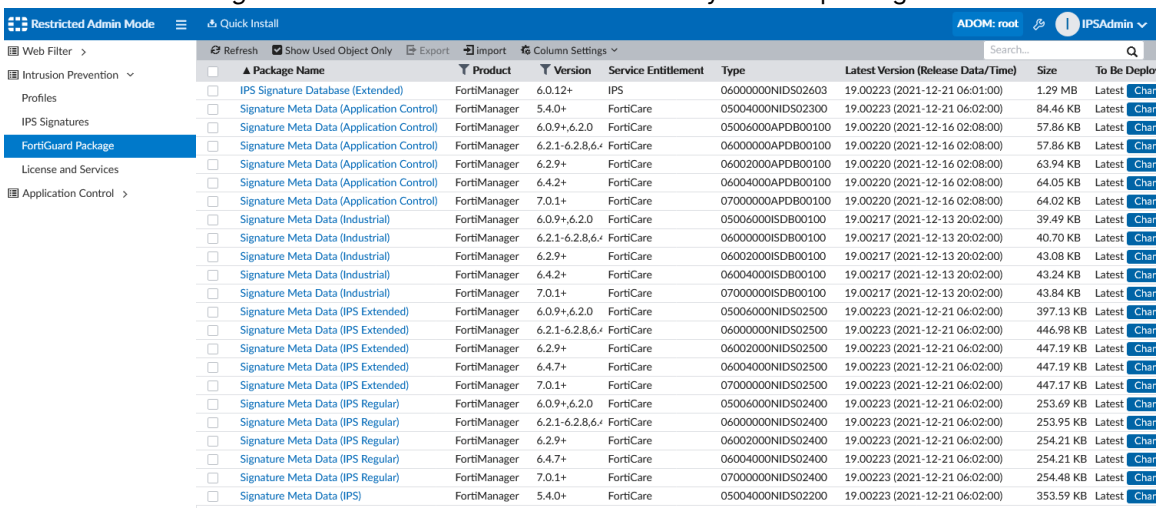
CVE pattern filters

The CVE pattern option allows you to filter IPS signatures based on CVE IDs or with a CVE wildcard, ensuring that any signatures tagged with that CVE are automatically included.

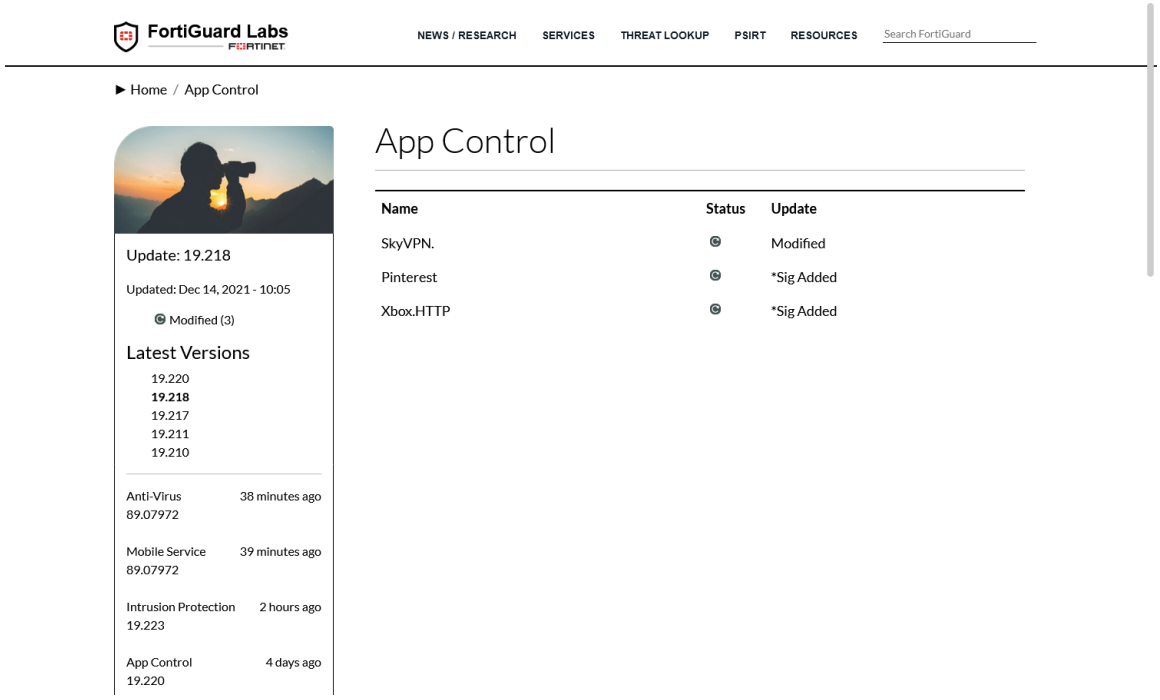
For more information on configuring CVE filters, see Intrusion prevention filtering options on page 567 in Policy & Objects.

Intrusion prevention FortiGuard packages

Intrusion prevention restricted administrators can view FortiGuard packages at *Intrusion Prevention > FortiGuard Package*. IPS restricted administrators can only see IPS packages from FortiGuard.



Each FortiGuard package name includes a link to the package details on the FortiGuard website. Click on a package name to view detailed information about the package, including the changes that happened with the latest versions.

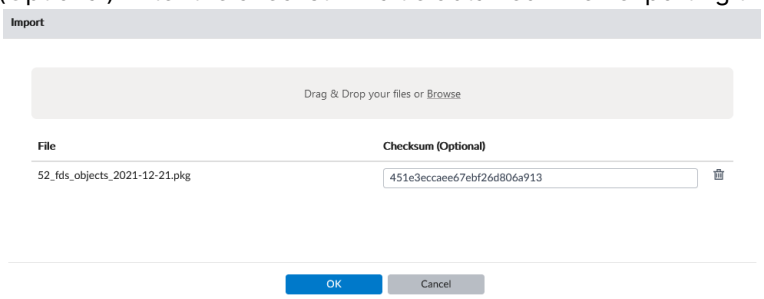


FortiGuard packages can be imported or exported.

To import a FortiGuard package:

1. As a restricted administrator, go to *Intrusion Prevention > FortiGuard Package*.
2. Click *Import* in the toolbar.

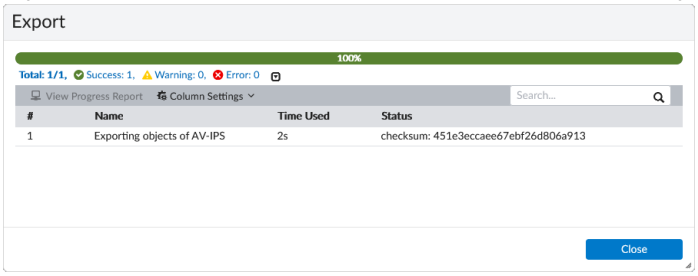
3. Drag and drop the file or browse to the location of the file and select it.
4. (Optional) Enter the checksum value obtained when exporting the package to verify the file's integrity.



5. Click *OK*.

To export a FortiGuard package:

1. As a restricted administrator, go to *Intrusion Prevention* > *FortiGuard Package*.
2. Click *Export* in the toolbar.
   A dialog appears to confirm the number and size of the objects you have selected to export.
3. Click *OK*, and the *Export* window appears to confirm the status of the task.
4. (Optional) Record the checksum value to include when importing this package in order to verify its integrity.



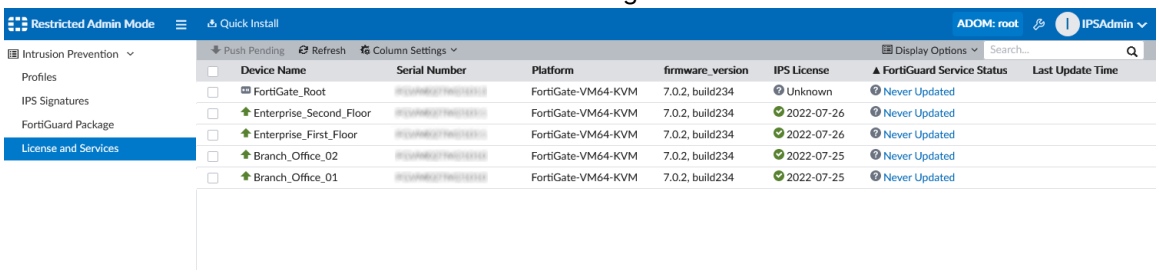
Intrusion prevention licenses and services

Intrusion prevention restricted administrators can view the *IPS License* and *FortiGuard Service Status* for managed devices at *Intrusion Prevention* > *License and Services*. You can refresh the information in this pane by right clicking on a list in the table and clicking *Refresh*.

The *Feature Visibility* dropdown in the toolbar includes settings to *Show Pending Device Only* and *Group By ADOMs*.

Restricted administrators can push pending updates for managed FortiGate units by selecting the device in the table and clicking *Push Pending*.

The *License and Services* table includes the following information:



Device Name	The FortiGate device's name.
Serial Number	The FortiGate device's serial number.
Platform	The FortiGate device's platform type.
firmware_version	The FortiGate device's firmware version.
IPS License	The status of the IPS license for the FortiGate device. Valid licenses include a green checkmark icon and display the expiration date of the license.
FortiGuard Service Status	The status of the FortiGuard service for the FortiGate device. The status includes only IPS related objects.
Last Update Time	The last updated time.

Intrusion prevention templates

IPS administrators can use IPS templates to modify and assign IPS objects to devices. Once a template has been created, it can be assigned to a device or device group in the ADOM.

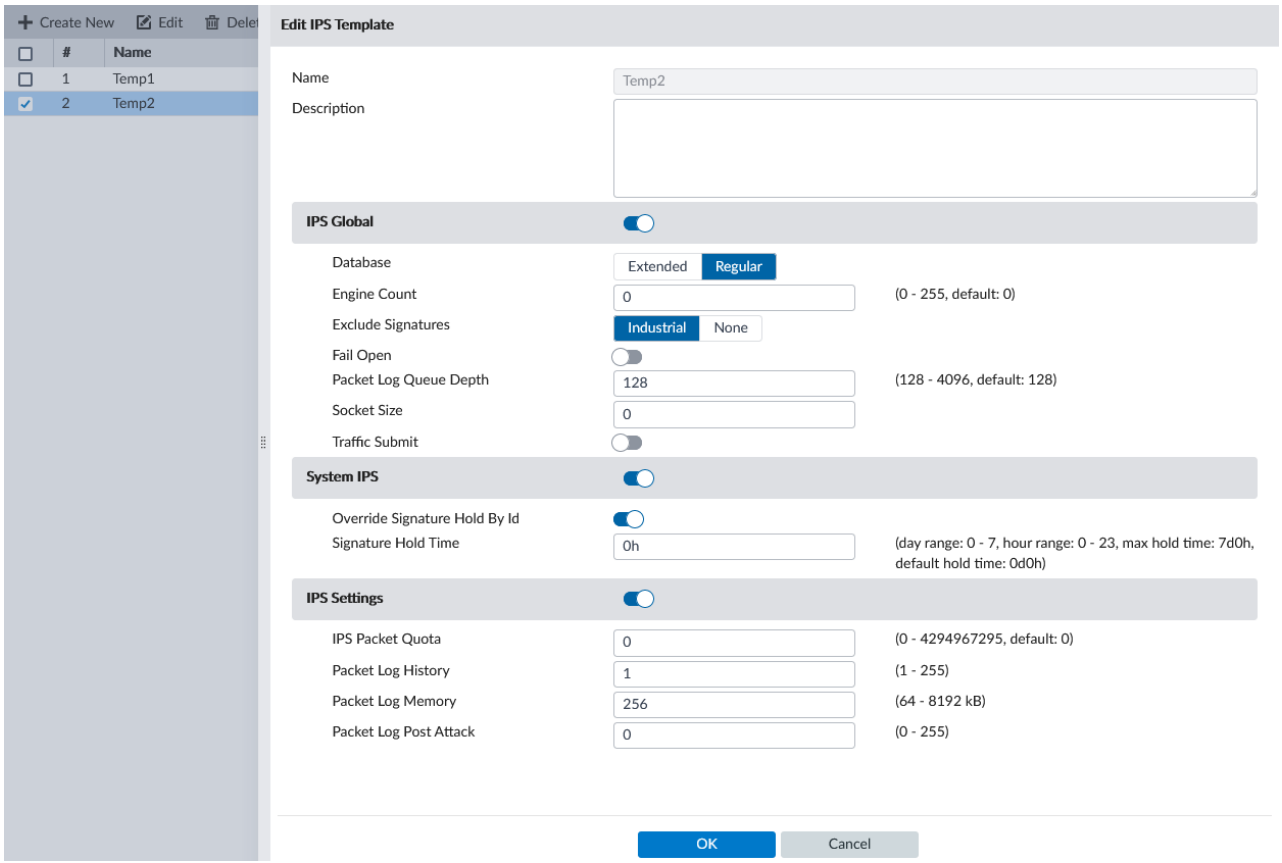
IPS templates can be created, edited, deleted and cloned.

To create an IPS template:

1. Log in as an Administrator, and go to *Device Manager > Provisioning Templates > IPS Templates*. Alternatively, if you are using a IPS restricted administrator profile, go to *Intrusion Prevention > IPS Templates*.
2. Click *Create New* to create a new IPS template.
   The *Create IPS Template* wizard opens.
3. Enter a name and optional description for the template, and click *OK*.
   The template is created and you can now edit the IPS template details.
4. Enable and configure one or more of the following IPS objects: *IPS Global* (global settings), *System IPS* (VDOM-based), and *IPS Settings* (VDOM-based).



When copying the IPS template to a device VDOM, if the target is "root" or "mgmt", only the IPS Global are coppied.



5. Click *OK* to save the template.

To assign a template to a device or group:

1. Log in as an Administrator, and go to *Device Manager > Provisioning Templates > IPS Templates*. Alternatively, if you are using a IPS restricted administrator profile, go to *Intrusion Prevention > IPS Templates*.
2. Select a IPS template from the table, and click *Assign to Device/Group* in the toolbar.
3. In the *Available Entries* pane, double-click a device to add it to the *Selected Entries* pane, and click *OK*.

Intrusion prevention global headers and footers

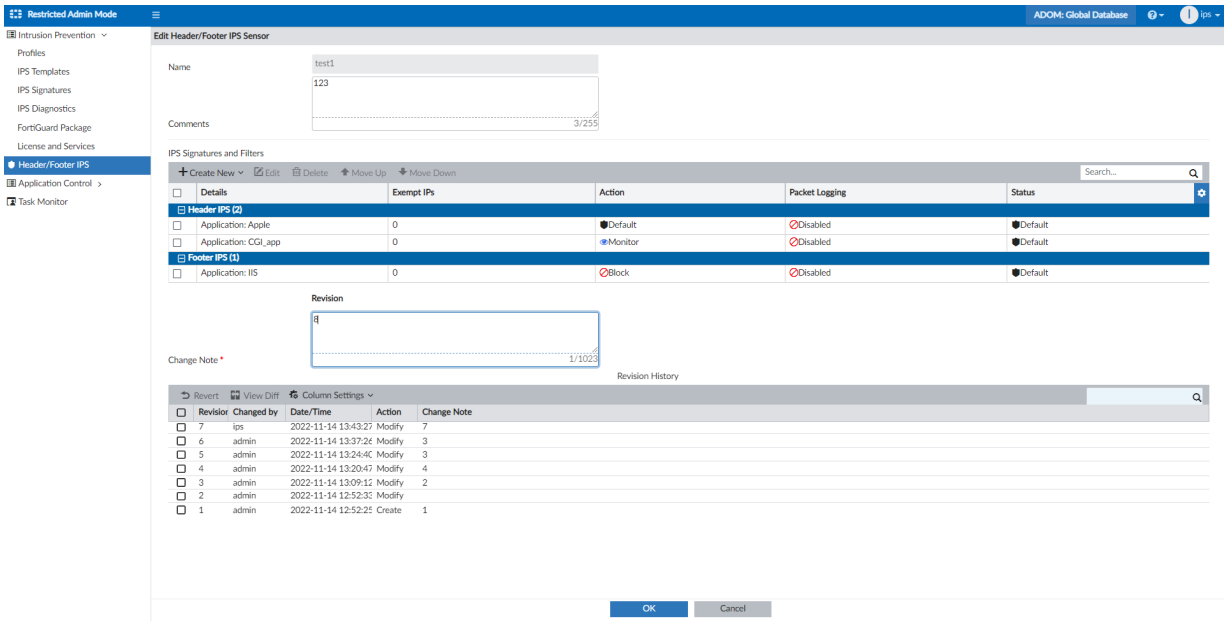
Restricted IPS admins can manage the IPS headers and footers and perform IPS installations in the *Global Database* ADOM.

For more information, see Global Database on page 950 and Header/Footer IPS on page 951.

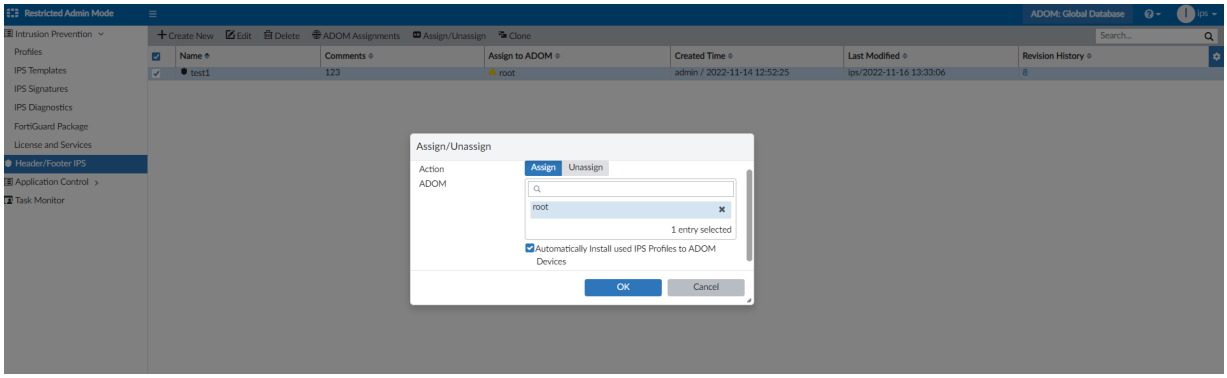
To manage IPS headers and footers in the global ADOM:

1. Sign in to FortiManager as a restricted IPS administrator.
2. Go to the *Global Database* ADOM.

3. Go to *Intrusion Prevention* > *Header/Footer IPS*.
   - Restricted administrators can create, modify, and assign global IPS headers and footers from the *Global Database* ADOM.



   - When assigning IPS headers and footers, you can select the option to *Automatically Install Used IPS Profiles to ADOM Devices*.



IPS administration permissions

FortiManager includes IPS specific administrator profile permissions that can be used to determine an administrator's ability to view and manage IPS objects and IPS attributes within policies.

The following IPS permissions can be applied to an administrator profile. See Administrator profiles on page 1010.

Permission	Description
IPS Objects `ips-object`	Determines an administrator's ability to view and manage IPS objects.

Permission	Description
Policy IPS Attributes `policy-ips-attrs`	Determines the administrator's ability to manage IPS attributes (IPS and SSL/SSH Inspection) in Policies.

For more information on configuring administrator profile permissions, see Permissions on page 1011.

Firewall and IPS administrators with role separation

To configure firewall and IPS administrators with role separation:

1. Create a new admin profile with *Read Only* permissions for *IPS Objects* and *Edit Policy IPS Attributes*, and assign the admin profile to a firewall administrator.
   The firewall administrators will have the following permissions for IPS objects and attributes:
   - The firewall admin can create and update Policies, but cannot set or change IPS sensors and SSH/SSL inspection profiles in Policies.
   - The firewall admin can set and change Profile Groups and apply them to a Policy, but cannot set or change the IPS sensors and SSH/SSL inspection profiles in a Profile Group.
   - The firewall admin has Read-only permission for IPS objects.
2. Create a new restricted IPS administrator using the default *IPSadmin* admin profile.
   The IPS administrator will have the following permissions for IPS objects and attributes:
   - The IPS admin can set and change IPS sensors and SSH/SSL inspection profiles in Policies after the Firewall administrator has created the Policy.
   - The IPS admin can set and change IPS sensor and SSH/SSL inspection profiles in Profile Groups after the Firewall administrator has created the Profile Group.
   - The IPS admin can create and update IPS sensors and SSH/SSL inspection profiles and their settings within Policies.
   - The IPS admin can select individual IPS sensors or SSH/SSL inspection profiles to install to devices.

To configure a firewall admin profile in the CLI:

```
config system admin profile
   edit "FirewallAdmin"
      set system-setting read-write
      ...
      ...
      set ips-objects read <------ this is for IPS and SSH/SSL Inspection objects
      ...
      set policy-ips-attrs read <------ this is for IPS and SSH/SSL Inspection attributes setting
            in policy
      next
```

To view the default IPS admin profile in the CLI:

```
config sys admin profile
    edit IPSadmin
   show
      config system admin profile
         edit "IPSadmin"
            set type restricted
            set web-filter enable
```

```
            set ips-filter enable
            set app-filter enable
            set device-fortiextender none
            set update-incidents none
            set triage-events none
            set run-report none
            set fgt-gui-proxy disable
            set ips-lock none
            set policy-ips-attrs none
        next
    end
```

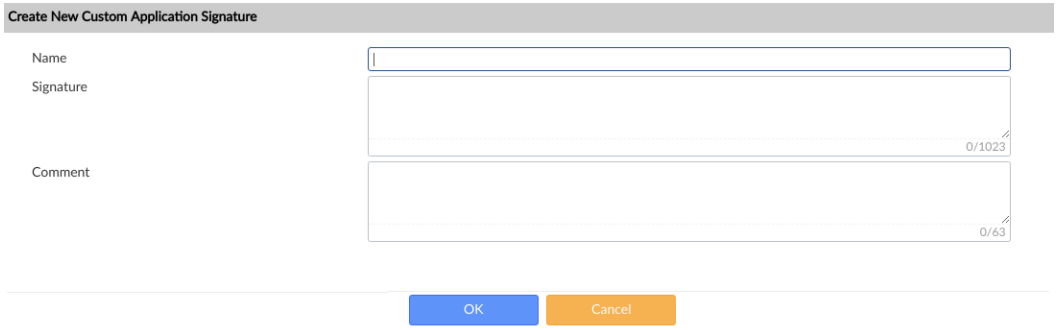
Application control restricted administrator

Application control sensors specify what action to take with network traffic generated by a large number of applications.

Custom signatures for application control

To create a custom signature for Application Control:

1. Log on as a Restricted Administrator.
2. Go to *Application Control* > *Custom Signatures*.
3. Click *Create New*. The *Create New Custom Application Signature* screen appears.



4. Specify the values for the following and click *OK*.
   - Name - specify a name for the custom signature.
   - Signature - add a custom signature.
   - Comment - toggle the status to ON.

Application control profiles

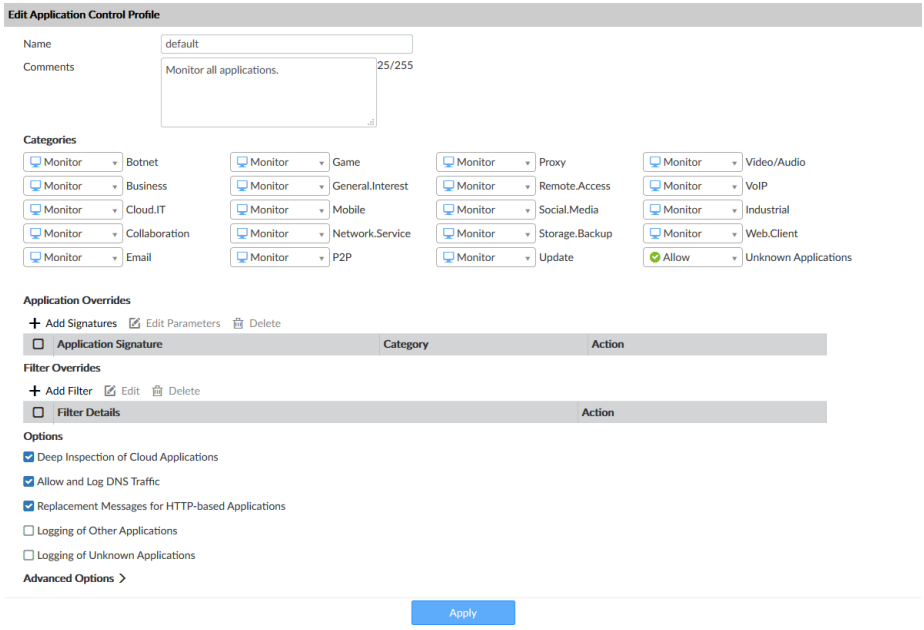
To create a profile:

1. Log in as a Restricted Administrator.
2. In the tree menu, select *Application Control*, and then select a profile category.
3. In the toolbar, click *Create New*.
4. Configure the profile settings, and click *OK*.

To clone an existing profile, right-click the profile in the content pane, and select *Clone*.

To edit a profile:

1. Log in as a Restricted Administrator.
2. In the tree menu, select *Application Control*, and then select a profile category.
3. In the content pane select a profile, and take one of the following actions:
   - In the toolbar, click *Edit*.
   - Right-click the profile, and select *Edit*.
4. Edit the settings, and click *OK*.



Name	The profile name.
Comment	Optionally, enter a description of the profile.
Categories	Select the action to take for each of the available categories: *Allow*, *Monitor*, *Block*, *Traffic Shaping*, *Quarantine*, or *Reset*.
Application Overrides	Click *Add Signatures* to add application override signatures to the table. The signatures list can be filtered to simplify adding them. Right-click on a signature to change the action (*Allow*, *Monitor*, *Block*, *Traffic Shaping*, *Quarantine*, or *Reset*).
Filter Overrides	Click *Add Filter* to add filter overrides to the table. The filters list can be searched and filtered to simplify adding them. Right-click on an override to change the action (*Allow*, *Monitor*, *Block*, *Traffic Shaping*, *Quarantine*, or *Reset*).

Deep Inspection of Cloud Applications	Select to enable deep inspections of cloud applications.
Allow and Log DNS Traffic	Select to allow and log DNS traffic.
Replacement Messages for HTTP-based Applications	Select to enable replacement messages for HTTP based applications.
Logging of Other Applications	Select to enable the logging of other applications.
Logging of Unknown Applications	Select to enable the logging of unknown applications.
Advanced Options	Configure advanced options: • p2p-block-list: Select from *bittorent*, *edonkey*, and *skype*. • replacemsg-group: Select an option from the dropdown list.

To view where a profile is being used:

1. Log in as a restricted administrator.
2. In the tree menu, select *Profiles*.
3. In the content pane, select a profile from the list, and click *Where Used* in the *More* dropdown menu. The dialog window displays the ADOM and policy package/block where the package is currently being used.
4. (Optional) Select a policy in the list, and click *View* to display the policy details.

Installing profiles as a restricted administrator

Restricted administrators can install the profiles they can access to their designated devices. Administrators can also view where a profile is used.



Restricted administrators must have *Allow to Install* enabled to install a profile. See Creating administrator profiles on page 1015.

To install a profile:



Use this option to install a modified profile to specified devices, such as a test environment.

1. Log in as a Restricted Administrator.
2. Select an ADOM.
3. In the tree menu, select a profile.
4. In the content pane, right-click a profile, and select *Install*. The *Select Installation Targets* window opens.
5. In the *Available Entries* pane, double-click a device to add it to the *Selected Entries* pane.

6. Click *Install Preview* to view the CLI script that will be installed on the selected devices. Click *Download* to download a copy of the install preview.
7. Click *Install*. The *Install* window opens and a progress bar appears at the top of the page.
8. Click *Close*.

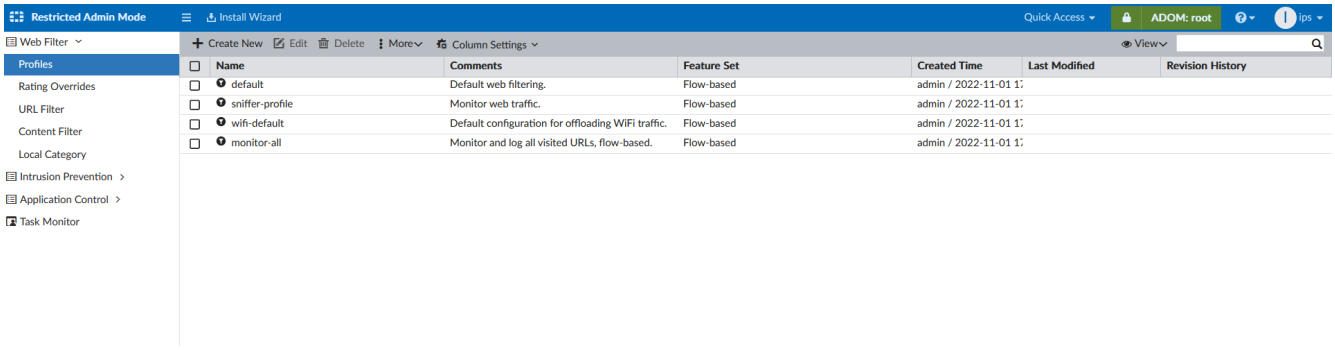
To install IPS profiles:

1. Log in as a Restricted Administrator.
2. At the top-left side of the page, click *Install Wizard*.
3. Select the IPS Sensors to be installed, and click *Next*.
4. In the *Available Entries* pane, double-click a device to add it to the *Selected Entries* pane, and click *Next*.
5. Click *Install Preview* to view the CLI script that will be installed on the selected devices. Click *Download* to download a copy of the install preview.
6. Click *Next* to begin installation to the selected device(s).
7. Click *Close*.

Workspace mode for restricted administrators

Workspace mode is supported for restricted administrators. For more information on Workspace mode, see Workspace on page 1018.

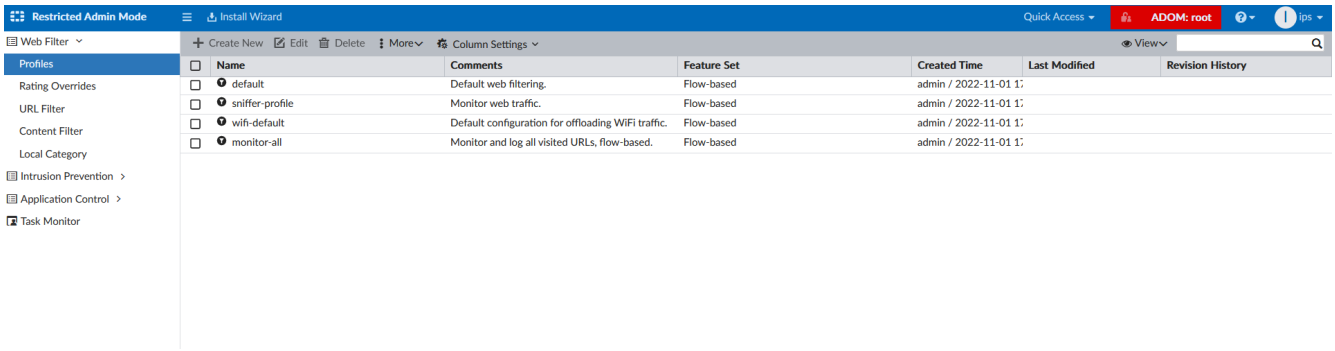
When Workspace mode is enabled on an ADOM (or all ADOMs), a lock icon appears next to the ADOM name for the restricted administrator.



Clicking the lock icon will allow restricted administrators to create, edit, and delete profiles. Once changes have been completed, the administrator can click the unlock icon. Clicking the lock icon as a restricted administrator does not lock the whole ADOM, and IPS, Web Filter, and Application Control objects can still be edited by other local and restricted administrators.

When a local administrator locks an ADOM, the entire ADOM is locked, and restricted administrators will have read-only access permissions to the ADOM until it is unlocked. The lock icon and ADOM name is displayed in red

to indicate the ADOM is locked.



Restricted administrators with read-only access permissions will not see the lock icon when Workspace mode is enabled.

Workflow mode is not supported for restricted administrators. See Workflow mode on page 1026.

Administrator profiles

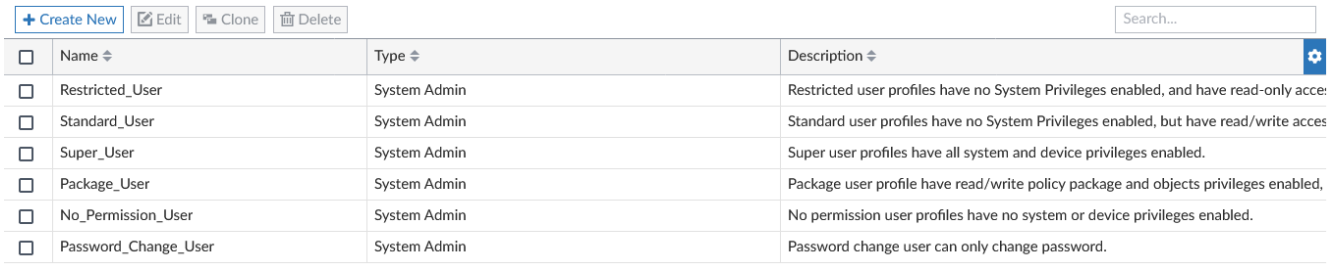
Administrator profiles are used to control administrator access privileges to devices or system features. Profiles are assigned to administrator accounts when an administrator is created. The profile controls access to both the FortiManager GUI and CLI.

There are four predefined system profiles:

Restricted_User	Restricted user profiles have no system privileges enabled, and have read-only access for all device privileges.
Standard_User	Standard user profiles have no system privileges enabled, and have read/write access for all device privileges.
Super_User	Super user profiles have all system and device privileges enabled. It cannot be edited.
Package_User	Package user profile have read/write policy and objects privileges enabled, and have read-only access for system and other privileges.
No_Permission_User	No permission user profiles have no system or device privileges enabled.
Password_Change_User	Password change user profiles can only change passwords using the CLI or API and have no access to the FortiManager GUI or other features.

These profiles cannot be deleted, but standard and restricted profiles can be edited. New profiles can also be created as required. Only super user administrators can manage administrator profiles. Package user administrators can view the profile list.

Go to *System Settings* > *Admin Profiles* to view and manage administrator profiles.



The following options are available:

Create New	Create a new administrator profile. See Creating administrator profiles on page 1015.
Edit	Edit the selected profile. See Editing administrator profiles on page 1016.
Clone	Clone the selected profile. See Cloning administrator profiles on page 1017.
Delete	Delete the selected profile or profiles. See Deleting administrator profiles on page 1017.
Search	Search the administrator profiles list.

The following information is shown:

Name	The name the administrator uses to log in.
Type	The profile type, either *System Admin* or *Restricted Admin*.
Description	A description of the system and device access permissions allowed for the selected profile.

Permissions

The below table lists the default permissions for the Super_User, Standard_User, Restricted_User and Package_User administrator profiles.

When *Read-Write* is selected, the user can view and make changes to the FortiManager system. When *Read-Only* is selected, the user can only view information. When *None* is selected, the user can neither view or make changes to the FortiManager system.



The *FortiView* setting is only available in the GUI when FortiAnalyzer features are disabled.

The *Log View/FortiView*, *Incidents & Events*, *Create & Update Incidents*, *Triage Event*, *Reports*, and *Run Report* settings are only available in the GUI when FortiAnalyzer features are enabled. See FortiAnalyzer Features on page 41.

Setting	Predefined Administrator Profile			
	Super User	Standard User	Restricted User	Package User
System Settings `system-setting`	Read-Write	None	None	Read-Only
Administrative Domain `adom-switch`	Read-Write	Read-Write	None	Read-Write
FortiGuard Center `fgd_center`	Read-Write	None	None	Read-Only
License Management `fgd-center-licensing`	Read-Write	None	None	Read-Only
Firmware Management `fgd-center-fmw-mgmt`	Read-Write	None	None	Read-Only
Settings `fgd-center-advanced`	Read-Write	None	None	Read-Only
Device Manager `device-manager`	Read-Write	Read-Write	Read-Only	Read-Write
Add/Delete/Edit Devices/Groups `device-op`	Read-Write	Read-Write	None	Read-Write
Retrieve Configuration from Devices `config-retrieve`	Read-Write	Read-Write	Read-Only	Read-Only
Revert Configuration from Revision History `config-revert`	Read-Write	Read-Write	Read-Only	Read-Only
Delete Device Revision `device-revision-deletion`	Read-Write	Read-Write	Read-Only	Read-Write
Terminal Access `term-access`	Read-Write	Read-Write	Read-Only	Read-Only
Manage Device Configurations `device-config`	Read-Write	Read-Write	Read-Only	Read-Write

Setting	Predefined Administrator Profile			
	Super User	Standard User	Restricted User	Package User
Firmware Upgrade `device-fwm-profile`	Read-Write	Read-Write	Read-Only	Read-Write
Provisioning Templates `device-profile`	Read-Write	Read-Write	Read-Only	Read-Write
SD-WAN `device-wan-link-load-balance`	Read-Write	Read-Write	Read-Only	Read-Write
Script Access `script-access`	Read-Write	Read-Write	None	Read-Write
Policy & Objects `policy-objects`	Read-Write	Read-Write	Read-Only	Read-Write
Global Policy Packages & Objects `global-policy-packages`	Read-Write	Read-Write	None	Read-Write
Assignment `assignment`	Read-Write	None	None	Read-Only
Policy Packages & Objects `adom-policy-packages`	Read-Write	Read-Write	Read-Only	Read-Write
Policy Check `consistency-check`	Read-Write	Read-Write	Read-Only	Read-Only
Edit Installation Targets `set-install-targets`	Read-Write	Read-Write	Read-Only	Read-Write
IPS Objects `ips-objects`	Read-Write	Read-Write	Read-Only	Read-Write
Edit Policy IPS Attributes `policy-ips-attrs`	Read-Write	Read-Write	Read-Only	Read-Write
Lock/Unlock ADOM `adom-lock`	Read-Write	Read-Write	Read-Only	Read-Write

Setting	Predefined Administrator Profile			
	Super User	Standard User	Restricted User	Package User
Lock/Unlock Device/Policy Package `device-policy-package-lock`	Read-Write	Read-Write	Read-Only	Read-Write
Install Policy Package or Device Configuration `deploy-management`	Read-Write	Read-Write	Read-Only	Read-Write
Import Policy Package `import-policy-packages`	Read-Write	Read-Write	Read-Only	Read-Write
Interface Mapping `intf-mapping`	Read-Write	Read-Write	Read-Only	Read-Write
AP Manager `device-ap`	Read-Write	Read-Write	Read-Only	Read-Write
FortiSwitch Manager `device-fortiswitch`	Read-Write	Read-Write	Read-Only	Read-Write
Extender Manager `device-fortiextender`	Read-Write	Read-Write	Read-Only	Read-Write
VPN Manager `vpn-manager`	Read-Write	Read-Write	Read-Only	Read-Write
Extension Access `extension-access`	Read-Write	Read-Write	None	Read-Only
FortiView `log-viewer`	Read-Write	Read-Write	Read-Only	Read-Only
Log View/FortiView `log-viewer`	Read-Write	Read-Write	Read-Only	Read-Only
Incidents & Events `event-management`	Read-Write	Read-Write	Read-Only	Read-Only
Create & Update Incidents `update-incidents`	Read-Write	Read-Write	None	None
Triage Event `triage-events`	Read-Write	Read-Write	None	None
Reports `report-viewer`	Read-Write	Read-Write	Read-Only	Read-Only
Run Report	Read-Write	Read-Write	None	None

Setting	Predefined Administrator Profile			
	Super User	Standard User	Restricted User	Package User
`run-report`				
Fabric View `fabric-viewer`	Read-Write	Read-Write	Read-Only	Read-Only
CLI only settings				
`ips-lock`	Read-Write	Read-Write	Read-Only	Read-Write



For a description of each permission, see the FortiManager CLI Reference.

Remote GUI access

The Remote GUI Access toggle can be enabled to grant administrators with the specified Admin Profile the ability to remotely access managed FortiGate devices. By default, this setting is enabled for the Super_User profile and is disabled when creating a new profile. See Remotely access a managed FortiGate on page 238.

Creating administrator profiles

To create a new administrator profile, you must be logged in to an account with sufficient privileges, or as a super user administrator.

To create a custom administrator profile:

1. Go to *System Settings* > *Admin Profiles*.
2. Click *Create New* in the toolbar. The *New Profile* pane is displayed.
3. Configure the following settings:

Profile Name	Enter a name for this profile.
Description	Optionally, enter a description for this profile. While not a requirement, a description can help to know what the profiles is for, or the levels it is set to.
Type	Select the type of profile, either *System Admin* or *Restricted Admin*.
Permission	Select which permissions to enable from *Web Filter* , *Application Control*, and *Intrusion Prevention*. This option is only available when *Type* is *Restricted Admin*. See Restricted administrators on page 989 for information.

	Allow to Install	Allows restricted administrators to install Web Filters, Intrusion Prevention, and Application Control profiles. See Installing profiles as a restricted administrator on page 1008.
Permissions		Select *None*, *Read Only*, or *Read-Write* access for the categories as required. This option is only available when *Type* is *System Admin*.
Privacy Masking		Enable/disable privacy masking. This option is only available when FortiAnalyzer features are enabled.
	Masked Data Fields	Select the fields to mask: *Destination Name*, *Source IP*, *Destination IP*, *User*, *Source Name*, *Email*, *Message*, and/or *Source MAC*.
	Data Mask Key	Enter the data masking encryption key. You need the *Data Mask Key* to see the original data.
	Data Unmasked Time(0-365 Days)	Enter the number of days the user assigned to this profile can see all logs without masking. The logs are masked if the time period in the *Log View* toolbar is greater than the number of days in the *Data Masked Time* field.
		 • Only integers between 0-365 are supported. • Time frame masking does not apply to real time logs. • Time frame masking applies to custom view and drill-down data.

4. Click *OK* to create the new administrator profile.

To apply a profile to an administrator:

1. Go to *System Settings* > *Administrators*.
2. Create a new administrator or edit an existing administrator. The *Edit Administrator* pane is displayed.
3. From the *Admin Profile* list, select a profile.

Editing administrator profiles

To edit an administrator profile, you must be logged in to an account with sufficient privileges, or as a super user administrator. The profile's name cannot be edited. The *Super_User* profile cannot be edited, and the predefined profiles cannot be deleted.

To edit an administrator:

1. Go to *System Settings* > *Admin Profiles*.
2. Double-click on a profile, right-click on a profile and then select *Edit* from the menu, or select the profile then click *Edit* in the toolbar. The *Edit Profile* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

Cloning administrator profiles

To clone an administrator profile, you must be logged in to an account with sufficient privileges, or as a super user administrator.

To edit an administrator:

1. Go to *System Settings* > *Admin Profiles*.
2. Right-click on a profile and select *Clone* from the menu, or select the profile then click *Clone* in the toolbar. The *Clone Profile* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

Deleting administrator profiles

To delete a profile or profiles, you must be logged in to an account with sufficient privileges, or as a super user administrator. The predefined profiles cannot be deleted.

To delete a profile or profiles:

1. Go to *System Settings* > *Admin Profiles*.
2. Select the profile or profiles you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the profile or profiles.

Workspace

Workspace mode enables locking ADOMs, devices, or policy packages so that an administrator can prevent other administrators from making changes to the elements that they are working in.

In workspace mode, ADOMs, or individual devices or policy packages must be locked before policy, object, or device changes can be made. Multiple administrators can lock devices and policy packages within a single, unlocked ADOM at the same time. When an individual device or policy package is locked, other administrators can only lock the ADOM that contains the locked device or policy package by disconnecting the administrator that locked it.

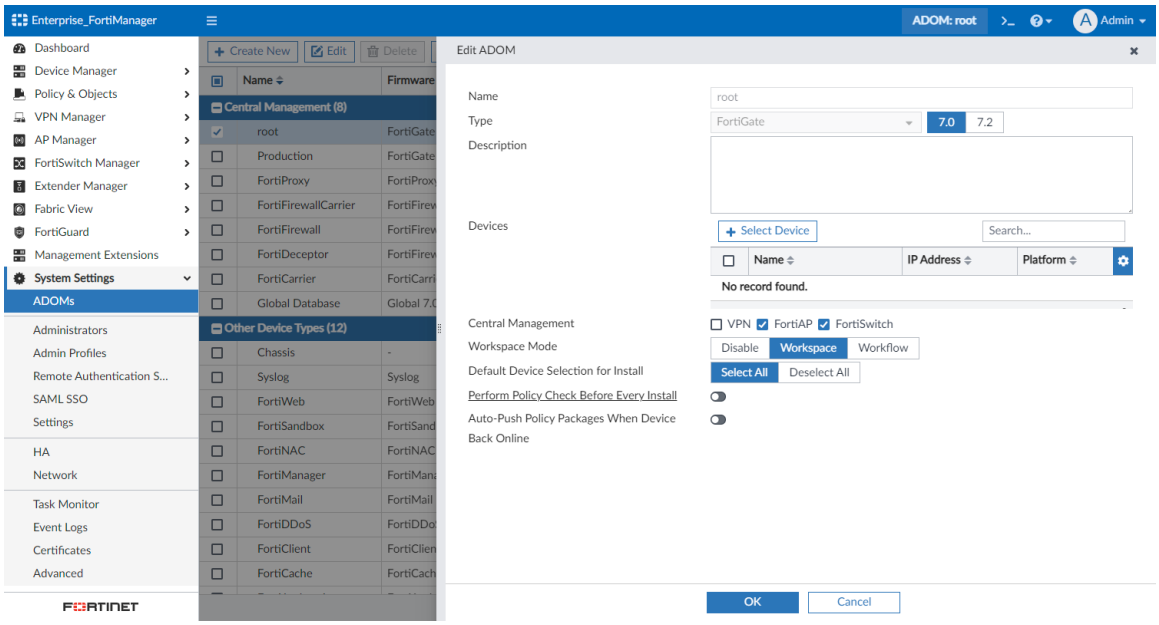
In workflow mode, only the entire ADOM can be locked. The ADOM must be locked before changes can be made, and a workflow session must be started before policy changes can be made. See Workflow mode on page 1026.

In both modes, the ADOM must be locked before changes can be made in AP Manager, FortiClient Manager, VPN Manager, and FortiSwitch Manager, and some settings in System Settings.

Workspace mode can be applied per ADOM or on all ADOMS. See Enable workspace mode on page 1019.

To enable or disable workspace in the GUI:

1. Go to *System Settings* > *ADOMs*.
2. Double-click an ADOM or device. The *Edit ADOM* page is displayed.
3. In the *Workspace Mode* area, click *Disable*, *Workspace*, or *Workflow*.



4. Click *OK*. Your session ends, and the FortiManager login screen is displayed.

To enable or disable workspace in the CLI:

1. In the *CLI Console* enter the following CLI commands:

```
config system global
   set workspace-mode {workflow | normal | disable}
end
```



A green padlock icon indicates that the current administrator locked the element. A red padlock icon indicates that another administrator locked the element.

Workspace mode

Workspace mode is used to control the creation, configuration, and installation of devices, policies, and objects. It helps to ensure that only one administrator can make changes to an element at one time.

When workspace mode is enabled, individual devices and policy packages can be locked, as well as entire ADOMs. When an individual device or policy package is locked, other administrators can only lock the ADOM that contains the locked device or policy package by disconnecting the administrator that locked it and thus breaking the lock.

Devices and policy packages can only be added if the entire ADOM is locked.



Individual devices cannot be locked if ADOMs are in advanced mode (ADOM device modes on page 928).



The entire ADOM must be locked to create a script, but the script can be run directly on a device when only the device is locked. See Run a script on page 241.

Enable workspace mode

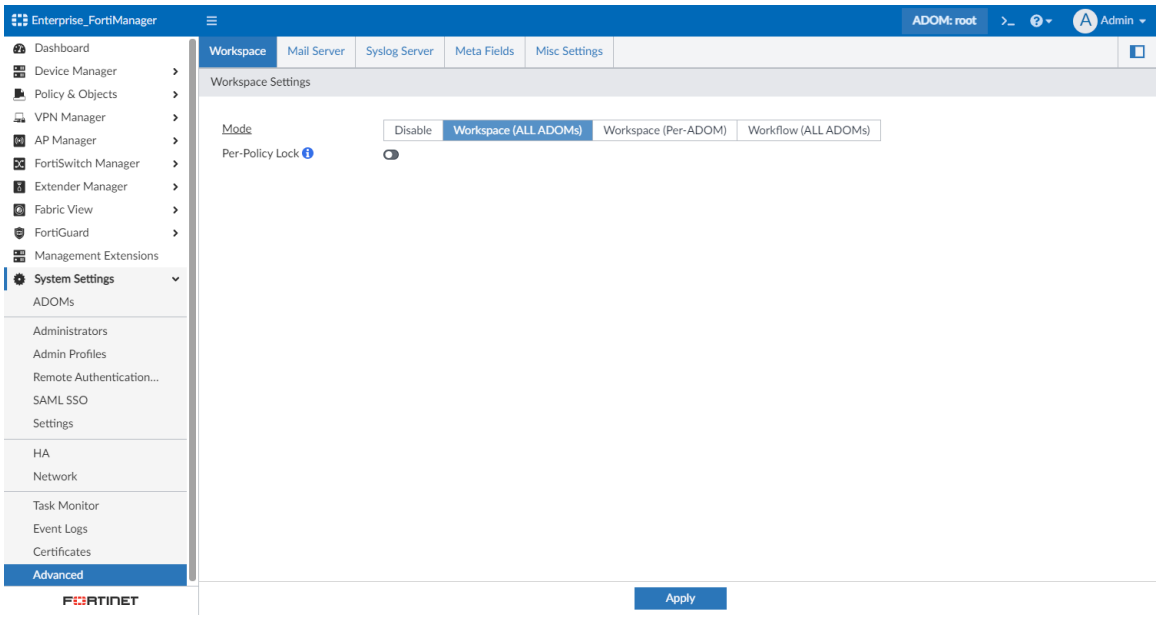
Workspace mode can be enabled per ADOM or in all ADOMs.



After changing the workspace mode, your session will end, and you will be required to log back into the FortiManager.

To enable workspace mode on all ADOMs in the GUI:

1. Go to *System Settings* > *Advanced* > *Workspace*.
2. Click *Workspace (ALL ADOMS)*.



3. Click *Apply*. Your session ends, and the FortiManager login screen is displayed.

To enable workspace mode on all ADOMs in the CLI:

```
config system global
   set workspace-mode normal
end
```

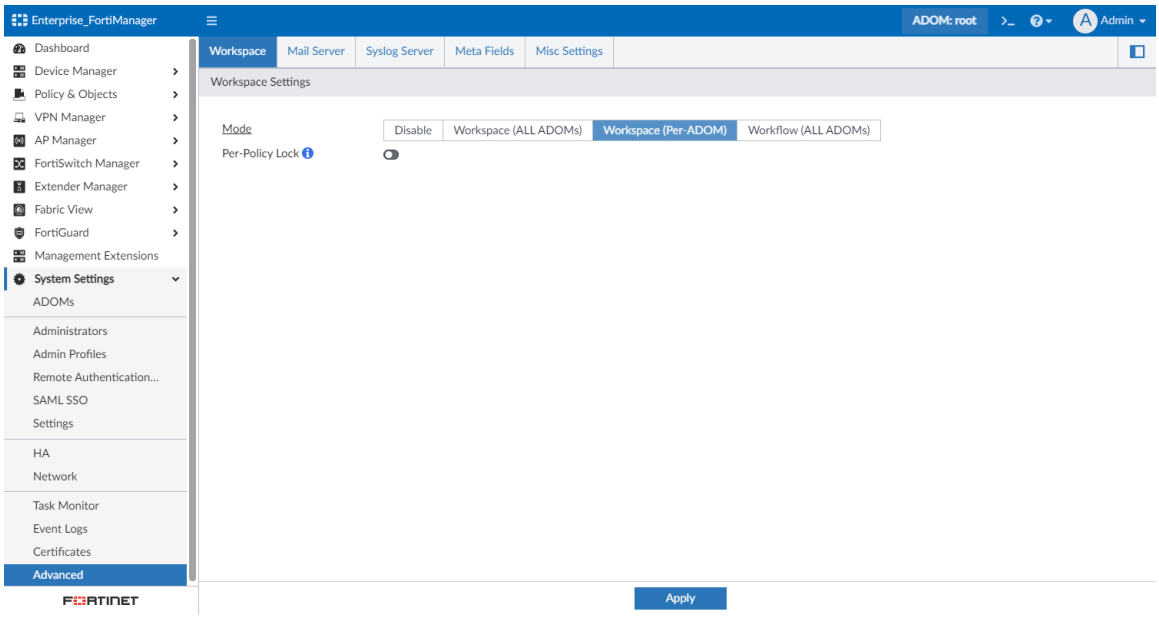


When workspace mode is enabled, *Device Manager* and *Policy & Objects* are read-only. You must lock the ADOM, a device, or a policy package before you can make any changes.

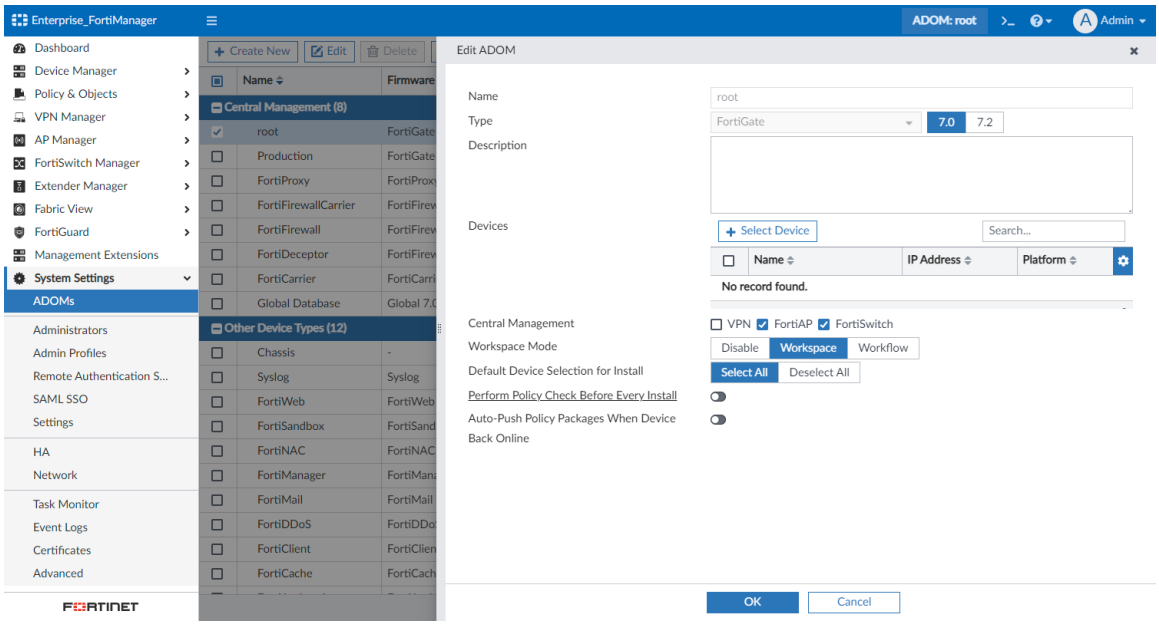
To enable workspace mode per ADOM in the GUI:

1. Ensure ADOMs are enabled.
2. Go to *System Settings* > *Advanced* > *Workspace*.

3. Click *Workspace (Per-ADOM)*. The Per-ADOM setting is enabled.



4. Click *Apply*. Your session ends, and the FortiManager login screen is displayed.
5. Log in to FortiManager, and go to *System Settings* > *ADOMs*. Ensure you are in the correct ADOM.
6. Double-click an ADOM, or right-click the ADOM and select *Edit*. The *Edit ADOM* page is displayed.
7. In the *Workspace Mode* area, click *Workspace*.



8. Click *OK*. Your session ends, and the FortiManager login screen is displayed.

To enable Per-ADOM mode in the CLI:

```
config system global
   set workspace-mode per-adom
end
```

After the Per-ADOM setting is enabled, you can update the workspace setting in the GUI.

Locking an ADOM

If workspace is enabled, you must lock an ADOM prior to making changes in Policy & Objects, AP Manager, VPN Manager, FortiSwitch Manager, and Extender Manager, as well as performing any device-level changes to a device, such as upgrading firmware for a device.



When using the FortiManager API, the ADOM does not need to be locked in order to perform device-level changes.



Policy packages, policies, objects, and devices can be individually locked. See:

- Locking a policy package on page 1024
- Lock an individual policy on page 1025
- Lock an individual object on page 1026
- Locking a device on page 1023

In the GUI, the padlock icon shown next to the ADOM name on the banner and in the *All ADOMs* list will turn green when you lock an ADOM. If it is red, it means that another administrator has locked the ADOM.

When an ADOM is locked, other administrators are unable to make changes in that ADOM until you either unlock the ADOM, or log out of the FortiManager. Optionally, ADOM lock override can be enabled, allowing an administrator to unlock an ADOM that has been locked by another administrator and discard all of their unsaved changes.

To lock the ADOM you are in:

1. Ensure you are in the ADOM that will be locked.
2. Click *Lock* in the banner, next to the ADOM name.
   The padlock icon changes to a locked state, and the ADOM is locked.

To lock an ADOM from System Settings:

1. Go to *System Settings* > *ADOMs*.
2. Right-click on the ADOM and select *Lock*, or select the ADOM then click *Lock* in the toolbar. You do not need to be in that ADOM to lock it.
   The padlock icon next to the ADOM's name changes to a locked state, and the ADOM is locked.



Locking an ADOM automatically removes locks on devices and policy packages that you have locked within that ADOM.

If you have unsaved changes, a confirmation dialog box will give you the option to save or discard them.

To unlock the ADOM you are in:

1. Ensure you are in the locked ADOM.
2. Ensure that you have saved any changes by clicking *Save* in the toolbar.

3. Click *Unlock* in the banner, next to the ADOM name. Only the administrator who locked the ADOM can unlock it. If you have not saved your changes, a confirmation dialog box will give you the option to save or discard your changes.
   The padlock icon changes to an unlocked state, and the ADOM is unlocked.

To unlock an ADOM from System Settings:

1. Go to *System Settings* > *ADOMs*.
2. Right-click on the locked ADOM and select *unlock*, or select the ADOM then click *Unlock* in the toolbar. You do not need to be in that ADOM to unlock it, but you must be the administrator that locked it. If you have not saved your changes, a confirmation dialog box will give you the option to save or discard your changes.
   The padlock icon next to the ADOM's name changes to a locked state, and the ADOM is unlocked.



All elements are unlocked when you log out of the FortiManager. If you have unsaved changes, a confirmation dialog box will give you the option to save or discard your changes.

To enable or disable ADOM lock override:

Enter the following CLI commands:

```
config system global
   set lock-preempt {enable | disable}
end
```

Locking a device

In workspace mode, a device must be locked before changes can be made to it. Other administrators will be unable to make changes to that device until you unlock it, log out of the FortiManager, or they forcibly disconnect you when they are locking the ADOM that the device is in.

Individual device locks will be removed if you lock the ADOM that the device is in.

To lock a device:

1. Ensure you are in the correct ADOM.
2. Go to *Device Manager* > *Device & Groups*.
3. In the device list, right-click on the device and select *Lock*. A padlock icon in the locked state is shown next to the device name to indicate that the device is locked.
   Other administrators are now unable to make changes to the device, and cannot lock the ADOM without first forcing you to disconnect.



Individual devices cannot be locked if ADOMs are in advanced mode (ADOM device modes on page 928).

To unlock a device:

1. Ensure you are in the correct ADOM.
2. Go to *Device Manager* > *Device & Groups*.
3. Ensure that you have saved any changes by clicking *Save* in the toolbar.
4. In the device list, right-click on the locked device and select *Unlock*. If you have not saved your changes, a confirmation dialog box will give you the option to save or discard your changes.
   After unlocking, the padlock icon next to the device name is removed, and the device is unlocked. The device will also be unlocked when you log out of the FortiManager.



All devices are unlocked when you log out of the FortiManager. If you have unsaved changes, a confirmation dialog box will give you the option to save or discard them.

Locking a policy package

In workspace mode, a policy package must be locked before changes can be made to it. Other administrators will be unable to make changes to that policy package until you unlock it, log out of the FortiManager, or they forcibly disconnect you when they are locking the ADOM that the package is in.

Individual device locks will be removed if you lock the ADOM that the package is in.

To lock a policy package:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the policy package list, right-click on the package and select *Lock*. A padlock icon in the locked state is shown next to the package name to indicate that it is locked.
   Other administrators are now unable to make changes to the policy package, and cannot lock the ADOM without first forcing you to disconnect.

To unlock a policy package:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Ensure that you have saved any changes by clicking *Save* in the toolbar.
4. In the policy package list, right-click on the locked package and select *Unlock*. If you have not saved your changes, a confirmation dialog box will give you the option to save or discard your changes.
   After unlocking, the padlock icon next to the package name is removed, and the package is unlocked. The package will also be unlocked when you log out of the FortiManager.



All policy packages are unlocked when you log out of the FortiManager. If you have unsaved changes, a confirmation dialog box will give you the option to save or discard them.

Lock an individual policy

In workspace mode, administrators can lock individual policies, except for policies used by policy blocks. You cannot lock an individual policy when the policy is used in a policy block.

If you want to modify a policy, you don't need to lock the entire policy package. Once you lock a policy, a padlock icon appears beside the policy. Others are now unable to modify your policy or lock the policy package where the locked policy is in, and unable to lock the ADOM.

You cannot lock an individual policy when the policy it is used in a policy block.



If you move your cursor to the padlock icon, you can see who locked the policy and the time at which it was locked.

To enable per-policy lock in the GUI:

1. Go to *System Settings* > *Advanced* > *Workspace*.
2. Enable Workspace mode.
3. Toggle the *Per-Policy Lock* setting to the *ON* position.

To enable per policy lock in the CLI:

1. In the *CLI Console* widget enter the following CLI commands:

```
config system global
   set per-policy-lock enable
end
```

To lock a policy:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the policy package list, select the policy package, and right-click on the policy and select *Edit*.
   The *Edit IPv4 Policy* pane opens.
4. In the *Edit IPv4 Policy* pane, modify the name and then click *OK*.
   A padlock icon in the locked state is shown next to the policy name to indicate that it is locked.
   You can still lock the policy package or the whole ADOM with confirmation.
   Other administrators are now unable to make changes to this policy or the policy package, and cannot lock the ADOM without first forcing you to disconnect.
5. Click *Save* in the toolbar to save your changes.



A green padlock icon next to the sequence number of the policy indicates that the current administrator locked the policy. A red padlock icon indicates that another administrator locked the policy.

Sequence lock:

If you add two or more policies, a sequence lock appears at the top. The sequence lock ensures that the order of the policies is managed by one administrator at any given time, other administrators see a red padlock icon at the top.

Once you save your changes, the sequence lock disappears allowing other administrators to change the order of the policies.



If an administrator sets up a sequence lock, other administrators can neither create a new policy nor insert a policy. They can however, edit an existing policy.

Lock an individual object

In Workspace mode, when you lock an ADOM, all objects in that ADOM are locked, and other administrators are prevented from modifying any objects within the ADOM.

You can alternatively lock individual objects so that others remain available for other administrators to modify. To lock an individual object, you must first lock a policy package or individual policy (if per-policy lock is enabled). Once the policy package or policy is locked, you can proceed to lock and modify individual objects in the ADOM.

When editing a policy package or policy, you do not need to lock an individual object before editing it, but doing so will prevent any potential conflicts that may occur if another administrator chooses to edit the same object at the same time.

To lock an individual object in Workspace mode:

1. Lock a Policy Package or individual Policy. See Locking a policy package on page 1024 and Lock an individual policy on page 1025
2. Go to *Policy & Objects* and locate the object you want to modify.
3. Right-click on the object in the table, and select *Lock*.
   The object is now locked. Other administrators will see a red lock icon next to the object indicating that it cannot be edited.
4. Complete and save your changes to the object.
5. Right-click on the object in the table, and select *Unlock*.

Workflow mode

Workflow mode is used to control the creation, configuration, and installation of policies and objects. It helps to ensure all changes are reviewed and approved before they are applied.

When workflow mode is enabled, the ADOM must be locked and a session must be started before policy or object changes can be made in an ADOM. Workflow approvals must be configured for an ADOM before any sessions can be started in it.

Once the required changes have been made, the session can either be discarded and the changes deleted, or it can be submitted for approval. The session can also be saved and continued later, but no new sessions can be created until the saved session has been submitted or discarded.

When a session is submitted for approval, email messages are sent to the approvers, who can then approve or reject the changes directly from the email message. Sessions can also be approved or rejected by the approvers from within the ADOM itself.



Sessions must be approved in the order they were created.

If one approver from each approval group approves the changes, then another email message is sent, and the changes are implemented. If any of the approvers reject the changes, then the session can be repaired and resubmitted as a new session, or discarded. When a session is discarded, all later sessions are also discarded. After multiple sessions have been approved, a previous session can be reverted to, undoing all the later sessions.

The changes made in a session can be viewed at any time from the session list in the ADOM by selecting *View Diff*. The ADOM does not have to be locked to view the differences.

Enable workflow mode

Workflow mode can be enabled per ADOM or in all ADOMs at the same time.



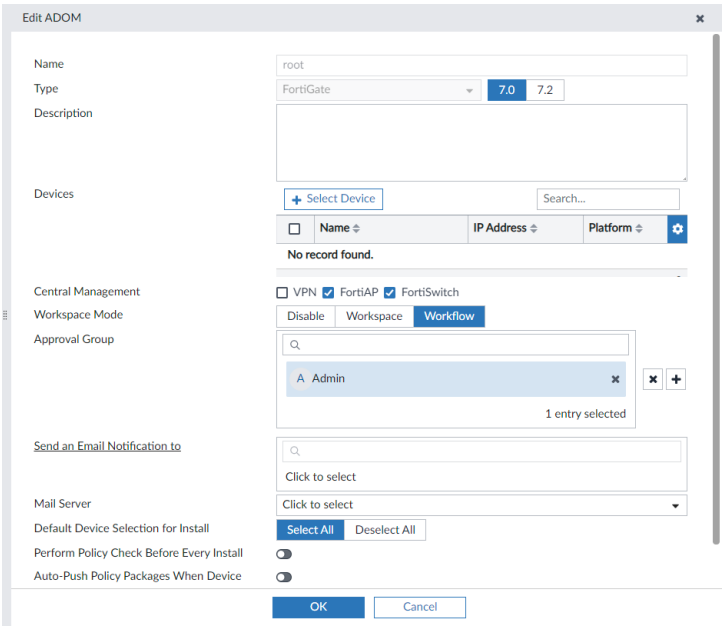
After changing the workspace mode, your session will end, and you will be required to log back in to the FortiManager.

To enable workflow mode on all ADOMs in the GUI:

1. Go to *System Settings* > *Advanced* > *Workspace*.
2. Click *Workflow (ALL ADOMS)*.
3. Create the workflow approvals.
   a. Click Create New.
   b. Click the *ADOM* dropdown, and select an ADOM.
   c. Click the *Approval Group # 1* dropdown, select the users who will approve changes.
   d. (Optional) Click the add (+) button to add another approval group.
   e. In the *Send an Email Notification to* field, select the user who will receive the email notification.
   f. (Optional) from the *Mail Server* dropdown, select the mail server.
   g. Click *OK*.
4. Click *Apply*. Your session ends, and the FortiManager login screen is displayed.

To enable workflow mode per-ADOM in the GUI:

1. Enable Per-ADOM mode.
   a. Go to *System Settings* > *Advanced* > *Workspace*.
   b. Click *Workspace (Per-ADOM)*.
   c. Click *Apply*.Your session ends, and the FortiManager login screen is displayed.
2. Log in to FortiManager, and go to *System Settings* > *ADOMs*.
3. Double-click an ADOM, or right-click the ADOM and select *Edit*. The *Edit ADOM* page is displayed.
4. In the *Workspace Mode* area, click *Workflow*.
5. In the *Approval Group* field, select the users who will approve changes.
6. (Optional) Click the add (+) button to add another approval group.
7. In the *Send an Email Notification to* field, select the user who will receive the email notification.



8. (Optional) from the *Mail Server* dropdown, select the mail server.
9. Click *OK*. Your session ends, and the FortiManager login screen is displayed.

When workflow mode is enabled, *Device Manager* and *Policy & Objects* become read-only. You must lock the ADOM to create a new workflow session.

To disable workflow mode in all ADOMs in the GUI:

1. Go to *System Settings* > *Advanced* > *Workspace*.
2. Click *Disable*.

To enable per-ADOM mode in the CLI:

```
config system global
   set workspace-mode per-adom
end
```

Once `per-adom` is enabled, you can configure the workflow setting in the GUI.

To enable workflow mode in all ADOMs in the CLI:

```
config system global
   set workspace-mode workflow
end
```

When `workspace-mode` is `workflow`, *Device Manager* and *Policy & Objects* are read-only. You must lock the ADOM to create a new workflow session.

Workflow approval

Workflow approval matrices specify which users must approve or reject policy changes for each ADOM.

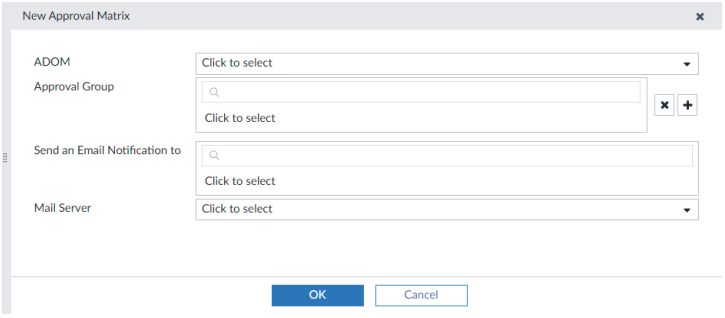
Up to eight approval groups can be added to an approval matrix. One user from each approval group must approve the changes before they are accepted. An approval email will automatically be sent to each member of each approval group when a change request is made.

Email notifications are automatically sent to each approver, as well as other administrators as required. A mail server must be configured, see Mail Server on page 964, and each administrator must have a contact email address configured, see Managing administrator accounts on page 977.

This menu is only available when `workspace-mode` is set to `workflow`.

To create a new approval matrix:

1. Go to *System Settings* > *Advanced* > *Workspace* and ensure *Mode* is set to *Workflow (ALL ADOMs)*.
2. Click *Create New*.



3. Configure the following settings:

ADOM	Select the ADOM from the dropdown list.
Approval Group	Select to add approvers to the approval group. Select the add icon to create a new approval group. Select the delete icon to remove an approval group.

	At least one approver from each group must approve the change for it to be adopted.
Send an Email Notification to	Select to add administrators to send email notifications to. The administrator must have a valid email address. See Creating administrators on page 979.
Mail Server	Select the mail server from the dropdown list. A mail server must already be configured. See Mail Server on page 964.

4. Click *OK* to create the approval matrix.

Workflow sessions

Administrators use workflow sessions to make changes to policies and objects. The session is then submitted for review and approval or rejection by the administrators defined in the ADOMs workflow approval matrix.

Administrators with the appropriate permissions will be able to approve or reject any pending requests. When viewing the session list, they can choose any pending sessions, and click the approve or reject buttons. They can also add a comment to the response. A notification will then be sent to the administrator that submitted the session and all of the approvers.



You cannot prevent administrators from approving their own workflow sessions.

If the session was approved, no further action is required. If the session was rejected, the administrator will need to either repair or discard the session.

The Global Database ADOM includes the *Assignment* option, for assigning the global policy package to an ADOM. Assignments can only be created and edited when a session is in progress. After a global database session is approved, the policy package can be assigned to the configured ADOM. A new session will be created on the assigned ADOM and automatically submitted; it must be approved for the changes to take effect.

A session can be discarded at any time before it is approved.

After multiple sessions have been submitted or approved, a previously approved session can be reverted to, undoing all the later sessions. This creates a new session at the top of the session list that is automatically submitted for approval.



A workflow approval matrix must be configure for the ADOM to which the session applies before a workflow session can be started. See Workflow approval on page 1029.

Starting a workflow session

A workflow session must be started before changes can be made to the policies and objects. A session can be saved and continued at a later time, discarded, or submitted for approval.

While a session is in progress, devices cannot be added or installed.

To start a workflow session:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. Click *Lock* in the banner. The padlock icon changes to a locked state and the ADOM is locked.
4. From the *Sessions* menu, select *Session List*. The *Session List* dialog box opens; see The session list on page 1035.
5. Click *Create New Session*.



6. Enter a name for session, add a comment describing the session, then click *OK* to start the session. You can now make the required changes to the policy packages and objects. See Policy & Objects on page 407.

Saved sessions

A session can be saved and continued later.

A new session cannot be started until the in-progress or saved session has either been submitted for approval or discarded.

To save your session:

While currently working in a session, click *Save* in the toolbar. After saving the session, the ADOM will remain locked, and you can continue to edit it.

To continue a saved session:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and lock the ADOM.
3. Go to *Sessions* > *Session List*. The *Session List* dialog box opens.

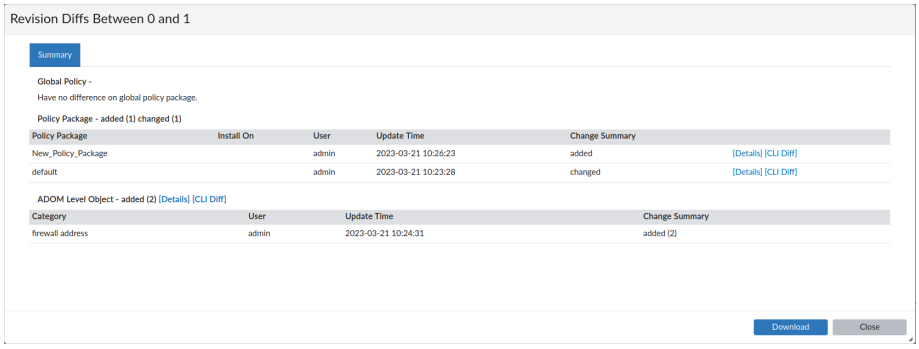
4. Click *Continue Session In Progress* to continue the session.

View session diff

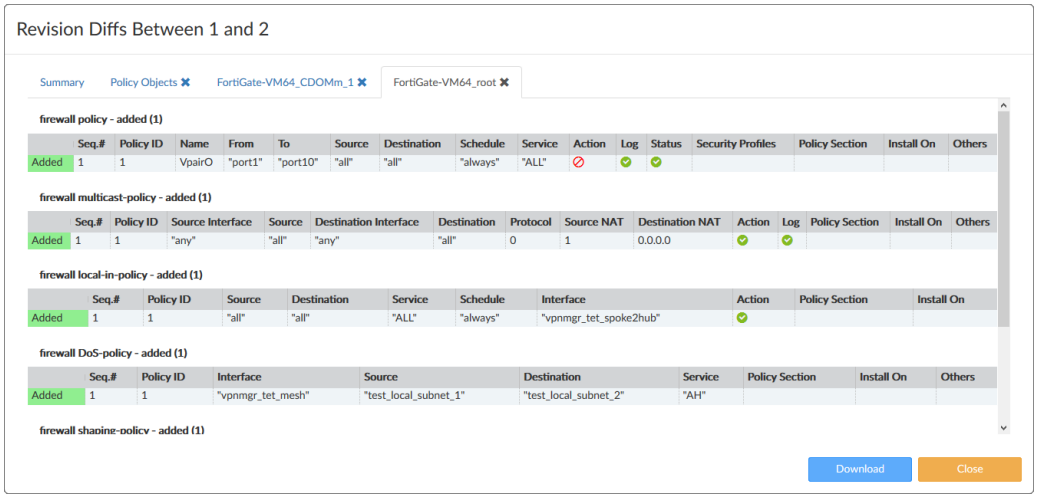
A session diff can be viewed prior to submitting the session for approval.

To view the session diff:

1. While currently working in a session, ensure that the session has been saved. See Saved sessions on page 1031.
2. Click *Sessions* > *View Diff*. The *Revisions Diff* dialog box opens.



3. Select *Details* to view specific changes within a policy package or the policy objects.



4. Select *CLI Diff* to view the specific CLI configuration changes.
5. Click *Download* to download a CSV file of the changes to your management computer.
6. Click *Close* to close the dialog box and return to the session.

Discarding a session

A session can be discarded at any time before it is approved. A session cannot be recovered after it is discarded.

When a session is discarded, all sessions after it in the session list will also be discarded.

To discard an in-progress session:

1. Select *Session* > *Discard*.
2. Enter comments in the *Discard Session* dialog box.
3. Click *OK*. The changes are deleted and the session is discarded.

To discard saved, submitted, or rejected sessions:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and lock the ADOM.
3. Go to *Sessions* > *Session List*. The *Session List* dialog box opens.
4. Select the session that is to be discarded, then click *Discard*.
5. Select *OK* in the *Discard* Session pop-up.

Submitting a session

When all the required changes have been made, the session can be submitted for approval. A session must be open to be submitted for approval.

When the session is submitted, email messages are sent to all of the approvers and other administrators defined in the approval matrix (see Workflow approval on page 1029), and the ADOM is automatically unlocked.

To submit a session for approval:

1. Select *Sessions* > *Submit*.
2. Enter the following in the *Submit for Approval* dialog box:

Comments	Enter a comment describing the changes that have been made in this session.
Attach configuration change details	Select to attach configuration change details to the email message.

3. Click *OK* to submit the session.

Approving or rejecting a session

Sessions can be approved or rejected by the members of the approval groups either directly from the email message that is generated when the session is submitted, or from the session list. Sessions must be approved in order they were submitted. A session that has been rejected must be repaired or discarded before the next session can be approved.

When a session is approved or rejected, new email messages are sent out.

To approve or reject a session from the email message:

1. If the configuration changes HTML file is attached to the email message, open the file to review the changes.
2. Select *Approve this request* or *Reject this request* to approve or reject the request. You can also Select *Login FortiManager to process this request* to log in to the FortiManager and approve or reject the session from the session list.

   A web page will open showing the basic information, approval matrix, and session log for the session, highlighting if the session was approved or rejected. A new email message will also be sent containing the same information.
3. On the last line of the session log on the web page, select *Click here to add comments* to add a comment about why the session was approved or rejected.

To approve a session from the session list:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and lock the ADOM.
3. Go to *Sessions* > *Session List*. The *Session List* dialog box opens; see The session list on page 1035.
4. Select a session that can be approved from the list.
5. Optionally, click *View Diff* to view the changes that you are approving.
6. Click *Approve*.
7. Enter a comment in the *Approve Session* pop-up, then click *OK* to approve the session.

To reject a session from the session list:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and lock the ADOM.
3. Go to *Sessions* > *Session List*. The *Session List* dialog box opens; see The session list on page 1035.
4. Select a session that can be rejected from the list.
5. Optionally, click *View Diff* to view the changes that you are rejecting.
6. Click *Reject*.
7. Enter a comment in the *Reject Session* pop-up, then click *OK* to reject the session.

Repairing a rejected session

When a session is rejected, it can be repaired to correct the problems with it.

To repair a workflow session:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and lock the ADOM.
3. Go to *Sessions* > *Session List*. The *Session List* dialog box opens; see The session list on page 1035.
4. Select a rejected session, then click *Repair*.
   A new session is created and started, with the changes from the rejected session, so it can be corrected.

Reverting a session

A session can be reverted to after other sessions have been submitted or approved. If this session is approved, it will undo all the changes made by later sessions, though those sessions must be approved before the reverting session can be approved. You can still revert to any of those sessions without losing their changes.

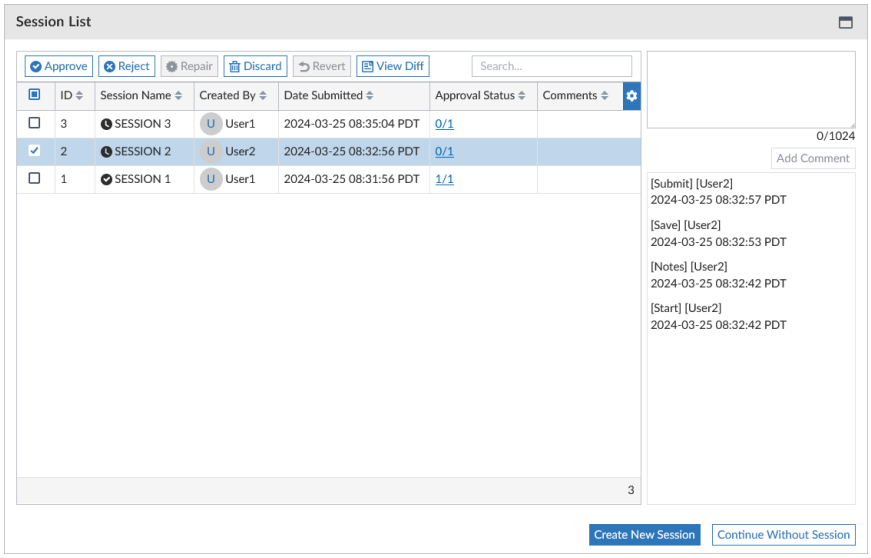
When a session is reverted, a new session is created and automatically submitted for approval.

To revert a session:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and lock the ADOM.
3. Go to *Sessions* > *Session List*. The *Session List* dialog box opens; see The session list on page 1035.
4. Select the session, then click *Revert*.

The session list

To view the session list, In *Policy & Objects*, go to *Sessions* > *Session List*. Different options will be available depending on the various states of the sessions (in progress, approved, etc.). When an ADOM is unlocked, only the comments and *View Diff* command are available.



The following options and information are available:

Approve	Approve the selected session. Enter comments in the *Approve Session* dialog box as required. See Approving or rejecting a session on page 1033.
Reject	Reject the selected session. Enter comments in the *Reject Session* dialog box as required. A rejected session must be repaired before the next session in the list can be approved. See Approving or rejecting a session on page 1033.
Discard	Discard the selected session. If a session is discarded, all later sessions are also discarded.

Repair	Repair the selected rejected session. A new session will be created and added to the top of the session list with the changes from the rejected session so they can be repaired as needed. See Repairing a rejected session on page 1034.
Revert	Revert back to the selected session, undoing all the changes made by later sessions. A new session will be created, added to the top of the session list, and automatically submitted for approval. See Reverting a session on page 1035.
View Diff	View the changes that were made prior to approving or rejecting the session. Select *Details* to view specific changes within a policy package.
ID	A unique number to identify the session.
Name	The user-defined name to identify the session. The icon shows the status of the session: waiting for approval, approved, rejected, repaired, or in progress. Hover the cursor over the icon to see a description.
User	The administrator who created the session.
Date Submitted	The date and time the session was submitted for approval.
Approved/...	The number of approval groups that have approved the session out of the number of groups that have to approve the session. Hover the cursor over the table cell to view the group members.
Comments	The comments for the session. All the comments are shown on the right of the dialog box for the selected session. Session approvers can also add comments to the selected session without having to approve or reject the session.
Create New Session	Select to create a new workflow session. This option is not available when a session has been saved or is already in progress.
Continue Session in Progress	Select to continue a session that was previously saved or is already in progress. This option is only available when a session is in progress or saved.
Continue Without Session	Select to continue without starting a new session. When a new session is not started, all policy and objects are read-only.

Install and unlock setting for Workspace mode

You can optionally configure Workspace mode to include the *Install and Unlock* option when performing an installation.

This setting is helpful for ensuring that ADOMs do not remain locked after the administrator has completed their work.

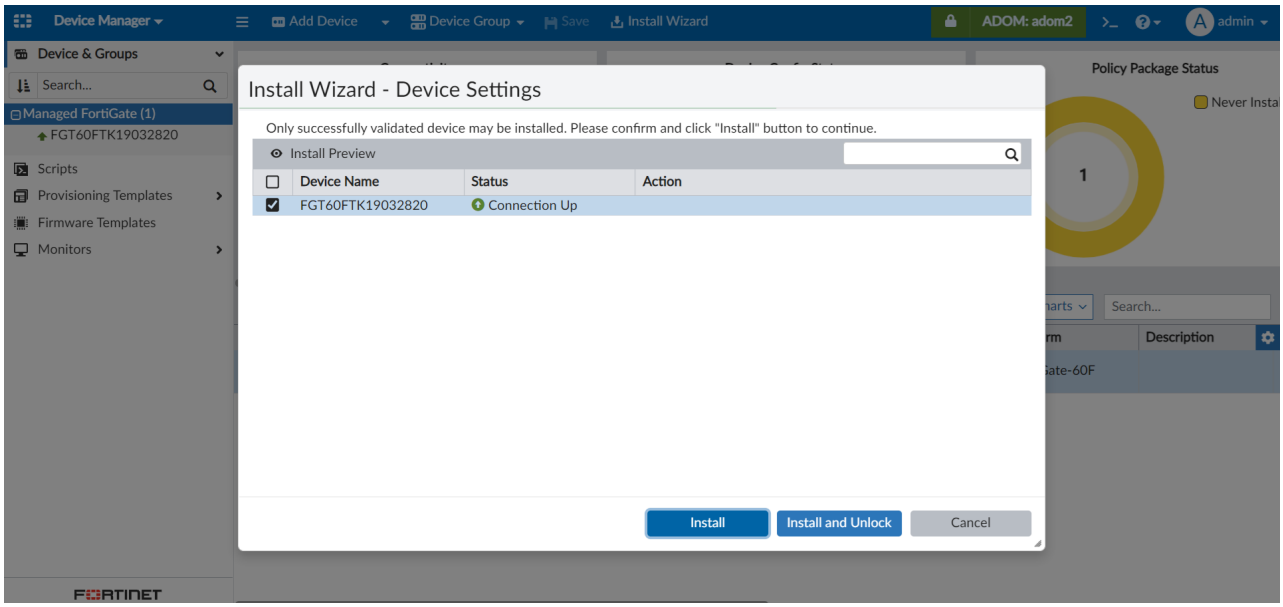
This setting can only be configured in the CLI after workspace mode has been enabled.

To enable the install and unlock setting in Workspace mode:

1. In the FortiManager CLI, enter the following commands:

```
config system global
set workspace-unlock-after-install enable
```

2. The next time an administrator performs work in a locked ADOM and opens the Install Wizard, they will see the following option included to *Install and Unlock*. When selecting this option, the ADOM will be automatically unlocked once the install is complete.



Authentication

The FortiManager system supports authentication of administrators locally, remotely with RADIUS, LDAP, or TACACS+ servers, and using PKI. Remote authentication servers can also be added to authentication groups that administrators can use for authentication.

To use PKI authentication, you must configure the authentication before you create the administrator accounts. See Public Key Infrastructure on page 1037 for more information.

To use remote authentication servers, you must configure the appropriate server entries in the FortiManager unit for each authentication server in your network. New LDAP remote authentication servers can be added and linked to all ADOMs or specific ADOMs. See LDAP servers on page 1040, RADIUS servers on page 1042, TACACS+ servers on page 1044, and Remote authentication server groups on page 1045 for more information.

Public Key Infrastructure

Public Key Infrastructure (PKI) authentication uses X.509 certificate authentication library that takes a list of peers, peer groups, and user groups and returns authentication successful or denied notifications. Administrators only need a valid X.509 certificate for successful authentication; no username or password is necessary.

To use PKI authentication for an administrator, you must configure the authentication before you create the administrator accounts. You will also need the following certificates:

- an X.509 certificate for the FortiManager administrator (administrator certificate)
- an X.509 certificate from the Certificate Authority (CA) which has signed the administrator's certificate (CA Certificate)

For more information on the CSR generation process, see Local certificates on page 956.

To get the CA certificate:

1. Log into your FortiAuthenticator.
2. Go to *Certificate Management > Certificate Authorities > Local CAs*.
3. Select the certificate and select *Export* in the toolbar to save the `ca_fortinet.com` CA certificate to your management computer. The saved CA certificate's filename is `ca_fortinet.com.crt`.

To get the administrator certificate:

1. Log into your FortiAuthenticator.
2. Go to *Certificate Management > End Entities > Users*.
3. Select the certificate and select *Export* in the toolbar to save the administrator certificate to your management computer. The saved CA certificate's filename is `admin_fortinet.com.p12`. This PCKS#12 file is password protected. You must enter a password on export.

To import the administrator certificate into your browser:

1. In Mozilla Firefox, go to *Options > Advanced > Certificates > View Certificates > Import*.
2. Select the file `admin_fortinet.com.p12` and enter the password used in the previous step.

To import the CA certificate into the FortiManager:

1. Log into your FortiManager.
2. Go to *System Settings > Certificates*.
3. Click *Create New/Import > CA Certificate*, and browse for the `ca_fortinet.com.crt` file you saved to your management computer, or drag and drop the file onto the dialog box. The certificate is displayed as *CA_Cert_1*.

To create a new PKI administrator account:

1. Go to *System Settings > Administrators*.
2. Click *Create New*. The *Create New Administrator* pane opens.
   See Creating administrators on page 979 for more information.
3. Select *PKI* for the *Admin Type*.
4. Enter a comment in the *Subject* field for the PKI administrator.
5. Select the CA certificate from the dropdown list in the *CA* field.
6. Click *OK* to create the new administrator account.

PKI authentication must be enabled via the FortiManager CLI with the following commands:

```
config system global
   set clt-cert-req enable
end
```

When connecting to the FortiManager GUI, you must use HTTPS when using PKI certificate authentication.

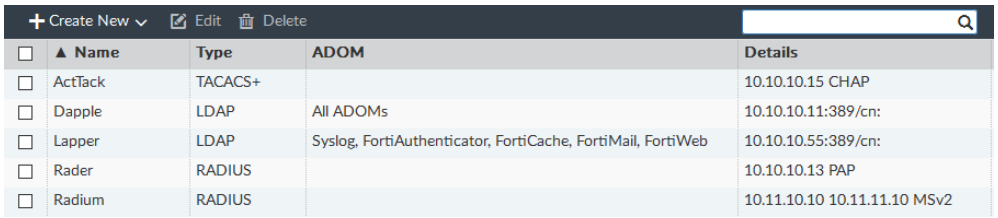
When `clt-cert-req` is set to optional, the user can use certificate authentication or user credentials for GUI login.

Managing remote authentication servers

The FortiManager system supports remote authentication of administrators using LDAP, RADIUS, and TACACS+ remote servers. To use this feature, you must configure the appropriate server entries for each authentication server in your network, see LDAP servers on page 1040, RADIUS servers on page 1042, and TACACS+ servers on page 1044 for more information.

Remote authentication servers can be added, edited, deleted, and added to authentication groups (CLI only).

Go to *System Settings* > *Remote Authentication Server* to manage remote authentication servers.



The following options are available:

Create New	Add an LDAP, RADIUS, or TACACS+ remote authentication server. See LDAP servers on page 1040, RADIUS servers on page 1042, and TACACS+ servers on page 1044.
Edit	Edit the selected remote authentication server. See Editing remote authentication servers on page 1040.
Delete	Delete the selected remote authentication server or servers. See Deleting remote authentication servers on page 1040.

The following information is displayed:

Name	The name of the server.

Type	The server type: *LDAP*, *RADIUS*, or *TACACS+*.
ADOM	The administrative domain(s) which are linked to the remote authentication server.
Details	Details about the server, such as the IP address.

Editing remote authentication servers

To edit a remote authentication server, you must be logged in to an account with sufficient privileges, or as a super user administrator. The server's name cannot be edited.

To edit a remote authentication server:

1. Go to *System Settings > Remote Authentication Server*.
2. Double-click on a server, right-click on a server and then select *Edit* from the menu, or select the server then click *Edit* in the toolbar. The *Edit Server* pane for that server type opens.
3. Edit the settings as required, and then select *OK* to apply the changes.
   See LDAP servers on page 1040, RADIUS servers on page 1042, and TACACS+ servers on page 1044 for more information.

Deleting remote authentication servers

To delete a remote authentication server or servers, you must be logged in to an account with sufficient privileges, or as a super user administrator.

To delete a remote authentication server or servers:

1. Go to *System Settings > Remote Authentication Server*.
2. Select the server or servers you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the server or servers.

LDAP servers

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

If you have configured LDAP support and an administrator is required to authenticate using an LDAP server, the FortiManager unit sends the administrator's credentials to the LDAP server for authentication. If the LDAP server can authenticate the administrator, they are successfully authenticated with the FortiManager unit. If the LDAP server cannot authenticate the administrator, the FortiManager unit refuses the connection.

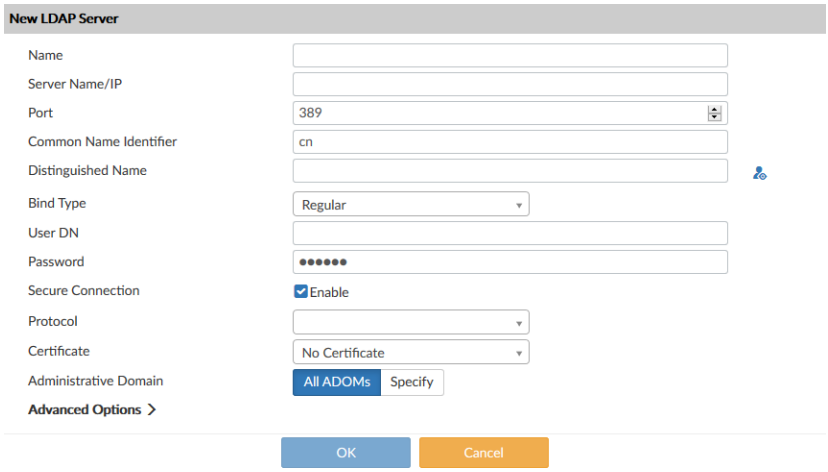
When configuring an LDAP connection to an Active Directory server, an administrator must provide Active Directory user credentials.

- To secure this connection, use LDAPS on both the Active Directory server and FortiManager.
- Apply the principle of least privilege. For the LDAP regular bind operation, do not use credentials that provide full administrative access to the Windows server when using credentials.

To use an LDAP server to authenticate administrators, you must configure the server before configuring the administrator accounts that will use it.

To add an LDAP server:

1. Go to *System Settings* > *Remote Authentication Server*.
2. Select *Create New* > *LDAP Server* from the toolbar. The *New LDAP Server* pane opens.



3. Configure the following settings, and then click *OK* to add the LDAP server.

Name	Enter a name to identify the LDAP server.
Server Name/IP	Enter the IP address or fully qualified domain name of the LDAP server.
Port	Enter the port for LDAP traffic. The default port is 389.
Common Name Identifier	The common name identifier for the LDAP server. Most LDAP servers use `cn`. However, some servers use other common name identifiers such as `UID`.
Distinguished Name	The distinguished name is used to look up entries on the LDAP server. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier. Clicking the *query distinguished name* icon will query the LDAP server for the name and open the *LDAP Distinguished Name Query* window to display the results.
Bind Type	Select the type of binding for LDAP authentication: *Simple*, *Anonymous*, or *Regular*.
User DN	When the *Bind Type* is set to *Regular*, enter the user DN.

Password	When the *Bind Type* is set to *Regular*, enter the password.
Secure Connection	Select to use a secure LDAP server connection for authentication.  When configuring LDAP settings with a secure connection, certificates signed using the sha1RSA algorithm are not accepted; use supported algorithms such as sha256RSA instead.
Protocol	When *Secure Connection* is enabled, select either LDAPS or STARTTLS.
Certificate	When *Secure Connection* is enabled, select the certificate from the dropdown list.
Administrative Domain	Choose the ADOMs that this server will be linked to for reporting: *All ADOMs* (default), or *Specify* for specific ADOMs.
Advanced Options	
adom-attr	Specify an attribute for the ADOM.
attributes	Specify the attributes such as *member*, *uniquemember*, or *memberuid*.
filter	Specify the filter in the format `(objectclass=*)`
group	Specify the name of the LDAP group.
memberof-attr	Specify the value for this attribute. This value must match the attribute of the group in LDAP Server. All users part of the LDAP group with the attribute matching the *memberof-attr* will inherit the administrative permissions specified for this group.
profile-attr	Specify the attribute for this profile.
secondary-server	Specify a secondary server.

ssl-protocol	Set the lowest SSL protocol version for connection to LDAP server.
	By default, this will follow the global SSL protocol, which is configured in the CLI using the following command:
	`config system global`
	`set global-ssl-protocol {sslv3 | tlsv1.0 | tlsv1.1 | tlsv1.2 | tlsv1.3}`
	`end`
	For more information, see the FortiManager CLI Reference.

tertiary-server	Specify a tertiary server.

RADIUS servers

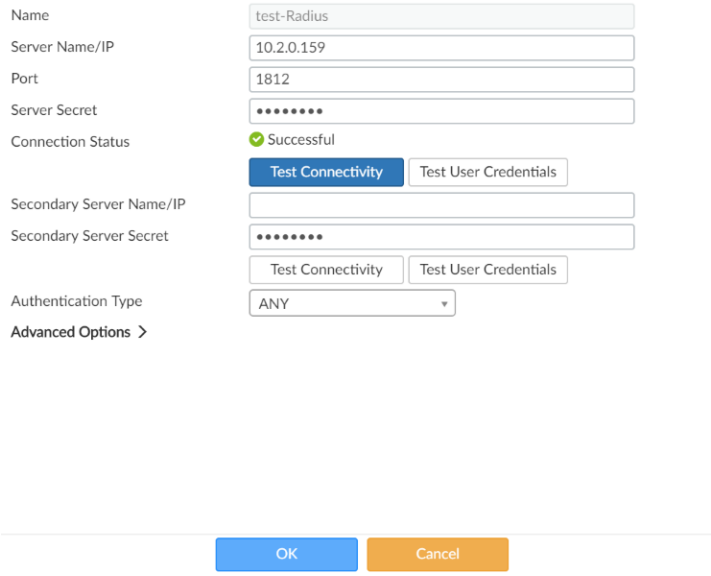
Remote Authentication Dial-in User (RADIUS) is a user authentication and network-usage accounting system. When users connect to a server they type a user name and password. This information is passed to a RADIUS server, which authenticates the user and authorizes access to the network.

You can create or edit RADIUS server entries in the server list to support authentication of administrators. When an administrator account's type is set to RADIUS, the FortiManager unit uses the RADIUS server to verify the administrator password at log on. The password is not stored on the FortiManager unit.

To use a RADIUS server to authenticate administrators, you must configure the server before configuring the administrator accounts that will use it.

To add a RADIUS server:

1. Go to *System Settings* > *Remote Authentication Server*.
2. Select *Create New* > *RADIUS Server* from the toolbar. The *New RADIUS Server* pane opens.



3. Configure the following settings, and then click *OK* to add the RADIUS server.

Name	Enter a name to identify the RADIUS server.
Server Name/IP	Enter the IP address or fully qualified domain name of the RADIUS server.
Port	Enter the port for RADIUS traffic. The default port is 1812. Some RADIUS servers use port 1645.
Server Secret	Enter the RADIUS server secret. Click the eye icon to Show or Hide the server secret.
Test Connectivity	Click *Test Connectivity* to test the connectivity with the RADIUS server. Shows success or failure.
Test User Credentials	Click *Test User Credentials* to test the user credentials. Shows success or failure.
Secondary Server Name/IP	Enter the IP address or fully qualified domain name of the secondary RADIUS server.
Secondary Server Secret	Enter the secondary RADIUS server secret.
Authentication Type	Select the authentication type the RADIUS server requires. If you select the default *ANY*, FortiManager tries all authentication types.

Advanced Options	
nas-ip	Specify the IP address for the Network Attached Storage (NAS).

TACACS+ servers

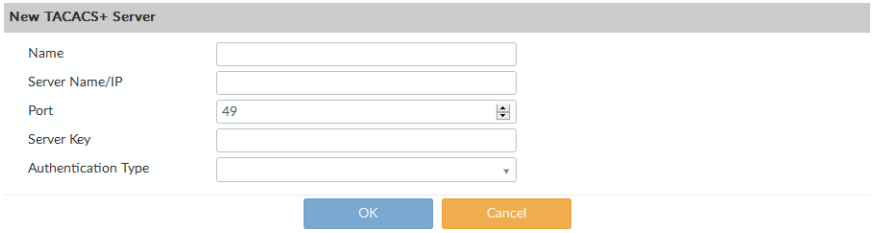
Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol that provides access control for routers, network access servers, and other network computing devices via one or more centralized servers. It allows a client to accept a user name and password and send a query to a TACACS authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies network access to the user. The default TCP port for a TACACS+ server is 49.

If you have configured TACACS+ support and an administrator is required to authenticate using a TACACS+ server, the FortiManager unit contacts the TACACS+ server for authentication. If the TACACS+ server can authenticate the administrator, they are successfully authenticated with the FortiManager unit. If the TACACS+ server cannot authenticate the administrator, the connection is refused by the FortiManager unit.

To use a TACACS+ server to authenticate administrators, you must configure the server before configuring the administrator accounts that will use it.

To add a TACACS+ server:

1. Go to *System Settings > Remote Authentication Server*.
2. Select *Create New > TACACS+ Server* from the toolbar. The *New TACACS+ Server* pane opens.



3. Configure the following settings, and then click *OK* to add the TACACS+ server.

Name	Enter a name to identify the TACACS+ server.
Server Name/IP	Enter the IP address or fully qualified domain name of the TACACS+ server.
Port	Enter the port for TACACS+ traffic. The default port is 49.
Server Key	Enter the key to access the TACACS+ server. The server key can be a maximum of 16 characters in length.
Authentication Type	Select the authentication type the TACACS+ server requires. If you select the default *ANY*, FortiManager tries all authentication types.

Remote authentication server groups

Remote authentication server groups can be used to extend wildcard administrator access. Normally, a wildcard administrator can only be created for a single server. If multiple servers of different types are grouped, a wildcard administrator can be applied to all of the servers in the group.

Multiple servers of the same type can be grouped to act as backups - if one server fails, the administrator can still be authenticated by another server in the group.

To use a server group to authenticate administrators, you must configure the group before configuring the administrator accounts that will use it.

Remote authentication server groups can only be managed using the CLI. For more information, see the *FortiManager CLI Reference*.

To create a new remote authentication server group:

1. Open the admin group command shell:
   ```
   config system admin group
   ```
2. Create a new group, or edit an already create group:
   ```
   edit <group name>
   ```
3. Add remote authentication servers to the group:
   ```
   set member <server name> <server name> ...
   ```
4. Apply your changes:
   ```
   end
   ```

To edit the servers in a group:

1. Enter the following CLI commands:
   ```
   config system admin group
      edit <group name>
            set member <server name> <server name> ...
      end
   ```
   Only the servers listed in the command will be in the group.

To remove all the servers from the group:

1. Enter the following CLI commands:
   ```
   config system admin group
      edit <group name>
         unset member
      end
   ```
   All of the servers in the group will be removed.

To delete a group:

1. Enter the following CLI commands:
   ```
   config system admin group
      delete <group name>
   end
   ```

SAML admin authentication

SAML can be enabled across devices, enabling smooth movement between devices for the administrator. FortiManager can play the role of the identity provider (IdP) or the service provider (SP) when an external identity provider is available.

Devices configured to the IdP can be accessed through the Quick Access menu which appears in the top-right corner of the main menu. The current device is indicated with an asterisk (currently only supported between FAZ/FMG).

Logging into an SP device will redirect you to the IdP login page. By default, it is a Fortinet login page. After successful authentication, you can access other SP devices from within the same browser without additional authentication.

When FortiManager is registered to FortiCloud, you can enable *Allow admins to login with FortiCloud*. This feature allows administrators to log in to FortiManager using their FortiCloud SSO account credentials. See FortiCloud SSO admin authentication on page 1049.



The admin user must be created on both the IdP and SP, otherwise you will see an error message stating that the admin doesn't exist.

Alternatively, you can configure the ADOM and profile names in the SP to match the IdP. When this is done, you can create one SAML SSO wildcard admin user on the SP to match all users on the IdP server.



When accessing FortiGate from the *Quick Access* menu, if FGT is set up to use the default login page with SSO options, you must select the *via Single Sign-On* button to be automatically authenticated.

To configure FortiManager as the identity provider:

1. Go to *System Settings > SAML SSO*.
2. Select *Identity Provider (IdP)*.
3. In the *IdP Certificate* dropdown, choose a certificate where IdP is used.
4. Select *Download* to get the IdP certificate, used later to configure SPs.
5. (Optional) A custom login page can be created by moving the *Login Page Template* toggle to the *On* position and selecting *Customize*.
6. In the *SP Settings* table, select *Create New* to add a service provider.
7. In the *Edit Service Provider* window, configure the following information:

Name	Enter a name for the service provider.
IdP Prefix	Copy the IdP prefix. This will be required when configuring your service providers.
SP Type	Select *Fortinet* as the *SP Type*. If the SP is not a Fortinet product, select *Custom* as the *SP Type* and copy the *SP Entity ID*, *SP ACS (Login) URL*, and *SP SLS (Logout) URL* from your SPs configuration page.

SP Address	Enter the IP address of the service provider.
SAML Attributes	SAML attributes can be added to a service provider to specify ADOM and/or profile names. FortiManager acting as IdP supports the following SAML attributes: • Type: *Username*, Attribute: *username* • Type: *Profile Name*, Attribute: *profilename* • Type: *ADOM*, Attribute: *adoms* • Type: *Group Match*, Attribute: *groupmatch*  **SAML SSO Wildcard users** As long as the SP has the same user profile, ADOM names, and user group as the IdP, you do not need to re-create each user from the IdP on the SP. Instead, you can create one SAML SSO wildcard admin user on the SP with the *Match all users on remote server* setting enabled to match all users on the IdP server. When logging in as an SSO user on the SP, the user is assigned the same profile and ADOMs as are configured on the IdP. See Creating administrators on page 979.  **Using the groupmatch attribute for SSO users** You can specify that an SSO user must match a specific user group on the IdP by configuring the `ext-auth-group-match` setting for the SSO user. See Creating administrators on page 979. When an SSO user has a group configured using the `ext-auth-group-match` setting, the login will be granted when the IdP user and SSO user have the same group value, and the group exists on the IdP. If the IdP user and SP SSO user have different group values, the login will fail.

8. Select *OK* to save changes to the service provider.
9. Click *Apply* to save the IdP configuration.

To configure FortiManager as a service provider:

1. Go to *System Settings* > *SAML SSO*.
2. Select *Service Provider (SP)*.
3. Enter the *Server Address* which is the browser accessible address for this device.
4. If applicable, select an *SP Certificate*.
5. For *Default Login Page*, select one of the following options:
   - *Normal*: User sees a normal login page with an SSO option.
   - *Single-Sign On*: Automatically redirects the user to the IdP's SSO login page.
6. Enable or disable *Auto Create Admin*.

- *Enable*: Automatically create SSO admins if they do not exist.
- *Disable*: SSO admins must be predefined.

7. Optionally, configure the signing options:
   - *Authentication Request Signed*: Enable this setting to require that all authentication requests sent by the FortiManager service provider are signed. A valid SP certificate is required to enable this option.
   - *Logout Request Signed*: FortiManager as SP will sign the SAML Request during logout. A valid SP certificate is required to enable this option.
   - *Require Assertions Signed from IdP*: Enable this setting to require that all assertions received from the IdP are signed.
   - *Require Logout Response Signed*: FortiManager as SP will require the SAML Response to be signed by IdP during logout.
8. Configure the IdP Settings:
   a. Select the IdP type as *Fortinet* or *Custom*.
   b. Enter the *IdP Address* and the *Prefix* that you obtained while configuring the IdP device.
   c. Select the IdP certificate. If this is a first-time set up, you can import the IdP certificate that you downloaded while configuring the IdP device.
9. Confirm that the information is correct and select *Apply*.
10. Repeat the steps for each FAZ/FMG that is to be set as a service provider.

Supported SAML attribute overrides

The following SAML attributes are accepted by FortiManager SAML service provider.

SAML Attribute	Description

username	The username of the local/SSO user. This attribute is mandatory.
	Example:
	`<Attribute Name="username">`
	`<AttributeValue>user1</AttributeValue>`
	`</Attribute>`

profilename	The *Profile* assigned to the user. If a matching profile exists on the FortiManager, it will be assigned to the user. This attribute is optional.
	Example:
	`<Attribute Name="profilename">`
	`<AttributeValue>SSOPROFILE</AttributeValue>`
	`</Attribute>`

adoms	The *ADOM(s)* to which the user will have access. Multiple ADOMs can be specified in the SAML assertion if supported by the IdP. This attribute is optional.
	Example:
	`<Attribute Name="adoms">`
	`<AttributeValue>ADOM1</AttributeValue>`
	`<AttributeValue>ADOM2</AttributeValue>`
	`</Attribute>`

SAML Attribute	Description

groupmatch	The remote user groups to which the user belongs. You can specify the remote user group for a user by configuring the `ext-auth-group-match` value under *Advanced Options* when creating or editing an SSO user or wildcard user. See Creating administrators on page 979.
	When the IdP user and matching SP SSO user have the same group specified, the user will be able to log in. If the values differ, login will fail.
	Example:
	`<Attribute Name="groupmatch">`
	`<AttributeValue>grp1</AttributeValue>`
	`</Attribute>`

You can use the following command in the CLI to verify the correct adoption of the SAML attributes by FortiManager.

```
diagnose system admin-session list
```

For example:

```
diagnose system admin-session list
*** entry 0 ***
   session_id: 57410 (seq: 0)
   username: user1
   admin template: SSO
   from: SSO(192.168.50.188) (type 7)
   profile: SSOPROFILE
   adom: adom1
   session length: 3 (seconds)
```

FortiCloud SSO admin authentication

When FortiManager is registered to FortiCloud, you can enable login to FortiManager using your FortiCloud SSO account.

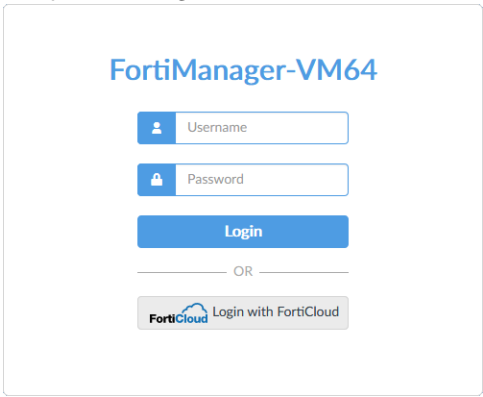
By default, only the FortiCloud account ID which the FortiManager is registered to can be used to log into FortiManager. Additional SSO users can be configured as IAM users in FortiCloud. See IAM user account login on page 1050.

To enable login with FortiCloud:

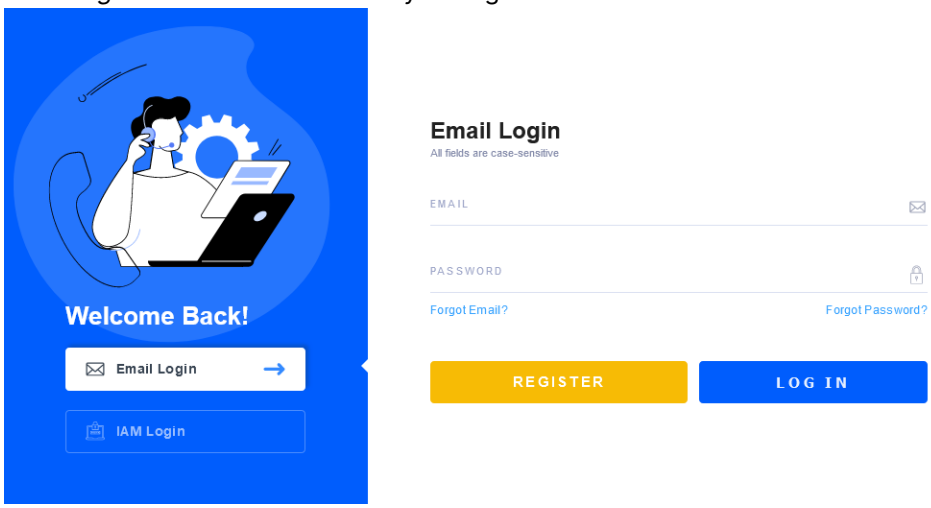
1. Before enabling this feature, FortiManager must be registered to FortiCloud, and a FortiCloud account must be configured.
   You can check your FortiCloud registration status in *Dashboard* in the *License Information* widget.
2. Go to *System Settings* > *SAML SSO*, and enable *Allow admins to login with FortiCloud*.



3. Sign out of FortiManager to return to the sign in screen.
An option to *Login with FortiCloud* is now visible on the FortiManager login page.



4. Click *Login with FortiCloud*. Enter your login credentials from FortiCloud and click *LOGIN*.



You are signed in with your FortiCloud user account.

IAM user account login

FortiCloud supports the creation of additional users called IAM users. Once created, you can use the IAM user account to sign in to FortiManager.

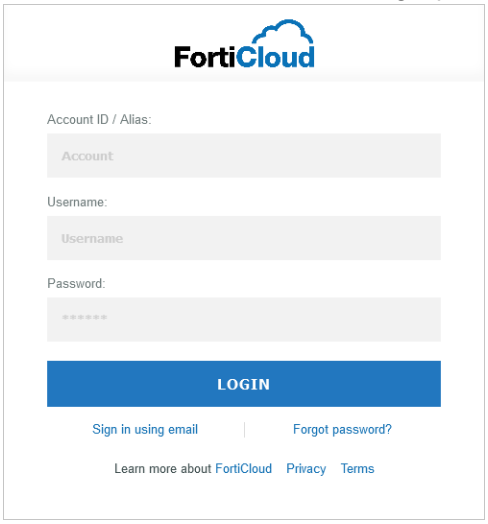
To sign in using a FortiCloud IAM user:

1. In FortiCloud, create one or more additional IAM user accounts. See Identity and Access Management (IAM).

The IAM users must have the following portal included in their *Permission Profile*:
- *FortiOS SSO*
  - *Access* = enabled
  - *Access Type* = *Admin*

2. In FortiManager, enable *Allow admins to login with FortiCloud* in *System Settings* > *SAML SSO*.

3. Sign out of FortiManager, return to the FortiManager sign on page, and click *Login with FortiCloud*.
4. At the bottom of the FortiCloud login portal, click *Sign in as IAM user*.



5. Enter your IAM user credentials.
   You are signed in using your FortiCloud IAM account.

Global administration settings

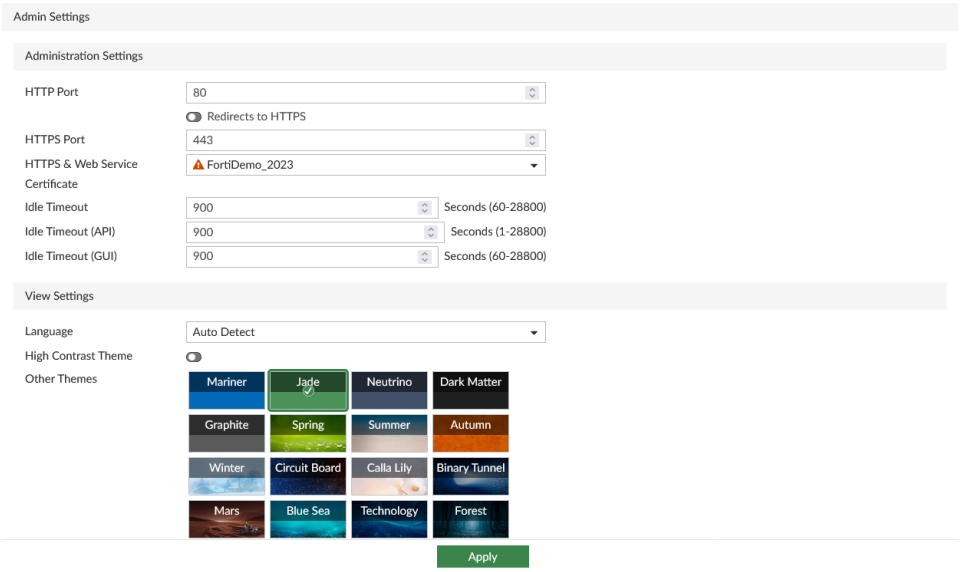
The administration settings page provides options for configuring global settings for administrator access to the FortiManager device. Settings include:

- Ports for HTTPS and HTTP administrative access
  To improve security, you can change the default port configurations for administrative connections to the FortiManager. When connecting to the FortiManager unit when the port has changed, the port must be included, such as `https://<ip_address>:<port>`. For example, if you are connecting to the FortiManager unit using port 8080, the URL would be `https://192.168.1.99:8080`. When you change to the default port number for HTTP or HTTPS, ensure that the port number is unique.
- Idle timeout settings
  By default, the GUI disconnects administrative sessions if no activity occurs for five minutes. This prevents someone from using the GUI if the management computer is left unattended.
- GUI language
  The language the GUI uses. For best results, you should select the language used by the management computer.
- GUI theme
  The default color theme of the GUI is *Jade*. You can choose another color or an image.
- Password policy
  Enforce password policies for administrators.
- Display options on GUI
  Display or hide advanced configuration options in the GUI. Only the *admin* administrator can configure these options.

Only super user administrators can access and configure the administration settings. The settings are global and apply to all administrators of the FortiManager unit.

To configure the administration settings:

1. Go to *System Settings* > *Settings*.



2. Configure the following settings as needed, then click *Apply* to save your changes to all administrator accounts:

Administration Settings	
HTTP Port	Enter the TCP port to be used for administrative HTTP access. Default: 80. Select *Redirect to HTTPS* to redirect HTTP traffic to HTTPS.
HTTPS Port	Enter the TCP port to be used for administrative HTTPS access. Default: 443.
HTTPS & Web Service Server Certificate	Select a certificate from the dropdown list.
Idle Timeout	Enter the number of seconds an administrative connection can be idle before the administrator must log in again, from 60 to 28800 (eight hours). See Idle timeout on page 1058 for more information.
Idle Timeout (API)	Enter the number of seconds an administrative connection to the API can be idle before the administrator must log in again, from 1 to 28800 (eight hours). Default: 900.
Idle Timeout (GUI)	Enter the number of seconds an administrative connection to the GUI can be idle before the administrator must log in again, from 60 to 28800 (eight hours). Default: 900.

Access Remote GUI via Port	Enter the port used to remotely connect to managed FortiGate devices. The default port used is 8082. See Remotely access a managed FortiGate on page 238.
View Settings	
Language	Select a language from the dropdown list. See GUI language on page 1058 for more information.
High Contrast Theme	Toggle *ON* to enable a high contrast dark theme in order to make the FortiManager GUI more accessible, and to aid people with visual disability in using the FortiManager GUI.
Other Themes	Select a theme for the GUI. The selected theme is not applied until you click *Apply*, allowing to you to sample different themes. Default: Jade.
Password Policy	Click to enable administrator password policies. See Password policy on page 1054 and Password lockout and retry attempts on page 1057 for more information.
Minimum Length	Select the minimum length for a password, from 8 to 32 characters. Default: 8.
Must Contain	Select the types of characters a password must contain.
Admin Password Expires after	Select the number of days a password is valid for, after which it must be changed.
Display Options on GUI	Click to expand the display options.
Show Script	Display the *Script* menu item. This menu is located on the *Device Manager* pane. This is an advanced FortiManager feature.
Show Add Multiple Button	Display the *Add Multiple Devices* option. This option is located on the *Device Manager* > *Devices & Groups* pane, under the *More* option in the toolbar. This is an advanced FortiManager feature.
Show Device List Import/Export	Select to display the *Import Device List* and *Export Device List* buttons. This option is located on the *Device Manager* > *Devices & Groups* pane, under the *More* option in the toolbar. This is an advanced FortiManager feature.
Fabric Authorization	Specifies the accessible management IP of FortiManager for FortiOS to retrieve and use for authorization of a Security Fabric connection to FortiManager. When you are using FortiOS to create a Security Fabric connection to FortiManager, a browser pop window is displayed and connects to FortiManager as part of the authorization process. FortiOS retrieves the information specified in FortiManager and provides it to the browser popup window to successfully connect to FortiManager. Without this information, the browser popup window cannot connect to FortiManager in certain topologies, such as when NAT is used.

		See also Security Fabric authorization information for FortiOS on page 1059.
	Authorization Address	Type the accessible management IP for FortiManager.
	Authorization Port	If a non-default port is used for the management port of FortiManager, specify the custom port.

Password policy

You can enable and configure password policy for the FortiManager.



When a password policy is enabled, only the current password is remembered for each user in password reuse history.

To configure the password policy:

1. Go to *System Settings* > *Settings*.
2. Click to enable *Password Policy*.
3. Configure the following settings, then click *Apply* to apply to password policy.

Minimum Length	Specify the minimum number of characters that a password must be, from 8 to 32. Default: 8.
Must Contain	Specify the types of characters a password must contain: uppercase and lowercase letters, numbers, and/or special characters.
Admin Password Expires after	Specify the number of days a password is valid for. When the time expires, an administrator will be prompted to enter a new password.

Enhanced administrator password security

The PBKDF2 hashing scheme with randomized salts is now used to store system administrator passwords on the FortiManager to enhance security. Previously the SHA256 hashing algorithm was used.

With this change, a new command is available to maintain FortiManager downgrade:

```
config system password-policy
    set login-lockout-upon-downgrade {enable | disable}
end
```

`set login-lockout-upon-downgrade {enable | disable}`	Enable/disable system administrator login lockout after downgrade to FortiManager firmware that does not support safer passwords (default = disable).

	When disabled, system administrator passwords with SHA256 hash are kept after successfully converting to PBKDF2 hash. SHA256 hashed passwords are used after downgrading to a firmware version that does not support PBKDF2 hashed passwords. When enabled, system administrator passwords that are converted to PBKDF2 hash will immediately remove the SHA256 hashed password. Upon downgrading the FortiManager firmware to a lower version, where safer passwords are unsupported, the administrators will be locked out.

When creating a new administrative user in FortiManager 7.4.7 / 7.6.3 or later, the PBKDF2 hashing scheme is used to store the password. When displayed in the CLI, the password is encoded with a prefix of PB2:

```
# config system admin user
(user)# edit admin2
new entry 'admin2' added
(admin2)# set profileid Super_User
Super user profile selected, adom-access will be set to all
(admin2)# set password 123456
(admin2)# show
config system admin user
    edit "admin2"
        set password ENC
PB2q4Knobgbqda31z0OHOvc19fq5QhvXCuLqXqyaMK3k2iN3zgvyaLAxLKAThYl8U+teWCAeW2rOMYodqCtQi9rOjQkSEdZ1hH
TBMiZAqirRVA=
        set old-password ENC SH2ak0hUxGlkppXtwCaAz0wKZrHiFKTdjOO7XDDSoTQibDNyqfkFYKLLocCHz0=
        set profileid "Super_User"
            config meta-data
                edit "Contact Email"
                next
                edit "Contact Phone"
                next
            end
    next
end
```

Upgrade

To view system administrator passwords before and after upgrade to FortiManager 7.4.7 / 7.6.3:

1. Before upgrade to FortiManager 7.4.7 / 7.6.3 or later, view the encoded password. The encoded password shows a SH2 prefix because it was hashed with the SHA256 algorithm:

```
(admin2)# show
config system admin user
    edit "admin2"
        set password ENC SH2ak0hUxGlkppXtwCaAz0wKZrHiFKTdjOO7XDDSoTQibDNyqfkFYKLLocCHz0=
        set profileid "Super_User"
            config meta-data
                edit "Contact Email"
                next
```

```
                edit "Contact Phone"
                next
            end
    next
end
```

2. Upgrade to FortiManager 7.4.7 / 7.6.3 or later. Each system administrator password hashed with SHA256 is stored on FortiManager until each system administrator successfully logs in to FortiManager.

   If a system administrator does not log in to FortiManager after upgrading to 7.4.7 / 7.6.3 or later, their password remains saved as the SHA256 hashed password.
3. Log in to FortiManager. The password is converted to a PBKDF2 hashed password.
4. View the encoded password. The encoded password shows a PB2 prefix because it was hashed with the PBKDF2 algorithm:

```
FMG-VM64-HV # show system admin user
config system admin user
    ...
    edit "admin2"
        set password ENC
PB2q4Knobgbqda31z0OHOvc19fq5QhvXCuLqXqyaMK3k2iN3zgvyaLAxLKAThYl8U+teWCAeW2rOMYodqCtQi9rOjQkSEd
Z1hHTBMiZAqirRVA=
        set old-password ENC SH2ak0hUxGlkppXtwCaAz0wKZrHiFKTdjOO7XDDSoTQibDNyqfkFYKLLocCHz0=
        set profileid "Super_User"
            set policy-package "all_policy_packages"
            set policy-block "all_policy_blocks"
            config meta-data
                edit "Contact Email"
                next
                edit "Contact Phone"
                next
            end
    next
end
```

Downgrade

To support downgrading to an older version that does not support the PBKDF2 hashed password, by default, the old SHA256 hashed password is still stored in the system after being converted to PBKDF2. This is controlled by the following setting that is disabled by default:

```
config system password-policy
    set login-lockout-upon-downgrade disable
end
```

The SHA256 hashed password will be removed from the system as soon as it is converted to a PBKDF2 hashed password upon a successful login.

During a downgrade operation, the system will display the following (see bold text below):

```
Downgrade FMG_VM64 image from v7.6.3-b3481-250409(Interim) to v7.4.6-b2588-241218(GA.M)

Configure may be lost in a downgrade.

Warning: downgrade image from maturity Interim to GA.M

Image is GA Certified

You are downgrading to a version that does not support safer passwords.
After downgrade, some administrative user no longer will be able to login with local
authentication.

This operation will replace the current firmware version and reboot the system!
Do you want to continue? (y/n)y
```

Administrators can choose to proceed or abort this downgrade.

Finally, if an administrator wants to restore the SHA256 hashed password for a downgrade, they can do the following:

1. Disable the login-lockout-upon-downgrade option.
2. Log out the current administrator.
3. For each system administrator, log in to the FortiManager to generate the SHA256 hashed password.



After administrator passwords are converted to PBKDF2 hashed passwords, loading the config file to an older version that does not support safer passwords will lock out the administrators.

Password lockout and retry attempts

By default, the number password retry attempts is set to three, allowing the administrator a maximum of three attempts at logging in to their account before they are locked out for a set amount of time (by default, 60 seconds).

The number of attempts and the default wait time before the administrator can try to enter a password again can be customized. Both settings can be configured using the CLI.

To configure the lockout duration:

1. Enter the following CLI commands:
```
config system global
   set admin-lockout-duration <seconds>
end
```

To configure the number of retry attempts:

1. Enter the following CLI commands:
```
config system global
   set admin-lockout-threshold <failed_attempts>
end
```

Example

To set the lockout threshold to one attempt and set a five minute duration before the administrator can try to log in again, enter the following CLI commands:

```
config system global
   set admin-lockout-duration 300
   set admin-lockout-threshold 1
end
```

GUI language

The GUI supports multiple languages, including:

- English
- Simplified Chinese
- Traditional Chinese
- Japanese
- Korean
- Spanish
- French

By default, the GUI language is set to *Auto Detect*, which automatically uses the language used by the management computer. If that language is not supported, the GUI defaults to English. For best results, you should select the language used by the operating system on the management computer.

For more information about language support, see the FortiManager Release Notes.

To change the GUI language:

1. Go to *System Settings* > *Settings*.
2. Under the *View Settings*, in the *Language* field, select a language, or *Auto Detect*, from the dropdown list.
3. Click *Apply* to apply the language change.

Idle timeout

To ensure security, the idle timeout period should be short. By default, administrative sessions are disconnected if no activity takes place for 900 seconds (15 minutes). This idle timeout is recommended to prevent anyone from using the GUI on a PC that was logged in to the GUI and then left unattended.

There are multiple idle timeout settings, which allows you to control idle timeout for API, GUI, and SSO sessions individually. The *Idle Timeout* setting controls all other idle timeout, including the idle timeout for SSH and console.

The idle timeout for SSO can only be set in the CLI using the following command:

```
config system admin setting
   set idle_timeout_sso <integer>
end
```

For more information, see the FortiManager CLI Reference in the Fortinet Document Library.

To change the idle timeout:

1. Go to *System Settings* > *Settings*.
2. In the *Idle Timeout* field, enter the idle timeout in seconds (60 - 28800, default = 900).
3. In the *Idle Timeout (API)* field, enter the idle timeout for API sessions in seconds (1 - 28800, default = 900).
4. In the *Idle Timeout (GUI)* field, enter the idle timeout in seconds (60 - 28800, default = 900).
5. Click *Apply*.
   If you need to set the idle timeout for SSO sessions, you must use the FortiManager CLI.

Security Fabric authorization information for FortiOS

When using FortiOS to create a Security Fabric connection to FortiManager, the process includes device authorization. The authorization process uses a browser popup window that requires communication to FortiManager. Depending on the topology, communication might fail, unless you specify the accessible management IP address and/or port of FortiManager that the browser popup window in FortiOS can use to connect with FortiManager.

FortiOS retrieves this information from FortiManager and makes it available to the browser popup window used for the authorization process.

To specify the authorization address and/or port:

1. In FortiManager, go to *System Settings* > *Settings*.
2. Under *Fabric Authorization*, set the following options:

Authorization Address	Type the GUI-accessible URL for FortiManager.
Authorization Port	If a non-default port is used, type the port number used for GUI access to FortiManager.

3. Click *Apply*.

Control administrative access with a local-in policy

Administrative access to FortiManager can be controlled by a IPv4/IPv6 local-in policy. This feature can only be configured using the FortiManager CLI.

For more information, see the FortiManager CLI Reference Guide on the Fortinet Docs Library.

To create an IPv4 local-in policy to control administrator access to FortiManager:

1. Access the FortiManager CLI.
2. Enter the following command to create the IPv4 local-in policy:
```
config system local-in-policy
   (local-in-policy)# edit <policy ID>
   new entry '<Policy ID>' added
```
3. Configure additional settings for the local-in policy using the `set` command.
   For example:
```
set
   action Action performed on traffic matching this policy.
   dport Destination port number (0 for all).
   dst Destination IP and mask.
   intf Incoming interface name.
   protocal Traffic protocal.
   src Source IP and mask.
```

To create an IPv6 local-in policy to control administrator access to FortiManager:

1. Access the FortiManager CLI.
2. Enter the following command to create the IPv6 local-in policy:
```
config system local-in-policy6
   (local-in-policy6)# edit <policy ID>
   new entry '<Policy ID>' added
```
3. Configure additional settings for the local-in policy using the `set` command.
   For example:
```
 set
   action Action performed on traffic matching this policy.
   dport Destination port number (0 for all).
   dst Destination IP and mask.
   intf Incoming interface name.
   protocal Traffic protocal.
   src Source IP and mask.
```

Multi-factor authentication

FortiManager supports the following two methods for two-factor authentication:

- FortiAuthenticator
- FortiToken Cloud

Multi-factor authentication with FortiAuthenticator

To configure multi-factor authentication for administrators with FortiAuthenticator you will need the following:

- FortiManager
- FortiAuthenticator

- FortiToken

Configuring FortiAuthenticator

On the FortiAuthenticator, you must create a local user and a RADIUS client.

Before proceeding, ensure you have configured your FortiAuthenticator, created a NAS entry for your FortiManager, and created or imported FortiTokens.

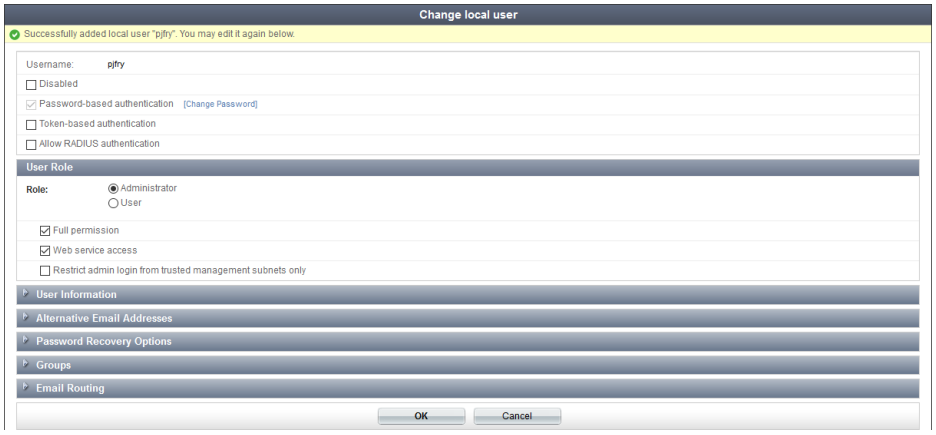
For more information, see the RADIUS Interoperability Guide and FortiAuthenticator Administration Guide in the Fortinet Document Library.

To create a local user:

1. Go to *Authentication > User Management > Local Users*.
2. Click *Create New* in the toolbar.
3. Configure the following settings:

Username	Enter a user name for the local user.
Password creation	Select Specify a password from the dropdown list.
Password	Enter a password. The password must be a minimum of 8 characters.
Password confirmation	Re-enter the password. The passwords must match.
Allow RADIUS authentication	Enable to allow RADIUS authentication.
Role	Select the role for the new user.
Enable account expiration	Optionally, select to enable account expiration. For more information see the *FortiAuthenticator Administration Guide*.

4. Click *OK* to continue to the *Change local user* page.



5. Configure the following settings, then click *OK*.

Disabled	Select to disable the local user.

Password-based authentication	Leave this option selected. Select *[Change Password]* to change the password for this local user.
Token-based authentication	Select to enable token-based authentication.
Deliver token code by	Select to deliver token by FortiToken, email, or SMS. Click *Test Token* to test the token.
Allow RADIUS authentication	Select to allow RADIUS authentication.
Enable account expiration	Optionally, select to enable account expiration. For more information see the *FortiAuthenticator Administration Guide*.
User Role	
Role	Select either *Administrator* or *User*.
Full Permission	Select to allow Full Permission, otherwise select the admin profiles to apply to the user. This option is only available when *Role* is *Administrator*.
Web service	Select to allow Web service, which allows the administrator to access the web service via a REST API or by using a client application. This option is only available when *Role* is *Administrator*.
Restrict admin login from trusted management subnets only	Select to restrict admin login from trusted management subnets only, then enter the trusted subnets in the table. This option is only available when *Role* is *Administrator*.
Allow LDAP Browsing	Select to allow LDAP browsing. This option is only available when *Role* is *User*.

Create a RADIUS client:

1. Go to *Authentication > RADIUS Service > Clients*.
2. Click *Create New* in the toolbar.
3. Configure the following settings, then click *OK*.

Name	Enter a name for the RADIUS client entry.
Client name/IP	Enter the IP address or Fully Qualified Domain Name (FQDN) of the FortiManager.
Secret	Enter the server secret. This value must match the FortiManager RADIUS server setting at *System Settings > Remote Authentication Server*.
First profile name	See the *FortiAuthenticator Administration Guide*.
Description	Enter an optional description for the RADIUS client entry.
Apply this profile based on RADIUS attributes	Select to apply the profile based on RADIUS attributes.
Authentication method	Select *Enforce two-factor authentication* from the list of options.

Username input format	Select specific user name input formats.
Realms	Configure realms.
Allow MAC-based authentication	Optional configuration.
Check machine authentication	Select to check machine based authentication and apply groups based on the success or failure of the authentication.
Enable captive portal	Enable various portals.
EAP types	Optional configuration.



For more information, see the *FortiAuthenticator Administration Guide*, available in the Fortinet Document Library.

Configuring FortiManager

On the FortiManager, you need to configure the RADIUS server and create an administrator that uses the RADIUS server for authentication.

To configure the RADIUS server:

1. Go to *System Settings* > *Remote Authentication Server*.
2. Click *Create New* > *RADIUS Server* in the toolbar.
3. Configure the following settings, then click *OK*.

Name	Enter a name to identify the FortiAuthenticator.
Server Name/IP	Enter the IP address or fully qualified domain name of your FortiAuthenticator.
Port	Enter the port for FortiAuthenticator traffic.
Server Secret	Enter the FortiAuthenticator secret.
Secondary Server Name/IP	Enter the IP address or fully qualified domain name of the secondary FortiAuthenticator, if applicable.
Secondary Server Secret	Enter the secondary FortiAuthenticator secret, if applicable.
Authentication Type	Select the authentication type the FortiAuthenticator requires. If you select the default *ANY*, FortiManager tries all authentication types. **Note**: RADIUS server authentication for local administrator users stored in FortiAuthenticator requires the *PAP* authentication type.

To create the administrator:

1. Go to *System Settings* > *Administrators*.
2. Click *Create New* from the toolbar.

3. Configure the settings, selecting the previously added RADIUS server from the *RADIUS Server* dropdown list. See Creating administrators on page 979.
4. Click *OK* to save the settings.

To test the configuration:

1. Attempt to log in to the FortiManager GUI with your new credentials.
2. Enter your user name and password and click *Login*.
3. Enter your FortiToken pin code and click *Submit* to log in to the FortiManager.

Multi-factor authentication with FortiToken Cloud

FortiManager supports MFA with FortiToken Cloud.

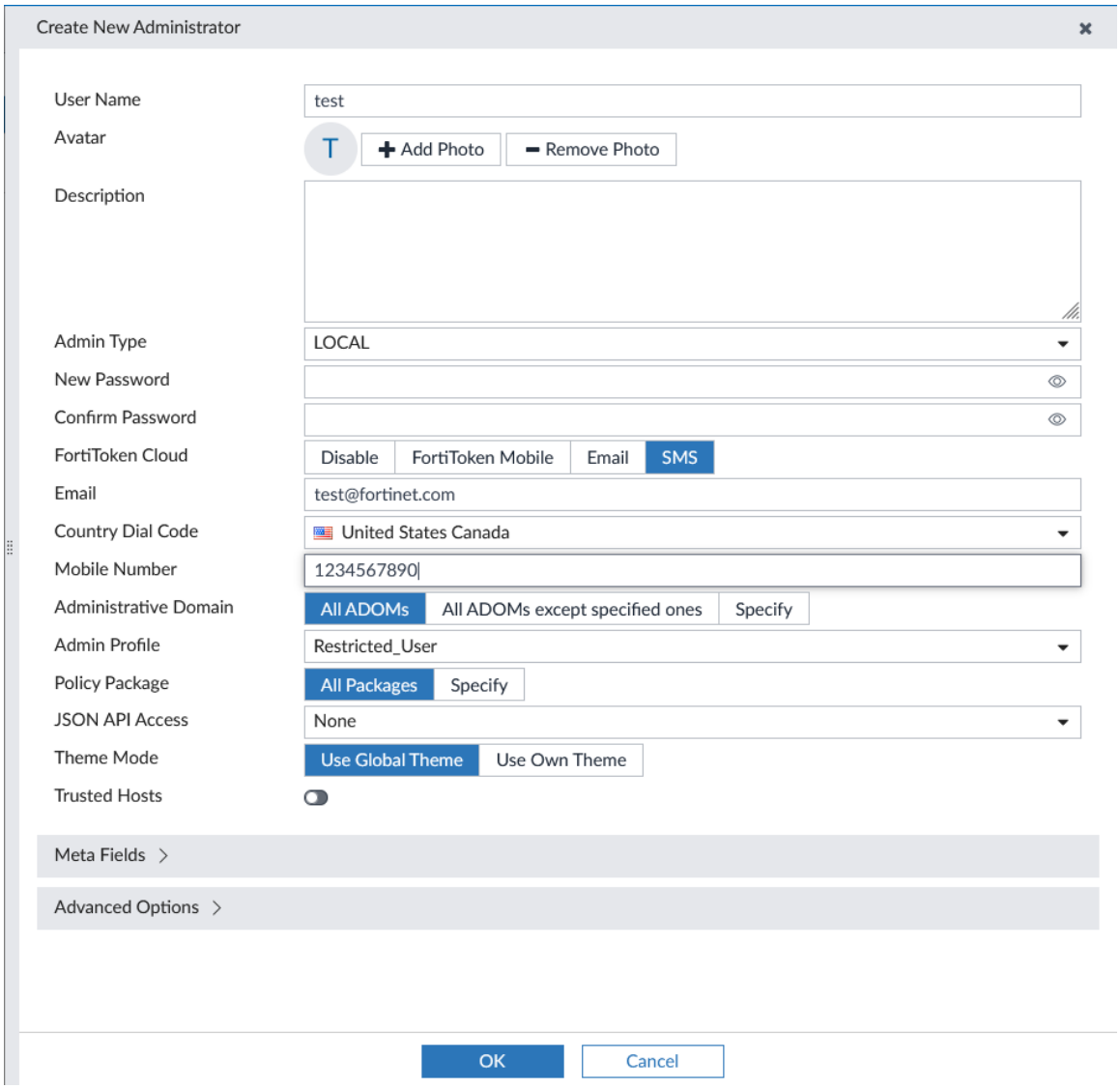
To use MFA with FortiToken Cloud, you must have an active FortiToken Cloud license registered on the same FortiCloud account as FortiManager. For more information about how to register your FortiToken license on FortiCloud, see How to register your FTC license and the FortiCloud Asset Management guide.

For information about licenses for FortiToken Cloud, see How to Add Licenses to FortiToken Cloud.

To configure an administrator to use MFA with FortiToken Cloud:

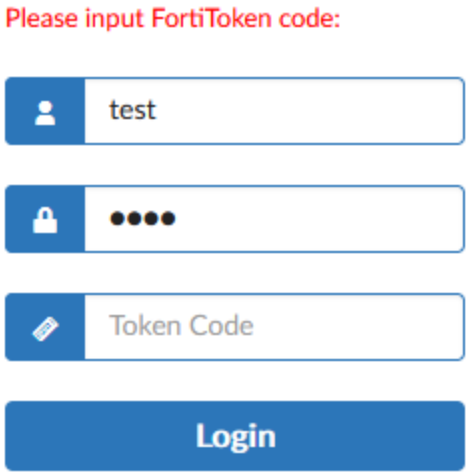
1. Register FortiToken Cloud and FortiManager to the same FortiCloud account.
2. In FortiManager, go to *System Settings > Admin > Administrators* and click *Create New* or edit an existing administrator.
3. In the *FortiToken Cloud* field, select the token delivery method from the following options:

FortiToken Mobile	Use the FortiToken Mobile app to get tokens. The following information must be provided: • **Email**: Provide the administrator's email address. The administrator is sent an email to the specified address with a link to activate their token in the FortiToken Mobile app on their mobile device. After FortiToken Mobile app is activated, they will receive their token codes through the app.
Email	Receive the token by email. The following information must be provided: • **Email**: Provide the administrator's email address. Token codes will be sent to the specified email address.
SMS	Receive the token by SMS message. The following information must be provided: • **Email**: Provide the administrator's email address. • **Country Dial Code**: Select a country code for the mobile number. • **Mobile Number**: Enter a valid mobile phone number for receiving SMS messages.



4. Edit other fields as needed and click *OK* to save the administrator configuration.

   When the FortiToken Cloud is registered to the same FortiCloud account as FortiManager and the license permits adding a new user, the administrator is automatically synchronized to FortiToken Cloud with the specified *FortiToken Cloud* MFA method. Otherwise, an error message is displayed.
   You can view the user in *FortiToken Cloud under User Management > Users*. For more information, see the FortiToken Cloud Administration Guide.
5. When the administrator logs in, they are prompted to enter the token code from their email, SMS, or FortiToken Mobile app.


Please input FortiToken code:
test
Token Code
Login

High Availability

FortiManager high availability (HA) provides a solution for a key requirement of critical enterprise management and networking components: enhanced reliability. Understanding what's required for FortiManager reliability begins with understanding what normal FortiManager operations are and how to make sure normal operations continue if a FortiManager unit fails.

Most of the FortiManager operations involve storing FortiManager and FortiGate configuration and related information in the FortiManager database on the FortiManager unit hard disk. A key way to enhance reliability of FortiManager is to protect the data in the FortiManager database from being lost if the FortiManager unit fails. This can be achieved by dynamically backing up FortiManager database changes to one or more backup FortiManager units. Then, if the operating FortiManager unit fails, a backup FortiManager unit can take the place of the failed unit.

FortiAnalyzer Features must be disabled on FortiManager before you can form a FortiManager HA cluster. A FortiManager HA cluster can have a maximum of five units: one primary unit with up to four backup or secondary units. All units in the cluster must be of the same FortiManager series. All units are visible on the network.

The primary unit and the secondary units can be in the same location or different locations. FortiManager HA supports geographic redundancy so the primary unit and secondary units can be in different locations attached to different networks as long as communication is possible between them (for example, on the Internet, on a WAN, or in a private network).

Administrators connect to the primary unit GUI or CLI to perform FortiManager operations. Managed devices connect with the primary unit for normal management operations (configuration push, auto-update, firmware upgrade, and so on). If FortiManager is used to distribute FortiGuard updates to managed devices, managed devices can connect to the primary FortiManager unit or one of the secondary units.

FortiManager supports manual and automatic (VRRP) failover settings. Automatic failover can be enabled by selecting the VRRP failover mode during HA configuration. See Configuring HA options on page 1070.

When using manual failover settings, you must manually configure one of the secondary units to become the primary unit when the primary unit fails. The new primary unit will keep its IP address. FortiManager's IP address registered on FortiGate will be automatically changed when the new primary unit is selected.



You don't need to reboot the FortiManager device when it is promoted from a backup to the primary unit.



FortiManager HA can be formed between all types of FortiManager-VM platforms. For example, you can deploy the Primary device using KVM and the secondary using VMware ESXi. The steps to configure HA are unchanged.

FortiManager HA clusters can also be formed using devices on different license types (e.g. Subscription and Perpetual VM licenses).



When devices with different licenses are used to create an HA cluster, the license that allows for the smallest number of managed devices is used.

Synchronizing the FortiManager configuration and HA heartbeat

All changes to the FortiManager database are saved on the primary unit, and then these changes are synchronized to the backup units. The FortiManager configuration of the primary unit is also synchronized to the backup units, except for the following settings:

- Hostname
- System time and NTP server
- Network
- Web proxy settings
- HA
- Local certificates
- SNMP
- Mail server
- Syslog server
- LDAP servers and LDAP admin users
- FortiCloud account associated with the FortiManager
- FortiGuard database downloaded by FortiManager
- FortiGuard settings (FortiManager CM database also known as CMDB)

Aside from these settings, the backup units always match the primary unit. So if the primary unit fails, a backup unit can be configured to take the place of the primary unit and continue functioning as a standalone FortiManager unit.

While the FortiManager cluster is operating, all backup units in the cluster exchange HA heartbeat packets with the primary unit so the primary unit can verify the status of the backup units and the backup units can verify the status of the primary unit. The HA heartbeat packets use TCP port 5199. HA heartbeat monitoring, as well as FortiManager database and configuration synchronization takes place using the connections between the FortiManager units in the cluster. As part of configuring the primary unit you add peer IPs and peer serial numbers of each of the backup FortiManager units in the cluster. You also add the peer IP of the primary unit and the primary unit serial number to each of the backup units.



Depending on the peer IPs that you use, you can isolate HA traffic to specific FortiManager interfaces and connect those interfaces together so they function as synchronization interfaces between the FortiManager units in the cluster. Communication between the units in the cluster must be maintained for the HA cluster to operate.

The interfaces used for HA heartbeat and synchronization communication can be connected to your network. However, if possible you should isolate HA heartbeat and synchronization packets from your network to save bandwidth.

If the primary or a backup unit fails

Manual failover

If the primary unit fails, the backup units stop receiving HA heartbeat packets from the primary unit. If one of the backup units fails, the primary unit stops receiving HA heartbeat packets from the backup unit. In either case, the cluster is considered down until it is reconfigured.

When the cluster goes down, the cluster units still operating send SNMP traps and write log messages to alert the system administrator that a failure has occurred. You can also see the failure on the *HA Status* page.

Reconfigure the cluster by removing the failed unit from the cluster configuration. If the primary unit has failed, this means configuring one of the backup units to be the primary unit and adding peer IPs for all of the remaining backup units to the new primary unit configuration.

If a backup unit has failed, reconfigure the cluster by removing the peer IP of the failed backup unit from the primary unit configuration.

Once the cluster is reconfigured, it will continue to operate as before but with fewer cluster units. If the failed unit is restored you can reconfigure the cluster again to add the failed unit back into the cluster. In the same way you can add a new unit to the cluster by changing the cluster configuration to add it.

Automatic (VRRP) failover

When the monitored interface for the primary FortiManager is down, HA automatic failover will occur, and the secondary FortiManager will automatically become the new primary. The *Priority* setting determines which device will be primary and secondary in an HA configuration. See Configuring HA options on page 1070.

FortiManager HA cluster startup steps

FortiManager units configured for HA start up begin sending HA heartbeat packets to their configured peer IP addresses and also begin listening for HA heartbeat packets from their configured peer IP addresses.

When the FortiManager units receive HA heartbeat packets with a matching HA cluster ID and password from a peer IP address, the FortiManager unit assumes the peer is functioning.

When the primary unit is receiving HA heartbeat packets from all of the configured peers or backup units, the primary unit sets the cluster status to up. Once the cluster is up the primary unit then synchronizes its configuration to the backup unit. This synchronization process can take a few minutes depending on the size of the FortiManager database. During this time database and configuration changes made to the primary unit are not synchronized to the backup units. Once synchronization is complete, if changes were made during synchronization, they are re-synchronized to the backup units.

Most of the primary unit configuration, as well as the entire FortiManager database, are synchronized to the backup unit. For settings that are not synchronized, you must configure the settings on each cluster unit. For a list of settings not synchronized, see Synchronizing the FortiManager configuration and HA heartbeat on page 1068.

Once the synchronization is complete, the FortiManager HA cluster begins normal operation.

Configuring HA options

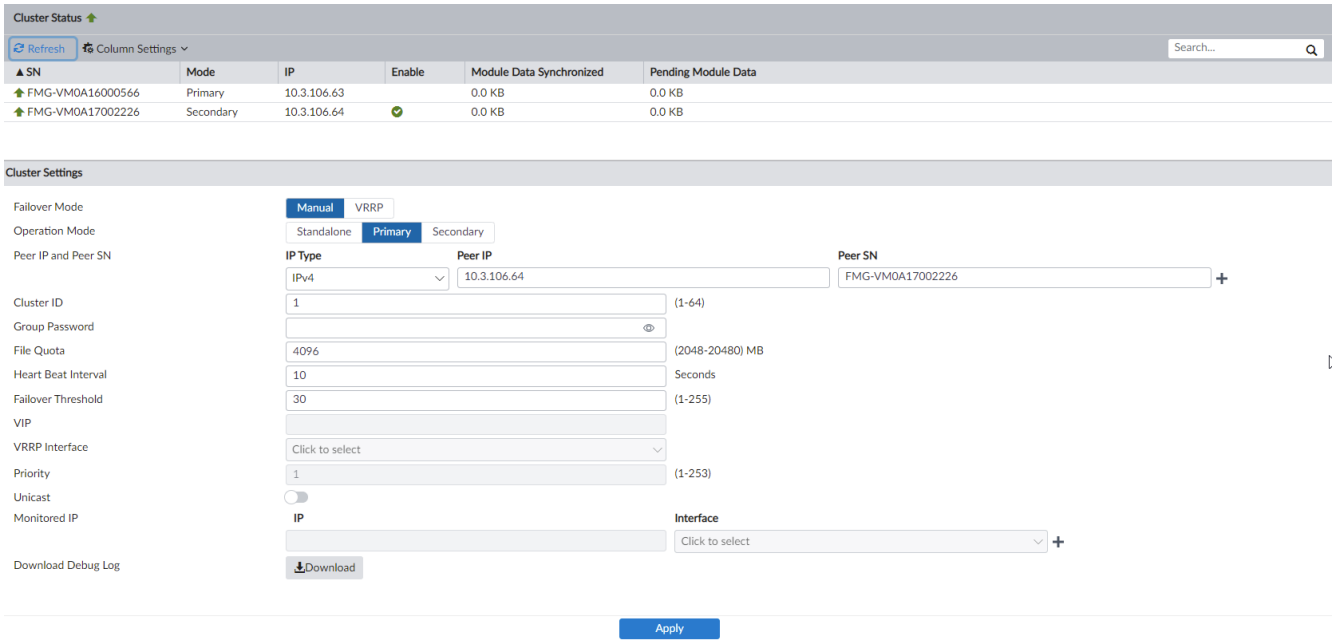
To configure HA options go to *System Settings* > *HA*. Use the *Cluster Settings* pane to configure FortiManager units to create an HA cluster or change cluster configuration.

To configure a cluster, set the *Operation Mode* of the primary unit to *Primary* and the modes of the backup units to *Secondary*. Then add the IP addresses and serial numbers of each backup unit to primary unit peer list. The IP address and serial number of the primary unit must be added to each backup unit's HA configuration. The primary unit and all backup units must have the same *Cluster ID* and *Group Password*.

You can connect to the primary unit GUI to work with FortiManager. Using configuration synchronization, you can configure and work with the cluster in the same way as you work with a standalone FortiManager unit.

If the FortiManager HA is behind a NAT device while using *Manual Failover Mode*, you must configure the FortiManager management address for the Primary and Secondary device. By configuring the management address setting, FortiManager knows the public IP for Primary and Secondary devices, and can configure it on FortiGate. See Configuring the management address on page 131.

This is not required when using *VRRP Failover Mode*.



Configure the following settings:

Cluster Status	Monitor FortiManager HA status. See Monitoring HA status on page 1087.
SN	The serial number of the device.
Mode	The high availability mode, either *Primary* or *Secondary*.
IP	The IP address of the device.

	Enable	Shows if the peer is currently enabled.
	Module Data Synchronized	Module data synchronized in bytes.
	Pending Module Data	Pending module data in bytes.
Cluster Settings		
	Failover Mode	Select *Manual* to configure manual failover. When the primary unit fails, you must manually configure one of the secondary units to become the primary unit. The new primary unit will keep its IP address. FortiManager's IP address registered on FortiGate will be automatically changed when the new primary unit is selected. Select *VRRP* to configure automatic failover. When the monitored interface for the primary FortiManager is unreachable or down, HA automatic failover will occur, and the secondary FortiManager will automatically become the primary.
	Operation Mode	Select *Primary* to configure the FortiManager unit to be the primary unit in a cluster. Select *Secondary* to configure the FortiManager unit to be a backup unit in a cluster. Select *Standalone* to stop operating in HA mode.
	Peer IP	Select the peer IP version from the dropdown list, either *IPv4* or *IPv6*. Then, type the IP address of another FortiManager unit in the cluster. For the primary unit you can add up to four Peer IP addresses for up to four backup units. For a backup unit you can only add the IP address of the primary unit. Type the IP address of another FortiManager unit in the cluster. For the primary unit you can add up to four Peer IP addresses for up to four backup units. For a backup unit you can only add the IP address of the primary unit.
	Peer SN	Type the serial number of the FortiManager unit corresponding to the entered IP address.
	Cluster ID	A number between 1 and 64 that identifies the HA cluster. All members of the HA cluster must have the same cluster ID. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different cluster ID. The FortiManager GUI browser window title changes to include the cluster ID when FortiManager unit is operating in HA mode.
	Group Password	A password for the HA cluster. All members of the HA cluster must have the same password. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different password. The maximum password length is 19 characters.
	File Quota	Enter the file quota, from 2048 to 20480 MB (default: 4096 MB). You cannot configure the file quota for backup units.

Heart Beat Interval	The time the primary unit waits between sending heartbeat packets, in seconds. The heartbeat interval is also the amount of time that backup units waits before expecting to receive a heartbeat packet from the primary unit. The default heartbeat interval is 5 seconds. The heartbeat interval range is 1 to 255 seconds. You cannot configure the heartbeat interval on the backup units.
Failover Threshold	The number of heartbeat intervals that one of the cluster units waits to receive HA heartbeat packets from other cluster units before assuming that the other cluster units have failed. The default failover threshold is 3. The failover threshold range is 1 to 255. You cannot configure the failover threshold of the backup units. In most cases you do not have to change the heartbeat interval or failover threshold. The default settings mean that if the a unit fails, the failure is detected after 3 x 5 or 15 seconds; resulting in a failure detection time of 15 seconds. If the failure detection time is too short, the HA cluster may detect a failure when none has occurred. For example, if the primary unit is very busy it may not respond to HA heartbeat packets in time. In this situation, the backup unit may assume the primary unit has failed when the primary unit is actually just busy. Increase the failure detection time to prevent the backup unit from detecting a failure when none has occurred. If the failure detection time is too long, administrators will be delayed in learning that the cluster has failed. In most cases, a relatively long failure detection time will not have a major effect on operations. But if the failure detection time is too long for your network conditions, then you can reduce the heartbeat interval or failover threshold.
VIP	Enter the VIP of the FortiManager-HA. This setting can only be configured when the *Failover Mode* is *VRRP*.
VRRP Interface	Select the VRRP interface. This setting can only be configured when the *Failover Mode* is *VRRP*.
Priority	Set the priority for this device between 1 (lowest) and 253 (highest). The device with a higher priority will operate as the primary unit when possible. This setting can only be configured when the *Failover Mode* is *VRRP*.
Unicast	Optionally, toggle this setting *ON* to use Unicast for the VRRP message. This setting can only be configured when the *Failover Mode* is *VRRP*.
Monitored IP	Configure the monitored IP and interface. You can add additional monitored IPs by clicking the add icon. This setting can only be configured when the *Failover Mode* is *VRRP*.
Download Debug Log	Select to download the HA debug log file to the management computer.

General FortiManager HA configuration steps

1. Configure the FortiManager units for HA operation:
   - Configure the primary unit.
   - Configure the backup units.
2. Change the network configuration so the remote backup unit and the primary unit can communicate with each other.
3. Connect the units to their networks.
4. Add basic configuration settings to the cluster:
   - Add a password for the admin administrative account.
   - Change the IP address and netmask of the port1 interface.
   - Add a default route.

Configuring HA using manual failover mode

Use the following procedures to configure the FortiManager units for HA operation from the FortiManager unit GUI. It assumes you are starting with three FortiManager units with factory default configurations. The primary unit and the first backup unit are connected to the same network. The second backup unit is connected to a remote network and communicates with the primary unit over the Internet. Sample configuration settings are also shown.

To configure the primary unit for HA operation:

1. Connect to the primary unit GUI.
2. Go to *System Settings* > *HA*.
3. Configure HA settings.
   Example HA primary configuration:

Failover Mode	Manual
Operation Mode	Primary
Peer IP	172.20.120.23
Peer SN	<serial_number>
Peer IP	192.268.34.23
Peer SN	<serial_number>
Cluster ID	15
Group Password	password
File Quota	4096
Heartbeat Interval	5 (Keep the default setting.)
Failover Threshold	3 (Keep the default setting.)

4. Click *Apply*.

To configure the backup unit on the same network for HA operation:

1. Connect to the backup unit GUI.
2. Go to *System Settings > HA*.
3. Configure HA settings.
   Example local backup configuration:

Failover Mode	Manual
Operation Mode	Secondary
Priority	5 (Keep the default setting.)
Peer IP	172.20.120.45
Peer SN	<serial_number>
Cluster ID	15
Group Password	password
File Quota	4096
Heartbeat Interval	5 (Keep the default setting.)
Failover Threshold	3 (Keep the default setting.)

4. Click *Apply*.

To configure a remote backup unit for HA operation:

1. Connect to the backup unit GUI.
2. Go to *System Settings > HA*.
3. Configure HA settings.
   Example remote backup configuration:

Failover Mode	Manual
Operation Mode	Secondary
Priority	5 (Keep the default setting.)
Peer IP	192.168.20.23
Peer SN	<serial_number>
Cluster ID	15
Group Password	password
File Quota	4096
Heartbeat Interval	5 (Keep the default setting.)
Failover Threshold	3 (Keep the default setting.)

4. Click *Apply*.

To change the network configuration so that the remote backup unit and the primary unit can communicate with each other:

Configure the appropriate firewalls or routers to allow HA heartbeat and synchronization traffic to pass between the primary unit and the remote backup unit using the peer IPs added to the primary unit and remote backup unit configurations.

HA traffic uses TCP port 5199.

To connect the cluster to the networks:

1. Connect the cluster units.
   No special network configuration is required for the cluster.
2. Power on the cluster units.
   The units start and use HA heartbeat packets to find each other, establish the cluster, and synchronize their configurations.

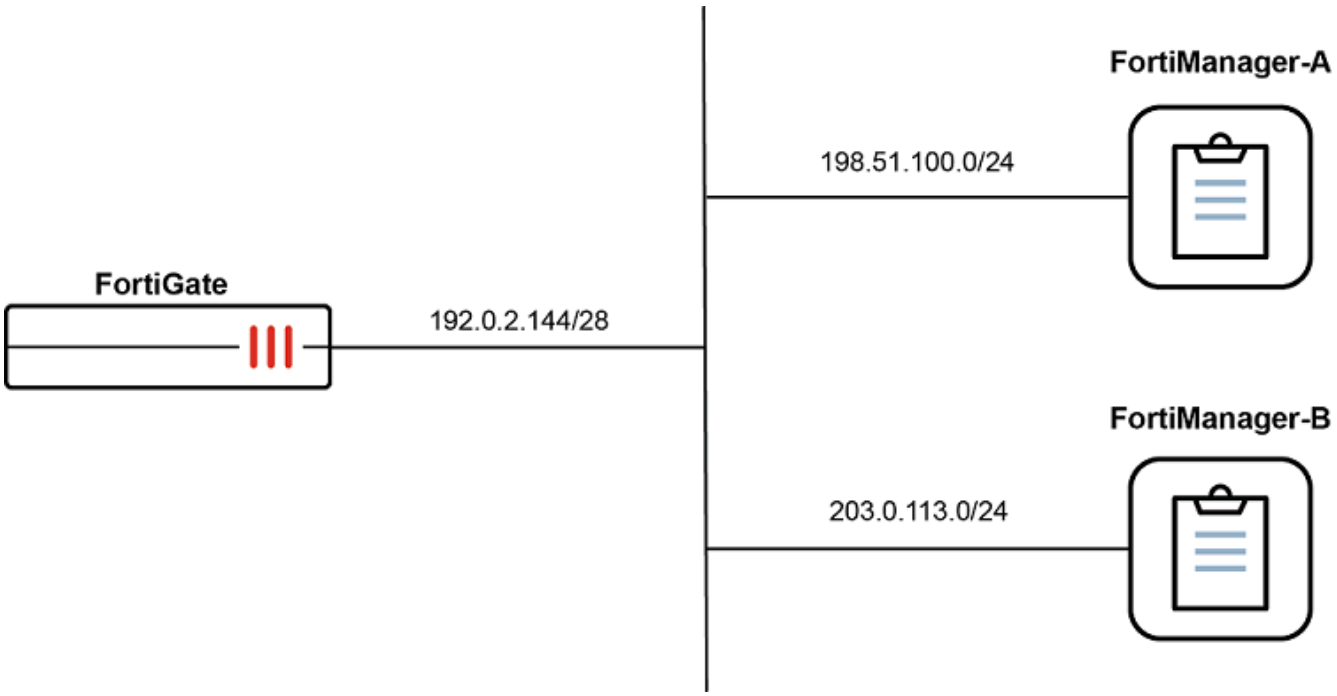
To add basic configuration settings to the cluster:

Configure the cluster to connect to your network as required.

Configuring geo-redundant HA with VRRP failover

In the following scenario, HA with VRRP failover is configured for two FortiManager devices in different geographic areas for geo-redundancy using Layer 3.

In this example, FortiManager-A is on the `198.51.100.0/24` subnet and FortiManager-B is on the `203.0.113.0/24` subnet.



This topic includes the following sections:

- Configure geo-redundant FortiManager HA with VRRP failover on page 1076
- Verifying the HA status on page 1077
- Additional FortiManager configuration on page 1077
- Adding a managed FortiGate to the FortiManager cluster on page 1078
- Testing VRRP failover on page 1078

Configure geo-redundant FortiManager HA with VRRP failover

To configure geo-redundant HA with VRRP failover:

1. Configure the HA settings on FortiManager-A.
   a. On FortiManager-A, go to *System Settings* > *HA*.
   b. Configure the *Cluster Settings* as follows, and click *Apply*.

Failover Mode	*VRRP*
Peer IP and Peer SN	Choose the following: • **IP Type**: `IPv4` • **Peer IP**: Enter the IP address of FortiManager-B (example, `203.0.113.1`) • **Peer SN**: Enter the serial number of the peer device.
VIP	Enter the VIP address for the cluster (example, `192.0.2.1`). This is a dummy IP and will not be used for deployment or management. The VIP IP **MUST** be identical in all peers.
VRRP Interface	Choose the VRRP interface (example, `port1`).
Priority	`200`
Unicast	On. In Geo-HA it is mandatory to use Unicast as peers will not be in the same Layer2.

2. Configure the HA settings on FortiManager-B.
   a. On FortiManager-B device, go to *System Settings* > *HA*.
   b. Configure the *Cluster Settings* as follows, and click *Apply*.

Failover Mode	*VRRP*
Peer IP and Peer SN	Choose the following: • **IP Type**: `IPv4` • **Peer IP**: Enter the IP address of FortiManager-A (example, `198.51.100.1`). • **Peer SN**: Enter the serial number of the peer device.
VIP	Enter the VIP address for the cluster (example, `192.0.2.1`).

	This is a dummy IP and will not be used for deployment or management. The VIP IP **MUST** be identical in all peers.
VRRP Interface	Choose the VRRP interface (example, `port1`).
Priority	`100`
Unicast	On. In Geo-HA it is mandatory to use Unicast as peers will not be in the same Layer2.

Verifying the HA status

To verify the HA status:

1. Access both FortiManager-A and FortiManager-B.
2. Using the GUI, you can view the *HA Status* on the top-right corner of each FortiManager and from *System Settings* > *HA*.
3. Using the CLI, you can run the following commands to get additional information about the HA status:

Command	Description
`get system ha-status`	Print the HA status.
`diagnose ha stats`	Diagnose the HA status.
`diagnose sniffer packet <interface> "vrrp"`	Perform a packet sniffer on the port used by the VRRP protocol using "vrrp" as a filter. This command can be used to verify that the advertisements are sent using the preferred method when *Unicast* mode is disabled/enabled.

Additional FortiManager configuration

In this scenario, FortiManager is using 2 IP addresses (`198.51.100.1` and `203.0.113.1`) to manage FortiGates. It is a best practice to define all FortiManager IPs that will be used to manage FortiGates so that it is reflected in the FortiGate `config system central-management` settings if FortiGate is added from FortiManager.

Defining FortiManager IPs:

- Using the FortiManager CLI, you can run the following configuration:

```
config system admin setting
   set mgmt-fqdn <FQDN_1 | IP_1> <FQDN_2 | IP_2> ... <FQDN_N | IP_N>
end
```



You can add up to a total of 10 IP addresses or FQDNs to the `mgmt-fqdn` attribute.

- For example, in this scenario it will be as follows:
```
config system admin setting
   set mgmt-fqdn 198.51.100.1 203.0.113.1
end
```

Adding a managed FortiGate to the FortiManager cluster

To onboard using the FortiManager Device Manager:

1. On FortiManager-A, go to *Device Manager* > *Device & Groups* > *Managed FortiGate*.
2. Click *Add Device* > *Discover Device*.
3. Enable Use Legacy Device Login and enter the device IP Address, User Name, and Password.
4. Click *Next*, *Next*, and *Import Later*.
5. Run the `show system central-management` command in the FortiGate CLI to check the management IP addresses:
```
show system central-management
   config system central-management
      set type fortimanager
      set fmg "198.51.100.1" "203.0.113.1"
end
```
The IP addresses shown should reflect the IP addresses and FQDNs configured in FortiManager under `config system admin setting` as explained in the previous section.

To onboard using the Central Management connector on FortiGate:

1. On FortiGate, go to *Security Fabric* > *Fabric Connectors* > *Central Management*.
2. Under *IP/Domain*, click the *+* button to add more IP addresses.
3. Enter all of the FortiManager IP addresses and click *OK*.
For example, in this scenario the IPs are `198.51.100.1` and `203.0.113.1`.
4. You can authorize the device using the dialog from the FortiGate or from the Device Manager on the Primary FortiManager.
5. Run `show system central-management` in the FortiGate CLI to check the management IP addresses. For example:
```
show system central-management
   config system central-management
      set type fortimanager
      set fmg "198.51.100.1" "203.0.113.1"
end
```
The IP addresses displayed should match those configured in step 2.

Testing VRRP failover

To test the failover configuration:

1. On the FortiGate, run the following command in the CLI:
```
get system central-management
```
In the serial-number field, the serial numbers for both FortiManager-A and FortiManager-B are listed. FortiManager-A is listed first because it is currently acting as the Primary device.

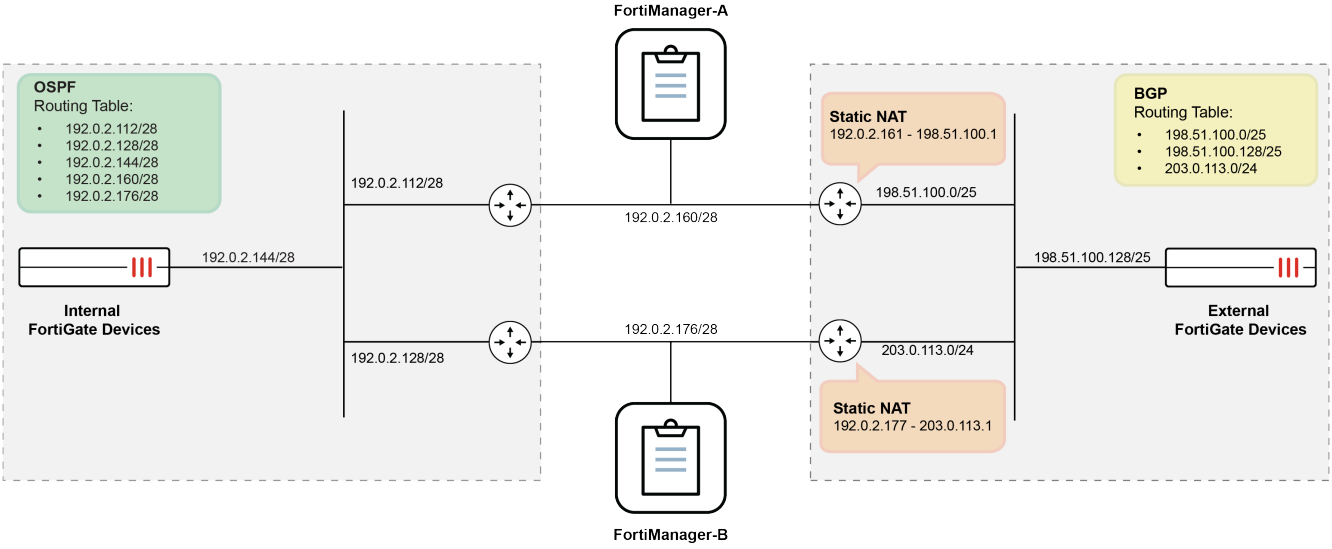
2. In the CLI for FortiManager-A, run `diagnose ha force-vrrp-election` which will trigger failover to the FortiManager with the next highest priority.
3. Refresh the page and you will notice that the HA status of FortiManager-A becomes Secondary.
4. Go to FortiManager-B, and confirm that the HA status has changed to Primary.
5. Enter the following command in the CLI to confirm the status of FortiManager-A. FortiManager-A continues to act as the Secondary device until the next VRRP election occurs.
   ```
   diagnose ha stats
   ```
6. On the FortiGate, run the following command in the CLI.
   ```
   get system central-management
   ```
   In the serial-number field, the serial numbers for both FortiManager-A and FortiManager-B are listed. FortiManager-B will be listed first because it is now acting as the Primary device.

Configuring geo-redundant HA with VRRP failover with NAT

In the following scenario, HA with VRRP failover is configured for two FortiManager devices in different geographic areas for geo-redundancy using Layer 3.

In this example, FortiManager-A is on the `192.0.2.160/28` subnet and FortiManager-B is on the `192.0.2.176/28` subnet. FortiManager-A has a static NAT to public IP `198.51.100.1`, and FortiManager-B has static NAT to public IP `203.0.113.1`.

The internal FortiGates have internal routing to both FortiManagers using the private IPs `192.0.2.161` and `192.0.2.177` for FortiManager-A and FortiManager-B respectively. External FortiGates can reach the public IPs `198.51.100.1` and `203.0.113.1` for FortiManager-A and FortiManager-B respectively.



This topic includes the following sections:

- Configure geo-redundant FortiManager HA with VRRP failover on page 1080
- Verifying the HA status on page 1081
- Additional FortiManager configuration on page 1081
- Adding a managed FortiGate to the FortiManager cluster on page 1082

- Testing VRRP failover on page 1082

Configure geo-redundant FortiManager HA with VRRP failover

To configure geo-redundant HA with VRRP failover:

1. Configure the HA settings on FortiManager-A.
   a. On FortiManager-A, go to *System Settings* > *HA*.
   b. Configure the *Cluster Settings* as follows, and click *Apply*.

Failover Mode	*VRRP*
Peer IP and Peer SN	Choose the following: • **IP Type**: `IPv4` • **Peer IP**: Enter the IP address of FortiManager-B (example, `192.0.2.177`) • **Peer SN**: Enter the serial number of the peer device.
VIP	Enter the VIP address for the cluster (example, `192.0.2.1`). This is a dummy IP and will not be used for deployment or management. The VIP **MUST** be identical in all peers.
VRRP Interface	Choose the VRRP interface (example, `port1`).
Priority	`200`
Unicast	On. In Geo-HA it is mandatory to use Unicast as peers will not be in the same Layer2.

2. Configure the HA settings on FortiManager-B.
   a. On FortiManager-B device, go to *System Settings* > *HA*.
   b. Configure the *Cluster Settings* as follows, and click *Apply*.

Failover Mode	*VRRP*
Peer IP and Peer SN	Choose the following: • **IP Type**: `IPv4` • **Peer IP**: Enter the IP address of FortiManager-A (example, `192.0.2.161`). • **Peer SN**: Enter the serial number of the peer device.
VIP	Enter the VIP address for the cluster (example, `192.0.2.1`). This is a dummy IP and will not be used for deployment or management. The VIP **MUST** be identical in all peers.
VRRP Interface	Choose the VRRP interface (example, `port1`).

Priority	`100`
Unicast	On. In Geo-HA it is mandatory to use Unicast as peers will not be in the same Layer2.

Verifying the HA status

To verify the HA status:

1. Access both FortiManager-A and FortiManager-B.
2. Using the GUI, you can view the *HA Status* on the top-right corner of each FortiManager and from *System Settings* > *HA*.
3. Using the CLI, you can run the following commands to get additional information about the HA status:

Command	Description
`get system ha-status`	Print the HA status.
`diagnose ha stats`	Diagnose the HA status.
`diagnose sniffer packet <interface> "vrrp"`	Perform a packet sniffer on the port used by the VRRP protocol using "vrrp" as a filter. This command can be used to verify that the advertisements are sent using the preferred method when *Unicast* mode is disabled/enabled.

Additional FortiManager configuration

Depending on the scenario, FortiManager can be using either 2 or 4 IP addresses (`192.0.2.161` and `192.0.2.177` for internal FortiGates and `198.51.100.1` and `203.0.133.1` for external FortiGates). It is a best practice to define all FortiManager IPs that will be used to manage FortiGates so that it is reflected in the FortiGate `config system central-management` settings if FortiGate is added from FortiManager.

Defining FortiManager IPs:

- Using the FortiManager CLI, you can run the following configuration:

```
config system admin setting
   set mgmt-fqdn <FQDN_1 | IP_1> <FQDN_2 | IP_2> ... <FQDN_N | IP_N>
end
```



You can add up to a total of 10 IP addresses or FQDNs to the `mgmt-fqdn` attribute.

- For example, in this scenario it will be as follows:

```
config system admin setting
   set mgmt-fqdn 192.0.2.161 192.0.2.177 198.51.100.1 203.0.113.1
end
```

Adding a managed FortiGate to the FortiManager cluster

To onboard using the FortiManager Device Manager:

1. On FortiManager-A, go to *Device Manager* > *Device & Groups* > *Managed FortiGate*.
2. Click *Add Device* > *Discover Device*.
3. Enable Use Legacy Device Login and enter the device IP Address, User Name, and Password.
4. Click *Next*, *Next*, and *Import Later*.
5. Run the `show system central-management` command in the FortiGate CLI to check the management IP addresses:

```
show system central-management
   config system central-management
      set type fortimanager
      set fmg "192.0.2.161" "192.0.2.177" "198.51.100.1" "203.0.113.1"
end
```

The IP addresses shown should reflect the IP addresses and FQDNs configured in FortiManager under `config system admin setting` as explained in the previous section.



In case of failover, FortiGate will try to reach out to **all IP addresses** configured under `system central management` and only the Primary FortiManager will respond.

To onboard using the Central Management connector on FortiGate:

1. On FortiGate, go to *Security Fabric* > *Fabric Connectors* > *Central Management*.
2. Under *IP/Domain*, click the *+* button to add more IP addresses.
3. Enter all of the FortiManager IP addresses and click *OK*.
   For example, in this scenario the external FortiGate devices will use the public IPs `198.51.100.1` and `203.0.113.1`.
4. You can authorize the device using the dialog from the FortiGate or from the Device Manager on the Primary FortiManager in the root ADOM.
5. Run `show system central-management` in the FortiGate CLI to check the management IP addresses. For example:

```
show system central-management
   config system central-management
      set type fortimanager
      set fmg "198.51.100.1" "203.0.113.1"
end
```

   The IP addresses displayed should match those configured in step 2.

Testing VRRP failover

To test the failover configuration:

1. On the FortiGate, run the following command in the CLI:

```
get system central-management
```

In the serial-number field, the serial numbers for both FortiManager-A and FortiManager-B are listed. FortiManager-A is listed first because it is currently acting as the Primary device.

2. In the CLI for FortiManager-A, run `diagnose ha force-vrrp-election` which will trigger failover to the FortiManager with the next highest priority.
3. Refresh the page and you will notice that the HA status of FortiManager-A becomes Secondary.
4. Go to FortiManager-B, and confirm that the HA status has changed to Primary.
5. Enter the following command in the CLI to confirm the status of FortiManager-A. FortiManager-A continues to act as the Secondary device until the next VRRP election occurs.
   ```
   diagnose ha stats
   ```
6. On the FortiGate, run the following command in the CLI.
   ```
   get system central-management
   ```
   In the serial-number field, the serial numbers for both FortiManager-A and FortiManager-B are listed. FortiManager-B will be listed first because it is now acting as the Primary device.

Certificate best practices for FortiManager HA with VRRP

Modern web browsers no longer use the *Common Name (CN)* field for hostname verification. Instead, they rely exclusively on the Subject Alternative Name (SAN) extension.

This document outlines best practices for deploying GUI certificates in a High Availability (HA) setup using Virtual Router Redundancy Protocol (VRRP), ensuring secure and seamless communication with your FortiManager HA environment.

For steps on configuring and uploading local certificates, refer to the following:

- Local certificates on page 956
- How to upload and set local certificate to be used in FortiManager.

Recommended certificate configuration approaches

There are two primary options for configuring certificates for your FortiManager HA with VRRP deployment.

1. Option 1: Use a single certificate with comprehensive SAN entries on page 1083.
2. Option 2: Use distinct certificates for each FortiManager on page 1084.

To illustrate the certificate configurations, the examples below use the following FortiManager HA VRRP setup details:

Component	IP Type	IP Address	FQDN
FMG1	Dedicated IP	10.0.0.1/24	fmg1.example.com
FMG2	Dedicated IP	10.0.0.2/24	fmg2.example.com
FortiManager HA VRRP	VIP (Virtual IP)	10.0.0.100	fmg_vip.example.com

Option 1: Use a single certificate with comprehensive SAN entries

This approach uses one certificate that includes all relevant identities in its SAN extension.

The certificate must contain the following in its SAN entries:

- The FQDN and/or IP address of the VRRP Virtual IP (VIP) address.
  - This is required to trust the certificate when you access the FortiManager HA setup using the VRRP VIP address.
- The FQDN and/or IP address of your primary FortiManager.
  - In some scenarios, you may need to access the primary FortiManager directly. Including its FQDN and/or IP address here ensures the certificate is trusted for direct access.
- The FQDN and/or IP address of your secondary FortiManager.
  - Similarly, you may need to access the secondary FortiManager directly in certain situations. Adding its FQDN and/or IP address ensures the certificate is trusted for direct access.



Since the CN is no longer used for the hostname verification by modern browsers, you can use any name for this field, or simply use the VRRP VIP address.

An example of the certificate configuration would look as follows:

- Shared certificate:

Field	Value
CN	fmg_vip.example.com
SAN	DNS: fmg_vip.example.com, DNS: fmg1.example.com, DNS: fmg2.example.com

The certificate configuration can also include the IP addresses in the SAN for broader access if required.

Option 2: Use distinct certificates for each FortiManager

If your organization's security policies require each FortiManager in the HA setup to have its own unique certificate, you can configure them as follows:

- Primary FortiManager's Certificate SAN
  - The FQDN and/or IP address of the primary FortiManager.
  - The FQDN and/or IP address of the VRRP VIP address.

  The CN for this certificate can be set to the FQDN or IP address of the primary FortiManager.
- Secondary FortiManager's Certificate SAN:
  - The FQDN and/or IP address of the secondary FortiManager.
  - The FQDN and/or IP address of the VRRP VIP address.

  The CN for this certificate can be set to the FQDN or IP address of the secondary FortiManager.

An example of the certificate configuration would look as follows:

- FMG1 certificate:

Field	Value
CN	fmg1.example.com
SAN	DNS: fmg_vip.example.com, DNS: fmg1.example.com

- FMG2 certificate:

Field	Value
CN	fmg2.example.com
SAN	DNS: fmg_vip.example.com, DNS: fmg2.example.com

The certificate configuration can also include the FMG2 and FortiManager HA VRRP IP addresses in the SAN for broader access if required.

Example - Demonstrating CN versus SAN behavior

This example scenario demonstrates that a certificate with the primary FortiManager's FQDN in the CN and the VRRP VIP FQDN in the SAN is only valid for the VIP FQDN. It's not trusted for direct access to the primary FortiManager FQDN. This further emphasizes the need to include all relevant FQDNs and/or IP addresses in the SAN extension for the certificate to be trusted across all access points.

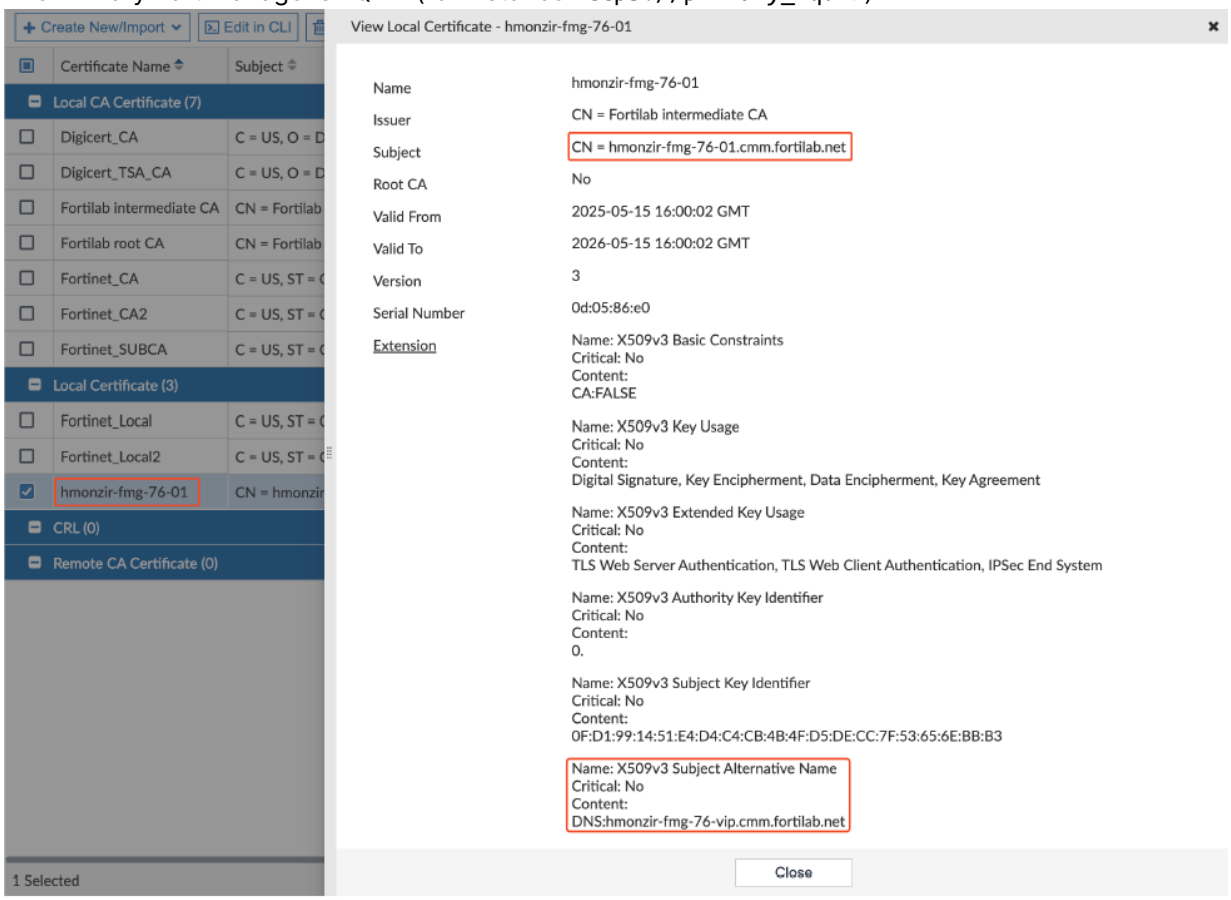
In this example scenario, a certificate is configured as follows:

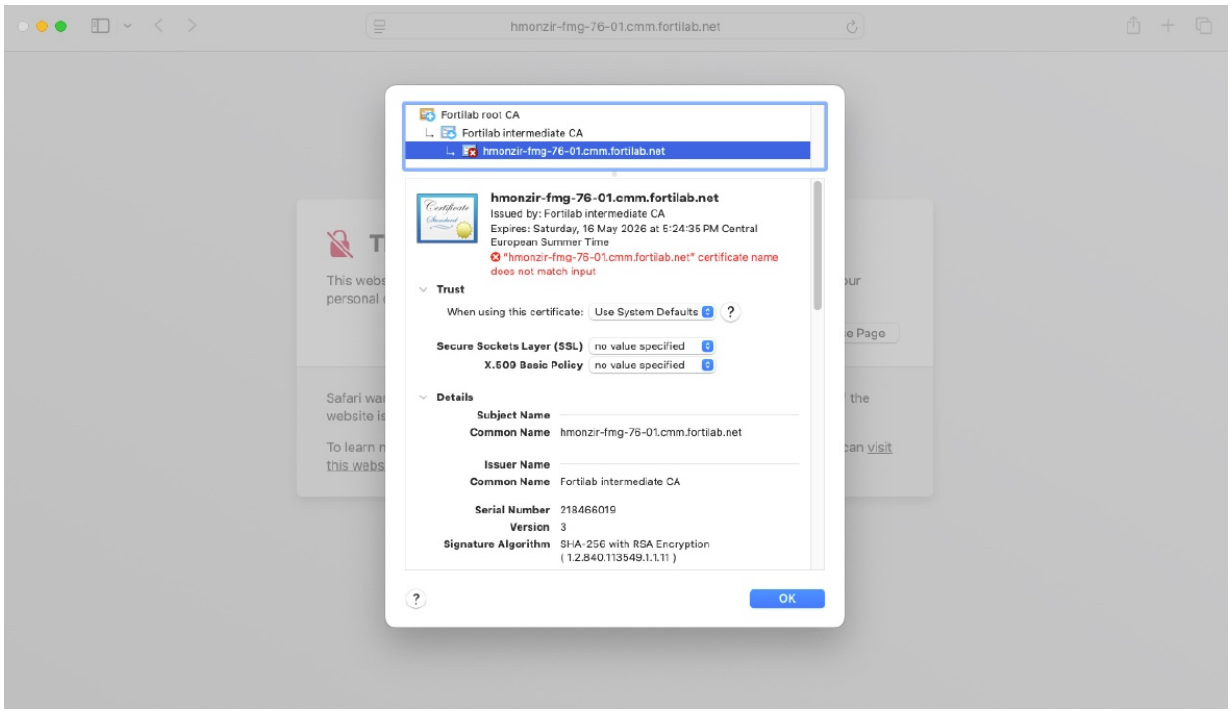
Field	Value
CN	Primary FortiManager's FQDN
SAN	VRRP VIP address's FQDN

Result:

- The certificate is trusted when accessing the FortiManager using:
  - The VRRP VIP FQDN (for instance `https://<vip_fqdn>`)
- The certificate is not trusted when accessing the primary FortiManager directly using its FQDN:

- The Primary FortiManager's FQDN (for instance `https://primary_fqdn>`)





Note that in this case, the certificate isn't trusted even though the URL used matches the certificate's CN.

Additional resources

- Safari: About trusted certificates
- Chrome: Deprecations and removals
- Firefox: Remove commonName matching from certificate hostname verification
- RFC 2818: HTTP Over TLS

Monitoring HA status

Go to *System Settings* > *HA* to monitor the status of the FortiManager units in an HA cluster. The FortiManager HA status pane displays information about the role of each cluster unit, the HA status of the cluster, and the HA configuration of the cluster.



The FortiManager GUI browser window title changes to indicate that the FortiManager unit is operating in HA mode. The following text is added to the title *HA (Group ID: <group_id>)*. Where <group_id> is the HA Group ID.



You can use the CLI command `get system ha` to display the same HA status information.

The following information is displayed:

Cluster Status	The cluster status can be *Up* if this unit is received HA heartbeat packets from all of its configured peers. The cluster status will be *Down* if the cluster unit is not receiving HA heartbeat packets from one or more of its configured peers.
Mode	The role of the FortiManager unit in the cluster. The role can be: • *Primary*: for the primary unit. • *Secondary*: for the backup units.
Module Data Synchronized	The amount of data synchronized between this cluster unit and other cluster units.
Pending Module Data	The amount of data waiting to be synchronized between this cluster unit and other cluster units.

Upgrading the FortiManager firmware for an operating cluster

For information on upgrading the FortiManager firmware for an operating cluster, see the *FortiManager Upgrade Guide* on the Fortinet Docs Library.

Appendix A - Supported RFC Notes

This section identifies the request for comment (RFC) notes supported by FortiManager.

RFC 2548

Description:

Microsoft Vendor-specific RADIUS Attributes

Category:

Informational

Webpage:

http://tools.ietf.org/html/rfc2548

RFC 3414

Description:

User-Based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).

Category:

Standards Track

Webpage:

http://tools.ietf.org/html/rfc3414

RFC 2665

Description:

Ethernet-like MIB parts that apply to FortiManager units.

Category:

Standards Track

Webpage:

http://tools.ietf.org/html/rfc2665

RFC 1213

Description:

MIB II parts that apply to FortiManager units.

Category:

FortiManager (SNMP)

Webpage:

http://tools.ietf.org/html/rfc1213

Notes

RFC support for SNMP v3 includes Architecture for SNMP Frameworks (as described in RFC 3411). Generic Fortinet traps : ColdStart, WarmStart, LinkUp, LinkDown (as described in RFC 1215).

Appendix B - Policy ID support

FortiGate allows a `policy-id` value in the range of `0-4294967294`.

However, FortiManager only supports a range of `0–1071741824`. As a result, you can only import into FortiManager or create in FortiManager a policy item with a policy ID up to `1071741824`.

FortiManager has reserved all policy IDs >= `1071741825` for internal use, and current features use the following reserved policy ID ranges:

Item	FortiManager reserved policy ID range
Policy block	1071741825 - 1072741824
VPN policy	1072741825 - 1073741824
Global header policy	1073741825 - 1074741824
Global footer policy	1074741825 - 1075741824
Internal & Future Use	1075741825 - 4294967294

Appendix C - Re-establishing the FGFM tunnel after VM license migration

When migrating a FortiManager to a new license type, the serial number associated with the FortiManager is also changed. This impacts the FGFM (FortiGate to FortiManager) tunnel that exists between FortiManager and its managed FortiGate devices.

Depending on how the FortiGate was initially added to the FortiManager (through the FortiManager or through the FortiGate), you may need to manually update the username and password of FortiGate devices in the FortiManager database before the FGFM tunnel can be re-established.

Follow the steps below to re-establish the FGFM connection with managed FortiGate devices.

- FGFM connection established through FortiManager on page 1092
- FGFM connection established through FortiGate on page 1093

FGFM connection established through FortiManager

If the device was added from the FortiManager using the *Add Device* wizard, after the migration the FortiManager will automatically have the correct device's username and password and the FGFM tunnel can be immediately re-established.

To re-stablish the FGFM tunnel:

1. In the FortiManager CLI, execute the following to bring the tunnel up:
   `execute fgfm reclaim-dev-tunnel`



If the `execute fgfm reclaim-dev-tunnel` fails to establish a connection between the FortiManager and one or more FortiGate device, it is likely because the FGFM connection was originally established through the FortiGate for those devices. See FGFM connection established through FortiGate on page 1093.

FGFM connection established through FortiGate

If the FGFM tunnel was initialized through the FortiGate, and FortiManager was used to promote (authorize) the device, the FortiManager may not have the device's administrator username and password. You can configure the credentials required for the FGFM tunnel through the FortiManager GUI, CLI, or through the FortiGate CLI. See Step 1: Configure the FGFM credentials on page 1093

After updating the FGFM credentials, perform the `execute fgfm reclaim-dev-tunnel` command to bring the tunnel up. See Step 2: Re-establish the FGFM tunnel on page 1094.

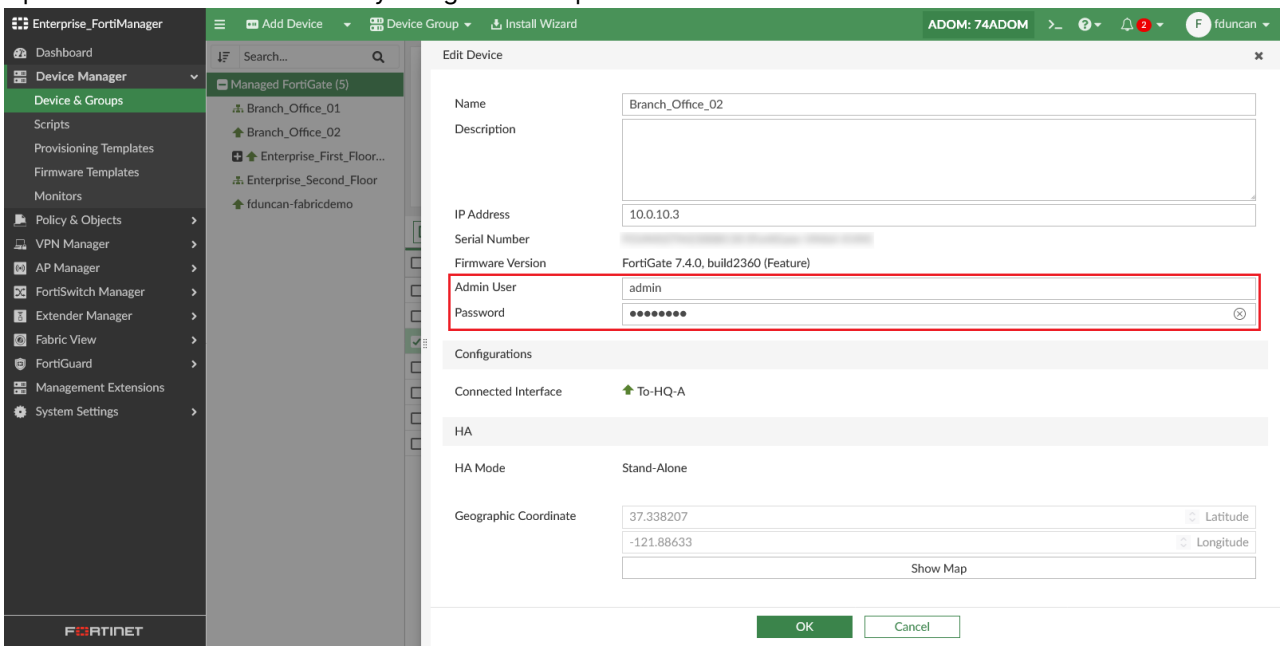
Step 1: Configure the FGFM credentials

Configure the FGFM credentials through one of the following methods:

- Configure the FGFM credentials using the FortiManager GUI
- Configure the FGFM credentials using the FortiManager CLI
- Configure the FGFM credentials using the FortiGate CLI

To configure the FGFM credentials using the FortiManager GUI:

1. Log in to the FortiManager.
2. In the GUI, go to *Device Manager*, select the FortiGate device in the list of managed devices, and click *Edit*.
3. Update the FGFM credentials by using a valid super admin account for the FortiGate.



4. Click *OK*.
5. Repeat this process for each FortiGate that needs to be updated.

To update the device's FGFM credentials in the CLI:

1. In the FortiManager CLI, enter the following commands:
   `execute device replace user <device name> <user>`
   `execute device replace pw <device name> <password>.`
2. Repeat this process for each FortiGate that needs to be updated.

To configure the device's FGFM credentials in the FortiGate CLI:

1. In the FortiGate CLI, enter the following command:
   `execute central-mgmt register-device <FMG Serial Number> <FGT admin password>.`
2. Repeat this process for each FortiGate that needs to be updated.

Step 2: Re-establish the FGFM tunnel

To re-establish the FGFM tunnel after the FGFM credentials are updated:

1. Enter the following command in the FortiManager CLI to re-establish the FGFM tunnel:
   `execute fgfm reclaim-dev-tunnel`

Appendix D - FortiManager Ansible Collection documentation

Documentation for the Fortinet FortiManager Ansible Collection is available through the link below.

- FortiManager Ansible Collection documentation



www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.