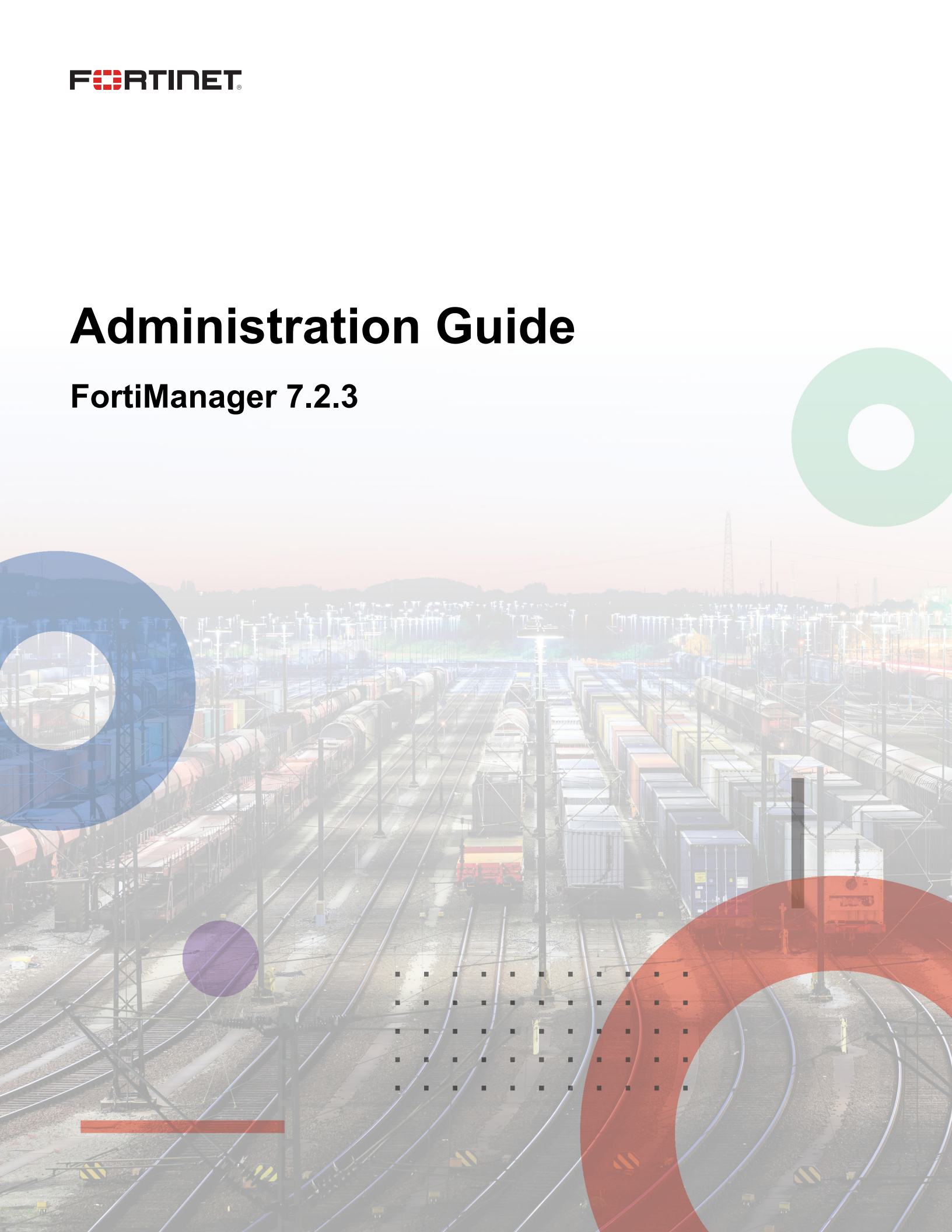


# Administration Guide

**FortiManager 7.2.3**



**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](mailto:techdoc@fortinet.com)



October 23rd, 2023

FortiManager 7.2.3 Administration Guide

02-723-781535-20231023



# TABLE OF CONTENTS

<b>Change Log</b>	<b>14</b>
<b>Setting up FortiManager</b>	<b>15</b>
Connecting to the GUI	15
FortiManager Setup wizard	16
Activating VM licenses	21
Security considerations	23
Restricting GUI access by trusted host	23
Trusted platform module support	23
Other security considerations	25
GUI overview	25
Panels	27
Color themes	27
Side menu open or closed	27
Switching between ADOMs	28
Using the right-click menu	28
Avatars	28
Showing and hiding passwords	29
FortiAnalyzer Features	29
Enable or disable FortiAnalyzer features	30
Initial setup	30
Restarting and shutting down	31
<b>FortiManager Key Concepts</b>	<b>32</b>
Communication through protocols	33
FortiGuard	34
Device Manager	34
FortiAnalyzer features	34
Configuration through Device Manager	35
Direct device database editing	35
Indirect device database editing	35
Model devices	36
ADOMs and devices	36
Global ADOM layer	37
ADOM and policy layer	37
Device Manager layer	38
Operations	38
Install device settings only	38
Quick install (device db)	39
Install policy package	39
Re-install policy	39
Import configuration	39
Retrieve configuration	40
Auto-update and auto-retrieve	40
Auto-backup	41
Refresh	41

Revert .....	41
Sequence of operations for installation to managed devices .....	41
Key features of the FortiManager system .....	46
Security Fabric .....	46
Configuration revision control and tracking .....	46
Centralized management .....	46
Administrative domains .....	46
Local FortiGuard service provisioning .....	46
Firmware management .....	46
Scripting .....	47
Logging and reporting .....	47
Fortinet device life cycle management .....	47
<b>Device Manager .....</b>	<b>48</b>
ADOMs .....	49
Device & Groups .....	49
Add devices .....	51
Add FortiAnalyzer or FortiAnalyzer BigData .....	85
Add VDOM .....	92
Device groups .....	94
Table view .....	95
Ring view .....	106
Map view .....	109
Folder view .....	113
Import Configuration wizard .....	117
Install wizard .....	120
Firmware upgrade .....	125
Device database (DB) .....	132
Device DB - Dashboard .....	137
Device DB - configuration management .....	142
Device DB - Network Interface .....	147
Device DB - System Virtual Domain .....	150
Device DB - System SD-WAN .....	154
Device DB - System HA .....	162
Device DB - Router BGP .....	162
Device DB - CLI Configurations .....	163
Device maintenance .....	163
Managing FortiGate HA clusters .....	165
FortiManager supports FortiGate auto-scale clusters .....	166
Example of how FortiManager manages auto-scale clusters .....	166
Scripts .....	168
Enabling scripts .....	169
Configuring scripts .....	169
CLI script group .....	175
Script syntax .....	176
Script history .....	179
Script samples .....	180
Provisioning Templates .....	200
Template groups .....	201

Fabric authorization templates .....	205
System templates .....	207
IPsec tunnel templates .....	212
SD-WAN templates .....	231
SD-WAN overlay templates .....	245
Static route templates .....	262
BGP templates .....	264
Certificate templates .....	268
Threat Weight templates .....	269
CLI templates .....	270
NSX-T service templates .....	277
Export and import provisioning template configurations .....	280
Firmware templates .....	280
Creating firmware templates .....	281
Editing firmware templates .....	283
Deleting firmware templates .....	284
Assigning firmware templates to devices .....	284
Previewing upgrades .....	285
Reviewing upgrade history .....	285
Upgrading devices now .....	286
Monitors .....	286
SD-WAN Monitor .....	286
VPN Monitor .....	291
Asset Identity Center .....	292
AI Analysis .....	294
FortiMeter .....	295
Overview .....	296
Points .....	297
Authorizing metered VMs .....	297
Monitoring VMs .....	298
FortiGate chassis devices .....	298
Viewing chassis dashboard .....	299
<b>Policy &amp; Objects .....</b>	<b>304</b>
About policies .....	306
Policy theory .....	306
Global policy packages .....	307
Policy workflow .....	308
Provisioning new devices .....	308
Day-to-day management of devices .....	308
Feature visibility .....	309
Managing policy packages .....	310
Create new policy packages .....	310
Create new policy package folders .....	311
Edit a policy package or folder .....	312
Clone a policy package .....	312
Remove a policy package or folder .....	313
Assign a global policy package .....	313
Install a policy package .....	314



Reinstall a policy package .....	315
Schedule a policy package install .....	317
Export a policy package .....	318
Policy package installation targets .....	318
Perform a policy consistency check .....	320
View logs related to a policy rule .....	321
Find and replace objects .....	322
Managing policies .....	322
Policy Lookup .....	328
Creating policies .....	329
Editing policies .....	329
Create a new firewall policy .....	335
Create a new SSL inspection and authentication policy .....	343
Create a new security policy .....	349
Create a new firewall virtual wire pair policy .....	353
Create a new virtual wire pair SSL inspection and authentication policy .....	360
Create a new security virtual wire pair policy .....	366
Create a new proxy policy .....	369
Create a new central SNAT policy .....	373
Create a new central DNAT or IPv6 central DNAT policy .....	375
Create a new DoS policy .....	382
Create a new interface policy .....	385
Create a new multicast policy .....	386
Create a new local-in policy .....	388
Create a new traffic shaping policy .....	388
Create a new authentication rule .....	391
Hyperscale policies .....	392
Create a new NAC policy .....	393
Create a new FortiProxy firewall policy .....	395
Create a new FortiProxy proxy auto-configuration (PAC) policy .....	397
Using Policy Blocks .....	398
Creating Policy Blocks .....	398
Adding policies to a Policy Block .....	399
Appending a Policy Block to a Policy Package .....	400
Using Policy Blocks versus Global Policy Packages .....	401
Role-based access control for Policy Blocks .....	402
Managing objects and dynamic objects .....	402
Create a new object .....	403
Creating an IPv6 Address Template .....	405
Promote an Object to Global Database .....	407
Normalized interfaces .....	408
Map a dynamic ADOM object .....	417
Map a dynamic device object .....	418
Map a dynamic device group .....	420
Remove an object .....	421
Edit an object .....	421
Push to device .....	422
Clone an object .....	422
Search objects .....	422

Find unused objects .....	423
Find and merge duplicate objects .....	423
Export signatures to CSV file format .....	423
CLI Configurations .....	424
FortiToken configuration example .....	425
FSSO user groups .....	425
Interface mapping .....	429
VIP mapping .....	429
Modify existing interface-zone mapping .....	429
Create a new shaping profile .....	431
Intrusion Prevention filtering options .....	433
IPS Signatures .....	435
ADOM-level metadata variables .....	437
Default address space objects .....	440
Persistent object search menu .....	441
Zero Trust Network Access (ZTNA) objects .....	442
FortiProxy content analysis objects .....	446
ADOM revisions .....	448
<b>AP Manager .....</b>	<b>451</b>
Device & Groups .....	451
Quick status bar .....	452
Managing APs .....	453
FortiAP groups .....	458
Device summary .....	459
Authorizing and deauthorizing FortiAP devices .....	459
Installing changes to FortiAP devices .....	460
Rogue APs .....	460
Authorizing unknown APs .....	462
Connected clients .....	462
Spectrum analysis for managed APs .....	463
Clients Monitor .....	464
Health Monitor .....	465
Replacing APs .....	466
Map view .....	467
Google map .....	468
Floor map .....	469
WiFi Templates .....	470
WiFi profiles for central management .....	470
Enabling FortiAP central management .....	471
WiFi settings .....	471
FortiAP profiles .....	474
SSIDs .....	480
WIDS profiles .....	489
Bluetooth profiles .....	493
QoS profiles .....	496
Bonjour profiles .....	498
ARRP profiles .....	500
L3 Firewall Profiles .....	503

Assigning profiles to FortiAP devices .....	505
FortiAP configuration profiles .....	506
MPSK profiles .....	507
WiFi profiles for per-device management .....	509
Enabling FortiAP per-device management .....	509
Creating profiles .....	510
<b>VPN Manager .....</b>	<b>511</b>
Overview .....	511
Enabling central VPN management .....	512
DDNS support .....	513
VPN Setup Wizard supports device groups .....	514
IPsec VPN .....	527
IPsec VPN Communities .....	527
IPsec VPN gateways .....	536
Using Map View .....	543
Monitoring IPsec VPN tunnels .....	544
SSL VPN .....	544
Manage SSL VPNs .....	544
Portal profiles .....	547
Monitoring SSL VPNs .....	553
VPN security policies .....	553
Defining policy addresses .....	554
Defining security policies .....	554
<b>Fabric View .....</b>	<b>556</b>
Security Fabric Topology .....	556
Physical Topology .....	557
Logical Topology .....	558
Filter Topology Views .....	559
Search Topology Views .....	560
Security Rating .....	560
Enabling the Security Rating tab .....	561
Viewing Security Fabric Ratings .....	562
Security Fabric score .....	562
Fabric Connectors .....	563
Core Network Security .....	563
External Connectors .....	565
Public and private SDN .....	565
Threat Feeds .....	591
Endpoint/Identity .....	592
<b>FortiGuard .....</b>	<b>627</b>
Licensing status .....	628
View licensing status .....	628
Package management .....	630
Receive status .....	630
Service status .....	631
IoT packages .....	633
Exporting packages example .....	634



Importing packages example .....	635
Query server management .....	637
Receive status .....	637
Query status .....	638
Exporting web filter databases example .....	638
Importing web filter databases example .....	639
Firmware images .....	641
Download prioritization .....	642
Product download prioritization .....	643
Package download prioritization .....	644
Settings .....	645
Connecting the built-in FDS to the FDN .....	648
Operating as an FDS in a closed network .....	649
Licensing in an air-gap environment .....	651
Enabling FDN third-party SSL validation and Anycast support .....	657
Configuring devices to use the built-in FDS .....	658
Matching port settings .....	658
Handling connection attempts from unauthorized devices .....	658
Configure a FortiManager without Internet connectivity to access a local FortiManager as FDS .....	659
Configuring FortiGuard services .....	660
Enabling push updates .....	660
Enabling updates through a web proxy .....	662
Overriding default IP addresses and ports .....	662
Scheduling updates .....	663
Accessing public FortiGuard web and email filter servers .....	663
Logging events related to FortiGuard services .....	664
Logging FortiGuard antivirus and IPS updates .....	664
Logging FortiGuard web or email filter events .....	664
Restoring the URL or antispam database .....	665
<b>FortiSwitch Manager .....</b>	<b>666</b>
Device & Groups .....	666
Managed Switches .....	667
Monitors .....	680
FortiSwitch Templates for central management .....	682
Enabling FortiSwitch central management .....	682
FortiSwitch Templates .....	683
FortiSwitch Profiles for per-device management .....	700
Enabling per-device management .....	700
FortiSwitch profiles .....	701
CLI Configurations .....	705
Configuring a port on a single FortiSwitch .....	706
<b>Extender Manager .....</b>	<b>708</b>
Managed extenders .....	708
Managing FortiExtender devices .....	709
FortiExtender profiles .....	711
FortiExtender templates .....	711

SIM Profiles .....	713
Data plans .....	715
<b>System Settings .....</b>	<b>718</b>
Dashboard .....	719
Customizing the dashboard .....	720
System Information widget .....	721
System Resources widget .....	729
License Information widget .....	729
Unit Operation widget .....	734
Alert Messages Console widget .....	734
Log Receive Monitor widget .....	735
Insert Rate vs Receive Rate widget .....	735
Log Insert Lag Time widget .....	736
Receive Rate vs Forwarding Rate widget .....	736
Disk I/O widget .....	737
Logging Topology .....	737
Network .....	738
Configuring network interfaces .....	739
Disabling ports .....	740
Changing administrative access .....	741
Static routes .....	741
Packet capture .....	742
Aggregate links .....	743
VLAN interfaces .....	744
RAID Management .....	744
Supported RAID levels .....	744
Configuring the RAID level .....	747
Monitoring RAID status .....	747
Checking RAID from command line .....	748
Swapping hard disks .....	749
Adding hard disks .....	750
Administrative Domains (ADOMs) .....	750
FortiProxy ADOMs .....	752
Enabling and disabling the ADOM feature .....	753
ADOM device modes .....	754
ADOM modes .....	754
Managing ADOMs .....	758
Deleting ADOMs .....	763
Checking ADOM health .....	764
ADOM versions .....	766
Concurrent ADOM access .....	768
Locking an ADOM .....	770
Upgrading an ADOM .....	770
Using mixed versions in ADOMs .....	771
Global Database .....	772
Certificates .....	777
Local certificates .....	778
CA certificates .....	780

Certificate revocation lists .....	782
Event Log .....	782
Event log filtering .....	784
Task Monitor .....	785
SNMP .....	786
SNMP agent .....	786
SNMP v1/v2c communities .....	788
SNMP v3 users .....	791
SNMP MIBs .....	792
SNMP traps .....	793
Fortinet & FortiManager MIB fields .....	794
Mail Server .....	795
Syslog Server .....	797
Send local logs to syslog server .....	798
Meta Fields .....	798
Device logs .....	800
Configuring rolling and uploading of logs using the GUI .....	801
Configuring rolling and uploading of logs using the CLI .....	802
File Management .....	804
Advanced Settings .....	804
Restart, shut down, or reset FortiManager .....	805
Restarting FortiManager .....	806
Shutting down FortiManager .....	806
Resetting system settings .....	806
<b>Administrators .....</b>	<b>808</b>
Trusted hosts .....	808
Monitoring administrators .....	809
Disconnecting administrators .....	809
Managing administrator accounts .....	809
Creating administrators .....	811
Editing administrators .....	816
Deleting administrators .....	816
Override administrator attributes from profiles .....	817
Restricted administrators .....	818
Web Filter restricted administrator .....	820
Intrusion prevention restricted administrator .....	823
Application control restricted administrator .....	834
Installing profiles as a restricted administrator .....	837
Workspace mode for restricted administrators .....	838
Administrator profiles .....	839
Permissions .....	840
Creating administrator profiles .....	843
Editing administrator profiles .....	846
Cloning administrator profiles .....	846
Deleting administrator profiles .....	846
Workspace .....	847
Workspace mode .....	848



Workflow mode .....	854
Workflow sessions .....	857
Install and unlock setting for Workspace mode .....	863
Authentication .....	864
Public Key Infrastructure .....	864
Managing remote authentication servers .....	866
LDAP servers .....	867
RADIUS servers .....	869
TACACS+ servers .....	871
Remote authentication server groups .....	871
SAML admin authentication .....	872
FortiCloud SSO admin authentication .....	875
Global administration settings .....	877
Password policy .....	880
Password lockout and retry attempts .....	880
GUI language .....	881
Idle timeout .....	881
Security Fabric authorization information for FortiOS .....	882
Control administrative access with a local-in policy .....	882
Two-factor authentication .....	883
Two-factor authentication with FortiAuthenticator .....	883
Two-factor authentication with FortiToken Cloud .....	886
<b>High Availability .....</b>	<b>889</b>
Synchronizing the FortiManager configuration and HA heartbeat .....	890
If the primary or a backup unit fails .....	890
FortiManager HA cluster startup steps .....	891
Configuring HA options .....	891
General FortiManager HA configuration steps .....	894
GUI configuration steps .....	895
Monitoring HA status .....	897
Upgrading the FortiManager firmware for an operating cluster .....	897
FortiManager support for FortiAnalyzer HA .....	897
<b>Management Extensions .....</b>	<b>900</b>
FortiAIOps MEA .....	900
FortiPortal MEA .....	901
FortiSigConverter MEA .....	901
FortiSOAR MEA .....	901
FortiWLM MEA .....	901
Policy Analyzer MEA .....	902
Universal Connector MEA .....	902
Enabling management extension applications .....	902
CLI for management extensions .....	903
Accessing management extension logs .....	904
Checking for new versions and upgrading .....	904

---

<b>Appendix A - Supported RFC Notes .....</b>	<b>906</b>
<b>Appendix B - Policy ID support .....</b>	<b>908</b>
<b>Appendix C - Re-establishing the FGFM tunnel after VM license migration ..</b>	<b>909</b>
FGFM connection established through FortiManager .....	909
FGFM connection established through FortiGate .....	909
<b>Appendix D - FortiManager Ansible Collection documentation .....</b>	<b>912</b>

## Change Log

Date	Change Description
2023-06-08	Initial release.
2023-06-13	Updated <a href="#">Viewing configuration status on page 97</a>
2023-06-15	Updated <a href="#">Creating policy packages on page 776</a> .
2023-06-21	Updated <a href="#">Assign a global policy package on page 313</a> .
2023-06-23	Updated <a href="#">Create a new proxy policy on page 369</a> to include ZTNA proxy.
2023-06-26	Updated <a href="#">Policy search and filter on page 324</a> .
2023-06-29	Updated <a href="#">Licensing in an air-gap environment on page 651</a> .
2023-07-12	Updated <a href="#">Enabling SD-WAN monitoring history on page 290</a> .
2023-08-01	Updated <a href="#">Migrating the configuration on page 728</a> .
2023-08-03	Updated <a href="#">ADOM device modes on page 754</a> .
2023-08-18	Updated <a href="#">Password policy on page 880</a> .
2023-09-12	Updated <a href="#">Appendix C - Re-establishing the FGFM tunnel after VM license migration on page 909</a> .
2023-10-23	Updated <a href="#">Enabling and disabling the ADOM feature on page 753</a> .



# 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 23](#)
- [GUI overview on page 25](#)
- [FortiAnalyzer Features on page 29](#)
- [Initial setup on page 30](#)
- [Restarting and shutting down on page 31](#)

## 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 21](#).

---

### 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 postpone 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 25](#).



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 739](#).



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 741](#).

---



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 809](#) 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.

**FortiManager Setup - Welcome (1/4)**

**Welcome**

Perform the following steps to complete the setup of this FortiManager.

1. Register and SSO with FortiCare  
☐ Import the Entitlement File
2. Specify Hostname
3. Change Your Password
4. Upgrade Firmware

Begin

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 651](#).

### FortiManager Setup

#### Register

Serial Number

FMG-VMTM22001742

Account ID/Email

Password

✕ 👁

[Register](#)

[Forgot your password?](#)

#### SSO with Forticare

Country/Region

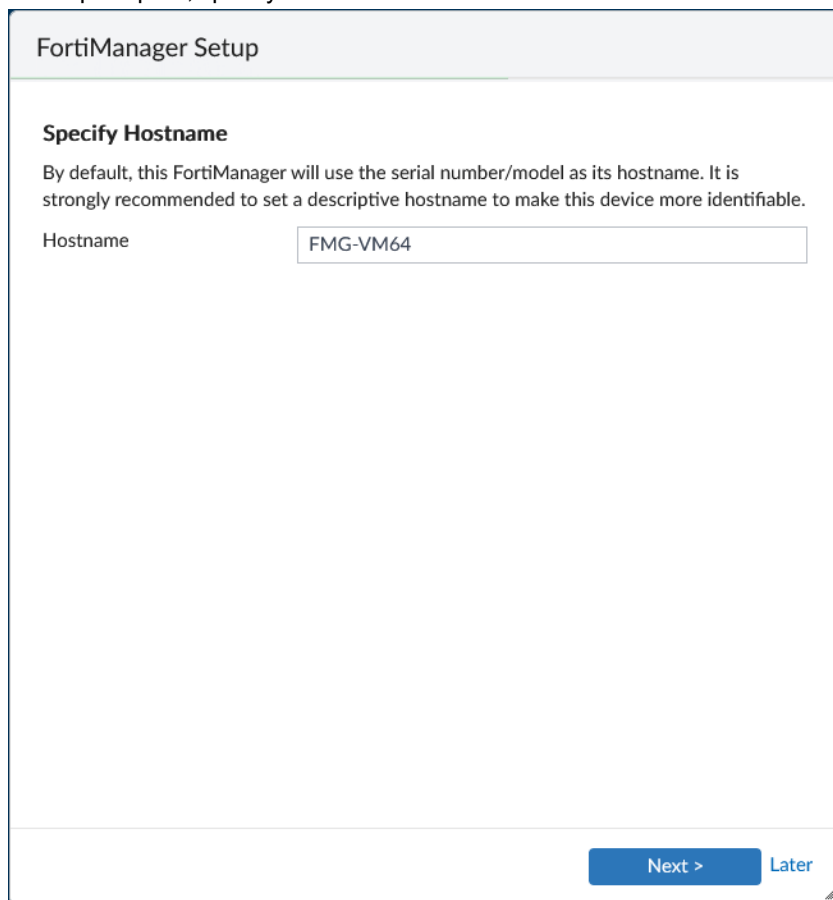
Reseller

FortiCloud Single Sign-on

📘 ☒

Next >

4. When prompted, specify the hostname.



**FortiManager Setup**

**Specify Hostname**

By default, this FortiManager will use the serial number/model as its hostname. It is strongly recommended to set a descriptive hostname to make this device more identifiable.

Hostname

Next > Later

5. In the *Hostname* box, type a hostname.
6. Click *Next*.

7. When prompted, change your password.

**FortiManager Setup**

**Change Your Password**

This account is using the default password. You are required to change your password.

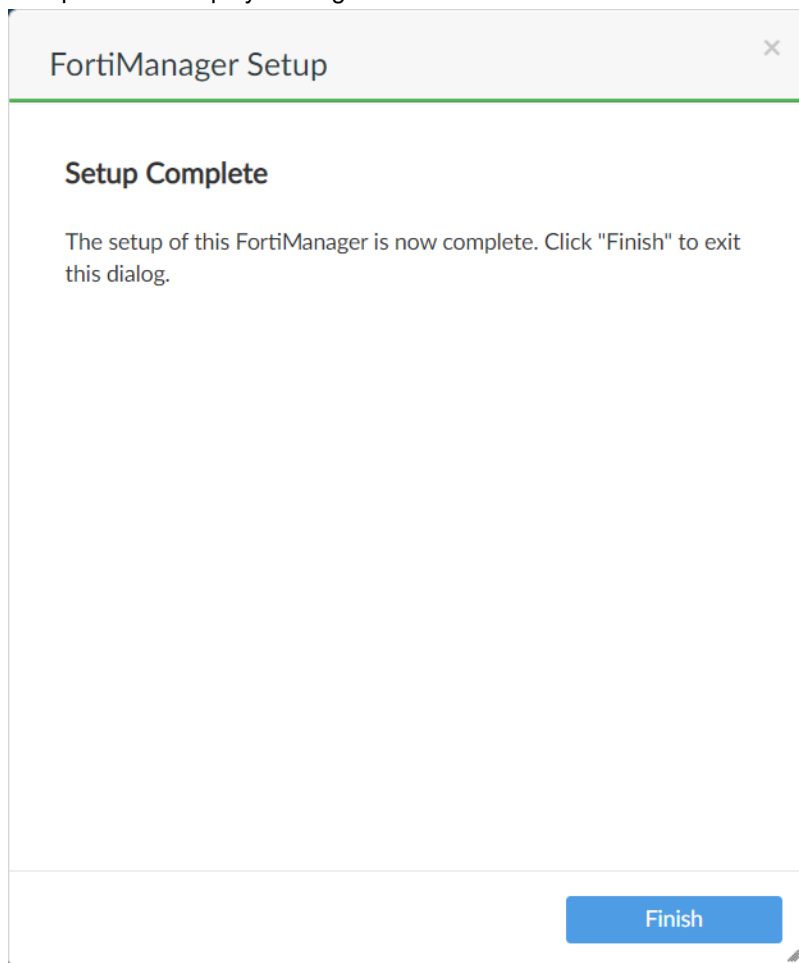
New Password

Confirm Password

Next >

- 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. Complete the setup by clicking *Finish*.



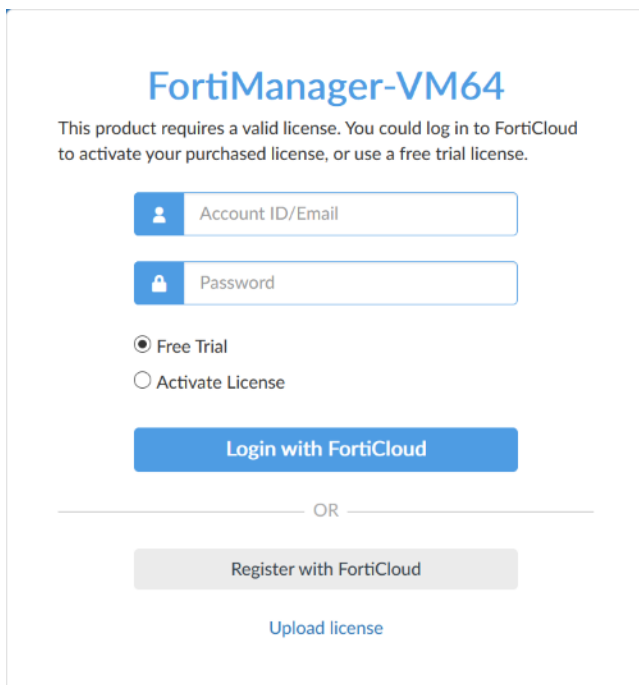
You are logged in to FortiManager.

## 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 box is displayed.



**FortiManager-VM64**

This product requires a valid license. You could log in to FortiCloud to activate your purchased license, or use a free trial license.

Account ID/Email

Password

☒ Free Trial  
☐ Activate License


Login with FortiCloud

OR

Register with FortiCloud

[Upload license](#)

2. Take one of the following actions:

Action	Description
<b>Free Trial</b>	<p>If a valid license is not associated with the account, you can start a free trial license.</p> <ol style="list-style-type: none"> <li>1. Select <i>Free Trial</i>, and click <i>Login with FortiCloud</i>.</li> <li>2. Use your FortiCloud account credentials to log in, or create a new account. FortiManager connects to FortiCloud to get the trial license. The system will restart to apply the trial license.</li> <li>3. Read and accept the license agreement.</li> </ol> <p>For more information, see the <a href="#">FortiManager VM Trial License Guide</a>.</p>
<b>Activate License</b>	<p>If you have a license file, you can activate it .</p> <ol style="list-style-type: none"> <li>1. Select <i>Activate License</i>, and click <i>Login with FortiCloud</i>.</li> <li>2. Use your FortiCloud account credentials to log in. FortiManager connects to FortiCloud, and the license agreement is displayed.</li> <li>3. Read and accept the license agreement.</li> </ol>
<b>Upload License</b>	<ol style="list-style-type: none"> <li>1. Click <i>Browse</i> to upload the license file, or drag it onto the field.</li> <li>2. Click <i>Upload</i>. After the license file is uploaded, the system will restart to verify it. This may take a few moments.</li> </ol> <div>  <p>To download the license file, go to the Fortinet Technical Support site (<a href="https://support.fortinet.com/">https://support.fortinet.com/</a>), and use your FortiCloud credentials to log in. Go to <i>Asset &gt; Manage/View Products</i>, then click the product serial number.</p> </div>



## 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 23](#)
- [Trusted platform module support on page 23](#)
- [Other security considerations on page 25](#)

### 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 808](#) for more details.

### Trusted platform module support

On supported FortiManager hardware devices, the Trusted Platform Module (TPM) can be used to protect your password and key against malicious software and phishing attacks. The dedicated module hardens the FortiManager by generating, storing, and authenticating cryptographic keys.

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. This encrypts sensitive data on the FortiManager using AES128-CBC. With the password, TPM generates a 2048-bit primary key to secure the master-encryption-password through RSA-2048 encryption. The master-encryption-password protects the data. The primary key protects the master-encryption-password.

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



The TPM module does not encrypt the disk drive of eligible FortiManager.

---

The primary key binds the encrypted configuration 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 configuration file. When restoring a configuration that includes a TPM protected master-encryption-password:

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

For information on backing up and restoring the configuration, see [Backing up the system on page 726](#) and [Restoring the configuration on page 728](#).

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 728](#).

Passwords and keys that can be encrypted by the master-encryption-key include:

- Admin password
- Alert email user's password
- BGP and other routing related configurations
- External resource
- FortiGuard proxy password
- FortiToken/FortiToken Mobile's seed
- HA password
- IPsec pre-shared key
- Link Monitor, server side password
- Local certificate's private key
- Local, LDAP, RADIUS, FSSO, and other user category related passwords
- Modem/PPPoE
- NST password
- NTP Password
- SDN connector, server side password
- SNMP
- Wireless Security related password



In HA configurations, each cluster member must use the same master-encryption-key so that the HA cluster can form and its members can synchronize their configurations.

---

### 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.
```

## 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 following home page of tiles is displayed:



Select one of the following tiles to display the respective pane. The available tiles vary depending on the privileges of the current user.

<b>Device Manager</b>	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 <a href="#">Device Manager on page 48</a> .
<b>Policy &amp; Objects</b>	Configure policy packages and objects. See <a href="#">Policy &amp; Objects on page 304</a> .
<b>AP Manager</b>	Configure and manage FortiAP access points. For more information, see <a href="#">AP Manager on page 451</a> .
<b>VPN Manager</b>	Configure and manage VPN connections. You can create VPN topologies and managed/external gateways. See <a href="#">VPN Manager on page 511</a> .

<b>Fabric View</b>	Configure fabric connectors and view Security Fabric Ratings. See <a href="#">Fabric View on page 556</a> .
<b>FortiGuard</b>	Manage communication between devices and the FortiManager using the FortiGuard protocol. See <a href="#">FortiGuard on page 627</a> .
<b>FortiSwitch Manager</b>	Configure and manage FortiSwitch devices. See <a href="#">FortiSwitch Manager on page 666</a> .
<b>Extender Manager</b>	Configure and manage FortiExtenders. See <a href="#">Extender Manager on page 708</a> .
<b>Management Extensions</b>	Enable and use management extension applications that are released and signed by Fortinet. See <a href="#">Management Extensions on page 900</a> .
<b>Log View</b>	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.
<b>Reports</b>	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.
<b>System Settings</b>	Configure system settings such as network interfaces, administrators, system time, server settings, and others. You can also perform maintenance and firmware operations. See <a href="#">System Settings on page 718</a> .
<b>Incidents &amp; Events</b>	Configure and view events for logging devices. This pane is only available when FortiAnalyzer features are enabled.

After you choose a tile, click the *Open/Close side menu* button beside the tile name to close the side menu and view only the content pane in the browser window, or click to display the side menu and the content pane. See [Side menu open or closed on page 27](#).

The top-right corner of the home page includes a variety of possible selections:

<b>HA status</b>	If HA is enabled, the status is shown.
<b>ADOM</b>	<p>If ADOMs are enabled, the required ADOM can be selected from the dropdown list.</p> <p>If enabled, ADOMs can also be locked or unlocked.</p> <p>The ADOMs available from the ADOM menu will vary depending on the privileges of the current user.</p>
<b>Tools</b>	Click to access the <i>CLI Console</i> and the <i>Online Help</i> .
<b>CLI Console</b>	<p>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.</p> <p>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.</p> <p>Click <i>Detach</i> in the CLI Console toolbar to open the console in a separate window.</p> <p><b>Note:</b> The <i>CLI Console</i> requires that your web browser support JavaScript.</p>

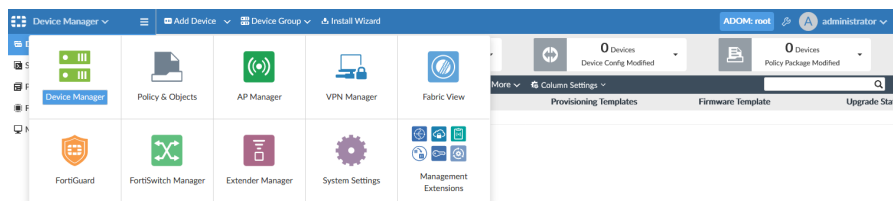
	<b>Online Help</b>	Click to open the FortiManager online help.
<b>Notification</b>		Click to display a list of notifications. Select a notification from the list to take action on the issue.
<b>admin</b>		Click to change the administrator profile, upgrade the firmware of FortiManager, change your password, or log out of the GUI.

## Panes

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

<b>Banner</b>	Along the top of the page; includes the home button (Fortinet logo), tile menu, open/close side menu, ADOM menu (when enabled), tools menu, notifications, and admin menu.
<b>Tree menu</b>	On the left side of the screen; includes the menus for the selected pane.
<b>Content pane</b>	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.
<b>Toolbar</b>	Directly above the content pane; includes options for managing content in the content pane, such as <i>Create New</i> and <i>Delete</i> .

To switch between panes, either select the home button to return to the home page, or select the tile menu then select a new tile.



## Color themes

You can choose a color theme for the FortiManager GUI. For example, you can choose a color, such as blue or plum, or you can choose an image, such as summer or autumn. See [Global administration settings on page 877](#).

## 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* menu in the banner.

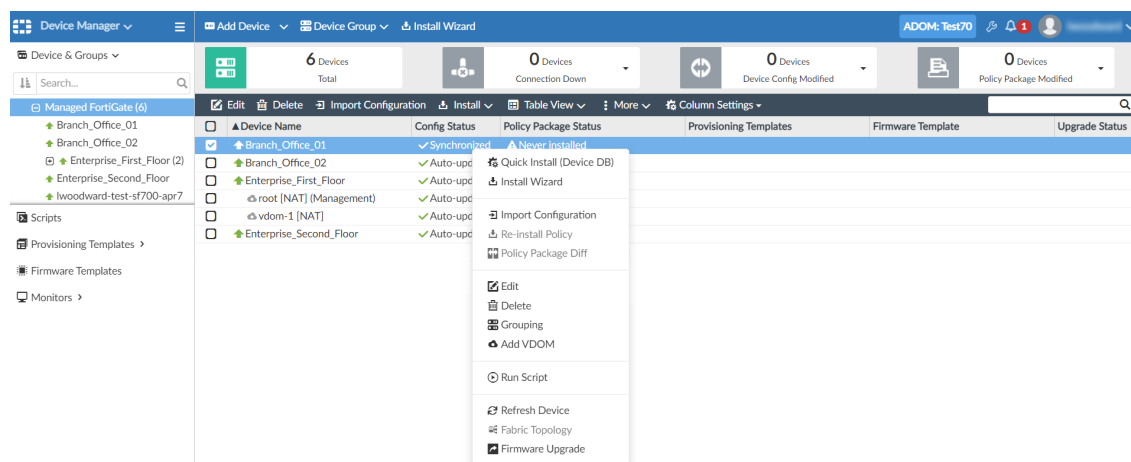


ADOM access is controlled by administrator accounts and the profile assigned to the administrator account. Depending on your account privileges, you might not have access to all ADOMs. See [Managing administrator accounts on page 809](#) for more information.

## Using the right-click menu

Options are sometimes available using the right-click menu. Right-click an item in the content pane, or within some of the tree menus, to display the menu that includes various options similar to those available in the toolbar.

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 so on.



## 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 811](#).

## Showing and hiding passwords

In some cases you can show and hide passwords by using the toggle icon. When you can view the password, the *Toggle show password* icon is displayed:

Password  

When you can hide the password, the *Toggle hide password* icon is displayed:

Password  

## FortiAnalyzer Features

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

When the features are enabled manually by using the *System Settings* module, logs are stored and FortiAnalyzer features are configured on the FortiManager.

When the features are enabled by adding a FortiAnalyzer to the FortiManager, logs are stored 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 85](#).

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

<b>FortiView</b>	Enables <i>FortiView</i> and additional <i>Monitors</i> , including monitoring network traffic, WiFi security, and system performance. See the <a href="#">FortiAnalyzer Administration Guide</a> .
<b>Log View</b>	View log messages from managed devices with logging enabled. You can view the traffic log, event log, or security log information. See the <a href="#">FortiAnalyzer Administration Guide</a> .
<b>Incidents &amp; Events</b>	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 <a href="#">FortiAnalyzer Administration Guide</a> .
<b>Reports</b>	Generate reports of data from logs. See the <a href="#">FortiAnalyzer Administration Guide</a> .

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

<b>Dashboard widgets</b>	The following widgets can be added to the dashboard: <i>Log Receive Monitor</i> , <i>Insert Rate vs Receive Rate</i> , <i>Log Insert Lag Time</i> , <i>Receive Rate vs Forwarding Rate</i> , and <i>Disk I/O</i> . The <i>License Information</i> widget will include a <i>Logging</i> section. See <a href="#">Dashboard on page 719</a> .
<b>Logging Topology</b>	View the logging topology. See <a href="#">Logging Topology on page 737</a> .
<b>Storage Info</b>	View and configure log storage policies. See the <a href="#">FortiAnalyzer Administration Guide</a> .

	This pane is only available when ADOMs are enabled.
<b>Device Log Settings</b>	Configure device log file size, log rolling, and scheduled uploads to a server. See <a href="#">Device logs on page 800</a> .
<b>File Management</b>	Configure the automatic deletion of device log files, quarantined files, reports, and content archive files after a set period of time. See <a href="#">File Management on page 804</a> .

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 when FortiAnalyzer features are enabled.

See [Add FortiAnalyzer or FortiAnalyzer BigData on page 85](#) for more information.

### To enable or disable the FortiAnalyzer features from the GUI:

1. Go to *System Settings > 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 744](#).
3. Configure network settings. See [Configuring network interfaces on page 739](#).



4. (Optional) Configure administrative domains. See [Managing ADOMs on page 758](#).
5. Configure administrator accounts. See [Managing administrator accounts on page 809](#).

## 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 805](#) in [System Settings on page 718](#).

# 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 7.2.3 Release Notes](#).

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

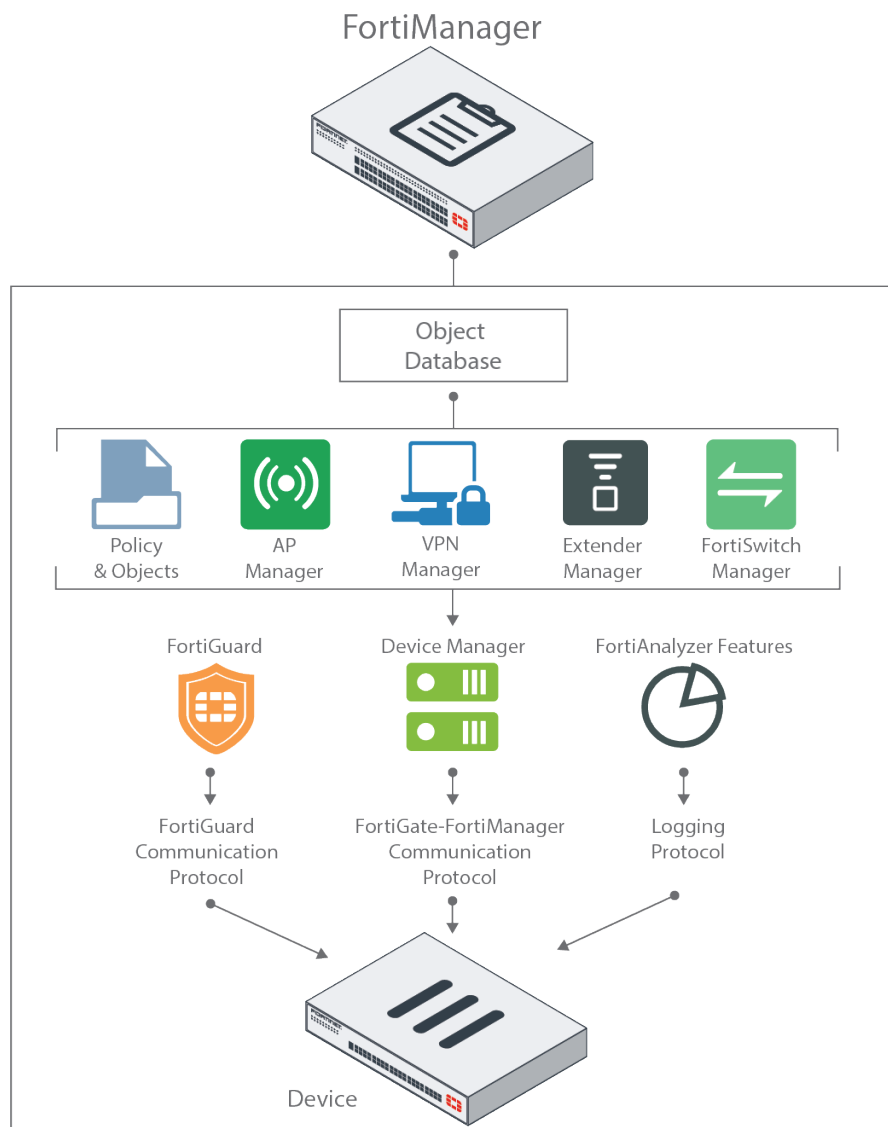
To reduce network delays and to minimize external Internet usage, a FortiManager installation can also act as an on-site FortiGuard Distribution Server (FDS) for your managed devices and FortiClient agents to download updates to their virus and attack signatures, and to use the built-in web filtering 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 33](#)
- [Configuration through Device Manager on page 35](#)
- [ADOMs and devices on page 36](#)
- [Operations on page 38](#)
- [Key features of the FortiManager system on page 46](#)

## 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 35](#).

## 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 627](#).

## 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 48](#).

## 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 35](#)
- [Indirect device database editing on page 35](#)

### 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.

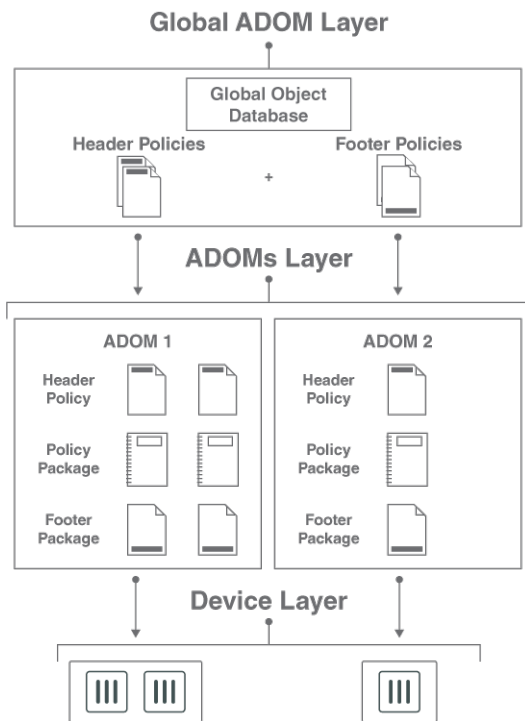
See also [Adding offline model devices on page 62](#).

## 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 37](#)
- [ADOM and policy layer on page 37](#)
- [Device Manager layer on page 38](#)

## 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

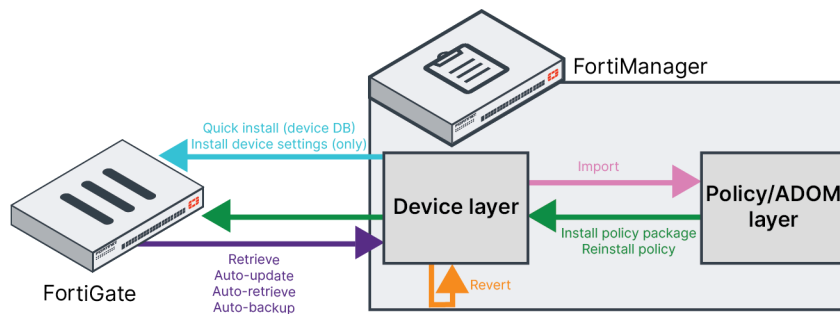
The ADOM layer is where FortiManager manages individual devices, VDOMs, or groups of devices. It is inside this layer where policy packages and folders are created, managed, and installed on managed devices. Multiple policy packages and folders can be created here. The ADOM layer contains one common 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 39](#)
- [Install device settings only on page 38](#)
- [Quick install \(device db\) on page 39](#)
- [Re-install policy on page 39](#)
- [Import configuration on page 39](#)
- [Retrieve configuration on page 40](#)
- [Auto-update and auto-retrieve on page 40](#)
- [Auto-backup on page 41](#)
- [Refresh on page 41](#)
- [Revert on page 41](#)
- [Sequence of operations for installation to managed devices on page 41](#)

## 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 122](#).

## 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 121](#).

## 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 315](#).

## Import configuration

The *Import Configuration* operation copies policies and policy-related objects from the device layer into the ADOM and policy layer, 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 117](#).

## 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 143](#).

## 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 754](#).

## Refresh

FortiManager queries FortiGate to update that FortiGate's current synchronization status. For more information, see [Refreshing a device on page 103](#).

## 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. Run the Install wizard and choose *Install Device settings (Only)*.
2. Import and then reinstall the policy package.  
By importing and reinstalling the policy package, you allow the device layer and the ADOM and policy layer to synchronize.

For more information, see [Viewing configuration revision history on page 143](#).

## 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 41](#)
- [Sequence for installing changes to managed devices on page 43](#)
- [Execution sequence for real devices on page 43](#)
- [Execution sequence for model devices on page 44](#)
- [Installation example on page 44](#)

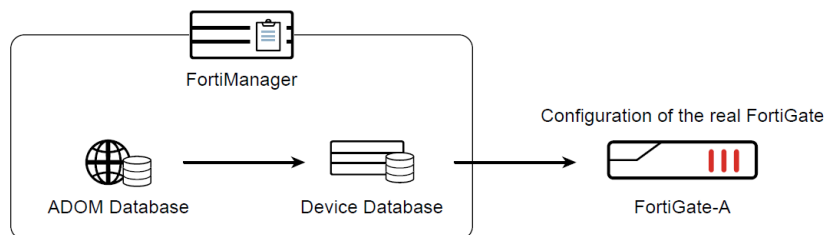
## FortiManager databases used during installation

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 43](#) and [Execution sequence for model devices on page 44](#) 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. Post-run 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. Once the pre-run CLI/Jinja template has been applied to the *Device Database* of a model device, it is automatically unassigned from that 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 always applied to the *Device Database* before any other Provisioning Template or Policy Packages.).
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. Post-run 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* 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 71](#). You can also display the security fabric topology (see [Displaying Security Fabric topology on page 103](#)) and view Security Fabric Ratings (see [Fabric View on page 556](#)).

### 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 750](#).

### 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 627](#).

### 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 168](#).

## 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 leak 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.

# 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 Manager* pane.

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

<b>Device &amp; Groups</b>	Add, configure, and view managed and logging devices. Use the toolbar to add devices, devices groups, and launch the install wizard. See <a href="#">Add devices on page 51</a> . The <i>Device &amp; Groups</i> tab also contains a quick status bar for a selected device group. See <a href="#">Using the quick status bar on page 96</a> .
<b>Scripts</b>	Create new or import scripts. Scripts is disabled by default. You can enable this advanced configuration option in <i>System Systems &gt; Admin &gt; Admin Settings</i> . Select <i>Show Script</i> to enable on this option in the <i>Device Manager</i> pane. See <a href="#">Scripts on page 168</a> .
<b>Provisioning Templates</b>	Configure provisioning templates. For information on system, Threat Weight, FortiClient, and certificate templates, see <a href="#">Provisioning Templates on page 200</a> .
<b>Firmware Templates</b>	Configure templates for upgrading firmware on FortiGates and all access devices, such as FortiAP, FortiSwitch, and FortiExtender. See <a href="#">Firmware templates on page 280</a> .
<b>Monitors</b>	Monitor traffic for all SD-WAN networks. See <a href="#">SD-WAN Monitor on page 286</a> . Monitor traffic for all VPN communities. See <a href="#">VPN Monitor on page 291</a> .
<b>VM Meter</b>	Monitor FortiMeter. See <a href="#">FortiMeter on page 295</a> .
<b>Chassis devices</b>	Add, configure, and monitor chassis devices. See <a href="#">FortiGate chassis devices on page 298</a> .

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 770](#).

---

## 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 750](#).



For information on adding devices to an ADOM by using the *Add Device* wizard, see [Adding online devices using Discover mode on page 51](#).

## 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 51](#).

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 85](#) or [Using device blueprints for model devices on page 78](#).

You can also add VDOMs to FortiGates. See [Add VDOM on page 92](#).

### Device Group

Click *Device Group* to create groups that you can use to organize managed devices. See [Device groups on page 94](#).

### 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 120](#).

The default view for the *Device Manager > Device & Groups* pane is *Table View*. See [Table view on page 95](#).

Under the banner in *Table View* is a quick status bar for all managed devices. See [Using the quick status bar on page 96](#).

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 133](#).
- 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:

<b>Edit</b>	In the content pane, select a device, and click <i>Edit</i> to edit device information. See <a href="#">Editing device information on page 100</a> .
<b>Delete</b>	In the content pane, select a device, and click <i>Delete</i> to remove the device from FortiManager management.
<b>Import Configuration</b>	In the content pane, select a device, and click <i>Import Configuration</i> to start the <i>Import Device</i> wizard. See <a href="#">Import Configuration wizard on page 117</a> .
<b>Install</b>	In the content pane, select a device, and from the <i>Install menu</i> menu, select one of the following options: <ul style="list-style-type: none"> <li>• <i>Install Wizard</i></li> <li>• <i>Quick Install (Device DB)</i></li> <li>• <i>Re-install Policy</i></li> </ul>
<b>Table View</b>	Click the <i>Table View</i> menu to choose the view format for managed devices. Choose from the following options: <ul style="list-style-type: none"> <li>• <a href="#">Table View</a></li> <li>• <a href="#">Map View</a></li> <li>• <a href="#">Ring View</a></li> <li>• <a href="#">Folder View</a></li> </ul>
<b>More</b>	In the content pane, select a device, and from the <i>More</i> menu, select one of the following options: <ul style="list-style-type: none"> <li>• <i>Refresh Device</i></li> <li>• <i>Configuration</i></li> <li>• <i>Add VDOM</i></li> <li>• <i>Firmware Upgrade</i></li> <li>• <i>Grouping</i></li> <li>• <i>Run Script</i></li> </ul>
<b>Column Settings</b>	From the <i>Column Settings</i> menu, select what columns to display for <i>Table View</i> .

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.

<b>Policy Package Diff</b>	View a diff on the policy package for the selected device.
<b>Edit Variable Mapping</b>	Edit the variable mappings for the selected device.

<b>Fabric Topology</b>	View the topology for Fabric devices.
<b>Install VM License</b>	Select to open the Install VM License wizard which includes options to install a BYOL VM license, or install a license from a Flex-VM connector. See <a href="#">Installing VM licenses on page 104</a> .

## 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 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 61](#).

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 85](#).

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.

**Add Device**

☐ **Discover Device**  
To add a device that is currently online.

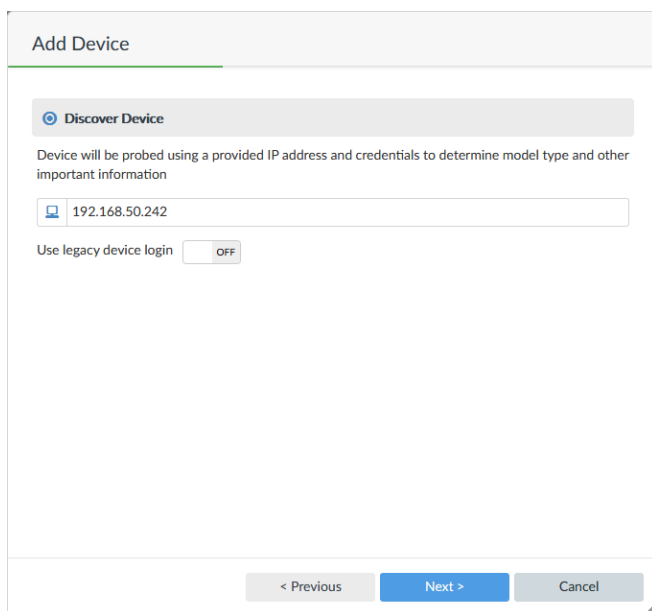
☐ **Add Model Device**  
To add a device that is not yet online. Configure a model device to complete authorization when the device is online.

☐ **Add Model HA Cluster**  
Adding an operating FortiGate HA cluster to Device Manager pane is similar to adding a standalone device. Specify the IP address of the primary device.

☐ **Import Model Devices from CSV File**  
Import multiple device definitions for devices that are not yet online.

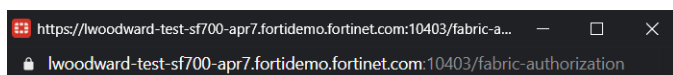
Cancel

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.



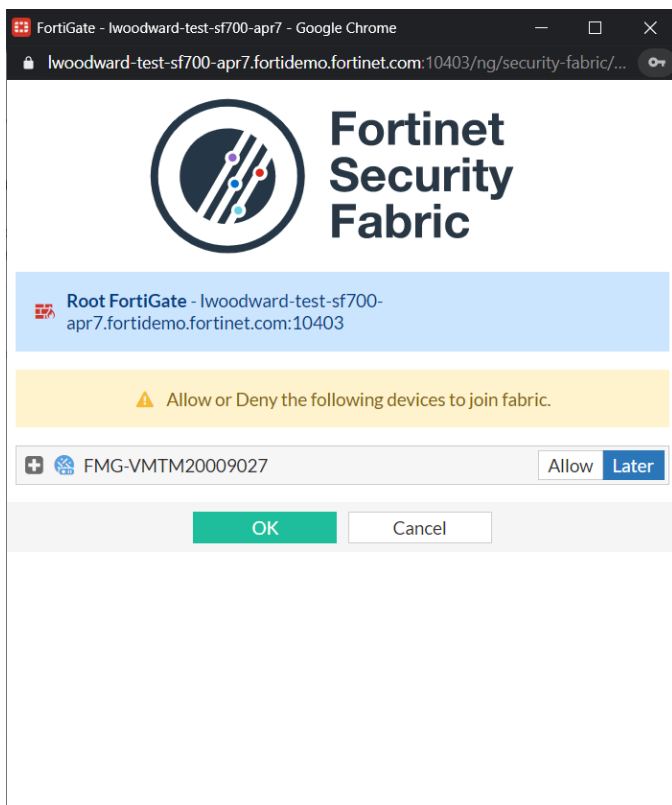
The 'Add Device' dialog box has a title bar 'Add Device'. Below it is a section titled 'Discover Device' with a sub-header 'Discover Device'. The text below says 'Device will be probed using a provided IP address and credentials to determine model type and other important information'. There is a text input field containing '192.168.50.242'. Below that is a checkbox labeled 'Use legacy device login' which is currently 'OFF'. At the bottom are three buttons: '< Previous', 'Next >', and 'Cancel'.

A login window for the device is displayed. If the login window is not displayed, see [How Security Fabric authorization works on page 59](#).

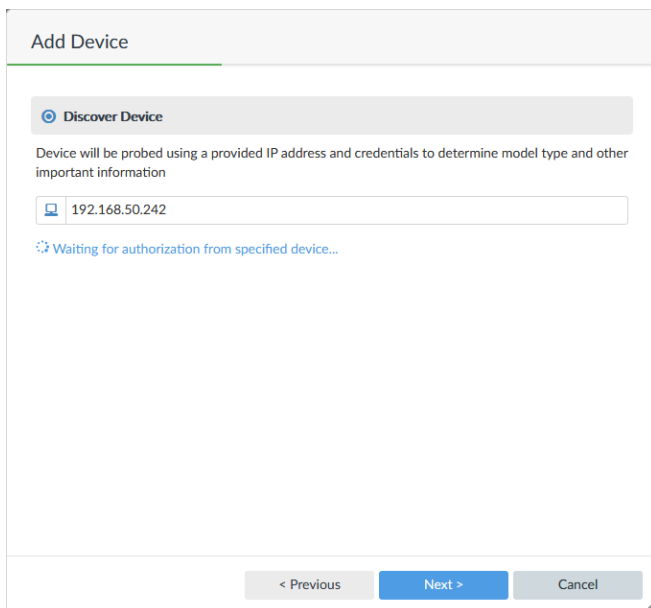


The image shows the Fortinet Security Fabric logo at the top. Below it is a login window titled 'woodward-test-sf700-apr7'. The window contains two input fields: 'Username' and 'Password', each with a small icon to its right. Below the fields is a red button labeled 'Login'.

- 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
<input type="checkbox"/> Add to Folder	/
<input type="checkbox"/> 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*:

<b>Name</b>	Type a unique name for the device. The device name cannot contain spaces or special characters.
<b>Description</b>	Type a description of the device (optional).
<b>System Template</b>	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 <i>Device Manager</i> . For more information, see <a href="#">Provisioning Templates on page 200</a> .
<b>Override Profile Value</b>	After selecting a system template, click to override values in the template.
<b>Add to Folder</b>	Select to add the device to any predefined folders.
<b>Add to Device Group</b>	Select to add the device to any predefined groups.
<b>Copy Device Dashboard</b>	Select a device to copy custom device dashboards from (optional). For more information about dashboards in the device database, see <a href="#">Device DB - Dashboard on page 137</a> .

More information about the device is checked.

Add Device

NameFGVM00TM21000676

IP Address192.168.50.242

Status

Discovering device

Creating device database

Initializing configuration database

Retrieving configuration

Retrieving support data

Updating group membership

Successfully add device

Check Device Status

Finish

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

Add Device

NameFGVM00TM21000676

IP Address192.168.50.242

Status

✔ Device is added successfully

✔ Discovering device

✔ Creating device database

✔ Initializing configuration database

✔ Retrieving configuration

✔ Retrieving support data

✔ Updating group membership

✔ Successfully add device

✔ Check Device Status

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

Import Now

Import 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*.

Import Device - FW148-1

Import Options

☒ Import each VDOM step by step

☐ Automatically import one VDOM at a time

☐ Automatically import all VDOMs

root  
T4

Next > Cancel

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

Import Device - FGVM00TM21000676

☐ **Import Policy Package**  
Import policy package used by the selected device.

☐ **Import AP Profiles or FortiSwitch Templates**  
Automatically import FortiAP profile and FortiSwitch template from selected device. For objects have the same name, configuration from device database will be used.

Next > Cancel

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.

### Import Device - FGVM00TM21000676 [ root ]

Create a new policy package for import.

Policy Package Name

Folder

Policy Selection  
☒ Import All (1)  
☐ Select Policies to Import

Object Selection  
☒ Import only policy dependent objects  
☐ Import all objects

When importing configuration from this device, all enabled interfaces require a mapping to an ADOM Level interface. Note, the same ADOM Level interface can map to different interfaces on the each device.

Device Interface	Mapping Type	Normalized Interface
No entry found.		

☒ Add mappings for all unused device interfaces

8. Set the following options, then click *Next*:
- In the *Policy Selection* section, select *Import All* or *Select Policies and Profile Groups to Import*.
  - In the *Object Selection* section, select *Import only policy dependent objects* or *Import all objects*.
  - Check the device interface mappings.
  - Select or clear the *Add mappings for all unused device interfaces* checkbox.
- The list of objects that will be updated is displayed.

### Import Device - FGVM00TM21000676 [ root ]

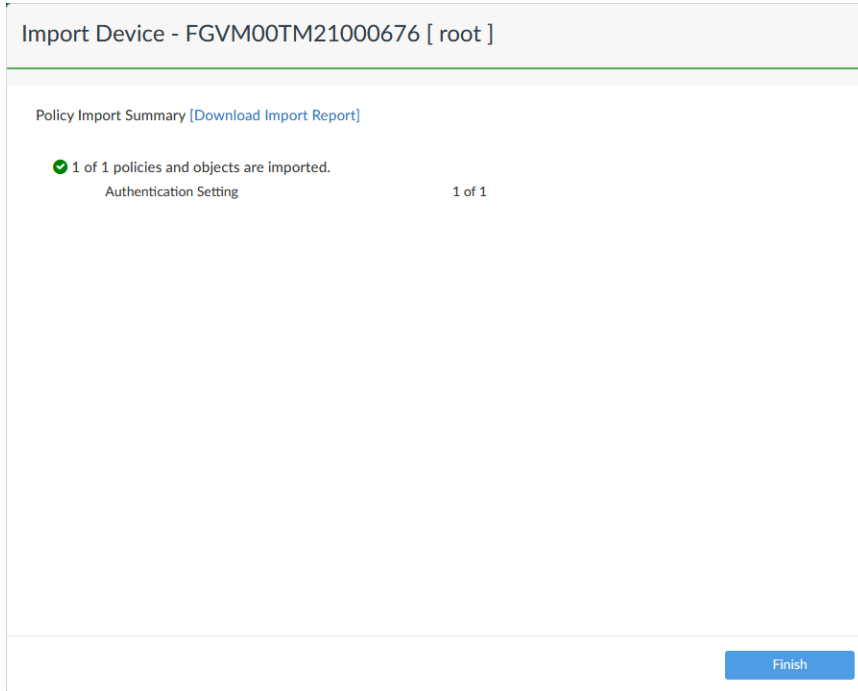
The following objects will be updated after import. Click 'Next' to start import process.

Duplicates (1)

Firewall Schedule Recurring (1)	default-darrp-optimize
---------------------------------	------------------------

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.

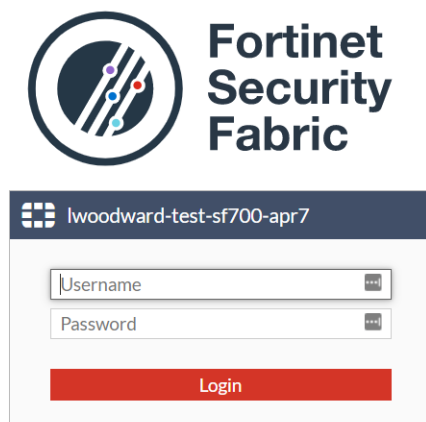
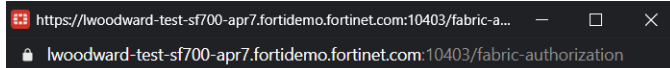
## How Security Fabric authorization works



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 OAUTH 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 61](#).

### 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 61](#)
- [NAT on page 61](#)
- [Non-default port on page 61](#)

#### 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 [How Security Fabric authorization works on page 59](#).

### 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*.

<b>IP Address</b>	Type the IP address of the management port for the device.
<b>User Name</b>	Type the username for the device.
<b>Password</b>	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 51](#).

## 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 36](#).

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.

### Add Device

☐ **Discover Device**  
To add a device that is currently online.

☐ **Add Model Device**  
To add a device that is not yet online. Configure a model device to complete authorization when the device is online.

☐ **Add Model HA Cluster**  
Adding an operating FortiGate HA cluster to Device Manager pane is similar to adding a standalone device. Specify the IP address of the primary device.

☐ **Import Model Devices from CSV File**  
Import multiple device definitions for devices that are not yet online.

Cancel

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

<b>Add Model Device</b>	Device will be added using the chosen model type and other explicitly entered information.
<b>Name</b>	Type a descriptive name for the device. This name is displayed in the <i>Device Name</i> column. Each device must have a unique name; otherwise, the wizard will fail.
<b>Link Device By</b>	<p>The method by which the model device will be linked to the real device. Model devices can be linked by <i>Serial Number</i> or <i>Pre-Shared Key</i>.</p> <p>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.</p> <p>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:</p> <pre>execute central-mgmt register-device &lt;fmg-serial-number&gt; &lt;preshared-key&gt;</pre>
<b>Serial Number or Pre-Shared Key</b>	<p>Type the device serial number or pre-shared key. This field is mandatory.</p> <p>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.</p> <p>See <a href="#">Editing device information on page 100</a>.</p>

<b>Use Device Blueprint</b>	<p>Toggle ON to enable the use of device blueprints.</p> <p>When a device blueprint is selected, the following configurations are imported from the blueprint and cannot be specified in the <i>Add Device</i> wizard: Enforce Firmware Version, Add to Device Group, Add to Folder, Pre-run CLI Templates, Assign Policy Package, Provisioning Template.</p> <p>See <a href="#">Using device blueprints for model devices on page 78</a>.</p>
<b>Device Model</b>	Select the device model from the list. If linking by serial number, the serial number must be entered before selecting a device model.
<b>Port Provisioning</b>	<p>Select the number of ports (1-10) to be provisioned for the FortiGate VM during initialization.</p> <p>This feature uses the <code>provision_instances_on_vm</code> script in <i>Device Manager &gt; Provisioning Templates &gt; CLI Templates</i> to configure the selected number of ports on the device. The script is performed while adding the offline model into the Device Manager.</p> <p>This option is only available for FortiGate-VM device models.</p>
<b>Split Switch Ports</b>	<p>Select to enable splitting virtual switch ports.</p> <p>This feature uses the <code>split_hardware_switch_ports_40_80_100</code> or <code>split_hardware_switch_ports_60_90</code> scripts in <i>Device Manager &gt; Provisioning Templates &gt; CLI Templates</i> to configure splitting virtual switch ports on the selected device. The script is performed while adding the offline model into the Device Manager.</p> <p>This option is only available on select hardware device models including FGT 40F/60F/80E/90E/100E/100F.</p>
<b>Enforce Firmware Version</b>	Select the check box to enforce the firmware version. The <i>Firmware Version</i> shows the firmware that will be upgraded or downgraded on the device.
<b>Add to Device Group</b>	Select the check box to choose a device group.
<b>Add to Folder</b>	Select the check box to choose a folder.
<b>Pre-run CLI Templates</b>	Select the check box to choose pre-run CLI templates. Pre-run CLI templates are run before provisioning templates.
<b>Assign Policy Package</b>	Select the check box and select a policy package from the drop-down to assign a particular policy package to the device.
<b>Provisioning Template</b>	Click to display the <i>Assign Provisioning Templates</i> dialog box. You can select one or more individual provisioning templates, or you can select a template group.
<b>Override Profile Value</b>	Click <i>Override Profile Value</i> to display the interface template and override settings. Overrides must be enabled in the interface template before you can override settings.
<b>Metadata Variables</b>	<p>Edit the metadata variables for the new model device.</p> <p>See <a href="#">ADOM-level metadata variables on page 437</a>.</p>
<b>Copy Device Dashboard</b>	<p>Select a device to copy custom device dashboards from (optional).</p> <p>For more information about dashboards in the device database, see <a href="#">Device DB - Dashboard on page 137</a>.</p>

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 143](#).

## 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 of adding an offline device by serial number on page 80](#).

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.



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 *HA Mode*, *Serial Number* for both the nodes, *Device Model* type, *Group Name* and *Password* for the HA cluster, *Node 1* and *Node 2* priority, *Monitor Interface* members, and *Heartbeat Interface* members, and click *Next*.



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*.

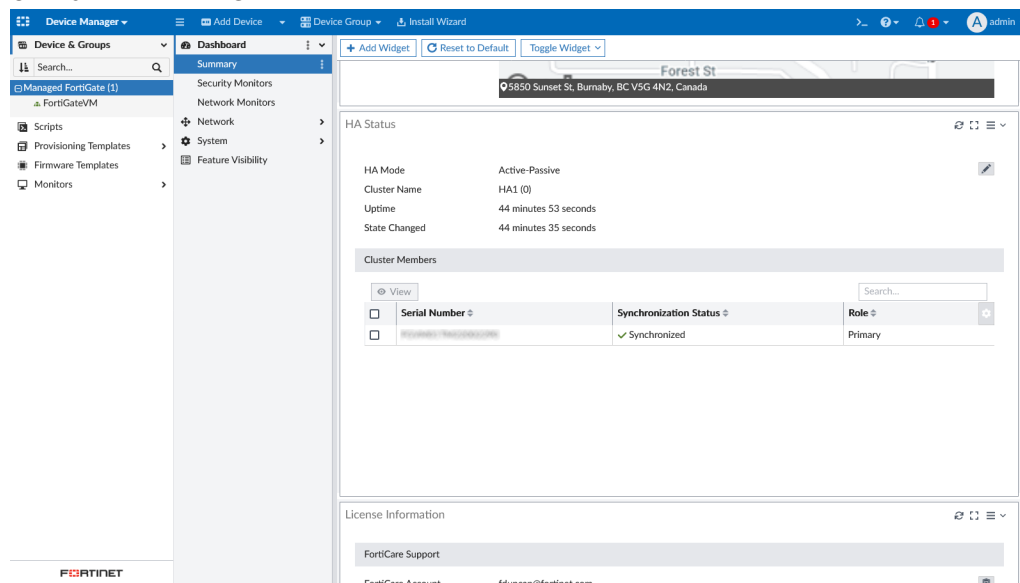
## Viewing the status of the HA cluster

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:

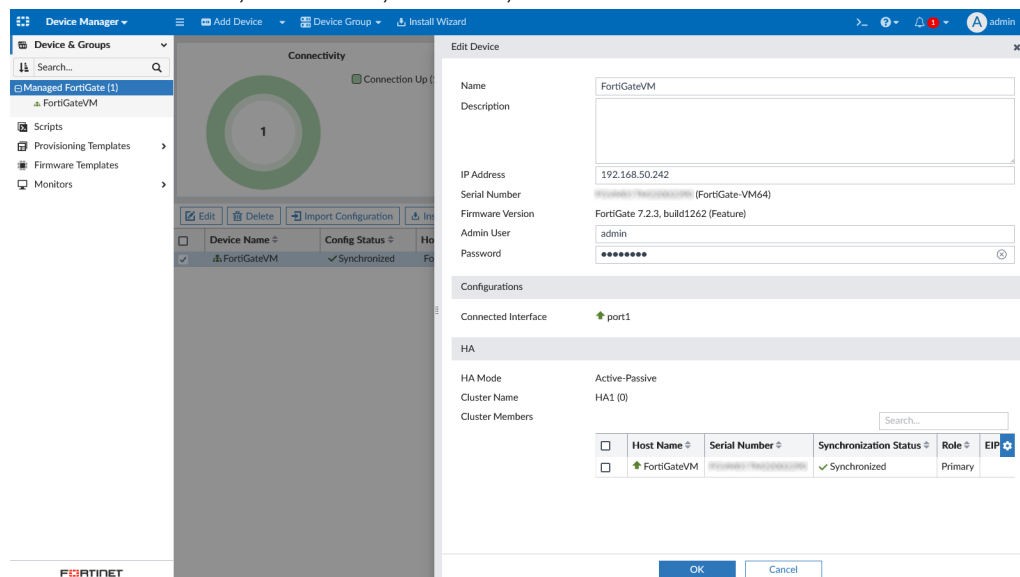
- *Synchronized*: The FortiGate HA cluster member is in sync.
- *Out of Sync*: The FortiGate HA cluster member is out of sync.

- **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*.



## 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 78](#).

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.

**Add Device**

☐ **Discover Device**  
To add a device that is currently online.

☐ **Add Model Device**  
To add a device that is not yet online. Configure a model device to complete authorization when the device is online.

☐ **Add Model HA Cluster**  
Adding an operating FortiGate HA cluster to Device Manager pane is similar to adding a standalone device. Specify the IP address of the primary device.

☒ **Import Model Devices from CSV File**  
Import multiple device definitions for devices that are not yet online.

Cancel

4. Click *Import Model Devices from CSV File*.
5. Configure your local CSV file for the devices that you want to import. CSV files must contain the following columns: `sn`, `device blueprint`, and `name`, with the respective data listed in the cells below. 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 437](#).

	A	B	C	D	E	F	G	H	I
1	sn	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									
17									
18									
19									
20									
21									
22									
23									
24									
25									

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 137](#).
8. Review the device list, and click *Next* to begin importing the devices. Click *Finish* when the import process is complete.

## 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 655](#) and [Uploading account entitlement files on page 657](#).

## 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 103](#).

### 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 51](#).

Alternatively, you can enable Central Management in the root FortiGate unit and specify the IP address of the FortiManager. See [Authorizing devices on page 71](#).

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
FG100D3G14B11667						
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	
FGP200A614800316						
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	

## 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.

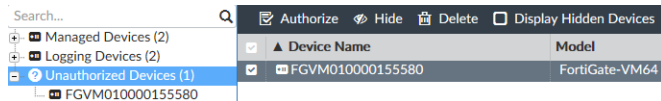
7. (Optional) In the *Assign New Device Name* list, type a different name for the device.
8. (Optional) In the *Assign Policy Package* list, select a policy package.
9. (Optional) In the *Assign Provisioning Template* list, select a profile.
10. (Optional) In the *Assign Dashboard Config* list, select a device to copy custom device dashboards from. For more information about dashboards in the device database, see [Device DB - Dashboard on page 137](#).
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 allow_register [enable | disable]
  set unreg_dev_opt add_allow_service
  set unreg_dev_opt add_no_service
end
```

<b>allow_register</b> <b>[enable   disable]</b>	When the <code>set allow_register</code> command is set to <code>enable</code> , you will not receive the <i>Authorize device</i> dialog box.
<b>unreg_dev_opt</b>	Set the action to take when an unauthorized device connects to FortiManager.
<b>add_allow_service</b>	Authorize unauthorized devices and allow service requests.
<b>add_no_service</b>	Authorize unauthorized devices but deny service requests.



When the `set allow_register` command is set to `disable`, you will not receive the *Authorize device* dialog box.

**Importing detected devices**

You can import detected devices to FortiManager.

**To import detected devices:**

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > Device & Groups*.
3. From the *Tools* menu, click *Global Display Options*.
4. In the *Detected Devices* area, select *Detected Devices*, and click *OK*.
5. In the tree menu, select a device. The device dashboard is displayed.
6. Click *Detected Devices*. The *Detected Devices* pane is displayed.
7. Click *Import*.

## 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:

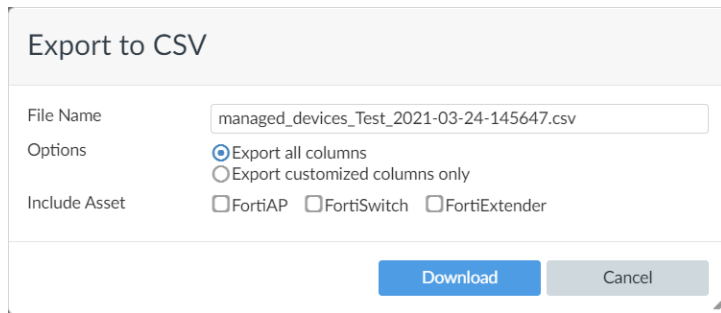
1. Enable the GUI options:
  - a. Go to *System Settings > Admin > Admin Settings*.
  - b. Expand the *Display Options on GUI* section, and select *Show Device List Import/Export buttons*.
  - c. Click *Apply*.
2. Go to *Device Manager > Device & Groups*.
3. In the toolbar, select *Table View* from the dropdown menu.
4. Select a device group, such as *Managed Devices*.
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.



The dialog box is titled "Export to CSV". It contains the following fields and options:

- File Name:** A text input field containing "managed\_devices\_Test\_2021-03-24-145647.csv".
- Options:** Two radio buttons. The first is "Export all columns" (selected). The second is "Export customized columns only".
- Include Asset:** Three checkboxes. "FortiAP" is selected. "FortiSwitch" and "FortiExtender" are unselected.
- Buttons:** "Download" (blue) and "Cancel" (grey).

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 systems 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 51](#).

### 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:

#### Warning

The following managed devices were detected having 'private-data-encryption' enabled. You are required to enter the encryption key as well on FortiManager side. Otherwise, configuration changes can not be installed successfully.

Status	▲ Device Name	IP Address	Platform	Private Data Encryption Key
	▲ FGTVM-196	10.3.121.196	FortiGate-VM64	<input type="password"/>

Verify

Close

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.

### Warning

The following managed devices were detected having 'private-data-encryption' enabled. You are required to enter the encryption key as well on FortiManager side. Otherwise, configuration changes can not be installed successfully.

Status	▲ Device Name	IP Address	Platform	Private Data Encryption Key
	FGTVM-196	10.3.121.196	FortiGate-VM64	..... 

Verify

Close



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

### Warning

The following managed devices were detected having 'private-data-encryption' enabled. You are required to enter the encryption key as well on FortiManager side. Otherwise, configuration changes can not be installed successfully.

1 out of 1 selected devices have been verified.

100%

Status	▲ Device Name	IP Address	Platform	Private Data Encryption Key
	FGTVM-196	10.3.121.196	FortiGate-VM64	..... 

Verify

Close

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

### Warning

The following managed devices were detected having 'private-data-encryption' enabled. You are required to enter the encryption key as well on FortiManager side. Otherwise, configuration changes can not be installed successfully.

0 out of 1 selected devices have been verified.

100%

Status	▲ Device Name	IP Address	Platform	Private Data Encryption Key
	FGTVM-195	10.3.121.195	FortiGate-VM64	..... 

Verify

Close

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.

### Install Wizard - Device Settings only

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

<input type="checkbox"/>	▲ Device Name	IP Address	Platform
<input type="checkbox"/>	▲ FGTVM-195	10.3.121.195	FortiGate-VM64

Mismatched private data encryption key detected.

< Back
Next >
Cancel

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



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 may need to manually retrieve device configuration settings again on FortiManager.

## 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 62](#).

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

As an example, 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 245](#).

### To create a new device blueprint:

1. Go to *Device Manager*, and select *Device Blueprint* from the *Add Device* dropdown menu.  
Previously configured blueprints are displayed in the table below and can be edited or deleted.
2. Click *Create New* to add a new blueprint.



### 3. Configure the following information for the blueprint:

The screenshot shows the 'Create New Device Blueprint' window. On the left, there's a sidebar with a '+ Create New' button and a 'Blueprint' tab. Below the sidebar, it says 'No record found'. The main panel has the title 'Create New Device Blueprint'. It contains several configuration options: 'Name' (text input), 'Device Model' (dropdown menu showing 'FortiGate-40F'), 'Enforce Firmware Version' (checkbox), 'Add to Device Group' (checkbox), 'Add to Folder' (checkbox), 'Pre-Run CLI Template' (checkbox), 'Assign Policy Package' (checkbox), and 'Provisioning Templates' (a button labeled 'Click here to assign'). At the bottom right, there are 'Ok' and 'Cancel' buttons.

<b>Name</b>	Enter a name for the blueprint.
<b>Device Model</b>	Select the device model type where the device blueprint can be applied.
<b>Enforce Firmware Version</b>	Select the checkbox to choose the firmware version that is enforced. By default, ADOM version 7.0 is enforced.
<b>Add to Device Group</b>	Select the checkbox to add one or more device groups. All devices assigned this device blueprint are added to the selected device group(s).
<b>Add to Folder</b>	Select the checkbox to add the devices to the specified folder in the Device Manager.
<b>Pre-Run CLI Template</b>	Select the checkbox to enable the use of a pre-run CLI template, and then select the template from the dropdown menu. See <a href="#">Adding CLI templates on page 272</a> .
<b>Assign Policy Package</b>	Select the checkbox to enable policy package assignment, and then select the policy package from the dropdown menu. See <a href="#">Managing policies on page 322</a> .
<b>Provisioning Template</b>	Select <i>Click here to assign</i> to choose provisioning templates. You can assign device blueprints system, IPsec, SD-WAN, static route, BGP, and Post-Run CLI templates, or alternatively select a template group. See <a href="#">Provisioning Templates on page 200</a> .

4. 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 51](#).

**To edit or delete a device blueprint:**

1. Go to *Device Manager*, and select *Device Blueprint* from the *Add Device* dropdown menu.
2. 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.

## Example of 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>}
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 of 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 of 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 screenshot shows the 'Edit Action' dialog box in the FortiManager GUI. The dialog is titled 'Edit Action' and contains the following fields and options:

- Action:** Config Interface (dropdown menu)
- Model:** FortiGate-200E (dropdown menu)
- Interface Name:** port1 (text input)
- Allow Override:** ☐ (checkbox)
- IP/Netmask:** 192.168.48.83/255.255.255.0 (text input)
- Allow Override:** ☒ (checkbox)
- Administrative Access:**
  - ☐ fabric
  - ☒ fgfm
  - ☐ ftm
  - ☒ http
  - ☒ https
  - ☒ ping
  - ☐ probe-response
  - ☐ radius-acct
  - ☐ snmp
  - ☐ ssh
  - ☐ telnet
  - ☒ Allow Override (checkbox)

At the bottom of the dialog are 'OK' and 'Cancel' buttons. In the background, a table shows the configuration for the FortiGate-200E model device, with columns for 'Model Match', 'Config Interface', and 'FortiGate-200E'.



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*.**

**Add Device**

☐ **Discover Device**  
To add a device that is currently online.

☐ **Add Model Device**  
To add a device that is not yet online. Configure a model device to complete authorization when the device is online.

☐ **Add Model HA Cluster**  
Adding an operating FortiGate HA cluster to Device Manager pane is similar to adding a standalone device. Specify the IP address of the primary device.

☐ **Import Model Devices from CSV File**  
Import multiple device definitions for devices that are not yet online.

Cancel

**4. Configure the settings as follows:**

<b>Name</b>	Enter a name for the model device.
<b>Link Device By</b>	Select <i>Serial Number</i> .
<b>Serial Number</b>	Add the serial number of the FortiGate device to be added.
<b>Device Model</b>	Select the device model from the drop-down list.
<b>Provisioning Template</b>	Click to display the <i>Assign Provisioning Templates</i> 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.

The screenshot shows the 'Edit Action' dialog box in the FortiManager interface. The dialog is titled 'Edit Action' and contains the following fields and options:

- Action: Config Interface
- Model: FortiGate-200E
- Interface Name: port1
- IP/Netmask: 192.168.48.183/255.255.255.0
- Administrative Access:
  - ☐ fabric
  - ☒ fgfm
  - ☐ ftm
  - ☒ http
  - ☒ https
  - ☒ ping
  - ☐ probe-response
  - ☐ radius-acct
  - ☐ snmp
  - ☐ ssh
  - ☒ telnet

At the bottom right of the dialog are 'OK' and 'Cancel' buttons. The background shows a partial view of the FortiManager interface with a 'Total' count and a list of devices.

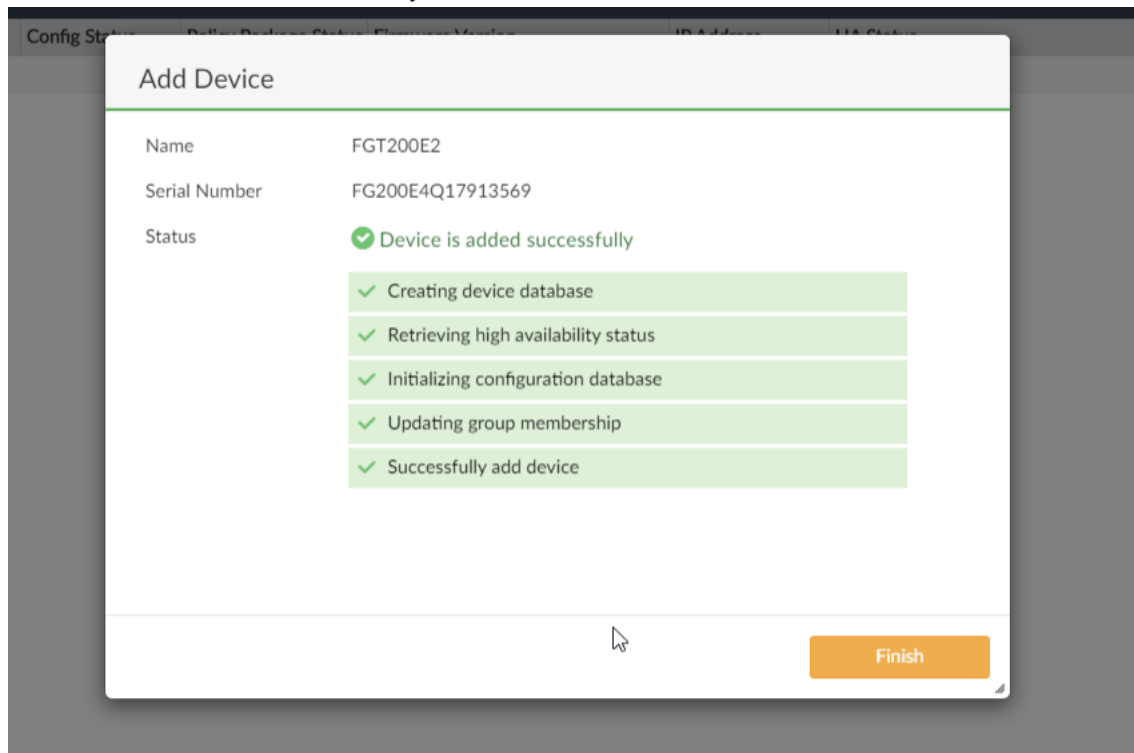
- c. Make the required changes and click *OK*.



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.

	1 Devices Total		0 Devices Connection Down		0 Devices Device Config Modified		0 Devices Policy Package Modified
<div>  Edit            Delete            Import Policy            Install            More            Column Settings           <input type="text"/> </div>							
<input type="checkbox"/>	▲ Device Name	Config Status	Policy Package Status	Firmware Version	IP Address	HA Status	SN
<input type="checkbox"/>	FGT200E2	✓ Synchronized	▲ Never installed	FortiGate 6.4.0,build1718 (Interim)	10.6.106.83	N/A	FG200E4Q17913569

## 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 member from the cluster.

---

For more information, see [the FortiGate CNF Administration Guide](#).

## 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 29](#). See also [Viewing policy rules on page 91](#) and [View logs related to a policy rule on page 321](#).



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 4500F devices are supported.

---



If FortiAnalyzer Features are enabled, you cannot add a FortiAnalyzer or FortiAnalyzer BigData to FortiManager. See [FortiAnalyzer Features on page 29](#).

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

---

### 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 207](#).

## 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 supports adding FortiAnalyzer BigData-VM and FortiAnalyzer BigData 4500F units.



FortiManager and FortiAnalyzer must be running 5.6 or later, and the 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 207](#).

## Add a new FortiAnalyzer or FortiAnalyzer BigData

### To add a FortiAnalyzer device:

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 on page 91](#).
6. Toggle *Use legacy device login* to ON.  
The *User Name* and *Password* boxes are displayed.

**Add FortiAnalyzer - Discover Device (1/3)**

**Add New FortiAnalyzer** | Add Existing FortiAnalyzer

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

Use legacy device login ☒

User Name

Password

Next > Cancel

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

Add FortiAnalyzer - Edit Device Details (2/3)

The following information has been discovered from the device:

IP Address	10.100.88.2
Host Name	Enterprise_FortiAnalyzer
SN	FAZVMSTM22003143
Model	FortiAnalyzer-VM64-KVM
Firmware Version	7.0.2, build1283
Administrator	fduncan

---

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

Name	<input type="text" value="Enterprise_FortiAnalyzer"/>
Description	<input type="text" value="Description"/>

< Previous
Next >
Cancel

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

<b>Name</b>	Type a unique name for the device. The device name cannot contain spaces or special characters (optional).
<b>Description</b>	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.

Add FortiAnalyzer - Validate Device (3/3)

Status: Verify managed/logging devices on both sides

50%

Search...

<input type="checkbox"/>	Status	Device Name	Platform
<input type="checkbox"/>	FortiAnalyzer Only	Branch_Office_02	FortiGate-VM64-KVM
<input type="checkbox"/>	FortiAnalyzer Only	Branch_Office_01	FortiGate-VM64-KVM

Click "Synchronize ADOM and devices" to proceed.

Synchronize ADOM and Devices
Cancel

The following table describes the different statuses:

Status	Description
<b>FMG Only</b>	The device was located in FortiManager, but not FortiAnalyzer. If you proceed with the wizard, the device will be added to FortiAnalyzer too.
<b>FAZ Only</b>	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.
<b>Sync</b>	The device was located in both FortiAnalyzer and FortiManager without any differences, and the wizard will synchronize the device between FortiManager and FortiAnalyzer.
<b>Mismatched</b>	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.

- Click *Finish* to close the wizard.

### Add FortiAnalyzer

✔ FortiAnalyzer Added Successfully

Finish

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

## Add an existing FortiAnalyzer

### To add an existing FortiAnalyzer device to a new ADOM:

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

Add FortiAnalyzer - Discover Device (1/3)

Add New FortiAnalyzer Add Existing FortiAnalyzer

Add an existing FortiAnalyzer to the current ADOM.

Select FortiAnalyzer FAZVM64

Next > Cancel

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

## 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 85](#).

**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.

## 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 150](#).

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 92](#)
- [Adding a multi VDOM on page 93](#)



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*.

<b>VDOM Name</b>	Type a name for the new virtual domain.
<b>Description</b>	Optionally, enter a description of the VDOM.
<b>Enable</b>	Select to enable the VDOM.
<b>Central SNAT</b>	Toggle <i>ON</i> to enable, and toggle <i>OFF</i> to disable.
<b>Operation Mode</b>	Select either <i>NAT</i> or <i>Transparent</i> .
<b>NGFW Mode</b>	Select either <i>Profile-based</i> or <i>Policy-based</i> .
<b>Interface Members</b>	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 Devices* table on the *Device Manager > Device & Groups* tab, 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 Devices* 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*.
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	Edit the selected device group. You cannot edit default device groups.
Delete	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 96](#)
- [Viewing managed devices on page 96](#)
- [Viewing configuration status on page 97](#)
- [Viewing policy package status on page 99](#)
- [Editing device information](#)
- [Setting values for required meta fields on page 101](#)
- [Customizing columns on page 102](#)
- [Displaying Security Fabric topology on page 103](#)
- [Refreshing a device](#)
- [Using device group tree menus on page 104](#)
- [Installing VM licenses on page 104](#)

## 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:

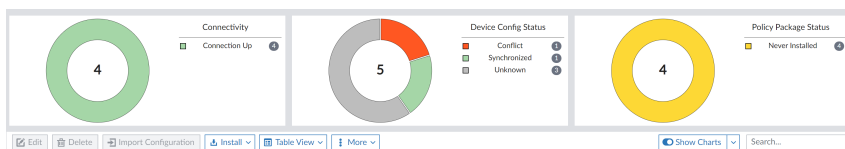
- *Connectivity*
- *Device Config Status*
- *Policy Package Status*
- *FortiAP Status*
- *FortiSwitch Status*
- *Firmware Status*
- *FortiGuard License Status*

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 102](#).

### 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.

<b>Device Name</b>	The name of the device and its connectivity status.
<b>Config Status</b>	Displays the status of the configuration for the managed device. For details, see <a href="#">Viewing configuration status on page 97</a> .

<b>Policy Package Status</b>	Displays the status of the policy package for the managed device. For details, see <a href="#">Viewing policy package status on page 99</a> . Click on the policy package name to go to view and manage the package. See <a href="#">Managing policy packages on page 310</a> .
<b>Provisioning Templates</b>	Displays one of the following: <ul style="list-style-type: none"> <li>The name of each assigned provisioning template.</li> <li>The name of the assigned template group.</li> </ul> Hover the mouse over the assigned template or group to display and access an edit option.
<b>Firmware Template</b>	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.
<b>Upgrade Status</b>	Displays whether a firmware upgrade is available for the managed device.
<b>Firmware Version</b>	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 <i>IR</i> , <i>Title</i> , <i>Severity</i> , and <i>CVE</i> for the vulnerability.
<b>Host Name</b>	The host name for the device (available for managed devices).
<b>IP Address</b>	The IP address of the device.
<b>Platform</b>	The platform of the device (available for managed devices).
<b>Description</b>	Description of the device.
<b>HA Status</b>	The HA status of the device.
<b>FortiGuard License</b>	Status of the FortiGuard license for the device.
<b>Management Mode</b>	Management mode of the device.
<b>SN</b>	The serial number of the device.
<b>Controller Counter</b>	The number of each device type controlled by this device, such as FortiAPs and FortiSwitches.
<b>Company/Organization</b>	The company or organization information.
<b>Contact Email</b>	Displays the email of a contact for the managed device.
<b>Contact Phone Number</b>	Displays the phone number of a contact for the managed device.
<b>Address</b>	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 96](#).

**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
<b>Synchronized</b>	Green check ✓	Configurations are synchronized between FortiManager and the managed device.
<b>Modified</b>	Yellow triangle ⚠	Configurations are modified on FortiManager and not synchronized between FortiManager and the managed device.
<b>Auto-update</b>	Green check ✓	Configurations modified on the managed device are auto synced to FortiManager.
<b>Modified (recent auto-updated)</b>	Yellow triangle ⚠	Configurations are modified on FortiManager and configurations modified on the managed device are auto synced to FortiManager.
<b>Out of Sync</b>	Red X ✖	Configurations are modified on the managed device and not synced to FortiManager.
<b>Conflict</b>	Red X ✖	When one of the following happens: <ul style="list-style-type: none"> <li>• Install failed</li> <li>• Configurations are modified on both FortiManager and the managed device, and not auto synced to FortiManager.</li> </ul>
<b>Unknown</b>	Gray question mark ?	When one of the following happens: <ul style="list-style-type: none"> <li>• Connection goes down</li> <li>• No revision is generated, like added model device</li> </ul>

**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 142](#).
  - 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 117](#).
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 122](#). 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 96](#).

### 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
<b>Imported</b>	Green check ✓	Policies and objects are imported into FortiManager.
<b>Modified</b>	Yellow triangle ⚠	Policies or objects are modified on FortiManager.
<b>Synchronized</b>	Green check ✓	Policies and objects are synchronized between FortiManager and the managed device.
<b>Out of Sync</b>	Red X ✖	Policies or objects are modified on the managed device.
<b>Unknown with policy package name</b>	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 <i>Unknown</i> .

Policy Package Status	Icon	Description
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*.

<b>Name</b>	Change the name of the device.
<b>Description</b>	Type a description of the device.
<b>IP Address</b>	Change the IP address.

<b>Pre-Shared Key</b>	Enter the model device's pre-shared key. Select <i>Show Pre-shared Key</i> to see the key. This option is only available when editing a model device that was added with a pre-shared key.
<b>Automatically link to real device</b>	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.
<b>Serial Number</b>	Displays the serial number of the device. For model devices added with a pre-shared key, this will show the device model.
<b>Firmware Version</b>	Displays the firmware version of the device.
<b>Admin User</b>	Change the administrator user name for the device.
<b>Password</b>	Change the administrator user password for the device.
<b>Connected Interface</b>	Displays the name of the connected interface, if the connection is up.
<b>HA Mode</b>	Displays whether the FortiGate unit is operating in stand-alone or high availability mode.
<b>Geographic Coordinate</b>	Displays the latitude and longitude of the device. Click <i>Show Map</i> to view and edit the device location.
<b>Meta Fields</b>	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 <a href="#">Setting values for required meta fields on page 101</a> .
<b>Company/Organization</b>	Optionally, enter the company or organization information.
<b>Contact Email</b>	Optionally, enter the contact email.
<b>Contact Phone Number</b>	Optionally, enter the contact phone number.
<b>Address</b>	Optionally, enter the address where the device is located.

## Setting values for required meta fields

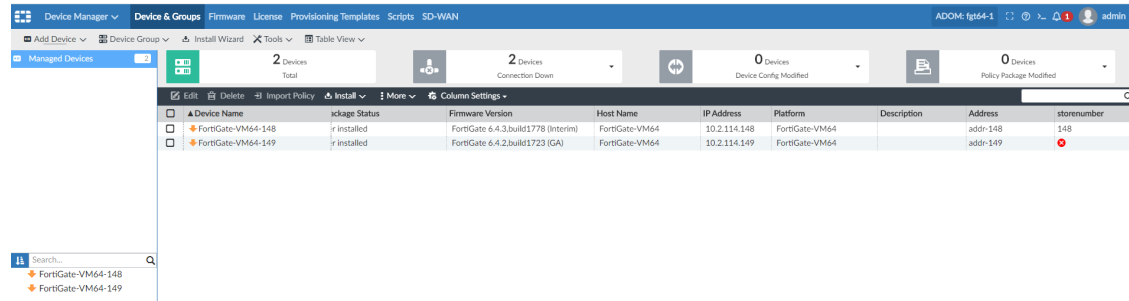
When a required meta field is defined for a device object, a column automatically displays on the *Device Manager* pane. The column displays the value for each device. When the required meta field lacks a value, an exclamation mark displays, indicating that you must set the value.

See also [Meta Fields on page 798](#).

### To set values for required meta fields:

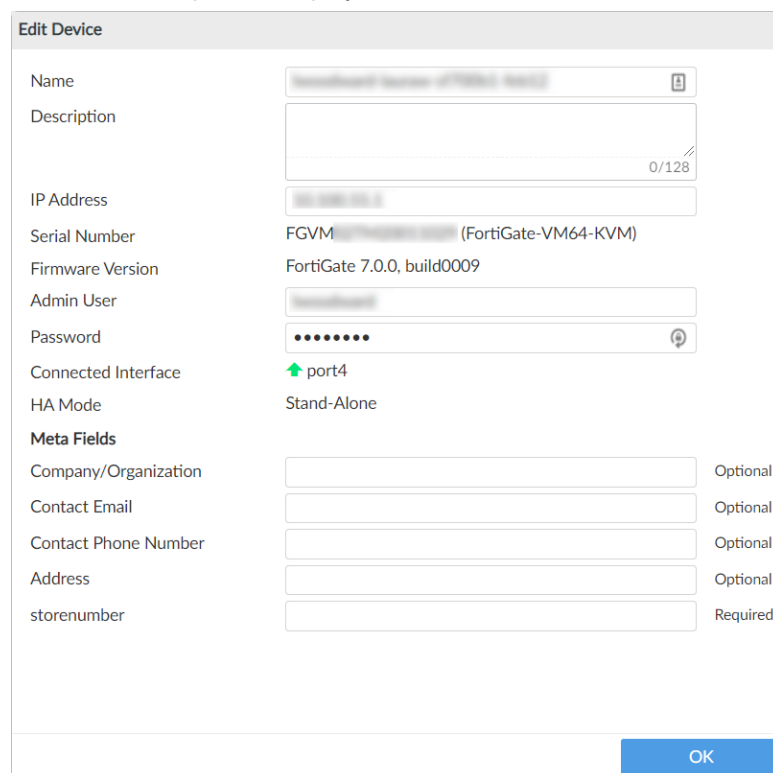
1. Go to *Device Manager > Device & Groups*.
2. In the toolbar, select *Table View* from the dropdown menu.
3. View the columns.  
A column displays for required meta fields.

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.



Device Name	Package Status	Firmware Version	Host Name	IP Address	Platform	Description	Address	storenumber
FortiGate-VM64-148	Installed	FortiGate 6.4.3.build1778 (Interim)	FortiGate-VM64	10.2.114.148	FortiGate-VM64		addr-148	148
FortiGate-VM64-149	Installed	FortiGate 6.4.2.build1723 (GA)	FortiGate-VM64	10.2.114.149	FortiGate-VM64		addr-149	

- Right-click the device that lacks a value, and select *Edit*. The *Edit Device* pane is displayed.



**Edit Device**

Name: [Text Field]

Description: [Text Field]

IP Address: [Text Field]

Serial Number: FGVM [Text Field] (FortiGate-VM64-KVM)

Firmware Version: FortiGate 7.0.0, build0009

Admin User: [Text Field]

Password: [Text Field]

Connected Interface: port4

HA Mode: Stand-Alone

**Meta Fields**

Company/Organization: [Text Field] Optional

Contact Email: [Text Field] Optional

Contact Phone Number: [Text Field] Optional

Address: [Text Field] Optional

storenumber: [Text Field] Required

OK

- 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 *Column Settings*, and select the columns you want to display.

**Displaying Security Fabric topology**

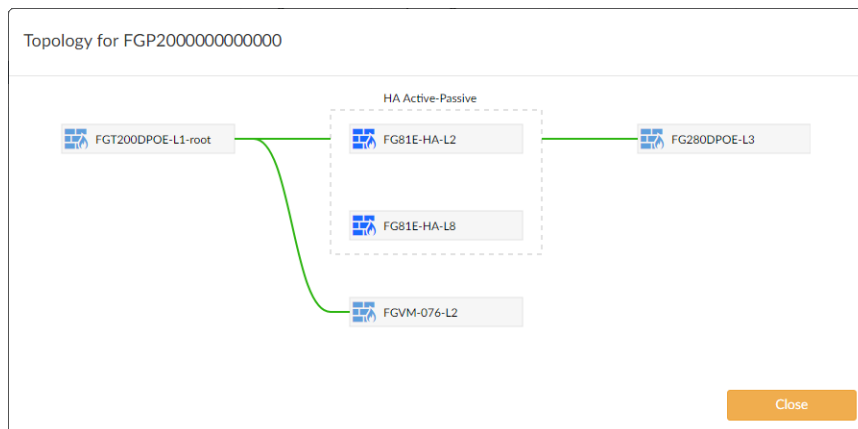
For Security Fabric devices, you can display the Security Fabric topology.

**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 Devices*
- *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 94](#).

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	<ul style="list-style-type: none"> <li>• Quick Install (Device DB)</li> <li>• Import Policy</li> <li>• Re-install Policy</li> <li>• Policy Package Diff</li> <li>• Edit</li> <li>• Delete</li> <li>• Grouping</li> <li>• Add VDOM</li> <li>• Run Script</li> <li>• Firmware Upgrade</li> </ul>
Logging Devices	<ul style="list-style-type: none"> <li>• Edit</li> <li>• Delete</li> </ul>
Unauthorized Devices	<ul style="list-style-type: none"> <li>• Authorize</li> <li>• Hide</li> <li>• Delete</li> </ul>

### 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

You can install VM licenses to managed FortiGate devices using the FortiManager Device Manager. This enables management and replacement of FortiGate license files without having to directly access the FortiGate-VM instance.

The device manager supports VM license installation with two options:

- License File (BYOL VM License)
- Flex-VM Connector

**To install a BYOL VM license in the Device Manager:**

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.

The screenshot shows the 'Install VM License' dialog box. It has a title bar 'Install VM License'. Below the title bar, there are two tabs: 'License File' (which is selected and highlighted in blue) and 'Flex-VM Connector'. Under the 'License File' tab, there is a section labeled 'From' with the text 'Upload License File' below it. To the right of this text is a large gray rectangular area with the text 'Add files by drag & drop here or [Add Files](#)'. Below this, there is a section labeled 'Preview' with a text box containing the text 'No License file Selected'. At the bottom right of the dialog box, there are two buttons: 'OK' (in blue) and 'Cancel' (in gray).

5. Select *License File*, and drag-and-drop your license file into the *Upload License File* field.
6. You can preview the license file selected, and click *OK*.

**To install a license using the Flex-VM connector in Device Manager:**

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.

## Install VM License

From	License File <b>Flex-VM Connector</b>
Flex-VM Connector	TEST ▼
Flex-VM Configuration	Click to select ▼

OK

Cancel



5. Select *Flex-VM Connector*, and select the previously configured Flex-VM connector in the dropdown menu.
6. Select a *Flex-VM Configuration*.  
Available configurations are pulled automatically from FlexVM using the selected connector.
7. Click OK.



For more information on creating Flex-VM connectors, see [Creating Flex-VM connectors on page 624](#).

## Ring view



To prevent timeout, ensure *Idle Timeout* is greater than the widget's *Refresh Interval*. See [Idle timeout on page 881](#) and [Settings icon on page 109](#).

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:

<b>Playing and Paused</b>	Click to start and pause the automatic rotation of the circle chart.
<b>Zoom in and out</b>	Use the <i>Zoom in</i> and <i>Zoom out</i> tools to enlarge and shrink areas of the circle chart. When zoomed in, use the scroll bar to move across the circle chart.
<b>Rotate Options</b>	Specify whether the chart automatically displays information about <i>Next Problematic Device</i> or <i>One by One</i> .
<b>Search Devices</b>	Select a device and display its information.
<b>Settings icon</b>	Change the settings of the widget. Widgets have settings applicable to that widget, such as how many of the top items to display, <i>Time Period</i> , <i>Refresh Interval</i> , and <i>Chart Type</i> .
<b>Remove widget icon</b>	Delete the widget from a predefined or custom dashboard.

The *Ring View* dashboard includes the following information:

<b>Overall Device Status</b>	<p>A summary of the status of all devices. The following colors are used to communicate status:</p> <ul style="list-style-type: none"> <li>Red indicates action is required now.</li> <li>Orange indicates action is required soon.</li> <li>Blue indicates no action is required.</li> </ul>
------------------------------	---

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.

<b>Require Action</b>	The number of devices that require configuration changes. The number is displayed in a red box.
<b>Will Soon Require Action</b>	The number of devices that will require configuration changes in the near future. The number is displayed in an orange box.
<b>Total Number of Devices</b>	The total number of devices displayed on the dashboard. The number is displayed in a blue box.
<b>Connectivity</b>	Displays the connectivity status for the selected device. Click the <i>Connectivity</i> link to display the selected device on the <i>Device Manager &gt; Device &amp; Groups</i> pane.
<b>Support Contracts</b>	Displays the expiration date of the support contracts for the selected device. Click the <i>Support Contracts</i> link to display the selected device on the <i>Device Manager &gt; License</i> pane.
<b>Licenses</b>	Displays the expiration date of the licenses for the selected device. Click the <i>Licenses</i> link to display the selected device on the <i>Device Manager &gt; License</i> pane.
<b>Configuration Status</b>	Displays the configuration status for the selected device. Click the <i>Configuration Status</i> link to display the selected device on the <i>Device Manager &gt; Device &amp; Groups</i> pane.
<b>Policy Package Status</b>	Displays the policy package status for the selected device. Click the <i>Policy Package Status</i> link to display the selected device on the <i>Device Manager &gt; Device &amp; Groups</i> pane.

## Using a Monitor dashboard

FortiView Monitor dashboards contain widgets that provide network and security information. Use the controls in the dashboard toolbar to work with a dashboard.

<b>Edit Layout</b>	Add, remove, resize, or move widgets on a predefined dashboard.
<b>Devices</b>	Select the devices to include in the widget data.
<b>Time Period</b>	Select a time period from the dropdown menu, or set a custom time period.
<b>Dark Mode</b>	Enable/disable dark mode. Dark mode shows a black background for the widgets in the dashboard.
<b>Refresh</b>	Refresh the data in the widgets.

<b>Hide Side-menu or Show Side-menu</b>	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.

<b>Settings icon</b>	Change the settings of the widget.
----------------------	------------------------------------

## Customizing a Monitor dashboard

You can add any widget to a custom or predefined dashboard. You can also move, resize, or delete widgets. You cannot rename or delete a predefined dashboard. To reset a predefined dashboard to its default settings, click *Dashboard settings icon* > *Reset*. The dashboard settings icon is visible when you mouse-over the dashboard in the tree menu.

### To create a dashboard:

1. In *FortiView* > *Monitor*, click the plus (+) at the bottom of the tree menu.
2. 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.
3. Click *OK*. The new dashboard appears in the tree menu.
4. 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.

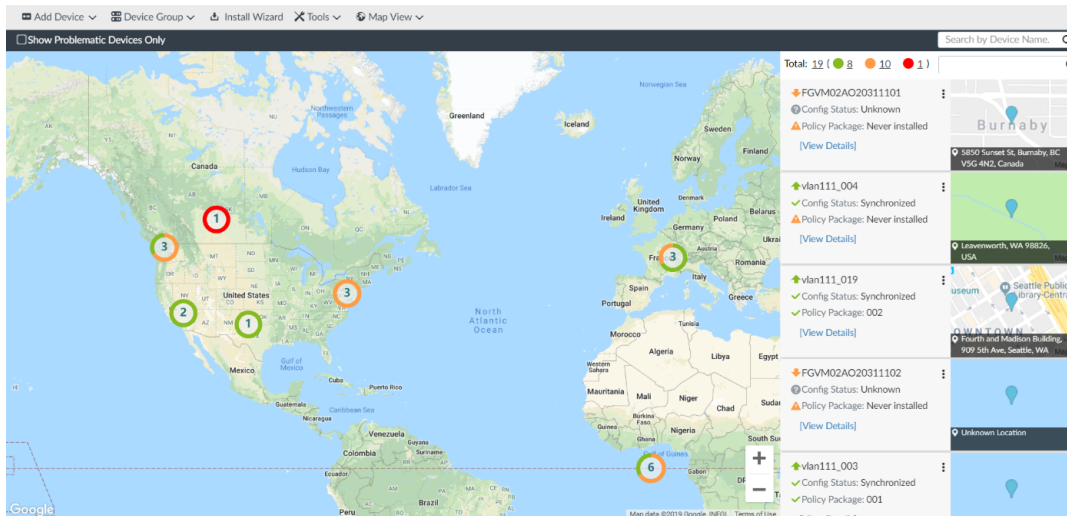
## Map view

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.

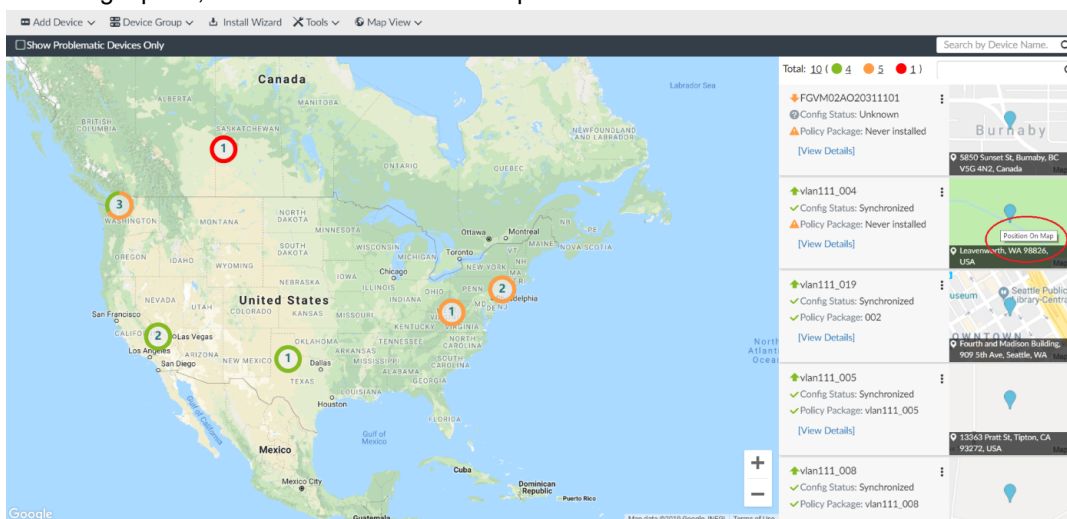


## Positioning devices on the map

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:

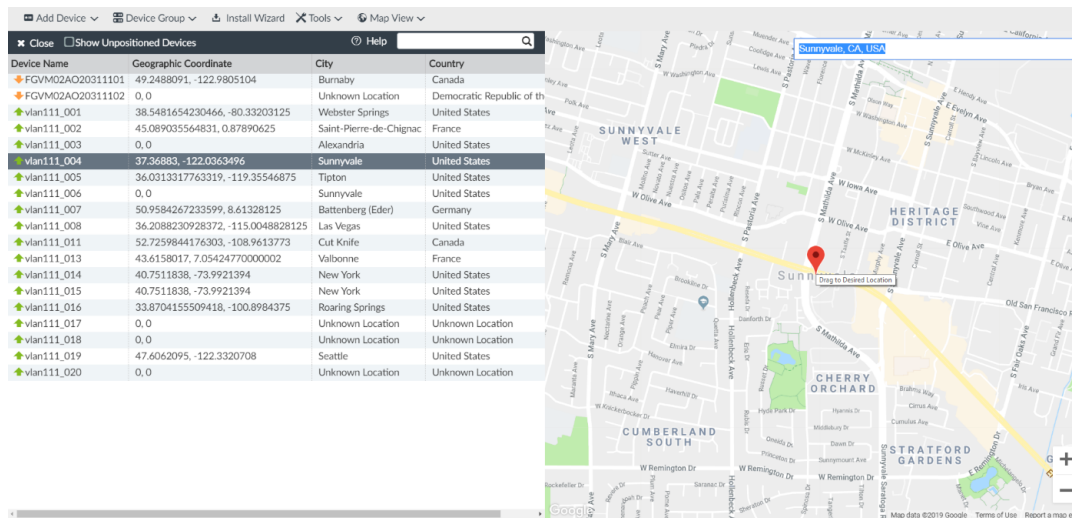
1. Go to *Device Manager > Device & Groups*.
2. In the toolbar, select *Map View* from the dropdown menu.
3. On the right pane, click a device on a small map.



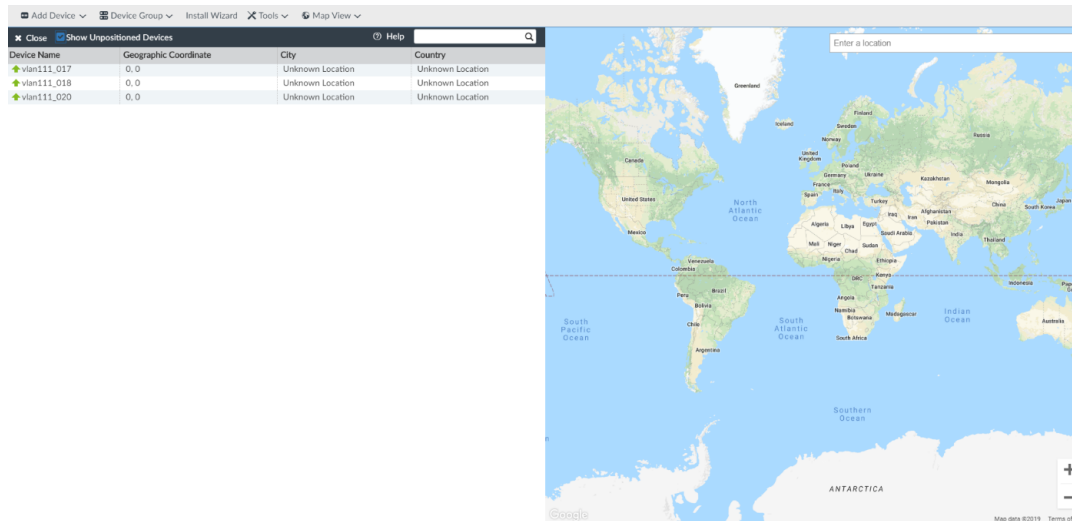
The small map opens and displays an *Enter a location* box for the selected device.

4. In the *Enter a location* box, type the city name, and press *Enter*.  
The device is positioned in the city on the map.





- On the map, drag the device to the desired location in the city.
- Select the **Show Unpositioned Devices** to display only devices with an unknown location and position them.



- Click **Close**.

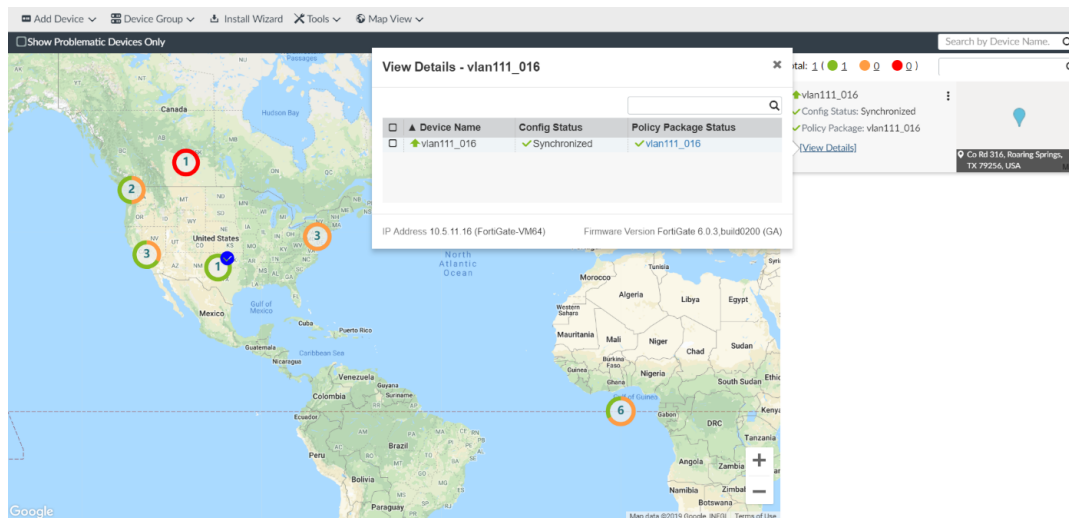
## Viewing device details

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.

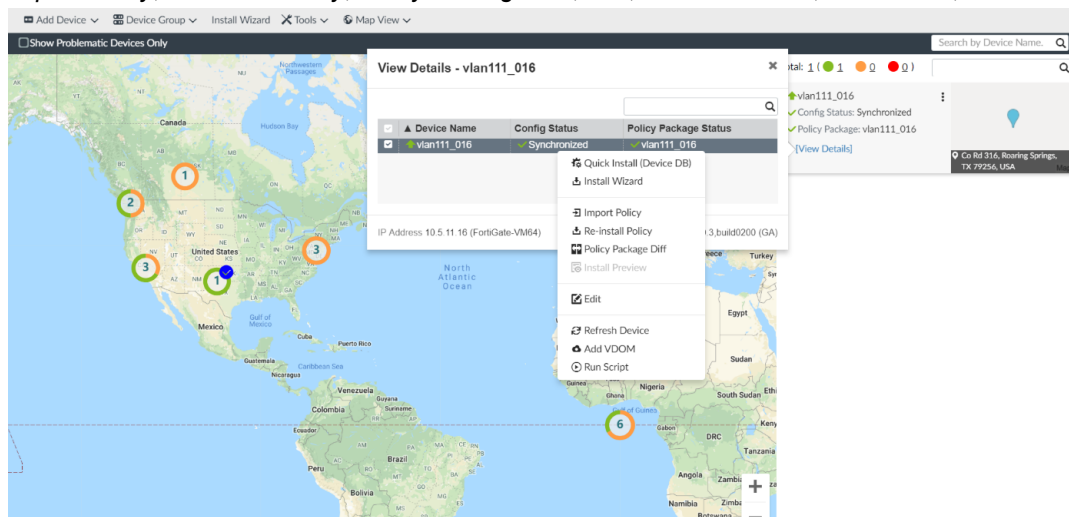
### To view device details:

- Go to **Device Manager > Device & Groups**.
- 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*.

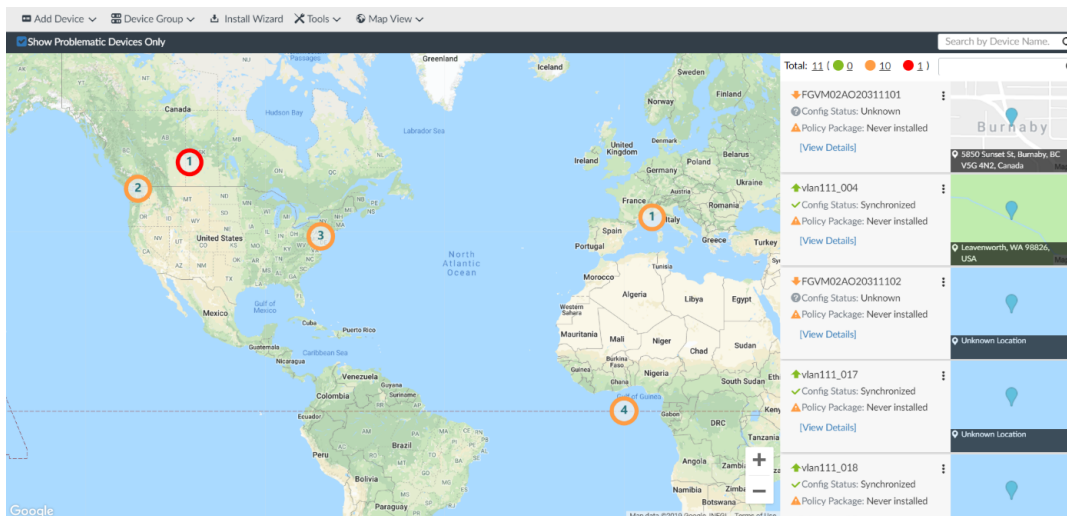


## Viewing problematic devices

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 280](#).



*Folder View* is not available when the ADOM device mode is set to *Advanced*. See [ADOM device modes on page 754](#).

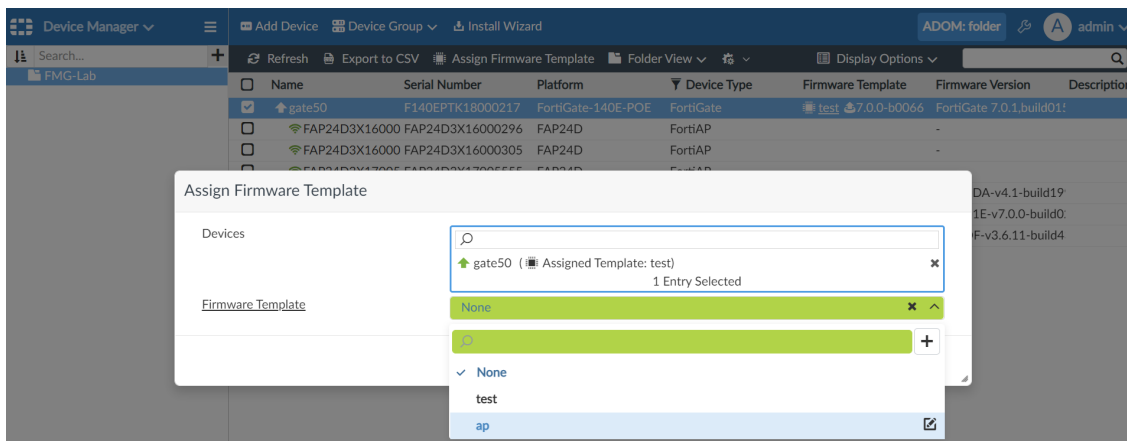
### To access Folder View:

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.

Device Manager						
Unassigned Devices (5)						
Name	Serial Number	Platform	Device Type	Firmware Template	Firmware Version	Description
Branch_Office_01	FGVM02TM21010587	FortiGate-VM64-KVM	FortiGate		FortiGate 7.0.1.build0157 (t	
S108DVCHTPDQH94	S108DVCHTPDQH946	FortiSwitch-108D-VM	FortiSwitch		S108DV-v7.0.0-build4062.2	
Branch_Office_02	FGVM02TM21010568	FortiGate-VM64-KVM	FortiGate		FortiGate 7.0.1.build0157 (t	
S108DVWNBPDQH9	S108DVWNBPDQH946	FortiSwitch-108D-VM	FortiSwitch		S108DV-v7.0.0-build4062.2	
Enterprise_First_Floor	FGVM02TM21012400	FortiGate-VM64-KVM	FortiGate		FortiGate 7.0.1.build0157 (t	
Enterprise_Second_Floor	FGVM02TM21010824	FortiGate-VM64-KVM	FortiGate		FortiGate 7.0.1.build0157 (t	
S108DVWA9XDKH9	S108DVWA9XDKH946	FortiSwitch-108D-VM	FortiSwitch		S108DV-v7.0.0-build4062.2	
FGT-Core	FGVM02TM21012652	FortiGate-VM64-KVM	FortiGate		FortiGate 7.0.1.build0157 (t	
FAP-Hallway	PS221E3X16000050	PS221E	FortiAP		-	
FAP-Cafeteria	PS321C3X16000050	PS321C	FortiAP		-	
FAP-Lobby	PU421E3X16000060	PU421E	FortiAP		-	

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.

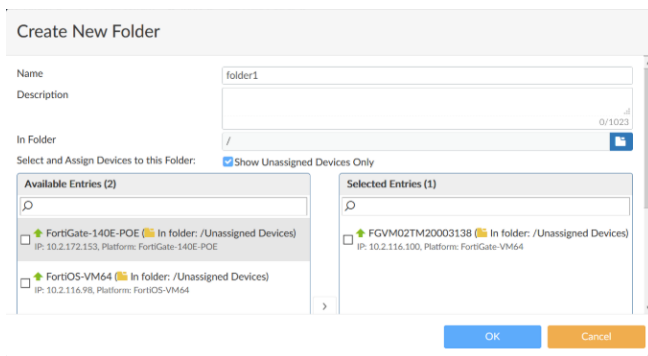


- b. In the *Devices* list, select one or more devices.
- c. In the *Firmware Template* list, select a firmware template, and click *OK*.  
A firmware template can include firmware for FortiGate as well as access devices, such as FortiAP, FortiSwitch, and FortiExtender.  
The firmware template is assigned 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.



**Create New Folder**

Name:

Description:

In Folder:

Select and Assign Devices to this Folder: ☒ Show Unassigned Devices Only

**Available Entries (2)**

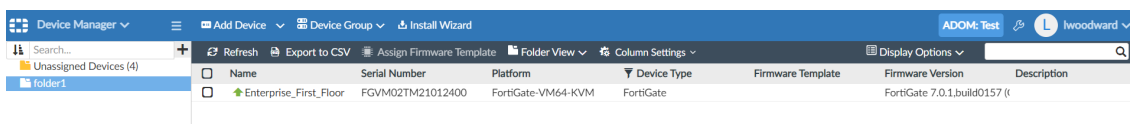
- FortiGate-140E-POE (In folder: /Unassigned Devices)  
IP: 10.2.172.153, Platform: FortiGate-140E-POE
- FortiOS-VM64 (In folder: /Unassigned Devices)  
IP: 10.2.116.98, Platform: FortiOS-VM64

**Selected Entries (1)**

- FGVM02TM20003138 (In folder: /Unassigned Devices)  
IP: 10.2.116.100, Platform: FortiGate-VM64

OK Cancel

- 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.



Name	Serial Number	Platform	Device Type	Firmware Template	Firmware Version	Description
Enterprise_First_Floor	FGVM02TM21012400	FortiGate-VM64-KVM	FortiGate		FortiGate 7.0.1.build0157 (	



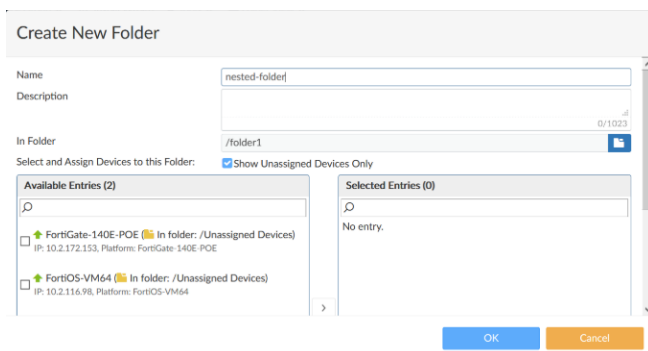
You can add FortiGates directly to a folder by selecting devices from the *Available Entries* list in the *Create New Folder* dialog.

## Nesting folders

The new *Folder View* supports nested folders.

### To create nested folders:

- 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`.



**Create New Folder**

Name:

Description:

In Folder:

Select and Assign Devices to this Folder: ☒ Show Unassigned Devices Only

**Available Entries (2)**

- FortiGate-140E-POE (In folder: /Unassigned Devices)  
IP: 10.2.172.153, Platform: FortiGate-140E-POE
- FortiOS-VM64 (In folder: /Unassigned Devices)  
IP: 10.2.116.98, Platform: FortiOS-VM64

**Selected Entries (0)**

No entry.

OK Cancel

- 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.

Name	Serial Number	IP Address	Platform	Device Type	Firmware Version	Description
FGVM02TM20003138	FGVM02TM20003138	10.2.116.100	FortiGate-VM64	FortiGate	FortiGate 6.4.0.build15	

## 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.

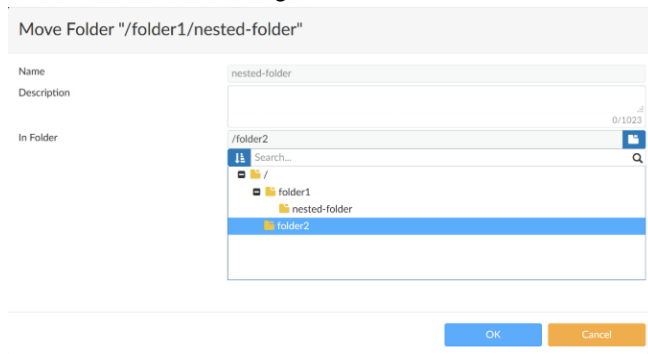
## Moving folders

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.

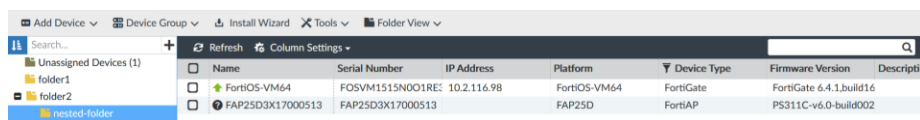
Name	Serial Number	IP Address	Platform	Device Type	Firmware Version	Description
FortiOS-VM64	FOSVM1515N001RE	10.2.116.98	FortiOS-VM64	FortiGate	FortiGate 6.4.1.build16	
FAP25D3X17000513	FAP25D3X17000513		FAP25D	FortiAP	PS311C-v6.0-build002	

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 117](#)
- [Importing AP profiles and FortiSwitch templates on page 119](#)

### Importing policies and objects

The import policy wizard helps you import policy packages and objects from managed FortiGate devices 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.



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.

#### 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.

Import Device - security-fabric [ root ]

Create a new policy package for import.

Policy Package Name

Folder

Policy Selection  
☒ Import All (21)  
☐ Select Policies to Import

Object Selection  
☒ Import only policy dependent objects  
☐ Import all objects

When importing configuration from this device, all enabled interfaces require a mapping to an ADOM Level interface. Note, the same ADOM Level interface can map to different interfaces on the each device.

Device Interface	Mapping Type	Normalized Interface
FortiDEMO	<input checked="" type="radio"/> Per-Device <input type="radio"/> Per-Platform	FortiDEMO
port2	<input type="radio"/> Per-Device <input checked="" type="radio"/> Per-Platform	port2
port3	<input type="radio"/> Per-Device <input checked="" type="radio"/> Per-Platform	port3

6. Specify what policies and objects to import:

<b>Policy Package Name</b>	(Optional) Type a name for the policy package.
<b>Folder</b>	(Optional) Select a folder on the dropdown menu. The default storage folder is <i>root</i> .
<b>Policy Selection</b>	Select <i>Import All</i> to import all policies. Select <i>Select Policies to Import</i> to select which policies and policy groups to import.
<b>Object Selection</b>	Select <i>Import only policy dependent objects</i> to import only policy dependent objects for the device. Select <i>Import all objects</i> 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.

<b>Device Interface</b>	Displays the enabled interfaces for the device for which you are importing policies.
<b>Mapping Type</b>	For each enabled device interface, select one of the of the following options: <i>Per-Device</i> or <i>Per-Platform</i> .
<b>Normalized Interface</b>	Displays the name of the normalized interface to which the device interface is mapped.
<b>Add mapping for all unused device interfaces</b>	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, choose whether to use the value from FortiGate or FortiManager, and click *Next*.  
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. If there are conflicts, you can select *View Conflict* to view details of each individual conflict. Duplicates will not be imported.  
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*.  
A list of objects to be imported is displayed.
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 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.

Import Device - gate50 [ root ]

Access Point	AP Profile Name
<input checked="" type="checkbox"/> FAP24D3X15001133	FAP24D-default-1
<input checked="" type="checkbox"/> FAP24D3X16000296	FAP24D-default-2
<input checked="" type="checkbox"/> FAP24D3X16000305	FAP24D-default-3
<input checked="" type="checkbox"/> FAP24D3X17000555	FAP24D-default-4

FortiSwitch Name	FortiSwitch Template Name
<input checked="" type="checkbox"/> S248DF3X17000116	Import-gate50-S248DF3X17000116

Next > Cancel

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.

Import Device - gate50 [ root ]

[Download Import Report]

100%

Total: 1/1, Success: 1, Warning: 0, Error: 0

View Progress Report

#	Name	Time Used	Status
1	gate50	5s	Import completed

Finish

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 121](#).
- To use the *Install Wizard* to install device settings only, see [Install device settings only on page 122](#).
- To reinstall a policy package without using the *Install Wizard*, see [Reinstall a policy package on page 315](#).



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 759](#) for information on enabling this feature.

# 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*.

Install Wizard - Choose what to install (1/4)

Install Policy Package & Device Settings

Policy Package

Branch\_Office\_01

Install Comments

Create ADOM Revision

☒

Revision Name

revision\_2023-05-10-03-30-55

Revision Comments

Schedule Install

☒

05 / 10 / 2023

03:30 PM

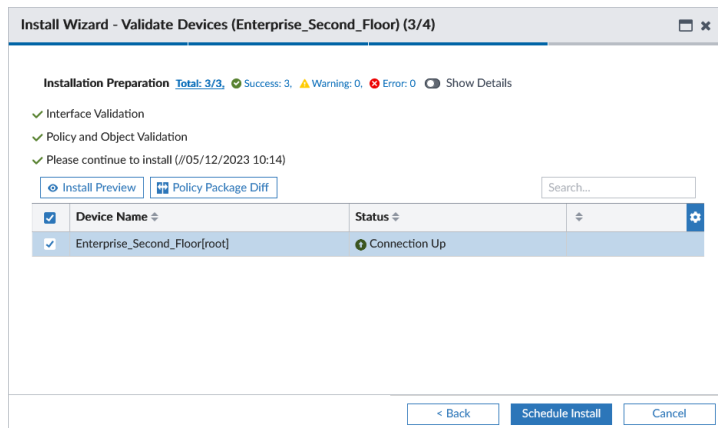
< Back

Next >

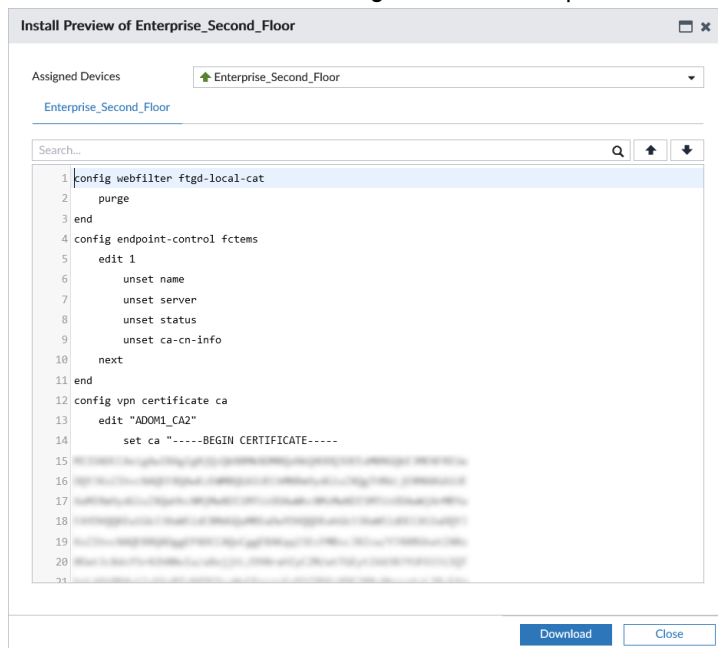
Cancel

<b>Policy Package</b>	Select the policy package from the dropdown list.
<b>Install Comments</b>	Type an optional comment.
<b>Create ADOM Revision</b>	Select the checkbox to create an ADOM revision.
<b>Revision Name</b>	Type the revision name.
<b>Revision Comments</b>	Type an optional comment.
<b>Schedule Install</b>	Select the checkbox to schedule the installation.
<b>Date</b>	Click the date field and select the date for the installation in the calendar pop-up.
<b>Time</b>	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 320](#)).



6. (Optional) Click the *Install Preview* button to view a preview of the installation. You can view multiple devices at the same time.
  - a. Click *Download* to download a text file of the installation preview details.
  - b. Select a device from the *Assigned Devices* dropdown menu to preview the installation on the chosen device.



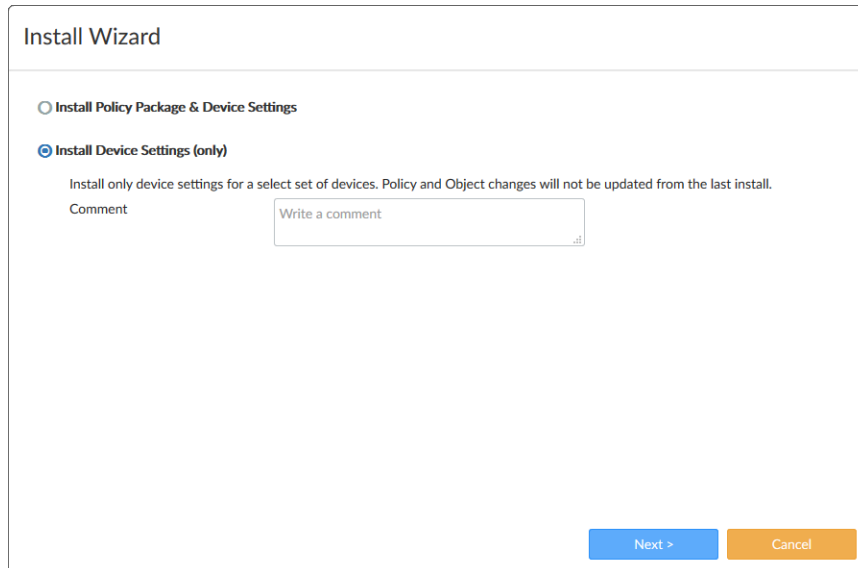
7. (Optional) Click the *Policy Package Diff* button to view the differences between the current policy and the policy in the device. See also [Viewing a policy package diff on page 124](#).
8. When validation is complete, click *Install* or *Schedule Install* (if you selected *Schedule Install*). FortiManager 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 785](#).

## 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.

The screenshot shows the 'Policy Package Diff (p1)' window. It has a 'Summary' tab selected. The window displays two tables of changes.

**Policy - added (1) [Details]**

Category	Change Summary	User	
IPv4 Policy	added (1)	admin	[Details]

**Policy Object - added (5) changed (3) deleted (106) [Details]**

Category	Change Summary	User	
CA Certificate	added (1)	admin	
Local User	deleted (1)	admin	
User Group	deleted (1)	admin	
Device Group	deleted (3)	admin	
Local Category	deleted (2)	admin	
Web Filter Profile	changed (1) deleted (4)	admin	
Address	added (1) changed (1) deleted (1)	admin	
Multicast Address	deleted (5)	admin	
IPv6 Address	deleted (1)	admin	

A 'Close' button is located at the bottom right of the window.

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 126](#)
- [Upgrading firmware on page 126](#)
- [Upgrading multiple firmware images on FortiGate on page 129](#)
- [Upgrading firmware downloaded from FortiGuard on page 130](#)

## 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 280](#).

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.

---

### 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 *Upgrade Firmware* dialog box opens.



Upgrade Firmware

Devices

Branch\_Office\_02: 7.0.2 (234)  
Enterprise\_Second\_Floor: 7.0.2 (234)

Upgrade to

7.0.2-b0234

☐ Boot From Alternate Partition After Upgrade  
☐ Let Device Download Firmware from FortiGuard ⓘ  
☐ Skip All Intermediate Steps in Upgrade Path if Possible ⓘ

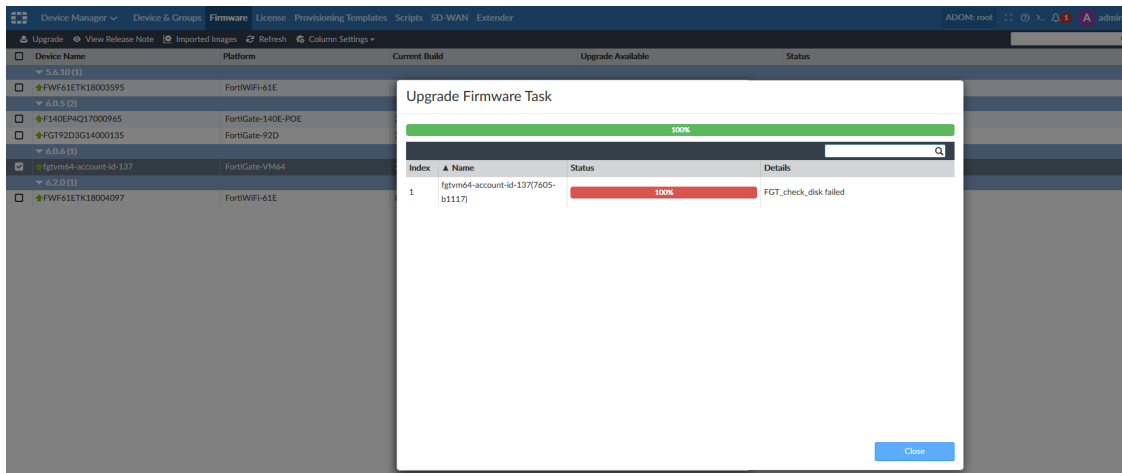
OK

Cancel

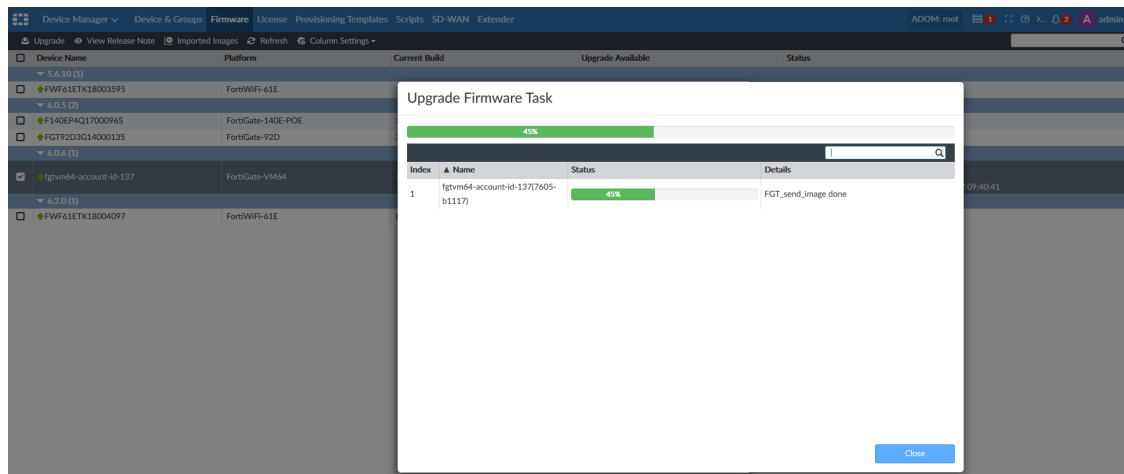
5. Configure the following settings, then click **OK**:

<b>Upgrade to</b>	Select a firmware version from the drop-down list.
<b>Boot From Alternate Partition After Upgrade</b>	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.
<b>Let Device Download Firmware from FortiGuard</b>	Select this option to download the firmware directly from FortiGuard. If this option is not selected, FortiManager will download the firmware from FortiGuard. Alternatively, you can import the firmware into FortiManager.
<b>Skip All Intermediate Steps in Upgrade Path if Possible</b>	FortiManager manages the most optimum upgrade path automatically. Select this option to install the selected version directly without going through the upgrade path.

FortiManager checks the FortiGate disk before upgrading. If the check fails, the following information is displayed, and the upgrade is not performed:



If the check passes, the upgrade proceeds:



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 images 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 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:

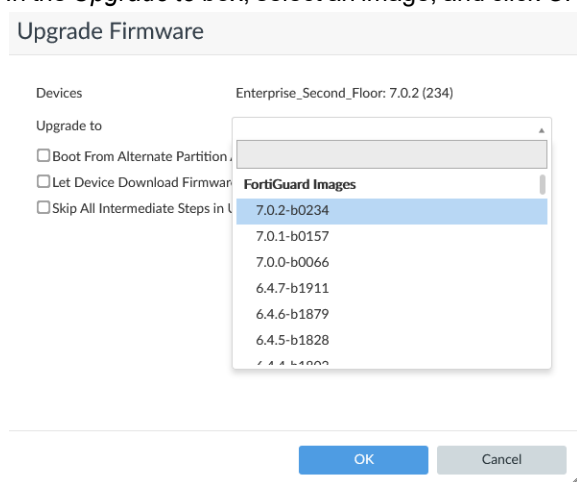
```
# diagnose fwmanager show-dev-upgrade-path 318 6.2.0
device FWF61ETK18003595(318), platform FWF61E, upgrade path from 5.6.10-1677 to 6.2.0-866
is: [6.0.0-76 --> 6.0.2-163 --> 6.0.3-200 --> 6.2.0-866]
```

It is recommended to also check that the upgrade path for FortiGate reported by FortiManager matches the upgrade path reported on the Fortinet Customer Service and Support site for the FortiGate device.

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

### To upgrade using the GUI:

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



The *Upgrade Path Preview* dialog box opens to let you review the upgrade before continuing.

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

Upgrade Firmware Task

10%

Index	Name	Status	Details
1	FWF61ETK18003595(6.0.0-b76)	10%	Downloading firmware from FortiGuard
2	FWF61ETK18003595(6.0.2-b163)	10%	Downloading firmware from FortiGuard
3	FWF61ETK18003595(6.0.3-b200)	10%	Downloading firmware from FortiGuard
4	FWF61ETK18003595(6.2.0-b866)	10%	Downloading firmware from FortiGuard

Close

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

Upgrade Firmware Task

100%

Index	Name	Status	Details
1	FWF61ETK18003595(6.0.0-b76)	100%	Upgrade complete successfully
2	FWF61ETK18003595(6.0.2-b163)	100%	Upgrade complete successfully
3	FWF61ETK18003595(6.0.3-b200)	100%	Upgrade complete successfully
4	FWF61ETK18003595(6.2.0-b866)	100%	Upgrade complete successfully

Close

- When the upgrade completes, click *Close*.

## Upgrading firmware downloaded from FortiGuard

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

### To upgrade firmware using images retrieved from FortiGuard:

1. Go to the device database. See [Displaying the device database on page 133](#).
2. In the *System Information* widget, click the *Update* icon beside *Firmware Version*.  
The *Device Firmware Upgrade* dialog box displays a list of images retrieved from FortiGuard.

**Device Firmware Upgrade**

Current Firmware

Partition	Active	Firmware	Status
1	✓	FortiGate 7.0.0,build0066 (GA)	Running

Available Upgrades    [Firmware Upgrade History](#)

Search...

#	Firmware	Release Date	Upgrade
▼ FortiGuard Images			
1	FortiGate 7.0.0, build (0066)	2021-04-02	[Upgrade]
2	FortiGate 6.4.5, build (1828)	2021-02-23	[Upgrade]
3	FortiGate 6.4.4, build (1803)	2020-12-11	[Upgrade]

Close

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

**Upgrade/Downgrade Firmware**

Upgrade to Official Image    FortiGate 7.0.0, build (0066)

☐ Boot From Alternate Partition After Upgrade

☐ Let Device Download Firmware from FortiGuard ⓘ

☐ Skip All Intermediate Steps in Upgrade Path if Possible ⓘ

OK    Cancel

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

### Upgrade Firmware Task

45%

Index	Name	Status	Details
1	F140EP4Q17000965(6.2.0-b866)	<div><div>45%</div></div>	FGT_send_image done

Close

The firmware upgrade completes.

### Upgrade Firmware Task

100%

Index	Name	Status	Details
1	F140EP4Q17000965(6.2.0-b866)	<div><div>100%</div></div>	reloadfin

Close

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 133](#)
- [Choosing display options for devices on page 134](#)
- [Using the CLI console for managed devices on page 136](#)

## 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.

The screenshot shows the FortiManager Device Manager interface. The left sidebar contains a tree menu with 'Device & Groups' expanded, showing 'Managed FortiGate (6)'. The main content area displays the 'Summary' dashboard for a device named 'lwoodward-test-sf700-apr7'. The dashboard is divided into two main sections: 'System Information' and 'License Information'. The 'System Information' section includes details like Host Name, Serial Number, IP Address, System Time, Uptime, Firmware Version, Hardware Status, Operation Mode, VDOM, and Operation. The 'License Information' section includes FortiCare Support details (FortiCare Account, Hardware, Firmware, Enhanced Support, Comprehensive Support) and FortiGuard Services (AntiVirus, IPS, Web Filtering, Email Filtering, Outbreak Protection, Industrial DB, VDOM). The VDOM section shows 'VDOMs allowed' as 10 (10%).

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.

System	From the <i>System</i> menu, you can access many panes, such as <i>Interface</i> , <i>SD-WAN</i> , <i>SNMP</i> , and <i>Replacement Message</i> .
Router	From the <i>Router</i> menu, you can access several panes, such as <i>Static Route</i> and <i>OSPF</i> .
Display Options	By default, some of the menu items are hidden. Click <i>Display Options</i> to choose what menu items to hide and display. See <a href="#">Choosing display options for devices on page 134</a> .

For information on configuring FortiGate settings, see the *FortiOS Administration Guide*.

## Choosing display options 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 display 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 display options apply to all devices in the ADOM, letting you specify different global display options for each ADOM.

### To specify global display options for all devices in an ADOM:

1. Go to the device database. See [Displaying the device database on page 133](#).  
The *Dashboard* for the device database is displayed.
2. In the left pane, click *Display Options*.  
The *Display Options* dialog box is displayed.



3. Select *Global Display Options*, 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 display options for a device:

1. Go to the device database. See [Displaying the device database on page 133](#).  
The *Dashboard* for the device database is displayed.
2. In the left pane, click *Display Options*.  
The *Display Options* dialog box is displayed.

Display Options

☐ Global Display Options ☒ Customize

<input checked="" type="checkbox"/> <b>System</b>	<input checked="" type="checkbox"/> Dashboard <input type="checkbox"/> SD-WAN <input checked="" type="checkbox"/> SNMP <input type="checkbox"/> DNS Database <input type="checkbox"/> Explicit Proxy <input type="checkbox"/> Admin Settings <input type="checkbox"/> Admin Profile <input type="checkbox"/> Certificates <input type="checkbox"/> FortiGuard <input type="checkbox"/> Automation Stitch <input type="checkbox"/> Alert Email <input type="checkbox"/> NAT64 Prefix	<input checked="" type="checkbox"/> Interface <input type="checkbox"/> DHCP Server <input type="checkbox"/> DNS <input type="checkbox"/> DNS Service on Interface <input type="checkbox"/> Management <input type="checkbox"/> Administrators <input type="checkbox"/> Local Host ID <input checked="" type="checkbox"/> Replacement Message <input type="checkbox"/> Security Fabric <input type="checkbox"/> Log Setting <input type="checkbox"/> Threat Weight <input type="checkbox"/> FortiSandbox
<input checked="" type="checkbox"/> <b>Router</b>	<input type="checkbox"/> Static Route <input type="checkbox"/> OSPF <input type="checkbox"/> BGP	<input type="checkbox"/> Policy Route <input type="checkbox"/> RIP <input type="checkbox"/> Multicast Route
<input checked="" type="checkbox"/> <b>WAN Opt. &amp; Cache</b>	<input type="checkbox"/> Settings	<input type="checkbox"/> URL Match List
<input checked="" type="checkbox"/> <b>Security Profiles</b>	<input type="checkbox"/> Web Filter Override	
<input checked="" type="checkbox"/> <b>VPN</b>	<input type="checkbox"/> IPsec Phase 1	<input type="checkbox"/> IPsec Phase 2

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 133](#).
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.

## Device DB - Dashboard

In the device database, the *Dashboard* menu provides access to the following dashboards:

- [Summary dashboard on page 137](#)
- Security Monitors dashboard
- Network Monitors dashboard
- User and Authentications dashboard

Each dashboard contains widgets that you can use to monitor information about the device. You can also create custom dashboards, selecting the desired widgets and changing the dashboard layout. See [Creating custom system dashboards on page 140](#).

Once a custom dashboard is created, it can be copied to other devices, as needed. See [Copying custom system dashboards on page 141](#).

### Summary dashboard

The *Summary* dashboard widgets provide quick access to device information. The following widgets are available:

- [System Information](#)
- [License Information](#)
- [Configuration and Installation](#)
- [Configuration Revision History](#) (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	
<b>Host Name</b>	The host name of the device.
<b>Serial Number</b>	The device serial number.
<b>IP Address</b>	The IP address of the device.
<b>Platform Type</b>	The platform type for the device.
<b>HA Status</b>	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.
<b>System Time</b>	The device system time and date information.
<b>Uptime</b>	Displays the duration the device has been up.
<b>Firmware Version</b>	The device firmware version and build number.
<b>Hardware Status</b>	The number of CPUs and the amount of RAM for the device.

## System Information

<b>Operation Mode</b>	Displays whether the device is in <i>NAT</i> or <i>Central NAT</i> operation mode.
<b>VDOM</b>	The status of VDOMs on the device.
<b>Operation</b>	Select one of the following: <ul style="list-style-type: none"> <li>• <i>Connect to CLI via SSH</i> to connect to the CLI console of the device</li> <li>• <i>Reboot</i> to reboot the device</li> <li>• <i>Shutdown</i> to shut down the device</li> </ul>
<b>System Configuration</b>	Displays the Last Backup. You can backup or restore.
<b>Current Administrators</b>	Displays the number of administrators configured on this device.
<b>Administrative Domain</b>	Toggle the switch <i>ON</i> or <i>OFF</i> to enable or disable ADOMs.
<b>Analyzer Features</b>	Toggle the switch <i>ON</i> or <i>OFF</i> to enable or disable FortiAnalyzer features.

## License Information

<b>VM License</b>	The VM license information.
<b>FortiCare Support</b>	<p>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.</p> <hr/> <div style="display: flex; align-items: center;">  <p>FortiManager does not retrieve <i>FortiCare Support</i> information when the device was added using <i>Add Model Device</i>, even when the device is registered to the same FortiCloud account.</p> </div> <hr/>
<b>FortiGuard Services</b>	The contract version, issue date and service status. FortiGuard Services includes the following: Antivirus, Intrusion protection, Web filtering, and Email filtering.
<b>VDOM</b>	The number of virtual domains that the device supports.

## Configuration and Installation

<b>Enforce Firmware Version</b>	<p>The firmware version enforced on the device. The firmware version is enforced when FortiGate is connected to the network. Click the <i>Edit</i> icon to select the firmware version. You can also select the firmware version in the <i>Add Device</i> screen when adding a model device.</p> <p>For more information, see <a href="#">Adding offline model devices on page 62</a>.</p>
<b>System Template</b>	<p>The system template installed on the device. The system template is installed when FortiGate is connected to the network. Click the <i>Edit</i> icon to select the system template. You can also select the system template in the <i>Add Device</i> screen when adding a model device.</p> <p>For more information, see <a href="#">Adding offline model devices on page 62</a>.</p>

Configuration and Installation	
<b>Policy Package</b>	<p>The policy package installed on the device. The policy package is installed when FortiGate is connected to the network. Click the <i>Edit</i> icon to select the policy package. You can also select the policy package in the <i>Add Device</i> screen when adding a model device.</p> <p>For more information, see <a href="#">Adding offline model devices on page 62</a>.</p>
<b>Database Configuration</b>	Select <i>View</i> to display the configuration file of the FortiGate unit.
<b>Total Revisions</b>	<p>Displays the total number of configuration revisions and the revision history. Select <i>Revision History</i> to view device history. Select the revision history icon to open the <i>Revision Diff</i> menu. You can view the diff from a previous revision or a specific revision and select the output.</p>
<b>Config Status</b>	<p>The synchronization status with the FortiManager:</p> <ul style="list-style-type: none"> <li>• <i>Synchronized</i>: The latest revision is confirmed as running on the device.</li> <li>• <i>Out_of_sync</i>: The configuration file on the device is not synchronized with the FortiManager system.</li> <li>• <i>Unknown</i>: The FortiManager system is unable to detect which revision (in revision history) is currently running on the device.</li> </ul> <p>Select <i>Refresh</i> to update the Installation Status.</p>
<b>Warning</b>	<p>Displays any warnings related to configuration and installation status:</p> <ul style="list-style-type: none"> <li>• <i>None</i>: No warning.</li> <li>• <i>Unknown configuration version running on FortiGate: FortiGate configuration has been changed!</i>: The FortiManager system cannot detect which revision (in <i>Revision History</i>) is currently running on the device.</li> <li>• <i>Unable to detect the FortiGate version</i>: Connectivity error!</li> <li>• <i>Aborted</i>: The FortiManager system cannot access the device.</li> </ul>
<b>Installation Tracking</b>	
<b>Device Settings Status</b>	<ul style="list-style-type: none"> <li>• <i>Modified</i>: Some configuration on the device has changed since the latest revision in the FortiManager database. Select <i>Save Now</i> to install and save the configuration.</li> <li>• <i>UnModified</i>: All configuration displayed on the device is saved as the latest revision in the FortiManager database.</li> </ul>
<b>Installation Preview</b>	Select the icon to display a set of commands that will be used in an actual device configuration installation in a new window.
<b>Last Installation</b>	The FortiManager system sent a configuration to the device at the indicated date and time.
<b>Scheduled Installation</b>	A new configuration will be installed on the device at the indicated date and time.
<b>Script Status</b>	Select <i>Configure</i> to view script execution history.
<b>Last Script Run</b>	Displays the date when the last script was run against the managed device.
<b>Scheduled Script</b>	Displays the date when the next script is scheduled to run against the managed device.

Configuration Revision History	
<b>View Config</b>	Click a configuration revision, and click <i>View Config</i> to view the configuration details.
<b>View Install Log</b>	Click a configuration revision, and click <i>View Install Log</i> to display the installation log.
<b>Revision Diff</b>	Click a configuration revision, and click <i>Revision Diff</i> to view the difference between the current and previous revisions.
<b>Retrieve Config</b>	Click to retrieve a configuration and create a new revision.
<b>ID</b>	The identification number for the configuration revision.
<b>Date &amp; Time</b>	The date and time for the configuration revision.
<b>Name</b>	The name of the device.
<b>Created by</b>	The name of the administrator who created the configuration revision.
<b>Installation</b>	The status of the installation for the configuration revision.
<b>Comments</b>	Comments about the device.



The information presented in the System Information, License Information, and Configuration and Installation Status widgets will vary depending on the managed device model.

## 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 133](#).
2. From the more options icon for the *Dashboard* menu, select *Create New*.



Hover your cursor next to the *Dashboard* to display the more options icon.

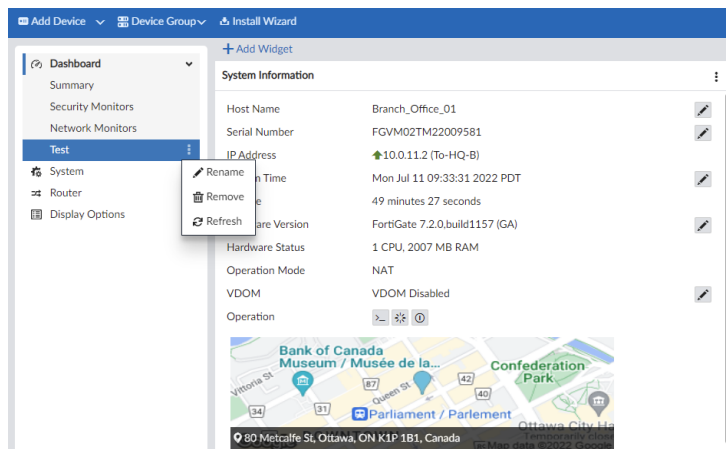
The *Create New Dashboard* pane is displayed.

3. In the *Dashboard Name* field, type a name, and click *OK*.  
The dashboard is created, and the *Add Dashboard Widget* pane is displayed.
4. Select widget(s) to add them to the dashboard, and click *Close*.  
The widgets are added to the dashboard.
5. Click *Grid Layout*, to change the dashboard layout to one, two, or three columns, or to fit the content.

6. (Optional) Click the more options icon for the custom dashboard to *Rename*, *Remove*, or *Refresh* the dashboard.



You cannot remove the *Summary*, *Resource Usage*, and *Network Monitors* dashboards.



You cannot remove the default dashboard widgets.

## 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, if needed.



When copying dashboards to and from other devices/VDOMs, the target device's/VDOM's current dashboard configurations will be overwritten.

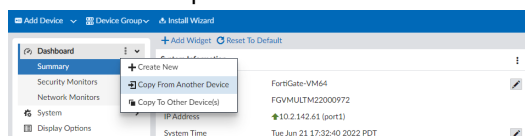
You cannot copy a dashboard to or from devices on different ADOMs.



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 51](#).

### 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 133](#).
2. From the more options 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 133](#).
2. From the more options 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*.

---

## 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 142](#)
- [Viewing configuration revision history](#)
- [Viewing configuration settings on FortiGate on page 145](#)
- [Adding a tag to configuration versions on page 145](#)
- [Downloading a configuration file on page 145](#)
- [Importing a configuration file on page 146](#)
- [Comparing different configuration files on page 146](#)
- [Reverting to another configuration file on page 147](#)

### 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 133](#).
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	
<b>Config Status</b>	<p>Displays the synchronization status of the configuration with FortiManager.</p> <ul style="list-style-type: none"> <li>• <i>Synchronized</i>: The latest revision is confirmed as running on the device.</li> <li>• <i>Out_of_sync</i>: The configuration file on the device is not synchronized with the FortiManager system.</li> <li>• <i>Unknown</i>: The FortiManager system is unable to detect which revision (in revision history) is currently running on the device.</li> <li>• <i>Auto-update</i>: The configuration was changed directly on the FortiGate, and the changes were automatically retrieved to the FortiManager's device database. See: <a href="#">Auto-update and auto-retrieve on page 40</a>.</li> </ul> <p>Click <i>Refresh</i> to update the synchronization status.</p>
<b>System Template</b>	<p>Displays the name of the selected system template. Click <i>Change</i> to change the system template.</p>
Revision	
<b>Total Revisions</b>	<p>Displays the total number of configuration revisions and the revision history. Click <i>Revision History</i> to view device history. For details, see <a href="#">Viewing configuration revision history on page 143</a>.</p> <p>Click <i>Revision Diff</i> to compare revisions. For details, see <a href="#">Comparing different configuration files on page 146</a>.</p>
<b>Last Installation</b>	<p>Displays the last installation's date, time, revision number, and the person who did the installation.</p>
<b>Device Configuration DB</b>	<p>Click <i>View Full Config</i> to display the database configuration file of the FortiGate unit.</p> <p>Click <i>View Diff</i> to display the <i>Device Revision Diff</i> dialog box.</p>

## 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 133](#).
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:

<b>View Config</b>	View the configuration for the selected revision.
<b>View Install Log</b>	View the installation log for the selected revision.
<b>Revision Diff</b>	Show only the changes or differences between two versions of a configuration file. For details, see <a href="#">Comparing different configuration files on page 146</a> .
<b>Retrieve Config</b>	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.
<b>More</b>	From the More menu, you can select one of the following: <ul style="list-style-type: none"> <li>• Download Factory Default</li> <li>• Revert</li> <li>• Delete</li> <li>• Rename</li> <li>• Import Revision</li> <li>• Download Revision</li> </ul>

You can also right-click a revision to access the same options.

The following columns of information are displayed:

<b>ID</b>	The revision number. Double-click an ID to view the configuration file. You can also click <i>Download</i> to save the configuration file.
<b>Date &amp; Time</b>	The time and date when the configuration file was created.
<b>Name</b>	A name assigned by the user to make it easier to identify specific configuration versions. You can rename configuration versions.
<b>Created by</b>	The name of the administrator account used to create the configuration file.
<b>Installation</b>	Display the status of the installation. <i>N/A</i> 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 <i>N/A</i> .
<b>Comments</b>	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 133](#).
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 133](#).
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 133](#).
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 133](#).
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 only import a configuration file that is downloaded from the FortiManager repository, otherwise the import fails.

---

**To import a configuration file from a local computer:**

1. Go to the device database. See [Displaying the device database on page 133](#).
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 133](#).
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 133](#).
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 148](#)
- [Interface packet capture on page 148](#)

#### To view interfaces for a device:

1. Go to the device database. See [Displaying the device database on page 133](#).
2. In the device database, go to *Network > Interfaces*. The *Interface* pane is displayed.

**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 408](#).

**To create a device zone:**

1. Go to the device database. See [Displaying the device database on page 133](#).
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.

Create New Device Zone

Zone Name  This field is required.

Interface Member  Click to select

Block intra-zone traffic ☒

Description  Write a description

OK Cancel

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 413](#).

## Interface packet capture

You can perform packet capture on a managed FortiGate's interface through the device database.

### 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*.

#	Name	Type	Normalized Interface	Addressing
<b>Physical (4)</b>				
1	port2 (DMZ Segment)	Physical	port2	Manual
2	port3 (ISFW)	Physical	port3	Manual
3	port4 (Management)	Physical	port4	Manual
4	port6 (MPLS-to-HQ)	Physical	port6	Manual
<b>Aggregate (1)</b>				
5	fortilink	Aggregate	fortilink	Manual
<b>Tunnel (4)</b>				
6	nafe.root	Tunnel	nafe.root	Manual
7	l2t.root	Tunnel	l2t.root	Manual
8	ssl.root (SSL VPN interface)	Tunnel	ssl.root	Manual
9	FortiDEMO	Tunnel	FortiDEMO	Manual
<b>Zone (7)</b>				
10	port1 (Internet_A)	Physical	port1	Manual
11	port5 (Internet_B)	Physical	port5	Manual
12	Branch-HQ-A (VPN_A_Tunnel)	Tunnel		Manual
13	Branch-HQ-B (VPN_B_Tunnel)	Tunnel		Manual
14	HQ-MPLS (HQ-MPLS)	Tunnel		Manual

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 50000 packets to preserve memory.

Packet Capture

Max Number of Packets: 50000

Filters: **Basic** | Advanced

Filtering syntax: Basic

Host: [ ] [x] [+]

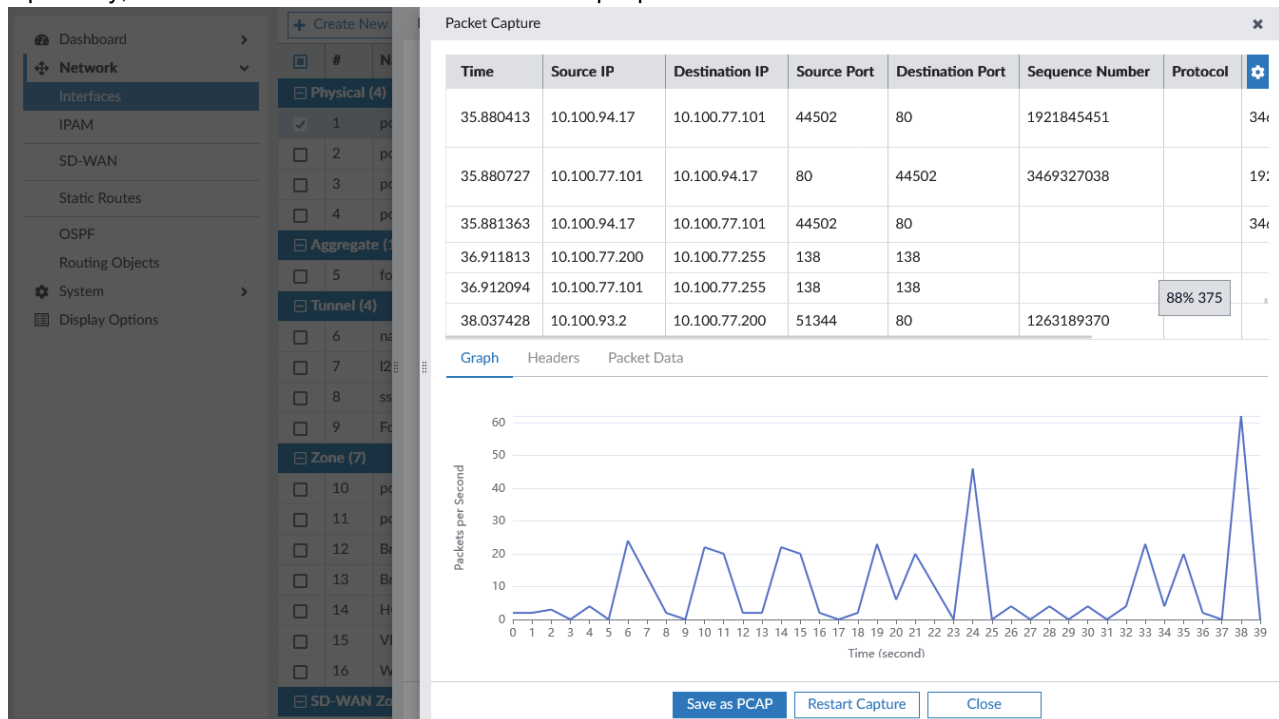
Protocol: [ ] +

Port: [ ] +

OK Cancel

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 (VDMs) 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 150](#)
- [Viewing virtual domains on page 151](#)
- [Creating virtual domains on page 152](#)
- [Configuring inter-VDM routing on page 152](#)
- [Deleting a virtual domain on page 153](#)
- [Editing resource limits on page 153](#)

For more information about VDMs, see the [FortiOS Administration Guide](#) available in the [Fortinet Document Library](#).

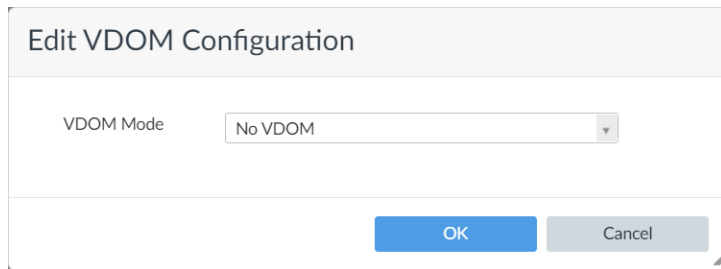
### Enabling virtual domains

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 133](#).
2. In the device database, go to *Dashboard > Summary*.
3. In the *System Information* widget, click the *Edit VDM* icon beside *VDM*.  
The *Edit VDM Configuration* dialog box is displayed.





The dialog box is titled "Edit VDOM Configuration". It contains a label "VDOM Mode" followed by a dropdown menu currently showing "No VDOM". At the bottom right, there are two buttons: "OK" (in blue) and "Cancel" (in grey).

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 152](#).

## 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 133](#).
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 display options for devices on page 134](#).

The following toolbar displays at the top of the page:

<b>Create New</b>	Select to create a new virtual domain.
<b>Edit</b>	Select a VDOM, and click <i>Edit</i> to edit the settings.
<b>Delete</b>	Select a VDOM, and click Delete to remove it. This function applies to all virtual domains except the root.
<b>Resource Limits</b>	Select a VDOM, and click <i>Resource Limits</i> to configure the resource limit profile.
<b>Set Management</b>	Select a VDOM, and click <i>Set Management</i> to define the VDOM as the root VDOM also known as the management VDOM.

Under the toolbar, the following columns of information are displayed:

<b>Name</b>	The name of the virtual domain and if it is the management VDOM.
<b>NGFW Mode</b>	Displays the Next Generation Firewall setting for the VDOM of <i>Profile-based</i> or <i>Policy-based</i> .
<b>Operation Mode</b>	Displays the operation mode for the VDOM.
<b>Status</b>	Displays the status of the VDOM.
<b>Interfaces</b>	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 150](#).

### To create virtual domains:

1. Go to the device database. See [Displaying the device database on page 133](#).
2. In the device database, go to *System > Virtual Domain*.



The *Virtual Domain* tab may be hidden. See [Choosing display options for devices on page 134](#).

---

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 133](#).
2. In the device database, go to *System > Interface*.

- Click **Create New > VDOM Link**. The **New VDOM Link** pane opens.

- 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 310](#)). All objects related to the VDOM must also be removed, such as routes, VPNs, and admin accounts.

### To delete a VDOM:

- Go to the device database. See [Displaying the device database on page 133](#).
- Go to **System > Virtual Domain**.
- Right-click the VDOM, and select **Delete**.
- Click **OK** in the confirmation dialog box to delete the VDOM.

## Editing resource limits

### To edit resource limits:

- Go to the device database. See [Displaying the device database on page 133](#).
- Go to **System > Virtual Domain**.
- Select the VDOM, and click **Resource Limits** in the toolbar.
- Edit the settings, and click **OK** to save the changes.

## Device DB - System 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 231](#).

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 161](#).
2. Configure SD-WAN settings for each device. See [SD-WAN per-device management on page 154](#).
3. Install device settings using the *Install Wizard*. See [Install device settings only on page 122](#).
4. Monitor SD-WAN networks. See [SD-WAN Monitor on page 286](#).

### 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 133](#).
2. In the device database, go to *System > SD-WAN*.

The *SD-WAN* pane opens.

**SD-WAN**

SD-WAN Status ☐ OFF

**Interface Members**

+ Create New Edit Delete Where Used Column Settings

ID	Interface Member	Status	Gateway	Cost
<input type="checkbox"/>	virtual-wan-link			

Create VPN

**Performance SLA**

+ Create New Edit Delete Where Used Column Settings

Name	Health-Check Server	Detect Protocol	Failure Threshold	Recovery Threshold
<input type="checkbox"/>	Default_AWS	aws.amazon.com	HTTP	5
<input type="checkbox"/>	Default_DNS	8.8.8.8, 208.91.112.52 (System DNS)	DNS	5
<input type="checkbox"/>	Default_FortiGuard	fortiguard.com	HTTP	5
<input type="checkbox"/>	Default_Gmail	gmail.com	Ping	5
<input type="checkbox"/>	Default_Google Search	www.google.com	HTTP	5
<input type="checkbox"/>	Default_Office_365	www.office.com	HTTP	5

SD-WAN Rules

+ Create New Edit Delete Move Up Move Down Column Settings

ID	Name	Source	Destination	Criteria	Members
----	------	--------	-------------	----------	---------

Apply

3. Configure the following options, and click *Apply*:

<b>SD-WAN Status</b>	Select <i>On</i> or <i>Off</i> .
<b>Interface Members</b>	Zones and interface members can be added, edited, and removed. See <a href="#">SD-WAN zones and interface members on page 155</a> .
<b>Create VPN</b>	See <a href="#">IPsec VPN Wizard on page 157</a> .
<b>Performance SLA</b>	See <a href="#">Performance SLA on page 158</a> .
<b>SD-WAN Rules</b>	See <a href="#">SD-WAN rules on page 159</a> .
<b>Neighbor</b>	See <a href="#">BGP Neighbors on page 161</a> .
<b>Duplication</b>	See <a href="#">Duplication on page 161</a> .
<b>Advanced Options</b>	Expand <i>Advanced Options</i> 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

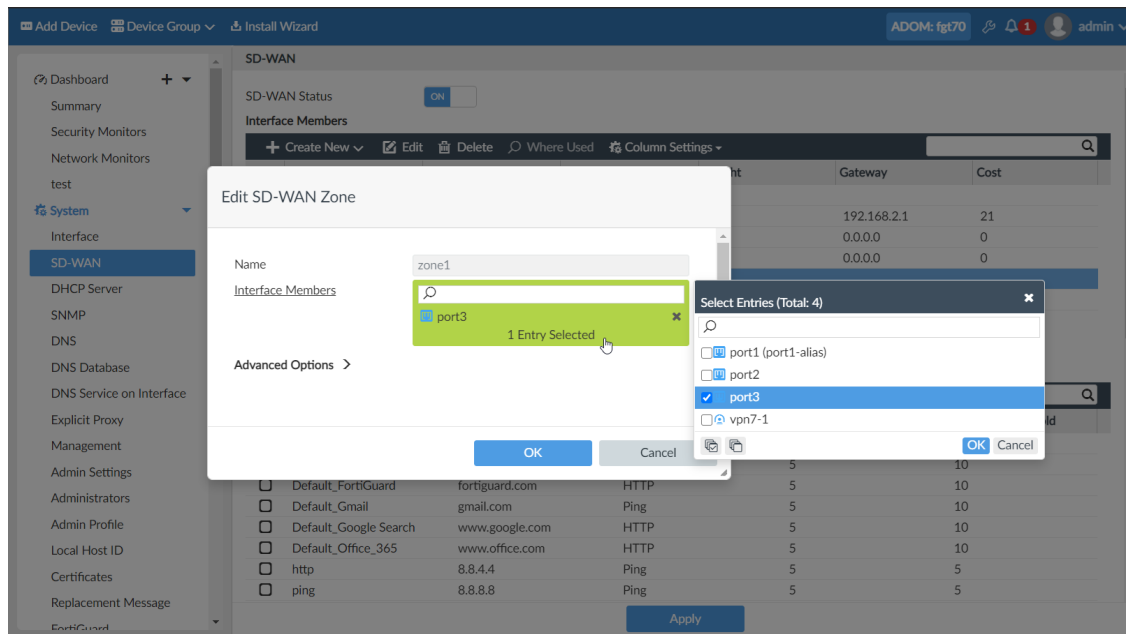
For each device, you can create SD-WAN zones and interface members. You can select SD-WAN zones as source and destination interfaces in firewall policies. You cannot select interface members of SD-WAN zones in firewall policies.

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 133](#).
2. In the device database, go to *System > 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 133](#).
2. In the device database, go to *System > 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.

Create New SD-WAN Interface Member

Sequence Number

Interface Member

SD-WAN Zone

Gateway IP

Cost

Status
☒ ON

Advanced Options >

4. Set the options, and click **OK**.  
The interface is added to the zone.

- 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:

- Go to the device database. See [Displaying the device database on page 133](#).
- In the device database, go to *System > SD-WAN*.  
The *SD-WAN* pane opens.
- In the *Interface Members* section, click *Create VPN*.

The screenshot shows the SD-WAN configuration page. At the top, there's a toggle for SD-WAN Status (OFF). Below it is the 'Interface Members' section with a table containing columns: ID, Interface Member, Status, Gateway, and Cost. A 'Create VPN' button is located below this table. The 'Performance SLA' section has a table with columns: Name, Health-Check Server, Detect Protocol, Failure Threshold, and Recovery Threshold. The 'SD-WAN Rules' section has a table with columns: ID, Name, Source, Destination, Criteria, and Members. An 'Apply' button is at the bottom right of the SD-WAN Rules section.

The *Create IPsec VPN for SD-WAN* dialog box is displayed.

The dialog box is titled 'Create IPsec VPN for SD-WAN'. It contains the following fields and controls:
 

- Name:** A text input field.
- Remote Device:** A dropdown menu with 'IP Address' (selected) and 'Dynamic DNS' tabs.
- IP Address:** A text input field showing '0.0.0.0'.
- Outgoing Interface:** A text input field with the placeholder 'Click here to select'.
- Authentication Method:** A dropdown menu with 'Pre-shared Key' (selected) and 'Signature' tabs.
- Pre-shared Key:** A text input field.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

- Configure the following settings, and click *OK* to generate IPsec VPNs:

<b>Name</b>	Specify a name for the VPN.
<b>Remote Device</b>	Select <i>IP Address</i> or <i>Dynamic DNS</i> .

<b>IP Address</b>	Specify the IP address if <i>IP Address</i> is selected for <i>Remote Device</i> .
<b>FQDN</b>	Specify the FQDN if <i>Dynamic DNS</i> is selected for <i>Remote Device</i> .
<b>Outgoing Interface</b>	Select the outgoing interface.
<b>Authentication Method</b>	Select <i>Pre-shared key</i> or <i>Signature</i> .
<b>Certificate Name</b>	Select the certificate (if <i>Signature</i> was selected as the <i>Authentication Method</i> )
<b>Peer Certificate CA</b>	Select the Peer Certificate CA (if <i>Signature</i> was selected as the <i>Authentication Method</i> )
<b>Pre-shared Key</b>	Select the pre-shared key (if <i>Pre-shared key</i> was selected as the <i>Authentication Method</i> )

The auto-generated VPN interface is automatically added to the list of SD-WAN interface members.

The screenshot shows the FortiManager SD-WAN configuration page. The left sidebar has a menu with 'SD-WAN' selected. The main content area is titled 'SD-WAN' and shows the configuration for 'ADOM: fgt70'. It includes a toggle for 'SD-WAN Status' (ON). Below this is the 'Interface Members' section with a table listing various interfaces. The 'Performance SLA' section is also visible, showing a table of SLA entries. An 'Apply' button is at the bottom right of the main configuration area.

ID	Interface Member	Status	Weight	Gateway	Cost
0	virtual-wan-link				
2	port2	Enable	21	192.168.2.1	21
4	vpn7-1	Enable	1	0.0.0.0	0
1	port1 (port1-alias)	Enable	1	0.0.0.0	0
3	port3	Enable	1	0.0.0.0	0

Name	Health-Check Server	Detect Protocol	Failure Threshold	Recovery Threshold
Default_AWS	aws.amazon.com	HTTP	5	10
Default_DNS	208.91.112.53, 208.91.112.5	DNS	5	10
Default_FortiGuard	fortiguard.com	HTTP	5	10
Default_Gmail	gmail.com	Ping	5	10
Default_Google Search	www.google.com	HTTP	5	10
Default_Office_365	www.office.com	HTTP	5	10
http	8.8.4.4	Ping	5	5
ping	8.8.8.8	Ping	5	5

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 133](#).
2. In the device database, go to *System > SD-WAN*.  
The *SD-WAN* pane opens.
3. In the *Performance SLA* section, click *Create New*.  
The *Create Performance SLA* dialog-box opens



Create New Performance SLA

Name

IP Version

Detect Protocol

Health-Check Server  + 🗑️

Participants  Specify

Enable Probe Packets ☒

SLA

+ Create New <span>✎ Edit</span> <span>🗑️ Delete</span> <span>⚙️ Column Settings</span> <input type="text" value=""/>			
<input type="checkbox"/> ID	Latency Threshold (Milliseconds)	Jitter Threshold (Milliseconds)	Packet Loss Threshold (%)
No record found.			

OK Cancel

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 133](#).
2. In the device database, go to *System > 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	<input type="text"/>		
IP Version	IPv4 <span>▼</span>		
<b>Source</b>			
Source Address	<input type="text"/> Click to select		
Users	<input type="text"/> Click to select		
User Groups	<input type="text"/> Click to select		
<b>Destination</b>			
	Address	Internet Service	
Internet Service	<input type="text"/> Click to select		
Internet Service Group	<input type="text"/> Click to select		
Custom Internet Service	<input type="text"/> Click to select		
Internet Service Custom Group	<input type="text"/> Click to select		
Application	<input type="text"/> Click to select		
Application Group	<input type="text"/> Click to select		
Application Category	<input type="text"/> Click to select		
Type of Service	0x00	Bit Mask	0x00
<b>Outgoing Interfaces</b>			
Strategy	Manual Best Quality Lowest Cost (SLA) Maximize Bandwidth (SLA)		
Interface Preference	<div>+</div>		

\*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 238](#).

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 - Router BGP on page 162](#).

### To add BGP neighbors:

1. Go to the device database. See [Displaying the device database on page 133](#).
2. In the device database, go to *System > 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 133](#).
2. In the device database, go to *System > 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.

Create New SD-WAN Duplication

Source Address	<input type="text" value="Click here to select"/>
Destination Address	<input type="text" value="Click here to select"/>
Source Address 6	<input type="text" value="Click here to select"/>
Destination Address 6	<input type="text" value="Click here to select"/>
Source Interface	<input type="text" value="Click here to select"/>
Destination Interface	<input type="text" value="Click here to select"/>
Service	<input type="text" value="Click here to select"/>
Packet Discard Duplication	<input type="checkbox"/> OFF
Packet Duplication	<input checked="" type="radio"/> Disable <input type="radio"/> Force <input type="radio"/> On Demand

OK Cancel

4. Configure the options, and click *OK*.
5. Click *Apply* to save the SD-WAN settings.

## Device DB - System HA

You cannot use FortiManager to configure high availability (HA) on 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*.

It is recommended to configure HA settings directly on FortiGate units. Another option is to run CLI scripts directly against FortiGate devices.

## Device DB - Router BGP

You can create Border Gateway Protocol (BGP) neighbors for FortiGates.

If BGP is hidden, see [Choosing display options for devices on page 134](#).

### To create BGP neighbors:

1. Go to the device database. See [Displaying the device database on page 133](#).
2. In the device database, go to *Router > 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 133](#).
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 163](#)
- [Replacing a managed device on page 164](#)

### 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 94](#)).
- If a template is assigned to the device, the template will remain with no device assignment ([Provisioning Templates on page 200](#)).
- 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 318](#)).
- 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 [Install policies only to specific devices on page 332](#)).
- If there are VDOMs in other ADOMs, they will be deleted with the device ([ADOM device modes on page 754](#)).

### 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 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*.
4. On the FortiGate *Central Management Settings* page, enter the FortiGate 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 165](#)
- [FortiManager supports FortiGate auto-scale clusters on page 166](#)



For information on adding offline model FortiGate HA clusters, see [Adding a model FortiGate HA cluster on page 66](#).

## 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.

The screenshot displays the FortiManager interface for an HA cluster. The left sidebar shows navigation options like Summary, Security Monitors, and Network Monitors. The main content area is divided into several sections:

- System Information:** Host Name (FGVM02), Serial Number (FGVM02), System Time (Mon Mar 08 13:47:38 2021 PST), Uptime (N/A), Firmware Version (FortiGate 6.4.build1774), Hardware Status (N/A), Operation Mode (NAT), and VDOM (VDOM Disabled).
- License Information:** FortiCare Support (Not Registered), FortiCare Account (Not Registered), Hardware (Not Registered), Firmware (Not Registered), Enhanced Support (Not Registered), Comprehensive Support (Not Registered), FortiGuard Services (Status: Expires on), AntiVirus (N/A), and IPS (N/A).
- HA Status:** HA Mode (Active-Active), Cluster Name (Region 1 (0)), Uptime (N/A), and State Changed (N/A).
- Cluster Members:** A table with columns for Host Name, Serial Number, Role, and Priority. It lists two members: FGVM02 (Primary, Priority 0) and FGVM02 (Secondary 1, Priority 1).
- Configuration and Installation:** Config Status (Unknown), Enforce Firmware Version (6.4.5-b1828), System Template (default), and Revision (Total Revisions: 0).
- Sessions:** A section for viewing active sessions.

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.

<b>Host Name</b>	Sets the hostname and password for each member in the cluster.
<b>Priority (0-512)</b>	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.
<b>Management Interface Reservation</b>	Enables a dedicated interface for individual cluster member management.
<b>Session Pickup</b>	Exposes the session-pick option from the GUI.
<b>Session Pickup Connectionless</b>	Exposes the connectionless sessions from the primary FortiGate.
<b>Heartbeat Interface</b>	Sets the heartbeat <i>Interface</i> and <i>Priority</i> .
<b>Monitor Interface</b>	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*.

## 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.

### 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.



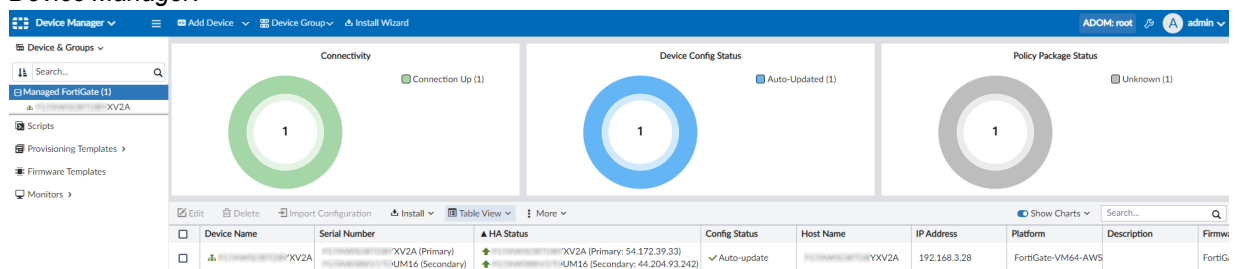


The amount of time required for FortiManager to add or remove FortiGate devices to or from the cluster depends upon the time it takes to deploy or terminate the FortiGate-VM on the cloud, and for the FortiGate clusters to resync.

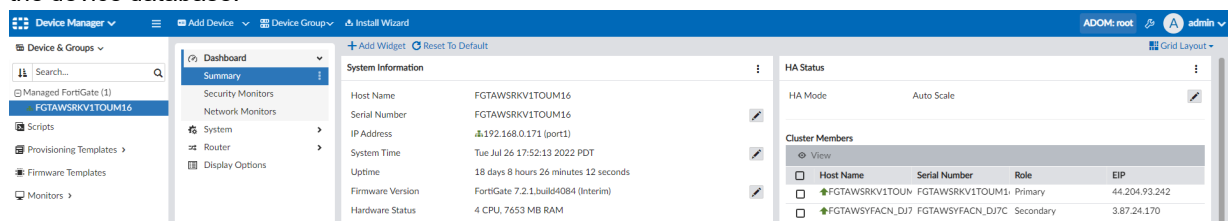
## To manage FortiGate auto-scale clusters on FortiManager:

### 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*.

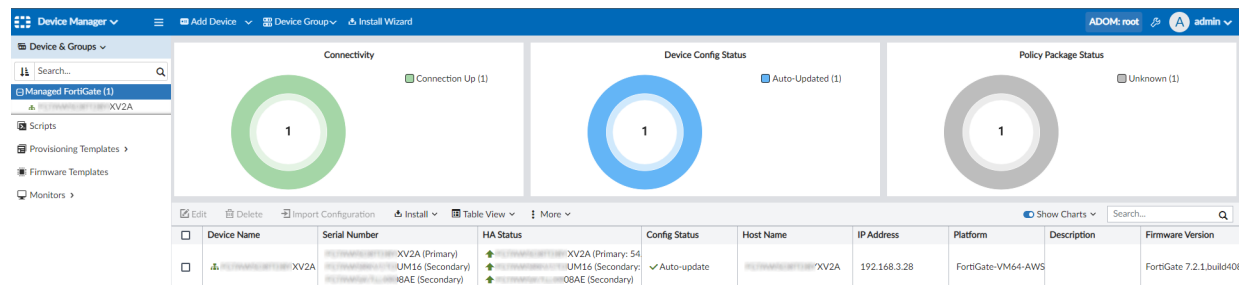


- Administrators can check the HA mode (i.e. auto-scale) along with cluster members, roles, and the elastic IP in the device database.



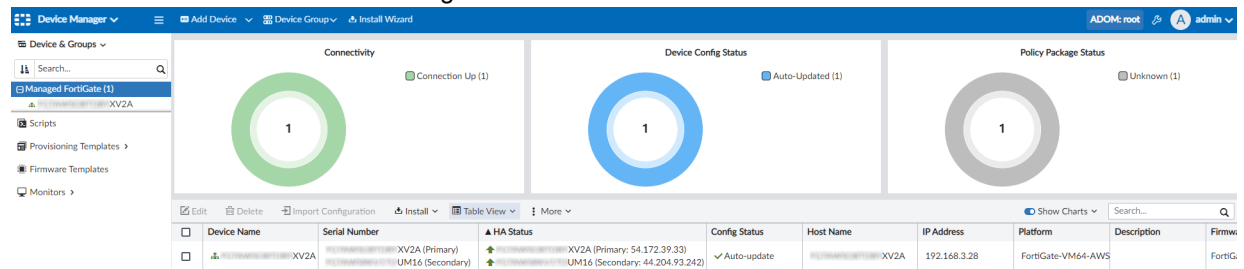
### 2. When a scale-out event occurs where the number of FortiGate devices in the cluster increases, once the newly added FortiGate becomes a part of the cluster and syncs its configuration with the cluster's Primary device, it is added to FortiManager.

On FortiManager, the device is automatically authorized and added to the existing cluster without manual intervention.



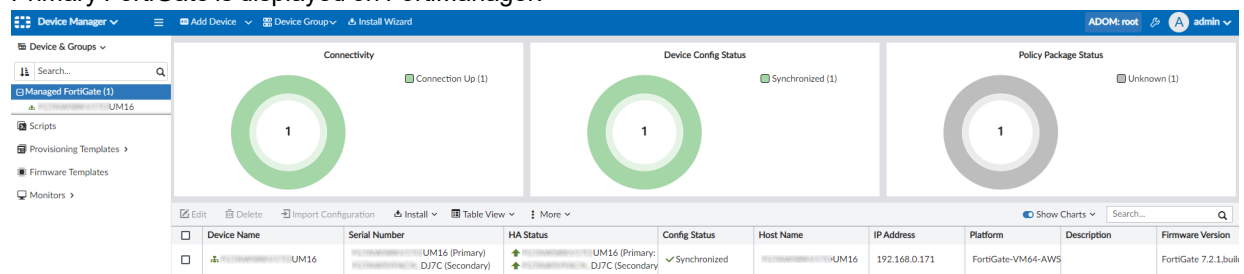
### 3. When a scale-in event occurs where the number of FortiGate devices in the cluster decreases, once the FortiGate is removed from the cluster on the cloud and the FGFM expires on the FortiManager, the FortiGate device will be

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.



## Scripts

FortiManager scripts enable you to create, execute, and view the results of scripts executed on FortiGate devices, policy packages, the ADOM database, the global policy package, 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 175](#) 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.

---

## Enabling scripts

You must enable scripts to make the *Scripts* option visible in the GUI.

### To enable scripts:

1. Go to *System Settings > Admin > Admin Settings*.
2. In the *Display Options on GUI* section, select *Show Scripts*. For more information, see [Global administration settings on page 877](#).
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:

<b>Name</b>	The user-defined script name.
<b>Type</b>	The script type.
<b>Target</b>	The script target.
<b>Comments</b>	User defined comment for the script.
<b>Last Modified</b>	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.

<b>Run Script / Run</b>	Run the selected script. See <a href="#">Run a script on page 170</a> .
<b>Schedule Script</b>	Schedule when the selected script will run. See <a href="#">Schedule a script on page 174</a> .
<b>Create New / New</b>	Create a new script. See <a href="#">Add a script on page 171</a> .
<b>Edit</b>	Edit the selected script. See <a href="#">Edit a script on page 172</a> .
<b>Delete</b>	Delete the selected script. See <a href="#">Delete a script on page 172</a> .
<b>Clone</b>	Clone the selected script. See <a href="#">Clone a script on page 172</a> .
<b>Import CLI Script / Import</b>	Import a script from your management computer. See <a href="#">Import a script on page 173</a> .
<b>Export</b>	Export the selected script as a <code>.txt</code> file to your management computer. See <a href="#">Export a script on page 173</a> .
<b>Select All</b>	Select all the scripts. This option is only available for Global Database scripts.
<b>Search</b>	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 174](#)).

### 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 179](#) 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 > Object Configurations > Scripts*. If it is not visible, enable it in the *Display Options* ([Feature visibility on page 309](#)).

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 drop-down 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 > Object Configurations > 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.

<b>Script Name</b>	Type a unique name for the script.
<b>View Sample Script</b>	This option points to the FortiManager online help.
<b>Comments</b>	Optionally, type a comment for the script.
<b>Type</b>	Specify the type of script. This option is not available for Global Database ADOM scripts.
<b>Run Script on</b>	Select the script target. This settings will affect the options presented when you go to run a script. The options include: <ul style="list-style-type: none"><li>• <i>Device Database</i></li><li>• <i>Policy Package or ADOM Database</i></li><li>• <i>Remote FortiGate Directly (via CLI)</i></li></ul> For Global Database ADOM scripts, this option is set to <i>Policy Package or ADOM Database</i> 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 174](#).

---

### 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 173](#)

Tcl scripts can be imported using the FortiManager CLI using FTP or SCP. See [Importing Tcl scripts on page 174](#)

## 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. Go to *System Settings > Dashboard* and click in the **CLI Console** widget, or connect to the FortiManager with terminal emulation software.
2. Enter the following CLI commands:
 

```
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:

<b>Devices</b>	Select the devices that the script will be run on. If required, use the search field to find the devices in the list.
<b>Enable Automatic execute after each device install</b>	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 <i>Remote FortiGate Directly (via CLI)</i> .
<b>Enable Schedule</b>	Select to schedule when the script or groups runs. This option is only available is the target is <i>Remote FortiGate Directly (via CLI)</i> .
<b>Recurring</b>	Select how frequently the script or script group will run: <ul style="list-style-type: none"> <li>• <i>One Time</i>- Set the date and time that script or group will run.</li> <li>• <i>Daily</i> - Set the time that the script or group will run everyday.</li> <li>• <i>Weekly</i> - Set the day of the week and the time of day that the script or</li> </ul>



- 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 *Device Manager > Scripts*. *Script* and *Script Group* entries are displayed in the content pane.

The following information is displayed:

<b>Name</b>	The user-defined script group name.
<b>Type</b>	The script type, for example <i>CLI Script</i> .
<b>Target</b>	The script group target.
<b>Comments</b>	User defined comment for the group.
<b>Members</b>	The scripts that are included in the script group.
<b>Last Modified</b>	The date and time the group was last modified.

The following options are available in the toolbar, or right-click menu.

<b>Create New</b>	Create a new script group.
<b>Edit</b>	Edit the selected group.
<b>Delete</b>	Delete the selected group or groups.
<b>Run Script</b>	Run the selected script group. If the target is <i>Device Database</i> or <i>Remote FortiGate Directly (via CLI)</i> , select the device or devices to run the scripts in the group on, then click <i>Run Now</i> . If the target is <i>Policy Package</i> or <i>ADOM Database</i> , select the policy package from the drop-down list, then click <i>Run Now</i> .
<b>Search</b>	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.:

<b>Script Group Name</b>	Enter a name for the script group.
<b>Comments</b>	Optionally, type a comment for the script group.
<b>Type</b>	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
    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 ikelproposal 3des-sha1 3des-md5 ...
    set ikeldhgroup XXXX
    set ikelkeylifesecc 28800
    set ikelmode aggressive|main
    set ikeldpd enable|disable
    set ikelnat traversal enable|disable
    set ikelnat keepalive 10
    set ike2proposal 3des-sha1 3des-md5
    set ike2dhgroup 5
    set ike2keylifetype seconds|kbyte|both
    set ike2keylifesecc 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 authusrgroup 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 170](#).
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 785](#).

## 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.

Error messages will help you determine the causes of any CLI scripting problems, and fix them. For more information, see [Error Messages on page 185](#).

The troubleshooting tips section provides some suggestions on how to quickly locate and fix problems in your CLI scripts. For more information, see [Troubleshooting Tips on page 185](#).

## CLI script samples

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.

Getting information remotely is one of the main purposes of your FortiManager system, 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.

To view interface information for port1:	
<b>Script</b>	<code>show system interface port1</code>
<b>Output</b>	<pre> 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 </pre>
<b>Variations</b>	Remove the interface name to see a list that includes all the interfaces on the FortiGate device including virtual interfaces such as VLANs.
<b>Note</b>	<p>This script does not work when run on a policy package.</p> <p>If the preceding script is used to be run on the FortiGate Directly (via CLI) or run on device database on a FortiGate has the VDOM enabled. The script will have be modified to the following:</p> <pre> config global   show system interface port1 end </pre> <p>Since running on device database does not yield any useful information.</p> <p>View the log of script running on device: FortiGate-VM64-70</p> <pre> ----- 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 ----- </pre> <p>The script should be run on the FortiGate Directly (via CLI).</p> <p>View the log of script running on device: FortiGate-VM64-70</p> <pre> ----- Executing time: 2013-10-15 13:52:02 ----- Starting log (Run on device) </pre>

```

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 -----

```

To view the entries in the static routing table. To get any useful information, the script has to be re-written for the following if the VDOM is enabled for FortiGate and has to be run on the FortiGate Directly (via CLI).

```

config vdom
    edit root
        show route static
    next
end

```

Here is a sample run of the preceding script running on the FortiGate Directly (via CLI).

View the log of script running on device: FortiGate-VM64-70

```

----- 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 -----

```

#### To view the entries in the static routing table:

<b>Script</b>	show route static
<b>Output</b>	<pre> 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 </pre>



	<pre>         next       end </pre>
<b>Variations</b>	none
<b>View information about all the configured FDN servers on this device:</b>	
<b>Script</b>	<pre> config global   diag debug rating end </pre>
<b>Output</b>	<p>View the log of script running on device: FortiGate-VM64</p> <pre> ----- 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 ----- </pre>
<b>Variations</b>	<p>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.</p> <p>For an authorized FortiGate device without a valid license, the output would be similar to:</p> <pre> 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 ** </pre>

Setting FortiGate device information with CLI scripts gives you access to more settings and allows you more fine grained control than you may have in the *Device Manager*. Also CLI commands 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 account profile called `policy_admin` allowing read-only access to policy related areas:

<b>Script</b>	<pre> config global   config system accprofile     edit "policy_admin"       set fwgrp read       set loggrp read     end   end end </pre>
---------------	--

```

        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.

With the introduction of global objects/security console (global database), you can run a CLI script on 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
    end

```

- Running a CLI script on the global database

```

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

```

## 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.



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
    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:**

```

----- Executing time: 2013-10-21 09:58:06 -----
Starting log (Run on device)

FortiGate-VM64 #

This machine is a VM64 platform.
It is running version v5.0 of FortiOS.
The firmware is build# 0228.
S/N: FGVM02Q105060070
This machine is called FortiGate-VM64

----- The 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 {$status(version) == 5.0} {
    # follow the version 5.0 commands
} elseif {$status(version) == 5.0} {
    # follow the version 5.0 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"
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 miss



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 `diffservcode_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 v5.00
#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 "v5.0"} {
    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: 2013-10-21 16:21:43 -----
Starting log (Run on device)
```

```
FortiGate-VM64 #
config global
FortiGate-VM64 (global) # get system performance status

CPU states: 0% user 0% system 0% nice 90% idle
CPU0 states: 0% user 0% system 0% nice 90% idle
CPU1 states: 0% user 0% system 0% nice 90% idle
Memory states: 73% used
Average network usage: 0 kbps in 1 minute, 0 kbps in 10 minutes, 0 kbps in 30 minutes
Average sessions: 1 sessions in 1 minute, 2 sessions in 10 minutes, 2 sessions in 30 minutes
```

```
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in
    last 10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 6 days, 1 hours, 34 minutes

FortiGate-VM64 (global) # end
FortiGate-VM64 #
----- The end of log -----

----- Executing time: 2013-10-21 16:16:58 -----
```

**Example: Configure common global settings.****Script:**

```
#!/
#Run on FortiOS v5.00
#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
    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: 2013-10-22 09:12:57 -----
Starting log (Run on device)

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
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 #
----- The end of log -----

```

**Example: Configure syslogd settings and filters.****Script:**

```

#!
#Run on FortiOS v5.00
#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} {csv 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 {{attack enable} {email enable} {severity} {traffic enable} {virus
        disable}
{web 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" "# "]
}
#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)

```

FortiGate-VM64 # config global
FortiGate-VM64 (global) # config log syslogd2 setting
FortiGate-VM64 (setting) # set status enable
FortiGate-VM64 (setting) # set csv enable
FortiGate-VM64 (setting) # set facility alert
FortiGate-VM64 (setting) # unset port
FortiGate-VM64 (setting) # set server 1.1.1.2
FortiGate-VM64 (setting) # end

FortiGate-VM64 (global) # config log syslogd2 filter
FortiGate-VM64 (filter) # set attack enable
FortiGate-VM64 (filter) # set email enable
FortiGate-VM64 (filter) # unset severity

```

```
FortiGate-VM64 (filter) # set traffic enable
FortiGate-VM64 (filter) # set virus disable
FortiGate-VM64 (filter) # set web enable
FortiGate-VM64 (filter) # end
FortiGate-VM64 (global) #
```

----- The 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 localid 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
get_sys_status sys_status
set localid $sys_status(Hostname)
#config system fortianalyzer---begin
fgt_cmd "config global"
fgt_cmd "config log fortianalyzer$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)
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 v5.00
#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"
}
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 disk space 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:

<b>Script</b>	<pre>#! set somefile [open "tcl_test" w] puts \$somefile "Hello, world!" close \$somefile</pre>
---------------	---

To read from a file:

<b>Script</b>	<pre>#! set otherfile [open "tcl_test" r] while {[gets \$otherfile line] &gt;= 0} {   puts [string length \$line] } close \$otherfile</pre>
---------------	---

<b>Output</b>	<pre>Hello, world!</pre>
---------------	--------------------------

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.
- 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:

<b>Syntax</b>	<code>puts [exec_ondb "/adom/&lt;adom_name&gt;/pkg/&lt;pkg_fullpath&gt;" "embedded cli commands" "# "]</code>
<b>Usage</b>	<code>puts [exec_ondb "/adom/52/pkg/default" " config firewall address edit port5_address next end " "# "]</code>

### Example 2:

Run the Tcl script on the current ADOM database for a specify policy package. For example, creating a new policy and object:

<b>Syntax</b>	<code>puts [exec_ondb "/adom/./pkg/&lt;pkg_fullpath&gt;" "embedded cli commands" "# "]</code> or <code>puts [exec_ondb "/pkg/&lt;pkg_fullpath&gt;" "embedded cli commands" "# "]</code>
<b>Usage</b>	<code>puts [exec_ondb "/adom/./pkg/default" " config firewall address edit port5_address next</code>

```
end
" "# "]"
```

**Example 3:**

Run Tcl script on a specific device in an ADOM:

<b>Syntax</b>	<code>puts [exec_ondb "/adom/&lt;adom_name&gt;/device/&lt;dev_name&gt;" "embedded cli commands" "# "]</code>
<b>Usage</b>	<pre>puts [exec_ondb "/adom/v52/device/FGT60CA" " config global config system global set admintimeout 440 end end " "# "]</pre>

**Example 4:**

Run Tcl script on current devices in an ADOM:

<b>Syntax</b>	<code>puts [exec_ondb "/adom/&lt;adom_name&gt;/device/." "embedded cli commands" "# "]</code>
<b>Usage</b>	<pre>puts [exec_ondb "/adom/v52/device/." " config global config system global set admintimeout 440 end end " "# "]</pre>



`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 201](#)
- [Fabric authorization templates on page 205](#)
- [System templates](#)
- [IPsec tunnel templates on page 212](#)
- [SD-WAN templates on page 231](#)
- [SD-WAN overlay templates on page 245](#)
- [Static route templates on page 262](#)
- [BGP templates on page 264](#)

- [Certificate templates](#)
- [Threat Weight templates](#)
- [CLI templates on page 270](#)
- [NSX-T service templates on page 277](#)
- [Export and import provisioning template configurations on page 280](#)

## 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
- Post-Run 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 201](#).
2. Assign the template group to one or more devices or to one or more device groups. See [Assigning template groups on page 203](#).
3. Edit template groups as needed. See [Editing template groups on page 204](#).

You can also delete template groups. See [Deleting template groups on page 205](#).

## 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.

Create New Template Group

Name

Description

Provisioning Templates

Click here to edit

\* Only one template can be selected for each template type.

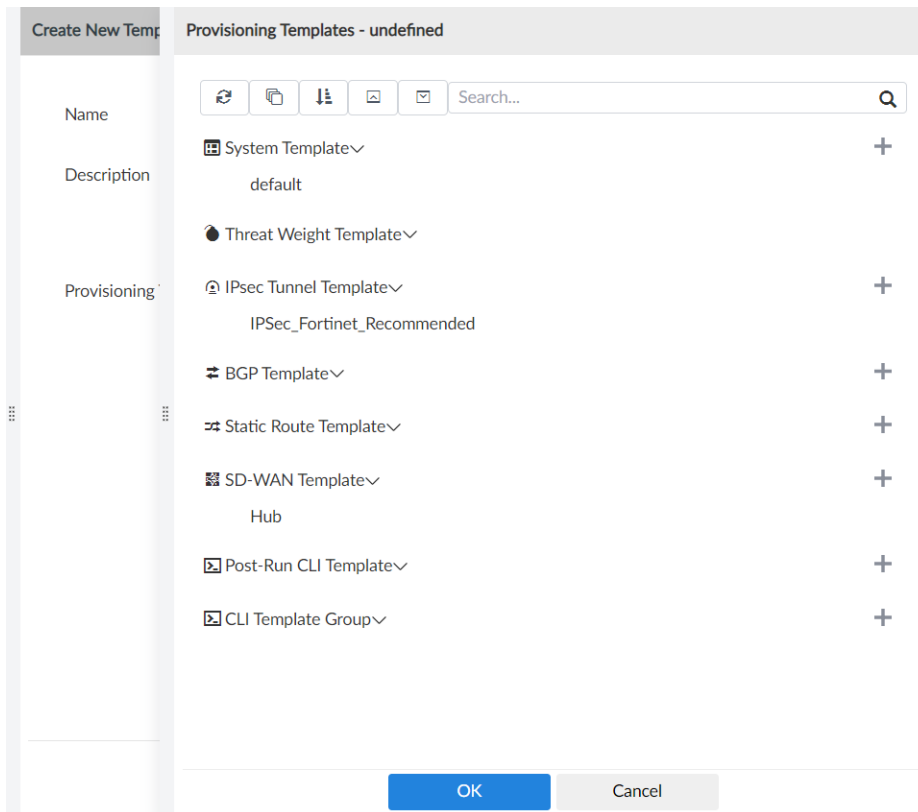
OK Cancel

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.



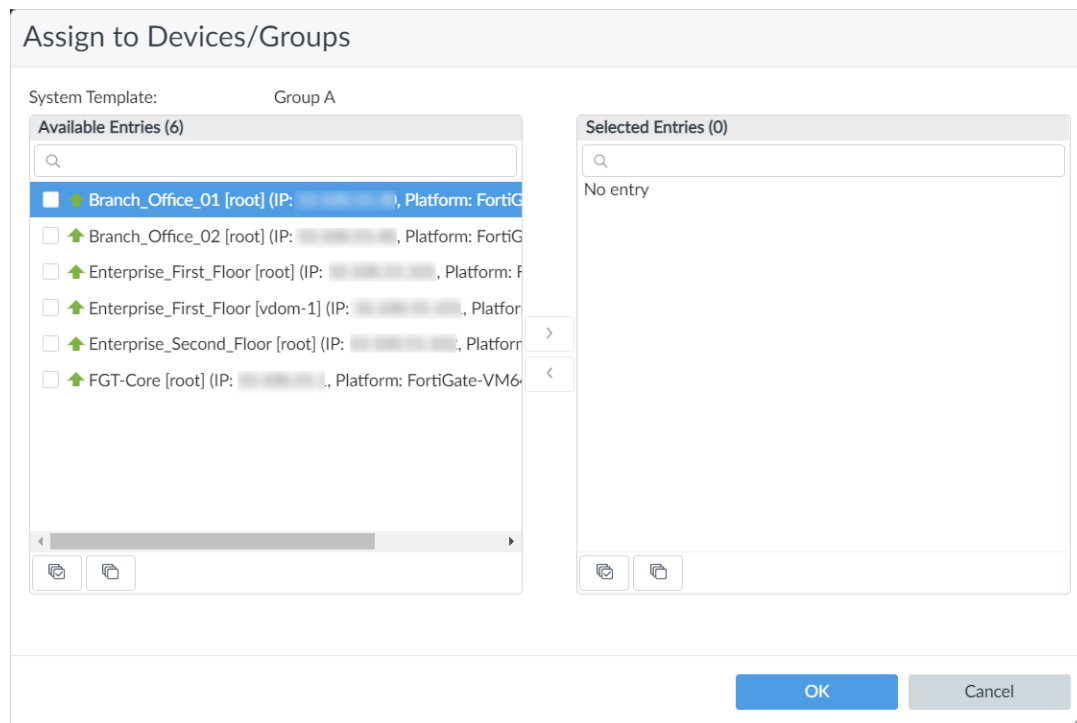
6. Select one or more templates, and click **OK**.  
You can only select one template for each template type.  
The templates are selected.
7. Click **OK**.  
The template group is created.

## 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:

<b>Create New</b>	Create a new template.
<b>Edit</b>	Edit a template. Right-click a template, and select <i>Edit</i> .
<b>Delete</b>	Delete a template. Right-click a template, and select <i>Delete</i> .
<b>Generate</b>	Generate the Fabric devices using the template.

### Fabric authorization template workflow

1. Create the Fabric authorization template.
2. Generate the template and select the required target FortiGate device(s).  
FortiManager will create or update the list of Fabric devices (FortiAP, FortiSwitch, and FortiExtender) on the device database according to the template configuration.
3. The device's *Config Status* will be set to *Modified*. The newly created entries can be modified/deleted at this stage as required.
4. Perform an install on the target FortiGate devices so the Fabric devices are pushed to the targets.

### 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.

Create New Fabric Authorization Template

Name

Fabric\_Template

Description

FortiAP

☒ Enable Wireless Controller

Platform 1

Prefix

FAP14C (FortiAP-14C)

Number of Devices

3

+

FortiSwitch

☐ Enable Switch Controller

FortiExtender

☐ Enable Extender Controller

OK

Cancel

3. Enter the following information, then click *OK* to create the certificate template:

<b>Name</b>	Enter a name for the Fabric authorization template.
<b>Description</b>	Optionally, provide a description for the template.
<b>FortiAP</b>	
<b>Enable Wireless Controller</b>	Toggle to enable wireless controllers. Additional settings are available once this option is selected.
<b>Platform 1</b>	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.
<b>Prefix</b>	Select the serial number prefix for the selected devices from the dropdown menu.



<b>Number of Devices</b>	Select the number of devices to pre-authorize.
<b>FortiSwitch</b>	
<b>Enable Switch Controller</b>	Toggle to enable switch controllers. Additional settings are available once this option is selected.
<b>Platform</b>	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.
<b>Prefix</b>	Select the serial number prefix for the selected devices from the dropdown menu.
<b>Number of Devices</b>	Select the number of devices to pre-authorize.
<b>FortiLink Interface</b>	Type the interface for FortiLink.
<b>FortiExtender</b>	
<b>Enable Extender Controller</b>	Toggle to enable extender controllers. Additional settings are available once this option is selected.
<b>Platform 1</b>	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.
<b>Prefix</b>	Select the serial number prefix for the selected devices from the dropdown menu.
<b>Number of Devices</b>	Select the number of devices to pre-authorize.
<b>Extension Type</b>	Select the extension type as either <i>WAN Extension</i> or <i>LAN Extension</i> .

#### 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*.
5. When the real devices comes 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.
6. 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.

## 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 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 settings in the widget or import settings from a specific device.

Go to the *Device Manager > Provisioning Templates > System Templates > default* pane to configure system templates.



Some settings may not be available in all ADOM versions.

After making changes in a widget, click *Apply* to save your changes.

To close a widget, click the *Close* icon in the widget's top right.

To select which widgets to display, click *Toggle Widgets* and select which widgets to display.

To import settings from another device, click the *Import* icon in the widget's top right and select the device from which to import.

The following widgets and settings are available:

Widget	Description
<b>DNS</b>	Primary DNS Server, Secondary DNS Server, Local Domain Name.
<b>NTP Server</b>	Synchronize with NTP Server and Sync Interval settings. You can select to use the FortiGuard server or specify one or more other servers.
<b>Alert Email</b>	SMTP Server settings including server, authentication, SMTP user ID, and password.
<b>Admin Settings</b>	Web Administration Ports, Timeout Settings, and Web Administration.

Widget	Description
<b>SNMP</b>	SNMP v1/v2 and SNMP v3 settings. In the toolbar, you can select to create, edit, or delete the record.  To create a new SNMP, click <i>Create New</i> and specify the community name, hosts, queries, traps, and SNMP events.
<b>Replacement Messages</b>	You can customize replacement messages. Click <i>Import</i> to select a device and the objects to import.
<b>FortiGuard</b>	Select <i>Enable FortiGuard Security Updates</i> to retrieve updates from FortiGuard servers or from this FortiManager. You can define multiple servers and specify <i>Update</i> , <i>Rating</i> , or <i>Updates and Rating</i> . You can also select <i>Include Worldwide FortiGuard Servers</i> .
<b>Log Settings</b>	Select <i>Send Logs to FortiAnalyzer/FortiManager</i> and/or <i>Send Logs to Syslog</i> . If selected, enter the requisite information for the option.
<b>Interface</b>	Zone and interface settings. In the toolbar, you can select to create, edit, or delete the record.  By default the <i>Interface</i> widget is hidden. From the <i>Toggle Widgets</i> menu, select <i>Interface</i> to display the <i>Interface</i> widget.  To create a new interface, click <i>Create New</i> 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 798](#).

### 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.

<div> + Create New Edit Delete Assign to Device/Group More Column Settings </div>					Search...
<input type="checkbox"/>	#	Name	Assigned to Device/Group	Description	
<input type="checkbox"/>	1	default	0 Devices in Total		

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.

Post Action Preview

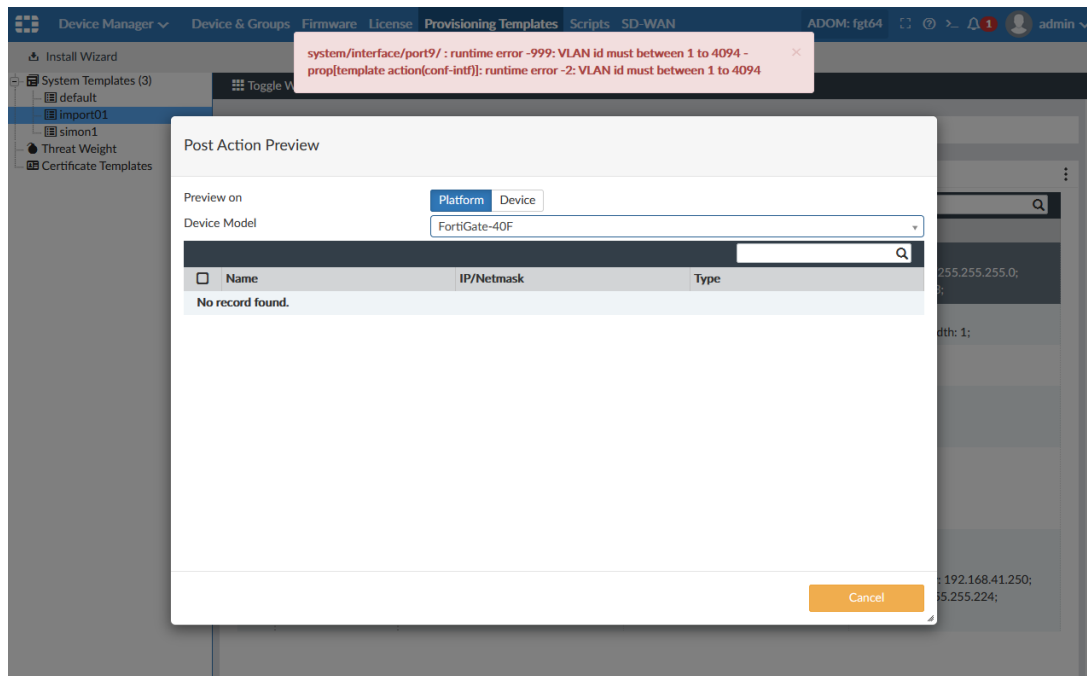
Preview on Platform Device

Device Model FortiOS-VM64

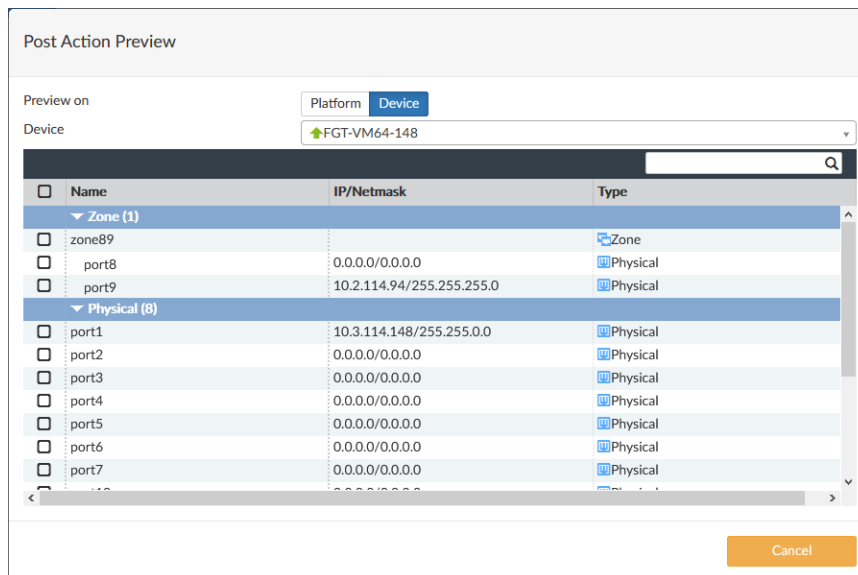
<input type="checkbox"/>	Name	IP/Netmask	Type
<b>Zone (1)</b>			
<input type="checkbox"/>	zone89		Zone
<input type="checkbox"/>	port8	0.0.0.0/0.0.0.0	Physical
<input type="checkbox"/>	port9	10.2.114.94/255.255.255.0	Physical
<b>Physical (8)</b>			
<input type="checkbox"/>	mgmt	0.0.0.0/0.0.0.0	Physical
<input type="checkbox"/>	port1	0.0.0.0/0.0.0.0	Physical
<input type="checkbox"/>	port2	0.0.0.0/0.0.0.0	Physical
<input type="checkbox"/>	port3	0.0.0.0/0.0.0.0	Physical
<input type="checkbox"/>	port4	0.0.0.0/0.0.0.0	Physical
<input type="checkbox"/>	port5	0.0.0.0/0.0.0.0	Physical
<input type="checkbox"/>	port6	0.0.0.0/0.0.0.0	Physical
<input type="checkbox"/>	port7	0.0.0.0/0.0.0.0	Physical
<b>VLAN (1)</b>			
<input type="checkbox"/>	vlan91	0.0.0.0/0.0.0.0	VLAN
<b>Aggregate (1)</b>			
<input type="checkbox"/>	aggr57	0.0.0.0/0.0.0.0	Aggregate
<b>Tunnel (1)</b>			
<input type="checkbox"/>	ssl.root	0.0.0.0/0.0.0.0	Tunnel

Cancel

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

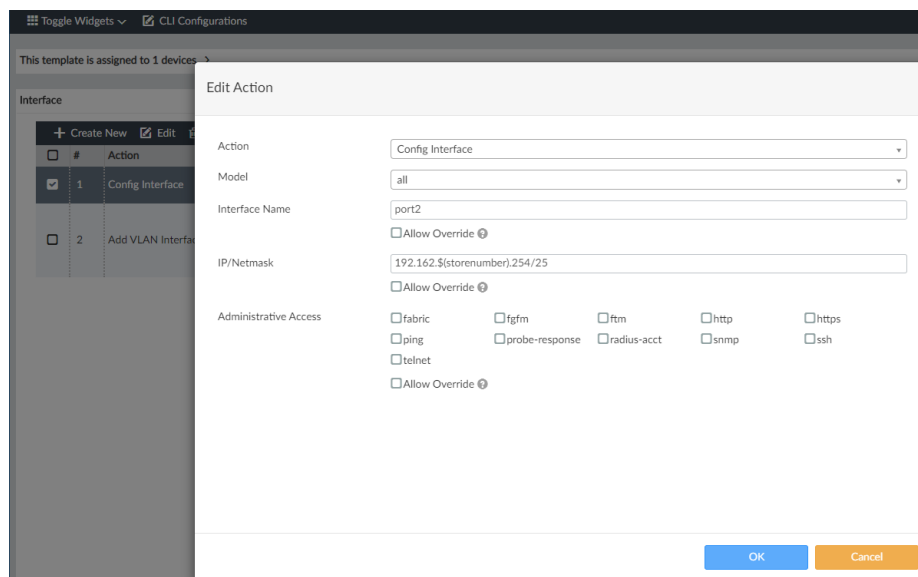
You can use metadata variables in interface templates.

For information about creating a meta field, see [ADOM-level metadata variables on page 437](#).

### 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 213.](#)
- [Creating new IPsec VPN templates on page 215](#)
- [Assigning IPsec VPN templates on page 217.](#)
- [Installing IPsec VPN configuration on page 217.](#)
- [Verifying IPsec template configuration status on page 218.](#)
- [Verifying IPsec VPN tunnel status on page 218.](#)

- [Un-assigning IPsec templates on page 218.](#)
- [IPsec tunnel template example on page 219.](#)

## 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 437](#).

The following IPsec recommended templates are available.

Template Name	Description
<b>HUB_IPSec_Recommended</b>	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 <i>Dynamic</i> for <i>Remote Devices</i> .
<b>Branch_IPSec_Recommended</b>	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.
<b>IPSec_Fortinet_Recommended</b>	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 437](#).

6. (Optional) Once a template has been created, it can be added to a template group. See [Template groups on page 201](#)
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.

<b>Template Name</b>	Enter a name for the template.
<b>Enable ADVPN</b>	Optionally, toggle this setting to enable Auto Discovery VPN (ADVPN).
<b>Outgoing Interface</b>	Enter the outgoing interface. This is the physical port that the branch devices will connect to.
<b>IPv4 Start IP</b>	Enter the first usable IP address in the range.
<b>IPv4 End IP</b>	Enter the last usable IP address in the range.
<b>IPv4 Netmask</b>	Enter the IPv4 netmask.
<b>Pre-shared Key</b>	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.

<b>Template Name</b>	Enter a name for the template.
<b>Enable ADVPN</b>	Optionally, enable or disable Auto Discovery VPN (ADVPN).
<b>Outgoing Interface</b>	Enter the outgoing interface. This is the physical port that the branch devices will use to connect to the HUB.
<b>Local ID</b>	Enter a Local ID. This is used by the HUB to identify the connecting device.
<b>Remote Gateway</b>	Enter the IP address of the HUB interface that the Branch will connect to.
<b>Pre-shared Key</b>	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.

<b>Template Name</b>	Enter a name for the template.
<b>Outgoing Interface</b>	Enter the outgoing interface. This is the physical port that the branch devices will connect to.
<b>Remote Gateway</b>	Enter the IP address of the destination device's interface that the assigned FortiGates will connect to.
<b>Pre-shared Key</b>	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 437](#).

Setting	Value/Description
<b>Tunnel Name</b>	Enter the name of the IPsec tunnel.
<b>Routing</b>	<i>Automatic</i> : Static routes to remote subnet will be created. See <a href="#">Remote Subnet on page 216</a> . <i>Manual</i> : Routes will not automatically created.
<b>Remote Device</b>	<i>IP Address</i> : Select when you know the IP address of the VPN tunnel destination. <i>Dynamic DNS</i> : Select when you will provide a FQDN for the VPN tunnel destination. <i>Dynamic</i> : 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.
<b>Remote Gateway (IP Address)</b>	Enter the IP address of the VPN tunnel destination. Only available when <i>IP Address</i> is selected.
<b>Remote Gateway (FQDN)</b>	Enter the FQDN of the VPN tunnel destination. Only available when <i>Dynamic DNS</i> is selected.
<b>IPv4 Start IP</b>	Enter the first usable IP address assigned to connecting dial-up devices.
<b>IPv4 End IP</b>	Enter the last usable IP address assigned to connecting dial-up devices.
<b>IPv4 Netmask</b>	Define the netmask for the IP addresses assigned to connecting dial-up devices.
<b>Outgoing Interface</b>	Define the interface used to establish the VPN tunnel.
<b>Local ID</b>	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.
<b>Network Overlay</b>	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.
<b>Remote Subnet</b>	Enter one or more remote subnets, with netmask. This field is available when <i>Automatic</i> routing is selected. This subnet is used to generate a static route.
<b>Proposal</b>	Define the cipher suites offered when negotiating the VPN tunnel settings.
<b>FEC Health Check</b>	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.
<b>Authentication Method</b>	<i>Pre-shared Key</i> : Alphanumeric key used for device authentication. <i>Signature</i> : Select a certificate to be used for authentication, including the Peer Certificate CA.

Setting	Value/Description
<b>Tunnel Interface Setup</b>	Configure the IP or remote IP for the tunnel to use in the IPsec template.
<b>Phase 2 Interface</b>	Click <i>Create New</i> to define the parameters for the phase 2 interface.
<b>Advanced Options</b>	Expand to access and set a number of advanced options.

- 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:

- Go to *Device Manager > Provisioning Templates > IPsec Tunnel Templates*.
- Click on the template name from the tree menu at the left.
- Click *Assign to Device/Group* from the toolbar.
- 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.
- 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:

- Go to *Policy & Objects > Policy Packages > Firewall Policy*.
- Click *Create New* from the toolbar. The *Create New Firewall Policy* pane appears.
- Create two firewall policies for traffic between the normalized interface and *HQ* site.

+ Create New ▾ Edit ▾ Delete Section ▾ Policy Lookup Column Settings ▾ View Mode ▾								
<input type="checkbox"/>	#	Name	From	To	Source	Destination	Schedule	Service
<input type="checkbox"/>	1		IPsecLAN	toHub	all	all	always	ALL
<input type="checkbox"/>	2		toHub	IPsecLAN	all	all	always	ALL

- Click *Install > Install Wizard* from the toolbar. The *Install Wizard* dialog appears.
- Continue with the policy installation on the appropriate devices.
- 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.

Edit          Delete          Import Policy          Install          More          Column Settings				
<input type="checkbox"/>	▲ Device Name	Config Status	Policy Package Status	IPSec Template
<input type="checkbox"/>	📶 Branch-A	✓ Synchronized	✓ spoke	✓ BranchTemplate
<input type="checkbox"/>	📶 Branch-B	✓ Synchronized		
<input type="checkbox"/>	🌐 root [NAT] (Management)	✓ Synchronized	✓ default	
<input type="checkbox"/>	🌐 vd_1 [NAT]	⚠ Modified	✓ spoke	⚠ BranchTemplate
<input type="checkbox"/>	📶 HQ	✓ Synchronized	✓ DClient-hub	

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.

Bring Tunnel Up          Bring Tunnel Down          Refresh          Column Settings							
<input type="checkbox"/>	Status	Device	P1 Name	Type	Remote Gateway	Uptime	P2 Name
<input checked="" type="checkbox"/>	Up	Branch-A[root]	toHub	automatic	101.71.61.1	32s	toHub
<input type="checkbox"/>	Up	Branch-B[vd_1]	toHub	automatic	101.71.61.1	31s	toHub

## Un-assigning IPsec templates

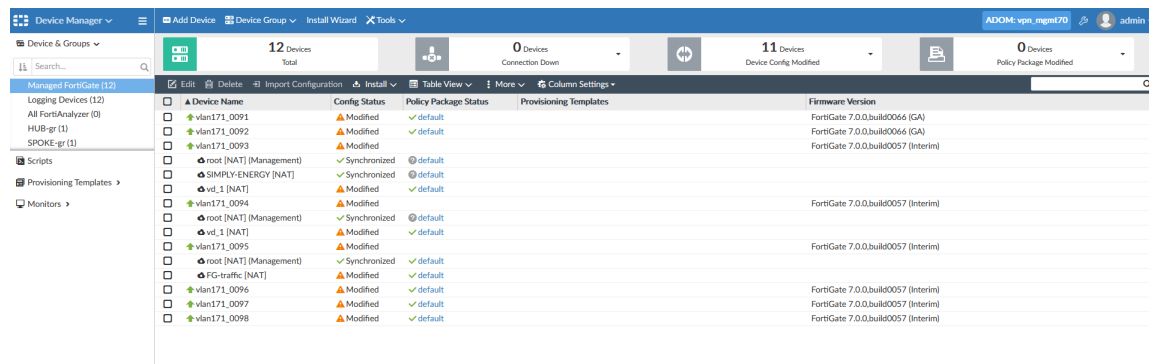
When you un-assign an IPsec template from a device, FortiManager modifies the configuration for the affected devices. When you install the modified configuration to devices, FortiManager automatically uninstalls the configuration (phase1 and phase2 interfaces) generated by the IPsec template from the 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.

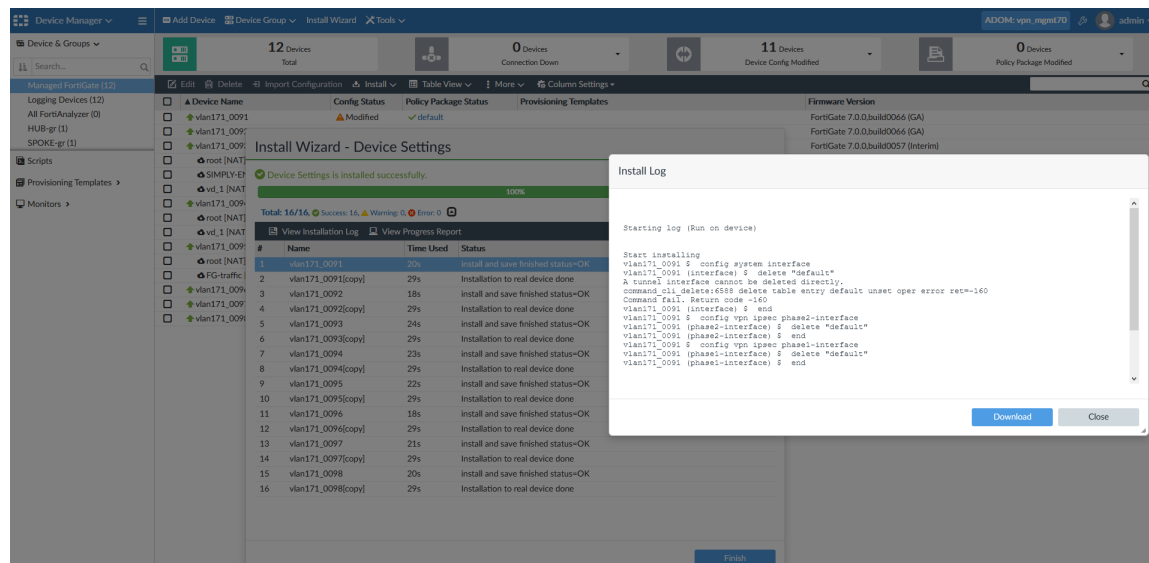
## To un-assign IPsec templates:

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**:



Device Name	Config Status	Policy Package Status	Provisioning Templates	Firmware Version
vlan171_0091	Modified	default		FortiGate 7.0.0.build40066 (GA)
vlan171_0092	Modified	default		FortiGate 7.0.0.build40066 (GA)
vlan171_0093	Modified	default		FortiGate 7.0.0.build40057 (Interim)
root (NAT) (Management)	Synchronized	default		
SIMPLY-ENERGY (NAT)	Synchronized	default		
vd_1 (NAT)	Modified	default		
vlan171_0094	Modified	default		FortiGate 7.0.0.build40057 (Interim)
root (NAT) (Management)	Synchronized	default		
vd_1 (NAT)	Modified	default		
vlan171_0095	Modified	default		FortiGate 7.0.0.build40057 (Interim)
root (NAT) (Management)	Synchronized	default		
FG-traffic (NAT)	Modified	default		
vlan171_0096	Modified	default		FortiGate 7.0.0.build40057 (Interim)
vlan171_0097	Modified	default		FortiGate 7.0.0.build40057 (Interim)
vlan171_0098	Modified	default		FortiGate 7.0.0.build40057 (Interim)

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.



#	Name	Time Used	Status
1	vlan171_0091	29s	Install and save finished status=OK
2	vlan171_0091(copy)	29s	Installation to real device done
3	vlan171_0092	18s	install and save finished status=OK
4	vlan171_0092(copy)	29s	Installation to real device done
5	vlan171_0093	24s	install and save finished status=OK
6	vlan171_0093(copy)	29s	Installation to real device done
7	vlan171_0094	23s	install and save finished status=OK
8	vlan171_0094(copy)	29s	Installation to real device done
9	vlan171_0095	22s	install and save finished status=OK
10	vlan171_0095(copy)	29s	Installation to real device done
11	vlan171_0096	18s	install and save finished status=OK
12	vlan171_0096(copy)	29s	Installation to real device done
13	vlan171_0097	21s	install and save finished status=OK
14	vlan171_0097(copy)	29s	Installation to real device done
15	vlan171_0098	20s	install and save finished status=OK
16	vlan171_0098(copy)	29s	Installation to real device done

## IPsec tunnel template example

The following example demonstrates the IPsec template features with the following assumptions:

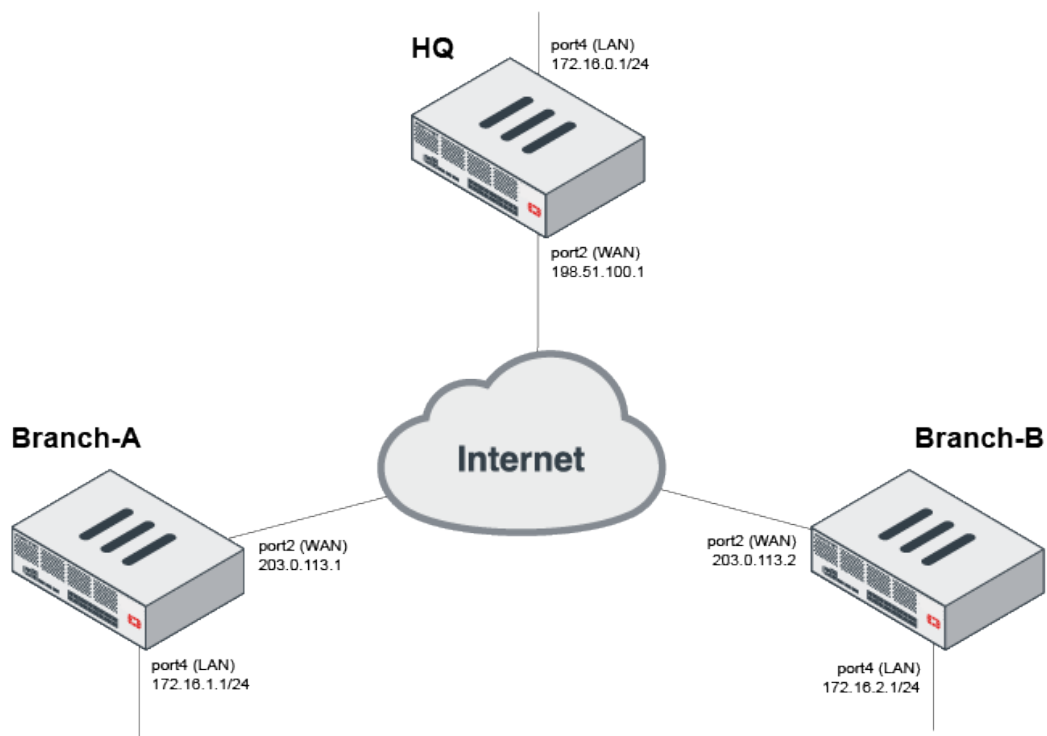
- All three FortiGates are added in FortiManager without prior configuration.
  - The branch FortiGates are added to a *Branches* device group. See [Adding custom device groups on page 94](#).
  - The hub *HQ* device is added to a *HUB* device group.
- Each FortiGate uses *port2* as the WAN and *port4* 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.
- 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 437](#).
  - 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.

Edit Metadata Variable Mapping - Branch-A(global) ✖

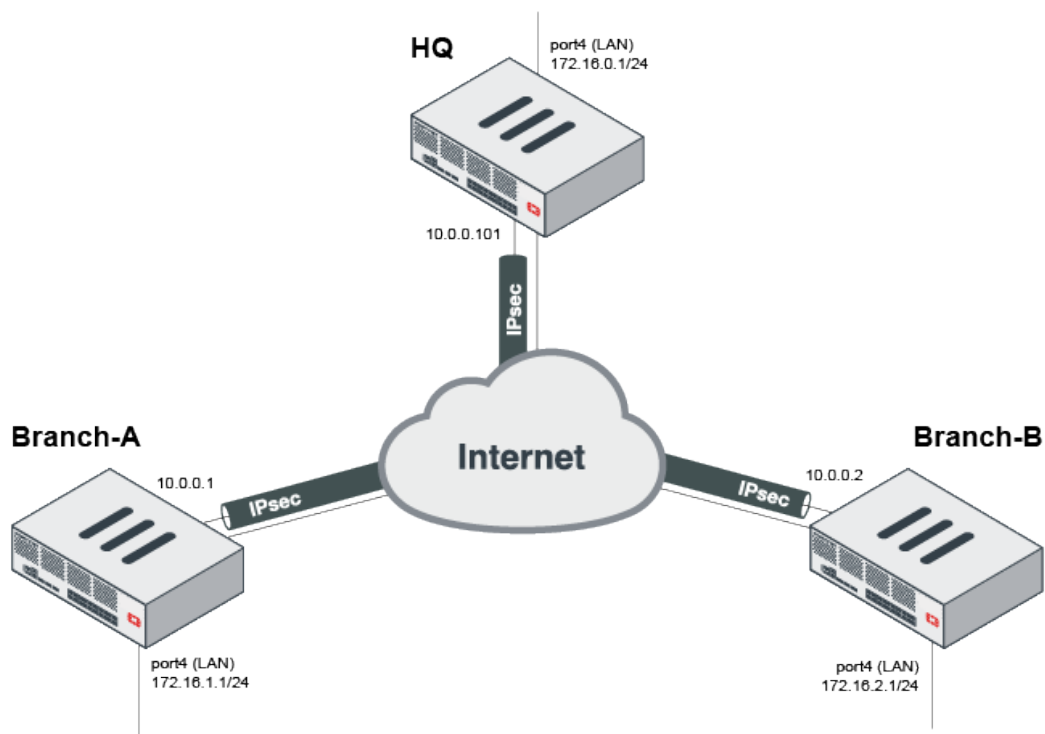
#	Variable Name	Mapping Value	Default Value
1	<code>\$(branch_id)</code>	1	

OK
Cancel

- 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.



### Activate HUB\_IPsec\_Recommended

Template Name	ACME_HUB
Enable ADVPN	<input type="checkbox"/>
<b>VPN1</b> <span>▼</span>	
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	..... <span>ⓧ</span> <span>👁</span>



*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

Template Name

Enable ADVPN ☐

**HUB1-VPN1** ▼

Outgoing Interface

Local ID

Remote Gateway

Pre-shared Key

- Click **OK** to save.
- Edit the newly created template, then edit the *HUB1-VPN1* tunnel.
- Change *Routing* from *Manual* to *Automatic*
- Under *Remote Subnet*, enter `172.16.0.0/255.255.255.0`.
- Click **OK** to save.

## Assigning templates to devices and groups

### To assign templates to devices:

- In *Device Manager > Provisioning Templates > IPsec Tunnel Templates*, Right click `ACME_BRANCH` and click *Assign to Devices/Groups*.
- Select *Branches* and move it to *Selected Entries*, then click **OK**.

## Assign to Devices/Groups

\_IPSEC Template: ACME\_BRANCH

**Available Entries (4)**

- ☐ HUB
- ☐ Branch-A [root] (IP: 192.168.2.2, Platform: FortiGate-V)
- ☐ Branch-B [root] (IP: 192.168.2.3, Platform: FortiGate-V)
- ☐ HQ [root] (IP: 192.168.2.1, Platform: FortiGate-VM64)

**Selected Entries (1)**

- ☐ Branches

3. Repeat the same procedure to assign the HUB device group to ACME\_HUB.

**Device Manager** Install Wizard

Name	Assigned to Device/Group
<input type="checkbox"/> HUB_IPsec_Recommended	0 Devices in Total
<input type="checkbox"/> BRANCH_IPsec_Recommended	0 Devices in Total
<input type="checkbox"/> IPsec_Fortinet_Recommended	0 Devices in Total
<input type="checkbox"/> ACME_BRANCH	2 Devices in Total <a href="#">View Details &gt;</a> Branches (2)
<input type="checkbox"/> ACME_HUB	1 Device in Total <a href="#">View Details &gt;</a> HUB (1)

**Device & Groups** >  
**Scripts**  
**Provisioning Templates** >  
 Template Groups  
 Fabric Authorization Temp...  
 System Templates  
**IPsec Tunnel Templates**  
 SD-WAN Templates  
 SD-WAN Overlay Templat...  
 Static Route Templates  
 BGP Templates  
 IPS Template  
 Certificate Templates  
 Threat Weight  
 CLI Templates  
 NSX-T Service Templates  
**Firmware Templates**  
**Monitors** >

## 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 > Object Configurations > Normalized Interface > 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 > Object Configurations > Normalized Interface > 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 > Object Configurations > Normalized Interface > 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 > Object Configurations > Firewall 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.

Edit Firewall Address

Name
Branch\_LAN

Color
4

Type
Subnet

IP/Netmask
172.16.0.0/255.255.0.0
Resolve from name

Interface
any

Static Route Configuration

Comments

Add To Groups

Advanced Options >

Per-Device Mapping

+ Create New
Edit
Delete

Search...

<input type="checkbox"/>	Mapped Device	Details	
<input type="checkbox"/>	Branch-B(root)	IP/Netmask: 172.16.2.0,255.255.255.0	
<input type="checkbox"/>	Branch-A(root)	IP/Netmask: 172.16.1.0,255.255.255.0	

### 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.

Policy Packages											
<div><div><div><div><div></div><div>Create New</div></div><div><div></div><div>Edit</div></div><div><div></div><div>Delete</div></div><div><div></div><div>Section</div></div><div><div></div><div>Policy Block</div></div><div><div></div><div>Policy Lookup</div></div><div><div></div><div>Collapse All</div></div><div><div></div><div>Column Settings</div></div><div><div></div><div>View Mode</div></div><div><div></div><div></div><div></div></div></div></div></div>											
<div><div></div><div>Search...</div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div>#</div></div>	<div><div></div><div>Name</div></div>	<div><div></div><div>From</div></div>	<div><div></div><div>To</div></div>	<div><div></div><div>Source</div></div>	<div><div></div><div>Destination</div></div>	<div><div></div><div>Schedule</div></div>	<div><div></div><div>Service</div></div>	<div><div></div><div>Users</div></div>	<div><div></div><div>Action</div></div>
Branches											
<div><div>Firewall Policy</div><div>Firewall Virtual Wire Pair Pol...</div><div>Proxy Policy</div></div>											
	<div><div></div><div>1</div></div>	<div><div></div><div>Branch to HQ</div></div>	<div><div></div><div>LAN</div></div>	<div><div></div><div>IPsec</div></div>	<div><div></div><div>Branch_LAN</div></div>	<div><div></div><div>HQ_LAN</div></div>	<div><div></div><div>always</div></div>	<div><div></div><div>ALL</div></div>	<div><div></div><div>Accept</div></div>		
<div><div></div><div>Implicit (2-2 / Total: 1)</div></div>											
	<div><div></div><div>2</div></div>	<div><div></div><div>Implicit Deny</div></div>	<div><div></div><div>any</div></div>	<div><div></div><div>any</div></div>	<div><div></div><div>all</div></div>	<div><div></div><div>all</div></div>	<div><div></div><div>always</div></div>	<div><div></div><div>ALL</div></div>	<div><div></div><div>Deny</div></div>		

## To create the HUB policy:

- In *Policy Packages*, select the *HUB* policy package and click *Create New*.
- 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.

Policy Packages		+ Create New Edit Delete Section Policy Block Policy Lookup Collapse All Column Settings View Mode									
Search...		#	Name	From	To	Source	Destination	Schedule	Service	Users	Action
Branches		1	Branches to HQ	IPsec	LAN	Branch_LAN	HQ_LAN	always	ALL		Accept
HQ		Implicit (2-2 / Total: 1)									
Firewall Policy		2	Implicit Deny	any	any	all all	all all	always	ALL		Deny
Firewall Virtual Wire Pair Pol...											

## 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.

## Install Wizard - Policy Package (Branches)

Installation Preparation Total: 3/3, ✔ Success: 3, ⚠ Warning: 0, ✖ Error: 0 

- ✔ Interface Validation
- ✔ Policy and Object Validation
- ✔ Ready to Install.

<div>  Install Preview            Policy Package Diff           <div style="float: right; border: 1px solid #ccc; padding: 2px 5px;"> <input type="text"/>  </div> </div>			
<input type="checkbox"/>	Device Name	Status	Action
<input checked="" type="checkbox"/>	Branch-A[root]	<span style="color: green;">✔</span> Connection Up	
<input checked="" type="checkbox"/>	Branch-B[root]	<span style="color: green;">✔</span> Connection Up	

Install

Cancel

For more information about installing policies and policy packages, see [Install a policy package on page 314](#).

### Verifying VPN template and tunnel status

#### To verify the template installation status:

- Go to *Device Manager > Device & Groups*. The list of *Managed FortiGate* devices is displayed.
- 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.

Device & Groups

Search...

Managed FortiGate (3)

- Branch-A
- Branch-B
- HQ

Logging Devices (3)

Managed FortiAnalyzer (1)

Branches (2)

HUB (1)

Scripts

Provisioning Templates

Firmware Templates

Monitors

Connectivity

Connection Up (3)

3

Device Config Status

Synchronized (3)

3

Policy Package Status

Installed (3)

3

Edit

Delete

Import Configuration

Install

Table View

More

Show Charts

Search...

<input type="checkbox"/>	Host Name	IP Address	Firmware Version	Config Status	Policy Package Status	Provisioning Templates
<input type="checkbox"/>	Branch-A	192.168.2.2	FortiGate 7.0.8,build0418 ...	✔ Synchronized	✔ Branches	✔ ACME_BRANCH
<input type="checkbox"/>	Branch-B	192.168.2.3	FortiGate 7.0.8,build0418 ...	✔ Synchronized	✔ Branches	✔ ACME_BRANCH
<input type="checkbox"/>	HQ	192.168.2.1	FortiGate 7.0.8,build0418 ...	✔ Synchronized	✔ HQ	✔ ACME_HUB

#### To verify the VPN tunnel status:

- Go to *Device Manager > Monitors > VPN Monitor*. A map displays.
- Enable *Show Table* to display the table of tunnels below the map.



### 3. Verify that the *Status* is *Up* for each tunnel.

- Device & Groups >
- Scripts
- Provisioning Templates >
- Firmware Templates
- Monitors >
  - SD-WAN Monitor
  - VPN Monitor**
  - Device Inventory
  - AI Analysis

☒ Show Table
☐ Show Tunnel Down Only
↺

⬆ Bring Tunnel Up
⬆ Bring Tunnel Down
⚙ Column Settings
🔍

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 - System SD-WAN on page 154](#).

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 245](#).

Using SD-WAN templates consists of the following steps:

FortiManager 7.2.3 Administration Guide  
Fortinet Inc.

231

1. Create an SD-WAN template. See [SD-WAN templates on page 232](#).
2. Assign the SD-WAN templates to FortiGate devices and device groups. See [Assign SD-WAN templates to devices and device groups on page 244](#).
3. Install device settings using the *Install Wizard*. See [Install device settings only on page 122](#).  
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 286](#).



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** page opens.

**Create New SD-WAN Template**

Name:

Description:

SD-WAN Status: ☒ ON

**Interface Members**

ID	Interface Member	Status	Gateway	Cost
<input type="checkbox"/>	virtual-wan-link			

**Performance SLA**

Name	Health-Check Server	Detect Protocol	Failure Threshold	Recovery Threshold
No record found.				

**SD-WAN Rules**

ID	Name	Source	Destination	Criteria	Members
<input type="checkbox"/>	sd-wan	ALL	ALL	Source IP	ALL

OK Cancel

4. In the **Name** box, type a name for the template.
5. Complete the following sections:
- In the **Interface Members** section, create SD-WAN zones and interface members. See [Zones and interface members on page 234](#).
  - In the **Performance SLA** section, use the defaults, or create new performance SLA. See [Performance SLA on page 236](#).
  - In the **SD-WAN Rules** section, create SD-WAN rules. See [SD-WAN rules on page 238](#).
  - (Optional) In the **Neighbor** section, create neighbors. See [Neighbors on page 242](#).
  - (Optional) In the **Duplication** section, configure packet duplication. See [Duplication on page 243](#).
  - (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:

- If using ADOMs, ensure that you are in the correct ADOM.
- Go to **Device Manager > Provisioning Templates > SD-WAN Templates**.
- Double-click the template, or select the template, and click **Edit** in the toolbar. The **Edit** page opens.
- Edit the template as required, and click **OK** to apply your changes.

#### To delete an SD-WAN template:

- If using ADOMs, ensure that you are in the correct ADOM.
- Go to **Device Manager > Provisioning Templates > SD-WAN Templates**.
- Select the template, and click **Delete** in the toolbar, or right-click the template and select **Delete**.
- 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.

#### Import SD-WAN templates

Name	<input type="text"/>
Device	<input type="button" value="Click to select"/>
Description	<div><div></div><div>0/255</div></div>

OK

Cancel

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:

Edit SD-WAN Interface Member	
Sequence Number	<input type="text" value="4"/>
Interface Member	<input type="text" value="\$int-memb6"/>
SD-WAN Zone	<input type="button" value="zone1"/>
Gateway IP	<input type="text" value="\$int-memb-gw"/>
Cost	<input type="text" value="10"/>
Status	<input checked="" type="checkbox"/>
Weight	<input type="text" value="1"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

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:

<b>Sequence Number</b>	Type a number to identify the sequence of the interface in the SD-WAN zone.
<b>Interface Member</b>	Type the name of the port. You can use meta fields for <i>Interface Members</i> .
<b>SD-WAN Zone</b>	Select the SD-WAN zone for the interface member.
<b>Gateway IP</b>	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 <i>Gateway IP</i> .
<b>Status</b>	Toggle On to enable the interface member. Toggle Off to disable the interface 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*:

<b>Name</b>	Type a name for the SD-WAN zone.
<b>Interface Members</b>	Click the box to select interface members for the zone.
<b>Advanced Options</b>	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:

<b>Name</b>	Enter the name of the performance SLA.
<b>IP Version</b>	Select <i>IPv4</i> or <i>IPv6</i> .
<b>Probe Mode</b>	Set the mode that determines how to detect the server: <ul style="list-style-type: none"> <li>• <i>Active</i>: the probes are sent actively (default).</li> <li>• <i>Passive</i>: the traffic measures health without probes.</li> <li>• <i>Prefer-passive</i>: the probes are sent in case of no new traffic.</li> <li>• <i>Remote</i>: the link health is obtained from remote peers.</li> </ul>
<b>Protocol</b>	Select the detection method for the profile check: <ul style="list-style-type: none"> <li>• Ping</li> <li>• TCP ECHO</li> <li>• UDP ECHO</li> <li>• HTTP</li> <li>• TWAMP</li> </ul>

	<ul style="list-style-type: none"> <li>• DNS</li> <li>• TCP Connect</li> <li>• FTP</li> </ul>
<b>Server</b>	Click <i>Add (+)</i> , and type the IP address of the health-check server.
<b>Participants</b>	Select available interface members or select <i>All SD-WAN Members</i> . The interfaces must already be added to the template.
<b>Embedded Measure Health</b>	Enable/disable embedding SLA information in ICMP probes (default = disable).
<b>Redistribute SLA ID</b>	Set the SLA entry (ID) that will be applied to the IKE routes (0 - 31, default = 0).
<b>Enable Probe Packets</b>	Set <i>Enable probe packets</i> to enable or disable sending probe packets.
<b>SLA Targets</b>	<p>Click <i>Add Target</i> to add a new SLA. Enable and enter the <i>Latency Threshold</i> (in milliseconds), <i>Jitter Threshold</i> (in milliseconds), <i>Packet Loss Threshold</i> (in percent), <i>Priority IN-SLA</i>, and <i>Priority OUT-SLA</i>, then click <i>OK</i> to create the SLA.</p> <p>SLAs can also be edited and deleted as required.</p>
<b>Link Status</b>	
<b>Interval</b>	Status check interval, or the time between attempting to connect to the server, in seconds (1 - 3600, default = 1).
<b>Failure Before Inactive</b>	Specify the number of failures before the link becomes inactive (1 - 10, default = 5).
<b>Restore Link After</b>	Specify the number of successful responses received before server is considered recovered (1 - 10, default = 5).
<b>Action When Inactive</b>	Specify what happens with the WAN link becomes inactive.
<b>Update Static Route</b>	Select to update the static route when the WAN link becomes inactive.
<b>Cascade Interfaces</b>	Select to cascade interfaces when the WAN link becomes inactive.
<b>Advanced Options</b>	<p>Expand to display the advanced options.</p> <p>Hover the mouse over each advanced option to view a description of the option.</p> <p>Set the options as desired.</p>

## 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.

**Create New SD-WAN Rule**

Name

IP Version

**Source**

Source Address

Users

User Groups

**Destination**

Internet Service

Internet Service Group

Custom Internet Service

Internet Service Custom Group

Application

Application Group

Application Category

Type of Service

**Outgoing Interfaces**

Strategy

Interface Preference

**Advanced Options** >

IPv4

Click to select

Click to select

Click to select

Address

Internet Service

Click to select

Click to select

Click to select

Click to select

Click to select

Click to select

0x00

Bit Mask

0x00

Manual

Best Quality

Lowest Cost (SLA)

Maximize Bandwidth (SLA)

+

\*re-order the members by dragging and dropping the item

OK

Cancel

FortiManager 7.2.3 Administration Guide  
Fortinet Inc.

240

5. Enter the following information, then click *OK* to create the new SD-WAN rule:

<b>Name</b>	Enter the name of the rule.
<b>IP Version</b>	Select either <i>IPv4</i> or <i>IPv6</i> .
<b>Source</b>	
<b>Source Address</b>	Add one or more address from the drop-down.
<b>Users</b>	Add one or more users from the drop-down.
<b>User Groups</b>	Add one or more groups from the drop-down.
<b>Destination</b>	
<b>Address</b>	Select an address or addresses from the drop-down list. This option is only available when <i>Destination</i> is <i>Address</i> .
<b>Route Tag</b>	Select a tag from the drop-down list. This option is only available when <i>Destination</i> is <i>Address</i> .
<b>Internet Service</b>	Select a service or services from the dropdown list. This option is only available when <i>Destination</i> is <i>Internet Service</i> .
<b>Internet Service Group</b>	Select a service group or groups from the dropdown list. This option is only available when <i>Destination</i> is <i>Internet Service</i> .
<b>Custom Internet Service</b>	Select a service or services from the dropdown list. This option is only available when <i>Destination</i> is <i>Internet Service</i> .
<b>Custom Internet Service Group</b>	Select a service group or groups from the dropdown list. This option is only available when <i>Destination</i> is <i>Internet Service</i> .
<b>Application</b>	Select an application or applications from the dropdown list. This option is only available when <i>Destination</i> is <i>Internet Service</i> .
<b>Application Group</b>	Select an application group or groups from the dropdown list. This option is only available when <i>Destination</i> is <i>Internet Service</i> .
<b>Application Categories</b>	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 <i>Destination</i> is <i>Internet Service</i> , and you are in a 7.2 or later ADOM.
<b>Protocol</b>	Select the protocol, or specify the protocol number.
<b>Port Range</b>	Enter the port range. This option is only available when the protocol is <i>TCP</i> or <i>UDP</i> .
<b>Type of Service</b>	Specify the type of service and bit mask.
<b>Outgoing Interface</b>	
<b>Strategy</b>	Select one of the following to specify how the traffic flows through the outgoing interface: <ul style="list-style-type: none"> <li><i>Manual</i> to specify what outgoing interface members to use.</li> <li><i>Best Quality</i> to identify outgoing interface members and have traffic flow</li> </ul>

	<p>based on quality status.</p> <ul style="list-style-type: none"> <li>• <i>Lowest Cost (SLA)</i> to identify outgoing interface members and have traffic flow based on the lowest cost.</li> <li>• <i>Maximize Bandwidth SLA</i> to identify outgoing interface members and have traffic flow to maximize bandwidth.</li> </ul>
<b>Interface Preference</b>	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.
<b>Measured SLA</b>	Select the SLA measurement for the selected strategy. This option is only available when <i>Strategy</i> is <i>Best Quality</i> .
<b>Zone Preference</b>	Select the zone preference. This option is only available when <i>Strategy</i> is <i>Lowest Cost (SLA)</i> or <i>Maximize Bandwidth (SLA)</i> .
<b>Required SLA Target</b>	Select the required SLA target. This option is only available when <i>Strategy</i> is <i>Lowest Cost (SLA)</i> or <i>Maximize Bandwidth (SLA)</i> .
<b>Advanced Options</b>	<p>Expand to display the advanced options.</p> <p>Hover the mouse over each advanced option to view a description of the option.</p> <p>Set the options as desired.</p>

## 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:

<b>IP</b>	Type the IP address for the BGP neighbor.
<b>Interface Member</b>	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.
<b>Performance SLA</b>	Click the list, and select the performance SLA.
<b>Role</b>	Select <i>Standalone</i> , <i>Primary</i> , or <i>Secondary</i> .

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.

### Create New SD-WAN Duplication

Source Address	<input type="text"/>	Click here to select
Destination Address	<input type="text"/>	Click here to select
Source Address 6	<input type="text"/>	Click here to select
Destination Address 6	<input type="text"/>	Click here to select
Source Interface	<input type="text"/>	Click here to select
Destination Interface	<input type="text"/>	Click here to select
Service	<input type="text"/>	Click here to select
Packet Discard Duplication	<input type="checkbox"/> OFF	
Packet Duplication	<input checked="" type="radio"/> Disable <input type="radio"/> Force <input type="radio"/> On Demand	

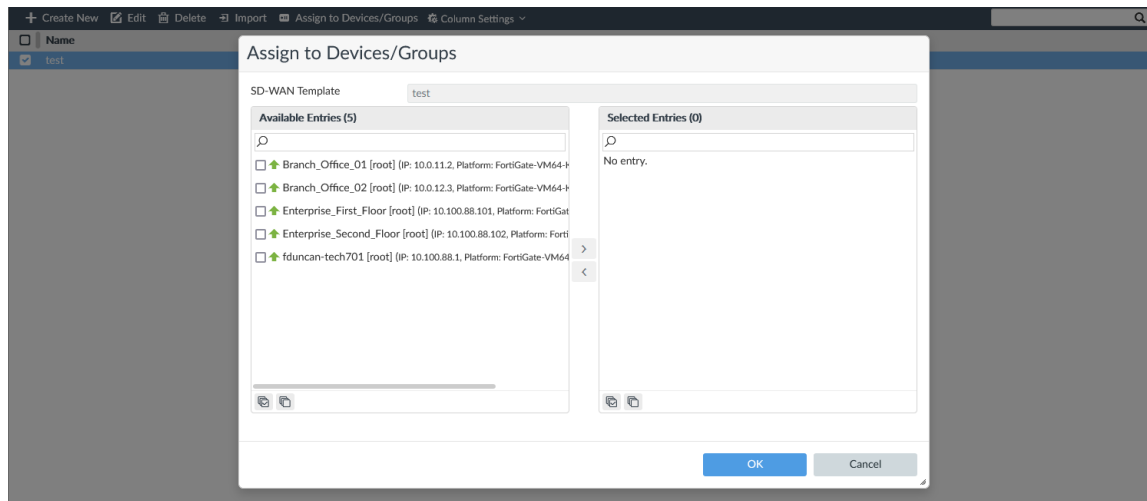
5. Enter the options, then click OK:

## 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.

## 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 a 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 201](#).

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 247](#).

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. 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 437](#).

You can configure a new SD-WAN Overlay Template by going to *Device Manager > Provisioning Templates > SD-WAN Overlay Templates*.

The screenshot shows the FortiManager Device Manager interface. The left sidebar contains a navigation menu with categories like 'Device & Groups', 'Scripts', 'Provisioning Templates', and 'Firmware Templates'. Under 'Provisioning Templates', 'SD-WAN Overlay Templates' is selected. The main area displays a table with columns: #, Template Name, Topology, Assign to Device/Group, Loopback IP Address, Overlay Network, and BGP AS Num. One template is listed: ID 1, Name 'SD-WAN-TEMPLATE', Topology 'Dual HUB (Primary & Secondary)', assigned to 'Enterprise\_First\_Floor', 'Enterprise\_Second\_Floor', and 'sd-wan-branches', with Loopback IP '172.16.0.0/255.255.0.0', Overlay Network '10.10.0.0/255.255.0.0', and BGP AS Num '65000'.

#	Template Name	Topology	Assign to Device/Group	Loopback IP Address	Overlay Network	BGP AS Num
1	SD-WAN-TEMPLATE	Dual HUB (Primary & Secondary)	Enterprise_First_Floor Enterprise_Second_Floor sd-wan-branches	172.16.0.0/255.255.0.0	10.10.0.0/255.255.0.0	65000

The following options are available:

<b>Create New</b>	Create a new SD-WAN overlay template.
<b>Edit</b>	Edit a template. Right-click a template, and select <i>Edit</i> .
<b>Delete</b>	Delete a template. Right-click a template, and select <i>Delete</i> .
<b>More</b>	View additional options, including the option to clone a template.
<b>Column Settings</b>	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 51](#).
- Configure the ISP links and other interfaces on your imported devices.
- Create a device group for your branch devices. See [Device groups on page 94](#)

### 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 257](#)



Note that the overlay template does not provide any SD-WAN intelligence. Please configure a 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 246](#).
2. Create an SD-WAN overlay template. See [Configuring an SD-WAN overlay template on page 247](#).
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. Additional custom metadata variables can be used if required. See [ADOM-level metadata variables on page 437](#).
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 238](#) and [SD-WAN templates on page 231](#).
5. Create the Policy Package for your branch and hub devices. See [Managing policy packages on page 310](#).
6. Install the changes to SD-WAN devices using the Install Wizard. See [Install wizard on page 120](#).
7. (Optional) Edit the SD-WAN overlay template. See [Editing the SD-WAN overlay template on page 253](#).
8. (Optional) Add new branch devices. See [Onboarding new branch devices on page 253](#).

## 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 253](#).

### 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*.

Edit SD-WAN Overlay Template - Region Settings (1/5)

Name: SD-WAN-TEMPLATE

Description:

Select New Topology

Single HUB

Dual HUB  
(Primary & Secondary)

Dual HUB  
(Primary & Primary)

Advanced ▾

Loopback IP Address: 172.16.0.0/255.255.0.0

Overlay Network: 10.10.0.0/255.255.0.0

BGP-AS Number: 65000

Auto-Discovery VPN: ☐

Next > Last Cancel

### 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. See [Template prerequisites and network planning on page 246](#).

#### 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*.

Edit SD-WAN Overlay Template - Role Assignment (2/5)

Name: SD-WAN-TEMPLATE

Topology: Single HUB **Dual HUB (Primary & Secondary)** Dual HUB (Primary & Primary)

**HUB**

Primary HUB: Enterprise\_HUB1

Secondary HUB: Enterprise\_HUB2

**Branch**

Device Group Assignment: sd-wan-branches

< Back   Next >   Cancel

### 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

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 253](#).

6. For the *Network Configuration*, configure the following settings and click *Next*.

Edit SD-WAN Overlay Template - Network Configuration (3/5)

Name: SD-WAN-TEMPLATE

**HUB**

**Primary HUB**

WAN Underlay 1: Enterprise\_HUB1

Private Link: ☐ port1

Override IP: ☐

Network Advertisement: **Connected** Static

Interface: +

Advanced >

**Secondary HUB**

WAN Underlay 1: Enterprise\_HUB2

Private Link: ☐ port1

Override IP: ☐

Network Advertisement: **Connected** Static

Interface: +

Advanced >

Branch Route Maps

Route map in: ☐

Route map out: ☐

**Branch**

Branch Device Group: sd-wan-branches

WAN Underlay 1: port1

Private Link: ☐

Network Advertisement: **Static** Connected

Network Prefix: +

Advanced >

< Back Next > Cancel

## 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.

<b>Advanced</b>	Expand to view advanced settings, including configuration of SD-WAN neighbors. Click <i>Neighbors &gt; Create New</i> to add a new SD-WAN neighbor for the hub.
<b>Branch Route Maps</b>	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 <a href="#">Using preconfigured route maps for self-healing with BGP on page 252</a> .
<b>Branch</b>	Configure the network settings for the branch devices in your configuration.
<b>WAN Underlay</b>	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: <ul style="list-style-type: none"> <li>• <i>Private Link</i>: No overlays will be created on private links.</li> </ul>
<b>Network Advertisement</b>	Configure network advertisement for the branch. Network advertisement can be set to one of the following: <ul style="list-style-type: none"> <li>• <i>Connected</i>: Type the network interface to advertise. Additional interfaces can be added by clicking the add icon.</li> <li>• <i>Static</i>: Type the network prefix to advertise. Additional network prefixes can be added by clicking the add icon.</li> </ul>
<b>Advanced</b>	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 <a href="#">Using preconfigured route maps for self-healing with BGP on page 252</a> .

7. For the *Template Options*, configure the following settings and click *Next*.

Edit SD-WAN Overlay Template - SD-WAN Template Options (4/5)

- Add Overlay Objects to SD-WAN Template ☐
- Add Overlay Interfaces and Zones ☐
- Add Healthcheck Servers for Each HUB as Performance SLA ☐

< Back

Next >

Cancel

**Add Overlay Objects to SD-WAN Template**

Optionally, you can 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 231](#).

**Add Overlay Interfaces and Zones**

Optionally, you can toggle this setting ON to add overlay interfaces and zones.

### Add Healthcheck Servers for Each HUB as Performance SLA

Optionally, you can toggle this setting ON to add health check servers for each hub as performance SLAs.

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.

#### Edit SD-WAN Overlay Template - Summary (5/5)

Please review the summary of SD-WAN Overlay configurations

NOTE: By clicking "Finish", multiple related provisioning templates will be automatically created based on the configurations. You could also re-run the SD-WAN Overlay wizard to re-generate the provisioning templates later.

<b>Template Name</b>	SD-WAN-TEMPLATE
<b>Topology</b>	Dual HUB (Primary & Secondary)
<a href="#">Region Network Settings</a>	Loopback Allocated: 172.16.0.0/255.255.0.0 Overlay Network: 10.10.0.0/255.255.0.0 BGP AS Number: 65000 Auto-Discovery VPN: <input type="checkbox"/>
<a href="#">Device Assignment</a>	
Primary HUB	Enterprise_HUB1 (10.100.88.101, Platform: FortiGate-VM64-KVM)
Secondary HUB	Enterprise_HUB2 (10.100.88.102, Platform: FortiGate-VM64-KVM)
Assign to	sd-wan-branches
<a href="#">Underlay Assignment</a>	
Primary HUB Underlays	port1
Secondary HUB Underlays	port1
Branch Underlays	port1
<a href="#">Network Advertisement</a>	
Primary HUB	Connected: None
Secondary HUB	Connected: None
Branch	Static: None
<a href="#">SD-WAN Template Options</a>	
Add Overlay Objects to SD-WAN Template	<input type="checkbox"/>
Add Overlay Interfaces and Zones	<input type="checkbox"/>
Add Healthcheck Servers for Each HUB as Performance SLA	<input type="checkbox"/>

< Back

Finish

Cancel

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 247](#).

## 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 78](#).
- Metadata variables can be used as variables in provisioning templates. By default, the `branch_id` metadata variable is created by the SD-WAN overlay template and must be specified for each branch device. See [ADOM-level metadata variables on page 437](#).

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 68](#).

### 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 78](#).
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.
4. Assign policy package for the branch device, and then install the changes using the Install Wizard. See [Install wizard on page 120](#).

## 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 247](#).

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

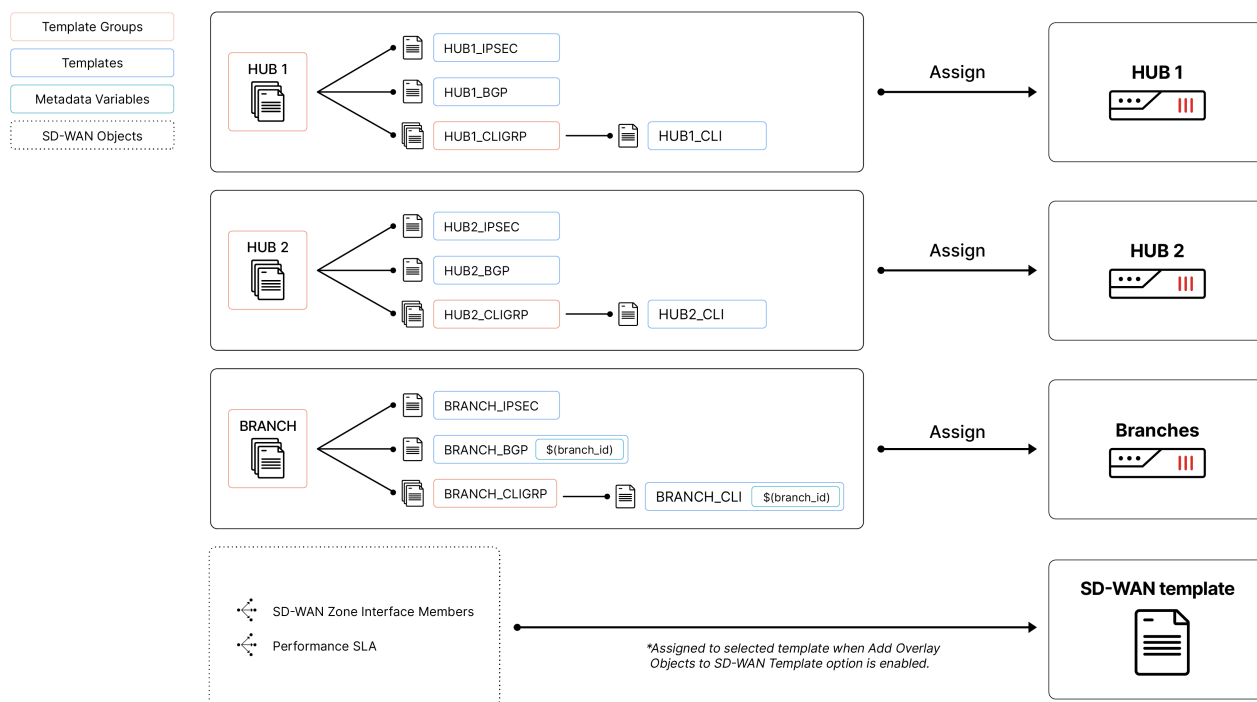
The SD-WAN overlay template wizard also configures the SD-WAN overlay network. The default overlay network used by the wizard is 10.10.0.0, but this can be configured for your environment. The number of subnets created from the overlay network depends on the number of overlays and hubs that are configured.

Below details the various templates and associated components that are defined in dual-hub and single-hub deployment scenarios.


- [Dual-hub deployments on page 254](#)
- [Single-hub deployments on page 256](#)

## Dual-hub deployments

### Template and object assignment (dual-hub)



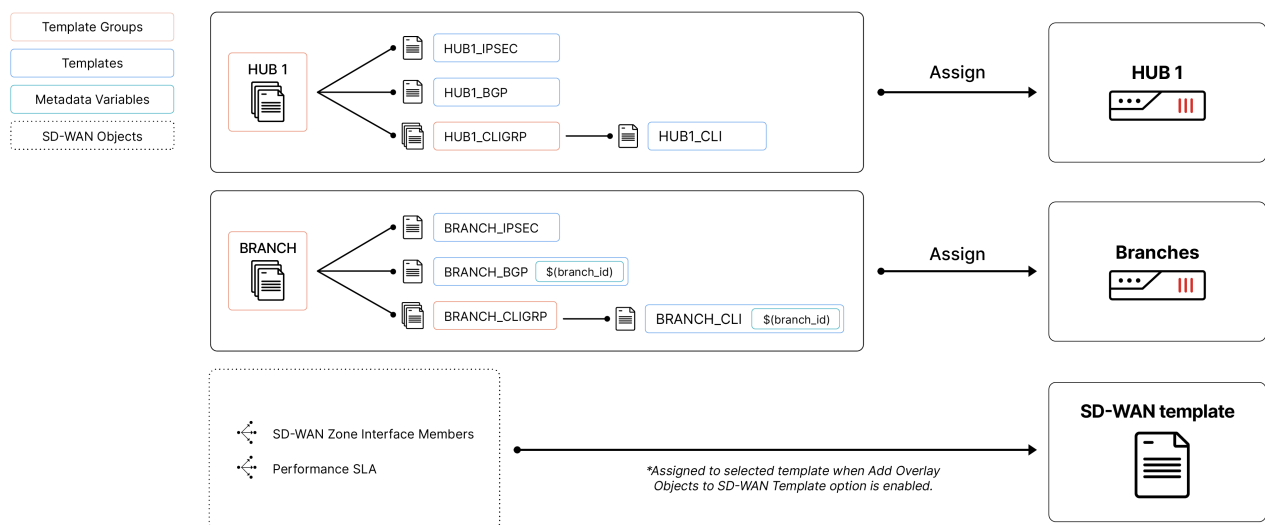


Category	Templates and Objects
<b>IPsec Templates</b>	<p>The following IPsec templates are created for configuration of IPsec in your SD-WAN environment:</p> <ul style="list-style-type: none"> <li>• <b>BRANCH_IPsec</b>: The IPsec template for IPsec tunnels for branch devices. This template includes the following IPsec tunnels to allow connection from branch devices to the hubs through VPN1 and VPN2: <i>HUB1-VPN1</i>, <i>HUB1-VPN2</i>, <i>HUB2-VPN1</i>, and <i>HUB2-VPN2</i>.</li> <li>• <b>HUB1_IPsec</b>: The IPsec template created for hub 1. This template includes the IPsec tunnels <i>VPN1</i> and <i>VPN2</i> to allow secure communication from hub 1 to branch devices.</li> <li>• <b>HUB2_IPsec</b>: The IPsec template created for hub 2. This template includes the IPsec tunnels <i>VPN1</i> and <i>VPN2</i> to allow secure communication from hub 2 to branch devices.</li> </ul>
<b>BGP Templates</b>	<p>The following BGP templates are created for configuration of BGP in your SD-WAN environment:</p> <ul style="list-style-type: none"> <li>• <b>BRANCH_BGP</b>: The BGP template generated for your SD-WAN branch devices. This template uses the <i>branch_id</i> metadata variable to configure the Router ID for each branch device.</li> <li>• <b>HUB1_BGP</b>: The BGP template created for hub 1.</li> <li>• <b>HUB2_BGP</b>: The BGP template created for hub 2.</li> </ul>
<b>SD-WAN Template configurations</b>	<p>The following SD-WAN zones/members and health check servers are configured for the SD-WAN template specified in the wizard.</p> <ul style="list-style-type: none"> <li>• <b>SD-WAN Zone/Interface Member</b>: WAN1/port1, WAN2/port2, HUB1/HUB1-VPN1 and HUB1-VPN2, HUB2/HUB2-VPN1 and HUB2-VPN2</li> <li>• <b>Performance SLA</b>: HUB1_HC and HUB2_HC</li> </ul> <hr/> <div>  <p>These settings are only applied when the <i>Add Overlay Objects to SD-WAN Template</i> option is enabled in the wizard.</p> </div> <hr/>
<b>CLI Templates</b>	<p>The following CLI templates are created to configure the device interfaces and BGP router ID.</p> <ul style="list-style-type: none"> <li>• <b>BRANCH_CLI</b>: 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 <i>BRANCH_CLIGRP</i> template group.</li> <li>• <b>HUB1_CLI</b>: Configure the HUB1-Lo interface on the hub 1 device. This template is added to the <i>HUB1_CLIGRP</i> template group.</li> <li>• <b>HUB2_CLI</b>: Configure the HUB2-Lo interface on the hub 2 device. This template is added to the <i>HUB2_CLIGRP</i> template group.</li> </ul>
<b>Template Groups</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• <b>HUB1</b>: Includes provisioning templates for the hub 1 device.</li> <li>• <b>HUB2</b>: Includes provisioning templates for the hub 2 device.</li> <li>• <b>BRANCH</b>: Includes provisioning templates for branch devices. This template is automatically applied to all devices included in the branch device group specified in the wizard.</li> </ul>


Category	Templates and Objects
	For information about onboarding new branch devices using template groups, see <a href="#">Onboarding new branch devices on page 253</a>
<b>Metadata Variables</b>	<p>ADOM-level metadata variables are used as variables in scripts and templates.</p> <ul style="list-style-type: none"> <li><b>branch_id</b>: The <code>branch_id</code> variable is automatically created by the template. Each branch device must be assigned a unique value. The <code>branch_id</code> metadata variable is used in branch provisioning templates to configure certain settings, such as the BGP router ID. See <a href="#">ADOM-level metadata variables on page 437</a>.</li> </ul>

## Single-hub deployments

### Template and object assignment (single-hub)



Category	Templates and Objects
<b>IPsec Templates</b>	<p>The following IPsec templates are created for configuration of IPsec in your SD-WAN environment:</p> <ul style="list-style-type: none"> <li><b>BRANCH_IPsec</b>: 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: <i>HUB1-VPN1</i> and <i>HUB1-VPN2</i>.</li> <li><b>HUB1_IPsec</b>: The IPsec template created for the hub. This template includes the IPsec tunnels <i>VPN1</i> and <i>VPN2</i> to allow secure communication from the hub to branch devices.</li> </ul>
<b>BGP Templates</b>	<p>The following BGP templates are created for configuration of BGP in your SD-WAN environment:</p> <ul style="list-style-type: none"> <li><b>BRANCH_BGP</b>: The BGP template generated for your SD-WAN branch devices. This template uses the <code>branch_id</code> metadata variable to configure the Router ID for each branch device.</li> <li><b>HUB1_BGP</b>: The BGP template created for the hub.</li> </ul>

Category	Templates and Objects
SD-WAN Template configurations	<p>The following SD-WAN zones/members and health check servers are configured for the SD-WAN template specified in the wizard.</p> <ul style="list-style-type: none"> <li>• <b>SD-WAN Zone/Interface Member:</b> WAN1/port1, WAN2/port2, HUB1/HUB1-VPN1 and HUB1-VPN2.</li> <li>• <b>Performance SLA:</b> HUB1_HC.</li> </ul> <hr/> <div>  <p>These settings are only applied when the <i>Add Overlay Objects to SD-WAN Template</i> option is enabled in the wizard.</p> </div>
CLI Templates	<p>The following CLI templates are created to configure the device interfaces and BGP router ID.</p> <ul style="list-style-type: none"> <li>• <b>BRANCH_CLI:</b> 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 <i>BRANCH_CLIGRP</i> template group.</li> <li>• <b>HUB1_CLI:</b> Configure the HUB1-Lo interface on the hub device. This template is added to the <i>HUB1_CLIGRP</i> template group.</li> </ul>
Template Groups	<p>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.</p> <ul style="list-style-type: none"> <li>• <b>HUB1:</b> Includes provisioning templates for the hub 1 device.</li> <li>• <b>BRANCH:</b> Includes provisioning templates for branch devices. The template is automatically applied to all devices included in the branch device group selected in the wizard.</li> </ul> <p>For information about onboarding new branch devices using template groups, see <a href="#">Onboarding new branch devices on page 253</a></p>
Metadata Variables	<p>ADOM-level metadata variables are used as variables in scripts and templates.</p> <ul style="list-style-type: none"> <li>• <b>branch_id:</b> The <code>branch_id</code> variable is automatically created by the template. Each branch device must be assigned a unique value. The <code>branch_id</code> metadata variable is used in branch provisioning templates to configure certain settings, such as the BGP router ID. See <a href="#">ADOM-level metadata variables on page 437</a>.</li> </ul>

## 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
<b>1 - 4 underlays</b> 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
<b>5 - 8 underlays</b> 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
<b>9 - 16 underlays</b>	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 overlay 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.

Create New SD-WAN Overlay Template - Network Configuration (3/5)

Name

Dual-Hub

HUB

Primary HUB

Hub1

WAN Underlay 1

Private Link

port1

Override IP

Private Link

port2

Override IP

Network Advertisement

Connected

Static

Interface

Advanced >

Secondary HUB

Hub2

WAN Underlay 1

Private Link

port1

Override IP

Private Link

port2

Override IP

Network Advertisement

Connected

Static

Interface

Advanced >

Branch Route Maps

Route map in

Route map out

Branch

Branch Device Group

BRANCH

WAN Underlay 1

Private Link

port1

Private Link

port2

Network Advertisement

Connected

Static

Interface

Advanced >

< Back

Next >

Cancel

With this configuration:

FortiManager 7.2.3 Administration Guide  
Fortinet Inc.

259

- 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:

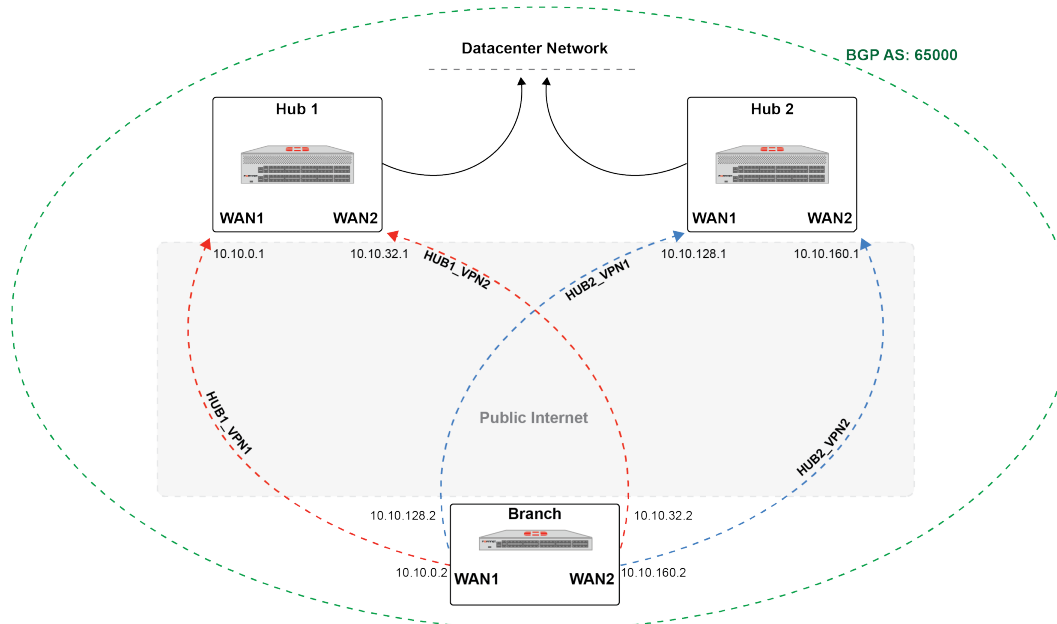


Figure 1 - SD-WAN overlay network topology for the default dual-hub (primary & secondary) configuration.

## 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.

Edit SD-WAN Overlay Template - Network Configuration (3/5)

Name
SINGLE-HUB

HUB

Standalone HUB
HA1

WAN Underlay 1
Private Link
port1

WAN Underlay 2
Override IP
Private Link
port2

Network Advertisement
Connected
Static

Interface

Advanced

Branch Route Maps
Route map in
Route map out

Branch

Branch Device Group
SD-Branches

WAN Underlay 1
Private Link
port1

WAN Underlay 2
Private Link
port2

Network Advertisement
Connected
Static

Interface

Advanced

< Back
Next >
Cancel

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:

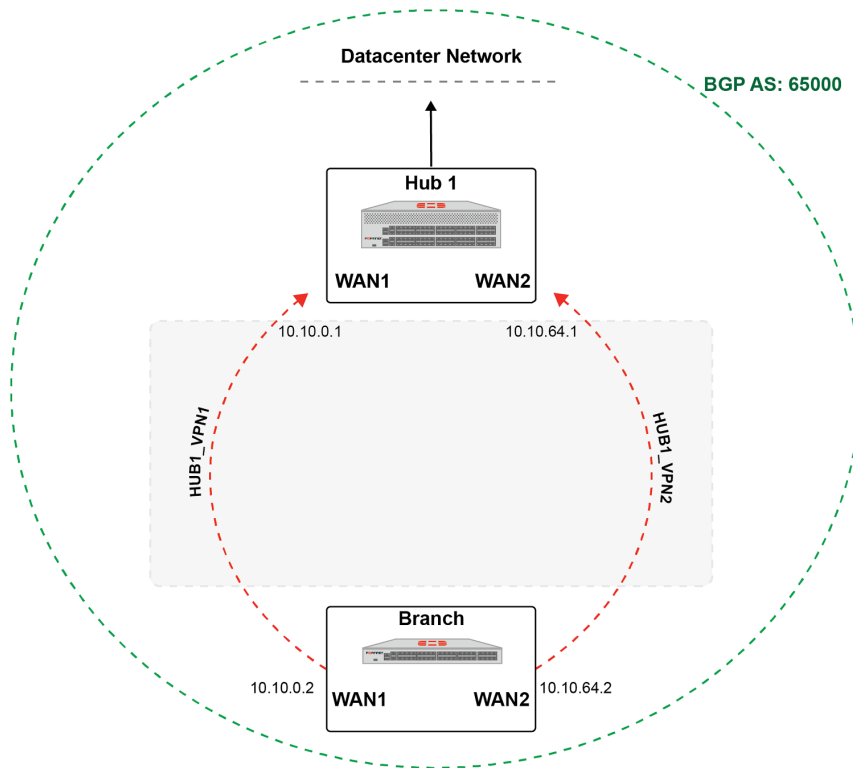


Figure 2 - SD-WAN overlay network topology for the default single-hub configuration.

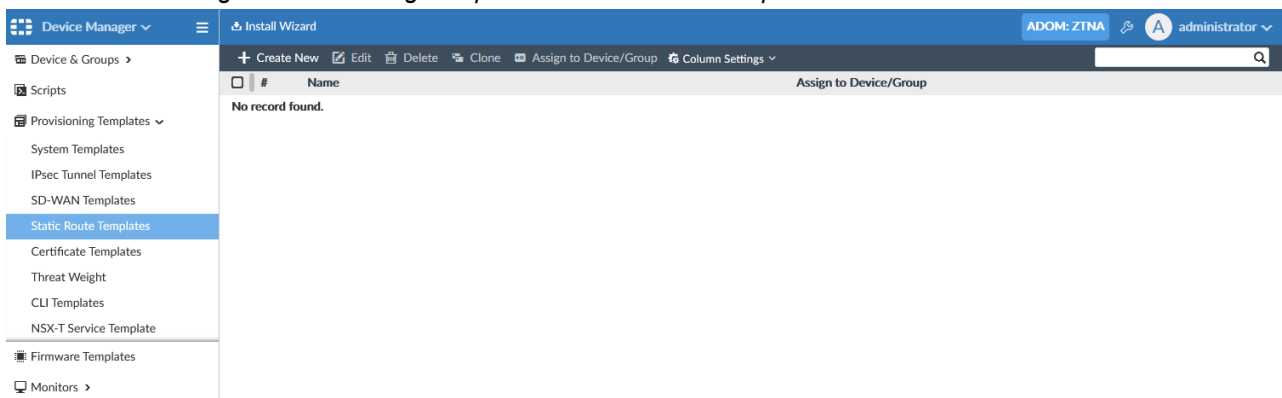
## Static route templates

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 798](#).

### To create a new static route template:

1. Go to *Device Manager > Provisioning Templates > Static Route Templates*.





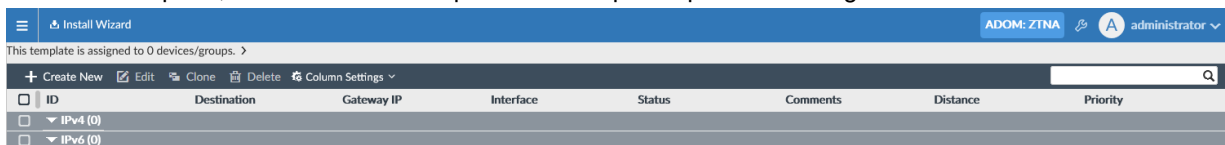
## 2. Create a static route template:

- 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.

Create New Static Route

To use meta field, the input format is \$(meta\_field\_name).

Type

IPv4

IPv6

Destination

Subnet

Internet Service

Internet Service Custom

Gateway Address

0.0.0.0/0.0.0.0

Gateway Address

0.0.0.0

Interface

Administrative Distance

10

Comments

0/255

Status

ON

Advanced Options >

OK

Cancel

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:

**Edit Static Route**

*To use meta field, the input format is \$(meta\_field\_name).*

Type: **IPv4** | IPv6

Destination: **Subnet** | Internet Service | Internet Service Custom

Gateway Address:

Interface:

Administrative Distance:

Comments:

Status: ☒ ON

Advanced Options >

- c. Complete the following options, and click OK.

<b>Type</b>	Select the type of static route. Choose between <i>IPv4</i> and <i>IPv6</i> .
<b>Destination</b>	Select the destination for the route. Choose between <i>Subnet</i> , <i>Internet Service</i> , and <i>Internet Service Custom</i> .  When you select <i>Type</i> of <i>IPv4</i> and <i>Destination</i> of <i>Subnet</i> , 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.
<b>Gateway Address</b>	Specify the IP address for the gateway.
<b>Interface</b>	Specify the interface.
<b>Comments</b>	(Optional) Type a comment about the static route.
<b>Advanced Options</b>	Expand to display advanced options.

The static route is created.

- Assign the template of static routes to one or more devices or device groups.
- 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:

- Go to *Device Manager > Provisioning Templates > BGP Template*.
- Click *Create New* in the toolbar.

3. In the *Create BGP Template* pane, configure the following settings:

**Create BGP Template**

Name: BGP\_Template\_NA

Local AS: 65000

Router ID: 10.101.\${site-id}.25

**Neighbors**

IP	Remote AS
<input type="checkbox"/> 10.0.10.1	65000
<input type="checkbox"/> 10.0.11.1	65000
<input type="checkbox"/> 10.0.12.1	65000

**Neighbor Group**

Name	Remote AS
<input type="checkbox"/> GRP1	65000
<input type="checkbox"/> SecondaryVPN	65000
<input type="checkbox"/> ThirdMPLS	65000

OK Cancel

<b>Name</b>	Enter a name for the BGP template.
<b>Local AS</b>	Enter the Local AS.
<b>Router ID</b>	Enter the Router ID.
<b>Neighbors</b>	Click <i>Create New</i> to add a BGP neighbor.
<b>Neighbor Group</b>	The BGP neighbor group feature allows a large number of neighbors to be configured automatically based on a range of neighbors' source addresses. Click <i>Create New</i> to add a BGP neighbor group.
<b>Neighbor Ranges</b>	Configure the neighbor ranges to be used by neighbor groups. Click <i>Create New</i> to add a neighbor range and select the neighbor group to which the range applies.
<b>Networks</b>	Add IP/Netmask for networks.
<b>IPv6 Networks</b>	Add IP/Netmask for IPv6 networks.
<b>IPv4 Redistribute</b>	Enable <i>Connected</i> , <i>RIP</i> , <i>OSPF</i> , <i>Static</i> , and <i>ISIS</i> for IPv4 redistribute.
<b>IPv6 Redistribute</b>	Enable <i>Connected</i> , <i>RIP</i> , <i>OSPF</i> , <i>Static</i> , and <i>ISIS</i> for IPv6 redistribute.
<b>Dampening</b>	Expand to see dampening options.
<b>Graceful Restart</b>	Expand to see options for graceful restarting.
<b>Advanced Options</b>	Expand to see advanced options.
<b>Best Path Selection</b>	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:

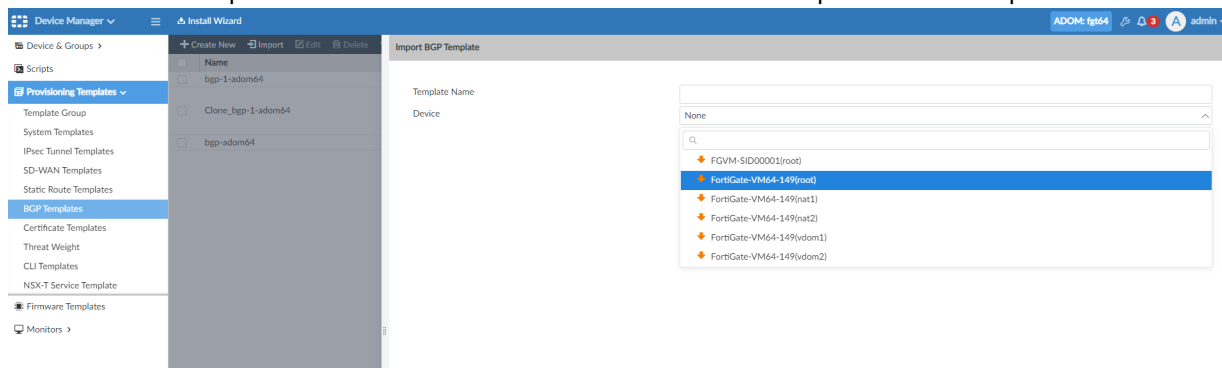
- Route Map
- Access List
- IPv6 Access List
- Prefix List
- IPv6 Prefix List
- AS Path List
- Community List

4. Click **OK** to save the template.  
See the [FortiGate Administration Guide on the Fortinet Docs Library](#) 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 798](#).

The following BGP recommended templates are available.

Template Name	Description
<b>BRANCH_BGP_Recommended</b>	Fortinet's recommended BGP template for branch device configurations.
<b>HUB_BGP_Recommended</b>	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.

The screenshot shows the FortiManager Device Manager interface. On the left, the 'Provisioning Templates' menu is expanded, and 'BGP Templates' is selected. The main area displays the 'Activate BRANCH\_BGP\_Recommended' dialog. The dialog has a list of templates on the left with 'BRANCH\_BGP\_Recommended' and 'HUB\_BGP\_Recommended' listed. On the right, there are input fields for configuration details: 'Template Name' (pre-filled with 'Activate\_BRANCH\_BGP\_Recommended'), 'Enable ADVPN' (a toggle switch), 'Local AS', 'Router ID', 'Neighbor IP', 'Remote AS', and 'Networks Prefix'. At the bottom, there are 'OK' and 'Cancel' buttons.

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. See [Template groups on page 201](#)
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.

<b>Template Name</b>	Enter a name for the template.
<b>Enable ADVPN</b>	Optionally, toggle this setting to enable Auto Discovery VPN (ADVPN).
<b>Local AS</b>	Enter the hub's local AS number.

<b>Router ID</b>	Enter the router ID. The router ID is the unique IP address used to identify the hub device.
<b>Neighbor</b>	Enter the neighbor <i>IP</i> and <i>Remote AS</i> . The neighbor IP is the IP address used while peering as a neighbor.
<b>Neighbor Group</b>	Enter the neighbor group's <i>Remote AS</i> .
<b>Neighbor Range</b>	Enter the neighbor range <i>Prefix</i> . This is the network range that branch devices use to connect to the hub.
<b>Networks</b>	Enter the networks <i>Prefix</i> .

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.

<b>Template Name</b>	Enter a name for the template.
<b>Enable ADVPN</b>	Optionally, toggle this setting to enable Auto Discovery VPN (ADVPN).
<b>Local AS</b>	Enter the branch's local AS number.
<b>Router ID</b>	Enter the router ID. The router ID is the unique IP address used to identify the branch device.
<b>Neighbor</b>	Enter the neighbor <i>IP</i> and <i>Remote AS</i> .
<b>Networks</b>	Enter the networks <i>Prefix</i> .

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:

<b>Create New</b>	Create a new certificate template.
<b>Edit</b>	Edit a certificate template. Right-click a certificate template, and select <i>Edit</i> .
<b>Delete</b>	Delete a certificate template. Right-click a certificate template, and select <i>Delete</i> .
<b>Generate</b>	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:

<b>Type</b>	Specify whether the certificate uses an external or local certificate authority (CA). When you select <i>External</i> , you must specify details about online SCEP enrollment. When you select <i>Local</i> , you are using the FortiManager CA server.
<b>Certificate Name</b>	Type a name for the certificate.
<b>Optional Information</b>	Optionally, type the organization unit, organization, locality (city), province or state, country or region, and email address.
<b>Key Type</b>	RSA is the default key type. This field cannot be edited.
<b>Key Size</b>	Select the key size from the dropdown list: 512 bit, 1024 bit, 1536 bit, or 2048 bit.
<b>Online SCEP Enrollment</b>	These options are only available when the certificate type is <i>External</i> .
<b>CA Server URL</b>	Type the server URL for the external CA.
<b>Challenge Password</b>	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.

## 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:

<b>Log Threat Weight</b>	Turn on threat weight tracking.
<b>Reset</b>	Reset all the threat level definition values to their defaults.
<b>Import</b>	Import threat level definitions from a device in the ADOM.
<b>Application Protection</b>	Adjust the tracking levels for the different application types that can be tracked.
<b>Intrusion Protection</b>	Adjust the tracking levels for the different attack types that can be tracked.
<b>Malware Protection</b>	Adjust the tracking levels for the malware or botnet connections that can be detected.
<b>Packet Based Inspection</b>	Adjust the tracking levels for failed connection attempts and traffic blocked by firewall policies.
<b>Web Activity</b>	Adjust the tracking levels for various types of web activity.
<b>Risk Level Values</b>	Adjust the values for the four risk levels.

#### To assign a threat weight profile to a device:

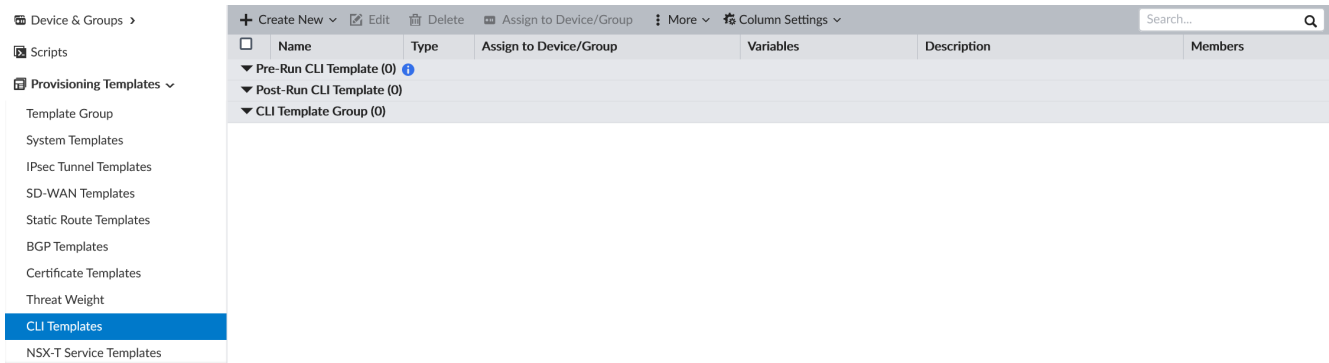
1. Select a threat weight profile and click *Assign to Device*.
2. Select devices to assign to and click *OK*.  
The devices assigned to the template are shown in the *Assign to Device* column.

## 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:

<b>Name</b>	The user-defined template name.
<b>Type</b>	The CLI template type (CLI or Jinja).
<b>Assigned Device/Group</b>	The device or device group to which the template is assigned.
<b>Variables</b>	The variables used in the script.
<b>Description</b>	User defined description for the template.
<b>Members</b>	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.

<b>Create New</b>	Create pre-run or post-run CLI templates. See <a href="#">Adding CLI templates on page 272</a> . You can also create a CLI template group. See <a href="#">CLI template groups on page 275</a> .
<b>Edit</b>	Edit the selected template or template group. See <a href="#">Editing CLI templates on page 273</a> .
<b>Delete</b>	Delete the selected template or template group. See <a href="#">Deleting CLI templates on page 273</a> .
<b>Assign to Device/Group</b>	Assign the selected template or template group to a managed device or device group. See <a href="#">Assigning CLI templates to managed devices on page 273</a> .
<b>More</b>	Select a template or template group, and click the <i>More</i> menu to access additional options including <i>Clone</i> , <i>Validate</i> , <i>Import CLI Template</i> , and <i>Export CLI Template</i> .
<b>Clone</b>	Clone the selected CLI template or template group. See <a href="#">Cloning CLI templates on page 274</a> .
<b>Validate</b>	Validate the selected CLI template. Template validation is used to determine if your template is producing the correct output based on the meta variables used. See <a href="#">Validate CLI templates on page 275</a> .
<b>Import CLI Template</b>	Import a template or template group from your management computer. See <a href="#">Importing CLI templates on page 274</a> .
<b>Export CLI Template</b>	Export a template or template group. See <a href="#">Exporting CLI templates on page 274</a> .
<b>Search</b>	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 275](#).



CLI templates do not support `execute` and `diagnose` commands. CLI templates will only work with `device` and `device VDOM` meta fields.

## Adding CLI templates

You can add pre-run and post-run CLI templates.



Pre-run CLI templates are intended for model devices and zero-touch provisioning. Pre-run CLI templates are run before provisioning 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 *Post-Run CLI Template*. The *Create New CLI Template* pane is displayed.

Create New Pre-Run CLI Template

Template Name	<input type="text"/>
Type	<div>CLI Script</div>
Comments	<div></div>
Script details	<div></div>

0/255

OK Cancel

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: <ul style="list-style-type: none"><li>• CLI Script</li><li>• Jinja Script</li></ul>
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 its appropriate category. For example, if you created a pre-run CLI template, it displays under the *Pre-Run CLI Template* category.

## 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

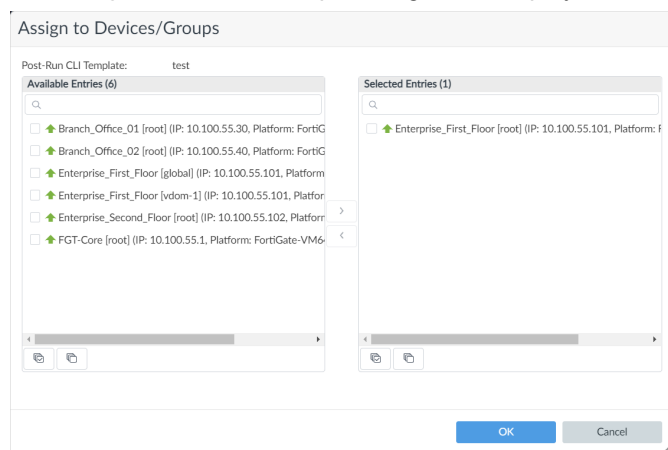
### To delete a template or templates:

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:

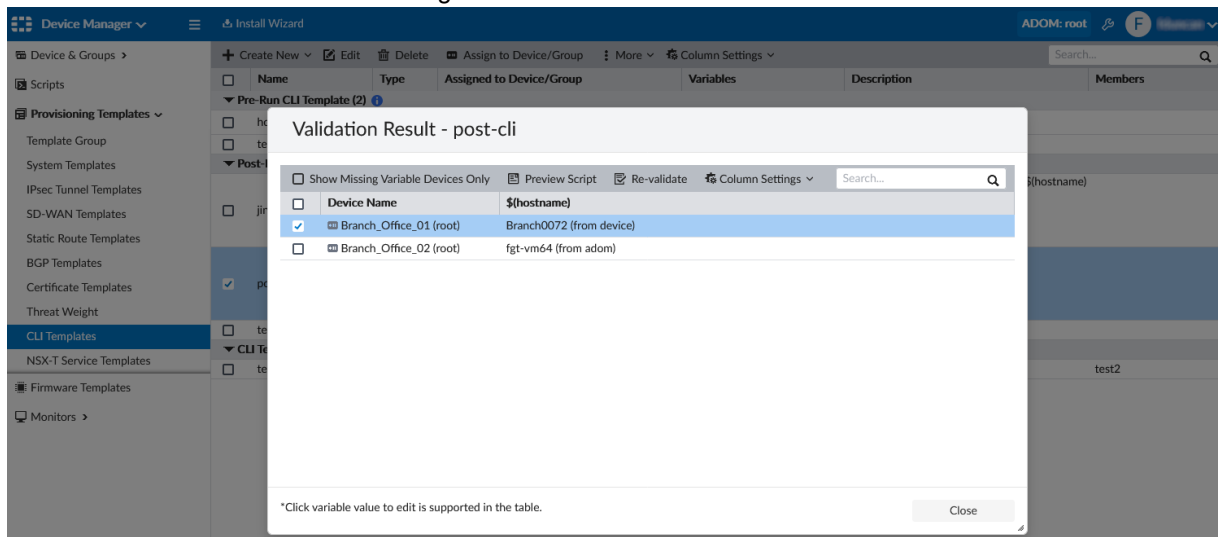
1. Go to *Device Manager > Provisioning Templates > CLI Templates*.
2. Right-click a template, and select *Export* from the menu, or select templates from the template list and click *More > Export* from the toolbar.
3. If prompted by your web browser, open the text file to view it or select a location 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 798](#).

### To validate the meta variables used in a CLI template:

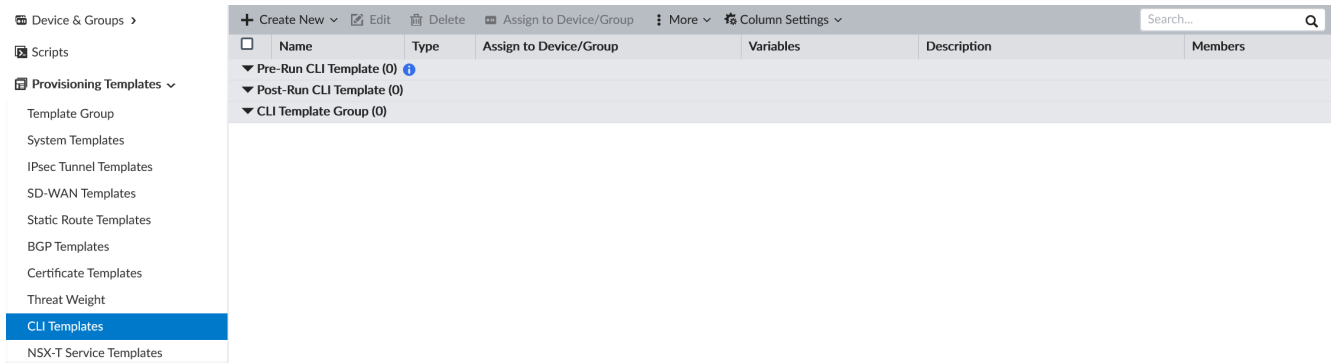
1. Go to *Device Manager > Provisioning Templates > CLI Templates*.
2. Select a template from the table that is assigned to one or more devices.
3. In the toolbar, click *More > Validate*.  
The Validate CLI Template dialog opens and displays each device to which the template is assigned, and the status 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.

Create New Template Group

Template Group Name

Comments

0/255

Members

+

\*re-order the members by dragging and dropping the item

OK

Cancel

3. Enter the required information:

<b>Template Group Name</b>	Type a unique name for the template group.
<b>Comments</b>	Optionally, type a comment for the template group.
<b>Members</b>	Click the + button to select templates or other template groups from the list, and click <b>OK</b> to add the selected entries as members.

4. Click **OK**.

## Default CLI templates

FortiManager includes the following default CLI templates:

<b>provision_interfaces_on_vm</b>	This predefined CLI template allows you to configure the number of ports that are created upon initialization of a FortiGate-VM.
<b>split_hardware_switch_ports_40_80_100</b>	This predefined CLI template allows you to configure splitting hardware switch ports for FortiGate 40F, 80E, 100E, and 100F models.
<b>split_hardware_switch_ports_60_90</b>	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 62](#).

## 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:

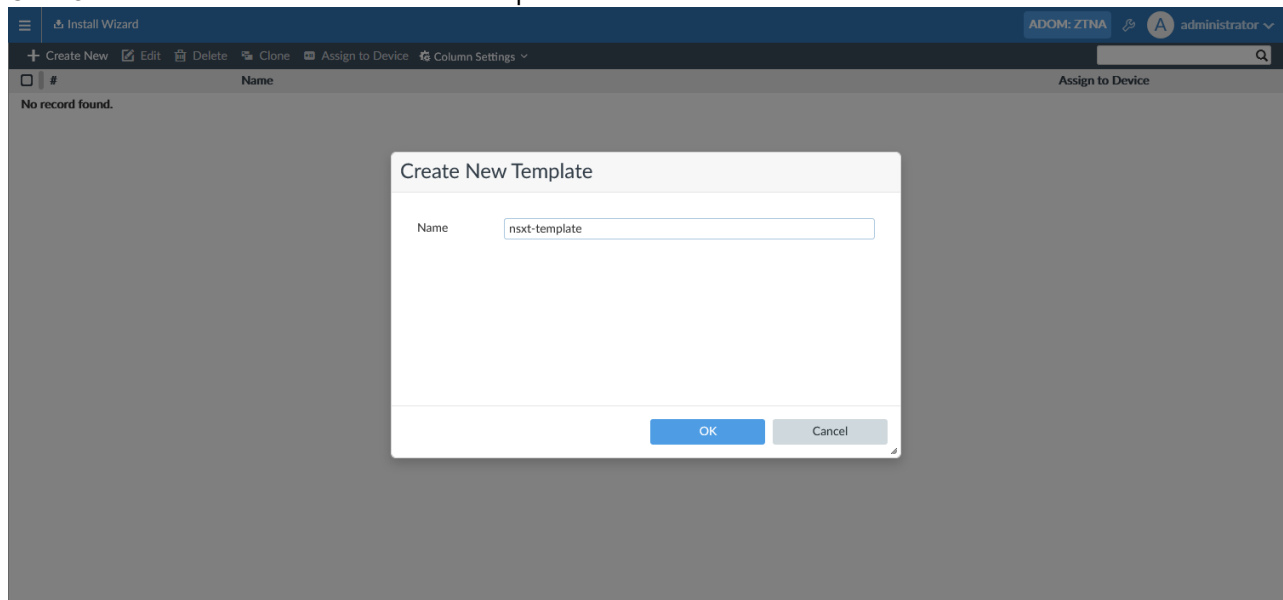
1. You need to deploy an additional VM in NSX-T.  
When a new VM is authorized in FortiManager, it has no configuration or policy. Using the NSX-T template, FortiManager automatically creates the VDOMs, links them to a policy package, and configures the service profile/VDOM association, log settings, 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:

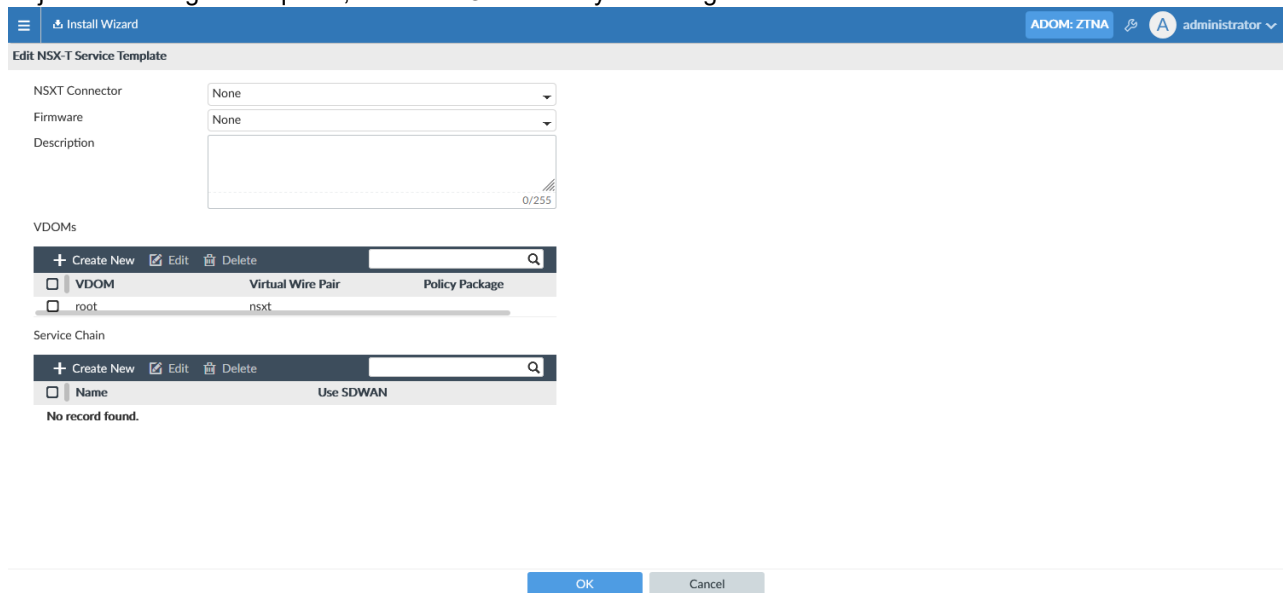
1. Go to *Device Manager > Provisioning Templates > NSX-T Service Template*.
2. Click *Create New* in the toolbar.
3. In the *Create New Template* pane, type a name for the template.

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.

Name	Remote IP	Interface	Dynamic Interface
demo--vdom_int_int	10.0.0.1	port2	
demo--vdom_int_ext	10.0.0.1	port2	

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. Right-click any template category in the sidebar, and click *Export Templates*.  
The *Export Template* dialog displays.
3. Select the template categories to export, and click *OK*.  
The *Export* dialog displays the progress of the export by template category.
4. When the export is complete, click *Close*.  
The exported JSON file can be edited offline, if needed, before it is imported to another ADOM.
5. Go to the FortiManager and/or ADOM to import the template(s).
6. In the ADOM, go to *Device Manager > Provisioning Templates*.
7. Right-click any template category in the sidebar, and click *Import Templates*.
8. The *Import Template* dialog displays.
9. 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.
10. When the import is complete, click *Close*.  
The provisioning templates are now available to edit and assign in the ADOM.

## 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 281](#).
2. Assign the firmware template to one or more devices. See [Assigning firmware templates to devices on page 284](#).  
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 286](#).
3. Preview the upgrade. See [Previewing upgrades on page 285](#).
4. View upgrade history. See [Reviewing upgrade history on page 285](#).
5. 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 283](#) and [Deleting firmware templates on page 284](#).

## 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 641](#).

---

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.

ADOM: Test7

Create New Firmware Template

Name

Description

Upgrade Details

+ Create New Edit Delete Column Settings

Platform	Upgrade to
FortiGate (0)	
FortiAP (0)	
FortiSwitch (0)	
FortiExtender (0)	

Install Window

Schedule Type: None Once Daily Weekly

Upgrade Options

☐ Boot From Alternate Partition After Upgrade

☐ Let Device Download Firmware From FortiGuard

Upgrade Path

☒ Skip All Intermediate Steps In Upgrade Path If Possible

☐ Follow The Recommended Upgrade Path

OK Cancel

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.

Create New Upgrade Firmware

Product: FortiGate

Platform:

Upgrade to: None

OK Cancel

b. In the *Product* list, select a product to upgrade.

c. In the *Platform* list, select the platform for the product.

d. In the *Upgrade to* list, 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:

<b>Schedule Type</b>	Specify whether to schedule the upgrade by selecting one of the following options: <ul style="list-style-type: none"> <li>• <i>None</i>: Select to have no schedule.</li> <li>• <i>Once</i>: Select to schedule the upgrade to occur once.</li> <li>• <i>Daily</i>: Select to schedule the upgrade to occur daily.</li> <li>• <i>Weekly</i>: Select to schedule the upgrade to occur weekly.</li> </ul>
<b>Day</b>	Available when you select <i>Weekly</i> . Select what day of the week to run the upgrade.
<b>Start Time</b>	Available when you select <i>Once</i> , <i>Daily</i> , or <i>Weekly</i> . Specify what time to start the upgrade.
<b>End Time</b>	Available when you select <i>Once</i> , <i>Daily</i> , or <i>Weekly</i> . 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:

<b>Boot from Alternate Partition After Upgrade</b>	Applies only to FortiGates. Select to upgrade the inactive partition. Clear to skip the inactive partition during upgrade.
<b>Let Device Download Firmware from FortiGuard</b>	Select to have the device download the firmware from FortiGuard for the upgrade. Clear to have the device download the firmware from FortiManager.

7. In the *Upgrade Path* area, set the following options:

<b>Skip All Intermediate Steps in Upgrade Path If Possible</b>	Select to skip some builds in an upgrade path.
<b>Follow The Recommended Upgrade Path</b>	Select to install all builds in an upgrade path.
<div style="display: flex; align-items: center;">  <div> <p>The <i>Follow The Recommended Upgrade Path</i> 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 <a href="https://support.fortinet.com">support.fortinet.com</a>.</p> </div> </div>	

8. Click **OK**.  
The upgrade template is created.
9. Assign the template to one or more devices.

## 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:**

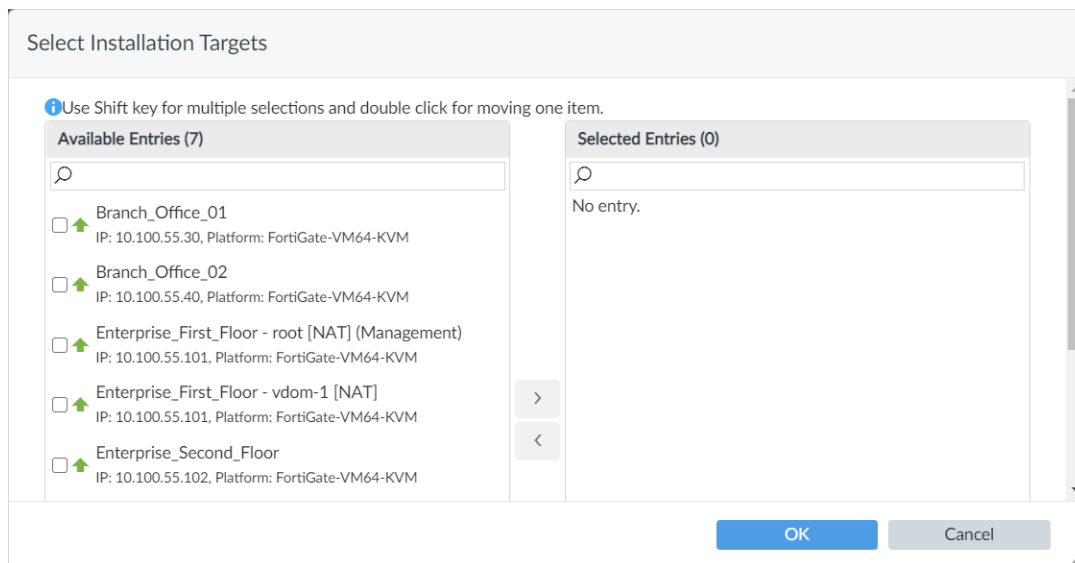
1. Go to *Device Manager > Firmware Templates*.  
The firmware templates are displayed in the content pane.
2. Select a template, and click *Delete*.  
Alternately you can right-click the template, and select *Delete*.  
The template is deleted.

## 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.

## Monitors

Use the monitors tree menu to access the following monitors:

- [SD-WAN Monitor on page 286](#)
- [VPN Monitor on page 291](#)
- [Asset Identity Center on page 292](#)
- [AI Analysis on page 294](#)

## 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 286](#)
- [Table View on page 287](#)
- [Enabling SD-WAN monitoring history on page 290](#)

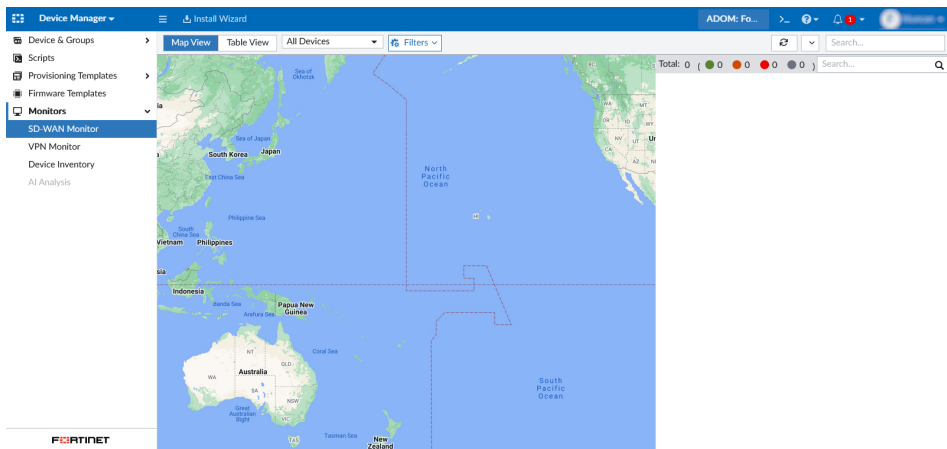
### Map View

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.





- (Optional) Click the *Filters* dropdown to view options to *Show Unhealthy Devices Only* and/or *Show Unhealthy Interfaces Only*.
- 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 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.

#### To monitor SD-WAN with Table View:

- Click *Table View* to view the SD-WAN parameters for each device.

Device	SD-WAN Interface	Upload	Download	Amazon-AWS	Amazon-Web	Microsoft-Office365	Microsoft-Skype_Teams	Snap-Snapchat
FGT-VM64-154[root]	port1	0%	0%					
	port2	0%	0%					
	port3	0%	0%					
	vpn7-1	0%	0%					
FGT-VM64-155								

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.

**Applications**

Add or remove the *Applications* from the *Services Settings* drop-down. 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.

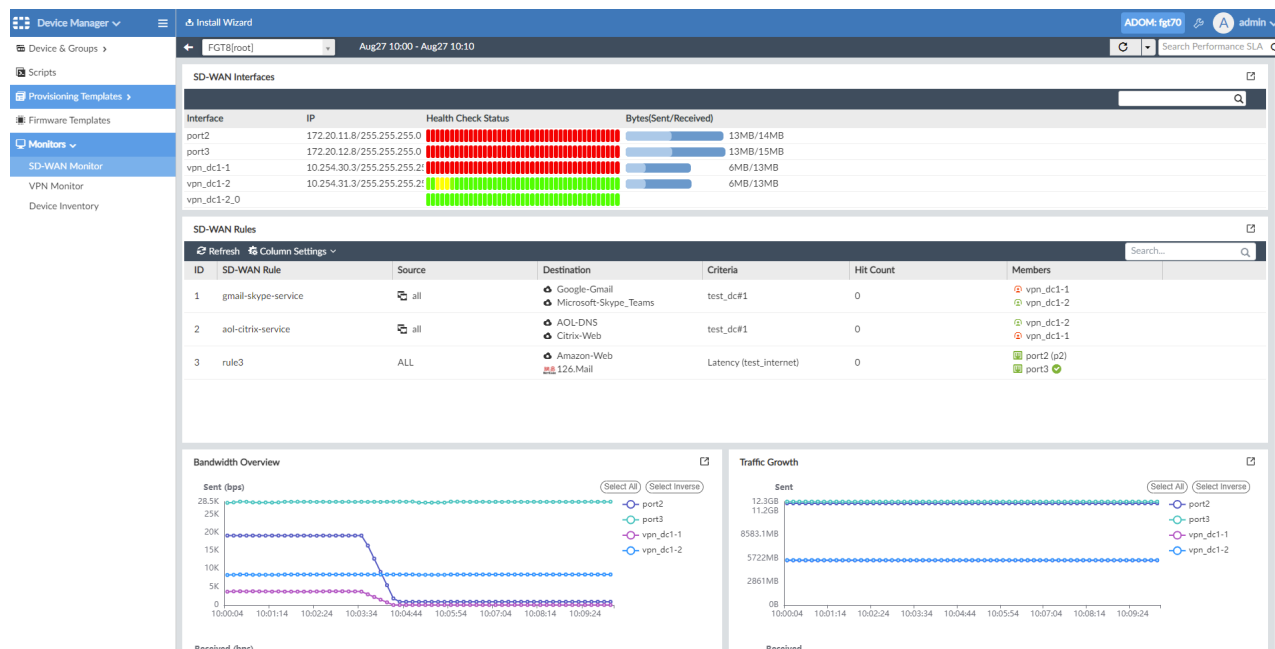
You can select *Manual Refresh* to refresh the data manually.



Hover over a service for a device that is shown in red. A pop-up shows the parameters that have failed the SLA criteria.

- (Optional) Click the *Filters* dropdown to view options to *Show Unhealthy Devices Only* and/or *Show Unhealthy Interfaces Only*.
- 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 290](#).



- 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.
- Hover over the charts to view additional details.

## 6. 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.

The screenshot shows the FortiManager interface with the SD-WAN configuration page. The left sidebar contains navigation options like Device Manager, Scripts, Provisioning Templates, Firmware Templates, Monitors, SD-WAN Monitor, VPN Monitor, and Device Inventory. The main content area displays the SD-WAN Interfaces table, which lists interfaces and their health check status. The SD-WAN Rules table is also visible, showing rules and their associated interfaces. The Interface Details panel for vpn\_dc1-1 is open, showing various settings like Link, Port Speed, Type, Role, IPv4 Addresses, SD-WAN Member ID, SD-WAN Zone, Bandwidth, and Performance SLA.

- 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.

The screenshot shows the FortiManager interface with the SD-WAN configuration page. The left sidebar contains navigation options like Device Manager, Scripts, Provisioning Templates, Firmware Templates, Monitors, SD-WAN Monitor, VPN Monitor, and Device Inventory. The main content area displays the SD-WAN Rules table, which lists rules and their associated interfaces. The table includes columns for ID, SD-WAN Rule, Source, Destination, Criteria, Hit Count, and Members. The Members column shows the interfaces selected for each rule, with a tooltip indicating that a member is selected (meets SLA).

- View interface statistics, including SLAs tied to that interface, upstream and downstream bandwidth, IP addresses, link speed, and more.

The screenshot shows the FortiManager interface with the SD-WAN configuration page. The left sidebar contains navigation options like Device Manager, Scripts, Provisioning Templates, Firmware Templates, Monitors, SD-WAN Monitor, VPN Monitor, and Device Inventory. The main content area displays the SD-WAN Interfaces table, which lists interfaces and their health check status. The SD-WAN Rules table is also visible, showing rules and their associated interfaces. The Interface Details panel for vpn\_dc1-1 is open, showing various settings like Link, Port Speed, Type, Role, IPv4 Addresses, SD-WAN Member ID, SD-WAN Zone, Bandwidth, and Performance SLA.

## 7. In the toolbar, click the *Go Back* arrow to exit the pane.

## 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 drilldown 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 [Configuring monitoring history storage on page 290](#).

## Configuring monitoring history storage

You can configure SD-WAN monitoring history using the following commands in the CLI.

- `rtm-max-monitor-by-days`: Maximum RTM monitor (sd-wan, traffic shaping, etc) history by days (1-180).
- `rtm-temp-file-limit`: Set the RTM monitor temp file limit by hours. A lower value will reduce disk usage, but may cause data loss (1 -120).

For example:

```
config system admin setting
  set sdwan-monitor-history enable
  set rtm-max-monitor-by-days <1-180>
  set rtm-temp-file-limit <1-120>
```



These commands are only available when SD-WAN monitoring history is enabled.

---

## 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 [Configuring monitoring history storage on page 290](#). 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.

## VPN Monitor

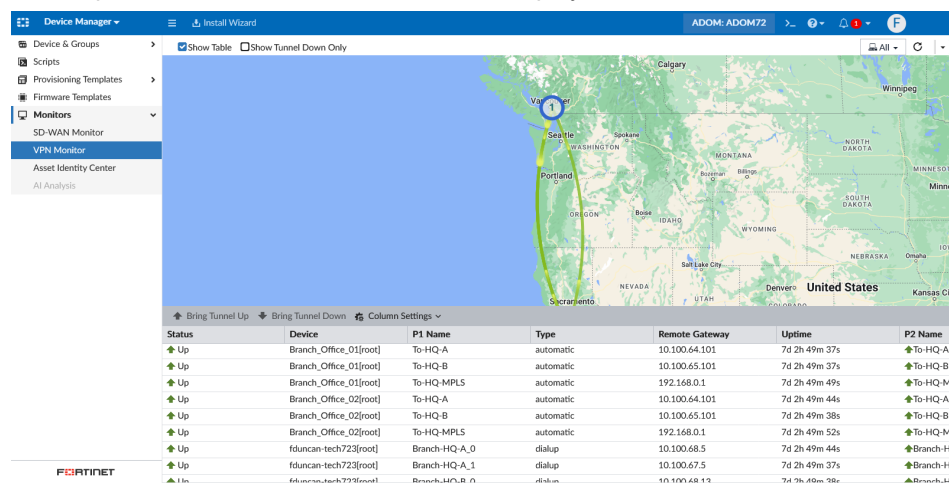
The VPN Monitor displays IPSec VPN tunnels created by IPSec Templates and the SD-WAN Overlay Wizard, with specific device icon identification for HUBs and the ability to drill down to a device group level.

For additional VPN monitoring options, see [VPN Manager on page 511](#).

### To view the VPN Monitor:

1. Go to *Device Manager > Monitors > VPN Monitor*.

The map view of traffic for all communities 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.

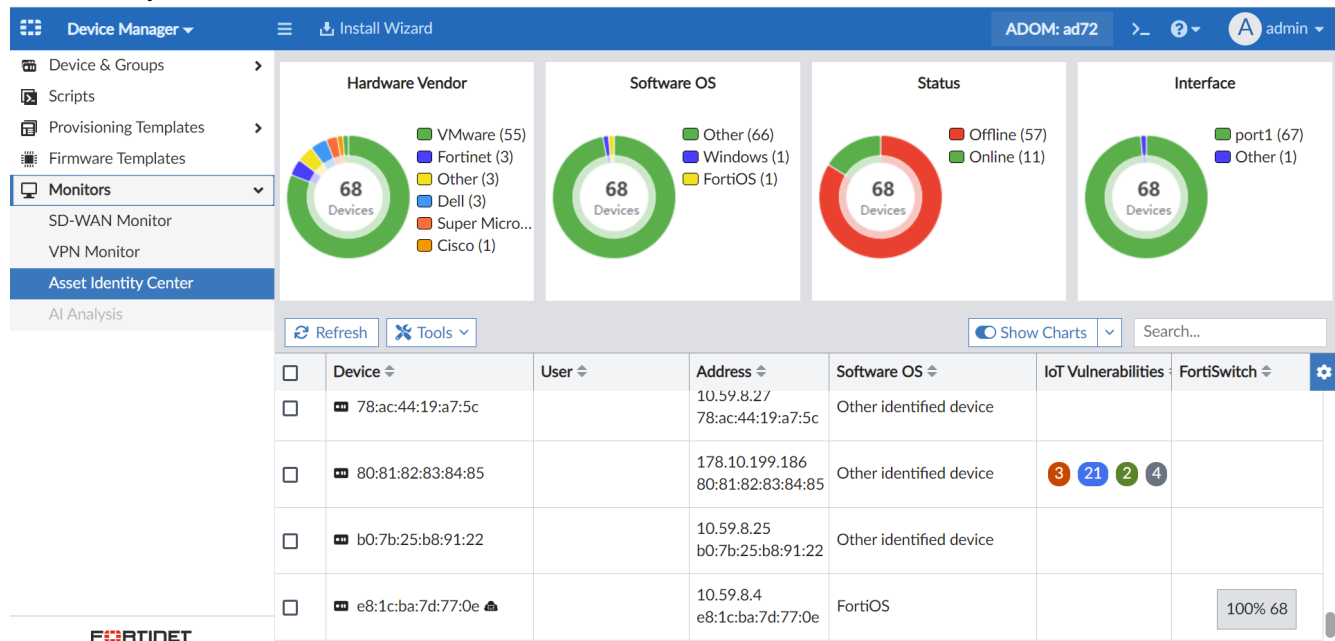
- To view a single device's IPsec VPN tunnel information, change *All* to *Others* in the toolbar menu, and select a device from the dropdown.
- To view a device group's IPsec VPN tunnel information, change *All* to *Others* in the toolbar menu, and select a device group from the dropdown.
- To view 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:

- |                          |  |
|--------------------------|--|
| <b>Bring Tunnel Up</b>   | Select a device in the table with a status of <i>Down</i> , and click <i>Bring Tunnel Up</i> . |
| <b>Bring Tunnel Down</b> | Select a device in the table with a status of <i>Up</i> , and click <i>Bring Tunnel Down</i> . |
| <b>Column Settings</b>   | Click to select which columns to hide and display.   |

## 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:

- 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.
- 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:

<b>Hardware Vendor</b>	Displays the distribution of hardware vendors for detected devices.
<b>Software OS</b>	Displays the distribution of software OS for detected devices.

<b>Status</b>	Displays the status (online or offline) of detected devices.
<b>Interface</b>	Displays the distribution of interfaces used in detected devices.
<b>FortiSwitch</b>	Displays the distribution of FortiSwitch devices.
<b>FortiAP</b>	Displays the distribution of FortiAP devices.
<b>WiFi SSID</b>	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.

The screenshot displays the FortiManager Device Manager interface. The top navigation bar includes 'Device Manager', 'Install Wizard', and user information 'ADOM: ad72' and 'admin'. The left sidebar lists navigation options: 'Device & Groups', 'Scripts', 'Provisioning Templates', 'Firmware Templates', 'Monitors' (selected), 'SD-WAN Monitor', 'VPN Monitor', 'Asset Identity Center', and 'AI Analysis'.

The main content area shows four donut charts: 'Hardware Vendor' (68 Devices), 'Software OS' (68 Devices), 'Status' (68 Devices), and 'Interface' (68 Devices). Below these charts is a table of devices with columns: Device, User, Address, Software OS, IoT Vulnerabilities, and FortiSwitch. A 'View Vulnerabilities' tooltip is visible over the 'IoT Vulnerabilities' column.

The 'View IoT Vulnerabilities for Device' window is open, showing a table of vulnerabilities for the device 'netgear d6200 1.0.0.60'. The table has columns: Vulnerability ID, Severity, Reference, and Description. The vulnerabilities listed are:

Vulnerability ID	Severity	Reference	Description
1254	High		Certain NETGEAR devices are affected by CSRF. This affects D6200 before 1.1.00.38
1256	High		Certain NETGEAR devices are affected by authentication bypass. This affects D6200
1252	Medium		Certain NETGEAR devices are affected by incorrect configuration of security settings
1257	Medium		Certain NETGEAR devices are affected by authentication bypass. This affects D6200
1258	Medium		Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauth
1260	Medium		Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauth
1261	Medium		Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauth
1262	Medium		Certain NETGEAR devices are affected by command injection by an authenticated us
1259	Low		Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1
1263	Low		Certain NETGEAR devices are affected by stored XSS. This affects D360

The window also shows a progress bar for the IoT Application: axis p3364v 5.50 (10) with a value of 0% 33. A 'Close' button is at the bottom right.

## AI Analysis

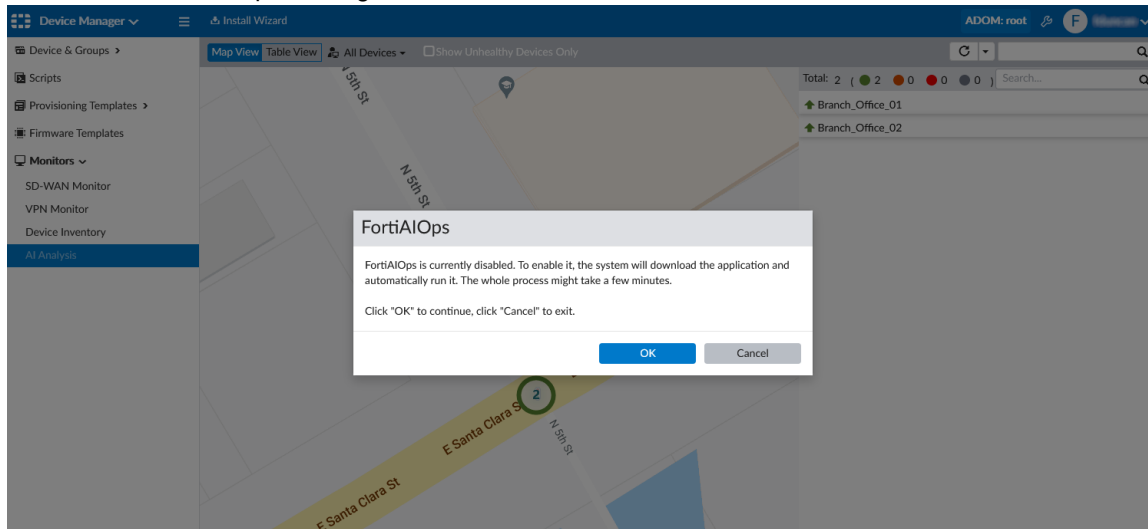
The AI Analysis monitor can be enabled in *Device Manager > Monitors* to redirect to the FortiAI Ops management extension.

### 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 FortiAI Ops is displayed.



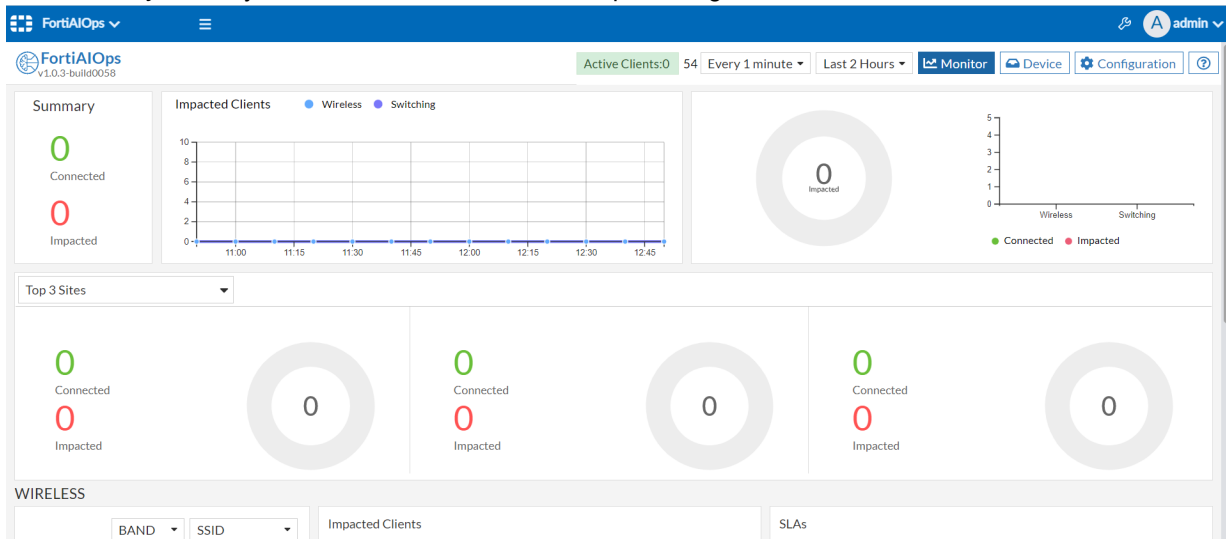
3. Click **OK**, and FortiAI Ops will begin to download.



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 FortiAI Ops management extension.



## FortiMeter

FortiMeter allows you turn FortiOS-VMs and FortiWebOS-VMs on and off as needed, paying only for the volume and consumption of traffic that you use. These VMs are also sometimes called pay-as-you-go VMs.

You must meet the following requirements to use metered VMs:

- You must have a FortiMeter license.
- The FortiMeter license must be linked with the FortiManager unit by using FortiCare.

## FortiOS VMs

FortiManager supports the following types of licenses for FortiMeter:

- Prepaid: FortiOS VM usage is prepaid by purchasing points.
- Postpaid: The FortiOS VM is billed monthly based on usage.

The license determines whether FortiMeter is prepaid or postpaid.

The VM deployment packages are included with firmware images on the [Customer Service & Support](#) site, and have the following format: FOS\_VMxx-vXx-buildXXXX-Fortinet.out. In FortiManager, the VM will be listed as a FortiOS VM.

FortiManager also supports metering for FortiOS VM HA clusters.

## FortiWeb VMs

FortiManager supports FortiWeb devices as logging devices. FortiWeb VMs are billed monthly based on usage.

The VM deployment packages are included with firmware images on the [Customer Service & Support](#) site, and have the following format: FWB\_OS1-vXxx-buildXXXX-FORTINET.out. In FortiManager, the VM will be listed as a FBV0X.

## Overview



FortiManager VM with a subscription license does not support FortiMeter.

The following is an overview of how to use metered VMs:

1. Purchase a FortiMeter license. Contact your sales representative for more information.
2. Go to [FortiCare](https://support.fortinet.com/) (https://support.fortinet.com/) and log into your account.  
You can also access FortiCare from FortiManager:
  - From *System Settings > Dashboard*, in the *License Information* widget, click the *Purchase* icon in the *VM Meter Service* field.
  - From *Device Manager > VM Meter*, click the *Purchase Points* icon in the toolbar.
3. Go to *Asset > Manage/View Products*, and locate the FortiMeter license.
4. Link the FortiMeter license with your FortiManager by using the *Link Device* option.  
You can only link FortiManager to one metering group at a time.
5. If you are prepaying (FortiOS VMs only), purchase a point package and add it to the FortiMeter license using the *Add Licenses* option. See [Points on page 297](#).
6. Ensure that the VM is authorized for central management by FortiManager. See [Add devices on page 51](#).
7. Authorize the metered VMs in FortiManager. See [Authorizing metered VMs on page 297](#).



If connectivity between the VM and FortiManager is lost, FortiManager will invalidate the VM instance after fifteen days. If the VM reconnects before fifteen days have elapsed, it will automatically synchronize with the FortiManager database.

## Points

Points can be purchased in packages of 1000 or 10000 from the FortiMeter product information page on FortiCare using the *Add Licenses* button.

Points are used based on the type of service and the volume of traffic sent to FortiGuard.

Type	Service Code	Points
VOLUME (1TB)	FW	4
VOLUME (1TB)	FWURL	10
VOLUME (1TB)	UTM	25

For prepaid FortiOS VMs, after the point balance has become negative, VMs can continue to be used for up to 15 days before the account is frozen or more points are purchased to restore a positive point balance.

With a negative point balance, the FortiMeter status will show the number of days until it is frozen, or *FREZ* when it is already frozen. FortiMeter will be unfrozen when a positive point balance is restored.

For FortiOS VM HA clusters, only the primary unit sends traffic to FortiMeter.

## Authorizing metered VMs

You must authorize all metered VMs in FortiManager before you can use them.

### Authorizing FortiOS VMs

FortiOS VMs must be authorized for central management by FortiManager before they can be authorized for metering. See [Add devices on page 51](#).

#### To authorize metered FortiOS VMs:

1. Ensure that the VM is authorized for central management by FortiManager. See [Add devices on page 51](#).
2. Ensure you are in the correct ADOM.
3. Go to *Device Manager > VM Meter*.
4. Select a device then click *Authorize* in the toolbar, right-click on a device then select *Authorize*, or double-click on a device. The *Authorize Device(s)* dialog box opens.  
An unauthorized device can use firewall services for up to 48 hours.
5. Select the *License Type*:

<b>Trial</b>	Maximum of two devices can have a trial license at any one time. No traffic data are sent to FortiGuard, so no points are used. Can be used for up to 30 days.
<b>Regular</b>	Regular license. Points used based on the service level and volume of traffic going to FortiGuard.

6. Select the *Services*:

<b>Firewall</b>	Firewall only. This option cannot be deselected.
<b>IPS</b>	IPS services.
<b>Web Filter</b>	Web filtering services.
<b>AntiVirus</b>	Antivirus services.
<b>App Control</b>	Application control services.
<b>Full UTM</b>	All services are selected.

7. Click *OK* to authorize the device.

## Authorizing FortiWeb VMs

FortiWeb VMs must be authorized for central management by FortiManager before they can be authorized for metering. See [Authorizing devices on page 71](#).

### To authorize metered FortiWeb VMs:

1. Ensure that the FortiWeb VM is authorized for central management by FortiManager. See [Add devices on page 51](#).
2. In the FortiWeb ADOM, go to *Device Manager > VM Meter*.
3. Select a device then click *Authorize* in the toolbar, right-click on a device then select *Authorize*, or double-click on a device. The *Authorize Device(s)* dialog box opens.
4. On the *Authorize Device* pane, confirm the devices name and serial number.  
The *License Type* is *Regular* - points are used based on the volume of traffic. The *Services - Security, Antivirus, IP Reputation* - cannot be deselected.
5. Click *OK* to authorize the device.

## Monitoring VMs

Go to *Device Manager > VM Meter*. For prepaid licenses (FortiOS VMs only), your total remaining point balance is shown in the toolbar. For postpaid licenses, the total points used and the billing period are shown.

You can also view details about the individual VMs, including: the device name and serial number, number of virtual CPUs, amount of RAM, service level, license status, volume of traffic used today, and more.

## 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 [Advanced Settings on page 804](#) 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*:

<b>Name</b>	Type a unique name for the chassis.
<b>Description</b>	Optionally, type any comments or notes about this chassis.
<b>Chassis Type</b>	Select the chassis type: Chassis 5050, 5060, 5140 or 5140B.
<b>IP Address</b>	Type the IP address of the Shelf Manager running on the chassis.
<b>Authentication Type</b>	Select Anonymous, MD5, or Password from the dropdown list.
<b>Admin User</b>	Type the administrator user name.
<b>Password</b>	Type the administrator password.
<b>Chassis Slot Assignment</b>	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:

<b>Refresh</b>	Select to update the current page. If there are no entries, Refresh is not displayed.
<b>Slot #</b>	The slot number in the chassis. <ul style="list-style-type: none"> <li>The FortiGate 5050 chassis contains five slots numbered 1 to 5.</li> <li>The FortiGate 5060 chassis contains six slots numbered 1 to 6.</li> <li>The FortiGate 5140 and 5140B chassis contains fourteen slots numbered 1 to 14.</li> </ul>
<b>Extension Card</b>	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.
<b>Slot Info</b>	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.
<b>State</b>	Indicates whether the card in the slot is installed or running, or if the slot is empty.
<b>Temperature Sensors</b>	Indicates if the temperature sensors for the blade in each slot are detecting a temperature within an acceptable range. <ul style="list-style-type: none"> <li><i>OK</i>: All monitored temperatures are within acceptable ranges.</li> <li><i>Critical</i>: A monitored temperature is too high (usually about 75°C or higher) or too low (below 10°C).</li> </ul>
<b>Current Sensors</b>	Indicates if the current sensors for the blade in each slot are detecting a current within an acceptable range. <ul style="list-style-type: none"> <li><i>OK</i>: All monitored currents are within acceptable ranges.</li> <li><i>Critical</i>: A monitored current is too high or too low.</li> </ul>
<b>Voltage Sensors</b>	Indicates if the voltage sensors for the blade in each slot are detecting a voltage within an acceptable range. <ul style="list-style-type: none"> <li><i>OK</i>: All monitored voltages are within acceptable ranges.</li> <li><i>Critical</i>: A monitored voltage is too high or too low.</li> </ul>
<b>Power Allocated</b>	Indicates the amount of power allocated to each blade in the slot.
<b>Action</b>	Select <i>Activate</i> to turn the state of a blade from <i>Installed</i> into <i>Running</i> . Select <i>Deactivate</i> to turn the state of a blade from <i>Running</i> into <i>Installed</i> .
<b>Edit</b>	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.
<b>Update</b>	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:

<b>Refresh</b>	Select to update the current page.
<b>PEM</b>	The order numbers of the PEM in the chassis.
<b>Presence</b>	Indicates whether the PEM is present or absent.
<b>Temperature</b>	The temperature of the PEM.
<b>Temperature State</b>	Indicates whether the temperature of the PEM is in the acceptable range. <ul style="list-style-type: none"> <li>• <i>OK</i>: The temperature is within acceptable range.</li> </ul>
<b>Threshold</b>	PEM temperature thresholds.
<b>Feed -48V</b>	Number of PEM fuses. There are four pairs per PEM.
<b>Status</b>	PEM fuse status: present or absent.
<b>Power Feed</b>	The power feed for each pair of fuses.
<b>Maximum External Current</b>	Maximum external current for each pair of fuses.
<b>Maximum Internal Current</b>	Maximum internal current for each pair of fuses.
<b>Minimum Voltage</b>	Minimum voltage for each pair of fuses.
<b>Power Available</b>	Available power for each pair of fuses.
<b>Power Allocated</b>	Power allocated to each pair of fuses.
<b>Used By</b>	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:

<b>Refresh</b>	Select to update the current page.
----------------	------------------------------------

<b>Thresholds</b>	Displays the fan tray thresholds.
<b>Fan Tray</b>	The order numbers of the fan trays in the chassis.
<b>Model</b>	The fan tray model.
<b>24V Bus</b>	Status of the 24V Bus: present or absent.
<b>-48V Bus A</b>	Status of the -48V Bus A: present or absent.
<b>-48V Bus B</b>	Status of the -48V Bus B: present or absent.
<b>Power Allocated</b>	Power allocated to each fan tray.
<b>Fans</b>	Fans in each fan tray.
<b>Status</b>	The fan status. <ul style="list-style-type: none"> <li>OK: It is working normally.</li> </ul>
<b>Speed</b>	The fan speed.

## Viewing shelf manager status

Go to *[chassis name] > Shelf Manager* to view the shelf manager status.

The following is displayed:

<b>Refresh</b>	Select to update the current page.
<b>Shelf Manager</b>	The order numbers of the shelf managers in the chassis.
<b>Model</b>	The shelf manager model.
<b>State</b>	The operation status of the shelf manager.
<b>Temperature</b>	The temperature of the shelf manager.
<b>-48V Bus A</b>	Status of the -48V Bus A: present or absent.
<b>-48V Bus B</b>	Status of the -48V Bus B: present or absent.
<b>Power Allocated</b>	Power allocated to each shelf manager.
<b>Voltage Sensors</b>	Lists the voltage sensors for the shelf manager.
<b>State</b>	Indicates if the voltage sensors for the shelf manager are detecting a voltage within an acceptable range. <ul style="list-style-type: none"> <li>OK: All monitored voltages are within acceptable ranges.</li> <li>Below lower critical: A monitored voltage is too low.</li> </ul>
<b>Voltage</b>	Voltage value for a voltage sensor.
<b>Edit</b>	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:

<b>Presence</b>	Indicates if the SAP is present or absent.
<b>Telco Alarm</b>	Telco form-c relay connections for minor, major and critical power faults provided by the external dry relay Telco alarm interface (48VDC).
<b>Air Filter</b>	Indicates if the air filter is present or absent.
<b>Model</b>	The SAP model.
<b>State</b>	The operation status of the shelf manager.
<b>Power Allocated</b>	Power allocated to the SAP.
<b>Temperature Sensors</b>	The temperature sensors of the SAP
<b>Temperature</b>	The temperature of the SAP read by each sensor.
<b>State</b>	Indicates if the temperature sensors for the SAP are detecting a temperature below the set threshold.
<b>Edit</b>	Select to modify the thresholds of a temperature sensor.

# Policy & Objects

The *Policy & Objects* pane enables you to centrally manage and configure the devices that are managed by the FortiManager unit. This includes the basic network settings to connect the device to the corporate network, antivirus definitions, intrusion protection signatures, access rules, and managing and updating firmware for the devices.

All changes related to policies and objects should be made on the FortiManager device, and not on the managed devices.



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 839](#).



If *Display Policy & Objects in Dual Pane* is enabled, the *Policy Packages* and *Object Configurations* tabs will be shown on the same pane, with *Object Configurations* on the lower half of the screen. See [Feature visibility on page 309](#).



If workspace is enabled, the ADOM must be locked before changes can be made. See [Locking an ADOM on page 770](#).

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 854](#).


#	Name	From	To	Source	Destination	Schedule	Service	Users
1	port1 -> port2 (1-1 / Total: 1)	port1	port2	all	all	always	ALL	
2	Implicit Deny (2-2 / Total: 1)	any	any	all	all	always	ALL	

The following sections are available in the tree menu in *Policy & Objects*:

Policy Packages	Click to view configured policy packages and folders in the tree menu.
Object Configurations	Click to view configurable objects in the tree menu.

If *Display Policy & Objects in Dual Pane* is enabled, both tabs will be shown on the same pane.

The following options are available on the *Policy Packages* tab:

<b>Policy Package</b>	Click to access the policy package menu. The menu options are the same as the right-click menu options.
<b>Install</b>	Click to access the Install menu. You can start the Install Wizard where you can install policy packages and device settings. You can also re-install a policy.
<b>ADOM Revisions</b>	Click to create, edit, delete, restore, lock, and unlock ADOM Revisions.
<b>Tools</b>	Click to select one of the following tools from the menu: <i>Find Unused Objects</i> , <i>Find Duplicate Objects</i> , <i>Find Unused Policies</i> , <i>Refresh Hit Counts</i> , <i>Feature Visibility</i> , or <i>Object Selection Pane</i> .
<b>Create New</b>	Create a new policy. See <a href="#">Creating policies on page 329</a> .
<b>Edit</b>	Edit a policy. See <a href="#">Editing policies on page 329</a> .
<b>Delete</b>	Delete a policy.
<b>Section</b>	Create a new policy section. You can apply colors to policy sections to help differentiate your different policies in the table. See <a href="#">Managing policies on page 322</a> .
<b>Policy Lookup</b>	Perform a policy lookup. See <a href="#">Policy Lookup on page 328</a>
<b>Collapse/Expand All</b>	Collapse or expand all the categories in the policy list.
<b>Column Settings</b>	Select which columns are displayed in the policy table.
<b>View Mode</b>	Toggle between the <i>By Sequence</i> and <i>Interface Pair View</i> display modes. See <a href="#">Managing policies on page 322</a> .
<div>  <p>View Mode is disabled when policy packages include policies using multiple source/destination interfaces (including the "Any" interface) or when policy blocks are used.</p> </div>	
<b>Search</b>	The tree menu can be searched and sorted using the search field and sorting button at the top of the menu.

The following options are available on the *Objects Configurations* tab:

<b>ADOM Revisions</b>	Click to create, edit, delete, restore, lock, and unlock ADOM Revisions.
<b>Tools</b>	Click to select one of the following tools from the menu: <i>Find Unused Objects</i> , <i>Find Duplicate Objects</i> , <i>Find Unused Policies</i> , <i>Refresh Hit Counts</i> , <i>Feature Visibility</i> , or <i>Object Selection Pane</i> .
<b>Create New</b>	Create a new object. See <a href="#">Create a new object on page 403</a> .
<b>Edit</b>	Edit an object. See <a href="#">Edit an object on page 421</a> .
<b>Delete</b>	Delete an object. See <a href="#">Remove an object on page 421</a> .
<b>More</b>	Select the dropdown to view additional options for objects.
<b>Column Settings</b>	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:

<b>Lock   Unlock</b>	Select to lock or unlock the ADOM.
<b>Sessions</b>	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 313](#).

Policy Blocks can be used within Global Policy packages. See [Using Policy Blocks on page 398](#).

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 401](#).

## 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.

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.

### To view policies and objects on a single pane:

1. Go to *System Settings > Advanced > Advanced Settings*.
2. Enable *Display Policy & Objects in Dual Pane*.
3. Click *Apply*.

The *Policy & Objects* pane will now display both the *Policy Packages* and *Object Configuration* tree menu panes at the same time.

The screenshot shows the FortiManager interface with the *Policy & Objects* pane. The left sidebar contains two main sections: *Policy Packages* and *Object Configurations*. The *Policy Packages* section is expanded, showing a search bar and a list of policies including *Branch\_Office\_01*, *Firewall Policy*, *Installation Targets*, *Enterprise\_First\_Floor*, *Enterprise\_Second\_Floor*, *FGT*, and *default*. The *Object Configurations* section is also expanded, showing a search bar and a list of objects including *Normalized Interface*, *Virtual Wire Pair*, *Firewall Objects*, *Security Profiles*, *Fabric Connectors*, and *User & Authentication*. The main content area displays two tables. The top table, titled *Policy Packages*, shows a list of policies with columns: *#*, *Name*, *From*, *To*, *Source*, *Destination*, *Schedule*, *Service*, and *Users*. The bottom table, titled *Object Configurations*, shows a list of objects with columns: *Normalized Interface*, *Mapping Rule*, *Mapped Interface/Zone*, *Description*, and *Created Time*.

#	Name	From	To	Source	Destination	Schedule	Service	Users
1	FW_Policy	any	any	all	all	always	ALL	
Implicit (2-2 / Total: 1)								
2	Implicit Deny	any	any	all	all	always	ALL	

Normalized Interface	Mapping Rule	Mapped Interface/Zone	Description	Created Time
any				
sslvpn_tun_intf				
a			added by creating adom	2021-03-30 08:42:10
	Per-platform (FortiGate-40F)	a		
	Per-platform (FortiGate-40F-3G4G)	a		
	Per-platform (FortiGate-60F)	a		
	Per-platform (FortiGate-61F)	a		
	Per-platform (FortiWiFi-40F)	a		
	Per-platform (FortiWiFi-40F-3G4G)	a		

## 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 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.



Create New Policy Package

Name

Central NAT

OFF

NGFW Mode ⓘ

Profile-based

Policy-based

Policy Offload Level

Disable

In Folder

OK

Cancel

4. Configure the following details, then click **OK** to create the policy package.

<b>Name</b>	Enter a name for the new policy package.
<b>Central NAT</b>	Select the <i>Central NAT</i> check box to enable <i>Central SNAT</i> and <i>Central DNAT</i> policy types.
<b>NGFW Mode</b>	Select the NGFW mode, <i>Profile-based</i> (default) or <i>Policy-based</i> .
<b>SSL/SSH Inspection</b>	Select an SSL/SSH inspection type from the dropdown list. This option is only available for version 5.6 and later ADOMs when <i>NGFW Mode</i> is <i>Policy-based</i> .
<b>Consolidated Firewall Mode</b>	Toggle the <i>Consolidated Firewall Mode</i> button to <i>ON</i> to create a consolidated IPv4 and IPv6 policy. By default, the button is turned to <i>OFF</i> .
<b>Policy Offload Level</b>	Select the policy offload level. When configuring hyperscale policies, select <i>Full Offload</i> .
<b>In Folder</b>	Optionally, click the <i>In Folder</i> 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.

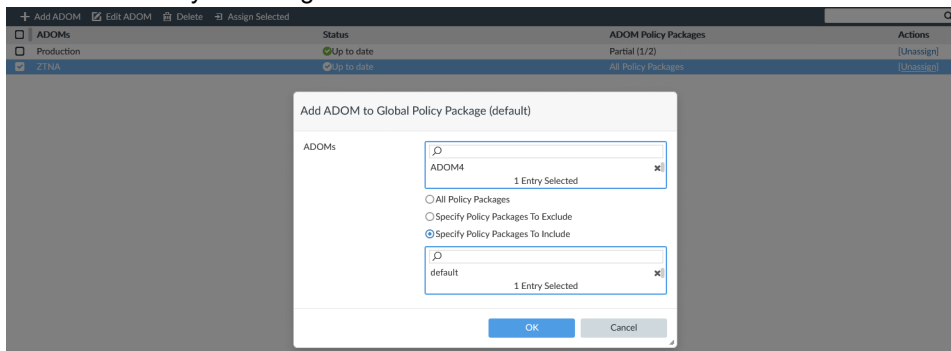
### To assign a global policy package:

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.

ADOMs	Status	ADOM Policy Packages	Actions
ADOM4	Up to date	All Policy Packages	<a href="#">Assign</a>
ZTNA	Up to date	All Policy Packages	<a href="#">Assign</a>

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 [Install policies only to specific devices on page 332](#).

### 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 121](#). For more information on editing the installation targets, see [Policy package installation targets on page 318](#).

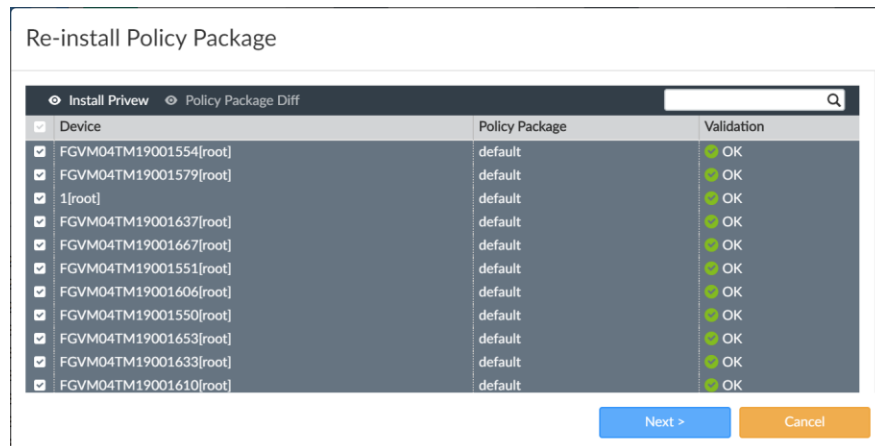
## Reinstall a policy package

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 320](#)).

a. Click the *Policy Check Result* button.

**Policy Consistency Check**

**Consistency Check**  
 FG60/FortiGate-VM64\_root (Created at Mon Mar 5 08:56:13 2018)  
 Policy Consistency Check (2 Occurrences)

Description  
 Policy consistency check based on these attributes: Interface (source/destination), Address (source/destination), Service, Schedule

#	Shadowing	Source	Destination	Service	Schedule	Action	Log	Comment
1	(2 policies may be shadowed by this policy)	any / all	port8 / all	ALL	always	deny	disable	

#	Shadowing	Source	Destination	Service	Schedule	Action	Log	Comment
4	(1 policies may be shadowed by this policy)	any / all	any / all	ALL	always	deny	disable	

**Policy optimization candidate(s)** (0 Occurrences)

**Duplicate Objects**  
 DLP FP-Sensitivity (1 Occurrences)  
 VPN SSL Web Host Check Software (5 Occurrences)  
 Device Category (1 Occurrences)  
 Address (2 Occurrences)  
 Service (1 Occurrences)

Description  
 Duplicate Service objects were detected in the database

#	Objects
1	FTP, FTP_GET, FTP_PUT

**Data Leak Prevention Sensor** (1 Occurrences)

Close

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.

**Reinstall Preview of Selected Devices**

1: config firewall policy  
 2: edit 2  
 3: set uuid 07b2b350-153c-51ea-e562-3ee33c2f1f92  
 4: set srcintf "any"  
 5: set dstintf "any"  
 6: set srcaddr "all"  
 7: set dstaddr "all"  
 8: set schedule "always"

Page 1 of 15

Download Previous Page Next Page Close

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.

Policy Package Diff (p1)

Summary

Policy - added (1) [\[Details\]](#)

Category	Change Summary	User	
IPv4 Policy	added (1)	admin	<a href="#">[Details]</a>

Policy Object - added (5) changed (3) deleted (106) [\[Details\]](#)

Category	Change Summary	User	
CA Certificate	added (1)	admin	
Local User	deleted (1)	admin	
User Group	deleted (1)	admin	
Device Group	deleted (3)	admin	
Local Category	deleted (2)	admin	
Web Filter Profile	changed (1) deleted (4)	admin	
Address	added (1) changed (1) deleted (1)	admin	
Multicast Address	deleted (5)	admin	
IPv6 Address	deleted (1)	admin	

Close

- 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:

<b>Installation Target</b>	The installation target and connection status.
<b>Config Status</b>	See the table below for config status details.
<b>Policy Package Status</b>	See the table below for policy package status details.

The following table identifies the different available config statuses.

Config Status	Icon	Description
<b>Synchronized</b>	Green check ✓	Configurations are synchronized between FortiManager and the managed device.
<b>Modified</b>	Yellow triangle ⚠	Configurations are modified on FortiManager and not synchronized between FortiManager and the managed device.
<b>Auto-update</b>	Green check ✓	Configurations modified on the managed device are auto synced to FortiManager.



Config Status	Icon	Description
<b>Modified (recent auto-updated)</b>	Yellow triangle ▲	Configurations are modified on FortiManager and configurations modified on the managed device are auto synced to FortiManager.
<b>Out of Sync</b>	Red X ❌	Configurations are modified on the managed device and not synced to FortiManager.
<b>Conflict</b>	Red X ❌	When one of the following happens: <ul style="list-style-type: none"> <li>• Install failed</li> <li>• Configurations are modified on both FortiManager and the managed device, and not auto synced to FortiManager.</li> </ul>
<b>Unknown</b>	Gray question mark ?	When one of the following happens: <ul style="list-style-type: none"> <li>• Connection goes down</li> <li>• No revision is generated, like added model device</li> </ul>

The following table identifies the different available policy package statuses.

Policy Package Status	Icon	Description
<b>Imported</b>	Green check ✓	Policies and objects are imported into FortiManager.
<b>Synchronized</b>	Green check ✓	Policies and objects are synchronized between FortiManager and the managed device.
<b>Modified</b>	Yellow triangle ▲	Policies or objects are modified on FortiManager.
<b>Out of Sync</b>	Red X ❌	Policies or objects are modified on the managed device.
<b>Unknown with policy package name</b>	Gray question mark ?	Configurations of the managed device are retrieved on FortiManager after being imported/installed.
<b>Never Installed</b>	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 fssso-polling* is *Modified*. This is because FortiManager sends all fssso-polling objects to all devices that are using agentless FSSO.

The following options are available:

<b>Add</b>	Select to add installation targets (device/group) for the policy package selected. Select the add icon beside <i>Device/Group</i> to select devices.
<b>Delete</b>	Select to delete the selected entries from the installation target for the policy package selected.
<b>Install</b>	Select an entry in the table and, from the <i>Install</i> menu, select <i>Install Wizard</i> or <i>Re-install Policy</i> .
<b>Search</b>	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.

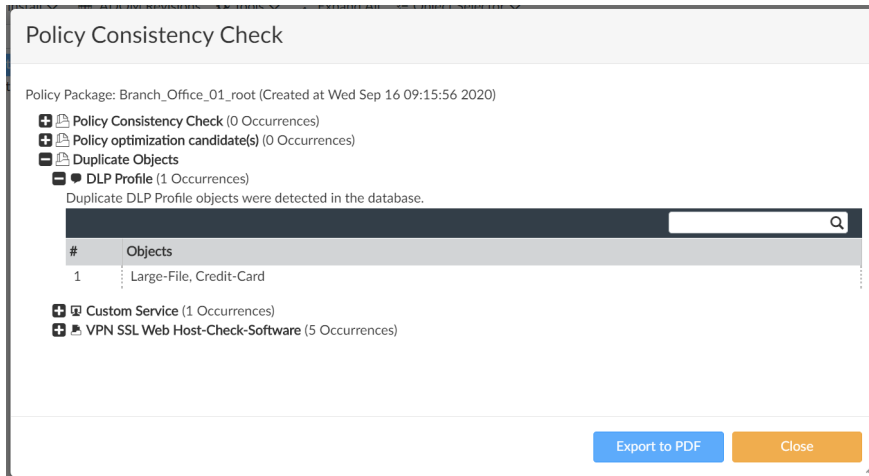


A policy consistency check can be automatically performed during every install. When doing the install, only modified or added policies are checked, decreasing the performance impact when compared to a full consistency check.

This function can be enabled when editing the ADOM (see [Editing an ADOM on page 763](#)).

### 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 *Export to PDF* to download the results.

#### 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 85](#).

#### 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, 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.

Find and Replace 'auth.gfx.ms'

There are 3 matches found. Please select one or multiple entries for replacements.

<input type="checkbox"/>	Policy Package	Referrer Type	Entry	Field
<input type="checkbox"/>	FortiGate-VM64_root_1	firewall policy	2	srcaddr
<input type="checkbox"/>		firewall ssl-ssh-profile=>ssl-exempt	26	address
<input type="checkbox"/>		firewall ssl-ssh-profile=>ssl-exempt	26	address

Replace with

0 records selected

Replace Close

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 309](#) for more information.

#	Name	From	To	Source	Destination	Schedule	Service	Users
1	matching	any	any	all	all	always	ALL	
2	FWPolicy	port10	any	all	all	always	ALL	
▼ Implicit (3-3 / Total: 1)								
3	Implicit Deny	any	any	all	all	always	ALL	

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
- 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 324](#).



If workspace or workflow is enabled, the ADOM must be locked before changes can be made. See [Locking an ADOM on page 770](#).



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.

## 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 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.

#	Name	From	To	Source	Destination	Schedule	Service	Action
1	PP1	any	any	all	all	always	ALL	Deny
2	PP2	any	any	all	all	always	ALL	Deny
Implicit (3/3 Total:1)								
3	Implicit Deny	any	any	all	all	always	ALL	Deny


## Strict search

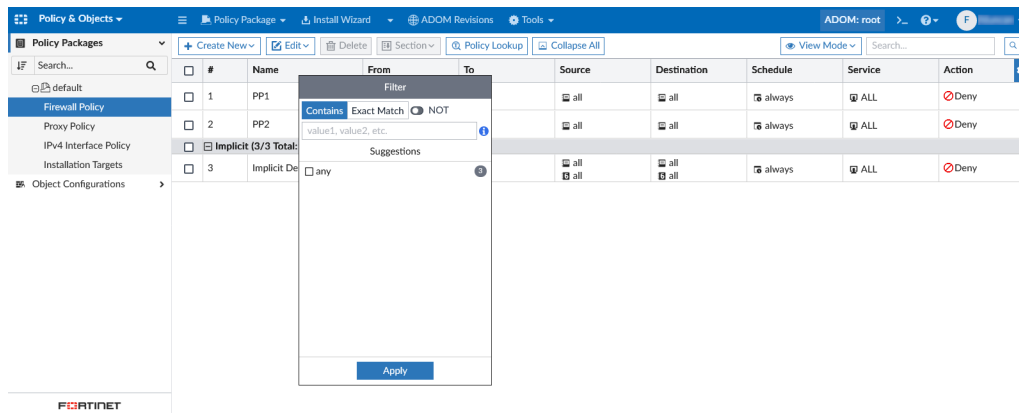
You can enable *Strict Search* to display only results that match the exact search entered, excluding "all". *Strict Search*


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.



- 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 " , ".
- 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

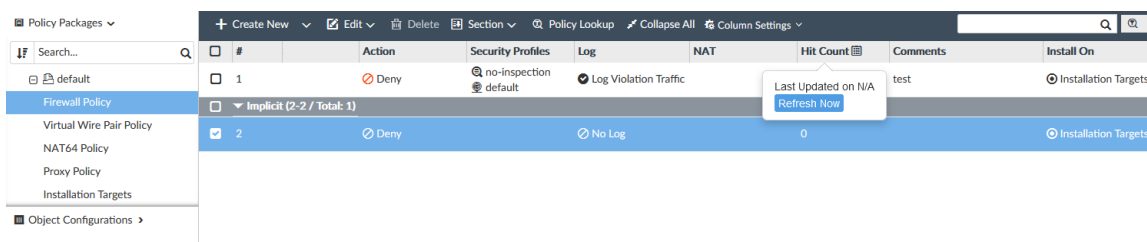
You can use FortiManager to view FortiGate policy hit counters. When you run a policy check on a policy package or select the *Find Unused Policies* option from the *Tools* dropdown for a policy package, FortiManager shows hit count information for unused policies with zero hit count.



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. When the policy hit counter is reset on the FortiGate, FortiManager subtracts the amount from its hit counters too.

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.

## Viewing unused policies

Use the Unused policies report to view and delete unused policies.

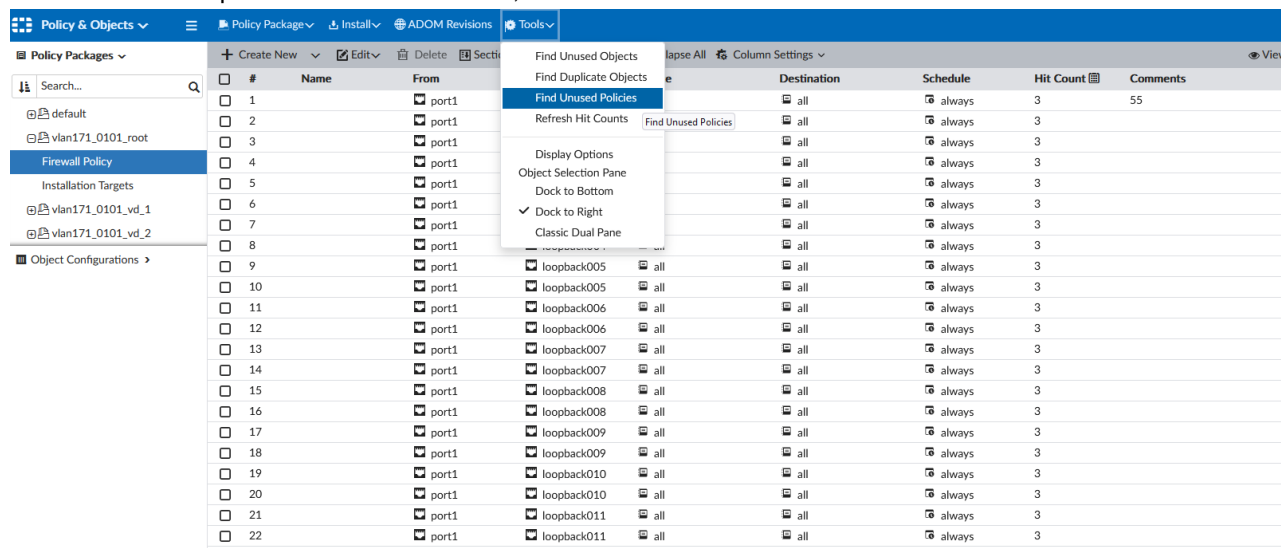
You may filter the unused policies report by date range to find policies that have not been used within a particular date range.

**To view the report:**

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.

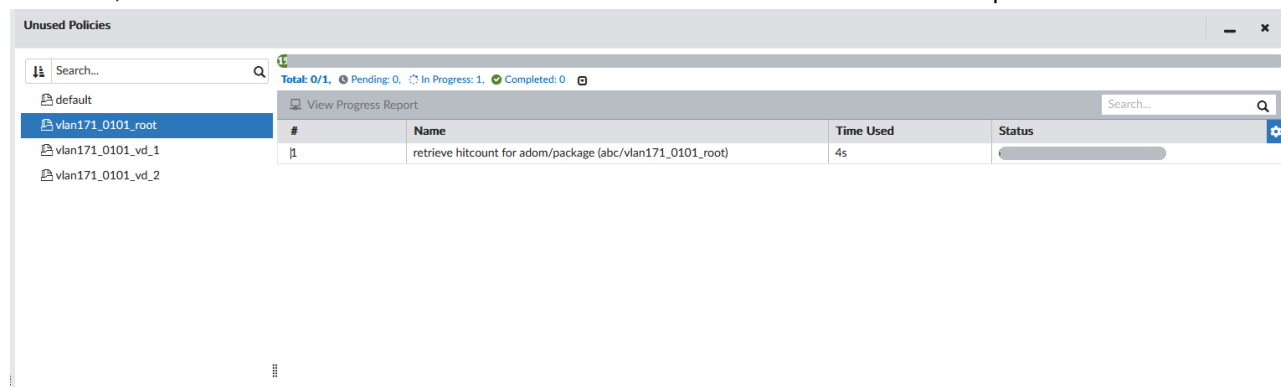


3. From the *Tools* dropdown menu in the toolbar, select *Find Unused Policies*.



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.

The screenshot shows the FortiManager interface. On the left, the 'Policy Packages' tree is visible. The main area shows 'Unused Policies'. A dropdown menu 'Show Unused Policy' is open, showing options for filtering by time range. The 'In Last 60 Days' option is selected. Below the dropdown, a table of unused policies is displayed. The table has columns: ID, Name, Source, Destination, Hit Count, First Used, Last Used, Active Sessions, First Session, and Last Session. The table shows several policies with hit counts and timestamps.

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.

Create New <input type="checkbox"/> Edit <input checked="" type="checkbox"/> Delete <input type="checkbox"/> Section <input type="checkbox"/> Policy Lookup <input checked="" type="checkbox"/> Column Settings <input type="checkbox"/>						
<input type="checkbox"/>	#	Name	From	To	Source	Destination
<input type="checkbox"/>	1	AllowAll	<input checked="" type="checkbox"/> any	<input checked="" type="checkbox"/> any	<input checked="" type="checkbox"/> swscan.appl	<input checked="" type="checkbox"/> all

5. Select or specify the values for the following fields and click *OK* to search for a policy.

<b>Device/VDOM</b>	Select the FortiGate device or the VDOM from the drop-down.
<b>Source Interface</b>	Select the source interface from the drop-down.
<b>Protocol</b>	Select the protocol from the drop-down.
<b>Protocol Number</b>	Specify a number between 1 to 255.
<b>Source</b>	Specify the source IP address.
<b>Destination</b>	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.

---

## 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.

---

## 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 [Object selector on page 331](#) and [Drag and drop objects on page 331](#).

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 from the *Edit* menu, select *Delete*.

**To add a section:**

You can use sections to help organize your policy list. Policies can also be appended to sections.

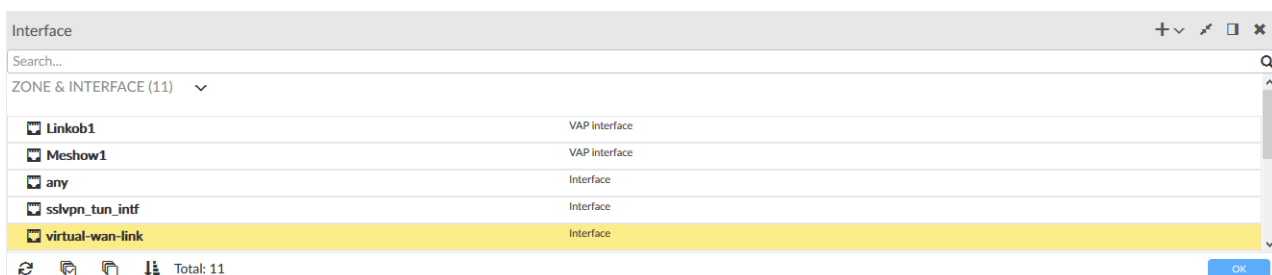
Select a policy, and from the *Section* menu, click *Add*. Type a section name, and click *OK* to add a section to the currently selected policy.

## 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 309](#).



<b>Create New</b>	Click the create new dropdown list, then select the object type to make a new object. See <a href="#">Create a new object on page 403</a> .
<b>Collapse / Expand All</b>	Expand or collapse all of the object groups shown in the pane.
<b>Dock to bottom / right</b>	Move the <i>Object Selector</i> frame to the bottom or right side of the content pane.
<b>Close</b>	Close the <i>Object Selector</i> frame.
<b>Search</b>	Enter a search term to search the object list.
<b>Refresh</b>	Refresh the list.
<b>Select All</b>	Select all objects in the list.
<b>Deselect All</b>	Deselect all objects in the list.
<b>Sort</b>	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 421](#) and [Clone an object on page 422](#).

## Drag and drop 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.

### Install policies only 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 318](#)), 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.

<b>Name</b>	Edit the service name as required.
<b>Comments</b>	Type an optional comment.
<b>Service Type</b>	Select <i>Firewall</i> or <i>Explicit Proxy</i> .
<b>Show in service list</b>	Select to display the object in the services list.
<b>Category</b>	Select a category for the service.
<b>Protocol Type</b>	Select the protocol from the dropdown list. Select one of the following: <i>TCP/UDP/SCTP</i> , <i>ICMP</i> , <i>ICMP6</i> , or <i>IP</i> .
<b>IP/FQDN</b>	Type the IP address or FQDN. This menu item is available when <i>Protocol</i> is set to <i>TCP/UDP/SCTP</i> . You can then define the protocol, source port, and destination port in the table.
<b>Type</b>	Type the service type in the text field. This menu item is available when <i>Protocol</i> is set to <i>ICMP</i> or <i>ICMP6</i> .
<b>Code</b>	Type the code in the text field. This menu item is available when <i>Protocol</i> is set to <i>ICMP</i> or <i>ICMP6</i> .

<b>Protocol Number</b>	Type the protocol number in the text field. This menu item is available when <i>Protocol Type</i> is set to <i>IP</i> .
<b>Advanced Options</b>	For more information on advanced option, see the <i>FortiOS CLI Reference</i> .
<b>check-reset-range</b>	<p>Configure ICMP error message verification.</p> <ul style="list-style-type: none"> <li><code>disable</code>: The FortiGate unit does not validate ICMP error messages.</li> <li><code>strict</code>: 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-&gt;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 <code>anti-replay</code> option checks packets.</li> <li><code>default</code>: Use the global setting defined in <code>system global</code>.</li> </ul> <p>This field is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i>. This field is not available if <i>explicit-proxy</i> is enabled.</p>
<b>Color</b>	Click the icon to select a custom, colored icon to display next to the service name.
<b>session-ttl</b>	<p>Type the default session timeout in seconds.</p> <p>The valid range is from 300 - 604 800 seconds. Type 0 to use either the <code>per-policy session-ttl</code> or <code>per-VDOM session-ttl</code>, as applicable.</p> <p>This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i>.</p>
<b>tcp-halfclose-timer</b>	<p>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 <code>system global</code>.</p> <p>This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i>.</p>
<b>tcp-halfopen-timer</b>	<p>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 <code>system global</code>.</p> <p>This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i>.</p>
<b>tcp-timewait-timer</b>	<p>Set the length of the TCP TIME-WAIT state in seconds. As described in <a href="#">RFC 793</a>, 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."</p> <p>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.</p> <p>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 <code>system global</code>.</p> <p>This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i>.</p>
<b>udp-idle-timer</b>	<p>Type the number of seconds before an idle UDP connection times out. The valid range is from 1 to 86400 seconds.</p>



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.

---

## 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
<b>ID</b>	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.
<b>Name</b>	Enter a unique name for the policy. Each policy must have a unique name.
<b>Incoming Interface</b>	Click the field then select interfaces. Click the remove icon to remove interfaces. New objects can be created by clicking the <i>Create New</i> icon in the <i>Object Selector</i> frame. See <a href="#">Create a new object on page 403</a> for more information.
<b>Outgoing Interface</b>	Select outgoing interfaces in the same manner as <i>Incoming Interface</i> .
<b>Source</b>	Select the source address, address groups, virtual IPs, virtual IP groups, user, user groups, and FSSO groups.
<b>IP/MAC Based Access Control</b>	Use ZTNA tags to allow access based on the IP/MAC address of a device.
<b>Destination</b>	Select the destination address, address groups, virtual IPs, virtual IP groups, and services.
<b>Service</b>	Select services and service groups. This option is only available when <i>Destination Internet Service</i> is off.
<b>Schedule</b>	Select a one-time schedule, recurring schedule, or schedule group.
<b>Action</b>	Select an action for the policy to take: <i>DENY</i> , <i>ACCEPT</i> , or <i>IPSEC</i> .
<b>Deny options</b>	
<b>Block Notification</b>	Turn block notification display on or off.
<b>Customize Messages</b>	Select or create a message to be displayed when traffic is blocked by this policy. This option is only available when <i>Block Notification</i> is on.

Deny options	
<b>Log Violation Traffic</b>	Turn violation logging on or off. Select whether to generate logs when the session starts.
Accept options	
<b>Inspection Mode</b>	Select <i>Flow-based</i> or <i>Proxy-based</i> inspection.
<b>Proxy HTTP(S) Traffic</b>	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 <i>Proxy-based</i> .
<b>NAT</b>	Select to enable NAT. If enabled, select <i>NAT</i> , <i>NAT46</i> , or <i>NAT64</i> .
<b>IP Pool Configuration</b>	If <i>NAT</i> is selected, select <i>Use Outgoing Interface Address</i> or <i>Use Dynamic IP Pool</i> .
<b>IPv4 Pool Name</b>	If <i>NAT64</i> is selected or <i>NAT</i> and <i>Use Dynamic IP Pool</i> are selected, select or create an IPv4 pool.
<b>IPv6 Pool Name</b>	If <i>NAT46</i> is selected or <i>NAT</i> and <i>Use Dynamic IP Pool</i> are selected, select or create an IPv6 pool.
<b>Preserve Source Port</b>	If <i>NAT</i> is on, select whether to preserve the source port.
<b>Protocol Options</b>	Select a protocol options profile.
<b>Display Disclaimer</b>	Turn the disclaimer display on or off.
<b>Customize Messages</b>	Select or create a disclaimer message to be displayed when traffic is allowed by this policy. This option is only available when <i>Display Disclaimer</i> is on.
<b>Security Profiles</b>	Select whether to apply security profiles to this policy, then select the security profiles.
<b>SSL/SSH Inspection</b>	Select one of the following options for SSL/SSH Inspection: <ul style="list-style-type: none"> <li>• certificate-inspection</li> <li>• custom-deep-inspection</li> <li>• deep-inspection</li> <li>• no-inspection</li> </ul>
<b>Shared Shaper</b>	Select shared traffic shapers.
<b>Reverse Shaper</b>	Select reverse traffic shapers.
<b>Per-IP Shaper</b>	Select per IP traffic shapers.
<b>Log Allowed Traffic</b>	Select one of the following options: <ul style="list-style-type: none"> <li>• <i>No Log</i></li> <li>• <i>Log Security Events</i></li> <li>• <i>Log All Sessions</i></li> </ul> If logging is on, select whether to capture packets. Select whether to generate logs when the session starts.

IPSEC options	
<b>Protocol Options</b>	Select a protocol options profile.
<b>VPN Tunnel</b>	Select or create a VPN tunnel dynamic object. Select whether to allow traffic to be initiated from the remote site.
<b>Security Profiles</b>	Select whether to apply security profiles to this policy, then select the security profiles.
<b>SSL/SSH Inspection</b>	Select one of the following options for SSL/SSH Inspection: <ul style="list-style-type: none"> <li>• certificate-inspection</li> <li>• custom-deep-inspection</li> <li>• deep-inspection</li> <li>• no-inspection</li> </ul>
<b>Shared Shaper</b>	Select shared traffic shapers.
<b>Reverse Shaper</b>	Select reverse traffic shapers.
<b>Per-IP Shaper</b>	Select per IP traffic shapers.
<b>Log Allowed Traffic</b>	Select one of the following options: <ul style="list-style-type: none"> <li>• <i>No Log</i></li> <li>• <i>Log Security Events</i></li> <li>• <i>Log All Sessions</i></li> </ul> If logging is on, select whether to capture packets. Select whether to generate logs when the session starts.
Advanced	
<b>WCCP</b>	Turn Web Cache Communication Protocol (WCCP) web caching on or off.
<b>Exempt from Captive Portal</b>	Select whether this traffic is exempt from any captive portals.
<b>Comments</b>	Add a description of the policy, such as its purpose, or the changes that have been made to it.
<b>Advanced Options</b>	Configure advanced options, see <a href="#">Advanced options</a> below. For more information on advanced option, see the <a href="#">FortiOS CLI Reference</a> .
Revisions	
<b>Change Note</b>	Add a description of the changes being made to the policy. This field is required.

- 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
<b>anti-replay</b>	Enable or disable anti-replay checking.	enable
<b>auth-cert</b>	Select the HTTPS server certificate for policy authentication.	none
<b>auth-path</b>	Enable or disable authentication-based routing.	disable
<b>auth-redirect-addr</b>	Select the HTTP-to-HTTPS redirect address for firewall authentication.	none
<b>auto-asic-offload</b>	Enable or disable policy traffic ASIC offloading.	enable
<b>block-notification</b>	Enable or disable block notification.	disable
<b>cgn-eif</b>	Enable or disable CGN endpoint independent filtering.	disable
<b>cgn-eim</b>	Enable or disable CGN endpoint independent mapping.	disable
<b>cgn-log-server-grp</b>	Select the NP log server group.	none
<b>cgn-resource-quota</b>	Set the allowed number of blocks assigned to a source IP address.	16
<b>cgn-session-quota</b>	Set the allowed concurrent sessions available for a source IP address.	16777215
<b>custom-log-fields</b>	Select custom fields to append to log messages for this policy.	none
<b>delay-tcp-npu-session</b>	Enable or disable TCP NPU session delay to guarantee packet order of 3-way handshake.	disable
<b>diffserv-copy</b>	Enable or disable copying of the DSCP values from the original direction to the reply direction.	disable
<b>diffserv-forward</b>	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic. If enabled, also configure <code>diffservcode-forward</code> .	disable
<b>diffserv-reverse</b>	Enable or disable application of the DSCP value to the DSCP field of reverse (reply) traffic. If enabled, also configure <code>diffservcode-rev</code> .	disable
<b>diffservcode-forward</b>	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
<b>diffservcode-rev</b>	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
<b>dlp-profile</b>	Select an existing data leak prevention (DLP) profile.	none
<b>dsri</b>	Enable to ignore HTTP server responses.	disable
<b>dstaddr-negate</b>	Enable to negate the destination IP address.	disable
<b>dstaddr6-negate</b>	Enable to negate the destination IPv6 address.	disable

Option	Description	Default
<b>dynamic-shaping</b>	Enable or disable dynamic RADIUS-defined traffic shaping.	disable
<b>email-collect</b>	Enable or disable email collection.	disable
<b>fec</b>	Enable or disable forward error correction (FEC) on traffic matching this policy on a FEC device.	disable
<b>firewall-session-dirty</b>	Select how to handle sessions if the configuration of this firewall policy changes.	check-all
<b>ffsso-agent-for-ntlm</b>	Select the FSSO agent for NTLM authentication.	none
<b>geoip-anycast</b>	Enable or disable recognition of anycast IP addresses using the geography IP database.	disable
<b>geoip-match</b>	Select whether to match the address based on the physical or registered location.	physical-location
<b>identity-based-route</b>	Select the identity-based routing rule.	none
<b>internet-service-negate</b>	Enable to negate the internet service set in the policy.	disable
<b>internet-service-src-negate</b>	Enable to negate the source internet service set in this policy.	disable
<b>internet-service6</b>	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
<b>internet-service6-custom</b>	Select a custom IPv6 internet service.	none
<b>internet-service6-custom-group</b>	Select a custom IPv6 internet service group.	none
<b>internet-service6-group</b>	Select an IPv6 internet service group.	none
<b>internet-service6-name</b>	Select an IPv6 internet service.	none
<b>internet-service6-negate</b>	Enable to negate the source IPv6 internet service set in this policy.	disable
<b>internet-service6-src</b>	Enable or disable use of the IPv6 internet services in the source for this policy. If enabled, the source address is not used.	disable
<b>internet-service6-src-custom</b>	Select the custom IPv6 internet service source.	none
<b>internet-service6-src-custom-group</b>	Select the custom IPv6 source group.	none
<b>internet-service6-src-group</b>	Select the IPv6 source group.	none
<b>internet-service6-src-name</b>	Select the IPv6 source.	none

Option	Description	Default
<b>internet-service6-src-negate</b>	Enable to negate the value set in <code>internet-service6-src</code> .	disable
<b>match-vip</b>	Enable or disable matching of packets that have had their destination address changed by a VIP.	disable
<b>match-vip-only</b>	Enable or disable matching only those packets that have had their destination addresses change by a VIP.	disable
<b>natinbound</b>	Enable or disable applying destination NAT to inbound traffic.	disable
<b>natip</b>	Set the source NAT IP address for inbound traffic.	0.0.0.0/0.0.0.0
<b>natoutbound</b>	Enable or disable applying destination NAT to outbound traffic.	disable
<b>network-service-dynamic</b>	Select a dynamic network service.	none
<b>network-service-src-dynamic</b>	Select a dynamic network service source.	none
<b>np-acceleration</b>	Enable or disable UTM network processor acceleration.	disable
<b>ntlm</b>	Enable or disable NTLM authentication.	disable
<b>ntlm-enabled-browsers</b>	Set the HTTP-User-Agent value of supported browsers.	none
<b>ntlm-guest</b>	Enable or disable NTLM guest user access.	disable
<b>outbound</b>	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic.	disable
<b>passive-wan-health-measurement</b>	Enable or disable passive WAN health measurement. When enabled, <code>auto-asic-offload</code> is disabled.	disable.
<b>permit-any-host</b>	Enable or disable accepting UDP packets from any host.	disable
<b>permit-stun-host</b>	Enable or disable accepting UDP packets from any session traversal utilities for NAT (STUN) host.	disable
<b>policy-expiry</b>	Enable or disable policy expiry.	disable
<b>policy-expiry-date</b>	If policy-expiry is enabled, set the policy expiry date.	0000-00-00,00:00:00
<b>policy-offload</b>	Enable or disable hardware session setup for CGNAT.	disable
<b>radius-mac-auth-bypass</b>	Enable or disable MAC authentication bypass. The bypassed MAC address must be received from the RADIUS server.	disable
<b>redirect-url</b>	Set the URL to which users are redirected after seeing and accepting the disclaimer or authenticating.	none
<b>reputation-direction</b>	Set the destination of the initial traffic for reputation to take effect.	destination
<b>reputation-direction6</b>	Set the destination of the initial traffic for IPv6 reputation to take effect.	destination

Option	Description	Default
<b>reputation-minimum</b>	Set the minimum reputation to take action.	0
<b>reputation-minimum6</b>	Set the minimum IPv6 reputation to take action.	0
<b>rtp-addr</b>	If this is an RTP NAT policy, set the address names.	none
<b>rtp-nat</b>	Enable or disable real time protocol (RTP) NAT.	disable
<b>schedule-timeout</b>	Enable or disable ending current sessions when the schedule object times out. Disable allows sessions to end from inactivity.	disable
<b>sctp-filter-profile</b>	Select an existing SCTP filter profile.	none
<b>send-deny-packet</b>	Enable or disable sending a reply when a session is denied or blocked by a firewall policy.	disable
<b>service-negate</b>	Enable or disable negation of the service set in the policy.	disable
<b>session-ttl</b>	Enter a value for the session time-to-live (TTL) from 300 to 604800, or type 0 for no limitation.	0
<b>sgt</b>	Enter security group tags (SGT).	none
<b>sgt-check</b>	Enable or disable SGT check.	disable
<b>src-vendor-mac</b>	Select the vendor MAC source.	none
<b>srcaddr-negate</b>	Enable or disable negation of the source address.	disable
<b>srcaddr6-negate</b>	Enable or disable negation of the source IPv6 address.	disable
<b>ssh-filter-profile</b>	Select an SSH filter profile from the drop-down list.	None
<b>ssh-policy-redirect</b>	Enable or disable SSH policy redirect.	disable
<b>tcp-mss-receiver</b>	Enter the receiver's TCP maximum segment size (MSS).	0
<b>tcp-mss-sender</b>	Enter the sender's TCP MSS.	0
<b>tcp-session-without-syn</b>	Enable or disable creation of a TCP session without the SYN flag.	disable
<b>tcp-timeout-pid</b>	Select the TCP timeout profile.	none
<b>timeout-send-rst</b>	Enable or disable the sending of RST packets when TCP sessions expire	disable
<b>tos</b>	Enter the type of service (TOS) value used for comparison.	0
<b>tos-mask</b>	Enter the bit mask for TOS. Non-zero bit positions are used for comparison while zero bit positions are ignored.	0
<b>tos-negate</b>	Enable or disable to negate the TOS match.	disable
<b>udp-timeout-pid</b>	Select the UDP timeout profile.	none
<b>uuid</b>	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000



Option	Description	Default
<b>vlan-cos-fwd</b>	Select the VLAN forward direction user priority. The available values are: <ul style="list-style-type: none"> <li>• 255 (passthrough)</li> <li>• 0 (lowest) - 7 (highest)</li> </ul>	255
<b>vlan-cos-rev</b>	Select the VLAN reverse direction user priority. The available values are: <ul style="list-style-type: none"> <li>• 255 (passthrough)</li> <li>• 0 (lowest) - 7 (highest)</li> </ul>	255
<b>vlan-filter</b>	Set VLAN filters.	none
<b>wanopt</b>	Enable or disable WAN optimization (IPv4 only).	disable
<b>wanopt-detection</b>	Select the WAN optimization as active, passive, or off.	active
<b>wanopt-passive-opt</b>	Select WAN optimization passive mode options. This option decides what IP address will be used to connect server (IPv4 only).	default
<b>wanopt-peer</b>	Select a WAN optimization peer (IPv4 only).	none
<b>wanopt-profile</b>	Select a WAN optimization profile (IPv4 only).	none
<b>webcache</b>	Enable or disable web cache (IPv4 only).	disable
<b>webcache-https</b>	Enable or disable the web cache for HTTPS (IPv4 only).	none
<b>webproxy-forward-server</b>	Select the webproxy forward server (IPv4 only).	none
<b>webproxy-profile</b>	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
<b>ID</b>	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.
<b>Name</b>	Enter a unique name for the policy. Each policy must have a unique name.
<b>Incoming Interface</b>	Click the field then select interfaces. Click the remove icon to remove interfaces. New objects can be created by clicking the <i>Create New</i> icon in the <i>Object Selector</i> frame. See <a href="#">Create a new object on page 403</a> for more information.
<b>Outgoing Interface</b>	Select outgoing interfaces in the same manner as <i>Incoming Interface</i> .
<b>Source</b>	Select the source address, address groups, virtual IPs, virtual IP groups, user, user groups, and FSSO groups.
<b>Enforce ZTNA</b>	Enable or disable ZTNA.
<b>EMS Tag</b>	Select the FortiClient EMS tag to match. This option is only available if Enforce ZTNA is enabled.
<b>Geographic IP Tag</b>	Select the Geographic IP tag to match. This option is only available if Enforce ZTNA is enabled.
<b>Destination</b>	Select the destination address, address groups, virtual IPs, virtual IP groups, and services.
<b>Service</b>	Select services and service groups. This option is only available when <i>Destination Internet Service</i> is off.
<b>SSL/SSH Inspection</b>	Select one of the following options for SSL/SSH Inspection: certificate-inspection custom-deep-inspection deep-inspection no-inspection
<b>Comments</b>	Add a description of the policy, such as its purpose, or the changes that have been made to it.
<b>Advanced Options</b>	Configure advanced options, see <a href="#">Advanced options</a> below. For more information on advanced option, see the <a href="#">FortiOS CLI Reference</a> .
<b>Change Note</b>	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
<b>anti-replay</b>	Enable or disable anti-replay checking.	enable

Option	Description	Default
<b>auth-cert</b>	Select the HTTPS server certificate for policy authentication.	none
<b>auth-path</b>	Enable or disable authentication-based routing.	disable
<b>auth-redirect-addr</b>	Select the HTTP-to-HTTPS redirect address for firewall authentication.	none
<b>auto-asic-offload</b>	Enable or disable policy traffic ASIC offloading.	enable
<b>block-notification</b>	Enable or disable block notification.	disable
<b>cgn-eif</b>	Enable or disable CGN endpoint independent filtering.	disable
<b>cgn-eim</b>	Enable or disable CGN endpoint independent mapping.	disable
<b>cgn-log-server-grp</b>	Select the NP log server group.	none
<b>cgn-resource-quota</b>	Set the allowed number of blocks assigned to a source IP address.	16
<b>cgn-session-quota</b>	Set the allowed concurrent sessions available for a source IP address.	16777215
<b>custom-log-fields</b>	Select custom fields to append to log messages for this policy.	none
<b>delay-tcp-npu-session</b>	Enable or disable TCP NPU session delay to guarantee packet order of 3-way handshake.	disable
<b>diffserv-copy</b>	Enable or disable copying of the DSCP values from the original direction to the reply direction.	disable
<b>diffserv-forward</b>	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic. If enabled, also configure <code>diffservcode-forward</code> .	disable
<b>diffserv-reverse</b>	Enable or disable application of the DSCP value to the DSCP field of reverse (reply) traffic. If enabled, also configure <code>diffservcode-rev</code> .	disable
<b>diffservcode-forward</b>	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
<b>diffservcode-rev</b>	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
<b>dlp-profile</b>	Select an existing data leak prevention (DLP) profile.	none
<b>dsri</b>	Enable to ignore HTTP server responses.	disable
<b>dstaddr-negate</b>	Enable to negate the destination IP address.	disable
<b>dstaddr6-negate</b>	Enable to negate the destination IPv6 address.	disable
<b>dynamic-shaping</b>	Enable or disable dynamic RADIUS-defined traffic shaping.	disable
<b>email-collect</b>	Enable or disable email collection.	disable

Option	Description	Default
<b>fec</b>	Enable or disable forward error correction (FEC) on traffic matching this policy on a FEC device.	disable
<b>firewall-session-dirty</b>	Select how to handle sessions if the configuration of this firewall policy changes.	check-all
<b>ffsso-agent-for-ntlm</b>	Select the FSSO agent for NTLM authentication.	none
<b>geoip-anycast</b>	Enable or disable recognition of anycast IP addresses using the geography IP database.	disable
<b>geoip-match</b>	Select whether to match the address based on the physical or registered location.	physical-location
<b>identity-based-route</b>	Select the identity-based routing rule.	none
<b>internet-service-negate</b>	Enable to negate the internet service set in the policy.	disable
<b>internet-service-src-negate</b>	Enable to negate the source internet service set in this policy.	disable
<b>internet-service6</b>	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
<b>internet-service6-custom</b>	Select a custom IPv6 internet service.	none
<b>internet-service6-custom-group</b>	Select a custom IPv6 internet service group.	none
<b>internet-service6-group</b>	Select an IPv6 internet service group.	none
<b>internet-service6-name</b>	Select an IPv6 internet service.	none
<b>internet-service6-negate</b>	Enable to negate the source IPv6 internet service set in this policy.	disable
<b>internet-service6-src</b>	Enable or disable use of the IPv6 internet services in the source for this policy. If enabled, the source address is not used.	disable
<b>internet-service6-src-custom</b>	Select the custom IPv6 internet service source.	none
<b>internet-service6-src-custom-group</b>	Select the custom IPv6 source group.	none
<b>internet-service6-src-group</b>	Select the IPv6 source group.	none
<b>internet-service6-src-name</b>	Select the IPv6 source.	none
<b>internet-service6-src-negate</b>	Enable to negate the value set in <code>internet-service6-src</code> .	disable

Option	Description	Default
<b>match-vip</b>	Enable or disable matching of packets that have had their destination address changed by a VIP.	disable
<b>match-vip-only</b>	Enable or disable matching only those packets that have had their destination addresses change by a VIP.	disable
<b>natinbound</b>	Enable or disable applying destination NAT to inbound traffic.	disable
<b>natip</b>	Set the source NAT IP address for inbound traffic.	0.0.0.0/0.0.0.0
<b>natoutbound</b>	Enable or disable applying destination NAT to outbound traffic.	disable
<b>network-service-dynamic</b>	Select a dynamic network service.	none
<b>network-service-src-dynamic</b>	Select a dynamic network service source.	none
<b>np-acceleration</b>	Enable or disable UTM network processor acceleration.	disable
<b>ntlm</b>	Enable or disable NTLM authentication.	disable
<b>ntlm-enabled-browsers</b>	Set the HTTP-User-Agent value of supported browsers.	none
<b>ntlm-guest</b>	Enable or disable NTLM guest user access.	disable
<b>outbound</b>	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic.	disable
<b>passive-wan-health-measurement</b>	Enable or disable passive WAN health measurement. When enabled, <code>auto-asic-offload</code> is disabled.	disable.
<b>permit-any-host</b>	Enable or disable accepting UDP packets from any host.	disable
<b>permit-stun-host</b>	Enable or disable accepting UDP packets from any session traversal utilities for NAT (STUN) host.	disable
<b>policy-expiry</b>	Enable or disable policy expiry.	disable
<b>policy-expiry-date</b>	If policy-expiry is enabled, set the policy expiry date.	0000-00-00,00:00:00
<b>policy-offload</b>	Enable or disable hardware session setup for CGNAT.	disable
<b>radius-mac-auth-bypass</b>	Enable or disable MAC authentication bypass. The bypassed MAC address must be received from the RADIUS server.	disable
<b>redirect-url</b>	Set the URL to which users are redirected after seeing and accepting the disclaimer or authenticating.	none
<b>reputation-direction</b>	Set the destination of the initial traffic for reputation to take effect.	destination
<b>reputation-direction6</b>	Set the destination of the initial traffic for IPv6 reputation to take effect.	destination
<b>reputation-minimum</b>	Set the minimum reputation to take action.	0

Option	Description	Default
<b>reputation-minimum6</b>	Set the minimum IPv6 reputation to take action.	0
<b>rtp-addr</b>	If this is an RTP NAT policy, set the address names.	none
<b>rtp-nat</b>	Enable or disable real time protocol (RTP) NAT.	disable
<b>schedule-timeout</b>	Enable or disable ending current sessions when the schedule object times out. Disable allows sessions to end from inactivity.	disable
<b>sctp-filter-profile</b>	Select an existing SCTP filter profile.	none
<b>send-deny-packet</b>	Enable or disable sending a reply when a session is denied or blocked by a firewall policy.	disable
<b>service-negate</b>	Enable or disable negation of the service set in the policy.	disable
<b>session-ttl</b>	Enter a value for the session time-to-live (TTL) from 300 to 604800, or type 0 for no limitation.	0
<b>sgt</b>	Enter security group tags (SGT).	none
<b>sgt-check</b>	Enable or disable SGT check.	disable
<b>src-vendor-mac</b>	Select the vendor MAC source.	none
<b>srcaddr-negate</b>	Enable or disable negation of the source address.	disable
<b>srcaddr6-negate</b>	Enable or disable negation of the source IPv6 address.	disable
<b>ssh-filter-profile</b>	Select an SSH filter profile from the drop-down list.	None
<b>ssh-policy-redirect</b>	Enable or disable SSH policy redirect.	disable
<b>tcp-mss-receiver</b>	Enter the receiver's TCP maximum segment size (MSS).	0
<b>tcp-mss-sender</b>	Enter the sender's TCP MSS.	0
<b>tcp-session-without-syn</b>	Enable or disable creation of a TCP session without the SYN flag.	disable
<b>tcp-timeout-pid</b>	Select the TCP timeout profile.	none
<b>timeout-send-rst</b>	Enable or disable the sending of RST packets when TCP sessions expire	disable
<b>tos</b>	Enter the type of service (TOS) value used for comparison.	0
<b>tos-mask</b>	Enter the bit mask for TOS. Non-zero bit positions are used for comparison while zero bit positions are ignored.	0
<b>tos-negate</b>	Enable or disable to negate the TOS match.	disable
<b>udp-timeout-pid</b>	Select the UDP timeout profile.	none
<b>uuid</b>	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000

Option	Description	Default
<b>vlan-cos-fwd</b>	Select the VLAN forward direction user priority. The available values are: <ul style="list-style-type: none"> <li>• 255 (passthrough)</li> <li>• 0 (lowest) - 7 (highest)</li> </ul>	255
<b>vlan-cos-rev</b>	Select the VLAN reverse direction user priority. The available values are: <ul style="list-style-type: none"> <li>• 255 (passthrough)</li> <li>• 0 (lowest) - 7 (highest)</li> </ul>	255
<b>vlan-filter</b>	Set VLAN filters.	none
<b>wanopt</b>	Enable or disable WAN optimization (IPv4 only).	disable
<b>wanopt-detection</b>	Select the WAN optimization as active, passive, or off.	active
<b>wanopt-passive-opt</b>	Select WAN optimization passive mode options. This option decides what IP address will be used to connect server (IPv4 only).	default
<b>wanopt-peer</b>	Select a WAN optimization peer (IPv4 only).	none
<b>wanopt-profile</b>	Select a WAN optimization profile (IPv4 only).	none
<b>webcache</b>	Enable or disable web cache (IPv4 only).	disable
<b>webcache-https</b>	Enable or disable the web cache for HTTPS (IPv4 only).	none
<b>webproxy-forward-server</b>	Select the webproxy forward server (IPv4 only).	none
<b>webproxy-profile</b>	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:

<b>ID</b>	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.
<b>Name</b>	Enter a unique name for the policy. Each policy must have a unique name.
<b>Policy Mode</b>	Select the mode for this policy: <i>Standard</i> or <i>Learn Mode</i> . 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 <a href="#">Learn mode in security policies in NGFW mode in the FortiOS Administration Guide</a> for more information.
<b>Incoming Interface</b>	Click the field then select interfaces. Click the remove icon to remove interfaces. New interfaces can be created by clicking the <i>Create New</i> icon in the <i>Interfaces</i> frame. See <a href="#">Create a new object on page 403</a> for more information.
<b>Outgoing Interface</b>	Select outgoing interfaces in the same manner as the incoming interfaces.
<b>Source</b>	Select the source address, address groups, virtual IPs, virtual IP groups, user, user groups, and FSSO groups.
<b>Destination</b>	Select the destination address, address groups, virtual IPs, virtual IP groups, and services.
<b>Schedule</b>	Select a one-time schedule, recurring schedule, or schedule group.
<b>Service</b>	Select the service. Select <i>App Default</i> or <i>Specify</i> . If <i>Specify</i> is selected, select the Service.
<b>Application</b>	Select applications.
<b>URL Category</b>	Select URL categories.
<b>Action</b>	Select an action for the policy to take: <i>DENY</i> or <i>ACCEPT</i> .
<b>Log Traffic</b>	When the <i>Action</i> is <i>DENY</i> , select <i>Log Violation Traffic</i> to log violation traffic. When the <i>Action</i> is <i>ACCEPT</i> , select one of the following options: <ul style="list-style-type: none"> <li>• <i>No Log</i></li> <li>• <i>Log Security Events</i></li> <li>• <i>Log All Sessions</i></li> </ul> Select whether to generate logs when the session starts.
<b>Protocol Options</b>	Select protocol options profiles for handling protocol-specific traffic. This option is available when the <i>Action</i> is <i>ACCEPT</i> .



<b>Security Profiles</b>	<p>Select to add security profiles or profile groups.</p> <p>This option is available when the <i>Action</i> is <i>ACCEPT</i>.</p> <p>If <i>Use Standard Security Profiles</i> is selected, the following standard security profile types can be added:</p> <ul style="list-style-type: none"> <li>• AntiVirus Profile</li> <li>• Web Filter Profile</li> <li>• IPS Profile</li> <li>• Email Filter</li> <li>• File Filter Profile</li> </ul> <p>If <i>Use Security Profile Group</i> is selected, select the <i>Profile Group</i>.</p>
<b>Comments</b>	Add a description of the policy, such as its purpose, or the changes that have been made to it.
<b>Advanced Options</b>	<p>Configure advanced options, see <a href="#">Advanced options</a> below.</p> <p>For more information on advanced option, see the <a href="#">FortiOS CLI Reference</a>.</p>
<b>Change Note</b>	Add a description of the changes being made to the policy. This field is required.

- 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
<b>application-list</b>	Select ...an existing application list.	none
<b>comments</b>	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 <i>Comments</i> field.	none
<b>dlp-profile</b>	Select an existing data leak prevention (DLP) profile.	none
<b>dnsfilter-profile</b>	Select an existing DNS filter profile.	none
<b>dstaddr-negate</b>	Enable to negate the values set in <i>IPv4 Destination Address</i> and <i>IPv6 Destination Address</i> .	disable
<b>global-label</b>	Set the label for the policy to be displayed when the GUI is in <i>Global View</i> mode.	none
<b>icap-profile</b>	Select an existing Internet Content Adaptation Protocol (ICAP) profile.	none
<b>internet-service-negate</b>	When enabled, Internet services match against any Internet service except the selected Internet service.	disable
<b>internet-service-src-negate</b>	Enables or disables the use of Internet Services in source for this policy. If enabled, <i>internet-service-src</i> specifies what the service must NOT be.	disable

Option	Description	Default
<b>internet-service6</b>	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
<b>internet-service6-custom</b>	Select a custom IPv6 internet service.	none
<b>internet-service6-custom-group</b>	Select a custom IPv6 internet service group.	none
<b>internet-service6-group</b>	Select an IPv6 internet service group.	none
<b>internet-service6-name</b>	Select an IPv6 internet service.	none
<b>internet-service6-negate</b>	Enable to negate the source IPv6 internet service set in this policy.	disable
<b>internet-service6-src</b>	Enable or disable use of the IPv6 internet services in the source for this policy. If enabled, the source address is not used.	disable
<b>internet-service6-src-custom</b>	Select the custom IPv6 internet service source.	none
<b>internet-service6-src-custom-group</b>	Select the custom IPv6 source group.	none
<b>internet-service6-src-group</b>	Select the IPv6 source group.	none
<b>internet-service6-src-name</b>	Select the IPv6 source.	none
<b>internet-service6-src-negate</b>	Enable to negate the value set in <code>internet-service6-src</code> .	disable
<b>nat46</b>	Enable or disable NAT46.	disable
<b>nat64</b>	Enable or disable NAT64.	disable
<b>sctp-filter-profile</b>	Select an existing stream control transmission protocol (SCTP) filter profile.	none
<b>send-deny-packet</b>	Enable or disable sending a reply packet when a session is denied or blocked by this policy.	disable
<b>service-negate</b>	Enable or disable negation of the selected <i>Service</i> .	disable
<b>srcaddr-negate</b>	Enable or disable negation of the <i>IPv4 Source Address</i> or <i>IPv6 Source Address</i> address.	disable
<b>ssh-filter-profile</b>	Select an existing SSH filter profile.	none
<b>ssl-ssh-profile</b>	Select an existing SSL SSH profile.	no-inspection
<b>utm-status</b>	Enable or disable the Unified Threat Management status.	disable

Option	Description	Default
<b>uuid</b>	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000
<b>voip-profile</b>	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 590](#).

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 366](#).

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
<b>ID</b>	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.
<b>Name</b>	Enter a unique name for the policy. Each policy must have a unique name.
<b>IP/MAC Based Access Control</b>	Use ZTNA tags to allow access based on the IP/MAC address of a device.
<b>Virtual Wire Pair Interface</b>	Select one or more virtual wire pair interfaces. This field is required.

Option	Description
	New objects can be created by clicking the <i>Create New</i> icon in the <i>Object Selector</i> frame. See <a href="#">Create a new object on page 403</a> for more information.
<b>Virtual Wire Pair</b>	Select an arrow to indicate the flow of traffic between the ports in the selected <i>Virtual Wire Pair Interface</i> .
<b>Source</b>	Select the source address, address groups, virtual IPs, virtual IP groups, user, user groups, and FSSO groups.
<b>Destination</b>	Select the destination address, address groups, virtual IPs, virtual IP groups, and services.
<b>Service</b>	Select services and service groups. This option is only available when <i>Destination Internet Service</i> is off.
<b>Schedule</b>	Select a one-time schedule, recurring schedule, or schedule group.
<b>Action</b>	Select an action for the policy to take: <i>DENY</i> or <i>ACCEPT</i> .
<b>Deny options</b>	
<b>Block Notification</b>	Turn block notification display on or off.
<b>Log Violation Traffic</b>	Turn violation logging on or off. Select whether to generate logs when the session starts.
<b>Accept options</b>	
<b>NAT</b>	Select to enable NAT. If enabled, select <i>NAT</i> , <i>NAT46</i> , or <i>NAT64</i> .
<b>IP Pool Configuration</b>	If <i>NAT</i> is selected, select <i>Use Outgoing Interface Address</i> or <i>Use Dynamic IP Pool</i> . <i>Use Outgoing Interface Address</i> is disabled in a firewall virtual pair policy.
<b>IPv4 Pool Name</b>	If <i>NAT64</i> is selected or <i>NAT</i> and <i>Use Dynamic IP Pool</i> are selected, select or create an IPv4 pool.
<b>IPv6 Pool Name</b>	If <i>NAT46</i> is selected or <i>NAT</i> and <i>Use Dynamic IP Pool</i> are selected, select or create an IPv6 pool.
<b>Preserve Source Port</b>	If <i>NAT</i> is on, select whether to preserve the source port.
<b>Protocol Options</b>	Select a protocol options profile.
<b>Display Disclaimer</b>	Turn the disclaimer display on or off.
<b>SSL/SSH Inspection</b>	Select one of the following options for SSL/SSH Inspection: certificate-inspection custom-deep-inspection deep-inspection no-inspection
<b>Shared Shaper</b>	Select shared traffic shapers.
<b>Reverse Shaper</b>	Select reverse traffic shapers.

Accept options	
<b>Per-IP Shaper</b>	Select per IP traffic shapers.
<b>Log Allowed Traffic</b>	Select one of the following options: <i>No Log</i> <i>Log Security Events</i> <i>Log All Sessions</i> If logging is on, select whether to capture packets.Select whether to generate logs when the session starts.
Advanced	
<b>WCCP</b>	Turn Web Cache Communication Protocol (WCCP) web caching on or off.
<b>Exempt from Captive Portal</b>	Select whether this traffic is exempt from any captive portals.
<b>Comments</b>	Add a description of the policy, such as its purpose, or the changes that have been made to it.
<b>Advanced Options</b>	Configure advanced options, see <a href="#">Advanced options</a> below. For more information on advanced option, see the <a href="#">FortiOS CLI Reference</a> .
Revision	
<b>Change Note</b>	Add a description of the changes being made to the policy. This field is required.

- 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
<b>anti-replay</b>	Enable or disable anti-replay checking.	enable
<b>auth-cert</b>	Select the HTTPS server certificate for policy authentication.	none
<b>auth-path</b>	Enable or disable authentication-based routing.	disable
<b>auth-redirect-addr</b>	Select the HTTP-to-HTTPS redirect address for firewall authentication.	none
<b>auto-asic-offload</b>	Enable or disable policy traffic ASIC offloading.	enable
<b>block-notification</b>	Enable or disable block notification.	disable
<b>cgn-eif</b>	Enable or disable CGN endpoint independent filtering.	disable
<b>cgn-eim</b>	Enable or disable CGN endpoint independent mapping.	disable
<b>cgn-log-server-grp</b>	Select the NP log server group.	none
<b>cgn-resource-quota</b>	Set the allowed number of blocks assigned to a source IP address.	16
<b>cgn-session-quota</b>	Set the allowed concurrent sessions available for a source IP address.	16777215

Option	Description	Default
<b>custom-log-fields</b>	Select custom fields to append to log messages for this policy.	none
<b>delay-tcp-npu-session</b>	Enable or disable TCP NPU session delay to guarantee packet order of 3-way handshake.	disable
<b>diffserv-copy</b>	Enable or disable copying of the DSCP values from the original direction to the reply direction.	disable
<b>diffserv-forward</b>	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic. If enabled, also configure <code>diffservcode-forward</code> .	disable
<b>diffserv-reverse</b>	Enable or disable application of the DSCP value to the DSCP field of reverse (reply) traffic. If enabled, also configure <code>diffservcode-rev</code> .	disable
<b>diffservcode-forward</b>	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
<b>diffservcode-rev</b>	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
<b>dlp-profile</b>	Select an existing data leak prevention (DLP) profile.	none
<b>dsri</b>	Enable to ignore HTTP server responses.	disable
<b>dstaddr-negate</b>	Enable to negate the destination IP address.	disable
<b>dstaddr6-negate</b>	Enable to negate the destination IPv6 address.	disable
<b>dynamic-shaping</b>	Enable or disable dynamic RADIUS-defined traffic shaping.	disable
<b>email-collect</b>	Enable or disable email collection.	disable
<b>fec</b>	Enable or disable forward error correction (FEC) on traffic matching this policy on a FEC device.	disable
<b>firewall-session-dirty</b>	Select how to handle sessions if the configuration of this firewall policy changes.	check-all
<b>ffsso-agent-for-ntlm</b>	Select the FSSO agent for NTLM authentication.	none
<b>geoip-anycast</b>	Enable or disable recognition of anycast IP addresses using the geography IP database.	disable
<b>geoip-match</b>	Select whether to match the address based on the physical or registered location.	physical-location
<b>identity-based-route</b>	Select the identity-based routing rule.	none
<b>internet-service-negate</b>	Enable to negate the internet service set in the policy.	disable
<b>internet-service-src-negate</b>	Enable to negate the source internet service set in this policy.	disable

Option	Description	Default
<b>internet-service6</b>	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
<b>internet-service6-custom</b>	Select a custom IPv6 internet service.	none
<b>internet-service6-custom-group</b>	Select a custom IPv6 internet service group.	none
<b>internet-service6-group</b>	Select an IPv6 internet service group.	none
<b>internet-service6-name</b>	Select an IPv6 internet service.	none
<b>internet-service6-negate</b>	Enable to negate the source IPv6 internet service set in this policy.	disable
<b>internet-service6-src</b>	Enable or disable use of the IPv6 internet services in the source for this policy. If enabled, the source address is not used.	disable
<b>internet-service6-src-custom</b>	Select the custom IPv6 internet service source.	none
<b>internet-service6-src-custom-group</b>	Select the custom IPv6 source group.	none
<b>internet-service6-src-group</b>	Select the IPv6 source group.	none
<b>internet-service6-src-name</b>	Select the IPv6 source.	none
<b>internet-service6-src-negate</b>	Enable to negate the value set in <code>internet-service6-src</code> .	disable
<b>match-vip</b>	Enable or disable matching of packets that have had their destination address changed by a VIP.	disable
<b>match-vip-only</b>	Enable or disable matching only those packets that have had their destination addresses change by a VIP.	disable
<b>natinbound</b>	Enable or disable applying destination NAT to inbound traffic.	disable
<b>natip</b>	Set the source NAT IP address for inbound traffic.	0.0.0.0/0.0.0.0
<b>natoutbound</b>	Enable or disable applying destination NAT to outbound traffic.	disable
<b>network-service-dynamic</b>	Select a dynamic network service.	none
<b>network-service-src-dynamic</b>	Select a dynamic network service source.	none
<b>np-acceleration</b>	Enable or disable UTM network processor acceleration.	enable
<b>ntlm</b>	Enable or disable NTLM authentication.	disable

Option	Description	Default
<b>ntlm-enabled-browsers</b>	Set the HTTP-User-Agent value of supported browsers.	none
<b>ntlm-guest</b>	Enable or disable NTLM guest user access.	disable
<b>outbound</b>	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic.	enable
<b>passive-wan-health-measurement</b>	Enable or disable passive WAN health measurement. When enabled, <code>auto-asic-offload</code> is disabled.	disable.
<b>permit-any-host</b>	Enable or disable accepting UDP packets from any host.	disable
<b>permit-stun-host</b>	Enable or disable accepting UDP packets from any session traversal utilities for NAT (STUN) host.	disable
<b>policy-expiry</b>	Enable or disable policy expiry.	disable
<b>policy-expiry-date</b>	If policy-expiry is enabled, set the policy expiry date.	0000-00-00,00:00:00
<b>policy-offload</b>	Enable or disable hardware session setup for CGNAT.	enable
<b>radius-mac-auth-bypass</b>	Enable or disable MAC authentication bypass. The bypassed MAC address must be received from the RADIUS server.	disable
<b>redirect-url</b>	Set the URL to which users are redirected after seeing and accepting the disclaimer or authenticating.	none
<b>reputation-direction</b>	Set the destination of the initial traffic for reputation to take effect.	destination
<b>reputation-direction6</b>	Set the destination of the initial traffic for IPv6 reputation to take effect.	destination
<b>reputation-minimum</b>	Set the minimum reputation to take action.	0
<b>reputation-minimum6</b>	Set the minimum IPv6 reputation to take action.	0
<b>rtp-addr</b>	If this is an RTP NAT policy, set the address names.	none
<b>rtp-nat</b>	Enable or disable real time protocol (RTP) NAT.	disable
<b>schedule-timeout</b>	Enable or disable ending current sessions when the schedule object times out. Disable allows sessions to end from inactivity.	disable
<b>sctp-filter-profile</b>	Select an existing SCTP filter profile.	none
<b>send-deny-packet</b>	Enable or disable sending a reply when a session is denied or blocked by a firewall policy.	disable
<b>service-negate</b>	Enable or disable negation of the service set in the policy.	disable
<b>session-ttl</b>	Enter a value for the session time-to-live (TTL) from 300 to 604800, or type 0 for no limitation.	0
<b>sgt</b>	Enter security group tags (SGT).	none
<b>sgt-check</b>	Enable or disable SGT check.	disable



Option	Description	Default
<b>src-vendor-mac</b>	Select the vendor MAC source.	none
<b>srcaddr-negate</b>	Enable or disable negation of the source address.	disable
<b>srcaddr6-negate</b>	Enable or disable negation of the source IPv6 address.	disable
<b>ssh-filter-profile</b>	Select an SSH filter profile from the drop-down list.	None
<b>ssh-policy-redirect</b>	Enable or disable SSH policy redirect.	disable
<b>tcp-mss-receiver</b>	Enter the receiver's TCP maximum segment size (MSS).	0
<b>tcp-mss-sender</b>	Enter the sender's TCP MSS.	0
<b>tcp-session-without-syn</b>	Enable or disable creation of a TCP session without the SYN flag.	disable
<b>tcp-timeout-pid</b>	Select the TCP timeout profile.	none
<b>timeout-send-rst</b>	Enable or disable the sending of RST packets when TCP sessions expire	disable
<b>tos</b>	Enter the type of service (TOS) value used for comparison.	0
<b>tos-mask</b>	Enter the bit mask for TOS. Non-zero bit positions are used for comparison while zero bit positions are ignored.	0
<b>tos-negate</b>	Enable or disable to negate the TOS match.	disable
<b>udp-timeout-pid</b>	Select the UDP timeout profile.	none
<b>uuid</b>	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000
<b>vlan-cos-fwd</b>	Select the VLAN forward direction user priority. The available values are: <ul style="list-style-type: none"> <li>• 255 (passthrough)</li> <li>• 0 (lowest) - 7 (highest)</li> </ul>	255
<b>vlan-cos-rev</b>	Select the VLAN reverse direction user priority. The available values are: <ul style="list-style-type: none"> <li>• 255 (passthrough)</li> <li>• 0 (lowest) - 7 (highest)</li> </ul>	255
<b>vlan-filter</b>	Set VLAN filters.	none
<b>wanopt</b>	Enable or disable WAN optimization (IPv4 only).	disable
<b>wanopt-detection</b>	Select the WAN optimization as active, passive, or off.	active
<b>wanopt-passive-opt</b>	Select WAN optimization passive mode options. This option decides what IP address will be used to connect server (IPv4 only).	default
<b>wanopt-peer</b>	Select a WAN optimization peer (IPv4 only).	none

Option	Description	Default
<b>wanopt-profile</b>	Select a WAN optimization profile (IPv4 only).	none
<b>webcache</b>	Enable or disable web cache (IPv4 only).	disable
<b>webcache-https</b>	Enable or disable the web cache for HTTPS (IPv4 only).	none
<b>webproxy-forward-server</b>	Select the webproxy forward server (IPv4 only).	none
<b>webproxy-profile</b>	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
<b>ID</b>	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.
<b>Name</b>	Enter a unique name for the policy. Each policy must have a unique name.
<b>Virtual Wire Pair Interface</b>	Select one or more virtual wire pair interfaces. This field is required. New objects can be created by clicking the <i>Create New</i> icon in the <i>Object Selector</i> frame. See <a href="#">Create a new object on page 403</a> for more information.

Option	Description
<b>Virtual Wire Pair</b>	Select an arrow to indicate the flow of traffic between the ports in the selected <i>Virtual Wire Pair Interface</i> .
<b>Source</b>	Select the source address, address groups, virtual IPs, virtual IP groups, user, user groups, and FSSO groups.
<b>Enforce ZTNA</b>	Enable or disable ZTNA.
<b>EMS Tag</b>	Select the FortiClient EMS tag to match. This option is only available if Enforce ZTNA is enabled.
<b>Geographic IP Tag</b>	Select the Geographic IP tag to match. This option is only available if Enforce ZTNA is enabled.
<b>Destination</b>	Select the destination address, address groups, virtual IPs, virtual IP groups, and services.
<b>Service</b>	Select services and service groups. This option is only available when <i>Destination Internet Service</i> is off.
<b>SSL/SSH Inspection</b>	Select one of the following options for SSL/SSH Inspection: certificate-inspection custom-deep-inspection deep-inspection no-inspection
<b>Comments</b>	Add a description of the policy, such as its purpose, or the changes that have been made to it.
<b>Advanced Options</b>	Configure advanced options, see <a href="#">Advanced options</a> below. For more information on advanced option, see the <a href="#">FortiOS CLI Reference</a> .
<b>Change Note</b>	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
<b>anti-replay</b>	Enable or disable anti-replay checking.	enable
<b>auth-cert</b>	Select the HTTPS server certificate for policy authentication.	none
<b>auth-path</b>	Enable or disable authentication-based routing.	disable
<b>auth-redirect-addr</b>	Select the HTTP-to-HTTPS redirect address for firewall authentication.	none
<b>auto-asic-offload</b>	Enable or disable policy traffic ASIC offloading.	enable
<b>block-notification</b>	Enable or disable block notification.	disable
<b>cgn-eif</b>	Enable or disable CGN endpoint independent filtering.	disable

Option	Description	Default
<b>cgn-eim</b>	Enable or disable CGN endpoint independent mapping.	disable
<b>cgn-log-server-grp</b>	Select the NP log server group.	none
<b>cgn-resource-quota</b>	Set the allowed number of blocks assigned to a source IP address.	16
<b>cgn-session-quota</b>	Set the allowed concurrent sessions available for a source IP address.	16777215
<b>custom-log-fields</b>	Select custom fields to append to log messages for this policy.	none
<b>delay-tcp-npu-session</b>	Enable or disable TCP NPU session delay to guarantee packet order of 3-way handshake.	disable
<b>diffserv-copy</b>	Enable or disable copying of the DSCP values from the original direction to the reply direction.	disable
<b>diffserv-forward</b>	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic. If enabled, also configure <code>diffservcode-forward</code> .	disable
<b>diffserv-reverse</b>	Enable or disable application of the DSCP value to the DSCP field of reverse (reply) traffic. If enabled, also configure <code>diffservcode-rev</code> .	disable
<b>diffservcode-forward</b>	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
<b>diffservcode-rev</b>	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
<b>dlp-profile</b>	Select an existing data leak prevention (DLP) profile.	none
<b>dsri</b>	Enable to ignore HTTP server responses.	disable
<b>dstaddr-negate</b>	Enable to negate the destination IP address.	disable
<b>dstaddr6-negate</b>	Enable to negate the destination IPv6 address.	disable
<b>dynamic-shaping</b>	Enable or disable dynamic RADIUS-defined traffic shaping.	disable
<b>email-collect</b>	Enable or disable email collection.	disable
<b>fec</b>	Enable or disable forward error correction (FEC) on traffic matching this policy on a FEC device.	disable
<b>firewall-session-dirty</b>	Select how to handle sessions if the configuration of this firewall policy changes.	check-all
<b>ffsso-agent-for-ntlm</b>	Select the FSSO agent for NTLM authentication.	none
<b>geoip-anycast</b>	Enable or disable recognition of anycast IP addresses using the geography IP database.	disable

Option	Description	Default
<b>geoip-match</b>	Select whether to match the address based on the physical or registered location.	physical-location
<b>identity-based-route</b>	Select the identity-based routing rule.	none
<b>internet-service-negate</b>	Enable to negate the internet service set in the policy.	disable
<b>internet-service-src-negate</b>	Enable to negate the source internet service set in this policy.	disable
<b>internet-service6</b>	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
<b>internet-service6-custom</b>	Select a custom IPv6 internet service.	none
<b>internet-service6-custom-group</b>	Select a custom IPv6 internet service group.	none
<b>internet-service6-group</b>	Select an IPv6 internet service group.	none
<b>internet-service6-name</b>	Select an IPv6 internet service.	none
<b>internet-service6-negate</b>	Enable to negate the source IPv6 internet service set in this policy.	disable
<b>internet-service6-src</b>	Enable or disable use of the IPv6 internet services in the source for this policy. If enabled, the source address is not used.	disable
<b>internet-service6-src-custom</b>	Select the custom IPv6 internet service source.	none
<b>internet-service6-src-custom-group</b>	Select the custom IPv6 source group.	none
<b>internet-service6-src-group</b>	Select the IPv6 source group.	none
<b>internet-service6-src-name</b>	Select the IPv6 source.	none
<b>internet-service6-src-negate</b>	Enable to negate the value set in <code>internet-service6-src</code> .	disable
<b>match-vip</b>	Enable or disable matching of packets that have had their destination address changed by a VIP.	disable
<b>match-vip-only</b>	Enable or disable matching only those packets that have had their destination addresses change by a VIP.	disable
<b>natinbound</b>	Enable or disable applying destination NAT to inbound traffic.	disable
<b>natip</b>	Set the source NAT IP address for inbound traffic.	0.0.0.0/0.0.0.0
<b>natoutbound</b>	Enable or disable applying destination NAT to outbound traffic.	disable

Option	Description	Default
<b>network-service-dynamic</b>	Select a dynamic network service.	none
<b>network-service-src-dynamic</b>	Select a dynamic network service source.	none
<b>np-acceleration</b>	Enable or disable UTM network processor acceleration.	enable
<b>ntlm</b>	Enable or disable NTLM authentication.	disable
<b>ntlm-enabled-browsers</b>	Set the HTTP-User-Agent value of supported browsers.	none
<b>ntlm-guest</b>	Enable or disable NTLM guest user access.	disable
<b>outbound</b>	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic.	enable
<b>passive-wan-health-measurement</b>	Enable or disable passive WAN health measurement. When enabled, <code>auto-asic-offload</code> is disabled.	disable.
<b>permit-any-host</b>	Enable or disable accepting UDP packets from any host.	disable
<b>permit-stun-host</b>	Enable or disable accepting UDP packets from any session traversal utilities for NAT (STUN) host.	disable
<b>policy-expiry</b>	Enable or disable policy expiry.	disable
<b>policy-expiry-date</b>	If policy-expiry is enabled, set the policy expiry date.	0000-00-00,00:00:00
<b>policy-offload</b>	Enable or disable hardware session setup for CGNAT.	enable
<b>radius-mac-auth-bypass</b>	Enable or disable MAC authentication bypass. The bypassed MAC address must be received from the RADIUS server.	disable
<b>redirect-url</b>	Set the URL to which users are redirected after seeing and accepting the disclaimer or authenticating.	none
<b>reputation-direction</b>	Set the destination of the initial traffic for reputation to take effect.	destination
<b>reputation-direction6</b>	Set the destination of the initial traffic for IPv6 reputation to take effect.	destination
<b>reputation-minimum</b>	Set the minimum reputation to take action.	0
<b>reputation-minimum6</b>	Set the minimum IPv6 reputation to take action.	0
<b>rtp-addr</b>	If this is an RTP NAT policy, set the address names.	none
<b>rtp-nat</b>	Enable or disable real time protocol (RTP) NAT.	disable
<b>schedule-timeout</b>	Enable or disable ending current sessions when the schedule object times out. Disable allows sessions to end from inactivity.	disable
<b>sctp-filter-profile</b>	Select an existing SCTP filter profile.	none

Option	Description	Default
<b>send-deny-packet</b>	Enable or disable sending a reply when a session is denied or blocked by a firewall policy.	disable
<b>service-negate</b>	Enable or disable negation of the service set in the policy.	disable
<b>session-ttl</b>	Enter a value for the session time-to-live (TTL) from 300 to 604800, or type 0 for no limitation.	0
<b>sgt</b>	Enter security group tags (SGT).	none
<b>sgt-check</b>	Enable or disable SGT check.	disable
<b>src-vendor-mac</b>	Select the vendor MAC source.	none
<b>srcaddr-negate</b>	Enable or disable negation of the source address.	disable
<b>srcaddr6-negate</b>	Enable or disable negation of the source IPv6 address.	disable
<b>ssh-filter-profile</b>	Select an SSH filter profile from the drop-down list.	None
<b>ssh-policy-redirect</b>	Enable or disable SSH policy redirect.	disable
<b>tcp-mss-receiver</b>	Enter the receiver's TCP maximum segment size (MSS).	0
<b>tcp-mss-sender</b>	Enter the sender's TCP MSS.	0
<b>tcp-session-without-syn</b>	Enable or disable creation of a TCP session without the SYN flag.	disable
<b>tcp-timeout-pid</b>	Select the TCP timeout profile.	none
<b>timeout-send-rst</b>	Enable or disable the sending of RST packets when TCP sessions expire	disable
<b>tos</b>	Enter the type of service (TOS) value used for comparison.	0
<b>tos-mask</b>	Enter the bit mask for TOS. Non-zero bit positions are used for comparison while zero bit positions are ignored.	0
<b>tos-negate</b>	Enable or disable to negate the TOS match.	disable
<b>udp-timeout-pid</b>	Select the UDP timeout profile.	none
<b>uuid</b>	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000
<b>vlan-cos-fwd</b>	Select the VLAN forward direction user priority. The available values are: <ul style="list-style-type: none"> <li>• 255 (passthrough)</li> <li>• 0 (lowest) - 7 (highest)</li> </ul>	255
<b>vlan-cos-rev</b>	Select the VLAN reverse direction user priority. The available values are: <ul style="list-style-type: none"> <li>• 255 (passthrough)</li> <li>• 0 (lowest) - 7 (highest)</li> </ul>	255

Option	Description	Default
<b>vlan-filter</b>	Set VLAN filters.	none
<b>wanopt</b>	Enable or disable WAN optimization (IPv4 only).	disable
<b>wanopt-detection</b>	Select the WAN optimization as active, passive, or off.	active
<b>wanopt-passive-opt</b>	Select WAN optimization passive mode options. This option decides what IP address will be used to connect server (IPv4 only).	default
<b>wanopt-peer</b>	Select a WAN optimization peer (IPv4 only).	none
<b>wanopt-profile</b>	Select a WAN optimization profile (IPv4 only).	none
<b>webcache</b>	Enable or disable web cache (IPv4 only).	disable
<b>webcache-https</b>	Enable or disable the web cache for HTTPS (IPv4 only).	none
<b>webproxy-forward-server</b>	Select the webproxy forward server (IPv4 only).	none
<b>webproxy-profile</b>	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 590](#).

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 353](#).

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
<b>ID</b>	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.



Option	Description
	Once a policy ID has been configured it cannot be changed.
<b>Name</b>	Enter a unique name for the policy. Each policy must have a unique name.
<b>Virtual Wire Pair Interface</b>	Select one or more virtual wire pair interfaces. This field is required..
<b>Virtual Wire Pair</b>	Select an arrow to indicate the flow of traffic between the ports in the selected <i>Virtual Wire Pair Interface</i> .
<b>Source</b>	Select the source address, address groups, virtual IPs, virtual IP groups, user, user groups, and FSSO groups.
<b>Destination</b>	Select the destination address, address groups, virtual IPs, virtual IP groups, and services.
<b>Schedule</b>	Select a one-time schedule, recurring schedule, or schedule group.
<b>Service</b>	Select the service. Select <i>App Default</i> or <i>Specify</i> . If <i>Specify</i> is selected, select the Service.
<b>Application</b>	Select applications.
<b>URL Category</b>	Select URL categories.
<b>Action</b>	Select an action for the policy to take: <i>DENY</i> or <i>ACCEPT</i> .
<b>Log Traffic</b>	<p>When the <i>Action</i> is <i>DENY</i>, select <i>Log Violation Traffic</i> to log violation traffic.</p> <p>When the <i>Action</i> is <i>ACCEPT</i>, select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>No Log</i></li> <li>• <i>Log Security Events</i></li> <li>• <i>Log All Sessions</i></li> </ul> <p>Select whether to generate logs when the session starts.</p>
<b>Protocol Options</b>	<p>Select protocol options profiles for handling protocol-specific traffic.</p> <p>This option is available when the <i>Action</i> is <i>ACCEPT</i>.</p>
<b>Security Profiles</b>	<p>Select to add security profiles or profile groups.</p> <p>This option is available when the <i>Action</i> is <i>ACCEPT</i>.</p> <p>If <i>Use Standard Security Profiles</i> is selected, the following standard security profile types can be added:</p> <ul style="list-style-type: none"> <li>• AntiVirus Profile</li> <li>• Web Filter Profile</li> <li>• IPS Profile</li> <li>• Email Filter</li> <li>• File Filter Profile</li> </ul> <p>If <i>Use Security Profile Group</i> is selected, select the <i>Profile Group</i>.</p>
<b>Comments</b>	Add a description of the policy, such as its purpose, or the changes that have been made to it.
<b>Advanced Options</b>	<p>Configure advanced options, see <a href="#">Advanced options</a> below.</p> <p>For more information on advanced option, see the <a href="#">FortiOS CLI Reference</a>.</p>

Option	Description
<b>Change Note</b>	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
<b>application-list</b>	Select ...an existing application list.	none
<b>comments</b>	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 <i>Comments</i> field.	none
<b>dlp-profile</b>	Select an existing data leak prevention (DLP) profile.	none
<b>dnsfilter-profile</b>	Select an existing DNS filter profile.	none
<b>dstaddr-negate</b>	Enable to negate the values set in <i>IPv4 Destination Address</i> and <i>IPv6 Destination Address</i> .	disable
<b>global-label</b>	Set the label for the policy to be displayed when the GUI is in <i>Global View</i> mode.	none
<b>icap-profile</b>	Select an existing Internet Content Adaptation Protocol (ICAP) profile.	none
<b>internet-service-negate</b>	When enabled, Internet services match against any Internet service except the selected Internet service.	disable
<b>internet-service-src-negate</b>	Enables or disables the use of Internet Services in source for this policy. If enabled, <i>internet-service-src</i> specifies what the service must NOT be.	disable
<b>internet-service6</b>	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
<b>internet-service6-custom</b>	Select a custom IPv6 internet service.	none
<b>internet-service6-custom-group</b>	Select a custom IPv6 internet service group.	none
<b>internet-service6-group</b>	Select an IPv6 internet service group.	none
<b>internet-service6-name</b>	Select an IPv6 internet service.	none
<b>internet-service6-negate</b>	Enable to negate the source IPv6 internet service set in this policy.	disable

Option	Description	Default
<b>internet-service6-src</b>	Enable or disable use of the IPv6 internet services in the source for this policy. If enabled, the source address is not used.	disable
<b>internet-service6-src-custom</b>	Select the custom IPv6 internet service source.	none
<b>internet-service6-src-custom-group</b>	Select the custom IPv6 source group.	none
<b>internet-service6-src-group</b>	Select the IPv6 source group.	none
<b>internet-service6-src-name</b>	Select the IPv6 source.	none
<b>internet-service6-src-negate</b>	Enable to negate the value set in <code>internet-service6-src</code> .	disable
<b>nat46</b>	Enable or disable NAT46.	disable
<b>nat64</b>	Enable or disable NAT64.	disable
<b>sctp-filter-profile</b>	Select an existing stream control transmission protocol (SCTP) filter profile.	none
<b>send-deny-packet</b>	Enable or disable sending a reply packet when a session is denied or blocked by this policy.	disable
<b>service-negate</b>	Enable or disable negation of the selected <i>Service</i> .	disable
<b>srcaddr-negate</b>	Enable or disable negation of the <i>IPv4 Source Address</i> or <i>IPv6 Source Address</i> address.	disable
<b>ssh-filter-profile</b>	Select an existing SSH filter profile.	none
<b>ssl-ssh-profile</b>	Select an existing SSL SSH profile.	no-inspection
<b>utm-status</b>	Enable or disable the Unified Threat Management status.	disable
<b>uuid</b>	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000
<b>voip-profile</b>	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 Packages > 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
<b>Name</b>	Enter a unique name for the policy. Each policy must have a unique name.
<b>Proxy</b>	Select the proxy type: <i>Explicit Web</i> , <i>Transparent Web</i> , <i>FTP</i> , <i>WAN Optimize</i> , or <i>ZTNA</i> .
<b>Incoming Interface</b>	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 <i>Transparent Web</i> .
<b>Outgoing Interface</b>	Select outgoing interfaces in the same manner as <i>Incoming Interface</i> .
<b>Source</b>	Select source addresses, address groups, virtual IPs, and virtual IP groups.
<b>ZTNA Tag</b>	For ZTNA proxy policies, select the ZTNA tags and tag groups. See <a href="#">Zero Trust Network Access (ZTNA) objects on page 442</a> . This option is only available when the proxy type is set to <i>ZTNA</i> .
<b>Destination</b>	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
<b>ZTNA Server</b>	For ZTNA proxy policies, select a ZTNA server. See <a href="#">Configuring a ZTNA server on page 445</a> . This option is only available when the proxy type is set to <i>ZTNA</i> .
<b>Service</b>	Select services and service groups from the object selector pane.
<b>Schedule</b>	Select a one-time schedule, recurring schedule, or schedule group.
<b>Action</b>	Select an action for the policy to take: <i>Deny</i> , <i>Accept</i> , or <i>Redirect</i> . <i>Redirect</i> is only available when the proxy type is set to <i>Explicit Web</i> or <i>Transparent Web</i> .
<b>Log Allowed Traffic</b>	Select one of the following options: <ul style="list-style-type: none"> <li>• <i>No Log</i></li> <li>• <i>Log Security Events</i></li> <li>• <i>Log All Sessions</i></li> </ul> If logging is set to <i>Log All Sessions</i> , select whether to generate logs when the session starts.

Option	Description
	This option is available when the <i>Action</i> is <i>Accept</i> .
<b>Log Violation Traffic</b>	Select to log violation traffic. This option is available when the <i>Action</i> is <i>Deny</i> .
<b>Display Disclaimer</b>	Set the Display Disclaimer: <i>Disable</i> , <i>By Domain</i> , <i>By Policy</i> , or <i>By User</i> . Optionally, if enabled, select a custom message in the <i>Customize Messages</i> field. This option is available when the <i>Action</i> is <i>Accept</i> .
<b>Security Profiles</b>	Select to add security profiles or profile groups. If <i>Use Standard Security Profiles</i> is selected the following profile types can be added: <ul style="list-style-type: none"> <li>• Antivirus Profile</li> <li>• Web Filter Profile (not available when the proxy type is set to <i>FTP</i>)</li> <li>• Video Profile Filter</li> <li>• Application Control (not available when the proxy type is set to <i>FTP</i>)</li> <li>• IPS Profile (not available when the proxy type is set to <i>FTP</i>)</li> <li>• File Filter Profile</li> <li>• ICAP (not available when the proxy type is set to <i>FTP</i>)</li> <li>• Web Application Firewall (not available when the proxy type is set to <i>FTP</i>)</li> </ul> In <i>Protocol Options</i> , select a protocol options group. If <i>Use Security Profile Group</i> is selected, select the <i>Profile Group</i> . This option is available when the <i>Action</i> is <i>Accept</i> .
<b>SSL/SSH Inspection</b>	Select one of the following options for SSL/SSH Inspection: certificate-inspection custom-deep-inspection deep-inspection no-inspection This option is not available when the <i>Security Profiles Profile Type</i> is set to <i>Use Security Profile Group</i> .
<b>Redirect URL</b>	Enter the redirect URL. This option is only available when the <i>Action</i> is <i>Redirect</i> . When the <i>Action</i> is <i>Redirect</i> , this field is required.
<b>Web Proxy Forwarding Server</b>	Select a web proxy forwarding server. This option is not available when the proxy type is set to <i>FTP</i> .
<b>Comments</b>	Add a description of the policy, such as its purpose, or the changes that have been made to it.
<b>Advanced Options</b>	Configure advanced options, see <a href="#">Advanced options</a> below. For more information on advanced option, see the <a href="#">FortiOS CLI Reference</a> .
<b>Change Note</b>	Add a description of the changes being made to the policy. This field is required.

- 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
<b>access-proxy</b>	Select an IPv4 access proxy.	none
<b>access-proxy6</b>	Select an IPv6 access proxy.	none
<b>block-notification</b>	Enable or disable block notification.	disable
<b>device-ownership</b>	Enable or disable ownership enforcement at the policy level.	disable
<b>dlp-profile</b>	Select an existing data leak prevention (DLP) profile.	none
<b>dstaddr-negate</b>	Enable or disable negation of the values set in <i>Destination</i> .	disable
<b>global-label</b>	Enter the label for the policy to be displayed when the GUI is in <i>Global View</i> mode.	none
<b>http-tunnel-auth</b>	Enable or disable HTTP tunnel authentication	disable
<b>internet-service-negate</b>	Enable or disable negation of the internet service.	disable
<b>label</b>	Set the label for the policy to be displayed in the VDOM.	none
<b>sctp-filter-profile</b>	Select an existing stream control transmission protocol (SCTP) filter profile.	none
<b>service-negate</b>	Enable or disable negation of the service specified in <i>Service</i> .	disable
<b>session-ttl</b>	Session TTL for sessions accepted by this policy (300 - 6040800 seconds, 0 = use system default).	0
<b>srcaddr-negate</b>	Enable or disable negation of the source address.	disable
<b>ssh-filter-profile</b>	Select an existing SSH filter profile.	none
<b>ssh-policy-redirect</b>	Enable or disable SSH policy redirect.	disable
<b>transparent</b>	Enable or disable using the IP address of the client to connect to the server.	disable
<b>uuid</b>	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000
<b>webcache</b>	Enable or disable web cache.	disable
<b>webcache-https</b>	Enable or disable web cache for HTTPS.	disable
<b>webproxy-profile</b>	Select a webproxy profile.	none
<b>ztna-ems-tag</b>	Select ZTNA EMS tags.	none
<b>ztna-tags-match-logic</b>	Set the logic used for matching ZTNA tags. The available options are <b>and</b> and <b>or</b> .	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 310](#).

*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
<b>Type</b>	Select whether to perform SNAT on IPv4 or IPv6.
<b>Incoming Interface</b>	Click the field then select interfaces. Click the remove icon to remove interfaces. New objects can be created by clicking the <i>Create New</i> icon in the <i>Object Selector</i> frame. See <a href="#">Create a new object on page 403</a> for more information.
<b>Outgoing Interface</b>	Select outgoing interfaces in the same manner as <i>Incoming Interface</i> .

Option	Description
<b>Source Address</b>	Select source addresses, address groups, virtual IPs, and virtual IP groups.
<b>Destination Address</b>	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
<b>NAT</b>	Select to enable NAT. If enabled, select <i>NAT</i> , <i>NAT46</i> , or <i>NAT64</i> . If <i>Type</i> is set to <i>IPv4</i> , <i>NAT64</i> is not available. If <i>Type</i> is set to <i>IPv6</i> , <i>NAT46</i> is not available.
<b>IP Pool Configuration</b>	If <i>NAT</i> is selected, select <i>Use Outgoing Interface Address</i> or <i>Use Dynamic IP Pool</i> .
<b>Protocol</b>	Select the protocol: <i>ANY</i> , <i>TCP</i> , <i>UDP</i> , <i>SCTP</i> , or <i>Specify</i> . If <i>Specify</i> is selected, specify the protocol number. This option is only available when <i>NAT</i> is selected.
<b>Explicit Port Mapping</b>	Enable or disable port mapping, then set the <i>Original Source Port</i> 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 <a href="#">Dynamic SNAT</a> in the FortiOS Administration Guide for more information about how each IP pool type works.
<b>Comments</b>	Add a description of the policy, such as its purpose, or the changes that have been made to it.
<b>Advanced Options</b>	Configure advanced options, see <a href="#">Advanced options</a> below. For more information on advanced option, see the <a href="#">FortiOS CLI Reference</a> .
<b>Change Note</b>	Add a description of the changes being made to the policy. This field is required.

- 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
<b>uuid</b>	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 (*Object Configurations > 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 310](#).

*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
<b>Name</b>	Enter a unique name for the policy. Each policy must have a unique name.
<b>Comments</b>	Add a description of the policy, such as its purpose, or the changes that have been made to it.
<b>Color</b>	Select a color. This color will be used to identify this DNAT in the fabric view.
<b>Status</b>	Enable or disable the policy.

Option	Description
	This option is not available for IPv6 policies.
<b>Interface</b>	Select an interface.
<b>Configure Default Value</b>	Enable or disable the default value.
<b>Type</b>	<p>Select the network type: <i>Static NAT</i>, <i>DNS Translation</i>, <i>FQDN</i>, or <i>Load balance</i>.</p> <p>This option is only available when <i>Configure Default Value</i> is enabled.</p> <p>For IPv6 policies, only <i>Static NAT</i> is available.</p>
<b>External IP Address/Range</b>	<p>Enter the start and end external IP addresses in the fields. If there is only one address, enter it in both fields.</p> <p>This option is only available when <i>Configure Default Value</i> is enabled and the network type is not <i>FQDN</i>.</p>
<b>Mapped IP [v4/v6] Address/Range</b>	<p>Enter the mapped IP address or address range.</p> <p>These options are only available when <i>Configure Default Value</i> is enabled and the network type is not <i>FQDN</i>.</p> <p>For IPv6 policies, select <i>Use Embedded</i> to use the lower 32 bits of the external IPv6 address as the mapped IPv4 address.</p>
<b>External IP Address</b>	<p>Enter the external IP address.</p> <p>This option is only available when <i>Configure Default Value</i> is enabled and the network type is <i>FQDN</i>.</p>
<b>Mapped Address</b>	<p>Select the mapped address.</p> <p>This option is only available when <i>Configure Default Value</i> is enabled and the network type is <i>FQDN</i>.</p>
<b>Source Interface Filter</b>	<p>Select a source interface filter.</p> <p>This option is only available when <i>Configure Default Value</i> is enabled.</p>
<b>Optional Filters</b>	<p>Enable or disable optional filters.</p> <p>This option is only available when <i>Configure Default Value</i> is enabled.</p>
<b>Source Address</b>	If <i>Optional Filters</i> is enabled, add source IP, range, or subnet filters. Multiple filters can be added using the <i>Add</i> icon.
<b>Services</b>	If <i>Optional Filters</i> is enabled, enable or disable and then select services.
<b>Port Forwarding</b>	<p>Enable or disable port forwarding and then configure the ports to map.</p> <p>This option is only available when <i>Configure Default Value</i> is enabled.</p>
<b>Protocol</b>	If <i>Port Forwarding</i> is enabled, select the protocol: <i>TCP</i> , <i>UDP</i> , <i>SCTP</i> , or <i>ICMP</i> . <i>ICMP</i> is not available for IPv6 policies.
<b>External Service Port</b>	<p>If <i>Port Forwarding</i> is enabled, enter the external service port.</p> <p>This option is not available when <i>Protocol</i> is <i>ICMP</i>.</p>
<b>Map to [IPv4/IPv6] Port</b>	<p>If <i>Port Forwarding</i> is enabled, enter the map to port.</p> <p>This option is not available when <i>Protocol</i> is <i>ICMP</i>.</p>

Option	Description
<b>Enable ARP Reply</b>	Select to enable address resolution protocol (ARP) reply. This option is only available when <i>Configure Default Value</i> is enabled.
<b>Add To Groups</b>	Select the groups to which the virtual IP should be added.
<b>Advanced Options</b>	Configure advanced options, see <a href="#">Advanced options</a> below. For more information on advanced option, see the <a href="#">FortiOS CLI Reference</a> .
<b>Per-Device Mapping</b>	Enable or disable per-device mapping. If multiple imported VIP objects have the same name but different details, the object type will become <i>Dynamic Virtual IP</i> , and the per-device mappings will be listed here. Mappings can also be manually added, edited, and deleted as needed.
<b>Change Note</b>	Add a description of the changes being made to the policy. This field is required.

- 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:

- Ensure you are in the correct ADOM.
- Go to *Policy & Objects > Policy Packages*.
- In the tree menu for the policy package, click *Central DNAT*.
- Click *Import* in the toolbar. The *Import* dialog box will open.
- Select the VIP object or objects that need to be imported. If necessary, use the search box to locate specific objects.
- Click **OK** to import the VIPs to the *Central DNAT* table.

#### Advanced options

Option	Description	Default
<b>add-nat46-route</b>	Enable or disable adding NAT46 to a route. This option is not available for IPv6 policies.	enable
<b>add-nat64-route</b>	Enable or disable adding NAT64 to a route. This option is only available for IPv6 policies.	enable
<b>dns-mapping-ttl</b>	Enter time-to-live for DNS response, from 0 to 604 800. Set to 0 to use the DNS server's response time. This option is not available for IPv6 policies.	0
<b>extaddr</b>	Select an external FQDN. This option is not available for IPv6 policies.	None
<b>gratuitous-arp-interval</b>	Set the time interval in 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	0

Option	Description	Default
	This option is not available for IPv6 policies.	
<b>http-cookie-age</b>	Set the time in minutes that client web browsers should keep a cookie. Set to 0 for no time limit.	60
<b>http-cookie-domain</b>	Enter the domain name to which cookie persistence should apply.	none
<b>http-cookie-domain-from-host</b>	Enable or disable use of the HTTP cookie domain from the <code>host</code> field in HTTP.	disable
<b>http-cookie-generation</b>	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
<b>http-cookie-path</b>	Specify the path to which cookie persistence is limited.	none
<b>http-cookie-share</b>	Configure to control the sharing of cookies across virtual servers. Using <code>same-ip</code> 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
<b>http-ip-header</b>	For HTTP multiplexing, enable or disable to add the original client IP address in the <code>X-Forwarded-For</code> HTTP header.	disable
<b>http-ip-header-name</b>	For HTTP multiplexing, enter a custom HTTP header name. The original client IP address is added to this header. If empty, <code>X-Forwarded-For</code> is used.	none
<b>http-multiplex</b>	Enable or disable HTTP multiplexing.	disable
<b>http-redirect</b>	Enable or disable redirection of HTTP to HTTPS.	disable
<b>https-cookie-secure</b>	Enable or disable verification that HTTPS cookies are secure.	disable
<b>id</b>	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
<b>lbd-method</b>	Select the method used to distribute sessions to real servers.	static
<b>max-embryonic-connections</b>	Set the maximum number of incomplete connections, from 0 to 100000.	1000
<b>monitor</b>	Select the health check monitor to use when polling to determine a virtual server's connectivity status.	none
<b>nat-source-vip</b>	Enable or disable forcing the source NAT mapped IP to the external IP for all traffic.	disable
<b>nat44</b>	Enable or disable NAT44. This option is not available for IPv6 policies.	enable

Option	Description	Default
<b>nat46</b>	Enable or disable NAT46. This option is not available for IPv6 policies.	disable
<b>nat64</b>	Enable or disable NAT64. This option is only available for IPv6 policies.	enable
<b>nat66</b>	Enable or disable NAT66. This option is only available for IPv6 policies.	disable
<b>outlook-web-access</b>	Enable to add the <code>Front-End-Https</code> header for Microsoft Outlook Web Access.	disable
<b>persistence</b>	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
<b>portmapping-type</b>	Select the port mapping type, either <code>1-to-1</code> or <code>m-to-n</code> (many to many). This option is not available for IPv6 policies.	1-to-1
<b>server-type</b>	Select the protocol to be load balanced by the virtual server (also called the server load balance virtual IP).	none
<b>ssl-accept-ffdhe-groups</b>	Enable or disable using the FFDHE cipher suite for SSL key exchange.	enable
<b>ssl-algorithm</b>	Set the permitted encryption algorithms for SSL sessions according to encryption strength: <ul style="list-style-type: none"> <li><code>high</code>: permit only high encryption algorithms: AES or 3DES.</li> <li><code>medium</code>: permit high or medium (RC4) algorithms.</li> <li><code>low</code>: permit high, medium, or low (DES) algorithms.</li> <li><code>custom</code>: only allow some preselected cipher suites to be used.</li> </ul>	high
<b>ssl-certificate</b>	Select the certificate to use for SSL handshake.	none
<b>ssl-client-fallback</b>	Enable or disable support for preventing downgrade attacks on client connections.	enable
<b>ssl-client-rekey-count</b>	Set the maximum length of data in MB before triggering a client rekey. Set to 0 to disable.	0
<b>ssl-client-renegotiation</b>	Select the SSL secure renegotiation policy. <ul style="list-style-type: none"> <li><code>allow</code>: allow, but do not require secure renegotiation.</li> <li><code>deny</code>: do not allow renegotiation.</li> <li><code>secure</code>: require secure renegotiation.</li> </ul>	allow
<b>ssl-client-session-state-max</b>	Set the maximum number of SSL session states to keep between the client and FortiGate, from 0 to 100000.	1000
<b>ssl-client-session-state-timeout</b>	Set the number of minutes to keep the SSL session states between the client and FortiGate, from 1 to 14400.	30

Option	Description	Default
<b>ssl-client-session-state-type</b>	Select the method to use to expire SSL sessions between the client and FortiGate. <ul style="list-style-type: none"> <li><b>both:</b> expire SSL session states when either <code>ssl-client-session-state-max</code> or <code>ssl-client-session-state-timeout</code> is exceeded, regardless of which occurs first.</li> <li><b>count:</b> expire SSL session states when <code>ssl-client-session-state-max</code> is exceeded.</li> <li><b>disable:</b> expire all SSL session states.</li> <li><b>time:</b> expire SSL session states when <code>ssl-client-session-state-timeout</code> is exceeded.</li> </ul>	both
<b>ssl-dh-bits</b>	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
<b>ssl-hpkp</b>	Enable or disable including HPKP header in the response.	disable
<b>ssl-hpkp-age</b>	Set the number of seconds that the client should honor the HPKP setting (60 - 157680000).	5184000
<b>ssl-hpkp-backup</b>	Select the certificate used to generate the backup HPKP pin from.	none
<b>ssl-hpkp-include-subdomains</b>	Enable or disable indicating that the HPKP header applies to all subdomains.	disable
<b>ssl-hpkp-primary</b>	Select the certificate used to generate the primary HPKP pin from.	none
<b>ssl-hpkp-report-uri</b>	Set the URL to report HPKP violations to (maximum size = 255).	none
<b>ssl-hsts</b>	Enable or disable including HSTS header in response.	disable
<b>ssl-hsts-age</b>	Set the number of seconds that the client should honour the HSTS setting (60 - 157680000).	5184000
<b>ssl-hsts-include-subdomains</b>	Enable or disable indicating that the HSTS header applies to all subdomains.	disable
<b>ssl-http-location-conversion</b>	Enable to replace HTTP with HTTPS in the reply's <code>Location</code> HTTP header field.	disable
<b>ssl-http-match-host</b>	Enable or disable HTTP host matching for location conversion.	disable
<b>ssl-max-version</b>	Select the highest version of SSL/TLS to allow in SSL sessions: <code>ssl-3.0</code> , <code>tls-1.0</code> , <code>tls-1.1</code> , <code>tls-1.2</code> , or <code>tls-1.3</code> .	tls-1.3
<b>ssl-min-version</b>	Select the lowest version of SSL/TLS to allow in SSL sessions: <code>ssl-3.0</code> , <code>tls-1.0</code> , <code>tls-1.1</code> , <code>tls-1.2</code> , or <code>tls-1.3</code> .	tls-1.1
<b>ssl-mode</b>	Select the method to use for SSL offloading between the client and FortiGate ( <code>half</code> ) or from the client to FortiGate and from FortiGate to the server ( <code>full</code> ).	half
<b>ssl-pfs</b>	Select the cipher suites that can be used for SSL perfect forward secrecy (PFS):	require

Option	Description	Default
	<ul style="list-style-type: none"> <li><b>allow:</b> allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.</li> <li><b>deny:</b> allow only non-Diffie-Hellman cipher suites, so PFS is not applied.</li> <li><b>require:</b> allow only Diffie-Hellman cipher suites, so PFS is applied.</li> </ul> <p>This setting applies to both client and server sessions.</p>	
<b>ssl-send-empty-frags</b>	<p>Enable or disable sending empty fragments to avoid CBC IV attacks (SSL 3.0 and TLS 1.0 only).</p> <p>This setting may need to be disabled for compatibility with older systems.</p>	enable
<b>ssl-server-algorithm</b>	<p>Set the permitted encryption algorithms for SSL server sessions according to encryption strength:</p> <ul style="list-style-type: none"> <li><b>high:</b> permit only high encryption algorithms: AES or 3DES.</li> <li><b>medium:</b> permit high or medium (RC4) algorithms.</li> <li><b>low:</b> permit high, medium, or low (DES) algorithms.</li> <li><b>custom:</b> only allow some preselected cipher suites to be used.</li> <li><b>client:</b> Use the same encryption algorithms for both client and server sessions.</li> </ul>	client
<b>ssl-server-max-version</b>	<p>Select the highest version of SSL/TLS to allow in SSL server sessions: <code>client</code>, <code>ssl-3.0</code>, <code>tls-1.0</code>, <code>tls-1.1</code>, <code>tls-1.2</code>, or <code>tls-1.3</code>.</p>	client
<b>ssl-server-min-version</b>	<p>Select the lowest version of SSL/TLS to allow in SSL server sessions: <code>client</code>, <code>ssl-3.0</code>, <code>tls-1.0</code>, <code>tls-1.1</code>, <code>tls-1.2</code>, or <code>tls-1.3</code>.</p>	client
<b>ssl-server-session-state-max</b>	<p>Set the maximum number of FortiGate to server SSL session states to keep, from 0 to 100000.</p>	100
<b>ssl-server-session-state-timeout</b>	<p>Set the number of minutes to keep FortiGate to server SSL session states, from 1 to 14400.</p>	60
<b>ssl-server-session-state-type</b>	<p>Select the method to use to expire FortiGate to server SSL sessions:</p> <ul style="list-style-type: none"> <li><b>both:</b> expire SSL session states when either <code>ssl-client-session-state-max</code> or <code>ssl-client-session-state-timeout</code> is exceeded, regardless of which occurs first.</li> <li><b>count:</b> expire SSL session states when <code>ssl-client-session-state-max</code> is exceeded.</li> <li><b>disable:</b> expire all SSL session states.</li> <li><b>time:</b> expire SSL session states when <code>ssl-client-session-state-timeout</code> is exceeded.</li> </ul>	both
<b>uuid</b>	<p>Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.</p>	00000000-0000-0000-0000-000000000000

Option	Description	Default
<b>weblogic-server</b>	Enable or disable adding an HTTP header to indicate SSL offloading for a WebLogic server.	disable
<b>websphere-server</b>	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
<b>Name</b>	Enter a unique name for the policy. Each policy must have a unique name.
<b>Incoming Interface</b>	Click the field then select interfaces. Click the remove icon to remove interfaces.
<b>Source Address</b>	Select source addresses, address groups, virtual IPs, and virtual IP groups.
<b>Destination Address</b>	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
<b>Service</b>	Select services and service groups.
<b>L3/L4 Anomalies</b>	Configure the anomalies: <ul style="list-style-type: none"> <li>• <b>Logging:</b> Enable or disable logging for the anomaly. Anomalous traffic will be logged when the action is Block or Monitor.</li> <li>• <b>Action:</b> Select the action to take when the threshold is reached: <ul style="list-style-type: none"> <li>• <b>Disable:</b> Do not scan for the anomaly.</li> <li>• <b>Block:</b> Block the anomalous traffic.</li> <li>• <b>Monitor:</b> Allow the anomalous traffic but record a log message if logging is enabled.</li> </ul> </li> <li>• <b>Threshold:</b> Set the number of detected instances per minute that triggers</li> </ul>



Option	Description
	<p>the anomaly action.</p> <ul style="list-style-type: none"> <li><i>Quarantine</i>: Select which system quarantine to use for blocked anomalous traffic.</li> </ul> <p>See below for descriptions of each anomaly type.</p>
<b>Advanced Options</b> <b>&gt; comments</b>	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 <i>Comments</i> field.
<b>Change Note</b>	Add a description of the changes being made to the policy. This field is required.

### L3 Anomalies

Anomaly	Description	Default Threshold
<b>ip_src_session</b>	If the number of concurrent IP connections from one source IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
<b>ip_dst_session</b>	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
<b>tcp_syn_flood</b>	<p>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.</p> <p>An additional <i>Proxy</i> action is available for this anomaly type. The anomalous traffic will be buffered and scanned when the complete file is downloaded.</p> <p>The <i>Proxy</i> 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.</p>	2000 packets per second.
<b>tcp_port_scan</b>	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.
<b>tcp_src_session</b>	If the number of concurrent TCP connections from one source IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.

L4 Anomalies		
Anomaly	Description	Default Threshold
<b>tcp_dst_session</b>	If the number of concurrent TCP connections to one destination IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
<b>udp_flood</b>	If the UDP traffic to one destination IP address exceeds the configured threshold value, the action is executed.	2000 packets per second.
<b>udp_scan</b>	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.
<b>udp_src_session</b>	If the number of concurrent UDP connections from one source IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
<b>udp_dst_session</b>	If the number of concurrent UDP connections to one destination IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
<b>icmp_flood</b>	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.
<b>icmp_sweep</b>	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.
<b>icmp_src_session</b>	If the number of concurrent ICMP connections from one source IP address exceeds the configured threshold value, the action is executed.	300 concurrent sessions.
<b>icmp_dst_session</b>	If the number of concurrent ICMP connections to one destination IP address exceeds the configured threshold value, the action is executed.	1000 concurrent sessions.
<b>sctp_flood</b>	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.
<b>sctp_scan</b>	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.
<b>sctp_src_session</b>	If the number of concurrent SCTP connections from one source IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
<b>sctp_dst_session</b>	If the number of concurrent SCTP connections to one destination IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.

- 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:

- If using ADOMs, ensure that you are in the correct ADOM.
- Go to *Policy & Objects > Policy Packages*.
- In the tree menu for the policy package, click *IPv4 Interface Policy* or *IPv6 Interface Policy*.
- Click *Create New*.
- Enter the following information:

Option	Description
<b>Source &gt; Interface</b>	Select the source interface.
<b>Source &gt; Address</b>	Select source addresses, address groups, virtual IPs, and virtual IP groups.
<b>Destination &gt; Address</b>	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
<b>Service</b>	Select services and service groups.
<b>Log Traffic</b>	Select the traffic to log: <i>No Log</i> , <i>Log Security Events</i> , or <i>Log All Sessions</i> .
<b>AntiVirus Profile</b>	Enable or disable, and then select, the antivirus profile.
<b>Web Filter Profile</b>	Enable or disable, and then select, the web filter profile.
<b>Application Control</b>	Enable or disable, and then select, the application control profile.
<b>IPS Profile</b>	Enable or disable, and then select the IPS profile.
<b>Email Filter Profile</b>	Enable or disable, and then select, the email filter profile.
<b>Advanced Options</b>	Configure advanced options, see <a href="#">Advanced options</a> below. For more information on advanced option, see the <a href="#">FortiOS CLI Reference</a> .
<b>Change Note</b>	Add a description of the changes being made to the policy. This field is required.

- 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
<b>address-type</b>	Select	none
<b>comments</b>	Add a description of the policy, such as its purpose, or the changes that have been made to it.	none
<b>dlp-profile</b>	Select an existing data leak prevention (DLP) profile.	none
<b>dlp-profile-status</b>	Enable or disable DLP.	disable
<b>dsri</b>	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
<b>Name</b>	Enter a unique name for the policy. Each policy must have a unique name.
<b>Incoming Interface</b>	Click the field then select interfaces. Click the remove icon to remove interfaces. New objects can be created by clicking the <i>Create New</i> icon in the <i>Object Selector</i> frame. See <a href="#">Create a new object on page 403</a> for more information.

Option	Description
<b>Outgoing Interface</b>	Select outgoing interfaces in the same manner as <i>Incoming Interface</i> .
<b>Source Address</b>	Select the source firewall address.
<b>Destination Address</b>	Select the destination multicast addresses.
<b>Action</b>	Select an action for the policy to take: <i>ACCEPT</i> or <i>DENY</i> .
<b>Source NAT</b>	Enable or disable source NAT, then enter the source NAT IP Address. This option is only available when <i>Action</i> is <i>Accept</i> .
<b>Destination NAT</b>	Enter the destination NAT IP address.
<b>Protocol Option</b>	Select a protocol option: <i>ANY</i> , <i>ICMP</i> , <i>IGMP</i> , <i>TCP</i> , <i>UDP</i> , <i>OSFP</i> , or <i>Others</i> .
<b>Port Range</b>	Set the port range. This option is only available when <i>Protocol Option</i> is <i>TCP</i> or <i>UDP</i> .
<b>Protocol Number</b>	Enter the protocol number, from 1 to 256. This option is only available when <i>Protocol Option</i> is <i>Others</i> .
<b>Log Traffic</b>	Enable or disable traffic logging.
<b>Advanced Options</b>	Configure advanced options, see <a href="#">Advanced options</a> below. For more information on advanced option, see the <a href="#">FortiOS CLI Reference</a> .
<b>Change Note</b>	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
<b>auto-asic-offload</b>	Enable or disable policy traffic ASIC offloading.	enable
<b>comments</b>	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 <i>Comments</i> field.	none
<b>uuid</b>	Enter the universally unique identifier (UUID). This value is automatically assigned but can be manually reset.	00000000-0000-0000-0000-000000000000
<b>traffic-shaper</b>	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
<b>Interface</b>	Select the interface.
<b>Source Address</b>	Select source addresses, address groups, virtual IPs, and virtual IP groups.
<b>Destination Address</b>	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
<b>Service</b>	Select services and service groups.
<b>Schedule</b>	Select a one-time schedule, recurring schedule, or schedule group.
<b>Action</b>	Select an action for the policy to take: <i>DENY</i> or <i>ACCEPT</i> .
<b>HA Management Interface Only</b>	Enable to dedicate the interface as an HA management interface. This option is only available for IPv4 policies.
<b>Change Note</b>	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
<b>IP Version</b>	Select the IP address version: <i>IPv4</i> or <i>IPv6</i> .
<b>Name</b>	Enter a unique name for the policy. Each policy must have a unique name.
<b>Status</b>	<i>Enable</i> or <i>Disable</i> this policy.
<b>Comments</b>	Add a description of the policy, such as its purpose, or the changes that have been made to it.
<b>If Traffic Matches:</b>	
<b>Source Internet Service</b>	<i>Enable</i> or <i>disable</i> source internet service, then select services. This option is only available when the <i>IP Version</i> is <i>IPv4</i> .
<b>Source Address</b>	Select source addresses, address groups, virtual IPs, and virtual IP groups. This option is only available when <i>Source Internet Service</i> is off.
<b>Source User</b>	Select source users. This option is only available when <i>Source Internet Service</i> is off.
<b>Source User Group</b>	Select source user groups. This option is only available when <i>Source Internet Service</i> is off.
<b>Destination Internet Service</b>	Turn destination internet service on or off, then select services.
<b>Destination Address</b>	Select destination addresses, address groups, virtual IPs, and virtual IP groups. This option is only available when <i>Destination Internet Service</i> is off.
<b>Schedule</b>	Select a one-time schedule, recurring schedule, or schedule group.
<b>Service</b>	Select services and service groups. This option is only available when <i>Destination Internet Service</i> is off.
<b>Application</b>	Select applications.
<b>Application Category</b>	Select application categories.

Option	Description
<b>Application Group</b>	Select application groups.
<b>URL Category</b>	Select URL categories.
<b>Type of Service</b>	Specify the type of service (ToS) hexadecimal value.
<b>Type of Service Mask</b>	Specify the hexadecimal mask to be matched against the ToS.
<b>Then:</b>	
<b>Action</b>	Select the action to take if traffic matches: <i>Apply Shaper</i> or <i>Assign Group</i> .
<b>Outgoing Interface</b>	Select outgoing interfaces.
<b>Shared Shaper</b>	Select a shared traffic shaper. This option is only available when <i>Action</i> is set to <i>Apply Shaper</i> .
<b>Reverse Shaper</b>	Select a reverse traffic shaper. This option is only available when <i>Action</i> is set to <i>Apply Shaper</i> .
<b>Per-IP Shaper</b>	Select a per-IP traffic shaper. This option is only available when <i>Action</i> is set to <i>Apply Shaper</i> .
<b>Traffic Shaping Class ID</b>	Select the shaping class to which this traffic should be assigned. This option is only available when <i>Action</i> is set to <i>Assign Group</i> .
<b>Differentiated Services</b>	Enable or disable application of a differentiated services tag to a packet's DiffServ value, then enter the tag.
<b>Differentiated Services Reverse</b>	Enable or disable application of a differentiated services tag to a packet's reverse DiffServ value, then enter the tag.
<b>Advanced Options</b>	Configure advanced options, see <a href="#">Advanced options</a> below. For more information on advanced option, see the <a href="#">FortiOS CLI Reference</a> .
<b>Change Note</b>	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
<b>srcintf</b>	Select one or more incoming interfaces.	none
<b>tos-negate</b>	Enable or disable negation of the ToS value.	disable
<b>uuid</b>	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
<b>Name</b>	Enter a unique name for the policy. Each policy must have a unique name.
<b>Source Address</b>	Select source addresses, address groups, virtual IPs, and virtual IP groups.
<b>Protocol</b>	Select the protocol this rule applies to.
<b>Authentication Scheme</b>	Select or create a new authentication scheme. For more information on authentication schemes, see the <a href="#">FortiOS Administration Guide</a> .
<b>IP-based Authentication</b>	Enable or disable IP-based authentication.
<b>SSO Authentication Scheme</b>	Select or create a new authentication scheme for single sign-on.
<b>Comments</b>	Add a description of the policy, such as its purpose, or the changes that have been made to it.
<b>Advanced Options</b>	Configure advanced options, see <a href="#">Advanced options</a> below. For more information on advanced option, see the <a href="#">FortiOS CLI Reference</a> .
<b>Change Note</b>	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
<b>dstaddr</b>	Select an IPv4 destination address. Required for web proxy authentication.	none
<b>dstaddr6</b>	Select an IPv6 destination address. Required for web proxy authentication.	none
<b>srcintf</b>	Select the incoming (ingress) interface.	none
<b>transaction-based</b>	Enable or disable transaction-based authentication.	disable
<b>transaction-based</b>	Enable or disable web authentication cookies.	disable
<b>web-portal</b>	Enable or disable the web portal for proxy transparent policy	disable

**Hyperscale policies**

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:

<b>Name</b>	Enter a name for the policy.
<b>Incoming Interface</b>	Select the incoming interface.
<b>Outgoing Interface</b>	Select the outgoing interface.
<b>Source Address</b>	Select the source address.
<b>Destination Address</b>	Select the destination address.
<b>Service</b>	Select services and service groups.
<b>Action</b>	Select an action for the policy to take: <i>ACCEPT</i> or <i>DENY</i> .
<b>Comments</b>	Optionally, enter comments about the policy.
<b>Advanced Options</b>	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
<b>Name</b>	Enter a unique name for the policy. Each policy must have a unique name. This field is required.
<b>Status</b>	Set the policy to <i>Enabled</i> or <i>Disabled</i> .
<b>FortiLink Interface</b>	Use the search field to find and select the FortiLink interface.
<b>FortiSwitch Groups</b>	Select <i>All</i> or <i>Specify</i> the FortiSwitch groups.
<b>Description</b>	Add a description of the policy, such as its purpose, or the changes that have been made to it.
<b>Device Patterns</b>	
<b>Category</b>	Select <i>Device</i> , <i>User</i> , or <i>EMS Tag</i> . For <i>Device</i> pattern fields, you can use the wildcard * character when entering the value to be matched.
<b>MAC Address</b>	Enable or disable matching a MAC address, then enter a MAC address. Only available if <i>Category</i> is <i>Device</i> .
<b>Hardware Vendor</b>	Enable or disable matching a hardware vendor, then enter a hardware vendor name. Only available if <i>Category</i> is <i>Device</i> .
<b>Device Family</b>	Enable or disable matching a device family, then enter a device family name. Only available if <i>Category</i> is <i>Device</i> .
<b>Type</b>	Enable or disable matching a device type, then enter a device type. Only available if <i>Category</i> is <i>Device</i> .
<b>Operating System</b>	Enable or disable matching an operating system, then enter an operating system. Only available if <i>Category</i> is <i>Device</i> .
<b>User group</b>	Select a user group. Only available if <i>Category</i> is <i>User</i> .
<b>FortiClient EMS Tag</b>	Select a FortiClient EMS tag. Only available if <i>Category</i> is <i>EMS Tag</i> .
<b>Switch Controller Action</b>	
<b>Assign VLAN</b>	Enable to select a VLAN interface for the switch controller action.
<b>Bounce Port</b>	Enable or disable the bounce port.
<b>Assign device to dynamic address</b>	Enable to use a dynamic firewall address for matching a device, then select the address. For more information, see <a href="#">To create a dynamic firewall address for the NAC policy</a> .

Option	Description
<b>Wireless Controller Action</b>	
<b>Assign VLAN</b>	Enable to select a VLAN interface for the wireless controller action.
<b>Revision</b>	
<b>Change Note</b>	Add a description of the changes being made to the policy. This field is required.

- 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:

- Go to *Policy & Objects > Object Configurations > Firewall Objects > Addresses*.
- Click *Create New*.
- From the *Type* dropdown, select *Dynamic*.
- For the *Sub Type* field, select *Switch Controller NAC Policy Tag*.
- From the *Interface* dropdown, select the FortiLink interface.
- Configure the other options, as needed.
- 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 752](#).

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:

- If using ADOMs, ensure that you are in the correct ADOM.
- Go to *Policy & Objects > Policy Packages*.
- In the tree menu for the policy package in which you will be creating the new policy, select *FortiProxy Policy*.

4. Click *Create New*.

**Create New Policy**

Type: Transparent

Name:

Incoming Interface: any

Outgoing Interface: any

Source: all

Destination: all

Schedule: always

Service: +

Action: Accept Deny Redirect Isolate

Log Violation Traffic: ☒

Comments:

Enable Policy Matching Pass Through: ☐

[Advanced Options >](#)

**Revision**

Change Note:

Revision History

Revisor	Changed by	Date/Time	Action	Change Note
No record found.				

OK Cancel

## 5. Enter the following information:

<b>Type</b>	Select the policy type from <i>Explicit</i> , <i>Transparent</i> , <i>FTP</i> , <i>SSH Tunnel</i> , <i>SSH Proxy</i> , and <i>Wanopt</i> .
<b>Name</b>	Enter a name for the policy.
<b>Incoming Interface</b>	Select the incoming interface(s) from the object selector pane.
<b>Outgoing Interface</b>	Select the outgoing interface(s) from the object selector pane.
<b>Source</b>	Select the source.
<b>Destination</b>	Select the destination.
<b>Schedule</b>	Select the schedule.
<b>Service</b>	Click the plus icon to add services to the policy, and then add services from the service selector pane.
<b>Action</b>	Select a policy action. Available actions include <i>Accept</i> , <i>Deny</i> , <i>Redirect</i> , and <i>Isolate</i> .  Depending on which option is selected, additional settings are available. For more information, see the FortiProxy Administration Guide on the <a href="#">Fortinet Document Library</a> .
<b>Enable Policy Matching Pass Through</b>	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 752](#).

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*.

Create New PAC Policy

ID

Status

Original Address

Source Address IPv6

Destination Address

PAC File Name

Comments

PAC File Content

Revision

Change Note

Revision History

0

Enable

Disable

all

+

all

proxy.pac

0/1023

0/262144

0/1023

View Diff

Column Settings

Revisor

Changed by

Date/Time

Action

Change Note

No record found.

OK

Cancel

6. Enter the following information:

<b>ID</b>	Enter a policy ID or leave the field as the default to automatically assign a policy ID.
<b>Status</b>	<i>Enable</i> or <i>Disable</i> the policy.
<b>Original Address</b>	Select the original address.
<b>Source Address IPv6</b>	Optionally, provide the source IPv6 address.
<b>Destination Address</b>	Select the destination address.

<b>PAC File Name</b>	The name of the PAC file.
<b>Comments</b>	Optionally, provide comments.
<b>PAC File Content</b>	Enter the PAC file content. For more information, see the FortiProxy Administration Guide on the <a href="#">Fortinet Document Library</a> .

- 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.

## 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 policies, 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 307](#).



You 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 information:

- [Creating Policy Blocks on page 398](#)
- [Adding policies to a Policy Block on page 399](#)
- [Appending a Policy Block to a Policy Package on page 400](#)
- [Using Policy Blocks versus Global Policy Packages on page 401](#)
- [Role-based access control for Policy Blocks on page 402](#)

## Creating Policy Blocks

### To create a new Policy Block:

- Ensure that you are in the correct ADOM.
- Go to *Policy & Objects*.
- 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*.



Create New Policy Block

Name

Central NAT

☐

NGFW Mode ⓘ

Profile-based

Policy-based

Policy Offload Level

Disable

OK

Cancel

4. Configure the following details, then click **OK** to create the Policy Block.

<b>Name</b>	Enter a name for the new Policy Block.
<b>Central NAT</b>	<p>Toggle <i>Central NAT</i> to <i>ON</i> to enable <i>Central SNAT</i> and <i>Central DNAT</i> policy types.</p> <p>This option is not available in the Global Database ADOM.</p>
<b>NGFW Mode</b>	<p>Select the NGFW mode, <i>Profile-based</i> (default) or <i>Policy-based</i>.</p> <p>This option is not available in the Global Database ADOM.</p>
<b>Policy Offload Level</b>	Select the policy offload level. Available options include <i>Disable</i> , <i>Default</i> , <i>DoS Offload</i> , or <i>Full Offload</i> .

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 329](#) 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

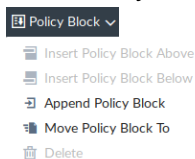
Once a Policy Block is created, it can be appended to a Policy Package. After appending the Policy Block to a Policy Package, assigning installation targets and installing the Policy Package to the installation targets, all the policies in the Policy Block are installed to the target.



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*.

Insert Policy Block





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.

---

## 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 767](#).

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 402](#)

## 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 329](#) and [Creating Policy Blocks on page 398](#).

## 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 843](#) and [Permissions on page 840](#).

## 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.

Many objects now include the option to enable dynamic mapping. You can create new dynamic maps. When this feature is enabled, a table is displayed which lists the dynamic mapping information. You can also choose to add the object to groups, when available, and add tags.

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.

Dynamic objects are used to map a single logical object to a unique definition per device. Addresses, interfaces, virtual IPs, and an IP pool can all be addressed dynamically.



Not all policy and object options are enabled by default. See [Feature visibility on page 309](#).

---

Objects and dynamic objects are managed under the *Object Configurations* tree menu in *Policy & Objects* (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 the *Policy Packages* tree menu 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 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 drop objects on page 331](#).



On the *Policy & Objects > 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.



FortiManager shows the last opened object for easy navigation. After opening an object, log off and log on in the same browser. Navigate to *Policy and Objects > Object Configurations* in the same ADOM. The last opened object is shown.

## Create a new object

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 > Object Configurations*.
3. Select the object type that you will be creating. For example, view the 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.
4. From the *Create New* menu, select the type of address. In this example, *Address* was selected. The *Create New Address* pane opens.

Name	Type
none	Firewall Address
login.microsoftonline.co	Firewall Address
login.microsoft.com	Firewall Address
login.windows.net	Firewall Address
gmail.com	Firewall Address
wildcard.google.com	Firewall Address
wildcard.dropbox.com	Firewall Address
SSLVPN_TUNNEL_ADD	Firewall Address
all	Firewall Address
FIREWALL_AUTH_POR	Firewall Address
FABRIC_DEVICE	Firewall Address
metadata-server	Firewall Address
INTRA_VPN	Firewall Address
LOOPBACK	Firewall Address
entcore.fortidemo.fortin	Firewall Address
Management-Gateway	Firewall Address
AWS_Quarantined	Firewall Address
AWS-us-west-2a	Firewall Address
AWS-us-east-1b	Firewall Address
AWS_private_cloud_ser	Firewall Address
HQ_ISFW	Firewall Address
Finance Network	Firewall Address
IT Network	Firewall Address

**Create New Firewall Address**

Address Name:

Color:

Type:

IP/Netmask:  Q Resolve from name

Interface:

Static Route Configuration: ☐

Comments:

Add To Groups:

**Advanced Options >**

Per-Device Mapping: ☐

**Revision**

Change Note:

**OK** **Cancel**



You can select to add the object to groups and enable dynamic mapping. These options are not available for all objects.

5. 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:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
3. Select the object type that you will be creating. For example, view the interface by going to *Normalized Interface > Normalized Interface*.

The interface list is displayed in the content pane. The available interfaces are selectable on the content pane toolbar.

4. In the content pane, click *Create New*.  
The *Create New Normalized Interface* pane opens.

Create New Normalized Interface

Name

test

Description

0/4096

Color

Per-Platform Mapping

OFF

Per-Device Mapping

OFF

OK

Cancel

5. Select or specify the values for the following fields:
  - Name - specify a name for the object.
  - Description - enter a brief description.
  - Color - click the black port to display the color options, and select a color for this object.
  - Default Mapping - select the check box to configure the default mapping for this object. See [Map a dynamic ADOM object on page 417](#)
  - Per-Platform mapping - switch the slider to *ON* for mapping this interface to a platform.
  - Per-Device Mapping - switch the slider to *ON* for mapping this interface to a FortiGate device. See [Interface mapping on page 429](#)
6. 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 > Object Configurations* .
3. Go to *Firewall Objects> Addresses*.

The address list is displayed in the content pane. The available interfaces are selectable on the content pane toolbar.

4. From the *Create New* menu, select *IPv6 Address Template*. The *IPv6 Address Template* pane opens.

Create New IPv6 Address Template

Name

IPv6 Address Prefix

Subnet Segments ⓘ

[+ Create New](#) [✎ Edit Segment](#) [⚙ Edit Values for Segment](#) [🗑 Delete](#)

<input type="checkbox"/> Segment Name	Bits	Exclusive	Defined Values
<input type="checkbox"/> country	4	Disable	
<input type="checkbox"/> state	4	Disable	
<input type="checkbox"/> city	4	Disable	
<input type="checkbox"/> site	4	Disable	
<input type="checkbox"/> lan	4	Disable	
<input type="checkbox"/> vlan	4	Disable	

Revision

Change Note \*

Revision History

[↶ Revert](#) [📄 View Diff](#) [⚙ Column Settings](#)

<input type="checkbox"/> Revision	Changed by	Date/Time	Entry Key	Entry name	Action	Change Note
No record found.						

5. Select or specify the values for the following and click *OK*:

<b>Name</b>	Specify the name for the IPv6 address template.
<b>IPv6 Address Prefix</b>	Specify a prefix for the IPv6 address.
<b>Subnet Segments</b>	<p>There can only be six subnet segments. These can either be predefined or user created subnet segments.</p> <p>Select one of the following predefined subnet segments:</p> <ul style="list-style-type: none"> <li>country</li> <li>state</li> <li>city</li> <li>site</li> <li>lan</li> <li>vlan</li> </ul>
<b>Create New</b>	To create a new segment, you must delete one of the existing predefined segments if you already have six subnet segments. Click <i>Create New</i> . Specify the <i>Segment Name</i> , <i>Bits</i> , and toggle <i>Exclusive</i> to <i>Enable</i> or <i>Disable</i> . Click <i>OK</i> .
<b>Edit Segment</b>	Click <i>Edit Segment</i> . Edit the <i>Segment Name</i> , <i>Bits</i> , and toggle <i>Exclusive</i> to <i>Enable</i> or <i>Disable</i> . Click <i>OK</i> .
<b>Edit Values for Segment</b>	Click <i>Edit values for Segment</i> . Click + to add a row. Specify the <i>Name</i> , select the <i>Format</i> , and specify the <i>Value</i> . Click <i>OK</i> .
<b>Delete</b>	Select one or more subnet segments and click <i>Delete</i> .





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.

---

## Promote an Object to Global Database

Objects from an ADOM can be promoted to the Global Database for reuse.

---



Existing objects or newly created 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 > Object Configurations* .
3. Select the object type that you want to promote. For example, view the interface by going to *Normalized Interface > Normalized Interface*.

The interface list is displayed in the content pane. The available interfaces are selectable on the content pane toolbar.

4. Right-click the object and select *Promote to Global*.
5. 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.
6. Click *Promote*.  
The object is now promoted to the Global Database.

## 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.

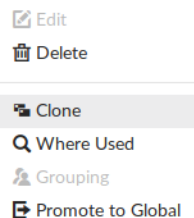
You can delete default normalized interfaces and create new normalized interfaces. You can also delete per-platform mappings in a default normalized interface.

Zones are created using *Device Manager*, and you can map zones to normalized interfaces. See also [Device zones on page 148](#).

You can also select normalized interfaces when you create virtual wire pairs.

This section contains the following topics:

- [Viewing normalized interfaces on page 408](#)
- [Viewing normalized interfaces mapped to devices on page 409](#)
- [Viewing where normalized interfaces are used on page 410](#)
- [Editing per-platform mapping rules on page 411](#)
- [Deleting per-platform mapping rules on page 412](#)
- [Deleting default normalized interfaces on page 412](#)
- [Creating normalized interfaces on page 413](#)
- [Creating virtual wire pairs on page 416](#)



## 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 > Object Configurations > Normalized Interface > Normalized Interface* pane.  
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.

+ Create New Edit Delete Collapse All More ▾ Column Settings ▾					View ▾		Q
<input type="checkbox"/>	Normalized Interface	Mapping Rule	Mapped Interface/Zone	Description	Created Time	Last Modified	Revision History
<input checked="" type="checkbox"/>	any						
<input type="checkbox"/>	tslvpn_tun_intf						
<input type="checkbox"/>	FortiDEMO				2021-04-14 09:39:10		1
<input type="checkbox"/>	VPN_Zone				2021-04-14 09:39:11		1
<input type="checkbox"/>	WAN_Zone				2021-04-14 09:39:11		1
<input type="checkbox"/>	a			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>	b			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>	dmz			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>		Per-platform (FortiGate-60E)	dmz				
<input type="checkbox"/>		Per-platform (FortiGate-60E-DSL)	dmz				
<input type="checkbox"/>		Per-platform (FortiGate-60E-DSL1)	dmz				
<input type="checkbox"/>		Per-platform (FortiGate-60F)	dmz				
<input type="checkbox"/>		Per-platform (FortiGate-61E)	dmz				
<input type="checkbox"/>		Per-platform (FortiGate-61F)	dmz				
<input type="checkbox"/>		Per-platform (FortiGate-80E)	dmz				
<input type="checkbox"/>		Per-platform (FortiGate-80E-POE)	dmz				
<input type="checkbox"/>		Per-platform (FortiGate-81E)	dmz				
<input type="checkbox"/>		Per-platform (FortiGate-81E-POE)	dmz				
<input type="checkbox"/>		Per-platform (FortiGate-90E)	dmz				
<input type="checkbox"/>		Per-platform (FortiGate-91E)	dmz				
<input type="checkbox"/>		Per-platform (FortiGate-100E)	dmz				
<input type="checkbox"/>		Per-platform (FortiGate-100EF)	dmz				
<input type="checkbox"/>		Per-platform (FortiGate-100F)	dmz				

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

For each managed FortiGate device, you can view the number of normalized interfaces mapped to it.

**To view normalized interfaces mapped to devices:**

1. Go to *Policy & Objects > Object Configurations > Normalized Interface > Normalized Interface*.
2. From the *More* menu, select *Normalized Interface Preview*.

Policy Package

Install

ADOM Revisions

Tools

ADOM: Test70

administrator

Create New

Edit

Delete

Expand All

More

Column Settings

View

<input type="checkbox"/>	Normalized Interface	Mapping Rule	Interface/Zone	Description	Created Time	Last Modified	Revision History
<input checked="" type="checkbox"/>	any						
<input type="checkbox"/>	sslvpn_tun_intf						
<input type="checkbox"/>	FortiDEMO				2021-04-14 09:39:10		1
<input type="checkbox"/>	VPN_Zone				2021-04-14 09:39:11		1
<input type="checkbox"/>	WAN_Zone				2021-04-14 09:39:11		1
<input type="checkbox"/>	a			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>	b			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>	dmz			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>	dmz1			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>	dmz2			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>	dsl			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>	external			added by creating adom	2021-04-14 09:24:30		
<input type="checkbox"/>	fortiblink				2021-04-14 09:39:12		1
<input type="checkbox"/>	ha			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>	ha1			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>	ha2			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>	internal			added by creating adom	2021-04-14 09:24:30		
<input type="checkbox"/>	mgmt			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>	mgmt1			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>	mgmt2			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>	modem			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>	port1			added by creating adom	2021-04-14 09:24:19		
<input type="checkbox"/>	port10			added by creating adom	2021-04-14 09:24:19		

Clone

Where Used

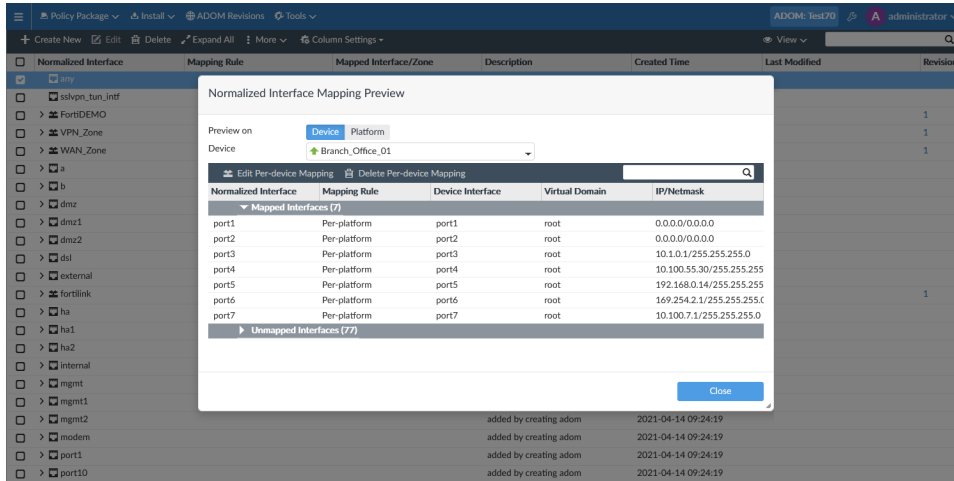
Promote to Global

Change Color

Normalized Interface Preview

The *Normalized Interface Mapping Preview* window is displayed.

- From the drop-down list, select a device.  
The mapping preview for the selected device is displayed.



Scroll to the bottom to view unmapped interfaces.

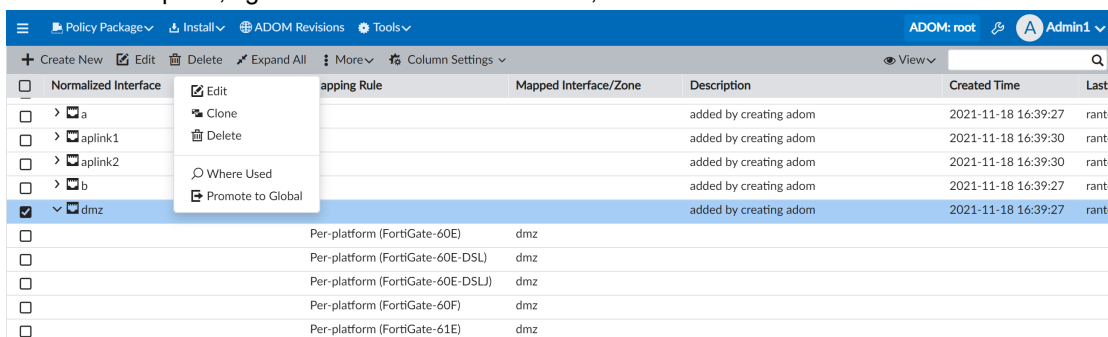
- (Optional) Select a mapping, and click *Edit Per-device Mapping* or *Delete Per-device Mapping*.
- Click *Close*.

## Viewing where normalized interfaces are used

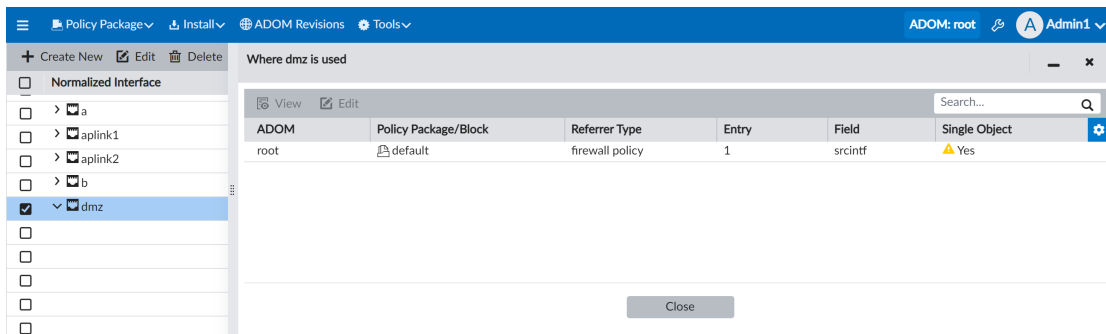
You can view what policy packages use a normalized interface.

**To view where normalized interfaces are used:**

- Go to *Policy & Objects > Object Configurations > Normalized Interface > Normalized Interface*.
- 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*.

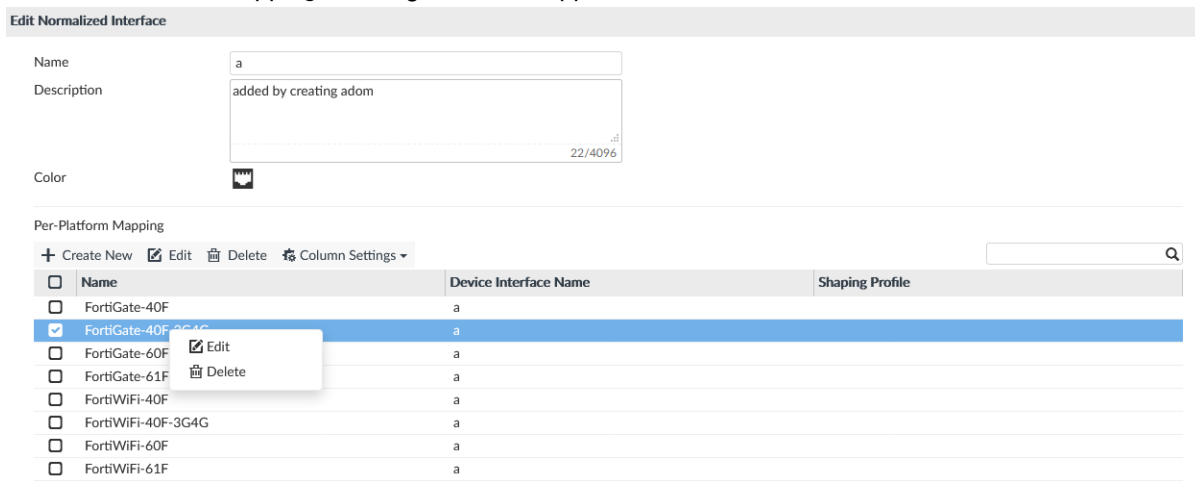
## Editing per-platform mapping rules

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 edit per-platform mapping rules:

1. Go to *Policy & Objects > Object Configurations > Normalized Interface > 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*.



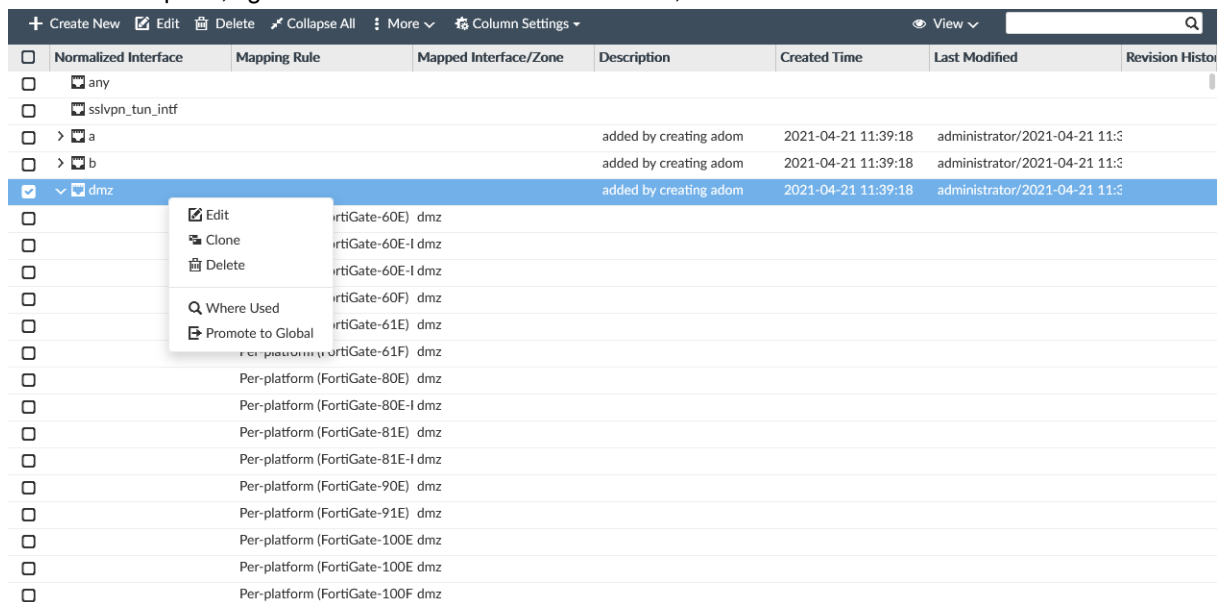
4. Edit the options, and click *OK*.  
The mapping rule is saved.
5. Click *OK*.  
The normalized interface is saved.

## 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 > Object Configurations > Normalized Interface > Normalized Interface*.
2. In the content pane, right-click a default normalized interface, and select *Edit*.



Normalized Interface	Mapping Rule	Mapped Interface/Zone	Description	Created Time	Last Modified	Revision History
<input type="checkbox"/> any						
<input type="checkbox"/> sslvpn_tun_intf						
<input type="checkbox"/> > a			added by creating adom	2021-04-21 11:39:18	administrator/2021-04-21 11:3	
<input type="checkbox"/> > b			added by creating adom	2021-04-21 11:39:18	administrator/2021-04-21 11:3	
<input checked="" type="checkbox"/> > dmz			added by creating adom	2021-04-21 11:39:18	administrator/2021-04-21 11:3	
<input type="checkbox"/>		FortiGate-60E dmz				
<input type="checkbox"/>		FortiGate-60E-I dmz				
<input type="checkbox"/>		FortiGate-60E-I dmz				
<input type="checkbox"/>		FortiGate-60F dmz				
<input type="checkbox"/>		FortiGate-61E dmz				
<input type="checkbox"/>		Per-platform (FortiGate-61F) dmz				
<input type="checkbox"/>		Per-platform (FortiGate-80E) dmz				
<input type="checkbox"/>		Per-platform (FortiGate-80E-I dmz				
<input type="checkbox"/>		Per-platform (FortiGate-81E) dmz				
<input type="checkbox"/>		Per-platform (FortiGate-81E-I dmz				
<input type="checkbox"/>		Per-platform (FortiGate-90E) dmz				
<input type="checkbox"/>		Per-platform (FortiGate-91E) dmz				
<input type="checkbox"/>		Per-platform (FortiGate-100E dmz				
<input type="checkbox"/>		Per-platform (FortiGate-100E dmz				
<input type="checkbox"/>		Per-platform (FortiGate-100F dmz				

The *Edit Normalized Interface* pane appears.

3. In the *Per-Platform Mapping* table, select a mapped device, and click *Delete*.
4. Click *OK*.

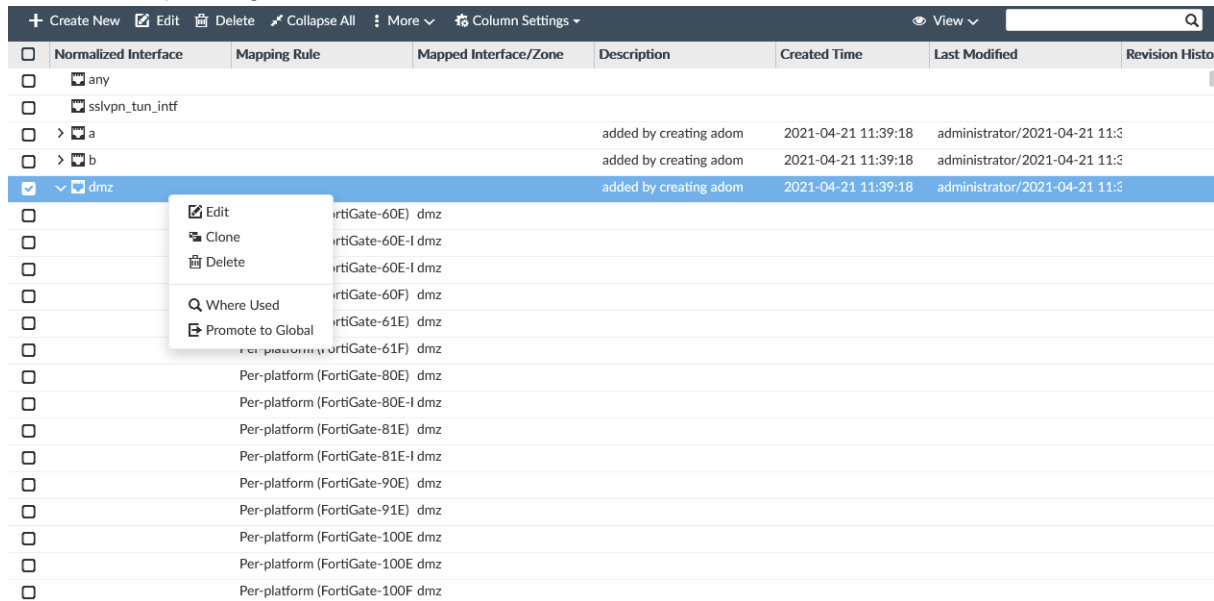
The normalized interface is saved.

## 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 > Object Configurations > Normalized Interface > 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:**

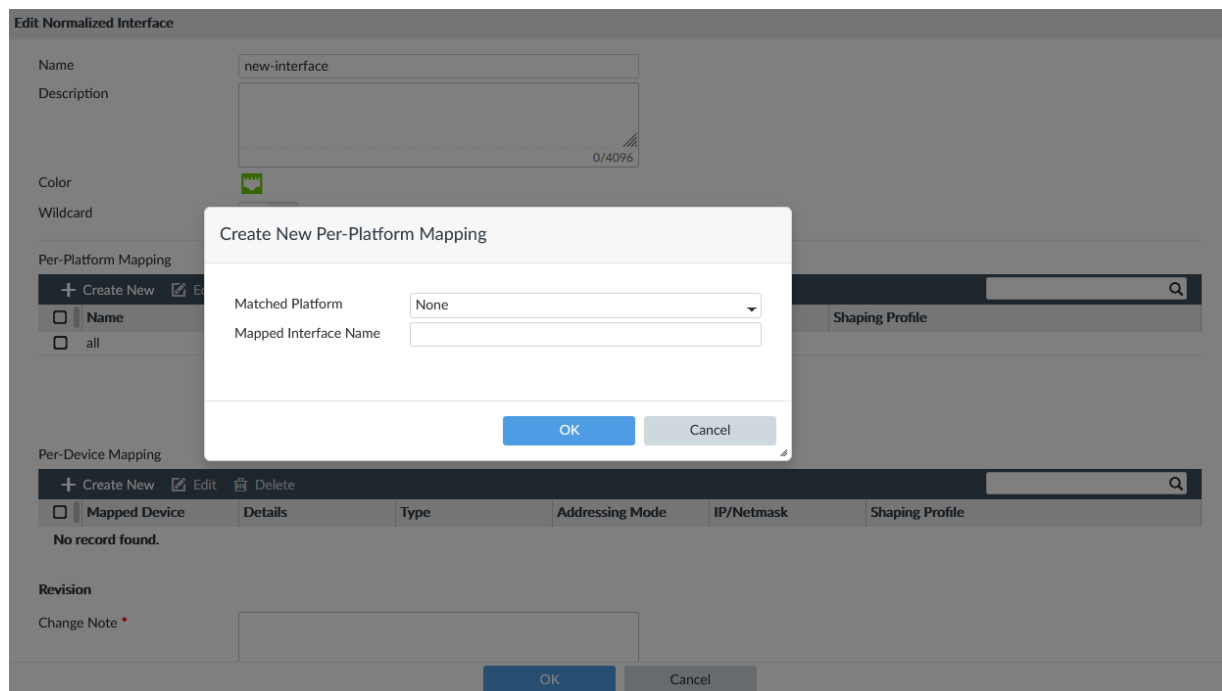
1. Go to *Policy & Objects > Object Configurations > Normalized Interface > Normalized Interface*.
2. In the content pane, right-click the default per-platform normalized interface, and select *Edit*.  
The *Edit Normalized Interface* page appears.
3. In the *Per-Platform Mapping* table, right-click the default per-platform mapping rule, and select *Delete*.
4. Click *OK*.

**To create normalized interfaces for zones:**

1. Go to *Policy & Objects > Object Configurations > Normalized Interface > 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. Toggle *Per-Platform Mapping* to *ON*.  
The *Per-Platform Mapping* table is displayed.

- b. Click *Create New*.

The Create new Per-Platform Mapping dialog box is displayed.



- c. In the *Model* list, select the model for which you created the zone.

- d. In the *Device Interface Name* box, type the name of the interface.

- e. Click *OK*.

5. Add a per-device mapping.

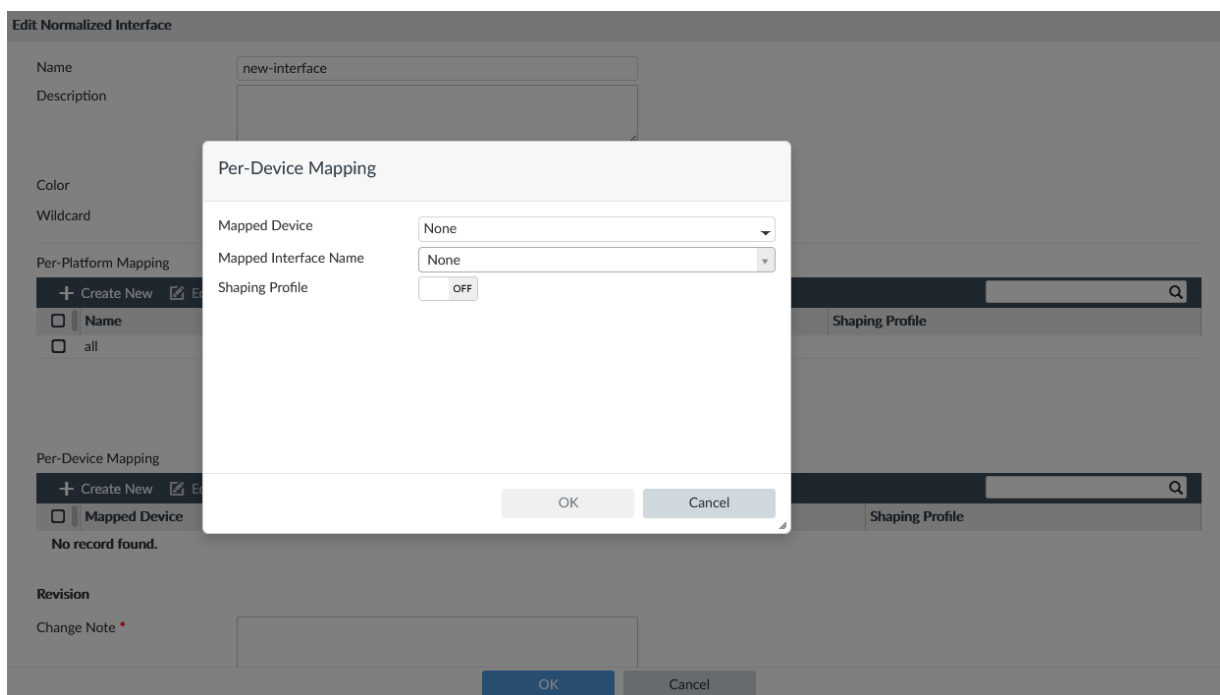
- a. Toggle *Per-Device Mapping* to *ON*.

The *Per-Device Mapping* table is displayed.

- b. Click *Create New*.

The *Create new Per-Device Mapping* dialog box is displayed.





- c. In the *Mapped Device* list, select the model for which you created the zone.
  - d. In the *Device Interface* list, select the zone.
  - e. Click *OK*.
6. Click *OK*.


#### To create a wildcard interface:

1. Go to *Policy & Objects > Object Configurations > Normalized Interface > 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.

**Create New Normalized Interface**

Name:

Description:

Color: 

Wildcard: ☐

Wildcard Interface:

**Revision**

Change Note:

Revision History

Reversion	Changed by	Date/Time	Entry Key	Entry name	Action	Change Note
No record found.						

OK Cancel



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. Go to *Policy & Objects > Object Configurations > Normalized Interface > Virtual Wire Pair*.
2. Click *Create New*.  
The *Create New Virtual Wire Pair* pane is displayed.
3. In the *Name* box, type a name for the virtual wire pair.
4. Click the *Interface Members* box.  
The list of normalized interfaces is displayed.

5. Select one or more normalized interfaces, and click OK.
6. Complete the remaining options, and click OK.

## Map a dynamic ADOM object

The devices and VDOMs to which a global object is mapped can also be viewed from the object list. You can add an object to groups and enable dynamic mapping. These options are not available for all objects.

When the *Dynamic Mapping* option is available, select *Create New* to configure the dynamic mapping.

To configure a dynamic mapping via a CLI script, the configuration for the mapping must be defined in the dynamic object under the *config dynamic\_mapping* sub-tree. The CLI script must be run on a policy package instead of the device database. For information on running CLI scripts, see [Scripts on page 168](#)



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.

## Examples:

### 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
  ...
  config dynamic_mapping
    edit "FW60CA3911000089"-"root"
      set local-intf internal
      set intrazone-deny disable
    next
  end
end
```

## Map a dynamic device object

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 > Object Configurations*.
3. Go to *Tools > Feature Visibility*.
4. Select *Dynamic Object* and click *OK*.

The following device objects are available:

- [Create a Local Certificate on page 418](#)
- [Create a VPN Tunnel on page 419](#)



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 Local Certificate

Create a local certificate to sync with devices using per-device mapping.

**To create a local certificate:**

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
3. Go to *Dynamic Object > Local Certificate*.
4. Click *Create New*. The *Create New Dynamic Local Certificate* pane opens.

Create New Dynamic Local Certificate

Name

Description

Per-Device Mapping ☒ ON

+ Create New ☒ Edit ☐ Delete ☐ Column Settings

<input type="checkbox"/> Name	VDOM	Details
-------------------------------	------	---------

OK Cancel

5. Select or specify the values for the following and click *OK*:

<b>Name</b>	Specify the name for the Dynamic Local Certificate.
<b>Description</b>	Specify a description.
<b>Per-Device Mapping</b>	Toggle Per-Device Mapping to <i>ON</i> . Click <i>Create New</i> . Select the <i>Mapped Device</i> and <i>VPN Local Certificate</i> . Click <i>OK</i> .

**Create a 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 > Object Configurations*.
3. Go to *Dynamic Object > VPN Tunnel*.
4. Click *Create New*. The *Create New Dynamic VPN Tunnel* pane opens.

Create New Dynamic VPN Tunnel

Name

Description

Per-Device Mapping

+ Create New

Edit

Delete

Column Settings

OK

Q

Name

VDOM

Details

OK

Cancel

5. Select or specify the values for the following and click *OK*:

<b>Name</b>	Specify the name for the Dynamic VPN Tunnel.
<b>Description</b>	Specify a description.
<b>Per-Device Mapping</b>	Toggle Per-Device Mapping to <i>ON</i> . Click <i>Create New</i> . Select the <i>Mapped Device</i> and <i>VPN Tunnel</i> . Click <i>OK</i> .

Map a dynamic device group

When you create and edit a device group, you can choose whether to use the FortiManager ADOM or the FortiGate device to manage members for the device group.

To create a dynamic device group:

- 1. Ensure you are in the correct ADOM.
- 2. Go to *Policy & Objects > Object Configurations > User & Device > Customer Devices & Groups*.
- 3. From the *Create New* menu, select *Device Group*.
- 4. Complete the following options, then click *OK*.

<b>Group Name</b>	Type a name for the device group.
<b>Managed on ADOM</b>	Specify whether to use the FortiManager ADOM or the FortiGate device to manage members for the device group. When you select the <i>Managed on ADOM</i> checkbox, the FortiManager ADOM manages members for the object, and you must specify members for the object. When you clear the <i>Manage on ADOM</i> checkbox, the FortiGate device manages members for the object, and you must specify members by using FortiGate, not FortiManager.
<b>Members</b>	Select members for the device group.
<b>Comments</b>	(Optional) Type a comment.
<b>Per-Device Mapping</b>	Select to enable dynamic mapping for a device.

## Remove an object

### To remove an object:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
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*.

## 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 [Push to device on page 422](#).

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 > Object Configurations*.
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 > Object Configurations*.
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*.

## Push to device

An object can be manually pushed 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 *CLI Console* widget, or any terminal emulation software, enter the following commands:

```
config system global
    set partial-install enable
end
```

### To push an object or objects to devices:

1. In the *Object Configurations* pane, locate the objects to push.
2. Select the objects then click *More > Push To Device* in the toolbar, or right-click on the objects and select *Push To Device*.

The *Push To Device* dialog box opens, and the selected object or objects are pushed to all of the devices that currently use them.



After an object is pushed to a device, policy packages will be flagged as modified until the next time the packages are installed.



Global database objects cannot be pushed to devices.

---

## 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 > Object Configurations*.
3. In the tree menu, select an object type. The content pane displays the objects for the object type.
4. Right-click an object, and select *Clone*. The *Clone* pane is displayed.
5. Adjust the information as required, and click *OK* to create the new object.

## 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 > Object Configurations*.
3. In the tree menu, select an object type. The content pane displays the objects for the object type.
4. In the search box on the right side lower content frame 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.

---

## Find unused objects

### To find unused objects:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. From the *Tools* menu, select *Unused Objects*. The *Unused Objects* dialog box is displayed.
4. 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*.

## Export 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 > Object Configurations*.
3. In the tree menu, select *Application Control* or *Intrusion Prevention*.
4. Click *Create New* to create a new object, or double-click an existing object to open it for editing.
5. Click *Add Signatures*.

The *Add Signatures* dialog box is displayed.

Name	Category	Technology	Popularity	Risk
126.Mail	Email	Browser-Based	★★★★★	Medium
1koun	Video/Audio	Client-Server	★★★★★	Medium
1und1.Mail	Email	Browser-Based	★★★★★	Medium
2ch	Social.Media	Browser-Based	★★★★★	Elevated
2ch_Post	Social.Media	Browser-Based	★★★★★	Elevated
360.Safeguard.Update	Update	Client-Server	★★★★★	Low
360.Yunpan	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium
360.Yunpan_File.Download	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium
360.Yunpan_File.Upload	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium
360.Yunpan_Login	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium
3PC	Network.Service		★★★★★	Elevated
4shared	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium
4shared_File.Download	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium
4shared_File.Upload	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium
5ch	Social.Media	Browser-Based	★★★★★	Elevated
5ch_Post	Social.Media	Browser-Based	★★★★★	Elevated

[Total: 3266]

Export to CSV    Use Selected Signatures    Cancel

6. Click *Export to CSV*.

The *Export to CSV* dialog box is displayed.

File Name: App\_Signatures\_root\_2018-01-31-155641.csv

Options:

☒ Export all columns

☐ Export customized columns only

Download    Cancel

7. (Optional) Change the file name.
8. Select whether to export all columns or only customized columns.
9. Click *Download*.

## CLI Configurations

FortiManager adds 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.

## FortiToken configuration example

### To configure FortiToken objects for FortiToken management:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
3. Go to *User & Authentication > FortiTokens*.
4. Click *Create New*.
5. 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 117](#). 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 > Object Configurations > User & Authentication > FortiTokens > Import* and upload the text file.
- Upload a FortiToken seed file (.ftk) through *Policy & Objects > Object Configurations > 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.

6. Go to *User & Authentication > User Definition* to create a new user.
7. When creating the new user, select *FortiToken*, and then select the FortiToken from the dropdown menu.
8. Go to *User & Authentication > User Groups*, create a new user group, and add the previously created user to this group.
9. Install a policy package to the FortiGate, as described in [Install a policy package on page 314](#).
10. 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.

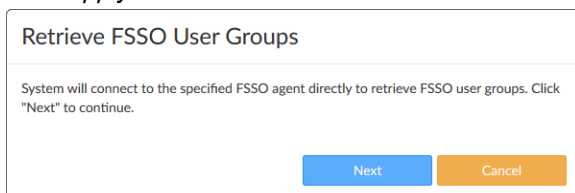
## FSSO user groups

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 > Object Configurations*.
3. Expand *Fabric Connectors*, and select *Endpoint/Identity*.
4. Click *Create New > Fortinet Single Sign-On Agent* from the drop-down list.
5. Enter a unique name for the agent in the *Name* field.
6. 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.
7. Select *Collector Agent* in the *User Group Source* field.
8. Click *Apply & Refresh*. The *Retrieve FSSO User Groups* dialog box will open.



**Retrieve FSSO User Groups**

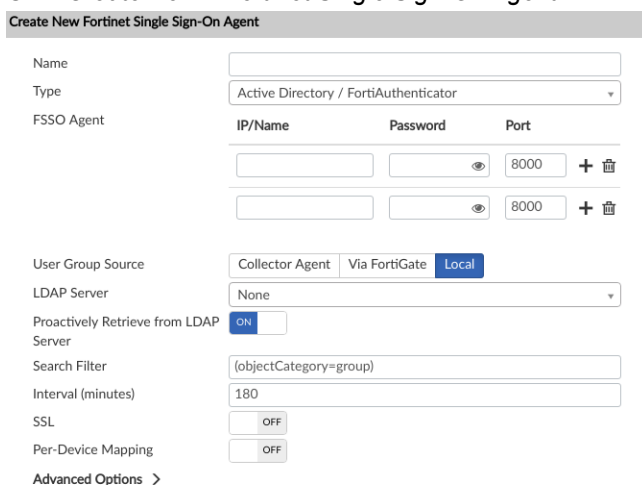
System will connect to the specified FSSO agent directly to retrieve FSSO user groups. Click "Next" to continue.

Next Cancel

9. Click *Next*. The groups are retrieved from the FSSO.
10. 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 > Object Configurations*.
3. Expand *Fabric Connectors*, and select *Endpoint/Identity*.
4. Click *Create New > Fortinet Single Sign-On Agent* from the drop-down list.



**Create New Fortinet Single Sign-On Agent**

Name:

Type:

FSSO Agent

IP/Name	Password	Port	
<input type="text"/>	<input type="password"/>	8000	+ -
<input type="text"/>	<input type="password"/>	8000	+ -

User Group Source:

LDAP Server:

Proactively Retrieve from LDAP Server: ☒

Search Filter:

Interval (minutes):

SSL:

Per-Device Mapping:

Advanced Options >

5. Enter a unique name for the agent in the *Name* field.
6. Select *Local* in the *User Group Source*.

7. Select an LDAP server from the drop-down list. LDAP Servers can be added and configured from *User & Device > LDAP Servers*.
8. Toggle *Proactively Retrieve from LDAP Server* to ON.
9. Specify the value for the *Search Filter* and the *Interval* in minutes.
10. For the Select LDAP Groups option, select *Remote Server*. Alternatively, select *Manually Specify* and specify the group names.
11. 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 142](#).

1. Go to *Policy & Objects > Object Configurations*.
2. Expand *Fabric Connectors*, and select *Endpoint/Identity*.
3. Click *Create New > Fortinet Single Sign-On Agent* from the drop-down list. The *Create New Fortinet Single Sign-On Agent* window opens.

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 *Via FortiGate* in the *Select FSSO Groups* field.
7. Click *Apply & Refresh*. The *Retrieve FSSO User Groups* wizard will open.

8. Click *Next* to proceed with the wizard.
9. 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.
10. Click *Next*. The FSSO agent is installed on the FortiGate, the FortiGate retrieves the groups, and then the groups are imported to the FortiManager.

Retrieve FSSO User Groups

Group Imported Successfully

100%

- ✓ Installing FSSO Agent to FortiGate
- ✓ Waiting for FortiGate to Sync with FSSO
- ✓ Retrieving FSSO Groups to Device Manager
- ✓ Importing FSSO Groups

Finish Cancel

11. After the groups have been imported, click *Finish*. The imported groups will be listed in the *User Groups* field.

Create New Fortinet Single Sign-On Agent

Name

FSSO Agent

IP/Name	Password	Port	
10.222.788.878	••••••••	8000	+ 🗑
<input type="text"/>	••••••••	8000	+ 🗑

Select FSSO Groups ☐ From FSSO Agents ☒ Via FortiGate

User Groups

CN=a'test,DC=FSSOtest,DC=com  
 CN=qa01 fmg,CN=Users,DC=FSSOtest,DC=com  
 CN=qa03,CN=Users,DC=FSSOtest,DC=com  
 CN=qa04,CN=Users,DC=FSSOtest,DC=com  
 OU=EQUIPE,DC=FSSOtest,DC=com

LDAP Server

Per-Device Mapping

Advanced Options >

Apply & Refresh OK Cancel

12. 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 > Object Configurations*.
3. Expand *Fabric Connectors*, and select *Endpoint/Identity*.
4. Click *Create New > Poll Active Directory Server* from the drop-down list.
5. Configure the server name, local user, password, and polling.
6. Select an LDAP server from the drop-down list. LDAP Servers can be added and configured from *User & Device > LDAP Servers*.
7. 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.
8. Select *OK*.

## Interface mapping

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 > Object Configurations*.
3. Go to *Normalized Interface > Normalized Interface* and click *Create New*.
4. Enter a name and description for the interface.
5. Turn on *Per-Device Mapping*.
6. Click *Create New*. The *Per-Device Mapping* dialog box opens.
7. Select the device or VDOM in the *Mapped Device* field, select the interface in the *Device Interface* field, then click *OK*.
8. Click *OK* to create the new dynamic interface object.

The mapped interface can now be used when creating policies.

## 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 be 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.

## 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 *System > Interface*.
    - 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 > Object Configurations > Normalized Interface > 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*.

## Create a new shaping profile

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 > Object Configurations*.
3. Go to *Firewall Objects > Shaping Profile*.
4. Click *Create New*. The *Create New Shaping Profile* pane opens.

Create New Shaping Profile

Name

Traffic Shaping Policy 1

Default Shaping Group (2-31)

2

Comments

0/1023

Additional Shaping Groups

+ Create New

Edit

Delete

Move Up

Move Down

Set to Default

Column Settings

<input type="checkbox"/> Shaping Group	Guaranteed Bandwidth(%)	Maximum Bandwidth(%)	Priority
<input type="checkbox"/> 3	20	30	High
<input type="checkbox"/> 4	20	30	High
<input type="checkbox"/> 5	29	45	High

OK

Cancel

5. Select or specify the values for the following and click *OK*:

<b>Name</b>	Specify the name for the shaping profile.
<b>Default Shaping Group</b>	Specify a default shaping group between 2-31.
<b>Comments</b>	Optionally enter comments about the shaping profile.
<b>Additional Shaping Groups</b>	Click <i>Create New</i> . Specify the <i>Shaping Group</i> , <i>Guaranteed Bandwidth(%)</i> , <i>Maximum Bandwidth(%)</i> and <i>Priority</i> . Click <i>OK</i> .

6. Assign the shaping profile to an interface. See [Assigning a shaping profile on page 432](#).



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 *System > Interface*.
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

### Viewing the traffic shaping widget

You can view the *Traffic Shaping* widget in the *Device Manager*.

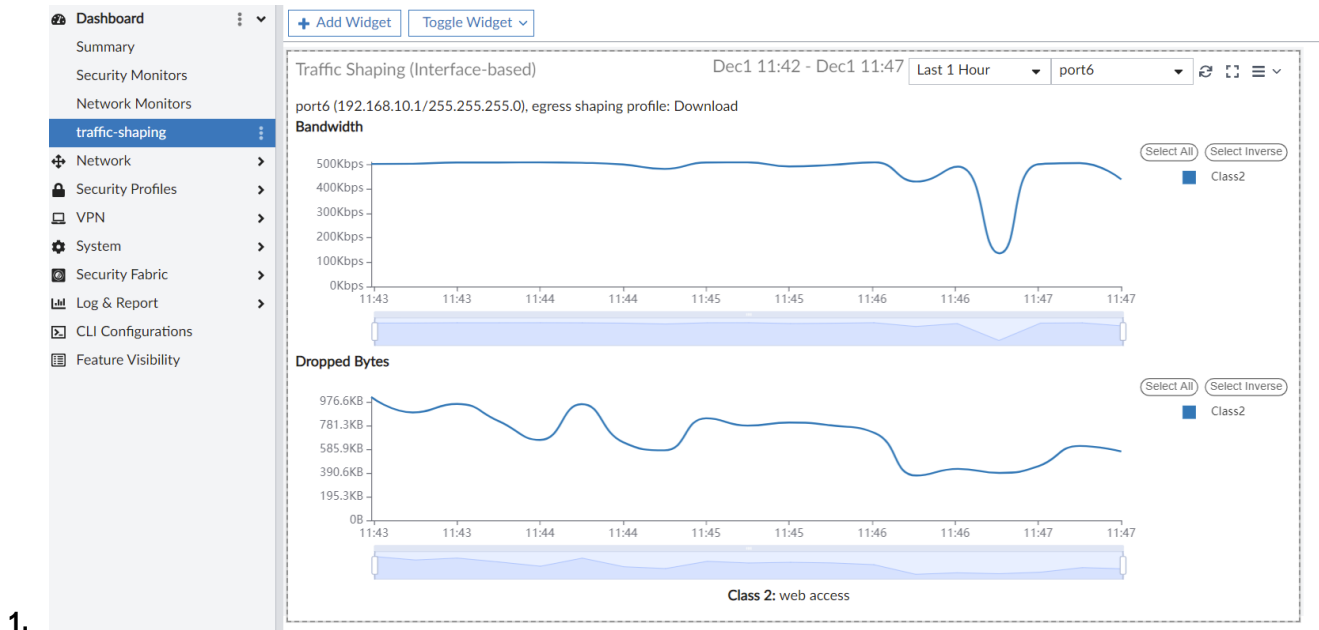


To view traffic shaping information, you must enable traffic shaping history. Traffic shaping history can be enabled in the CLI using the following commands:

```
config system admin setting
  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 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 > Object Configurations > 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 163](#).
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 > Object Configurations > 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*.

## IPS 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 827](#).

---

## 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 > Object Configurations > 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:**

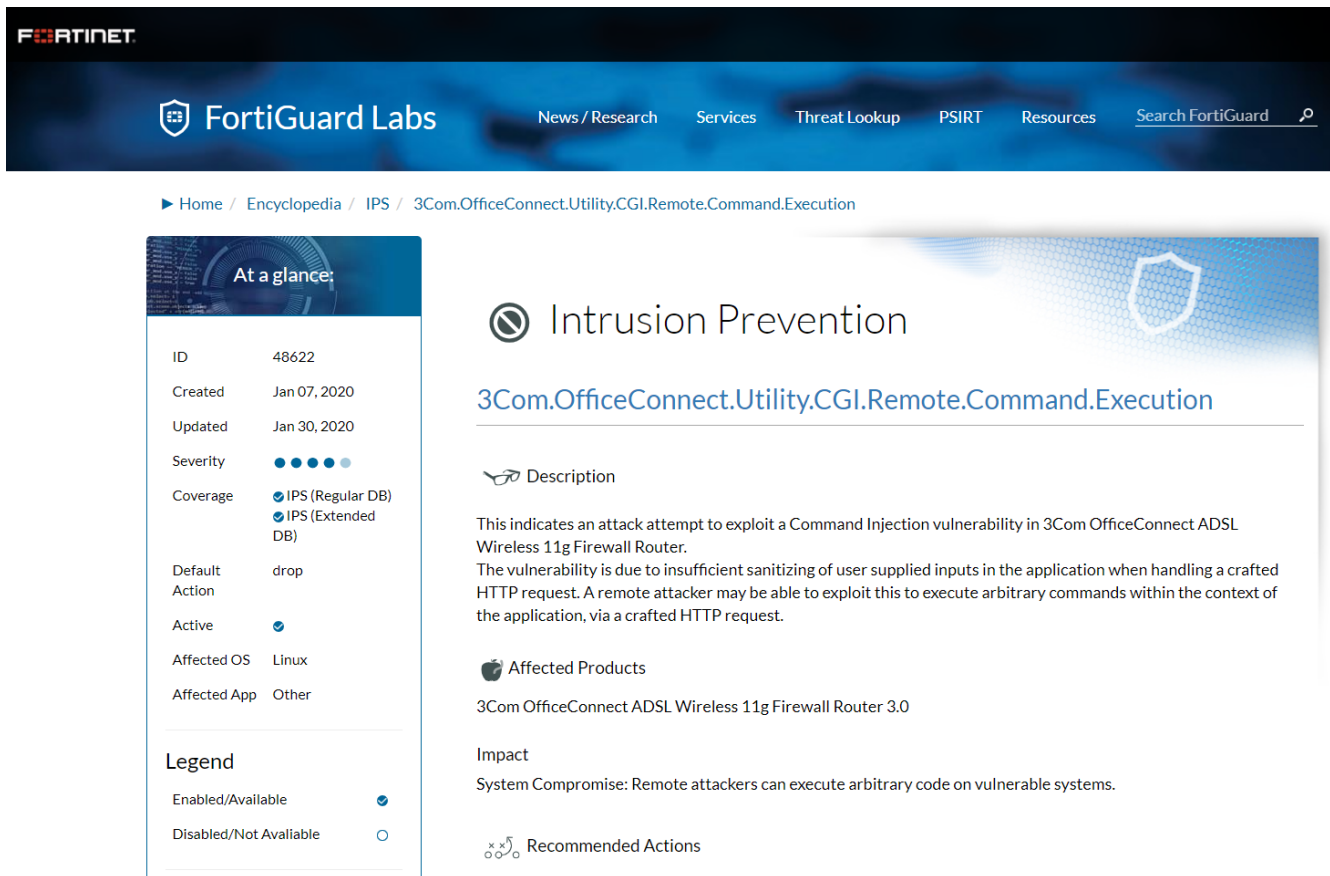
Right-click a signature, and select *Promote to Global*.

**Viewing IPS Signature details**

To view IPS Signature *Information* page, click the IPS signature name. The following information is displayed:

Section	Description
<b>Name</b>	The IPS signature name.
<b>Risk</b>	Displays the risk level.
<b>Summary</b>	Describes the threats and vulnerabilities detected by the IPS signature.
<b>Affected Products</b>	Displays the products that are vulnerable to the attack.
<b>Action</b>	Provides recommendations to prevent an attack.
<b>Analysis</b>	Provides specific details about how the vulnerability can be exploited.
<b>References</b>	A list of links you can visit for more information.
<b>Miscellaneous</b>	The signature ID.

To view information about the signature ID in FortiGuard, click the ID link in the *ID* column.



**FortiGuard Labs**

News / Research Services Threat Lookup PSIRT Resources Search FortiGuard

Home / Encyclopedia / IPS / 3Com.OfficeConnect.Utility.CGI.Remote.Command.Execution

**At a glance:**

ID	48622
Created	Jan 07, 2020
Updated	Jan 30, 2020
Severity	●●●●●
Coverage	<input checked="" type="checkbox"/> IPS (Regular DB) <input checked="" type="checkbox"/> IPS (Extended DB)
Default Action	drop
Active	<input checked="" type="checkbox"/>
Affected OS	Linux
Affected App	Other

**Legend**

Enabled/Available ☒

Disabled/Not Available ☐

## Intrusion Prevention

### 3Com.OfficeConnect.Utility.CGI.Remote.Command.Execution

**Description**

This indicates an attack attempt to exploit a Command Injection vulnerability in 3Com OfficeConnect ADSL Wireless 11g Firewall Router. The vulnerability is due to insufficient sanitizing of user supplied inputs in the application when handling a crafted HTTP request. A remote attacker may be able to exploit this to execute arbitrary commands within the context of the application, via a crafted HTTP request.

**Affected Products**

3Com OfficeConnect ADSL Wireless 11g Firewall Router 3.0

**Impact**

System Compromise: Remote attackers can execute arbitrary code on vulnerable systems.

**Recommended Actions**

## ADOM-level metadata variables

ADOM-level metadata variables can be used as variables in scripts, templates, firewall address objects, IP pools, and VIPs.

You can configure ADOM-level metadata variables in *Policy & Objects > Object Configurations > Advanced > Metadata Variables*. Metadata variables configured in this way are only available in the ADOMs in which they were created.

ADOM-level 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.

Typing `$` into an object's field where metadata variables are supported will display the available metadata variables for selection.



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 > Object Configurations > Advanced > Metadata Variables*.
2. Click *Create New*.

The *Create New Metadata Variables* window opens.

3. Enter the following information:

<b>Name</b>	Enter a name for the metadata variable.
<b>Description</b>	Optionally, enter a description.
<b>Default Value</b>	Set the default value for the variable. The default value is used whenever a per-device mapping is unavailable.
<b>Per-ADOM Mapping</b>	This setting is only available in the Global Database ADOM. Toggle ON to enable per-ADOM mapping. When enabled, click <i>Create New</i> to map an <i>ADOM</i> to a <i>Value</i> . This value will be applied to all devices in the selected ADOM.
<b>Per-Device Mapping</b>	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 <i>Create New</i> beneath <i>Per-Device Mapping</i> and specifying the <i>Mapped Device</i> and <i>Value</i> .
<b>Revision</b>	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 and import metadata variables:**

1. Go to *Policy & Objects > Object Configurations > Advanced > Metadata Variables*.
2. Select *More* in the toolbar and click *Export Metadata Variables*.  
The metadata variables are exported into a JSON format file.
3. In a second ADOM, go to *Policy & Objects > Object Configurations > Advanced > Metadata Variables*.
4. Select *More* from the toolbar and click *Import Metadata Variables*.
5. Browse to your exported JSON file, or drag and drop it into the file selector, and click *Import*.

**To use a metadata variable in dynamic objects:**

1. Go to *Policy & Objects > Object Configurations*.
2. Create or edit a Firewall Address, IP Pool, or Virtual IP object.
3. Add the metadata in 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.

Create New Firewall Address

Name

Branch-NET

Color

4

Type

Subnet

IP/Netmask

10.1.\${branch\_id}.0/24

Resolve from name

Interface

any

Static Route Configuration

Comments

Add To Groups

Click to select

Advanced Options >

Per-Device Mapping

Revision

Change Note \*

Revision History

Revert

View Diff

Column Settings

Search...

	Revision #	Changed by	Date/Time	Entry Key	Entry name	Action	Change Note
No record found.							

OK

Cancel

When using metadata variables in an object, per-device mappings are no longer required.

## 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 > Object Configurations > 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

<div>+ Create New</div> <div> Edit</div> <div> Delete</div> <div> More</div>				<div> View</div> <div>Search...</div>			
	Name	Type	Details	Interface	Comments	Created Time	Last Modified
	Management-Network	Firewall Address	IP/Netmask:: 10.100.55.0/255.255.255.0	any		2021-11-18 16:41:52	
	RFC1918-10	Firewall Address	IP/Netmask:: 10.0.0.0/255.0.0.0	any		admin / 2022-08-30 0'	
	RFC1918-172	Firewall Address	IP/Netmask:: 172.16.0.0/255.240.0.0	any		admin / 2022-08-30 0'	
	RFC1918-192	Firewall Address	IP/Netmask:: 192.168.0.0/255.255.0.0	any		admin / 2022-08-30 0'	
	MPLS-Interfaces	Firewall Address	IP/Netmask:: 192.168.0.0/255.255.254.0	any		2021-11-18 16:41:52	
	Branch-VPN-Interface	Firewall Address	IP/Netmask:: 10.0.0.0/255.255.0.0	any		2021-11-18 16:41:52	

The following default RFC1918 address group containing the three address objects is available under *Address Group*:

- **RFC1918-GRP**

<a href="#">+ Create New</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">More</a>			<a href="#">View</a> <input type="text" value="Search..."/>				
<input type="checkbox"/>	Name	Type	Details	Interface	Comments	Created Time	Last Modified
<input type="checkbox"/>	Remote-Branches	Address Group	<a href="#">+1</a> Branch_01 Branch_02 Branch-VPN-Interface MPLS-Interfaces			2021-11-18 16:41:52	
<input checked="" type="checkbox"/>	RFC1918-GRP	Address Group	RFC1918-10 RFC1918-172 RFC1918-192			admin / 2022-08-30 0	

## Persistent object search menu

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.

The screenshot displays the FortiManager interface for Policy & Objects. The left sidebar shows the 'Policy Packages' menu with 'Firewall Policy' selected. The main table lists policies with columns for #, Name, Service, Action, Security Profiles, and Log. Policy 1 is selected, showing details for 'ALL\_ICMP' with an 'Accept' action. The 'Object Search' panel is open on the right, showing a search bar with 'all' and a list of object categories: INTERFACE (0), SOURCE (4), DESTINATION (4), SCHEDULE (0), SERVICE (5), and UTM PROFILES (3). The Fortinet logo is visible at the bottom left of the interface.

3. From the search results, you can see which objects are configurable to which policy fields.

The screenshot shows the FortiManager Policy & Objects interface. The main table displays the following data:

#	Service	Action	Security Profiles	Log
1	ALL_ICMP	Accept	Log All Sessions	
2	taj-service	Accept	Log Security	
3	taj-service	Accept	Log Security	
Implicit (4/4 Total:1)				
4	ALL	Deny	No Log	

The right sidebar shows the Object Search results, categorized by type:

- INTERFACE (0)
- SOURCE (4)
- DESTINATION (4)
- SCHEDULE (0)
- SERVICE (5)
  - CUSTOM SERVICE (5)
    - ALL
    - ALL\_ICMP
    - ALL\_ICMP6
    - ALL\_TCP
    - ALL\_UDP
- UTM PROFILES (3)

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 same category.

The screenshot shows the FortiManager Policy & Objects interface with the drag-and-drop feature being demonstrated. The main table is the same as in the previous screenshot. The right sidebar shows the Object Search results. The object 'ALL\_TCP' is being dragged from the SERVICE category and dropped into the 'Service' column of policy 1.

## Zero Trust Network Access (ZTNA) objects

Zero Trust Network Access (ZTNA) objects and groups can be configured in FortiManager.

For more information on configuring ZTNA, see the [FortiGate Administration Guide](#).

## Viewing ZTNA tags

ZTNA Tags displays the ZTNA tags synchronized to FortiGate from FortiClient EMS or FortiClient EMS Cloud. You can dynamically synchronize ZTNA tags using a FortiClient EMS connector.

ZTNA 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 ZTNA 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 369](#).

### To view ZTNA tags:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations > Firewall Objects > ZTNA Tag*.  
ZTNA tags synchronized from the FortiGate are displayed.

### To clone ZTNA tags:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations > Firewall Objects > ZTNA 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 *ZTNA Tag*.

## Creating ZTNA geographic IP objects

### To create a Geographic IP address object:

1. Go to *Policy & Objects > Object Configurations > Firewall Objects > Addresses*, click *Create New*, and select *Address*.  
The Create New Address window opens.

**Create New Address**

Address Name:

Color:

Type:

Geography:

Interface:

Static Route Configuration: ☐

Comments:

Add To Groups:

Advanced Options >

Per-Device Mapping: ☐

Revision

Change Note:

Revision History

Revision #	Changed by	Date/Time	Action	Change Note
------------	------------	-----------	--------	-------------

OK Cancel

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 ZTNA 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 ZTNA 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 369](#).

### To create a ZTNA Tag Group:

1. Go to *Object Configurations > Firewall Objects > ZTNA Tag*, and click *Create New*. The *Create New ZTNA Tag Group* window opens.

**Edit ZTNA Tag Group**

Group Name: ZTNA\_Tag\_1

ZTNA Tag: EMS Geographic IP

Color: [icon]

Members: FCTEMS\_ALL\_FORTICLOUD\_SERVERS (1 Entry Selected)

Comments: [text area] 0/255

Advanced Options >

Revision

Change Note: [text area] 0/1023

Revision History

Revision #	Changed by	Date/Time	Action	Change Note
1	administrator	2021-06-29 11:07:51	Create	Creation.

OK Cancel

- Enter a name for the group.
- Select a *ZTNA Tag* type from one of the following:
  - EMS
  - Geographic IP
- Select *Members* to add to the ZTNA tag group.
  - When configuring an EMS tag group, members are configured in *Policy & Objects > Object Configurations > Firewall Objects > ZTNA Tag* with a *IP* or *MAC* object type. See [Viewing ZTNA tags on page 443](#).
  - When configuring a Geographic IP tag group, members are configured in *Policy & Objects > Object Configurations > Firewall Objects > Addresses* as a *Firewall Address* with the *Type* set as *Geography*. See [Creating ZTNA geographic IP objects on page 443](#).
- 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 369](#).

### To create a ZTNA Server:

- Go to *Policy & Objects > Object Configurations > Firewall Objects > ZTNA Server*, and click *Create New*.
- 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 752](#).

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 446](#)
- [ICAP remote server on page 447](#)
- [ICAP load balancing on page 447](#)

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 752](#).

### To create an ICAP profile:

1. Go to *Policy & Objects > Object Configurations > Content Analysis > ICAP Profile*, and click *Create New*. The *Create New ICAP Profile* window appears.
2. Enter the following information:

<b>Name</b>	Enter a name for the ICAP profile.
<b>Enable Request Processing</b>	<p>Enable or disable request processing.</p> <p>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 <i>Error</i> or <i>Bypass</i>.</p>
<b>Enable Response Processing</b>	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 752](#).

### To create an ICAP remote server:

1. Go to *Policy & Objects > Object Configurations > Content Analysis > ICAP Remote Server*, and click *Create New*. The *Create New ICAP Remote Server* window appears.
2. Enter the following information:

<b>Name</b>	Enter a name for the ICAP remote server.
<b>Address Type</b>	Select the address type.
<b>IP Address</b>	Enter the IP address of the ICAP remote server.
<b>Plain ICAP Connection and Secure ICAP Connection</b>	Select whether the ICAP connection is plain or secure. Only one setting can be enabled at a time.
<b>Max Connections</b>	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 752](#).

**To create an ICAP load balancing object:**

1. Go to *Policy & Objects > Object Configurations > Content Analysis > ICAP Load Balancing*, and click *Create New*. The *Create New ICAP Load Balancing* window appears.
2. Enter the following information:

<b>Name</b>	Enter a name for the ICAP load balancer.
<b>Method</b>	Select the load balancing method from <i>Weighted</i> , <i>Least Session</i> , or <i>Active Passive</i> .
<b>Remote Server</b>	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:

<b>ID</b>	The ADOM revision identifier.
<b>Name</b>	The name of the ADOM revision. This field is user-defined when creating the ADOM revision.  A green lock icon will be displayed beside the ADOM revision name when you have selected <i>Lock this revision from auto deletion</i> .
<b>Created by</b>	The administrator that created the ADOM revision.
<b>Created Time</b>	The ADOM revision creation date and time.
<b>Comment</b>	Optional comments typed in the <i>Description</i> field when the ADOM revision was created.

The following options are available:

<b>Create New</b>	Select to create a new ADOM revision.
<b>Edit</b>	Right-click on a revision in the table and select <i>Edit</i> in the menu to edit the ADOM revision.
<b>Delete</b>	Right-click on a revision in the table and select <i>Delete</i> in the menu to delete the ADOM revision.  When <i>Lock this revision from auto deletion</i> is selected, you are not able to delete the ADOM revision.

<b>View Revision Diff</b>	Right-click on a revision in the table and select <i>View Revision Diff</i> in the menu. The Summary page will be displayed. This page shows the revision differences between the selected revision and the current database.
<b>Restore</b>	Right-click on a revision in the table and select <i>Restore</i> in the menu to restore the ADOM revision. Restoring a revision will revert policy packages, objects and VPN console to the selected version. Select <i>OK</i> to continue.
<b>More &gt; Lock Revision</b>	Right-click on a revision in the table and select <i>Lock</i> from the <i>More</i> menu to lock this revision from auto deletion.
<b>More &gt; Unlock Revision</b>	Right-click on a revision in the table and select <i>Unlock</i> from the <i>More</i> 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.
<b>Settings</b>	Select to configure the automatic deletion settings for ADOM revisions.
<b>Close</b>	Select to close the <i>ADOM Revision</i> dialog box and return to the <i>Policy &amp; Objects</i> 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:**

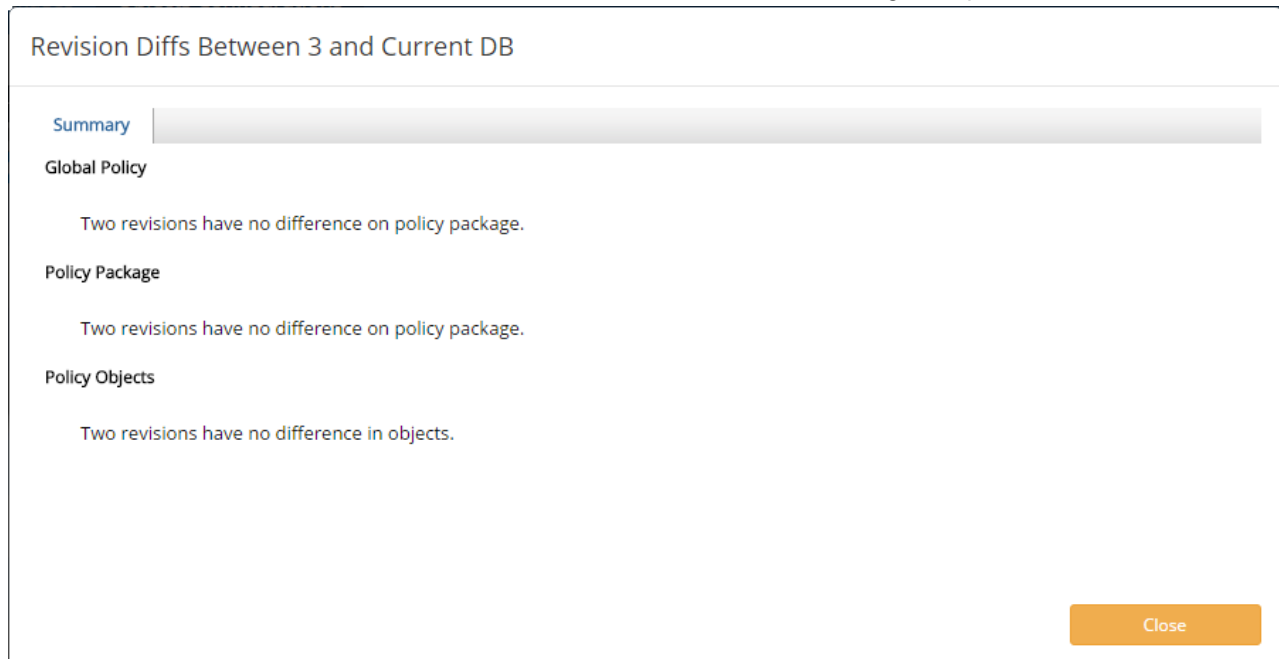
1. Open the *ADOM Revisions* window.
2. Select a revision, and click *Restore*. A confirmation dialog box will appear.
3. Click *OK* to continue.  
The *Restore Revision* dialog box opens. Restoring a revision will revert policy packages, objects and VPN console to the selected version.
4. Click *OK* 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 *Policy Objects* 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. You can select to download this information as a CSV file to your management computer.
5. 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. You can use *AP Manager* for the following modes of management:

- Central management of managed access points
- Per-device management of managed access points

The *AP Manager* tree menu contains the following items:

<b>Device &amp; Groups</b>	Displays unauthorized and authorized FortiAP devices. You can view, authorize, and edit authorized FortiAP devices.
<b>Map view</b>	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.
<b>WiFi profiles for central management on page 470</b>	<p>When central management is enabled, you can view, create, edit, and import profiles. WiFi profiles share a common database. You can apply profiles to any device, regardless of which FortiGate controller it is connected to.</p> <p>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.</p>

## Device & Groups

The *Device & Groups* pane allows you to manage FortiAP devices that are controlled by FortiGate devices and are managed by the FortiManager.

FortiAP devices, listed in the tree menu, 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 759](#)). 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 770](#).

**To manage FortiAP devices:**

1. Go to *AP Manager*.
2. In the tree menu, go to *Device & Groups > Managed FortiGate (#)*.
3. (Optional) In the toolbar, click *List > Group*, to view devices in a group. See [FortiAP groups on page 458](#)

Managed APs are organized by their FortiGate controller and group.

**Quick status bar**

You can quickly view the status of devices on the *Managed FortiGate* pane with the quick status bar, which contains the following information in pie charts:

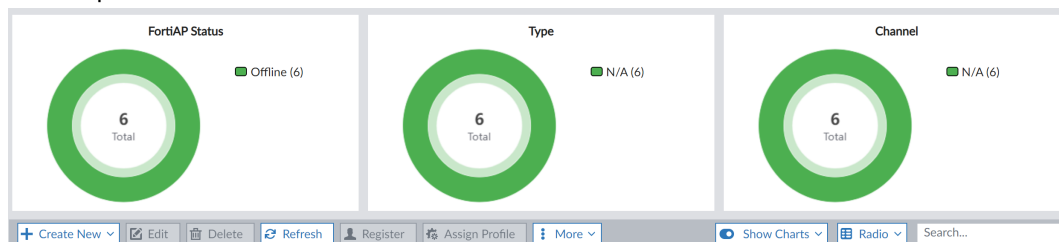
- Managed APs
- Online
- Offline
- Unauthorized
- Client Connected


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:**

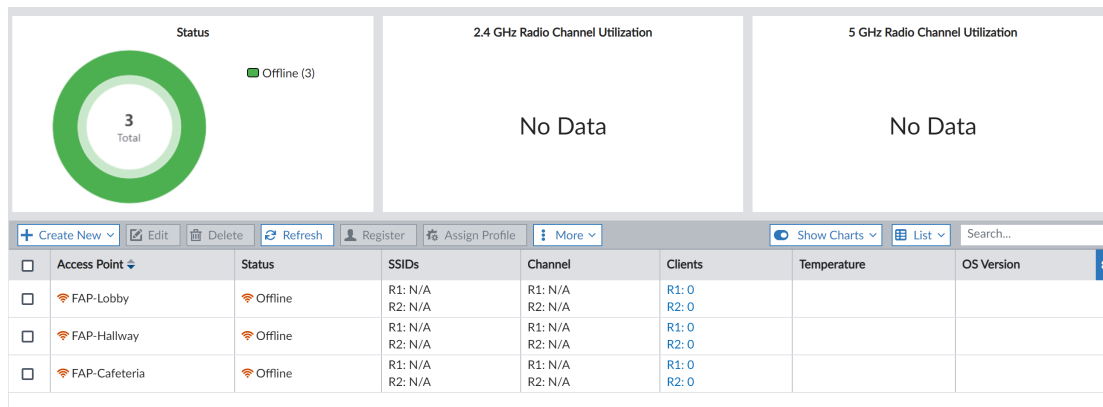
1. Ensure that you are in the correct ADOM.
2. Go to *AP Manager*.
3. In the tree menu, click *Device & Groups > Managed FortiGate (#)*. The quick status bar is displayed above the content pane.



4. In the tree menu, select a managed FortiGate if central management is enabled, or a FortiGate if per-device management is enabled.  
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.
5. Mouse over the charts to see more information about the data in a tooltip.
6. 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.
7. To remove the filters, click the chart title with the filter icon.
8. 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:

<b>Create New</b>	Add an AP or an AP group. The APs must be the same model to be grouped. See <a href="#">FortiAP groups on page 458</a> .
<b>Edit</b>	Edit the selected AP.
<b>Delete</b>	Delete the selected AP.
<b>Refresh</b>	Refresh the AP list, or refresh the selected FortiAP devices.
<b>Register</b>	Register the selected FortiAP device to your FortiCloud account.
<b>Assign Profile</b>	Assign a profile from the list to the AP. Only applicable profiles will be listed. See <a href="#">Assigning profiles to FortiAP devices on page 505</a> .
<b>More</b>	
<b>Authorize</b>	Authorize an AP. See <a href="#">Authorizing and deauthorizing FortiAP devices on page 459</a> . This option is also available in the toolbar by selecting <i>More</i> .
<b>Deauthorize</b>	Deauthorize an AP. See <a href="#">Authorizing and deauthorizing FortiAP devices on page 459</a> . This option is also available in the toolbar by selecting <i>More</i> .
<b>Upgrade</b>	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 <i>FortiGuard &gt; Firmware Images &gt; Product: FortiAP</i> and click the download icon to manually download the firmware images.
<b>Restart</b>	Restart the AP.

<b>Diagnostics and Tools</b>	View the device <i>Summary</i> , <i>Performance</i> , <i>Clients</i> , <i>Interfering SSIDs</i> , and <i>Spectrum Analysis</i> . View the clients connected to the AP. See <a href="#">Connected clients on page 462</a> . View the spectrum analysis for managed APs. See <a href="#">Spectrum analysis for managed APs on page 463</a> .
<b>Export to Excel/CSV</b>	Export the selected device details to an Excel or CSV file.
<b>View Rogue APs</b>	View the Rogue APs. See <a href="#">Rogue APs on page 460</a> .
<b>View Health Monitor</b>	View the AP status, clients counts, and wireless interference. See <a href="#">Health Monitor on page 465</a> .
<b>Replace</b>	Replace a FortiAP device. Selecting this option allows you to enter a new FortiAP Serial Number for the selected device. See <a href="#">Replacing APs on page 466</a> .
<b>LED Blink</b>	Start LED blink on the selected FortiAP for the specified period of time. This option is only available in the right-click menu.
<b>Show on Google Map</b>	Show the selected AP on Google Map. See <a href="#">Google map on page 468</a> . This option is only available in the right-click menu.
<b>Show on Floor Map</b>	Show the selected AP on the floor map. See <a href="#">Floor map on page 469</a> . This option is only available in the right-click menu.
<b>Grouping</b>	Move the selected FortiAP devices into a new group. The APs must be the same model to be grouped. See <a href="#">FortiAP groups on page 458</a> . This option is only available in the right-click menu.
<b>Search</b>	Enter a search string into the search field to search the AP list.
<b>Column Settings</b>	Click to select which columns to display or select <i>Reset to Default</i> to display the default columns.

The following information is available in the content pane:

<b>FortiGate</b>	The FortiGate unit that is managing the AP.
<b>Access Point</b>	The serial number of the AP.
<b>SSIDs</b>	The SSIDs associated with the AP.
<b>Channel</b>	The wireless radio channels that the access point uses.
<b>Clients</b>	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 <a href="#">Connected clients on page 462</a> .
<b>Temperature</b>	Device temperature information.
<b>OS Version</b>	The OS version on the FortiAP.
<b>AP Profile</b>	The AP Profile assigned to the device, if any.



<b>Connected Via</b>	The IP address of the AP.
<b>Model</b>	
<b>Channel Utilization</b>	
<b>Comments</b>	User entered comments.
<b>Country/Region</b>	The Country code that the FortiAP is using.
<b>Join Time</b>	The date and time that the FortiAP joined.
<b>LLDP</b>	The Link Layer Discovery Protocol
<b>Operating TX Power</b>	The transmit power of the wireless radios.
<b>Serials #</b>	The serial number of the device
<b>WTP Mode</b>	The Wireless Transaction Protocol (WTP) mode, or 0 if none.

### To add a FortiAP:

- From the *Create New* dropdown, select *Managed AP*. The *Add FortiAP* dialog box opens.

- Enter the following information, then click *OK* to add the device:

<b>FortiGate</b>	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.
<b>Serials Number</b>	Enter the device's serial number.
<b>Name</b>	Enter a name for the device.
<b>AP Profile</b>	Select an AP profile to apply to the device from the dropdown list. See <a href="#">FortiAP profiles on page 474</a> .
<b>Enforce Firmware Version</b>	Toggle <i>ON</i> to enforce a firmware version and select the firmware version from the drop-down menu. Toggle <i>OFF</i> 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.

### To edit FortiAP devices:

1. In the tree menu, go to *Device & Groups > Managed FortiGate (#)*, 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 458](#).
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 *Config FortiAP* window opens.

4. Edit the following options, then click *Apply* to apply your changes:

<b>Serial Number</b>	The device's serial number. This field cannot be edited.
<b>Name</b>	The name of the AP.
<b>Comments</b>	Comments about the AP, such as its location or function.
<b>Managed AP Status</b>	Various information about the AP.
<b>Status</b>	The status of the AP, such as <i>Connected</i> , or <i>Idle</i> . Click <i>Restart</i> to restart the AP.
<b>Connected Via</b>	The method by which the device is connected to the controller.
<b>Base MAC Address</b>	The MAC address of the device.
<b>Join Time</b>	The time that the AP joined.
<b>Clients</b>	The number of clients currently connected to the AP.
<b>State</b>	The state of the AP, such as <i>Authorized</i> , or <i>Discovered</i> .
<b>Current</b>	The AP's current firmware version. Select <i>Upgrade</i> to upgrade the firmware to a newer version if you have one available.
<b>FortiAP Profile</b>	Select a profile from the dropdown list (see <a href="#">FortiAP profiles on page 474</a> )
<b>Bonjour Profile</b>	Select a profile from the dropdown list (see <a href="#">Bonjour profiles on page 498</a> )
<b>Override Radio</b>	Override the selected profiles settings.

<b>Band</b>	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.
<b>Channels</b>	Select the channel or channels to include, or let them be automatically assigned. The available channels depend on the selected platform and band.
<b>TX Power Control</b>	Enable/disable automatic adjustment of transmit power. <ul style="list-style-type: none"> <li>• <i>Auto</i>: Enter the TX power low and high values, in dBm.</li> <li>• <i>Manual</i>: Enter the TX power in the form of the percentage of the total available power.</li> </ul>
<b>SSIDs</b>	Manually choose the SSIDs that APs using this profile will carry, or let them be selected automatically.
<b>Override AP Login Password</b>	Enable/disable overriding the login password: <ul style="list-style-type: none"> <li>• <i>Set</i>: Set the AP login password.</li> <li>• <i>Leave Unchanged</i>: Leave the password unchanged.</li> <li>• <i>Set Empty</i>: Remove the password.</li> </ul>
<b>Advanced Options</b>	Configure advanced options. For information, see the <i>FortiOS CLI Reference</i> . <a href="https://help.fortinet.com/cli/fos60hlp/60/index.htm">https://help.fortinet.com/cli/fos60hlp/60/index.htm</a> .

#### To delete FortiAP devices:

1. In the tree menu, under *Device & Groups*, 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 120](#).



A FortiAP device cannot be deleted if it is currently being used. For example, if a firewall profile has been assigned to it.

#### To upgrade multiple FortiAP devices:

1. In the tree menu, go to *Device & Groups > Managed FortiGate (#)*, 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 458](#).
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*.



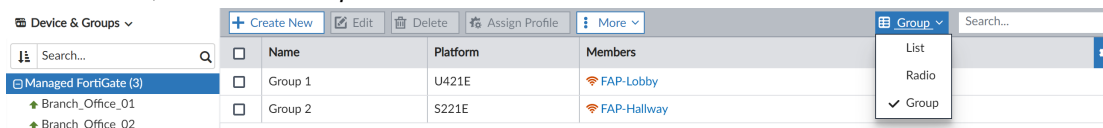
Before upgrading FortiAP, go to *FortiGuard > Firmware Images > Product: FortiAP* and click the download icon to manually download the firmware images.

## 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*.
2. In the tree menu, go to *Device & Groups > Managed FortiGate (#)*, select a managed device.
3. In the toolbar, click *List > Group*.



### To create a FortiAP group:

1. Go to *AP Manager*.
2. In the tree menu, go to *Device & Groups > Managed FortiGate (#)*, 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:

<b>Name</b>	Enter a name for the group.
<b>FortiGate</b>	Select the FortiGate under which the group will be created.
<b>FortiAPs</b>	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*.
2. In the tree menu, go to *Device & Groups > Managed FortiGate (#)*, 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*.
2. In the tree menu, go to *Device & Groups > Managed FortiGate (#)*, 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 statistics for the device, such as *CPU Usage*, *Memory Usage*, *Connection Uptime*, and *Temperature*.

**To view the FortiAP device summary:**

1. Go to *AP Manager*.
2. In the tree menu, go to *Device & Groups > Managed FortiGate (#)*, select a managed device. Alternatively, you can select a device in a group, see [FortiAP groups on page 458](#).
3. Right-click a managed device and click *Diagnostics and Tools*. The *Summary* tab opens.

S108DVWA9XDVG54		General Health <span>Good</span>	
Name	S108DVWA9XDVG54	10%	CPU Usage
Serial Number	S108DVWA9XDVG54	24%	Memory Usage
Version	S108DV-v7.0.0-build4062,210406 (Interim)	13 day(s)	Connection Uptime
Model	S108DV	Unknown	Temperature
FortiLink Interface	port1		
IP Address	169.254.2.2		
Join Time	Tue Sep 21 11:03:29 2021		
Status	Online		
Registration	Not Registered		

## Authorizing and deauthorizing FortiAP devices

**To authorize FortiAP devices:**

1. Go to *AP Manager*.
2. In the tree menu, go to *Device & Groups > Managed FortiGate (#)*, and select the FortiGate that contains the unauthorized FortiAP devices. Alternatively, you can select a device in a group, see [FortiAP groups on page 458](#).
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. In the tree menu, 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*.
2. In the tree menu, go to *Device & Groups*.
3. In the toolbar, click *More > View Rogue APs*. The rogue AP list is displayed.

View Rogue APs

<div> <span>Mark As</span> <span>Suppress AP</span> <span>Unsuppress AP</span> <span>Refresh</span> <span>Column Settings</span> </div> <div> <input type="checkbox"/> Show Offline (198)           <input type="checkbox"/> Show Accepted (0)           <input type="text"/> </div>									
State	Status	SSID	Security Type	Channel	MAC Address	Vendor Info	Signal Strength	Detected By	On-Wire
<input type="checkbox"/>		fortinet	WPA2 Personal	6	70:4ca5:99:da:22	Fortinet, Inc.	-47dBm	PS311C3U15000439(192.168.1.111:5246)	
<input type="checkbox"/>		FTNT-Guest	WPA2 Personal	6	70:4ca5:a3:87:e0	Fortinet, Inc.	-55dBm	PS311C3U15000439(192.168.1.111:5246)	
<input type="checkbox"/>		FTNT-Staff	WPA2 Enterprise	6	70:4ca5:a3:87:e1	Fortinet, Inc.	-56dBm	PS311C3U15000439(192.168.1.111:5246)	
<input type="checkbox"/>		DU_EPCR580	WPA Personal	11	7c:e1:ff:01:09:b0	Computer	-55dBm	PS311C3U15000439(192.168.1.111:5246)	
<input type="checkbox"/>		IPADS	WPA2 Personal	100	90:6cac:28:89:a8	Fortinet, Inc.	-13dBm	PS311C3U15000439(192.168.1.111:5246)	
<input type="checkbox"/>		fortinet	WPA2 Personal	11	90:6cac:7c:9b:aa	Fortinet, Inc.	-64dBm	PS311C3U15000439(192.168.1.111:5246)	
<input type="checkbox"/>		fortinet35	WPA/WPA2 Pers	6	90:6cac:a4:37:76	Fortinet, Inc.	-23dBm	PS311C3U15000439(192.168.1.111:5246)	
<input type="checkbox"/>		GuestWireless	WPA2 Personal	100	a2:6cac:28:89:a8		-14dBm	PS311C3U15000439(192.168.1.111:5246)	
<input type="checkbox"/>		LB_CP	OPEN	6	a2:6cac:28:89:e8		-10dBm	PS311C3U15000439(192.168.1.111:5246)	
<input type="checkbox"/>		StaffWireless	WPA2 Personal	6	b2:6cac:1b:72:be		-17dBm	PS311C3U15000439(192.168.1.111:5246)	
<input type="checkbox"/>		StaffWireless	WPA2 Personal	1	b2:6cac:25:d4:64		-22dBm	PS311C3U15000439(192.168.1.111:5246)	
<input type="checkbox"/>		StaffWireless	WPA2 Personal	100	b2:6cac:28:89:a8		-14dBm	PS311C3U15000439(192.168.1.111:5246)	
<input type="checkbox"/>		demo-112	WPA2 Personal	100	c2:6cac:28:89:a8		-13dBm	PS311C3U15000439(192.168.1.111:5246)	
<input type="checkbox"/>		fortinet	WPA2 Personal	6	e8:1cba:39:97:fa		-64dBm	PS311C3U15000439(192.168.1.111:5246)	
<input type="checkbox"/>		fortinetsz2	WPA2 Personal	1	e8:1cba:39:a2:32		-65dBm	PS311C3U15000439(192.168.1.111:5246)	
<input type="checkbox"/>		fortinet	WPA2 Personal	11	e8:1cba:51:cb:1a		-48dBm	PS311C3U15000439(192.168.1.111:5246)	

Close

The following options are available:

<b>Mark As</b>	<p>Mark a rogue AP as:</p> <ul style="list-style-type: none"> <li>• <i>Accepted</i>: for APs that are an authorized part of your network or are neighboring APs that are not a security threat.</li> <li>• <i>Rogue</i>: for unauthorized APs that On-wire status indicates are attached to your wired networks.</li> <li>• <i>Unclassified</i>: the initial status of a discovered AP. You can change an AP back to unclassified if you have mistakenly marked it as <i>Rogue</i> or <i>Accepted</i>.</li> </ul>
<b>Suppress AP</b>	<p>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.</p> <p>Before enabling this feature, verify that operation of Rogue Suppression is compliant with the applicable laws and regulations of your region.</p>
<b>Unsuppress AP</b>	Turn of suppression for the selected rogue APs.
<b>Refresh</b>	Refresh the rogue AP list.
<b>Column Settings</b>	Click to select which columns to display or select <i>Reset to Default</i> to display the default columns.

The following columns are available:

<b>State</b>	<p>The state of the AP:</p> <ul style="list-style-type: none"> <li>• Suppressed: red suppressed icon</li> <li>• Rogue: orange rogue icon</li> <li>• Accepted: green wireless signal mark</li> <li>• Unclassified: gray question mark</li> </ul>
<b>Status</b>	Whether the AP is active (green) or inactive (orange).
<b>SSID</b>	The wireless service set identifier (SSID) or network name for the wireless interface.
<b>Security Type</b>	The type of security currently being used.
<b>Channel</b>	The wireless radio channel that the access point uses.
<b>MAC Address</b>	The MAC address of the wireless interface.
<b>Vendor Info</b>	The name of the vendor.
<b>Signal Strength</b>	The relative signal strength of the AP.
<b>Detected By</b>	The name or serial number of the AP unit that detected the signal.
<b>On-Wire</b>	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.
<b>First Seen</b>	How long ago this AP was first detected. This column is not visible by default.

<b>Last Seen</b>	How long ago this AP was last detected. This column is not visible by default.
<b>Rate</b>	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*.
- 3. In the tree menu, go to *Device & Groups > Managed FortiGate (#)*, and 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 458](#).

2 Managed APs 0 Online 0 Offline 2 Unauthorized		
+ Create New	Edit	Delete
Assign Profile	More	Column Settings
Access Point	Connected Via	SSIDs
<input type="checkbox"/> FP320C3X15000146		
<input type="checkbox"/> FP320C3X15002273		

- 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.

2 Managed APs 2 Online 0 Offline 0 Unauthorized			
+ Create New	Edit	Delete	Assign Profile
More	Column Settings		
Access Point	Connected Via	SSIDs	Channel
<input type="checkbox"/> FP320C3X15000146	192.168.100.111		Radio 1: 1 Radio 2: 132
<input checked="" type="checkbox"/> FP320C3X15002273	192.168.100.112		Radio 1: 6 Radio 2: 140

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*.
2. In the tree menu, go to *Device & Groups > Managed FortiGate (#)*, and select a managed device. Alternatively, you can select a device in a group, see [FortiAP groups on page 458](#).
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:

<b>IP</b>	The IP address assigned to the wireless client.
<b>SSID</b>	The SSID that the client connected to.
<b>FortiAP</b>	The serial number of the FortiAP unit that the client connected to.
<b>Device</b>	The type of device that the client is using.
<b>Channel</b>	The wireless radio channel that is used.
<b>Bandwidth Tx/Rx</b>	Client received and transmitted bandwidth, in Kbps.
<b>Signal Strength/Noise</b>	The signal-to-noise ratio in dBs calculated from signal strength and noise level.
<b>Signal Strength</b>	The relative signal strength of the AP.
<b>Association Time</b>	How long the client has been connected to this access point.
<b>Authentication</b>	The type of authentication used.
<b>Bandwidth RX</b>	Client received bandwidth, in Kbps.
<b>Bandwidth TX</b>	Client transmitted bandwidth, in Kbps.
<b>Device OS</b>	The OS version on the FortiAP.
<b>Host Information</b>	The host name of the WiFi client, if available.
<b>Idle Time</b>	The amount of time that the client has been idle.
<b>Manufacturer</b>	The manufacturer of the client device.
<b>Rate</b>	The connection rate between the WiFi client and the AP.
<b>Name</b>	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 474](#).
3. Assign the profile to the managed AP. See [Assigning profiles to FortiAP devices on page 505](#).
4. Use the *Install Wizard* to install the changes to FortiGate. See [Install device settings only on page 122](#).

**To view the spectrum analysis for a managed AP:**

1. Go to *AP Manager*.
2. In the tree menu, go to *Device & Groups > Managed FortiGate (#)*, select a managed device. Alternatively, you can select a device in a group, see [FortiAP groups on page 458](#).
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
<b>Signal Interference</b>	The noise levels for each channel
<b>Signal Interference Spectrogram</b>	A spectrogram of 60 samples of noise levels for different channels at specific time intervals.
<b>Duty Cycle</b>	The extent of a non-WiFi device/neighbouring AP is interfering with the signal.
<b>Duty Cycle Spectrogram</b>	A spectrogram of 60 duty samples for each channel over a period of time
<b>Detected Interference</b>	The detected interference <i>Type</i> , <i>Frequency</i> , and <i>Last Detected</i> 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*.
2. In the tree menu, go to *Device & Groups > Managed FortiGate (#)*, and select a managed device. Alternatively, you can select a device in a group, see [FortiAP groups on page 458](#).
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.

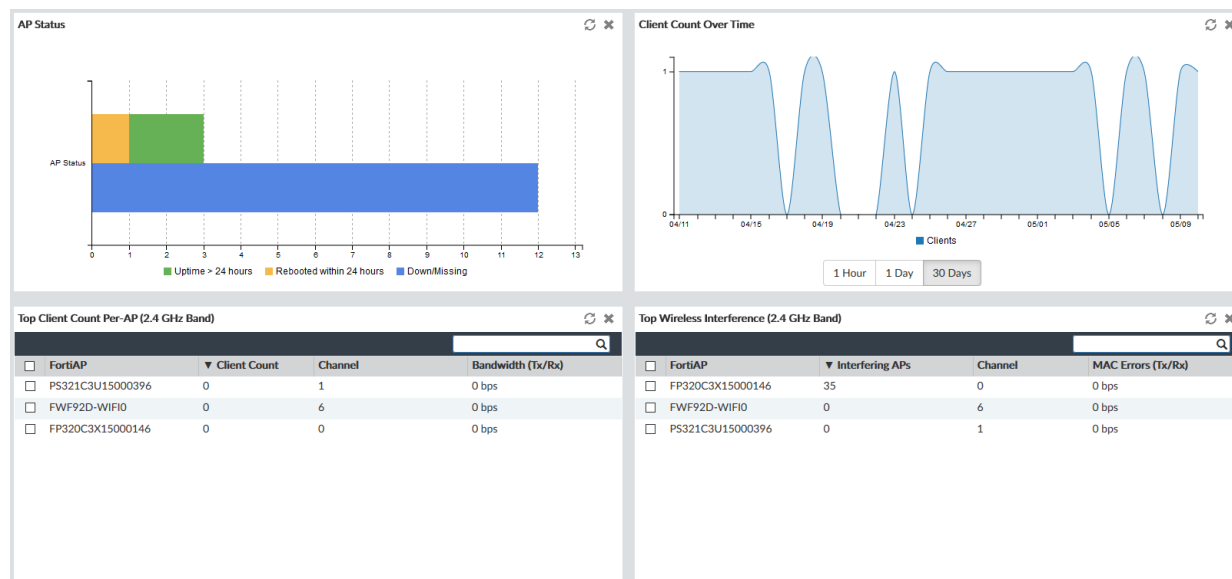
The following columns are available:

<b>IP</b>	The IP address assigned to the wireless client.
<b>SSID</b>	The SSID that the client connected to.
<b>FortiAP</b>	The serial number of the FortiAP unit that the client connected to.

<b>Device</b>	The type of device that the client is using.
<b>Channel</b>	The wireless radio channel that is used.
<b>Bandwidth TX/RX</b>	Client received and transmitted bandwidth, in Kbps.
<b>Signal Strength/Noise</b>	The signal-to-noise ratio in dBs calculated from signal strength and noise level.
<b>Signal Strength</b>	The relative signal strength of the AP.
<b>Association Time</b>	How long the client has been connected to this access point.
<b>Authentication</b>	The type of authentication used.
<b>Bandwidth RX</b>	Client received bandwidth, in Kbps.
<b>Bandwidth TX</b>	Client transmitted bandwidth, in Kbps.
<b>Device OS</b>	The OS version on the FortiAP.
<b>Host Information</b>	The host name of the WiFi client, if available.
<b>Idle Time</b>	The amount of time that the client has been idle.
<b>Manufacturer</b>	The manufacturer of the client device.
<b>Rate</b>	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*.
2. In the tree menu, go to *Device & Groups > Managed FortiGate (#)*, select a managed device. Alternatively, you can select a device in a group, see [FortiAP groups on page 458](#).
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:

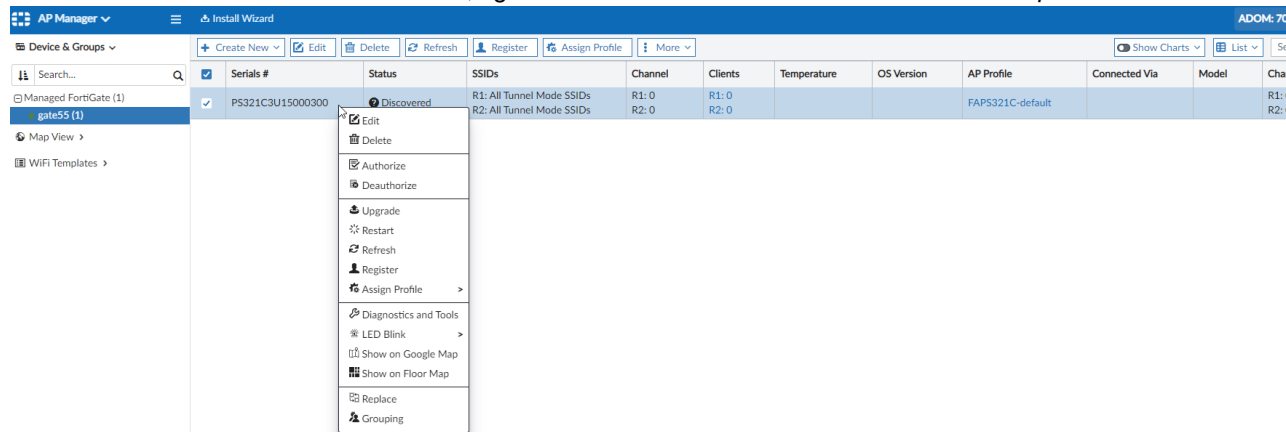
Widget	Description
<b>AP Status</b>	<p>Displays a bar graph of:</p> <ul style="list-style-type: none"> <li>• <i>Uptime &gt; 24 hours</i>: The number of APs that have been up for over 24 hours.</li> <li>• <i>Rebooted within 24 hours</i>: the number of APs that have been rebooted within the past 24 hours.</li> <li>• <i>Down/Missing</i>: Down or missing APs.</li> </ul> <p>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.</p> <p>Select the name of a column in the legend to add or remove it from the graph.</p> <p>This widget is only available when the <i>All FortiAPs</i> group is selected in the tree menu.</p>
<b>Client Count Over Time</b>	<p>A graph of the number of connected clients over the specified time period: 1 hour, 1 day, or 30 days.</p> <p>This widget is only available when the <i>All FortiAPs</i> group is selected in the tree menu.</p>
<b>Top Client Count Per-AP (2.4 GHz or 5 GHz Band)</b>	<p>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.</p>
<b>Top Wireless Interference (2.4 GHz or 5 GHz Band)</b>	<p>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.</p>
<b>Login Failures Information</b>	<p>Lists the time of a log in failure, the SSID involved, the Host Name/MAC, and the User Name.</p>

## Replacing APs

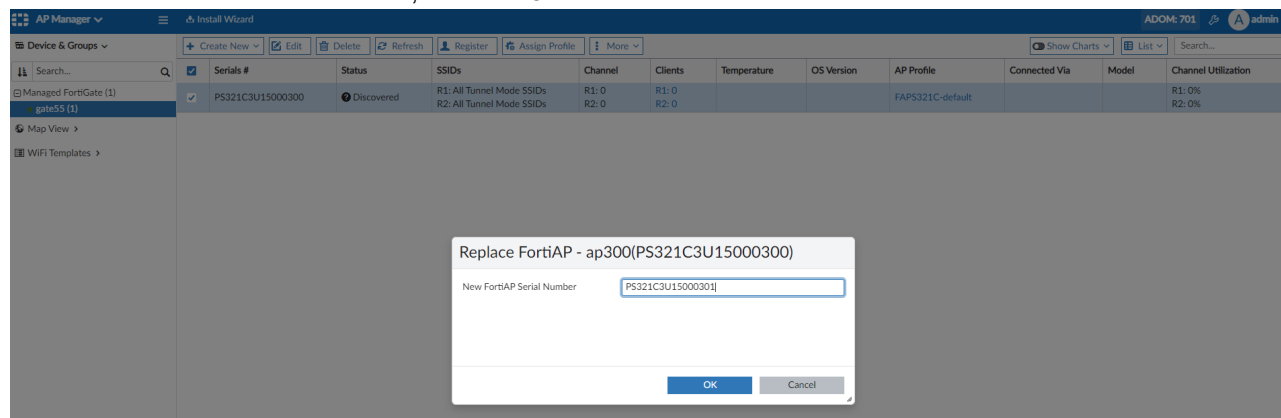
FortiAP devices can be replaced from the *AP Manager > Device & Groups* pane.

### To replace a FortiAP device:

1. Go to *AP Manager > Device & Groups*, and select a managed FortiGate.
2. Right-click on a FortiAP device in the table and click *Deauthorize*.
3. When the device's status is *Unauthorized*, right-click on the same FortiAP device and click *Replace*.

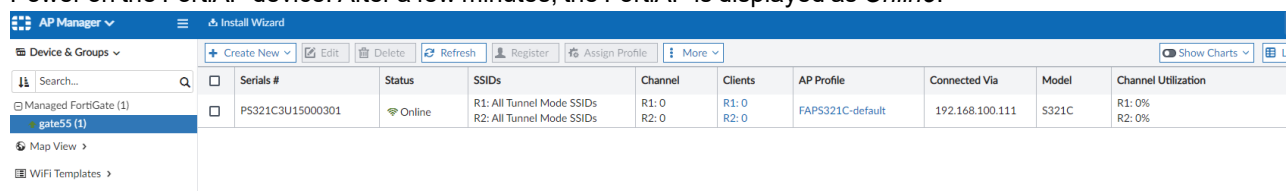


4. Enter the new FortiAP serial number, and click *OK*.



After the FortiAP has been replaced successfully, refresh the page and the new FortiAP is displayed.

5. Authorize the FortiAP device, then connect the FortiAP to the FortiGate.
6. Power on the FortiAP device. After a few minutes, the FortiAP is displayed as *Online*.



## Map view

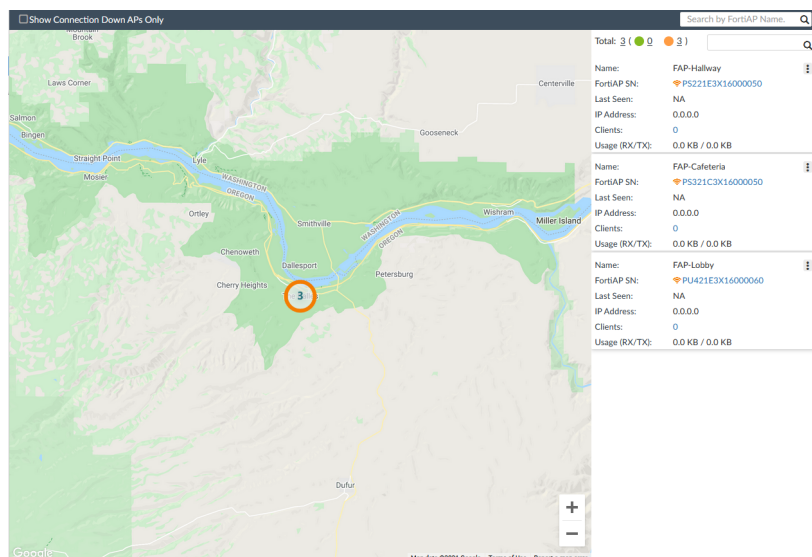
The *Map View* in AP Manager displays the global and local locations of your FortiAP devices.

There are two types of maps in *Map View*:

- **Google Map:** Shows all of the FortiGate devices on an interactive world map. See [Google map on page 468](#).
- **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 469](#)

## 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*.
2. In the tree menu, go to *Map View > Google Map*.
3. 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.
4. (Optional) In the toolbar, click *Connection Down APs Only*.
5. View the AP on a Google or floor map.

#### Google Map

In the *Name* row, click the AP name to zoom to the location on the map and view more information about the AP including the serial number, IP address, number of clients, usage, and the last time the AP was seen offline.

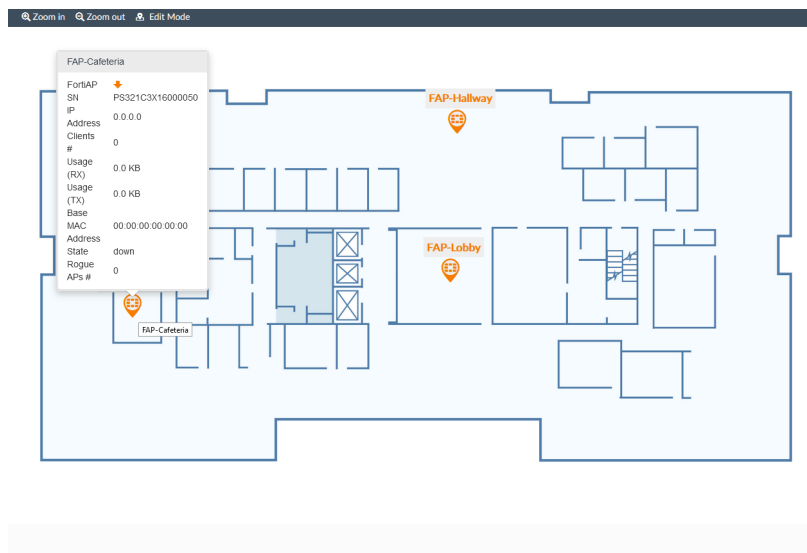
#### Floor Map

Click the options menu next to the AP *Name*, and click *Show on Floor Map*, to view AP's physical location.

6. In the *Clients* row, click the number to open the *View WiFi Clients* window. See [Connected clients on page 462](#).
7. In the *Serial Number* column, click the device serial number to open the *Config FortiAP* window, where you can edit the AP settings. See [Managing APs on page 453](#).

## 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 Templates

The WiFi Templates allow you to create and manage the following templates that can be assigned to managed FortiAP devices: access point (AP) settings, AP profile, SSIDs, Wireless Intrusion Detection System (WIDS), Bluetooth profile, Quality of Service (QoS), Bonjour profile, ARRP profile, and access control list. When per-device management is enabled, you can configure changes on each managed access point.

## WiFi profiles for central management

*WiFi Profiles* allows you to create and manage profiles that can be assigned to managed FortiAP devices.

---



Settings may vary for different ADOM versions.

---

**To use WiFi profiles in central management:**

1. Enable central management of access points.  
See [Enabling FortiAP central management on page 471](#).



2. Create profiles. AP Manager in central management includes the following profiles:

<b>SSIDs</b>	<ul style="list-style-type: none"> <li>• <a href="#">SSIDs on page 480</a></li> </ul>
<b>Operation Profiles</b>	<ul style="list-style-type: none"> <li>• <a href="#">FortiAP profiles on page 474</a></li> <li>• <a href="#">QoS profiles on page 496</a></li> <li>• <a href="#">FortiAP configuration profiles on page 506</a></li> </ul>
<b>Connectivity Profiles</b>	<ul style="list-style-type: none"> <li>• <a href="#">MPSK profiles on page 507</a></li> <li>• <a href="#">Bonjour profiles on page 498</a></li> <li>• <a href="#">Bluetooth profiles on page 493</a></li> </ul>
<b>Protection Profiles</b>	<ul style="list-style-type: none"> <li>• <a href="#">WIDS profiles on page 489</a></li> <li>• <a href="#">L3 Firewall Profiles on page 503</a></li> <li>• <a href="#">ARRP profiles on page 500</a></li> </ul>
<b>WiFi Settings</b>	<ul style="list-style-type: none"> <li>• <a href="#">WiFi settings on page 471</a></li> </ul>

3. Assign profiles to FortiAP devices.  
See [Assigning profiles to FortiAP devices on page 505](#).
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 460](#).

## 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 > All 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.

## 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 Profiles > WiFi Settings*.

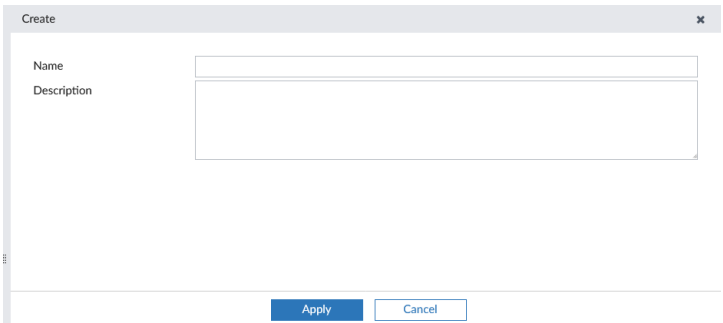
The following options are available in the toolbar and right-click menu:

<b>Create New</b>	Create a new AP settings profile.
<b>Edit</b>	Edit the selected AP settings profile.
<b>Delete</b>	Delete the selected AP settings profile.
<b>Assign to Device/Group</b>	Assign the selected AP settings profile to one or more devices.
<b>Clone</b>	Clone the selected AP settings profile.

**To create WiFi settings profiles:**

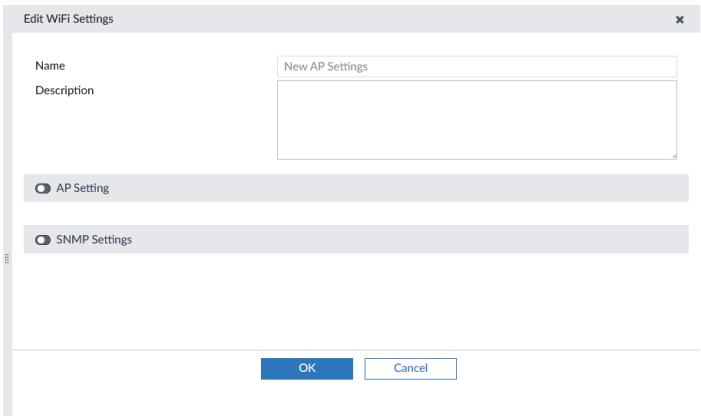
1. Ensure you are in the correct ADOM.
2. Go to *AP Manager > WiFi Profiles > WiFi Settings*.
3. In the toolbar, click *Create New*.

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 AP settings profile:

<b>Description</b>	Optionally, enter a description of the settings.
--------------------	--

<b>AP Setting</b>	Enable to access and set AP settings.
<b>WiFi country/region</b>	Select a country/region.
<b>FortiAP auto firmware provisioning</b>	When enabled, newly discovered FortiAPs will automatically be upgraded to the latest compatible firmware. This will happen once during authorization.
<b>Duplicate SSID</b>	Enable/disable allowing Virtual Access Points (VAPs) to use the same SSID name in the same VDOM (default = disable).
<b>DARRP Optimize Interval (seconds)</b>	Enter the time for running Dynamic Automatic Radio Resource Provisioning (DARRP) (0 to 86400, default = 86400).
<b>DARRP Optimize Schedule</b>	Select the schedule name. Firewall schedules for DARRP running time. DARRP will run periodically based on darrp-optimize within the schedules.
<b>Phishing SSID Detect</b>	Enable/disable phishing SSID detection (default = enable).
<b>Advanced Options</b>	Expand to display and set the advanced options. Hover the mouse over the <i>i</i> icon to view a tooltip of each advanced option. For more information, refer to the <i>FortiOS CLI Reference</i> .
<b>SNMP Profile</b>	Enable to access and set SNMP profile settings.
<b>Engine ID</b>	Enter the SNMP engine ID (maximum 24 characters).
<b>Contact Info</b>	Enter the contact information for the contact information for the SNMP (maximum 31 characters).
<b>CPU Usage Threshold</b>	Enter CPU usage when trap is sent (10 to 100, default = 80).
<b>Memory Usage Threshold</b>	Enter the memory usage when trap is sent (10 to 100, default = 80).
<b>User List</b>	Click <i>Create New</i> to create a new user. Select the following, then click <i>OK</i> : <ul style="list-style-type: none"> <li>• <i>Name</i>: Enter a name for the SNMP user.</li> <li>• <i>Current SNMP User</i>: Enable/disable this user.</li> <li>• <i>Queries</i>: Enable/disable SNMP queries for this user.</li> <li>• <i>Traps</i>: Enable/disable traps for this SNMP user.</li> <li>• <i>Authentication</i>: Select the security level for message authentication and encryption. Configure the authentication and encryption, as needed.</li> <li>• <i>Notify Host IP</i>: Enter the IPv4-address to configure SNMP User Notify Hosts.</li> </ul>
<b>Community List</b>	Click <i>Create New</i> to create a community. Select the following, then click <i>OK</i> : <ul style="list-style-type: none"> <li>• <i>ID</i>: Enter the ID for the community.</li> <li>• <i>Name</i>: Enter a name for the community.</li> </ul>

- *Current SNMP community*: Enable/disable this SNMP community.
- *V1 Queries*: Enable/disable SNMP v1 queries.
- *V2c Queries*: Enable/disable SNMP v2c queries.
- *V1 Traps*: Enable/disable SNMP v1 traps.
- *V2c Traps*: Enable/disable SNMP v2c traps.
- *Host list*: Create new hosts. Enter the IP/netmask for the SNMP manager (host).

#### To assign AP settings profiles to devices:

1. Select the AP 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.

#### To edit AP settings profiles:

1. Select the profile.
2. In the toolbar, click *Edit*.  
Alternatively, you can right-click the profile and select *Edit*, or double-click the profile.  
The *Edit AP Settings* pane opens.
3. Edit the settings as required. The name cannot be edited.
4. Click *OK* to apply your changes.

#### To delete AP settings profiles:

1. Select the profile to be deleted.
2. In the toolbar, click *Delete*.  
Alternatively, you can right-click the settings and select *Delete*.
3. Click *OK* in the confirmation dialog to delete the profile.

#### To clone AP settings profiles:

1. Select the profile to be cloned.
2. In the toolbar, click *More > Clone*.  
Alternatively, you can right-click the settings and select *Clone*.
3. Edit the name of the profile, and click *Apply*.  
The *Edit AP Settings* pane opens.
4. Edit the settings, and click *OK* to clone the profile.

## 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 FortiAP profiles can be created as needed for new devices.

When you create FortiAP profiles, you can select a Bluetooth profile and/or a WIDS profile.

### To view AP profiles:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager > WiFi Profiles > Operation Profiles > FortiAP Profiles*.

The following options are available in the toolbar and right-click menu:

<b>Create New</b>	Create a new AP profile.
<b>Edit</b>	Edit the selected AP profile.
<b>Delete</b>	Delete the selected AP profile.
<b>Clone</b>	Clone the selected AP profile.
<b>Where Used</b>	View where the selected AP profile is used.
<b>Import</b>	Import AP profiles from a connected FortiGate (toolbar only).

### To create custom AP profiles:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager > WiFi Profiles > 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:

<b>Name</b>	Type a name for the profile.
<b>Comment</b>	Optionally, enter comments.
<b>Platform</b>	Select the platform that the profile will apply to from the dropdown list.
<b>Indoor / Outdoor</b>	Select <i>Default (Indoor)</i> , <i>Indoor</i> , or <i>Outdoor</i> . The selection can affect the available channels due to regulatory rules.

<b>Country / Region</b>	Select the country or region from the drop-down list.
<b>AP Login Password</b>	Set, leave unchanged (default), or empty the AP login password.
<b>Administrative Access</b>	Allow management access to the managed AP via <i>telnet</i> , <i>http</i> , <i>https</i> , and/or <i>ssh</i> .
<b>Client Load Balancing</b>	Select the client load balancing methods to use: Frequency Handoff and/or AP Handoff.
<b>Bluetooth Profile</b>	If available for the platform, select a profile from the list or click the plus (+) to create a new Bluetooth profile.
<b>Radio 1 &amp; 2</b>	Configure the radio settings. The Radio 2 settings will only appear if the selected platform has two radios.
<b>Mode</b>	Select the radio operation mode: <ul style="list-style-type: none"><li>• <i>Disabled</i>: The radio is disabled. No further radio settings are available.</li><li>• <i>Access Point</i>: The device is an access point. See options below.</li><li>• <i>Dedicated Monitor</i>: The device is a dedicated monitor. See options below.</li><li>• <i>SAM</i>: The device is a station that can connect to a neighboring AP for connectivity and health check. See options below.</li></ul>

<b>Mode = Access Point</b>	<b>WIDS Profile</b>	Select a WIDS profile from the dropdown list. See <a href="#">WIDS profiles on page 489</a> .
	<b>Radio Resource Provision</b>	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.
	<b>ARRP Profile</b>	Select an Automatic Radio Resource Provisioning (ARRP) profile. See <a href="#">ARRP profiles on page 500</a> . This option is only available if <i>Radio Resource Provision</i> is enabled.
	<b>Band</b>	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.
	<b>Channel Width</b>	Select 20MHz or 40MHz channel width. This option is only available for 802.11n bands.
	<b>Channel Plan</b>	Select <i>Three Channels</i> or <i>Four Channels</i> to select predefined channels. Select <i>Custom</i> to specify custom channels.
	<b>Channels</b>	Available when <i>Channel Plan</i> is set to <i>Custom</i> . Select the channel or channels to include. The available channels depend on the selected platform and band.
	<b>Short Guard Interval</b>	Select to enable the short guard interval. This option is only available for 802.11n bands.
	<b>Transmit Power Mode</b>	Select <i>Percent</i> or <i>dBm</i> to specify the minimum and maximum power levels by percent or dBm. Select <i>Auto</i> to specify a range of dBm and allow the level to be automatically set within the range.
	<b>Transmit Power</b>	If <i>Transmit Power Mode</i> is <i>Percent</i> or <i>dBm</i> , specify the percentage or dBm of the total available power. If <i>Transmit Power Mode</i> is <i>Auto</i> , enter the power low and high values in dBm.
<b>Mode = Dedicated Monitor</b>	<b>SSIDs</b>	Manually choose the SSIDs that APs using this profile will carry, or let them be selected automatically.
	<b>Monitor Channel Utilization</b>	Enable/disable monitoring channel utilization.
	<b>WIDS Profile</b>	Select a WIDS profile from the dropdown list. See <a href="#">WIDS profiles on page 489</a> .

<b>Mode = SAM</b>	<b>SSID</b>	Enter the SSID for the WiFi network.
	<b>BSSID</b>	Enter the BSSID for the WiFi network.
	<b>Security Type</b>	Select <i>Open</i> , <i>WPA/WPA2 Personal</i> , or <i>WPA/WPA2 Enterprise</i> for the WiFi network.
	<b>WiFi Username</b>	Enter the WiFi username. This option is only available if <i>Security Type = WPA/WPA2 Personal</i> .
	<b>WiFi Password</b>	Enter the WiFi password. This option is not available if <i>Security Type = Open</i> .
	<b>Captive Portal Authentication</b>	Enable/disable captive portal authentication. This option is not available if <i>Security Type = WPA/WPA2 Enterprise</i> .
	<b>Test Type</b>	Select <i>ping</i> or <i>Iperf</i> for the SAM test type.
	<b>Test Server Type</b>	Select <i>ip</i> or <i>fqdn</i> for the SAM server type.
	<b>Test Server</b>	Enter the SAM IP address or the FQDN according to the Test Server Type.
	<b>Iperf Server Port</b>	Enter the Iperf service port number.
	<b>Iperf Protocol</b>	Select <i>UDP</i> or <i>TCP</i> for the Iperf test protocol.
	<b>Report Interval (seconds)</b>	Enter the SAM report interval in seconds (60-864000, default = 0). Enter 0 for a one-time report.
<b>System Log</b>		
	<b>Syslog Profile</b>	Click the add icon to create a new syslog profile.
<b>LAN Configuration</b>		
	<b>Port ESL Mode</b>	Select <i>Offline</i> , <i>NAT to WAN</i> , <i>Bridge to WAN</i> , or <i>Bridge to SSID</i> .
	<b>Port ESL SSID</b>	Available when <i>Port ESL Mode</i> is set to <i>Bridge to SSID</i> . Select the SSID.
	<b>Handoff STA Thresh</b>	Threshold value for AP handoff (default = 55).
	<b>WAN Port Mode</b>	Enable/disable using a WAN port as a LAN port. Select <i>wan-lan</i> or <i>wan-only</i> (default = <i>wan-only</i> ).
<b>ESL SES Dongle Configuration</b>		
	<b>APC FQDN</b>	Enter the FQDN of the ESL SES-imagotag Access Point Controller (APC).
<b>Location Based Services</b>		
<b>FortiPresence</b>		
<b>Mode</b>	Select the FortiPresence mode: <ul style="list-style-type: none"> <li>• <i>Disable</i></li> <li>• <i>Foreign channels only</i></li> <li>• <i>Foreign and home channels</i></li> </ul>	
<b>Project name</b>	The FortiPresence project name.	



<b>Password</b>	FortiPresence secret password.
<b>FortiPresence Server Type</b>	Select <i>IP</i> or <i>FQDN</i> .
<b>FortiPresence server IP/FQDN</b>	FortiPresence server IP address or FQDN.
<b>FortiPresence server port</b>	FortiPresence server UDP listening port (default = 3000).
<b>Report rogue APs</b>	Enable/disable FortiPresence reporting of Rogue APs.
<b>Report unassociated clients</b>	Enable/disable FortiPresence reporting of unassociated devices.
<b>Report transmit frequency (in seconds)</b>	FortiPresence report transmit frequency, in seconds (5 - 65535, default = 30).
<b>Ekahau blink</b>	Enable/disable Ekahau blink location based services.
<b>RTLS controller server IP</b>	Enter the realtime location services (RTLS) controller server IP address.
<b>RTLS controller server port</b>	The RTLS controller server port (default = 8569).
<b>Ekahau tag MAC address</b>	Enter the Ekahau tag MAC address.
<b>AeroScout</b>	Enable/disable AeroScout location based services.
<b>AeroScout server IP</b>	Enter the AeroScout server IP address.
<b>AeroScout server port</b>	Enter the AeroScout server port.
<b>MU mode dilution factor</b>	Enter the MU mode dilution factor (default = 20).
<b>MU mode dilution timeout</b>	Enter the MU mode dilution timeout (default = 5).
<b>Locate WiFi clients when not connected</b>	Enable/disable locating WiFi client when they are not connected.
<b>Advanced Options</b>	Expand to display and set the advanced options. Hover the mouse over the <i>i</i> icon to view a tooltip of each advanced option. For more information, refer to the <i>FortiOS CLI Reference</i> .

#### To edit a custom AP profile:

1. Select the profile.
2. In the toolbar, click *Edit*.

Alternatively, you can right-click the profile and select *Edit*, or you can double-click the profile.

The *Edit AP Profile* pane opens.

3. Edit the settings as required. The profile name cannot be edited.
4. Click *OK* to apply your changes.

#### **To delete custom AP profiles:**

1. Select the AP profile or profiles to be deleted. Default profiles cannot be deleted.
2. In the toolbar, click *Delete*.  
Alternatively, you can right-click the profile and select *Delete*.
3. Click *OK* in the confirmation dialog to delete the profile.

#### **To clone a custom AP profile:**

1. Select the profile to be cloned.
2. In the toolbar, click *Clone*.  
Alternatively, you can right-click the 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 view where an AP 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*.

#### **To import a AP 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 the profile(s).
4. Click *OK* to import the profile or profiles.



AP profiles can also be imported through the Device Manager. See [Importing AP profiles and FortiSwitch templates on page 119](#).

---

## **SSIDs**

You can use the AP Manager to create and manage SSID groups.

**To view SSIDs and SSID groups:**

1. Go to *AP Manager*.
2. In the tree menu, go to *Wifi Templates > SSIDs*.

The following options are available in the toolbar and right-click menu:

<b>Create New</b>	Create a new SSID (see <a href="#">Creating SSIDs on page 482</a> ) or SSID group.
<b>Edit</b>	Edit the selected SSID or group.
<b>Clone</b>	Clone the selected SSID or group.
<b>Delete</b>	Delete the selected SSID or group.
<b>Import</b>	Import SSIDs from a connected FortiGate (toolbar only).
<b>Where Used</b>	View where the SSID is used.
<b>Column Settings</b>	Adjust the visible columns.

**To create a new SSID group:**

1. In the toolbar, click *Create New > SSID Group*. The *Create New SSID Group* window 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 an 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.

**To create a new SSID:**

1. Go to *AP Manager*.
2. In the tree menu, go to *Wifi Templates > SSID*.
3. In the toolbar, click *Create New > SSID*. The *Create New SSID Profile* windows opens.

4. Enter the following information, then click *OK* to create the new tunnel to wireless controller SSID:

**Interface Name**

Type a name for the SSID.

<b>Alias</b>	Set the alias for SSID.																		
<b>Traffic Mode</b>	Select the traffic mode: <i>Tunnel</i> , <i>Bridge</i> , or <i>Mesh</i> .																		
<b>Address</b>	These options are only available when <i>Traffic Mode</i> is <i>Tunnel</i> .																		
<b>IP/Network Mask</b>	Enter the IP address and netmask.																		
<b>IPv6 Address</b>	Enter the IPv6 address.																		
<b>Administrative Access</b>	Select the allowed administrative service protocols.																		
<b>IPv6 Administrative Access</b>	Select the allowed administrative service protocols.																		
<b>DHCP Server</b>	Turn the DHCP server on or off.																		
<b>WiFi Settings</b>																			
<b>SSID</b>	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.																		
<b>Security Mode</b>	<p>Select a security mode:</p> <table> <tr> <td><i>Captive Portal</i></td><td><i>WPA Only Personal</i></td></tr> <tr> <td><i>OPEN</i></td><td><i>WPA Only Personal Captive Portal</i></td></tr> <tr> <td><i>Osen</i></td><td><i>OWE</i></td></tr> <tr> <td><i>WPA Personal</i></td><td><i>WEP 128</i></td></tr> <tr> <td><i>WPA Personal Captive Portal</i></td><td><i>WEP 64</i></td></tr> <tr> <td><i>WPA2 Only Enterprise</i></td><td><i>WPA Enterprise</i></td></tr> <tr> <td><i>WPA2 Only Personal</i></td><td><i>WPA Only Enterprise</i></td></tr> <tr> <td><i>WPA2 Only Personal Captive Portal</i></td><td><i>WPA3 Enterprise</i></td></tr> <tr> <td><i>WPA3 SAE</i></td><td><i>WPA3 SAE Transition</i></td></tr> </table> <p>Only WPA and WPA2 Personal modes are available when the traffic mode is <i>Mesh</i>.</p>	<i>Captive Portal</i>	<i>WPA Only Personal</i>	<i>OPEN</i>	<i>WPA Only Personal Captive Portal</i>	<i>Osen</i>	<i>OWE</i>	<i>WPA Personal</i>	<i>WEP 128</i>	<i>WPA Personal Captive Portal</i>	<i>WEP 64</i>	<i>WPA2 Only Enterprise</i>	<i>WPA Enterprise</i>	<i>WPA2 Only Personal</i>	<i>WPA Only Enterprise</i>	<i>WPA2 Only Personal Captive Portal</i>	<i>WPA3 Enterprise</i>	<i>WPA3 SAE</i>	<i>WPA3 SAE Transition</i>
<i>Captive Portal</i>	<i>WPA Only Personal</i>																		
<i>OPEN</i>	<i>WPA Only Personal Captive Portal</i>																		
<i>Osen</i>	<i>OWE</i>																		
<i>WPA Personal</i>	<i>WEP 128</i>																		
<i>WPA Personal Captive Portal</i>	<i>WEP 64</i>																		
<i>WPA2 Only Enterprise</i>	<i>WPA Enterprise</i>																		
<i>WPA2 Only Personal</i>	<i>WPA Only Enterprise</i>																		
<i>WPA2 Only Personal Captive Portal</i>	<i>WPA3 Enterprise</i>																		
<i>WPA3 SAE</i>	<i>WPA3 SAE Transition</i>																		
<b>Pre-shared Key Mode</b>	<p>Select <i>Single</i> to specify a single passphrase.</p> <p>Select <i>Multiple</i> to specify a multiple pre-shared key group.</p>																		
<b>Passphrase</b>	<p>When <i>Pre-shared Key Mode</i> is set to <i>Single</i>, enter the pre-shared key for the SSID.</p> <p>This option is only available when the security mode includes WPA or WPA2 personal.</p>																		
<b>Local Standalone</b>	<p>Enable/disable AP local standalone (default = disable).</p> <p>This option is only available when the traffic mode is <i>Bridge</i>.</p>																		
<b>Local Authentication</b>	<p>Enable/disable AP local authentication.</p> <p>This option is only available when the traffic mode is <i>Bridge</i>.</p>																		
<b>Client Limit</b>	The maximum number of clients that can simultaneously connect to the AP (0 - 4294967295, default = 0, meaning no limitation).																		

<b>Client Limit per Radio</b>	<p>The maximum number of clients that can simultaneously connect to each radio (0 - 4294967295, default = 0, meaning no limitation).</p> <p>This option is only available when <i>Local Standalone</i> is enabled.</p>
<b>Multiple Pre-Shared Keys</b>	<p>Enable/disable multiple pre-shared keys.</p> <p>In the table, click <i>Create</i> to create a new key. Enter the key name, value, client limit, and comments (optional), then click <i>OK</i>. Click <i>Edit</i> to edit the selected key. Click <i>Delete</i> to delete the selected key or keys.</p> <p>This option is only available when the security mode includes WPA or WPA2 personal and the traffic mode is not <i>Mesh</i>.</p>
<b>Default Client Limit Per Key</b>	<p>Enable/disable a maximum number of clients that can simultaneously connect using each pre-shared key, then enter the maximum number.</p> <p>This option is only available when the <i>Multiple Pre-Shared Keys</i> is enabled.</p>
<b>Portal Type</b>	<p>Select the portal type: <i>Authentication</i> (default), <i>Disclaimer + Authentication</i>, <i>Disclaimer Only</i>, or <i>Email Collection</i>.</p> <p>This option is only available when the security mode includes captive portal.</p>
<b>Authentication Portal</b>	<p>Select <i>Local</i> or <i>External</i>. If <i>External</i> is selected, enter the URL of the portal.</p> <p>This option is only available when the portal type includes authentication.</p>
<b>User Groups</b>	<p>Select the user group to add from the dropdown list. Select the plus symbol to add multiple groups.</p> <p>This option is only available when the portal type includes authentication.</p>
<b>Exempt Sources</b>	<p>Select exempt sources to add from the dropdown list.</p> <p>This option is only available when the portal type includes authentication.</p>
<b>Devices</b>	<p>Select exempt devices to add from the dropdown list.</p> <p>This option is only available when the portal type includes authentication.</p>
<b>Exempt Destinations</b>	<p>Select exempt destinations to add from the dropdown list.</p> <p>This option is only available when the portal type includes authentication.</p>
<b>Exempt Services</b>	<p>Select exempt services to add from the dropdown list.</p> <p>This option is only available when the portal type includes authentication.</p>
<b>Customize Portal Messages</b>	<p>Select to allow for customized portal messages. Portal messages cannot be customized until after the interface has been created.</p> <p>This option is only available when the portal type includes disclaimer, email collection, or CMCC without MAC authentication.</p>
<b>Redirect after Captive Portal</b>	<p>Select <i>Original Request</i> or <i>Specific URL</i>. If <i>Specific URL</i> is selected, enter the redirect URL.</p> <p>This option is only available when the security mode includes captive portal.</p>

<b>Authentication</b>	Select the authentication method for the SSID, either <i>Local</i> or <i>RADIUS Server</i> , then select the requisite server or group from the dropdown list. This option is only available when the security mode includes WPA or WPA2 enterprise.
<b>Broadcast SSID</b>	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.
<b>Schedule</b>	Select a schedule to control the availability of the SSID. For information on creating a schedule object, see <a href="#">Create a new object on page 403</a> .
<b>Access Control List</b>	Select an access control list profile from the drop-down list. See <a href="#">L3 Firewall Profiles on page 503</a> .
<b>Block Intra-SSID Traffic</b>	Enable/disable blocking communication between clients of the same AP (default = disable).
<b>Broadcast Suppression</b>	Optional suppression of broadcast message types: <ul style="list-style-type: none"> <li>• <i>All other broadcast</i>: All other broadcast messages</li> <li>• <i>All other multicast</i>: All other multicast messages</li> <li>• <i>ARP poison</i>: ARP poison messages from wireless clients</li> <li>• <i>ARP proxy</i>: ARP requests for wireless clients as a proxy</li> <li>• <i>ARP replies</i>: ARP replies from wireless clients</li> <li>• <i>ARPs for known clients</i>: ARP for known messages</li> <li>• <i>ARPs for unknown clients</i>: ARP for unknown messages</li> <li>• <i>DHCP downlink</i>: Downlink DHCP messages</li> <li>• <i>DHCP starvation</i>: DHCP starvation req messages</li> <li>• <i>DHCP uplink</i>: Uplink DHCP messages</li> <li>• <i>IPv6</i>: IPv6 packets</li> <li>• <i>NetBIOS datagram service</i>: NetBIOS datagram services packets</li> <li>• <i>NetBIOS name service</i>: NetBIOS name services packets</li> </ul>
<b>Filter Clients by MAC Address</b>	Enable/disable using a RADIUS server to filter clients by MAC address, then select the server from the drop-down list. See <a href="#">RADIUS servers on page 869</a> for information on adding a RADIUS server.
<b>VLAN Pooling</b>	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. <ul style="list-style-type: none"> <li>• <i>Managed AP Group</i>: Select devices to include in the group.</li> <li>• <i>Round Robin</i></li> <li>• <i>Hash</i></li> </ul> This option is not available when the traffic mode is <i>Mesh</i> .
<b>Quarantine Host</b>	Enable/disable station quarantine (default = enable). This option is only available when the security mode includes WPA or WPA2.
<b>Encrypt</b>	Select the data encryption protocol: <ul style="list-style-type: none"> <li>• <i>TKIP</i>: Temporal Key Integrity Protocol, used by the older WPA standard.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>AES:</b> Advanced Encryption Standard, commonly used with the newer WPA2 standard (default).</li> <li>• <b>TKIP-AES:</b> 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.</li> </ul>
<b>QoS Profile</b>	Select the QoS profile from the drop-down list. See <a href="#">QoS profiles on page 496</a> .
<b>Advanced Options</b>	Configure advanced options. For information, see the <i>FortiOS CLI Reference</i> .
<b>Per-Device Mapping</b>	Enable per-device mapping to override the SSID profile settings for selected devices. See <a href="#">Adding SSID per-device mapping on page 486</a> .



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 486](#).

## Adding SSID per-device mapping

To add SSID per-device mapping:

1. Go to *AP Manager*.
2. In the tree menu, go to *Wifi Templates > SSID*.
3. Double-click an SSID to edit it, or right-click the SSID and select *Edit*.
4. Enable *Per-Device Mapping*.
5. Click *Create New* in the per-device mapping toolbar. The *Per-Device Mapping* dialog-box opens.



6. Configure the following settings and click OK.

The screenshot shows the 'Per-Device Mapping' dialog box with the following settings:

- Mapped Device:** Click to select
- Mapped IP/Netmask:** 0.0.0.0/0.0.0.0
- Mapped DHCP Server:** OFF (Server, Relay buttons are visible)
- IP Range:** Start IP, End IP (No record found)
- Network Mask:** Same as Interface (Specify button)
- Default Gateway:** Same as Interface (Specify button)
- Next Server:** 0.0.0.0
- DNS Service:** Specify (Use System DNS Setting (Default), Same as Interface IP (Local) buttons)
- NTP Service:** Specify (Use System NTP Setting (Default), Use FortiGate as NTP Server (Local) buttons)
- FortiClient On-Net Status:** ON
- Timezone Option:** Specify (Disable, Default buttons)
- IP Address Assignment Rules:**
  - Type:** Implicit
  - Match Criteria:** Unknown MAC address
  - Action:** Assign IP
- Advanced... (DNS, WINS, Custom Options, Exclude Ranges.)** >
- Security Mode:** WPA2 Personal

Buttons: OK, Cancel



<b>Mapped Device</b>	Select the device to be mapped from the drop-down.
<b>Mapped IP/NetMask</b>	Specify the Mapped IP/NetMask.
<b>Mapped DHCP Server</b>	Set the <i>DHCP Server</i> to <i>ON</i> if you want to map a DHCP Server to this device.
<b>Address Range</b>	Configure address ranges for DHCP. Click <i>Create</i> to create a new range. Ranges can also be edited and deleted as required. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i> .
<b>Netmask</b>	Enter the netmask. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i> .
<b>Default Gateway</b>	Configure the default gateway: <i>Same as Interface IP</i> , or <i>Specify</i> . If set to <i>Specify</i> , enter the gateway IP address in the field. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i> .
<b>DNS Server</b>	Configure the DNS server: <i>Same as System DNS</i> , <i>Same as Interface IP</i> , or <i>Specify</i> . This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i> .
<b>Mode</b>	Select the DHCP mode: <i>Server</i> or <i>Relay</i> . This option is only available when <i>DHCP Server</i> is <i>ON</i> .
<b>NTP Server</b>	Configure the NTP server: <i>Local</i> , <i>Same as System NTP</i> , or <i>Specify</i> . If set to <i>Specify</i> , enter the NTP server IP address in the field. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i> .
<b>Time Zone</b>	Configure the timezone: <i>Disable</i> , <i>Same as System</i> , or <i>Specify</i> . If set to <i>Specify</i> , select the timezone from the dropdown list. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i> .
<b>Next Bootstrap Server</b>	Enter the IP address of the next bootstrap server. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i> .
<b>Additional DHCP Options</b>	In the <i>Lease Time</i> field, enter the lease time, in seconds (default = 604800 (7 days)). Add DHCP options to the table. For details, see <a href="#">Adding additional DHCP options on page 488</a> . Options can also be edited and deleted as required. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i> .
<b>MAC Reservation + Access Control</b>	Select the action to take with unknown MAC addresses: <i>assign</i> or <i>block</i> . Add MAC address actions to the table. For details, see <a href="#">Adding a MAC address reservation on page 489</a> . Reservations can also be edited and deleted as required. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i> .
<b>DHCP Server IP</b>	Enter the DHCP server IP address. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Relay</i> .
<b>Type</b>	Select the type: <i>Regular</i> , or <i>IPsec</i> . This option is only available when <i>DHCP Server</i> is <i>ON</i> .

## 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*.
2. In the tree menu, go to *WiFi Templates > SSID*. The *SSID* pane opens.
3. Create a new SSID profile, or double-click a profile in the list to edit it.
4. Ensure *DHCP Server* is enabled.

The screenshot shows the 'Create New SSID Profile' dialog box. The 'Interface Name' field is empty. The 'Traffic Mode' is set to 'Tunnel'. The 'Address' section shows 'IP/Network Mask' as '0.0.0.0/0.0.0.0' and 'IPv6 Address' as empty. The 'Administrative Access' section has checkboxes for HTTPS, SNMP, FMG-Access, PING, HTTP, Auto-Ipssec, SSH, TELNET, and RADIUS Accounting. The 'IPv6 Administrative Access' section has checkboxes for HTTPS, SNMP, Any, PING, HTTP, and FMG-Access. The 'DHCP Server' section has buttons for 'OFF', 'Server', and 'Relay', with 'Server' being the selected option.

5. Expand *Advanced...(DNS, WINS, Custom Options, Exclude Ranges.)*.

The screenshot shows the 'Advanced...(DNS, WINS, Custom Options, Exclude Ranges.)' section. It includes a table for 'IP Address Assignment Rules' with columns for 'Type', 'Match Criteria', 'Action', 'IP', and 'Description'. Below the table, there are sections for 'Networked Devices' and 'Device Detection'.

6. In the *Options* toolbar, click *Create New*. The *Create New Options* dialog opens.

The screenshot shows the 'Create New Options' dialog box. It includes fields for 'Domain', 'Lease Time', 'File Name', 'TFTP Server', 'IP Assignment Mode', 'WINS Server 1', and 'WINS Server 2'. Below these fields, there is a section for 'Options' with a table for 'Option Code', 'Type', and 'Value'. The 'Create New' button is highlighted.

7. Configure the additional DHCP options.

<b>Option Code</b>	Enter the option code.
<b>Type</b>	Select <i>HEX</i> , <i>String</i> , <i>IP</i> , or <i>FQDN</i>
<b>Value</b>	Enter the corresponding hexadecimal value.

The screenshot shows the 'Create New Options' dialog box. It includes fields for 'Option Code', 'Type', and 'Value'. The 'Type' is set to 'String'. The 'OK' and 'Cancel' buttons are at the bottom.

8. 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*.
2. In the tree menu, go to *WiFi Templates > SSID*. The *SSID* pane opens.
3. Create a new SSID profile, or double-click a profile in the list to edit it.
4. Ensure *DHCP Server* is enabled.

The screenshot shows the 'Create New SSID Profile' dialog box. It has several sections: 'Interface Name' with a text field, 'Alias' with a text field, 'Traffic Mode' with buttons for Tunnel, Bridge, and Mesh (Tunnel is selected), 'Address' with fields for IP/Network Mask (0.0.0.0/0.0.0.0) and IPv6 Address, 'Administrative Access' with checkboxes for HTTPS, SNMP, FMG-Access, PING, HTTP, Auto-Ipssec, SSH, TELNET, and RADIUS Accounting, 'IPv6 Administrative Access' with checkboxes for HTTPS, SNMP, Any, PING, HTTP, and FMG-Access, and 'DHCP Server' with buttons for OFF, Server (selected), and Relay.

5. In the *IP Address Assignment Rules* toolbar, click *Create New*. The *Create New IP Address Assignment Rule* dialog opens.

The screenshot shows the 'IP Address Assignment Rules' toolbar. It has a search bar and buttons for '+ Create New', 'Edit', and 'Delete'. Below the toolbar is a table with columns 'Type', 'Match Criteria', and 'Action'. The table contains one row with 'Implicit' type, 'Unknown MAC address' match criteria, and 'Assign IP' action.

6. Configure IP Address Assignment Rule.

Type	Select <i>MAC Address</i> .
MAC Address	Enter the MAC address.
Action	Select <i>Reserve IP</i> .
IP	Enter the IP address.
Description	(Optional) Enter a description of the Assignment Rule.

The screenshot shows the 'Create New IP Address Assignment Rule' dialog box. It has fields for 'Type' (MAC Address selected), 'MAC Address' (00:00:00:00:00:00), 'Action' (Assign IP, Block, Reserve IP selected), 'IP' (0.0.0.0), and 'Description' (0/255). There are 'OK' and 'Cancel' buttons at the bottom.

7. Click *OK*.

# 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 > WiFi Profiles > Protection Profiles > WIDS Profile*.

The following options are available in the toolbar and right-click menu:

<b>Create New</b>	Create a new WIDS profile.
<b>Edit</b>	Edit the selected WIDS profile.
<b>Delete</b>	Delete the selected WIDS profile.
<b>Clone</b>	Clone the selected WIDS profile.
<b>Where Used</b>	Displays the ADOM where the profile is used as well as the Policy Package/Block.
<b>Import</b>	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 > WiFi Profiles > Protection Profiles > WIDS Profile*.
3. In the toolbar, click *Create New*.

The *Create New WIDS Profile* pane opens.

Create New WIDS Profile

Name

Comments

Sensor Mode

Enable Rogue AP Detection

Intrusion Detection Settings

Intrusion Type	Enable	Threshold	Interval (Seconds)
Asleep Attack	<input type="button" value="OFF"/>		
Association Frame Flooding	<input type="button" value="OFF"/>	30	10
Authentication Frame Flooding	<input type="button" value="OFF"/>	30	10
Broadcasting Deauthentication	<input type="button" value="OFF"/>		
EAPOL-FAIL Flooding (to AP)	<input type="button" value="OFF"/>	10	1
EAPOL-LOGOFF Flooding (to AP)	<input type="button" value="OFF"/>	10	1
EAPOL-START Flooding (to AP)	<input type="button" value="OFF"/>	10	1
EAPOL-SUCC Flooding (to AP)	<input type="button" value="OFF"/>	10	1
Invalid MAC OUI	<input type="button" value="OFF"/>		
Long Duration Attack	<input type="button" value="OFF"/>	8200	μs
Null SSID Probe Response	<input type="button" value="OFF"/>		
Premature EAPOL-FAIL Flooding (to Client)	<input type="button" value="OFF"/>	10	1
Premature EAPOL-SUCC Flooding (to Client)	<input type="button" value="OFF"/>	10	1
Spoofed Deauthentication	<input type="button" value="OFF"/>		
Weak WEP IV (Initialization Vector)	<input type="button" value="OFF"/>		
Wireless Bridge	<input type="button" value="OFF"/>		

Advanced Options >

4. Enter the following information, and click *OK* to create the WIDS profile:

<b>Name</b>	Enter a name for the profile.
<b>Comments</b>	Optionally, enter comments.

<b>Sensor Mode</b>	
<b>Enable Rogue AP Detection</b>	Select to enable rogue AP detection.
<b>Background Scan Every</b>	Enter the number of seconds between background scans.
<b>Enable Passive Scan Mode</b>	Enable/disable passive scan mode.
<b>Auto Suppress Rouge APs in Foreground Scan</b>	Enable/disable automatically suppressing rogue APs in foreground scans. This options is only available when the sensor mode is not disabled.
<b>Disable Background Scan During Specified Time</b>	Enable/disable background scanning during the specified time. Specify the days of week, and the start and end times.
<b>Intrusion Type</b>	
<b>Enable</b>	Select to enable the intrusion type.
<b>Threshold</b>	If applicable, enter a threshold for reporting the intrusion, in seconds except where specified.
<b>Interval (Seconds)</b>	If applicable, enter the interval for reporting the intrusion, in seconds.
<b>Advanced Options</b>	
<b>ap-bgscan-duration</b>	Listening time on a scanning channel, in milliseconds (10 - 1000, default = 20).
<b>ap-bgscan-idle</b>	Waiting time for channel inactivity before scanning this channel, in milliseconds (0 - 1000, default = 0).
<b>ap-bgscan-intv</b>	Period of time between scanning two channels, in seconds (1 - 600, default = 1).
<b>ap-bgscan-report-intv</b>	Period of time between background scan reports, in seconds (15 - 600, default = 30).
<b>ap-fgscan-report-intv</b>	Period of time between foreground scan reports, in seconds (15 - 600, default = 15).
<b>deauth-broadcast</b>	Enable/disable broadcasting deauthentication detection (default = disable).
<b>deauth-unknown-src-thresh</b>	Threshold value per second to deauthenticate unknown sources for DoS attacks, in seconds (0 - 65535, 0 = no limit, default = 10).
<b>invalid-mac-oui</b>	Enable/disable invalid MAC OUI detection (default = disable).

### Intrusion types

Intrusion Type	Description
<b>Asleep Attack</b>	ASLEAP is a tool used to perform attacks against LEAP authentication.

Intrusion Type	Description
<b>Association Frame Flooding</b>	A Denial of Service attack using association requests. The default detection threshold is 30 requests in 10 seconds.
<b>Authentication Frame Flooding</b>	A Denial of Service attack using association requests. The default detection threshold is 30 requests in 10 seconds.
<b>Broadcasting Deauthentication</b>	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.
<b>EAPOL Packet Flooding (to AP)</b>	<p>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.</p> <p>Several types of EAPOL packets can be detected:</p> <ul style="list-style-type: none"> <li>• EAPOL-FAIL</li> <li>• EAPOL-LOGOFF</li> <li>• EAPOL-START</li> <li>• EAPOL-SUCC</li> </ul>
<b>Invalid MAC OUI</b>	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.
<b>Long Duration Attack</b>	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.
<b>Null SSID Probe Response</b>	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.
<b>Premature EAPOL Packet Flooding (to client)</b>	<p>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.</p> <p>Two types of EAPOL packets can be detected:</p> <ul style="list-style-type: none"> <li>• EAPOL-FAIL</li> <li>• EAPOL-SUCC</li> </ul>
<b>Spoofed Deauthentication</b>	Spoofed de-authentication frames form the basis for most denial of service attacks.
<b>Weak WEP IV Detection</b>	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.
<b>Wireless Bridge</b>	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.

**To edit a WIDS 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.  
The *Edit WIDS* dialog opens.
3. Edit the settings as required.
4. Click *OK* to apply your changes.

**To delete WIDS profiles:**

1. Select the profile or profiles to be deleted from the profile list.
2. In the toolbar click *Delete*.  
Alternatively, right-click and select *Delete*.  
The *Delete WIDS Profile(s)* dialog opens.
3. Click *OK*.

**To clone a WIDS profile:**

1. Select a profile to clone.
2. In the toolbar click *Clone*.  
Alternatively, right-click and select *Clone*.
3. Edit the name of the profile, then edit the remaining settings as required.
4. Click *OK*.

**To import a WIDS 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 the profile(s).
4. Click *OK*.

## 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 Bluetooth 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 > WiFi Templates > Connectivity Profiles > Bluetooth Profile*.

The following options are available in the toolbar and right-click menu:

<b>Create New</b>	Create a new Bluetooth profile.
<b>Edit</b>	Edit the selected Bluetooth profile.
<b>Delete</b>	Delete the selected Bluetooth profile.
<b>Clone</b>	Clone the selected Bluetooth profile.
<b>Import</b>	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 > WiFi Templates > Connectivity Profiles > Bluetooth Profile*.
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:

<b>Name</b>	Enter a name for the profile.
<b>Comments</b>	Optionally, enter comments.
<b>Advertising</b>	Select the advertising types: <i>iBeacon</i> , <i>Eddystone-UUID</i> , and <i>Eddystone-URL</i> .
<b>iBeacon UUID</b>	The iBeacon Universally Unique Identifier (UUID) is automatically assigned, but can be manually reset (63 characters).
<b>Major ID</b>	The major ID (1 - 65535, default = 1000).
<b>Minor ID</b>	The minor ID (1 - 65535, default = 2000).
<b>Eddystone Namespace</b>	The eddytone namespace ID (10 characters).
<b>Eddystone Instance</b>	The eddytone instance ID (6 characters).



<b>Eddystone URL</b>	The eddystone URL (127 characters).		
<b>TX Power</b>	Transmit power level:		
	0 = -21 dBm	5 = -6 dBm	10 = 3 dBm
	1 = -18 dBm	6 = -3 dBm	11 = 4 dBm
	2 = -15 dBm	7 = 0 dBm	12 = 5 dBm
	3 = -12 dBm	8 = 1 dBm	
	4 = -9 dBm	9 = 2 dBm	
<b>Beacon Interval</b>	The beacon interval, in milliseconds (40 - 3500, default = 100).		
<b>BLE Scanning</b>	Enable/disable Bluetooth Low Energy (BLE) scanning.		
<b>Advanced Options</b>	Enter the eddystone encoded URL hexadecimal string size (54 characters) in the <i>eddystone-url-encode-hex</i> field.		

### To edit a Bluetooth 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.  
The *Edit Bluetooth Profile* pane opens.
3. Edit the settings as required.
4. Click *OK* to apply your changes.

### To delete Bluetooth profiles:

1. Select the profile or profiles to be deleted.
2. In the toolbar, click *Delete*.  
Alternatively, right-click the profile and select *Delete*.
3. Click *OK*.

### To clone a Bluetooth profile:

1. Select a profile in the list.
2. In the toolbar, click *Clone*.  
Alternatively, right-click a profile and select *Clone*.  
The *Clone Bluetooth Profile* pane opens.
3. Edit the name of the profile, then edit the remaining settings as required.
4. Click *OK* to clone the profile.

### To import a Bluetooth 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*.

## 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.



QoS profiles are not available in version 5.4 ADOMs.

### To view Quality of Service (QoS) profiles:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager > WiFi Templates > Operation Profiles > QoS Profile*.

The following options are available in the toolbar and right-click menu:

<b>Create New</b>	Create a new QoS profile.
<b>Edit</b>	Edit the selected QoS profile.
<b>Delete</b>	Delete the selected QoS profile.
<b>Clone</b>	Clone the selected QoS profile.
<b>Where Used</b>	View where the selected QoS profile is used.
<b>Import</b>	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 > WiFi Templates > Operation Profiles > QoS Profile*.
3. In the toolbar, click *Create New*.

The *Create New QoS Profile* pane opens.

Create New QoS Profile

**Name**  \*This field is required.

**Comments**

Max Uplink Speed (VAPs)  0 Kbps

Max Downlink Speed (VAPs)  0 Kbps

Max Uplink Speed (Clients)  0 Kbps

Max Downlink Speed (Clients)  0 Kbps

Client Rate Burst ☐ OFF

WiFi Multimedia ☐ ON

U-APSD Power Save Mode ☐ ON

Call Admission Control ☐ ON

Call Capacity  10

Bandwidth Admission Control ☐ ON

Bandwidth Capacity  2000 Kbps

DSCP Mapping ☐ ON

Voice Access  48, 56

Video Access  32, 40

Best Effort Access  0, 24

Background Access  8, 16

**Advanced Options** >

4. Enter the following information, and click **OK** to create the QoS profile:

<b>Name</b>	Enter a name for the profile.
<b>Comments</b>	Optionally, enter comments.
<b>Maximum Uplink Bandwidth for SSIDs</b>	The maximum uplink bandwidth for SSIDs in Kbps (0 - 2097152, default = 0).
<b>Maximum Downlink Bandwidth for SSIDs</b>	The maximum downlink bandwidth for SSIDs in Kbps (0 - 2097152, default = 0).
<b>Maximum Uplink Bandwidth for Clients</b>	The maximum uplink bandwidth for clients in Kbps (0 - 2097152, default = 0).
<b>Maximum Downlink Bandwidth for Clients</b>	The maximum downlink bandwidth for clients in Kbps (0 - 2097152, default = 0).
<b>Client Rate Burst</b>	Enable/disable client rate burst (default = disable).
<b>Wi-Fi MultiMedia</b>	Enable/disable WiFi Multimedia (WMM) control (default = enable).
<b>U-APSD Power Save Mode</b>	Enable/disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode (default = enable). This option is only available if <i>Wi-Fi MultiMedia</i> is enabled.
<b>Call Admission Control</b>	Enable/disable WMM call admission control (default = disable). This option is only available if <i>Wi-Fi MultiMedia</i> is enabled.
<b>Call Capacity</b>	The maximum number of VoWLAN phones allowed (0 - 60, default = 10). This option is only available if <i>Call Admission Control</i> is enabled.
<b>Bandwidth Admission Control</b>	Enable/disable WMM bandwidth admission control (default = disable). This option is only available if <i>Call Admission Control</i> is enabled.
<b>Maximum Bandwidth Capacity</b>	The maximum bandwidth capacity allowed, in Kbps (1 - 600000, default = 2000). This option is only available if <i>Bandwidth Admission Control</i> is enabled.
<b>DSCP Mapping</b>	Enable/disable differentiated Services Code Point (DSCP) mapping (default = disable).
<b>Voice Access</b>	DSCP mapping for voice access category (default = 48, 56). This option is only available if <i>DSCP Mapping</i> is enabled.
<b>Video Access</b>	DSCP mapping for video access category (default = 32, 40). This option is only available if <i>DSCP Mapping</i> is enabled.
<b>Best Effort Access</b>	DSCP mapping for best effort access category (default = 0, 24). This option is only available if <i>DSCP Mapping</i> is enabled.
<b>Background Access</b>	DSCP mapping for background access category (default = 8, 16). This option is only available if <i>DSCP Mapping</i> is enabled.
<b>DSCP Marking</b>	Enable/disable WMM Differentiated Services Code Point (DSCP) marking.

**To edit a QoS 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.  
The *Edit QoS Profile* pane opens.
3. Edit the settings as required.
4. Click *OK*.

**To delete QoS profiles:**

1. Select the profile or profiles to be deleted.
2. In the toolbar, click *Delete*.  
Alternatively, right-click the profile and select *Delete*.
3. Click *OK*.

**To clone a QoS profile:**

1. In the toolbar, click *Clone*.  
Alternatively, right-click the profile and select *Clone*.  
The *Clone QoS Profile* pane opens.
2. Edit the name of the profile, then edit the remaining settings as required.
3. Click *OK*.

**To import a QoS profile:**

1. In the toolbar, click *Import*.  
The *Import* dialog opens.
2. From the FortiGate dropdown, select a device.
3. From the *Profiles* dropdown, select a profile.
4. Click *OK*.

## 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 > WiFi Templates > Bluetooth Profiles > Bonjour Profile*.  
The following options are available in the toolbar and right-click menu:

<b>Create New</b>	Create a new Bonjour profile.
<b>Edit</b>	Edit the selected Bonjour profile.
<b>Delete</b>	Delete the selected Bonjour profile.

<b>Clone</b>	Clone the selected Bonjour profile.
<b>Where Used</b>	View where the selected Bonjour profile is used.
<b>Import</b>	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 > WiFi Templates > Bluetooth Profiles > Bonjour Profile*.
3. In the toolbar, click *Create New*.

The *Create New Bonjour Profile* pane opens.

**Create New Bonjour Profile**

Name:

Comments:  0/63

**Policy List**

+ Create New    ☒ Edit    ☐ Delete

	Policy ID	Description	From VLAN	To VLAN	Services
No record.					

OK    Cancel

4. Enter the following information, and then click *OK* to create the Bonjour profile:

<b>Name</b>	Enter a name for the profile.
<b>Comments</b>	Optionally, enter comments.
<b>Policy List</b>	Configure the policy list.
<b>Create New</b>	<p>Create a new policy list entry.</p> <p>Select the following, then click <i>OK</i>:</p> <ul style="list-style-type: none"> <li>• <i>Description</i>: Description of the Bonjour profile policy.</li> <li>• <i>From VLAN</i>: The VLAN ID that the Bonjour service will be advertised from (0 - 4094, default = 0).</li> <li>• <i>To VLAN</i>: The VLAN ID that the Bonjour service will be made available to (0 - 4094, default = all).</li> <li>• <i>Services</i>: Services for the VLAN.</li> </ul>
<b>Edit</b>	Edit the selected entry.
<b>Delete</b>	Delete the selected entries.

### To edit a Bonjour 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.  
The *Edit Bonjour Profile* pane opens.
3. Edit the settings as required.
4. Click *OK*.

**To delete Bonjour profiles:**

1. Select the profile or profiles to be deleted.
2. In the toolbar, click *Delete*  
Alternatively, right-click the profile and select *Delete*.
3. Click *OK*.

**To clone a Bonjour profile:**

1. Select the profile to be cloned.
2. In the toolbar, click *Clone*.  
Alternatively, right-click the profile and select *Clone*.  
The *Clone Bonjour Profile* pane opens.
3. Edit the name of the profile, then edit the remaining settings as required.
4. Click *OK*.

**To import a Bonjour profile:**

1. In the toolbar, click *Import*.  
The *Import* dialog opens.
2. From the *FortiGate* dropdown, select a device.
3. From the *Profiles* dropdown, select a profile.
4. Click *OK*.

## 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 474](#)

**To view ARRP profiles:**

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager > WiFi Templates > Protection Profiles > ARRP Profile*.

The following options are available in the toolbar and right-click menu:

<b>Create New</b>	Create a new ARRP profile.
<b>Edit</b>	Edit the selected ARRP profile.
<b>Delete</b>	Delete the selected ARRP profile.
<b>Clone</b>	Clone the selected ARRP profile.
<b>Where Used</b>	View where the selected ARRP profile is used.
<b>Import</b>	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 > WiFi Templates > Protection Profiles > ARRP Profile*.
3. In the toolbar, click *Create New*.

The *Create New ARRP Profile* pane opens.

4. Enter the following information, and click *OK* to create the ARRP profile:

<b>Name</b>	Type a name for the profile.
<b>Comment</b>	Optionally, enter comments.
<b>Selection Period</b>	Period in seconds to measure average channel load, noise floor, spectral RSSI (0 to 65535, default = 3600).
<b>Monitor Period</b>	Period in seconds to measure average transmit retries and receive errors (0 to 65535, default = 300).
<b>Weight Managed AP</b>	Weight in DARRP channel score calculation for managed APs (0 to 65535, default = 50).
<b>Weight Rogue AP</b>	Weight in DARRP channel score calculation for rogue APs (0 to 2000, default = 10).
<b>Weight Noise Floor</b>	Weight in DARRP channel score calculation for noise floor (0 to 2000, default = 40).
<b>Weight Channel Load</b>	Weight in DARRP channel score calculation for channel load (0 to 2000, default = 20).
<b>Weight Spectral RSSI</b>	Weight in DARRP channel score calculation for spectral RSSI (0 to 2000, default = 40).
<b>Weight Weather Channel</b>	Weight in DARRP channel score calculation for weather channel (0 to 2000, default = 1000).

<b>Weight DFS Channel</b>	Weight in DARRP channel score calculation for DFS channel (0 to 2000, default = 500).
<b>Threshold AP</b>	Threshold to reject channel in DARRP channel selection phase 1 due to surrounding APs (0 to 500, default = 250).
<b>Threshold Noise Floor</b>	Threshold in dBm to reject channel in DARRP channel selection phase 1 due to noise floor (default = -85).
<b>Threshold Channel Load</b>	Threshold in percentage to reject channel in DARRP channel selection phase 1 due to channel load (0 to 100, default = 60).
<b>Threshold Spectral RSSI</b>	Threshold in dBm to reject channel in DARRP channel selection phase 1 due to spectral RSSI (default = -65).
<b>Threshold TX Retries</b>	Threshold in percentage for transmit retries to trigger channel reselection in DARRP monitor stage (0 to 1000, default = 300).
<b>Threshold RX Errors</b>	Threshold in percentage for receive errors to trigger channel reselection in DARRP monitor stage (0 to 100, default = 50).
<b>Include Weather Channel</b>	Enable/disable use of weather channel in DARRP channel selection phase 1 (default = disable).
<b>Include DFS Channel</b>	Enable/disable use of DFS channel in DARRP channel selection phase 1 (default = disable).
<b>Advanced Options</b>	Expand to display and set the advanced options. Hover the mouse over the <i>i</i> icon to view a tooltip of each advanced option. For more information, refer to the <i>FortiOS CLI Reference</i> .

#### To edit a custom ARRP profile:

1. Select the profile.
2. In the toolbar, click *Edit*.  
Alternatively, you can right-click the profile and select *Edit*, or double-click a profile.  
The *Edit ARRP Profile* pane opens.
3. Edit the settings as required. The profile name cannot be edited.
4. Click *OK* to apply your changes.

#### To delete custom ARRP profiles:

1. Select the ARRP profile or profiles to be deleted. Default profiles cannot be deleted.
2. In the toolbar, click *Delete*.  
Alternatively, you can right-click the profile and select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the profile.

#### To clone a custom ARRP profile:

1. Select the profile to be cloned.
2. In the toolbar, click *More > Clone*.  
Alternatively, you can right-click the 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 view where an ARRP 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*.

#### To import an ARRP profile:

1. In the toolbar, click *More > 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 the profile(s).
4. Click *OK* to import the profile or profiles.

## L3 Firewall Profiles

L3 Firewall Profiles define WiFi access permissions for SSIDs. When you create SSID profiles, you can select an access control list.

#### To view access control lists:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager > WiFi Templates > Protection Profiles > L3 Firewall Profiles*.

The following options are available in the toolbar and right-click menu:

<b>Create New</b>	Create a new access control list.
<b>Edit</b>	Edit the selected access control list.
<b>Delete</b>	Delete the selected access control list.
<b>Clone</b>	Clone the selected access control list.
<b>Where Used</b>	View where the selected access control list is used.
<b>Import</b>	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 > WiFi Templates > Protection Profiles > L3 Firewall Profiles*.
3. In the toolbar, *Create New*.  
The *Create New L3 Firewall Profile* pane opens.

Create New L3 Firewall Profiles

Name

This field is required.

Comments

IPv4 Rule List

+ Create New

Edit

Delete

Move Up

Move Down

Search...

☐

Source

Destination

Action

No record found.

0

IPv6 Rule List

+ Create New

Edit

Delete

Move Up

Move Down

Search...

☐

Source

Destination

Action

No record found.

0

OK

Cancel

4. Enter the following information:

<b>Name</b>	Type a name for the access control list.
<b>Comment</b>	Optionally, enter comments.
<b>IPv4 Rule List</b>	<p>Click <i>Create New</i> to define L3 firewall rules for IPv4 addresses</p> <p>Select the following, then click <i>OK</i>:</p> <ul style="list-style-type: none"> <li>• <i>ID</i>: Enter an ID for the rule.</li> <li>• <i>Comments</i>: Optionally, enter a description.</li> <li>• <i>Source Address</i>: Enter the source IP address.</li> <li>• <i>Source Port</i>: Enter the source port.</li> <li>• <i>Destination Address</i>: Enter the destination IP address.</li> <li>• <i>Destination Port</i>: Enter the destination port.</li> <li>• <i>IANA protocol number</i>: Enter the protocol.</li> <li>• <i>Action</i>: Select the policy action. Select <i>Allow</i> or <i>Deny</i> to allow or deny traffic matching the policy.</li> </ul>
<b>IPv6 Rule List</b>	<p>Click <i>Create New</i> to define L3 firewall rules for IPv6 addresses.</p> <p>Select the following, then click <i>OK</i>:</p> <ul style="list-style-type: none"> <li>• <i>ID</i>: Enter an ID for the rule.</li> <li>• <i>Comments</i>: Optionally, enter a description.</li> <li>• <i>Source Address</i>: Enter the source IP address.</li> <li>• <i>Source Port</i>: Enter the source port.</li> <li>• <i>Destination Address</i>: Enter the destination IP address.</li> <li>• <i>Destination Port</i>: Enter the destination port.</li> </ul>

- *IANA protocol number*: 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.

#### **To edit access control lists:**

1. Select the access control list.
2. In the toolbar, click *Edit*, or right-click the access control list and select *Edit*. You can also double-click an access control list to open it. The *Edit Access Control List* pane opens.
3. Edit the settings as required.
4. Click *OK* to apply your changes.

#### **To delete access control lists:**

1. Select one or more access control lists to be deleted.
2. In the toolbar, click *Delete*, or right-click the access control list and select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the access control list.

#### **To clone access control lists:**

1. Select the access control list to be cloned.
2. In the toolbar, click *More > Clone*, or right-click the access control list and select *Clone*.
3. Edit the name, then edit the remaining settings as required.
4. Click *OK* to clone the access control list.

#### **To view where an access control list is used:**

1. Select the access control list.
2. In the toolbar, click *More > Where Used*, or right-click the access control list and select *Where Used*. The *Where <profile name> is used* pane is displayed.
3. Click *Close*.

#### **To import access control lists:**

1. In the toolbar, click *More > Import*. The *Import* dialog opens.
2. From the *FortiGate* dropdown, select a FortiGate from the list. The list will include all of the devices in the current ADOM.
3. From the *Profiles* dropdown, select one or more access control lists to be imported.
4. Click *OK* to import the access control lists.

## **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 474](#).

**To assign profiles to FortiAP devices:**

1. Go to *AP Manager*.
2. In the tree menu, go to *Device & Groups > Managed FortiGate (#)*, and select a device. Alternatively, you can select a device in a group, see [FortiAP groups on page 458](#).
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.

## FortiAP configuration profiles

You can create or edit FortiAP configuration profiles for managing FortiAP configuration.

**To view FortiAP configuration profiles:**

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager > WiFi Profiles > Operation Profiles > FortiAP Configuration Profiles*.

The following options are available in the toolbar and right-click menu:

<b>Create New</b>	Create a new profile.
<b>Edit</b>	Edit the selected profile.
<b>Delete</b>	Delete the selected profile.
<b>Clone</b>	Clone the selected profile.
<b>Where Used</b>	View where the selected profile is used.
<b>Import</b>	Import profiles from a connected FortiGate (toolbar only).

**To create FortiAP configuration profiles:**

1. Click *Create New*.
2. Enter the following information for the profile:

<b>Name</b>	Enter a name for the profile.
<b>Comments</b>	Optionally, provide comments about the profile.
<b>FortiAP family</b>	Select a FortiAP family type.
<b>Command List</b>	Click <i>Create New</i> to create a new command list. You can reorder commands in the list using the <i>Move Up</i> and <i>Move Down</i> commands in the toolbar. When you create a new command list, you must enter an <i>ID</i> , <i>Name</i> , <i>Type</i> , and <i>Value/Password</i> .
<b>Wireless Controller</b>	

<b>Waiting Time</b>	Maximum waiting time for the AP to join the validation controller after applying AP local configuration (3 - 30 min, default = 10).
<b>Type</b>	Select a wireless controller type.

**To edit a profile:**

1. Select the profile.
2. In the toolbar, click *Edit*.  
Alternatively, you can right-click the profile and select *Edit*, or you can double-click the profile.  
The *Edit AP Profile* pane opens.
3. Edit the settings as required. The profile name cannot be edited.
4. Click *OK* to apply your changes.

**To delete profiles:**

1. Select the AP profile or profiles to be deleted. Default profiles cannot be deleted.
2. In the toolbar, click *Delete*.  
Alternatively, you can right-click the profile and select *Delete*.
3. Click *OK* in the confirmation dialog to delete the profile.

**To clone profiles:**

1. Select the profile to be cloned.
2. In the toolbar, click *Clone*.  
Alternatively, you can right-click the 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 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*.

**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 the profile(s).
4. Click *OK* to import the profile or profiles.

## MPSK profiles

You can create or edit MPSK profiles to manage multiple pre-shared keys.

**To view MPSK profiles:**

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *AP Manager > WiFi Profiles > Connectivity Profiles > MPSK Profiles*.

The following options are available in the toolbar and right-click menu:

<b>Create New</b>	Create a new profile.
<b>Edit</b>	Edit the selected profile.
<b>Delete</b>	Delete the selected profile.
<b>Clone</b>	Clone the selected profile.
<b>Where Used</b>	View where the selected profile is used.
<b>Import</b>	Import profiles from a connected FortiGate (toolbar only).

**To create MPSK profiles:**

1. Click *Create New*.
2. Enter the following information for the profile:

<b>Name</b>	Enter a name for the profile.
<b>Maximum Concurrent Client Count</b>	Configure the maximum concurrent client count.
<b>MPSK Group List</b>	<p>Click <i>Create New</i> to create a new MPSK group, and specify the following information:</p> <ul style="list-style-type: none"> <li>• <i>Group Name</i>: Enter a name for the MPSK group.</li> <li>• <i>VLAN Type</i>: Select the VLAN type.</li> <li>• <i>MPSK Key List</i>: Click <i>Create New</i> to create new keys, generate keys, and import keys.</li> </ul> <p>You can click <i>Export Groups</i> to export the configured MPSK group list.</p>

**To edit a profile:**

1. Select the profile.
2. In the toolbar, click *Edit*.  
Alternatively, you can right-click the profile and select *Edit*, or you can double-click the profile.  
The *Edit AP Profile* pane opens.
3. Edit the settings as required. The profile name cannot be edited.
4. Click *OK* to apply your changes.

**To delete profiles:**

1. Select the AP profile or profiles to be deleted. Default profiles cannot be deleted.
2. In the toolbar, click *Delete*.  
Alternatively, you can right-click the profile and select *Delete*.
3. Click *OK* in the confirmation dialog to delete the profile.

**To clone profiles:**

1. Select the profile to be cloned.
2. In the toolbar, click *Clone*.  
Alternatively, you can right-click the 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 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*.

**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 the profile(s).
4. Click *OK* to import the profile or profiles.

## WiFi profiles 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 509](#).
2. Configure profiles for each managed access point. See [Creating profiles on page 510](#).
3. Install changes to managed access points. See [Installing changes to FortiAP devices on page 460](#).

## 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 > All 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*.
2. Click *Managed FortiGate (#)*, and select a device from the list.
3. In the toolbar, go to *Operation Profile > FortiAP Profiles*, and click *Create New*.
4. 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:

<b>IPsec VPN</b>	Displays all of defined IPsec VPN communities and associated devices for the selected ADOM. You can create, monitor, and manage VPN settings. See <a href="#">IPsec VPN Communities on page 527</a>
<b>SSL-VPN</b>	Create, monitor, and manage SSL-VPN settings. You can also create, edit, and delete portal profiles for SSL-VPN settings. See <a href="#">SSL VPN on page 544</a> .

## 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* pane. However, you can access the settings on the *VPN Manager > SSL-VPN* pane without enabling central VPN management. See [Enabling central VPN management on page 512](#).

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 512](#).
2. Create a VPN community, sometimes called a VPN topology. See [Creating IPsec VPN communities on page 528](#).
3. Create a managed gateway. See [Creating managed gateways on page 537](#).

### To create SSL-VPN settings:

1. Create custom profiles. See [Creating SSL VPN portal profiles on page 547](#).  
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 545](#).

### To install VPN objects to devices:

1. Plan the VPN security policies. See [VPN security policies on page 553](#).
2. In a policy package, create VPN security policies, and select the VPN settings. See [Creating policies on page 329](#).
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 318](#).
4. Install the policy package to the devices. See [Install a policy package on page 314](#).

## 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 *System Settings > 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 > Central Management*.  
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 > All 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 *System Settings > 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 163](#).

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.

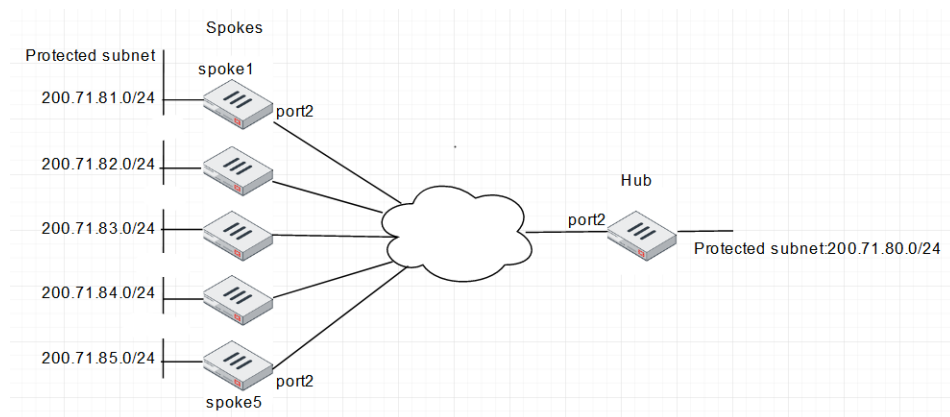
## VPN Setup Wizard supports device groups

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 515](#).
2. Create protected subnet firewall addresses for hub and spoke devices. See [Creating protected subnet firewall addresses on page 515](#).
3. Create a VPN community. See [Creating VPN communities on page 517](#).
4. Add spoke FortiGate units to the VPN community. See [Adding spoke FortiGate units to the VPN community on page 518](#).
5. Add the hub FortiGate units to the VPN community. See [Adding the hub FortiGate unit to the VPN community on page 520](#).  
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 523](#)

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 524](#)
- Add a spoke member to a VPN community. See [Adding a spoke member to a VPN community on page 526](#)

## Creating device groups

### To create device groups:

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

#### Create New Device Group

Group Name

spoke\_group

Description

+ Add Member

Remove Member

Search...

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

OK

Cancel

5. Click *OK* to save the group.

## Creating protected subnet firewall addresses

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

### To create protected subnet firewall addresses:

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

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

**Create New Address**

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

**Advanced Options** >

Per-Device Mapping	OFF
--------------------	-----

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

**Create New Address**

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

**Advanced Options** >

Per-Device Mapping	ON
--------------------	----

+ Create New   Edit   Delete   Column Settings ▾

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

## Creating VPN communities

### To create a VPN community:




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

#### VPN Topology Setup Wizard

 star

 Description

#### Choose VPN Topology

 Full Meshed
  Star
  Dial up

< Back

Next >

Cancel

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

#### VPN Topology Setup Wizard

#### Authentication & Encryption Settings:

#### Authentication

Pre-shared Key Certificates



- ☒ Generate (random)  
☐ Specify

#### Encryption

#### IKE Security (Phase 1) Properties

#### IKE Version

1 2

#	Encryption	Authentication	
1	AES128	SHA1	+ 
2	AES256	SHA256	+ 

#### IPsec Security (Phase 2) Properties

< Back

Next >

Cancel

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

#### VPN Topology Setup Wizard

VPN Zone ☒ ON

☒ Create Default Zones

☐ Use Custom Zone

**IKE Security Phase 1 Advanced Properties**

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

Exchange Mode ☐ Aggressive ☒ Main (ID Protection)

Key Life  (120-172800 seconds)

Dead Peer Detection ☐ Disable ☐ On Idle ☒ On Demand

**IPsec Security Phase 2 Advanced Properties**

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

< Back Next > Cancel

## Adding spoke FortiGate units to the VPN community

### To add spoke FortiGate units to the VPN community:

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

#### VPN Gateway Setup Wizard - star

Protected Network Device Default VPN Interface Local Gateway Advanced

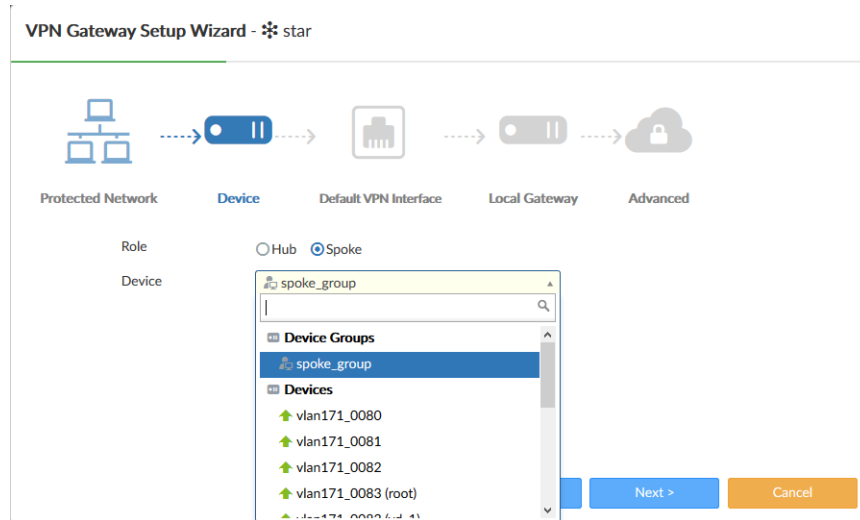
Protected Subnet

protected\_subnet\_spoke  
IP/Netmask: 210.71.0.0/255.255.0.0  
1 Entry Selected

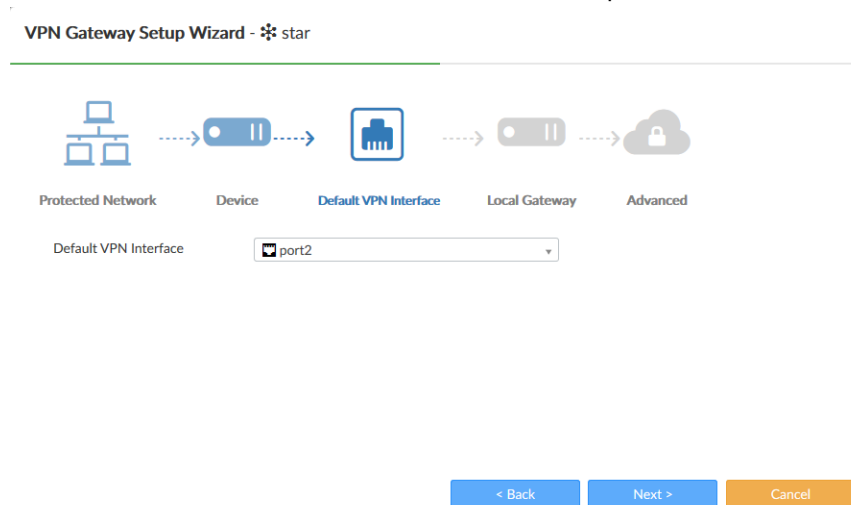
< Back Next > Cancel



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



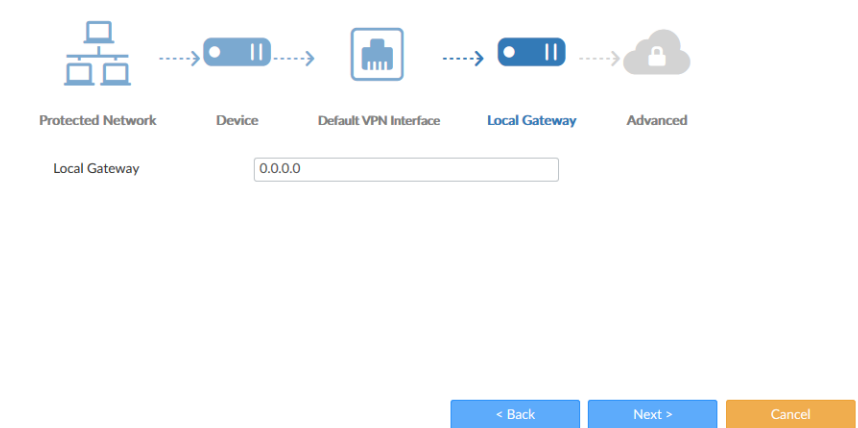
5. Set the *Default VPN Interface* options, and click *Next*.
  - a. Beside *Default VPN Interface*, select the interface for spokes, which is often the internet-facing interface.



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

VPN Gateway Setup Wizard - ⚙️ star

---



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

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

VPN Gateway Setup Wizard - ⚙️ star

---

Local ID

Routing ☐ Manual (via Device Manager) ☒ Automatic

Advanced Options >

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

## Adding the hub FortiGate unit to the VPN community

To add a hub FortiGate unit to the VPN community:






1. Go to *VPN Manager > IPsec VPN*, and click the community that you created.  
The community opens in the content 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.

VPN Gateway Setup Wizard - ⚙️ star

---



Protected Subnet

Protected\_subnet\_hub  
IP/Netmask:200.71.80.0/255.255.255.0  
1 Entry Selected

< Back

Next >






Cancel

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

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

VPN Gateway Setup Wizard - ⚙️ star

---



Role ☒ Hub ☐ Spoke

Device

< Back






Next >

Cancel

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

VPN Gateway Setup Wizard - ⚙️ star

---



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

Default VPN Interface






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

< Back    Next >    Cancel

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

VPN Gateway Setup Wizard - ⚙️ star

---



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

Local Gateway

< Back    Next >    Cancel

7. Set the *Advanced* options, and click *OK*.

- a. Beside *Routing*, select *Manual (via Device Manager)* or *Automatic*.

VPN Gateway Setup Wizard - star

Local ID:

Routing: ☐ Manual (via Device Manager) ☒ Automatic

Summary Network(s)

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

Advanced Options >

< Back OK Cancel

The hub and spoke are created.

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

VPN Community Install Wizard

star

Name: star

Number of VPN: 2

Authentication: Pre-shared Key

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

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

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

## 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:

- Go to *Policy & Object > Policy Packages*.
- Create firewall policies for hub and spoke FortiGates.

Policy & Objects Policy Packages Object Configurations ADOM: vpn\_mgmt

Policy Package Install ADOM Revisions Tools Collapse All Object Selector

Search...

default IPsec Policy Installation Targets

star IPsec Policy Installation Targets

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

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

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

#### Install Wizard

☒ **Install Policy Package & Device Settings**

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

Policy Package

star

Comment

0/127

☐ Create ADOM Revision

☐ Schedule Install

☐ **Install Device Settings (only)**

Next >

Cancel

5. Complete the wizard to install the configurations.

## Removing a spoke member from a VPN community

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

### To remove a spoke member from a VPN community:

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

- c. Select a device, for example, *vlan171\_0085*, and click *Remove Member*.

### Edit Device Group

Group Name: spoke\_group

Description:   
 0/128

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

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

OK Cancel

- d. Click OK to save the changes.

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

### Install Wizard - Policy Package (star)

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

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

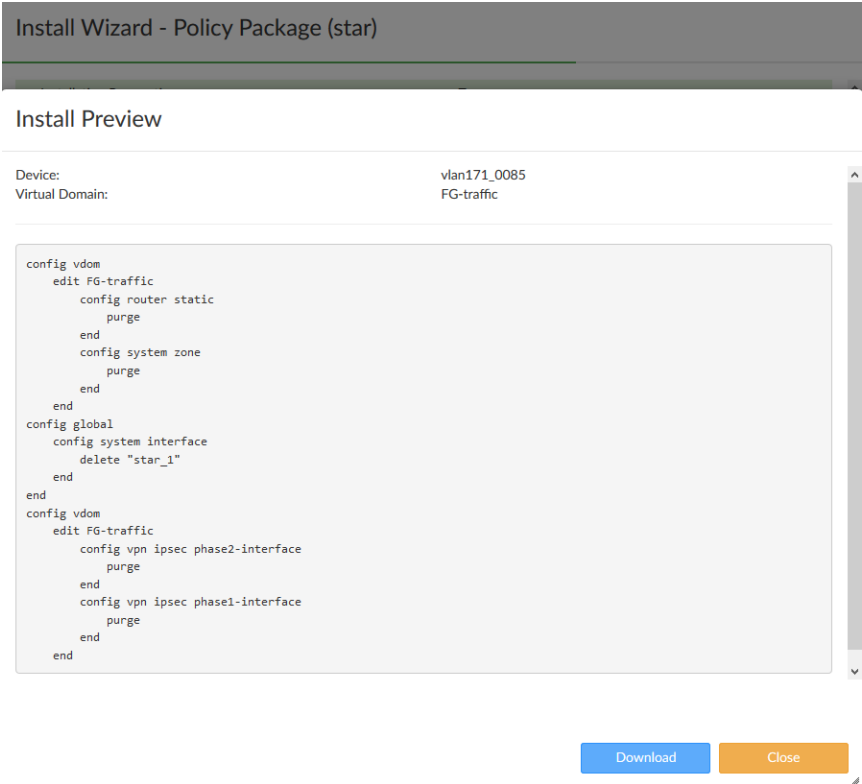
### Install Preview

Device: vlan171\_0080  
Virtual Domain: root

```

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

The *Install Preview* page shows that FortiManager will delete related configurations on the spoke FortiGate named *vlan171\_0085*.

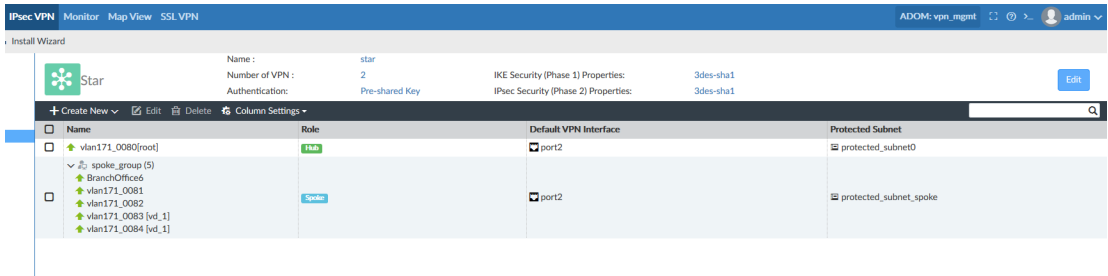


Adding a spoke member to a VPN community

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*.

#### Install Preview

Device: BranchOffice6  
Virtual Domain: root

```

config vpn ipsec phase1-interface
  edit "star_1"
    set interface "port2"
    set comments "[created by FMG VPN Manager]"
    set dhgrp 1 5
    set proposal 3des-sha1
    set keylife 28800
    set peertype any
    set remote-gw 100.71.80.1
    set net-device disable
    set add-gw-route enable
    set psksecret ENC Z8Zpc/bwU2j1HxCfWzO/Xkklz1iO6IOFpF2mmab0XvcAk+pnJrLz5+MLa6KZwR821VYN0GU4AL8P2BL5g5w1irFHSTRfIOE
  next
end
config system interface
  edit "star_1"
    set vdom "root"
    set type tunnel
    set snmp-index 114
    set interface "port2"
  next
end
config system zone
  edit "vpnmgr_star_spoke2hub"
    set interface "star_1"
  next
end
config vpn ipsec phase2-interface
  edit "star_1_0"
    set phase1name "star_1"
    set proposal 3des-sha1
    set auto-negotiate enable
    set comments "[created by FMG VPN Manager]"
    set dhgrp 1 5
    set keylifeseconds 1800

```

## IPsec VPN

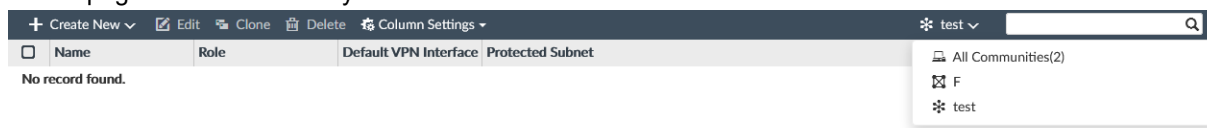
IPsec VPN includes the following topics:

- [IPsec VPN Communities on page 527](#)
- [IPsec VPN gateways on page 536](#)
- [Using Map View on page 543](#)
- [Monitoring IPsec VPN tunnels on page 544](#)

## IPsec VPN Communities

In the *VPN Management > IPsec VPN* pane, you can use the *Community List* tab to 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* and click the *All Communities* from the dropdown to view all IPsec VPN communities.

+ Create New Edit Clone Delete Column Settings			All Communities(2)
<input type="checkbox"/> Name	Gateways	Authentication	
<input type="checkbox"/> F	> 1 Gateway	Pre-shared Key	All Communities(2)
<input type="checkbox"/> TestCom	> 0 Gateways	Pre-shared Key	F
			TestCom

The following options are available:

<b>Install Wizard</b>	Launch the Install Wizard to install IPsec VPN settings to devices.
<b>Create New</b>	Create a new VPN community. See <a href="#">Creating IPsec VPN communities on page 528</a>
<b>Edit</b>	Edit the selected VPN community. See <a href="#">Editing an IPsec VPN community on page 535</a> .
<b>Clone</b>	Clone the selected VPN community.
<b>Delete</b>	Delete the selected VPN community or communities. See <a href="#">Deleting VPN communities on page 536</a> .
<b>Column Settings</b>	Configure which columns are displayed, or click <i>Reset to Default</i> to reset the display to the default columns.
<b>Search</b>	Enter a search term to search the communities list.
<b>Configure Gateways</b>	Go to the gateway list for the community. This option is only available from the right-click menu. See <a href="#">IPsec VPN gateways on page 536</a> .
<b>Add Managed Gateway</b>	Start the <i>VPN Gateway Setup Wizard</i> . This option is only available from the right-click menu. See <a href="#">Creating managed gateways on page 537</a> .

## 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 536](#).

### To create a new IPsec VPN community:


1. Go to *VPN Manager > IPsec VPN > VPN Communities* and click the *All Communities* from the dropdown to view all IPsec VPN communities.
2. Click *Create New* in the content pane toolbar.  
The *VPN Topology Setup Wizard* is displayed.


**VPN Topology Setup Wizard**


Name

Description

Choose VPN Topology


  
Full Meshed


  
Star


  
Dial up

< Back   Next >   Cancel

- Enter a name for the topology in the *Name* field.
- Optionally, enter a brief description of the topology in the *Description* field.
- 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.
- Click *Next*.

**VPN Topology Setup Wizard**

Authentication & Encryption Settings:

**Authentication**   Pre-shared Key   Certificates

☒ Generate(random)  
☐ Specify

**Encryption**

IKE Security (Phase 1) Properties

IKE Version   1   2

#	Encryption	Authentication	
1	3DES	MD5	+ 🗑
2	AES256	MD5	+ 🗑

IPsec Security (Phase 2) Properties

#	Encryption	Authentication	
1	CHACHA20POLY1305		+ 🗑
2	ARIA256	MD5	+ 🗑

< Back   Next >   Cancel

- 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 530](#).

## VPN community settings

The following table describes the options available in the *VPN Topology Setup Wizard* and on the *Edit VPN Community* page.

<b>Name</b>	Type a name for the VPN topology.
<b>Description</b>	Type an optional description.
<b>Choose VPN Topology</b>	Choose a topology type. Select one of: <ul style="list-style-type: none"> <li>• <i>Full Meshed</i>: Each gateway has a tunnel to every other gateway.</li> <li>• <i>Star</i>: Each gateway has one tunnel to a central hub gateway.</li> <li>• <i>Dial up</i>: Some gateways, often mobile users, have dynamic IP addresses and contact the gateway to establish a tunnel.</li> </ul>
<b>Authentication</b>	Select <i>Certificates</i> or <i>Pre-shared Key</i> . When you select <i>Pre-shared Key</i> , 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.
<b>Certificates</b>	If you selected <i>Certificates</i> , select a certificate template. Fortinet provides several default certificate templates. You can also create certificate templates on the <i>Device Manager &gt; Provisioning Templates &gt; Certificate Templates</i> pane.
<b>Pre-shared Key</b>	If you selected <i>Pre-shared Key</i> , select <i>Generate</i> or <i>Specify</i> . When you select <i>Specify</i> , 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.
<b>Encryption</b>	Define the IKE Profile. Configure IKE Phase 1 and IKE Phase 2 settings.

<b>IKE Security (Phase 1) Properties</b>	Define the Phase 1 proposal settings.
<b>IKE Version</b>	<p>Select IKE version 1 or 2 (default = 2).</p> <p>For more information about IKE v2, refer to RFC 4306.</p>
<b>Encryption Authentication</b>	<p>Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required.</p> <p>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.</p> <p>Select one of the following symmetric-key encryption algorithms:</p> <ul style="list-style-type: none"> <li>• 3DES: Triple-DES, in which plain text is encrypted three times by three keys.</li> <li>• AES128: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key.</li> <li>• AES128GCM: AES128 Galois/Counter Mode (GCM).</li> <li>• AES192: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key.</li> <li>• AES256: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key.</li> <li>• AES256GCM</li> <li>• ARIA128: A 128-bit block size that uses a 128-bit key.</li> <li>• ARIA192: A 128-bit block size that uses a 192-bit key.</li> <li>• ARIA256: A 128-bit block size that uses a 256-bit key.</li> <li>• CHACHA20POLY1305: Arbitrary length, 96-bit nonce, and 256-bit key.</li> <li>• DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.</li> <li>• SEED: A 16-round Feistel network with 128-bit blocks and a 128-bit key.</li> </ul> <p>Select either of the following authentication message digests to check the authenticity of messages during phase 1 negotiations:</p> <ul style="list-style-type: none"> <li>• MD5: Message Digest 5, the hash algorithm developed by RSA Data Security.</li> <li>• SHA1: Secure Hash Algorithm 1, which produces a 160-bit message digest.</li> <li>• SHA256: Secure Hash Algorithm 2, which produces a 256-bit message digest.</li> <li>• SHA384: Secure Hash Algorithm 3, which produces a 384-bit message digest.</li> <li>• SHA512: Secure Hash Algorithm 3, which produces a 512-bit message digest.</li> </ul> <p>Note: If the encryption is GCM or CHACHA20POLY1305, the authentication options are PRFSHA1, PRFSHA256, PRFSHA384, and PRFSHA512.</p> <p>To specify more combinations, use the <i>Add</i> button beside any of the table rows.</p>

<b>Network Overlay</b>	<p>When network overlay is enabled, FOS allows the creation of VPN IPsec Phase 1 interfaces with the same remote gateway and interface.</p> <p>You can specify the VPN gateway network ID in the <i>Network Overlay ID</i> field.</p> <p>This setting is only available if the IKE version is set to 2.</p>
<b>IPsec Security (Phase 2) Properties</b>	<p>Define the Phase 2 proposal settings.</p> <p>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.</p>
<b>Encryption Authentication</b>	<p>Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required.</p> <p>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.</p> <p>Select one of the following symmetric-key encryption algorithms:</p> <ul style="list-style-type: none"> <li>• 3DES: Triple-DES, in which plain text is encrypted three times by three keys.</li> <li>• AES128: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key.</li> <li>• AES128GCM: AES128 Galois/Counter Mode (GCM).</li> <li>• AES192: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key.</li> <li>• AES256: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key.</li> <li>• AES256GCM</li> <li>• ARIA128: A 128-bit block size that uses a 128-bit key.</li> <li>• ARIA192: A 128-bit block size that uses a 192-bit key.</li> <li>• ARIA256: A 128-bit block size that uses a 256-bit key.</li> <li>• CHACHA20POLY1305: Arbitrary length, 96-bit nonce, and 256-bit key.</li> <li>• DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.</li> <li>• NULL: Do not use an encryption algorithm.</li> <li>• SEED: A 16-round Feistel network with 128-bit blocks and a 128-bit key.</li> </ul> <p>Select either of the following authentication message digests to check the authenticity of messages during phase 1 negotiations:</p> <ul style="list-style-type: none"> <li>• NULL: Do not use a message digest.</li> <li>• MD5: Message Digest 5, the hash algorithm developed by RSA Data Security.</li> <li>• SHA1: Secure Hash Algorithm 1, which produces a 160-bit message digest.</li> <li>• SHA256: Secure Hash Algorithm 2, which produces a 256-bit</li> </ul>

	<p>message digest.</p> <ul style="list-style-type: none"> <li>• SHA384: Secure Hash Algorithm 3, which produces a 384-bit message digest.</li> <li>• SHA512: Secure Hash Algorithm 3, which produces a 512-bit message digest.</li> </ul> <p>Note: If the encryption is GCM or CHACHA20POLY1305, no authentication options can be selected.</p> <p>To specify more combinations, use the Add button beside any of the table rows.</p>
<b>VPN Zone</b>	Select to create VPN zones. When enabled, you can select to create default or custom zones. When disabled, no VPN zones are created.
<b>Create Default Zones</b>	Select to have default zones created for you.
<b>Use Custom Zone</b>	Select to choose what zones to create.
<b>IKE Security Phase 1 Advanced Properties</b>	
<b>Diffie Hellman Group(s)</b>	<p>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.</p> <p>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.</p> <p>Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode.</p>
<b>Exchange Mode</b>	<p>Select either <i>Aggressive</i> or <i>Main (ID Protection)</i>.</p> <p>The FortiGate unit and the remote peer or dialup client exchange phase 1 parameters in either <i>Main (ID Protection)</i> or <i>Aggressive</i> mode. This choice does not apply if you use IKE version 2, which is available only for route-based configurations.</p> <ul style="list-style-type: none"> <li>• In Main mode, the Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information</li> <li>• In Aggressive mode, the Phase 1 parameters are exchanged in single message with authentication information that is not encrypted.</li> </ul> <p>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.</p>
<b>Key Life</b>	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.

<b>Dead Peer Detection</b>	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.
<b>IPsec Security Phase 2 Advanced Properties</b>	
<b>Diffie Hellman Group(s)</b>	<p>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.</p> <p>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.</p> <p>Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode.</p>
<b>Replay detection</b>	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.
<b>Perfect forward secrecy (PFS)</b>	<p>Select to enable or disable perfect forward secrecy (PFS).</p> <p>Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.</p>
<b>Key Life</b>	Select the PFS key life. Select <i>Second</i> , <i>Kbytes</i> , or <i>Both</i> from the dropdown list and type the value in the text field.
<b>Autokey Keep Alive</b>	<p>Select to enable or disable autokey keep alive.</p> <p>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.</p> <p>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.</p>
<b>Auto-Negotiate</b>	Select to enable or disable auto-negotiation.
<b>NAT Traversal</b>	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.
<b>Keep-alive Frequency</b>	If NAT traversal is enabled or forced, type a keep-alive frequency setting (10-900 seconds).
<b>Advanced-Options</b>	For more information on advanced options, see the <i>FortiOS CLI Reference</i> .
<b>fcc-enforcement</b>	Enable or disable FCC enforcement.
<b>inter-vdom</b>	Enable or disable the inter-vdom setting.



<b>localid-type</b>	Select the local ID type from the dropdown list. Select one of: <ul style="list-style-type: none"> <li><i>address</i>: IP Address</li> <li><i>asn1dn</i>: ASN.1 Distinguished Name</li> <li><i>auto</i>: Select type automatically</li> <li><i>fqdn</i>: Fully Qualified Domain name</li> <li><i>keyid</i>: Key Identifier ID</li> <li><i>user-fqdn</i>: User Fully Qualified Domain Name</li> </ul>
<b>negotiate-timeout</b>	Enter the negotiation timeout value. The default is 30 seconds.
<b>npu-offload</b>	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 536](#) for information.

### To view IPsec VPN community details:

1. Go to *VPN Manager > IPsec VPN > VPN Communities* and select a community from the dropdown or double-click a community from the *All Communities* pane.

The community information pane opens.

Name	Default VPN Interface	Protected Subnet
EnterpriseCore[root]	a	FABRIC_DEVICE

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 > VPN Communities*.
2. Select *All Communities* from the communities dropdown, and do one of the following
  - Right-click on a community in the *All Communities* pane, and select *Edit* from the menu.
  - Select a community in the *All Communities* pane, and click *Edit* in the toolbar.

The *Edit 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 530](#).

## 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 > VPN Communities*.
2. Select *All Communities* from the communities dropdown, and do one of the following:
  - Select a community in the *All Communities* pane then click *Delete* in the toolbar.
  - Right-click on a community in the *All Communities* pane 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*, then select a community from the communities dropdown in the toolbar, or double-click on a community in the list, to manage the VPN gateways in that community.

Name : F  
 Number of VPN : 1  
 Authentication : Pre-shared Key

IKE Security (Phase 1) Properties: aes128-sha256, aes256-sha256, aes128-sha1, aes256-sha1  
 IPsec Security (Phase 2) Properties: aes128-sha1, aes256-sha1, aes128-sha256, aes256-sha256, aes128gcm, aes256gcm, chacha20poly1305

Edit

+ Create New ▾   Edit   Clone   Delete   Column Settings ▾   F ▾   🔍		
<input type="checkbox"/> Name	Default VPN Interface	Protected Subnet
<input type="checkbox"/> EnterpriseCore[root]	a	FABRIC_DEVICE

The following options are available:

### Create New

Create a new managed or external gateway. See [Creating managed gateways on page 537](#) and [Creating external gateways on page 541](#) for more information.

### Edit

Edit the selected gateway. See [Editing an IPsec VPN gateway on page 542](#).

<b>Delete</b>	Delete the selected gateway or gateways. See <a href="#">Deleting VPN gateways on page 542</a> .
<b>Column Settings</b>	Configure which columns are displayed, or click <i>Reset to Default</i> to reset the display to the default columns.
<b>Search</b>	Enter a search term to search the gateway list.

## 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 541](#).

### To create a managed gateway:

1. Go to *VPN Manager > IPsec VPN*.
2. Select a community from the communities dropdown in the toolbar, or double-click on a community in the list.
3. On the community information content pane, in the toolbar, select *Create New > Managed Gateway*.  
The *VPN Gateway Setup Wizard* opens.

4. Proceed through the five pages of the wizard, filling in the following values as required, then click *OK* to create the managed gateway.

<b>Protected Subnet</b>	Select a protected subnet from the drop-down list.
<b>Role</b>	Select the role of this gateway: <i>Hub</i> or <i>Spoke</i> . This option is only available for star and dial up VPN topologies.
<b>Device</b>	Select a <i>Device</i> or <i>Device Group</i> from the drop-down list.
<b>Default VPN Interface</b>	Select the interface to use for this gateway from the drop-down list.
<b>Hub-to-Hub Interface</b>	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 <i>Hub</i> .
<b>Local Gateway</b>	Enter the local gateway IP address.
<b>Local ID</b>	Enter a local ID.
<b>Routing</b>	Select the routing method: <i>Manual (via Device Manager)</i> , or <i>Automatic</i> .
<b>Summary Network(s)</b>	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 <i>Hub</i> .
<b>Peer Type</b>	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <i>Accept any peer ID</i></li> <li>• <i>Accept this peer ID</i>: Enter the peer ID in the text field</li> <li>• <i>Accept a dialup group</i>: Select a group from the drop-down list</li> <li>• <i>Accept peer</i>: Select a peer from the dropdown list</li> <li>• <i>Accept peer group</i>: Select a peer group from the drop-down list</li> </ul> <p>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.</p> <p>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.</p> <p>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.</p> <p>This option is only available for dial up topologies.</p>
<b>XAUTH Type</b>	Select the XAUTH type: <i>Disable</i> , <i>PAP Server</i> , <i>CHAP Server</i> , or <i>AUTO Server</i> . This option is only available for dial up topologies.
<b>User Group</b>	Select the authentication user group from the dropdown list. This field is available when <i>XAUTH Type</i> is set to <i>PAP Server</i> , <i>CHAP Server</i> , or <i>AUTO Server</i> .

	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.
<b>Enable IKE Configuration Method ("mode config")</b>	Select to enable or disable IKE configuration method. This option is only available for dial up topologies.
<b>Enable IP Assignment</b>	Select to enable or disable IP assignment. This option is only available for dial up topologies. When the role is set to <i>Hub</i> , this option is only available when <i>Enable IKE Configuration Method</i> is on.
<b>IP Assignment Mode</b>	Select the IP assignment mode: <i>Range</i> or <i>User Group</i> . This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IP Assignment</i> turned on.
<b>IP Assignment Type</b>	Select the IP assignment type: <i>IP</i> or <i>Subnet</i> . This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IP Assignment</i> turned on.
<b>IPv4 Start IP</b>	Enter the IPv4 start IP address. This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IP Assignment</i> turned on.
<b>IPv4 End IP</b>	Enter the IPv4 end IP address. This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IP Assignment</i> turned on.
<b>IPv4 Netmask</b>	Enter the IPv4 netmask. This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IP Assignment</i> turned on.
<b>Add Route</b>	Select to enable or disable adding a route for this gateway. This option is only available for dial up topologies.
<b>DNS Server #1 to #3</b>	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 <i>Hub</i> and either <i>Enable IKE Configuration Method</i> turned on, or <i>DNS Service</i> is set to <i>Specify</i> .
<b>WINS Server #1 and #2</b>	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 <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned on.
<b>IPv4 Split include</b>	Select the address or address group from the dropdown list. This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned on.
<b>Exclusive IP Range</b>	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 <i>Hub</i> and either <i>Enable IKE Configuration Method</i> and <i>Enable IP Assignment</i> turned on, or <i>Enable IKE Configuration Method</i> turned off.
<b>DHCP Server</b>	Select to enable or disable DHCP server. This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> is off.
<b>Default Gateway</b>	Enter the default gateway IP address. This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned off.
<b>DNS Service</b>	Select <i>Use System DNS setting</i> to use the system's DNS settings, or <i>Specify</i> to specify DNS servers #1 to #3. This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned off.
<b>Netmask</b>	Enter the netmask. This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned off.
<b>IPsec Lease Hold</b>	Enter the IPsec lease hold time. This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned off.
<b>Auto-Configuration</b>	Select to enable or disable automatic configuration. This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned off.
<b>DHCP Server IP Range</b>	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 <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned off.
<b>Advanced Options</b>	
<b>authpasswd</b>	Enter the XAuth client password for the FortiGate.
<b>authusr</b>	Enter the XAuth client user name for the FortiGate.
<b>banner</b>	Enter the banner value. Specify the message to send to IKE Configuration Method clients. Some clients display this message to users.
<b>dns-mode</b>	Select the DNS mode from the dropdown list: <ul style="list-style-type: none"> <li><i>auto</i>: Assign DNS servers in the following order: <ol style="list-style-type: none"> <li>Servers assigned to interfaces by DHCP</li> <li>Per-VDOM assigned DNS servers</li> <li>Global DNS servers</li> </ol> </li> <li><i>manual</i>: Use the DNS servers specified in <i>DNS Server #1 to #3</i>.</li> </ul>
<b>domain</b>	Enter the domain value.

<b>public-ip</b>	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.
<b>route-overlap</b>	Select the route overlap method from the dropdown list: <i>allow</i> , <i>use-new</i> , or <i>use-old</i> .
<b>spoke-zone</b>	Select a spoke zone from the dropdown list.
<b>unity-support</b>	Enable or disable unity support.
<b>vpn-interface-priority</b>	Set the VPN gateway interface priority. The default value is 1.
<b>vpn-zone</b>	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 > VPN Communities*.
2. Select a community from the communities dropdown in the toolbar, or double-click on a community in the list.
3. On the community information content pane, in the toolbar, select *Create New > External Gateway*. The *New VPN External Gateway* pane opens.

4. Configure the following settings, then click *OK* to create the external gateway:

<b>Node Type</b>	Select either <i>HUB</i> or <i>Spoke</i> from the dropdown list. This option is only available for star and dial up VPN topologies.
<b>Gateway Name</b>	Enter the gateway name.
<b>Gateway IP</b>	Select the gateway IP address from the dropdown list.
<b>Hub IP</b>	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 <i>Hub</i> .

<b>Create Phase2 per Protected Subnet Pair</b>	Toggle the switch to <i>On</i> to create a phase2 per protected subnet pair.
<b>Routing</b>	Select the routing method: <i>Manual (via Device Manager, or Automatic</i> . This option is only available for full meshed and star topologies.
<b>Peer Type</b>	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <i>Accept any peer ID</i></li> <li>• <i>Accept this peer ID</i>: Enter the peer ID in the text field</li> <li>• <i>Accept a dialup group</i>: Select a group from the dropdown list</li> </ul> <p>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.</p> <p>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.</p> <p>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.</p> <p>This option is only available for dial up topologies.</p>
<b>Protected Subnet</b>	Select a protected subnet from the list. You can add multiple subnets.
<b>Local Gateway</b>	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 > VPN Communities*.
2. Select a community from the communities dropdown in the toolbar, or double-click on a community in the *All Communities* pane.
3. Double-click on a gateway, right-click on a gateway and then 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.



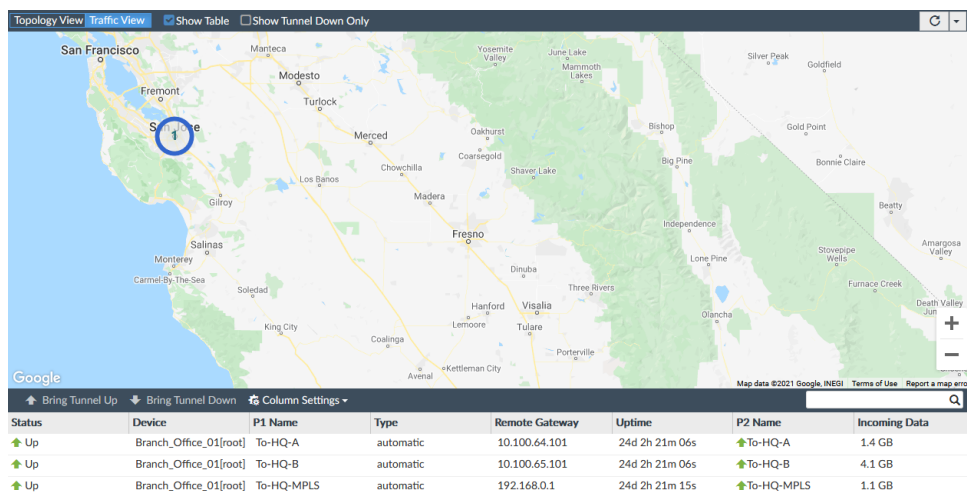
### To delete VPN gateways:

1. Go to *VPN Manager > IPsec VPN > VPN Communities*.
2. Select a community from the communities dropdown in the toolbar, or double-click on a community in the *All Communities* pane.
3. Select the gateway or gateways you need to delete.
4. Click *Delete* in the toolbar, or right-click and select *Delete*.
5. Select *OK* in the confirmation box to delete the gateway or gateways.

## Using Map View

The *Map View* 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.



The following options are available:

<b>Topology View</b>	The topology view shows the configured VPN gateways. See <a href="#">IPsec VPN gateways on page 536</a> .
<b>Traffic View</b>	The traffic view shows network traffic through the tunnels between protected subnets.
<b>Show Table</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• The topology table shows the VPN gateway list and toolbar, with a column added for location. See <a href="#">Managing VPN gateways on page 536</a> for information.</li> <li>• The traffic table shows the same information and options as the <i>Monitor</i> tab. See <a href="#">Monitoring IPsec VPN tunnels on page 544</a> for information.</li> </ul>
<b>Show Tunnel Down Only</b>	<p>Select to show only tunnels that are currently down.</p> <p>This option is only available on the traffic view.</p>

**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 100](#).

## Monitoring IPsec VPN tunnels

Go to *VPN Manager > IPsec VPN > Monitor* to view the list of IPsec VPN tunnels. You can also bring the tunnels up or down on this pane. Select a specific community from the tree menu to show only that community's tunnels.

<span>Bring Tunnel Up</span> <span>Bring Tunnel Down</span> <span>Refresh</span> <span>Column Settings</span>								
<input type="checkbox"/>	Status	Device	P1 Name	Type	Remote Gateway	Uptime	P2 Name	Incoming Data
<input type="checkbox"/>	Up	Branch_Office_01[root]	To-HQ-A	automatic	10.100.64.101	24d 2h 13m 20s	To-HQ-A	1.4 GB
<input type="checkbox"/>	Up	Branch_Office_01[root]	To-HQ-B	automatic	10.100.65.101	24d 2h 13m 20s	To-HQ-B	4.1 GB
<input type="checkbox"/>	Up	Branch_Office_01[root]	To-HQ-MPLS	automatic	192.168.0.1	24d 2h 13m 29s	To-HQ-MPLS	1.1 GB

### To bring tunnels up or down:

1. Go to *VPN Manager > IPsec VPN > Monitor*.
2. Find and select the tunnel or tunnels that you need to bring up or down in the list.
3. Click *Bring Tunnel Up* or *Bring Tunnel Down* from the toolbar or right-click menu
4. 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:

- [Manage SSL VPNs on page 544](#)
- [Portal profiles on page 547](#)
- [Monitoring SSL VPNs on page 553](#)

## Manage SSL VPNs

Go to *VPN Manager > SSL VPN > Settings* to manage SSL VPNs.

<span>Create New</span> <span>Edit</span> <span>Delete</span> <span>Column Settings</span>			
<input type="checkbox"/>	Device	Interface	Certificate
<input type="checkbox"/>	FGT54_1	loop1.port1	Fortinet_SSL
<input type="checkbox"/>	FGT54_2	loop1.port1	Fortinet_SSL

The following options are available:

<b>Install Wizard</b>	Launch the <i>Install Wizard</i> to install SSL VPN settings to devices.
<b>Create New</b>	Create a new SSL VPN with the <i>Create SSL VPN Settings</i> pane. See <a href="#">Creating SSL VPNs on page 545</a> .
<b>Edit</b>	Edit the selected VPN. This option is also available from the right-click menu. See <a href="#">Editing SSL VPNs on page 546</a> .
<b>Delete</b>	Delete the selected VPN or VPNs. This option is also available from the right-click menu. See <a href="#">Deleting SSL VPNs on page 547</a> .
<b>Column Settings</b>	Configure which columns are displayed, or click <i>Reset to Default</i> to reset the display to the default columns.
<b>Search</b>	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.

Create New SSL VPN Settings

Device:

**Connection Settings**

Listen on Interface(s):

Listen on Port:

Restrict Access: ☐ Allow access from any host ☐ Limit access to specific hosts

Idle Logout: ☐ OFF

Server Certificate:

Require Client Certificate: ☐ OFF

**Tunnel Mode Client Settings**

Address Range: ☐ Automatically assign addresses ☐ Specify custom IP ranges

DNS Server: ☐ Same as client system DNS ☐ Specify

Specify WINS Servers: ☐ OFF

Allow Endpoint Registration: ☐ OFF

**Authentication/Portal Mapping**

+ Create New ☒ Edit ☐ Delete ☐

#	User	Realm	Portal
1	All Other Users/Groups	/	

Advanced Options >

OK Cancel

3. Configure the following settings, then click *OK* to create the VPN.

<b>Device</b>	Select a FortiGate device or VDOM.
<b>Connection Settings</b>	Specify the connection settings.
<b>Listen on Interface(s)</b>	Define the interface the FortiGate will use to listen for SSL VPN tunnel requests. This is generally your external interface.
<b>Listen on Port</b>	Enter the port number for HTTPS access.

<b>Restrict Access</b>	Allow access from any hosts, or limit access to specific hosts. If limiting access, select the hosts that have access in the <i>Hosts</i> field.
<b>Idle Logout</b>	Select to enable idle timeout. When enabled, enter the amount of time that the connection can remain inactive before timing out in the <i>Inactive For</i> 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.
<b>Server Certificate</b>	Select the signed server certificate to use for authentication. Alternately, select a certificate template that is configured to use the FortiManager CA. See <a href="#">Certificate templates on page 268</a> .
<b>Require Client Certificate</b>	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.
<b>Tunnel Mode Client Settings</b>	Specify tunnel mode client settings. These settings determine how tunnel mode clients are assigned IP addresses.
<b>Address Range</b>	Either automatically assign address, or specify custom IP ranges.
<b>DNS Server</b>	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.
<b>Specify WINS Servers</b>	Select to specify WINS servers. Enter up to two WINS servers to be provided for the use of clients.
<b>Allow Endpoint Registration</b>	Select to allow endpoint registration.
<b>Authentication/Portal Mapping</b>	Select the users and groups that can access the tunnel. <b>Note:</b> the default portal cannot be empty.
<b>Create New</b>	Create a new authentication/portal mapping entry. Select the <i>Users</i> , <i>Groups</i> , <i>Realm</i> , and <i>Portal</i> , then click <i>OK</i> .
<b>Edit</b>	Edit the selected mapping.
<b>Delete</b>	Delete the selected mapping or mappings.
<b>Advanced Options</b>	Configure advanced SSL VPN options. For information, see the <i>FortiOS CLI Reference</i> .

## 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.

## Portal profiles

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 > Portal Profiles*.



The following options are available:

<b>Create New</b>	Create a new portal profile.
<b>Edit</b>	Edit the selected profile.
<b>Delete</b>	Delete the selected profile or profiles.
<b>Column Settings</b>	Adjust the visible columns.
<b>Search</b>	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 > Portal Profiles*.
2. Click *Create New* in the toolbar. The *Create New Portal Profile* pane is displayed.

Create New Portal Profile

Name

Limit Users to One SSL VPN Connection at a Time

OFF

Tunnel Mode

ON

Enable Split Tunneling ⓘ

ON

Routing Address

Click here to select

Source IP Pools

Click here to select

IPv6 Tunnel Mode

ON

IPv6 Split Tunneling

ON

IPv6 Routing Address

Click here to select

Source IPv6 Pools

Click here to select

Tunnel Mode Client Options

Allow client to save password

OFF

Allow client to connect automatically

OFF

Allow client to keep connections alive

OFF

Enable Web Mode

ON

Portal Message

SSL-VPN Portal

Theme

blue

Show Session Information

ON

Show Connection Launcher

ON

Show Login History

ON

User Bookmarks

ON

Predefined Bookmarks

+ Create New

✎ Edit

🗑 Delete

Name

Type

Location

Description

Enable FortiClient Download

ON

Download Method

Direct

SSL VPN Proxy

Customize Download Location

OFF

Advanced Options >

OK

Cancel

3. Configure the following settings, then select *OK* to create the profile.

<b>Name</b>	Enter a name for the portal.
<b>Limit Users to One SSL VPN Connection at a Time</b>	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.
<b>Tunnel Mode</b>	Select to configure and enable tunnel mode access. These settings determine how tunnel mode clients are assigned IPv4 addresses.
<b>Enable Split Tunneling</b>	Select so that the VPN carries only the traffic for the networks behind the FortiGate unit. The user's other traffic follows its normal route.
<b>Routing Address</b>	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.

<b>Source IP Pools</b>	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.
<b>IPv6 Tunnel Mode</b>	Select to configure and enable tunnel mode access. These settings determine how tunnel mode clients are assigned IPv6 addresses.
<b>Enable IPv6 Split Tunneling</b>	Select so that the VPN carries only the traffic for the networks behind the FortiGate unit. The user's other traffic follows its normal route.
<b>IPv6 Routing Address</b>	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.
<b>Source IP Pools</b>	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.
<b>Tunnel Mode Client Options</b>	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.
<b>Allow client to save password</b>	The user's password is stored on the user's computer and will automatically populate each time they connect to the VPN.
<b>Allow client to connect automatically</b>	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.
<b>Allow client to keep connections alive</b>	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.
<b>Enable Web Mode</b>	Select to enable web mode access.
<b>Portal Message</b>	The text header that appears on the top of the web portal.
<b>Theme</b>	A color styling specifically for the web portal: <i>blue</i> , <i>green</i> , <i>mariner</i> , <i>melongene</i> , or <i>red</i> .
<b>Show Session Information</b>	Display the <i>Session Information</i> 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.
<b>Show Connection Launcher</b>	Display the <i>Connection Launcher</i> 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.
<b>Show Login History</b>	Include user log in history on the web portal, then specify the number of history entries.
<b>User Bookmarks</b>	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.

<b>Pre-Defined Bookmarks</b>	The list of predefined bookmarks. Click <i>Create New</i> to add a bookmark. See <a href="#">Predefined bookmarks on page 550</a> for information.
<b>Enable FortiClient Download</b>	Select to enable FortiClient downloads.
<b>Download Method</b>	Select the method to use for downloading FortiClient from the SSL VPN portal. Choose between <i>Direct</i> and <i>SSL-VPN Proxy</i> . This option is only available when <i>Enable FortiClient Download</i> is <i>On</i> .
<b>Customize Download Location</b>	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 <i>Windows</i> box and/or <i>Mac</i> box. This option is only available when <i>Enable FortiClient Download</i> is <i>On</i> .
<b>Advanced Options</b>	Configure advanced options. For information, see the <i>FortiOS CLI Reference</i> .

## 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.

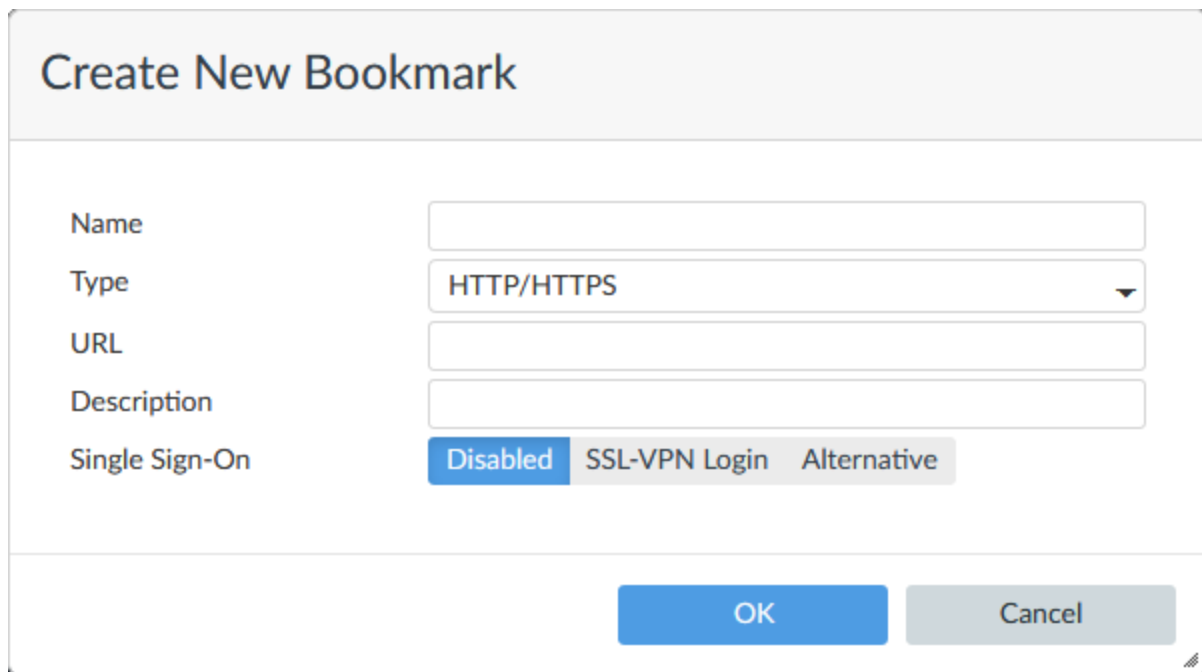
A web bookmark can include log in credentials to automatically log the SSL VPN user into the web site. When the administrator configures bookmarks, the web site credentials must be the same as the user's SSL VPN credentials. Users configuring their own bookmarks can specify alternative credentials for 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 > Portal Profiles*.
2. Edit an existing profile, or create a new profile. See [Editing portal profiles on page 552](#) or [Creating SSL VPN portal profiles on page 547](#).
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.





The dialog box titled "Create New Bookmark" contains the following fields and controls:

- Name:** A text input field.
- Type:** A dropdown menu with "HTTP/HTTPS" selected.
- URL:** A text input field.
- Description:** A text input field.
- Single Sign-On:** Three buttons: "Disabled" (highlighted in blue), "SSL-VPN Login", and "Alternative".
- Buttons:** "OK" (blue) and "Cancel" (grey) buttons at the bottom right.

4. Configure the following settings, then select **OK** to create the bookmark.

<b>Name</b>	Enter a name for the bookmark.
<b>Type</b>	Select the bookmark type: <i>CITRIX</i> , <i>FTP</i> , <i>HTTP/HTTPS</i> , <i>Port Forward</i> , <i>RDP</i> , <i>SMB</i> , <i>SSH</i> , <i>Telnet</i> , or <i>VNC</i> .
<b>URL</b>	Enter the bookmark URL. This option is only available when <i>Type</i> is <i>Citrix</i> , or <i>HTTP/HTTPS</i> .
<b>Folder</b>	Enter the bookmark folder. This option is only available when <i>Type</i> is <i>FTP</i> or <i>SMB</i> .
<b>Host</b>	Enter the host name. This option is only available when <i>Type</i> is <i>Port Forward</i> , <i>RDP</i> , <i>SSH</i> , <i>TELNET</i> , or <i>VNC</i> .
<b>Remote Port</b>	Enter the remote port. This option is only available when <i>Type</i> is <i>Port Forward</i> .
<b>Listening Port</b>	Enter the listening port. This option is only available when <i>Type</i> is <i>Port Forward</i> .
<b>Show Status Window</b>	Enable to show the status window. This option is only available when <i>Type</i> is <i>Port Forward</i> .
<b>Port</b>	Enter the port number. This option is only available when <i>Type</i> is <i>RDP</i> or <i>VNC</i> .
<b>Username</b>	Enter the user name. This option is only available when <i>Type</i> is <i>RDP</i> .
<b>Password</b>	Enter the password.

	This option is only available when <i>Type</i> is <i>RDP</i> or <i>VNC</i> .
<b>Keyboard Layout</b>	<p>Select the keyboard layout: <i>German (QWERTZ)</i>, <i>English (US)</i>, <i>Unknown</i>, <i>French (AZERTY)</i>, <i>Italian</i>, or <i>Swedish</i>.</p> <p>This option is only available when <i>Type</i> is <i>RDP</i>.</p>
<b>Security</b>	<p>Select the security type: <i>Allow the server to choose the type of security</i>, <i>Network Level Authentication</i>, <i>Standard RDP encryption</i>, or <i>TLS encryption</i>.</p> <p>This option is only available when <i>Type</i> is <i>RDP</i>.</p>
<b>Description</b>	Optionally, enter a description of the bookmark.
<b>Single Sign-on</b>	<p>Select the SSO setting for links that require authentication: <i>Disabled</i>, <i>Automatic</i>, or <i>Static</i>.</p> <p>If <i>Static</i> is selected, click the add icon, then enter the <i>Name</i> and <i>Value</i> to add SSO Form Data. Multiple fields can be added. Click <i>Remove</i> to remove a field.</p> <p>When including a link using SSO use the entire URL, not just the IP address.</p> <p>This option is only available when <i>Type</i> is <i>Citrix</i>, <i>FTP</i>, <i>HTTP/HTTPS</i>, <i>RDP</i>, or <i>SMB</i>.</p> <p>The <i>Static</i> option is only available when <i>Type</i> is <i>Citrix</i>, <i>HTTP/HTTPS</i>, or <i>RDP</i>.</p>

#### To edit a bookmark:

1. Go to *VPN Manager > SSL-VPN > Portal Profiles*.
2. Edit an existing profile, or create a new profile. See [Editing portal profiles on page 552](#) or [Creating SSL VPN portal profiles on page 547](#).
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 > Portal Profiles*.
2. Edit an existing profile, or create a new profile. See [Editing portal profiles on page 552](#) or [Creating SSL VPN portal profiles on page 547](#).
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 > Portal 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 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 > Portal 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 selected profile or profiles.

## Monitoring SSL VPNs

SSL VPNs can be monitored by going to *VPN Manager > SSL VPN > Monitor*.

The following information is shown:

<b>Device</b>	The device or VDOM name.
<b>User</b>	The user name.
<b>Remote Host</b>	The remote host.
<b>Last Login</b>	The time of the last log in.
<b>Active Connections</b>	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 322](#) 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:

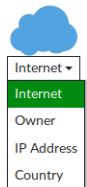
- [Security Fabric Topology on page 556](#)
- [Physical Topology on page 557](#)
- [Logical Topology on page 558](#)
- [Filter Topology Views on page 559](#)
- [Search Topology Views on page 560](#)
- [Security Rating on page 560](#)
- [Fabric Connectors on page 563](#)

## 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.

### WAN Cloud Icon

The WAN cloud icon, 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 WAN cloud icon to Owner, the destination hosts are simplified to a fixed size 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.

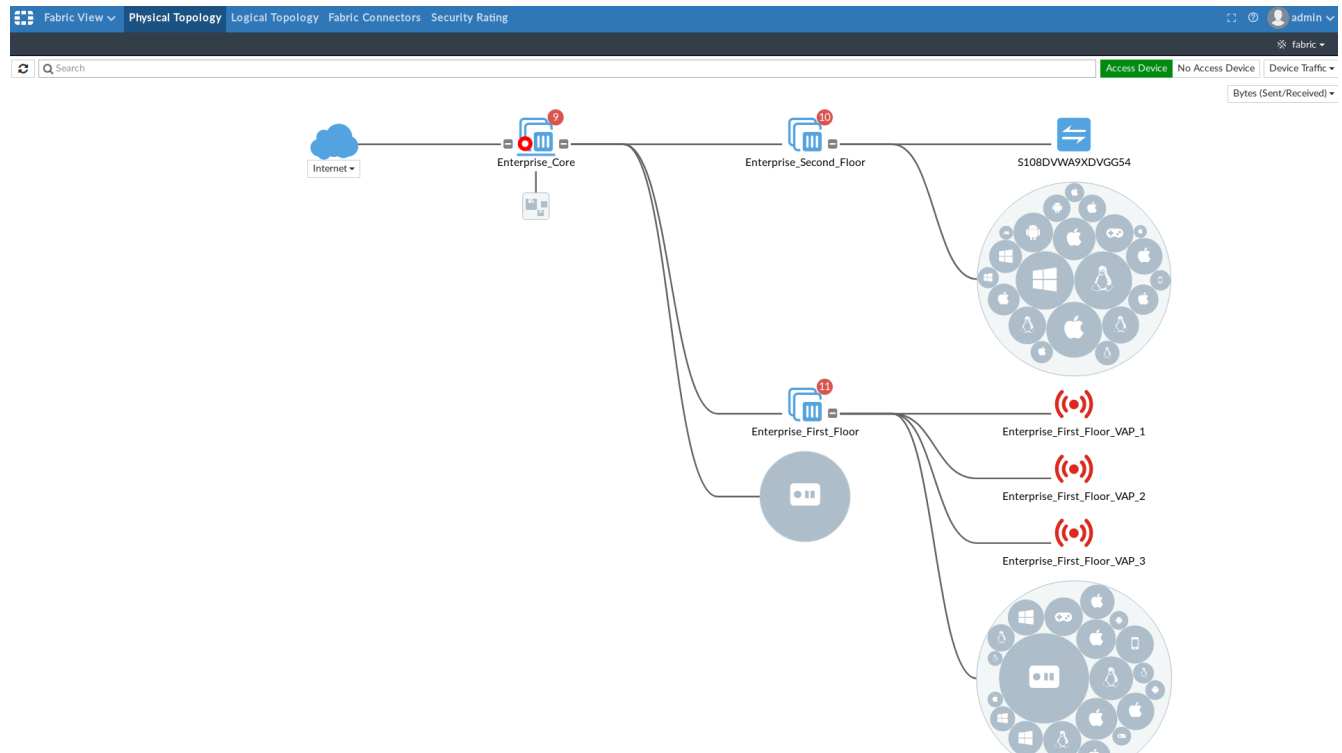
### Switch stacking

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*.



The Physical Topology view displays your network as a bubble chart of interconnected devices. These devices are grouped based on the upstream device they are connected to. The bubbles appear smaller or larger, based on their traffic volume. You can double-click any bubble to resize it and view more information about the device. FortiGate devices and other networking devices are depicted as boxes.

You can hover over the icon for each FortiGate to see information, such as serial number, hostname, and firmware version. You can hover over the bubbles of other devices to see information about them, such as name, IP address, and traffic volume data.

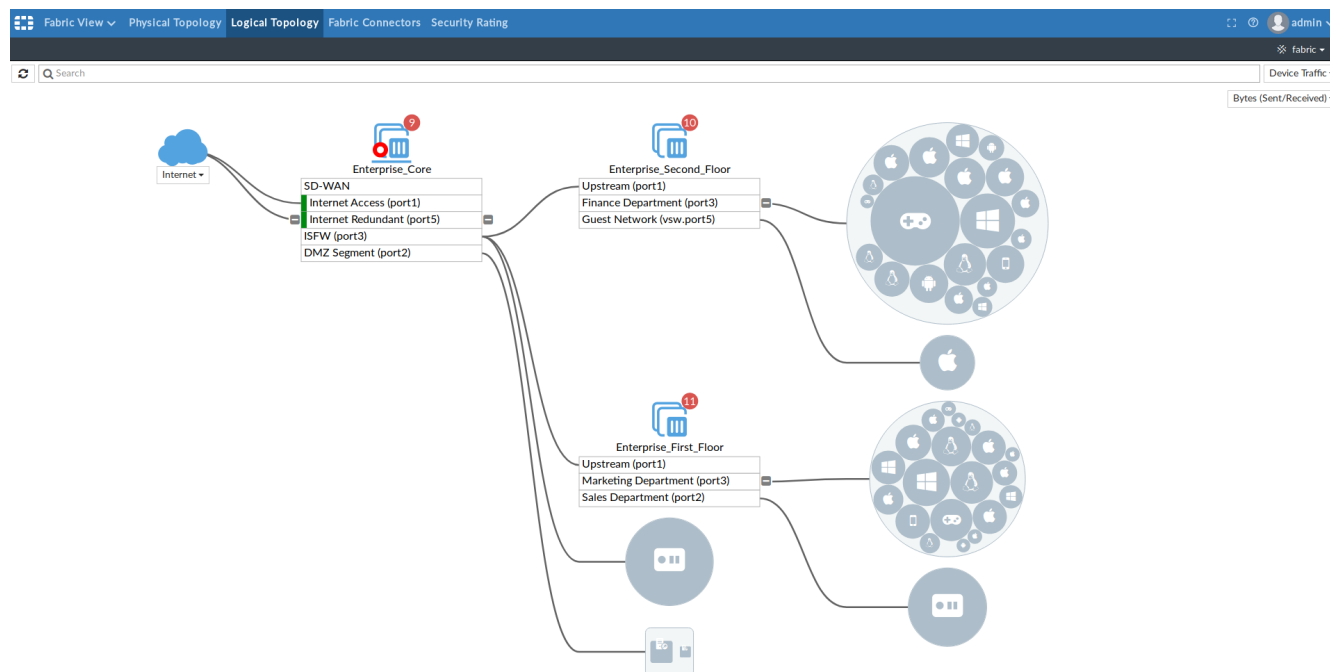
FortiGate	Enterprise_First_Floor
Hostname	Enterprise_First_Floor
Serial	FGVM010000154924
Model	FortiGate VM64-KVM
Version	v6.2.0 build0776
Operation Mode	NAT
Inspection Mode	Proxy-based
Topology	Enterprise_Core Enterprise_First_Floor 3 Downstream Fabric Devices
Management IP	10.100.88.101
CPU Usage	1%
Memory Usage	48%

Security Fabric Rating recommendations are also shown in the topology, beside the icon of the device the recommendations apply to.

## 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 bubble chart of network connection endpoints. These devices are grouped based on the upstream device interface they are connected to. The bubbles appear smaller or larger, based on their traffic volume. You can double-click any bubble to re-size it. FortiGate devices and other networking devices are depicted as boxes.

You can hover over the icon for each FortiGate 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. You can hover over the name of an interface to see its IP address, network (subnet), and role.



FortiGate	 Enterprise_First_Floor
Hostname	Enterprise_First_Floor
Serial	FGVM010000154924
Model	FortiGate VM64-KVM
Version	v6.2.0 build0776
Operation Mode	NAT
Inspection Mode	Proxy-based
Topology	 Enterprise_Core └─  Enterprise_First_Floor └─ 3 Downstream Fabric Devices
Management IP	10.100.88.101
CPU Usage	1%
Memory Usage	48%

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 drop-down menu to the right of the *Search* field, select one of the following:

Device Traffic ▾  
Device Traffic  
Device Count  
Device Type  
Vulnerability  
No Devices

- Device Traffic
- Device Count
- Device Type
- Vulnerability
- No Device

**To filter the topology views by traffic options:**

To sort the topology by traffic options, in the *Sort By* drop-down menu, select one of the following:

Bytes (Sent/Received) ▾  
Bytes (Sent/Received)  
Packets (Sent/Received)  
Bandwidth  
Sessions

- Bytes (Sent/Received)
- Packets (Sent/Received)
- Bandwidth
- Session

## 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.

To see a list of items that you can search for, mouse over the search bar and a tool tip appears that shows Searchable Information list, organized by host and by Fortinet device type. The following image shows the search bar and the Searchable Information list:

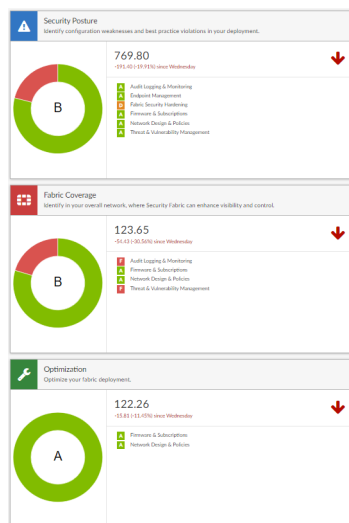
Searchable Information	
Host	Status, Host Name, Server, MAC Address, Other MAC Addresses, IP Address, Interface, Online Interfaces, Operating System, User, Comment, Authorized User, Unauthorized User
FortiGate	Serial Number, Host Name, Management IP, Model Label, Operating Mode, Parent, Version, IP Address
FortiSwitch	Serial Number, Name, Version
FortiAP	Serial Number, Name, Version

- For hosts, you can search for host information, such as status, host name, and server.
- For FortiGate, you can search for device information, such as serial number, host name, and management IP address.
- For FortiSwitch and FortiAP, you can search for device information, such as serial number, name and OS version.

## Security Rating

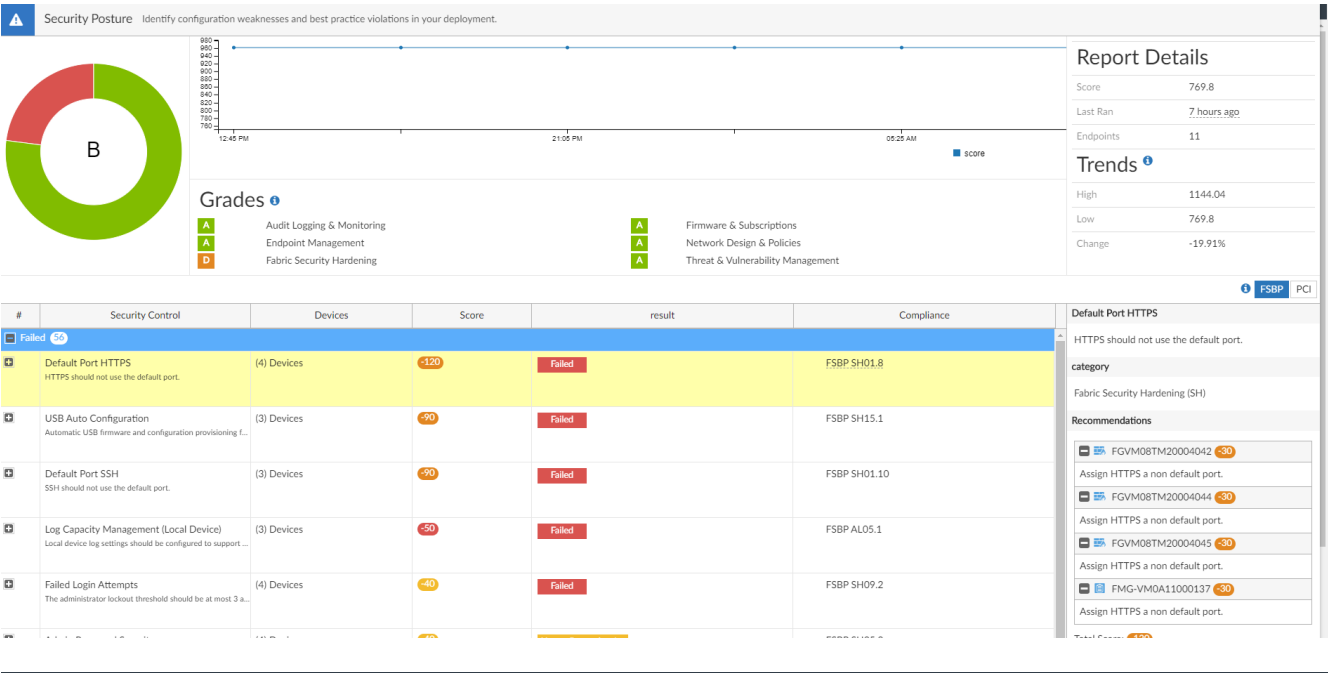
The *Fabric View > Security Rating* pane displays Security Fabric Ratings of configurations for FortiGate Security Fabric groups. You can view the results for multiple FortiGate Security Fabric groups. You must generate the Security Fabric Ratings by using FortiOS before you can view the information in 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 current view, click the icon beside 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.

## Enabling the Security Rating tab

The *Security Rating* tab is displayed when FortiManager is managing FortiGate units that have Security Fabric enabled and are part of a Security Fabric group.

If ADOMs are enabled in FortiManager, the *Security Rating* tab is only available in FortiGate ADOMs that contain a Security Fabric group.

## Viewing Security Fabric Ratings

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.



You cannot use FortiManager to generate Security Fabric Ratings; you must use FortiOS to generate Security Fabric Ratings for a FortiGate Security Fabric group, and then you can see the Security Fabric Ratings in FortiManager.

For more information about each of the checks that are performed, see the [Fortinet Recommended Security Best Practices](#) document.

### To view Security Fabric Ratings:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Fabric View > Security Rating*.
3. In the tree menu, select the *Security Fabric* group.  
The Security Fabric Rating results are displayed in the content pane for the selected Security Fabric group.  
You can filter the results. For example, you can view only failed results by clicking the *Failed <number>* button, and you can click the *All Results <number>* button to view all results again.
4. In the content pane, select *All FortiGates* to view results for all FortiGates in the group, or select individual FortiGate units to display results for only the selected unit.

## 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 calculate 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 563](#)

## 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 563](#)

### 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 ZTNA tags in policies. See [Zero Trust Network Access \(ZTNA\) objects on page 442](#) and [Configuring a ZTNA server on page 445](#).



FortiClient EMS connectors can also be configured from *Policy & Objects > Object Configurations > Fabric Connectors > 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*.

<b>Name</b>	Enter a name for the FortiClient EMS connector.
<b>Status</b>	Set the status of the connector to enabled.
<b>Type</b>	Select <i>FortiClient EMS</i> .
<b>IP/Domain name</b>	Enter the IP or domain name for the FortiClient EMS.
<b>HTTPS port</b>	Enter the HTTPS port for the FortiClient EMS.
<b>User Name</b>	Enter the FortiClient EMS administrator user name.
<b>Password</b>	Enter the FortiClient EMS administrator password.
<b>EMS Threat Feed</b>	Toggle ON to allow FortiManager to pull FortiClient malware hash from FortiClient EMS.
<b>Synchronize firewall addresses</b>	Toggle ON to automatically create and synchronize firewall addresses for all EMS tags.

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*.

<b>Name</b>	Enter a name for the FortiClient EMS connector.
<b>Status</b>	Set the status of the connector to enabled.
<b>Type</b>	Select <i>FortiClient EMS Cloud</i> .
	 <p>FortiManager can only connect to the FortiClient EMS Cloud that is registered to the same FortiCloud account.</p>
<b>EMS Threat Feed</b>	Toggle ON to allow FortiManager to pull FortiClient malware hash from FortiClient EMS.
<b>Synchronize firewall addresses</b>	Toggle ON to automatically create and synchronize firewall addresses for all EMS tags.
<b>Advanced Options</b>	Click to open and configure advanced options for the FortiClient EMS Cloud connector.

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 > Object Configurations > Firewall Objects > ZTNA Tags*.  
You can see imported IP and MAC tags available on the page. See [Viewing ZTNA tags on page 443](#).

**To use ZTNA 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 369](#).
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 568](#)
  - [Creating Microsoft Azure fabric connectors on page 569](#)
  - [Creating Google Cloud Platform connector on page 586](#)

- [Creating Oracle Cloud Infrastructure \(OCI\) connector on page 579](#)
- [Creating AliCloud Service connector on page 584](#)
- [Creating IBM Cloud connector on page 587](#)
- Private SDN
  - [Creating Kubernetes connector on page 582](#)
  - [Creating VMWare ESXi connector on page 580](#)
  - [Creating VMware NSX fabric connectors on page 571](#)
  - [Creating OpenStack \(Horizon\) connector on page 577](#)
  - [Creating ACI fabric connectors on page 566](#)
  - [Creating Nuage fabric connectors on page 573](#)
  - [Create Nutanix fabric connectors on page 575](#)

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 589](#)
- [Configuring dynamic firewall addresses for fabric connectors on page 590](#)

## 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.

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 > Fabric > 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.



Create New Fabric Connector - Application Centric Infrastructure (ACI) (2/2)

Type: Application Centric Infrastructure (ACI)

Connector Settings

Name:

Status: ☒

Cisco ACI Connector

ACI Type: FortiSDN Connector | Direct Connection

IP:

Port: Use Default | Specify

Username:

Password:

Advanced Options >

Revision

Change Note:

Revision History

Revert View Diff Search...

Revision #	Changed by	Date/Time	Entry Key	Entry name	Action	Change Note
------------	------------	-----------	-----------	------------	--------	-------------

Back OK Cancel

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

<b>Type</b>	Displays <i>Application Centric Infrastructure (ACI)</i> .
<b>Name</b>	Type a name for the fabric connector object.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
<b>ACI Type</b>	Select the <i>FortiSDN Connector</i> or <i>Direct Connection</i> .
<b>IP</b>	Type the IP address.
<b>Port</b>	Identify the port used for Fortinet SDN Connector. Perform one of the following options: <ul style="list-style-type: none"> <li>Click <i>Use Default</i> to use the default port.</li> <li>Click <i>Specify</i> and type the port number.</li> </ul>
<b>User Name</b>	Type the user name for Fortinet SDN Connector.
<b>Password</b>	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 589](#) and [Configuring dynamic firewall addresses for fabric connectors on page 590](#).

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 335](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 314](#).  
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 > Fabric > 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.

Create New Fabric Connector - Amazon Web Services (AWS) (2/2)

Type: Amazon Web Services (AWS)

Connector Settings

Name:

Status: ☒

Update Interval(s):

AWS Connector

Use Metadata IAM: ☒

Access Key ID:

Secret Access Key:

Region Name:

VPC ID: ☒

Advanced Options >

Revision

Change Note\*:

Revision History

<input type="checkbox"/>	Revision #	Changed by	Date/Time	Entry Key	Entry name	Action	Change Note
No record found.							

3. Configure the following options, and then click *OK*:

<b>Type</b>	Displays <i>Amazon Web Services (AWS)</i> .
<b>Name</b>	Type a name for the fabric connector object.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
<b>Update Interval (s)</b>	Specify how often in seconds that the dynamic firewall objects should be updated.
<b>Access Key ID</b>	Type the access key ID from AWS.
<b>Secret Access key</b>	Type the secret access key from AWS.
<b>Region Name</b>	Type the region name from AWS.
<b>VPC ID</b>	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 589](#) and [Configuring dynamic firewall addresses for fabric connectors on page 590](#).
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 335](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 314](#).  
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.

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 > Fabric > 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.

The screenshot shows the 'Create New Fabric Connector - Microsoft Azure (2/2)' configuration window. The 'Type' is set to 'Microsoft Azure'. Under 'Connector Settings', there are fields for 'Name', 'Status' (toggle), and 'Update Interval(s)' with 'Use Default' and 'Specify' buttons. The 'Microsoft Azure Connector' section includes 'Use Managed Identity' (toggle), 'Server Region' (dropdown), 'Directory ID', 'Application ID', 'Client Secret' (password field), and 'Resource Path' (toggle). Below this is the 'Advanced Options' section. The 'Revision' section has a 'Change Note' text area. At the bottom, there is a 'Revision History' table with columns: Revision #, Changed by, Date/Time, Entry Key, Entry name, Action, and Change Note. The table currently shows 'No record found.' and has 'Revert' and 'View Diff' buttons. At the very bottom are 'Back', 'OK', and 'Cancel' buttons.

3. Configure the following options, and then click *OK*:

<b>Type</b>	Displays <i>Microsoft Azure</i> .
<b>Name</b>	Type a name for the fabric connector object.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
<b>Update Interval (s)</b>	Specify how often in seconds that the dynamic firewall objects should be updated.
<b>Server Region</b>	Select an Azure region.
<b>Directory ID</b>	Enter the directory ID for your Azure AD tenant with Azure AD.
<b>Application ID</b>	Enter the application ID for your Azure application with Azure AD.
<b>Client Secret</b>	Enter the application secret created for your Azure application with Azure AD.
<b>Resource Path</b>	Optionally, enable the resource path to configure the <i>Subscription ID</i> and <i>Resource Group</i> .

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 589](#) and [Configuring dynamic firewall addresses for fabric connectors on page 590](#).
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 335](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 314](#).  
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 > Fabric > 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.

Create New Fabric Connector - VMware NSX-V (2/2)

Type: VMware NSX-V

Connector Settings

Name:

Status: ☒

Update Interval(s):

NSX Connector

Server:

Username:

Password:

VMX

Service Name:

Image Location:

REST API

Port:

Interface:

Password:

Advanced Options >

Revision

Change Note\*

3. Configure the following options, and then click *OK*:

<b>Type</b>	Displays <i>VMware NSX</i> .
<b>Name</b>	Type a name for the fabric connector object.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
<b>Update Interval (s)</b>	Specify how often in seconds that the dynamic firewall objects should be updated.
<b>Server</b>	Type the IP address for VMware NSX.
<b>Username</b>	Type the username for VMware NSX.
<b>Password</b>	Type the password for VMware NSX.
<b>VMX</b>	The VMX options identify settings used by the FortiGate VMX Service Manager to communicate with the REST API for NSX Manager.
<b>Service Name</b>	Type the name of the FortiGate VMX service defined on NSX Manager.
<b>Image Location</b>	Type the location of the FortiGate VMX deployment template used by NSX Manager to deploy the FortiGate VMX service.

<b>REST API</b>	The REST API options specify how the FortiGate VMX Service Manager communicates with the REST API for NSX Manager.
<b>Port</b>	Type the port used by the FortiGate VMX Service Manager to communicate with NSX Manager.
<b>Interface</b>	Select the interface used by the FortiGate VMX Service Manager to communicate with NSX Manager. Choose between <i>MGMT</i> and <i>Sync</i> .
<b>Password</b>	Type the password that FortiGate VMX Service Manager uses with the REST API to communicate with NSX Manager. <b>Note:</b> 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 589](#) and [Configuring dynamic firewall addresses for fabric connectors on page 590](#).
2. Create a virtual wire pair. See [Creating virtual wire pairs on page 416](#).
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 335](#).
4. Install the policy package to FortiGate. See [Install a policy package on page 314](#).  
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 > Fabric > 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**:

<b>Type</b>	Displays <i>Nuage Virtualized Services Platform</i> .
<b>Name</b>	Type a name for the fabric connector object.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
<b>IP</b>	Type the IP address.
<b>Port</b>	Perform one of the following options: <ul style="list-style-type: none"> <li>Click <i>Use Default</i> to use the default port.</li> <li>Click <i>Specify</i> and type the port number.</li> </ul>
<b>User Name</b>	Type the Nuage user name.
<b>Password</b>	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 589](#) and [Configuring dynamic firewall addresses for fabric connectors on page 590](#).
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 335](#).



3. Install the policy package to FortiGate. See [Install a policy package on page 314](#).  
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.

### To create a Nutanix fabric connector:

1. Go to *Fabric View > Fabric > 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.

**Edit SDN Connector**

Type: Nutanix

**Connector Settings**

Name: NutanixConnector

Status: ☒

Update Interval(s): [Use Default](#) [Specify](#)

**Nutanix Connector**

IP:

Port: [Use Default](#) [Specify](#)

Username:

Password:

**Advanced Options** >

**Revision**

Change Note\*  0/1023

**Revision History**

[↶ Revert](#) [📄 View Diff](#)

<input type="checkbox"/>	Revision #	Changed by	Date/Time	Action	Change Note	
--------------------------	------------	------------	-----------	--------	-------------	--

[OK](#) [Cancel](#)

3. Configure the following options, and then click *OK*.

<b>Type</b>	Displays <i>Nutanix</i> .
<b>Name</b>	Enter a name for the connector.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
<b>Update Interval(s)</b>	Specify how often in seconds that the dynamic firewall objects should be updated.
<b>IP</b>	Type the IP address for Nutanix.
<b>Port</b>	Select <i>Use Default</i> or <i>Specify</i> and enter the desired port.
<b>Username</b>	Enter the Nutanix account username.

<b>Password</b>	Enter your Nutanix account password.
<b>Advanced Options</b>	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 589](#) and [Configuring dynamic firewall addresses for fabric connectors on page 590](#).
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 335](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 314](#).  
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 > Fabric > 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.

Create New Fabric Connector - OpenStack (Horizon) (2/2)

Type: OpenStack (Horizon)

Connector Settings

Name:

Status: ☒

Update Interval(s):

OpenStack Connector

Server:

Username:

Password:

Domain:

Advanced Options >

Revision

Change Note\*:

Revision History

<input type="checkbox"/>	Revision #	Changed by	Date/Time	Entry Key	Entry name	Action	Change Note
--------------------------	------------	------------	-----------	-----------	------------	--------	-------------

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

<b>Type</b>	Displays OpenStack (Horizon).
<b>Name</b>	Type a name for the fabric connector object.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
<b>Update Interval (s)</b>	Select one of the following options: <ul style="list-style-type: none"><li>Click <i>Use Default</i> to use the default interval.</li><li>Click <i>Specify</i> and specify the interval.</li></ul>
<b>Server</b>	Type the IP address for the server.
<b>User Name</b>	Type the OpenStack Connector administrator user name.
<b>Password</b>	Type the OpenStack Connector administrator password.
<b>Domain</b>	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 589](#) and [Configuring dynamic firewall addresses for fabric connectors on page 590](#).

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 335](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 314](#).  
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 > Fabric > 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.

Create New Fabric Connector - Oracle Cloud Infrastructure (OCI) (2/2)

Type: Oracle Cloud Infrastructure (OCI)

Connector Settings

Name:

Status: ☒

Update Interval(s):

OCI Connector

Use Metadata IAM: ☒

Server Region Type: Commercial

Server Region:

User ID:

Tenant ID:

Compartment ID:

Certificate:

System Certificate for Connection:

Advanced Options >

Revision

Change Note\*

0/1023

3. Configure the following options, and then click *OK*:

<b>Type</b>	Displays Oracle Cloud Infrastructure (OCI).
<b>Name</b>	Type a name for the fabric connector object.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
<b>Update Interval (s)</b>	Select one of the following options: <ul style="list-style-type: none"> <li>Click <i>Use Default</i> to use the default interval.</li> <li>Click <i>Specify</i> and specify the interval.</li> </ul>
<b>Server Region</b>	Select the OCI Server Region from the drop-down.
<b>User ID</b>	Type the OCI User ID.
<b>Tenant ID</b>	Type the OCI Tenant ID.
<b>Compartment ID</b>	Type the OCI Compartment ID.
<b>Certificate</b>	Select the OCI Certificate from the drop-down.
<b>System Certificate for Connection</b>	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 589](#) and [Configuring dynamic firewall addresses for fabric connectors on page 590](#).
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 335](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 314](#).  
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 fabric connector for VMWare ESXi, and then import address names from VMWare ESXi 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 ESXi and dynamically populate the objects with IP addresses.

When you create a fabric connector for VMWare ESXi, you are specifying how FortiGate can communicate directly with VMWare ESXi.

#### Requirements:

- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with VMWare ESXi.

### To create a fabric connector object for VMWare ESXi:

1. Go to *Fabric View > Fabric > 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.

Create New Fabric Connector - VMWare ESXi (2/2)

Type: VMWare ESXi

**Connector Settings**

Name:

Status: ☒

Update Interval(s):

**ESXi Connector**

Server:

Username:

Password:

**Advanced Options**

Revision

Change Note:

Revision History

<input type="checkbox"/>	Revision #	Changed by	Date/Time	Entry Key	Entry name	Action	Change Note
No record found.							

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

<b>Name</b>	Type a name for the fabric connector object.
<b>Type</b>	Displays VMWare ESXi.
<b>Server</b>	Type the IP address for VMWare ESXi.
<b>User Name</b>	Type the VMWare ESXi user name.
<b>Password</b>	Type the VMWare ESXi password.
<b>Update Interval (s)</b>	Select one of the following options: <ul style="list-style-type: none"> <li>Click <i>Use Default</i> to use the default interval.</li> <li>Click <i>Specify</i> and specify the interval.</li> </ul>
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.

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 589](#) and [Configuring dynamic firewall addresses for fabric connectors on page 590](#).
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 335](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 314](#).  
FortiGate communicates with the SDN to dynamically populate the firewall address objects with IP addresses.

## 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 > Fabric > 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.

Create New Fabric Connector - Kubernetes (2/2) ✕

Type Kubernetes

Connector Settings

Name

Status ☒

Update Interval(s) ? Use Default Specify

Kubernetes Connector

IP

Port Use Default Specify

Secret Token

Advanced Options >

Revision

Change Note\*  0/1023

Revision History

↶ Revert 📄 View Diff Search...

<input type="checkbox"/>	Revision #	Changed by	Date/Time	Entry Key	Entry name	Action	Change Note	⚙
No record found.								

Back OK Cancel

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

Type	Displays Kubernetes.
Name	Type a name for the fabric connector object.
Status	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
Update Interval (s)	Select one of the following options: <ul style="list-style-type: none"><li>Click <i>Use Default</i> to use the default interval.</li><li>Click <i>Specify</i> and specify the interval.</li></ul>
IP	Type the IP address for Kubernetes.
Port	Select one of the following options: <ul style="list-style-type: none"><li>Click <i>Use Default</i> to use the default port.</li><li>Click <i>Specify</i> and specify the port.</li></ul>
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 589](#) and [Configuring dynamic firewall addresses for fabric connectors on page 590](#).
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 335](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 314](#).  
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 > Fabric > 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.

Create New Fabric Connector - AliCloud (2/2)

Type: Alibaba Cloud Service (ACS)

Connector Settings

Name:

Status: ☒

Update Interval(s):

AliCloud Connector

Access Key ID:

Access Key Secret:

Region ID:

Advanced Options >

Revision

Change Note\*:

0/1023

Revision History

<input type="checkbox"/>	Revision #	Changed by	Date/Time	Entry Key	Entry name	Action	Change Note	<input type="button" value="Settings"/>
No record found.								

3. Configure the following options, and then click *OK*:

<b>Type</b>	Displays Alibaba Cloud Service (ACS).
<b>Name</b>	Type a name for the fabric connector object.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
<b>Update Interval (s)</b>	Select one of the following options: <ul style="list-style-type: none"> <li>Click <i>Use Default</i> to use the default interval.</li> <li>Click <i>Specify</i> and specify the interval.</li> </ul>
<b>AccessKey ID</b>	Specify the AccessKey ID for AliCloud.
<b>AccessKey Secret</b>	Specify the AccessKey Secret for AliCloud.
<b>Region ID</b>	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 589](#) and [Configuring dynamic firewall addresses for fabric connectors on page 590](#).

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 335](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 314](#).  
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 > Fabric > 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.

Create New Fabric Connector - Google Cloud Platform (GCP) (2/2)

Type: Google Cloud Platform (GCP)

**Connector Settings**

Name:

Status: ☒

Update Interval(s):

**GCP Connector**

Use Metadata IAM: ☒

Projects:

Project Name:

Service Account Email:

Private Key:

**Advanced Options** >

**Revision**

Change Note\*:

0/1023

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

<b>Type</b>	Displays Google Cloud Platform (GCP).
<b>Name</b>	Type a name for the fabric connector object.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
<b>Update Interval (s)</b>	Select one of the following options: <ul style="list-style-type: none"> <li>Click <i>Use Default</i> to use the default interval.</li> <li>Click <i>Specify</i> and specify the interval.</li> </ul>
<b>Projects</b>	Select <i>Simple</i> or <i>Advanced</i> . When <i>Advanced</i> is selected, you can add <i>GCP Projects</i> .
<b>Project Name</b>	Specify the Project Name for the GCP.
<b>Service Account Email</b>	Specify the Service Account Email for GCP.
<b>Private Key</b>	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 589](#) and [Configuring dynamic firewall addresses for fabric connectors on page 590](#).
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 335](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 314](#).  
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 > Fabric > 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.

Create New Fabric Connector - IBM Cloud (2/2)

Type: IBM Cloud

Connector Settings

Name:

Status: ☒

Update Interval(s):

IBM Cloud Connector

Compute Generation:

Region: Dallas

API Key:

Advanced Options >

Revision

Change Note\*:

Revision History

<input type="checkbox"/>	Revision #	Changed by	Date/Time	Entry Key	Entry name	Action	Change Note
No record found.							

3. Configure the following options, and then click *OK*.

<b>Type</b>	Displays <i>IBM Cloud</i> .
<b>Name</b>	Enter a name for the connector.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
<b>Update Interval(s)</b>	Specify how often in seconds that the dynamic firewall objects should be updated.
<b>Compute Generation</b>	Specify the IBM Cloud computer generation.
<b>Region</b>	Select your IBM Cloud region from the dropdown list.
<b>API Key</b>	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 589](#) and [Configuring dynamic firewall addresses for fabric connectors on page 590](#).
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 335](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 314](#).  
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 590](#).

### To import address names for SDN connectors:

1. Go to *Policy & Objects > Object Configurations*.
2. In the tree menu, go to *External Connectors > Public SDN/Private SDN*.
3. In the content pane, right-click the fabric connector, and select *Import*.  
The *Import SDN Connector* dialog box is displayed.

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 566](#).

### To import by endpoint groups (EPGs) for ACI connectors:

1. Go to *Policy & Objects > Object Configurations > External Connectors > Private SDN*
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 > Object Configurations > 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 for fabric connectors:

1. Go to *Policy & Objects > Object Configurations*.
2. In the tree menu, go to *Firewall Objects > Addresses*.
3. In the content pane, click *Create New* and select *Address*.
4. Configure the firewall address settings for your chosen fabric connector:

<b>Address Name</b>	Type a name for the firewall address object.
<b>Type</b>	Select <i>Dynamic</i> .
<b>Sub Type</b>	Select <i>Fabric Connector Address</i> .
<b>SDN Connector</b>	Select the fabric connector.

5. Configure the remaining settings as needed, 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*.

<b>Name</b>	Type a name for the virtual wire pair.
<b>Interface Members</b>	Select two interface members.
<b>Wildcard VLAN</b>	<p>Toggle <i>ON</i> 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.</p> <p>Toggle <i>OFF</i> to disable wildcard VLANs for the virtual wire pair.</p>

## Threat Feeds

You can use the *Fabric > 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

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 591](#)

## 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 > Fabric > 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*:

<b>Name</b>	Type a name for the fabric connector object.
<b>URI of external resource</b>	Type the link to an external text file. The path must start with <code>http://</code> , <code>https://</code> , or <code>fmg://</code> , for example, <code>http://example.com/url</code> .

<b>HTTP Basic Authentication</b>	Toggle <i>On</i> to enable basic HTTP authentication, and type a username and password. Toggle <i>Off</i> to disable basic HTTP authentication.
<b>Category ID</b>	Type the category ID. The ID is between 192 and 221. Available only when <i>Type</i> displays <i>Domain List</i> .
<b>Refresh Rate</b>	The time in minutes to refresh the external resource.
<b>Comments</b>	(Optional) Type comments about the connector.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>Off</i> to disable the fabric connector object.
<b>Update Method</b>	Select the update method: <ul style="list-style-type: none"> <li>• <i>External Feed</i>: The threat feed will periodically fetch entries from the URI using HTTP or HTTPS.</li> <li>• <i>Push API</i>: The threat feed receives entry updates from webhook requests to the FortiGate REST API.</li> </ul>

## 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 593](#)
- [Creating FSSO connectors on page 593](#)
- [Creating RADIUS connectors on page 594](#)
- [Creating Cisco pxGrid connectors on page 595](#)
- [Creating ClearPass connectors on page 601](#)
- [Creating VMware NSX-T connectors on page 615](#)
- [Creating VMware vCenter connectors on page 621](#)
- [Creating JSON API connectors on page 625](#)

## 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 > Fabric > 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*:

<b>Server Name/IP</b>	Type the name or IP address for the Active Directory server.
<b>Local User</b>	Type the user name required to log into the Active Directory server.
<b>Password</b>	Type the password required to log into the Active Directory server.
<b>Enable Polling</b>	Toggle <i>On</i> to enable polling of the Active Directory server. Toggle <i>OFF</i> to disable this feature.
<b>LDAP Server</b>	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 > Fabric > 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*:

<b>Name</b>	Type a name for the connector object.
<b>Type</b>	Select the FSSO connector type as either <i>Active Directory / FortiAuthenticator</i> or <i>FortiNAC</i> .
<b>FSSO Agent</b>	Complete the <i>IP/Name</i> , <i>Password</i> , and <i>Port</i> options for each unit that will act as an SSO agent.
<b>User Group Source</b>	Specify whether to get FSSO groups from a <i>Collector Agents</i> , <i>Via FortiGate</i> , or <i>Local</i> .
<b>User Groups</b>	Displays imported FSSO groups from the selected source. This field is only displayed when the <i>User Group Source</i> is <i>Collector Agents</i> or <i>Via FortiGate</i> .

<b>LDAP Server</b>	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 <i>User Group Source</i> is <i>Local</i> .
<b>Proactively Retrieve from LDAP</b>	(Optional) Toggle this field <i>On</i> to proactively retrieve from the LDAP server.
<b>Select LDAP Groups</b>	Select the LDAP groups by choosing <i>Remote Server</i> or <i>Manually Specify</i> . When <i>Manually Specify</i> is selected, you can add each LDAP group in the <i>Group Name</i> field. This field is only displayed when the <i>User Group Source</i> is <i>Local</i> .
<b>SSL</b>	(Optional) Toggle this field <i>On</i> to enable SSL encryption. When enabled, the <i>SSL Trusted Certificate</i> field is displayed where you can specify the SSL certificate.
<b>Per-Device Mapping</b>	(Optional) Toggle <i>On</i> to set per-device mappings between FortiGate units and FSSO agents, and then create the mappings. Toggle <i>OFF</i> to disable this feature.
<b>Advanced Options</b>	Expand to view and configure advanced options for Fortinet single sign-on agents. For details, see the <i>FortiOS CLI Reference</i> .



When you have an FSSO polling server configured on the FortiManager fabric connector, FortiManager will import and install all *fssso-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 *fssso-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 > Fabric > 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*:

<b>Name</b>	Type the name of the RADIUS SSO agent.
<b>Use RADIUS Shared Secret</b>	Toggle <i>On</i> to enable the use of a RADIUS shared secret between collector agent and RADIUS server, and then enter the shared secret. Toggle <i>OFF</i> to disable this feature.
<b>Send RADIUS Responses</b>	Toggle <i>On</i> to send RADIUS response packets after receiving start and stop records. Toggle <i>OFF</i> 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.

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.

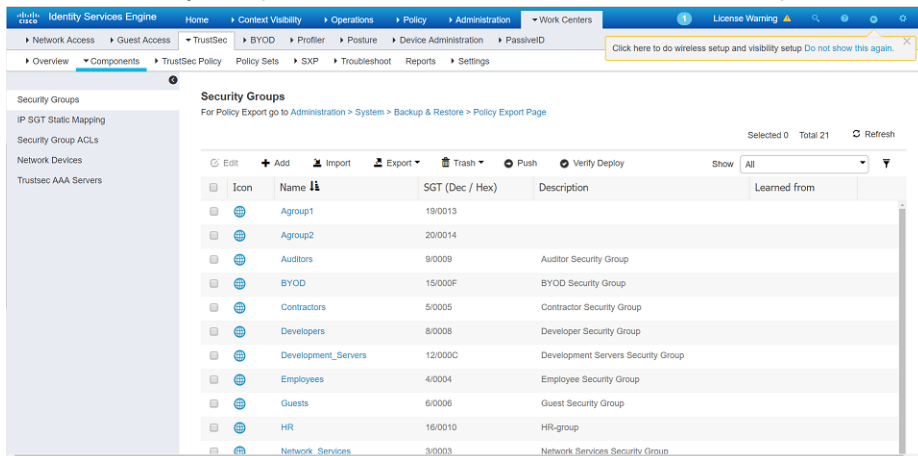


When the pxGrid connector is created, FortiManager will only process events with state "Started" or "Disconnected". All other Session Statuses possible on ISE, such as "Authenticated", are ignored by FortiManager.

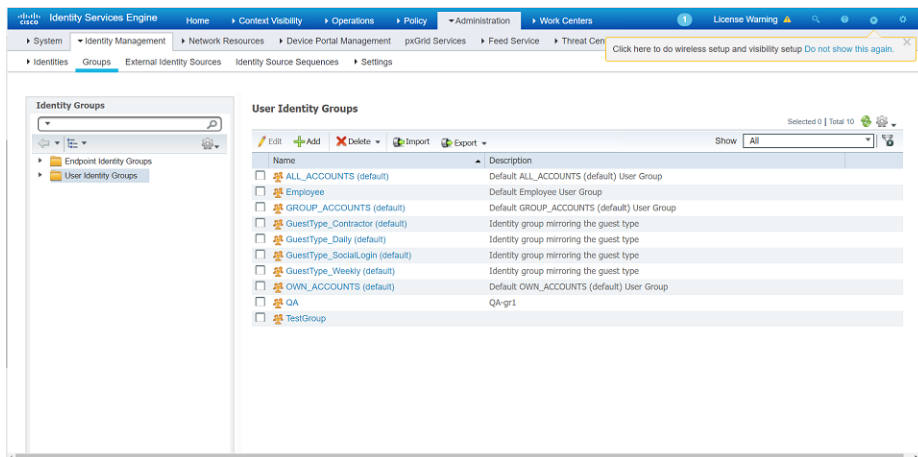
Additionally, a Security Group must be defined. See steps below. Users with null a Security Group are ignored by FortiManager.

### To configure Cisco ISE server:

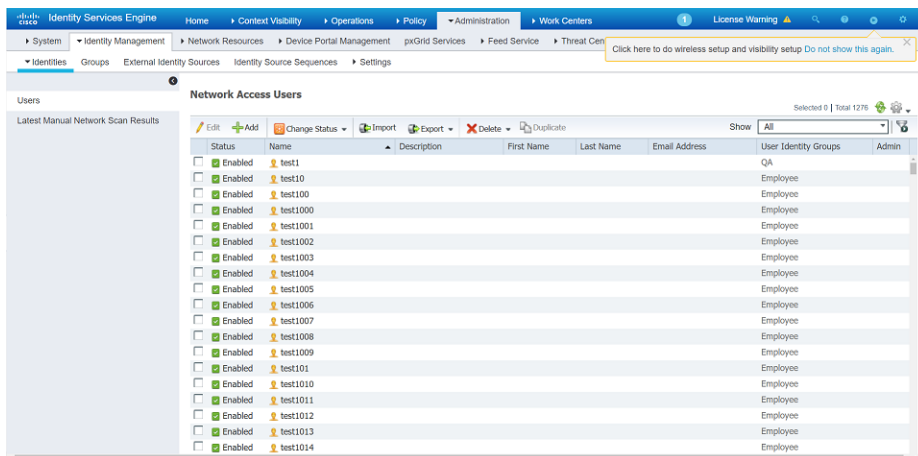
1. Create a Security Group: Go to *ISE > Work Centers > TrustSec > Components > Security Groups*. Click *Add*.



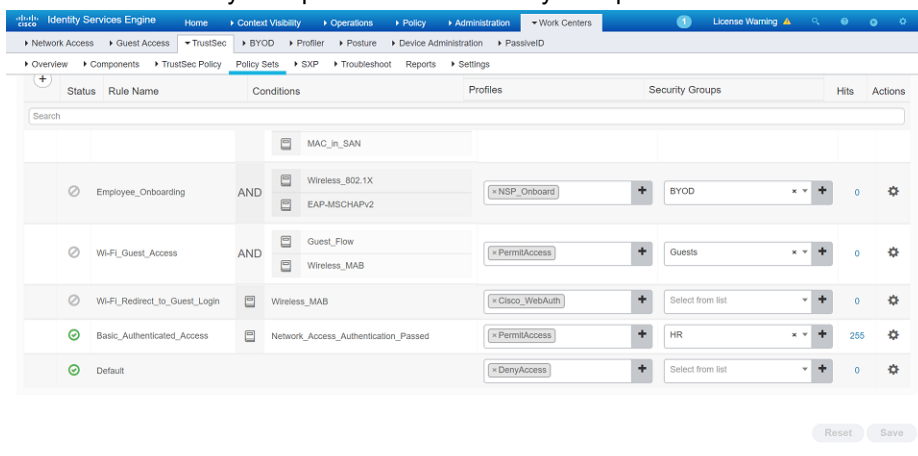
2. Create a User Identity Group: Go to *ISE > Administration > Identity Management > Groups > User Identity Groups*. Click *Add*.



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\_Authenticated\_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*.

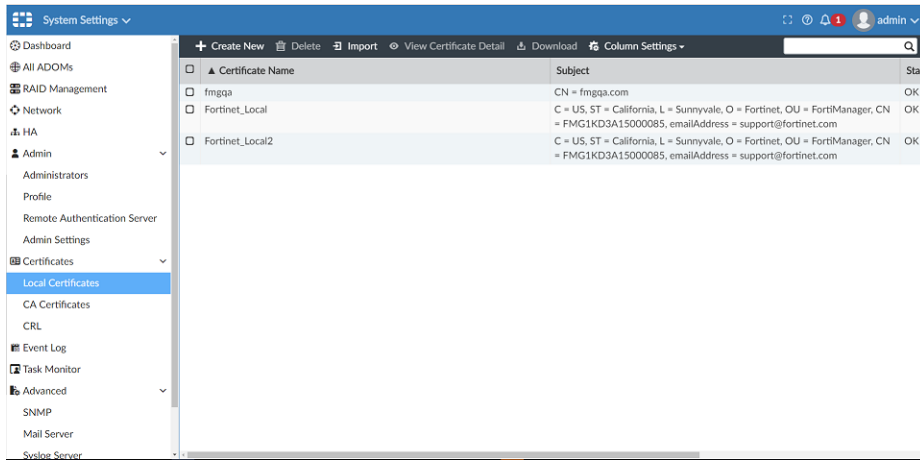
Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP #
Mar 01, 2019 02:52:32.196 PM	Success		0	test2	00:11:22:33:44:55	Unknown	Default >> D...	Default >> B...	PermitAcces...	192.
Mar 01, 2019 02:52:03.737 PM	Success			test2	00:11:22:33:44:55	Unknown	Default >> D...	Default >> B...	PermitAcces...	192.
Mar 01, 2019 02:44:06.881 PM	Failure			test2	00:11:22:33:44:55		Default >> D...	Default		192.

7. See live sessions of current users: Go to *ISE > Operations > RADIUS > Live Sessions*.

Initiated	Updated	Session Status	Action	Endpoint ID	Identity	IP Address	Endpoint Profile
Mar 01, 2019 02:52:03.737 PM	Mar 01, 2019 02:52:32.196 PM	Started	Show CoA Actions	00:11:22:33:44:55	test2	192.168.1.19	Unknown

## To configure FortiManager:

1. Go to *System Settings > Local Certificates > Import*. Import the downloaded certificate.



2. Go to *Fabric View > Fabric > 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:

Create New Fabric Connector

Endpoint/Identity  
User pxGrid

---

**Connector Settings**

Name:

Status: ☐ OFF

Server:

CA Certificate:

Client Certificate:

< Back   Apply & Refresh   OK   Cancel

<b>Name</b>	Type a name for the fabric connector object.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
<b>Server</b>	Type the IP address for Cisco ISE server.
<b>CA Certificate</b>	Select the imported CA Certificate.
<b>Client Certificate</b>	Select the imported Client Certificate.



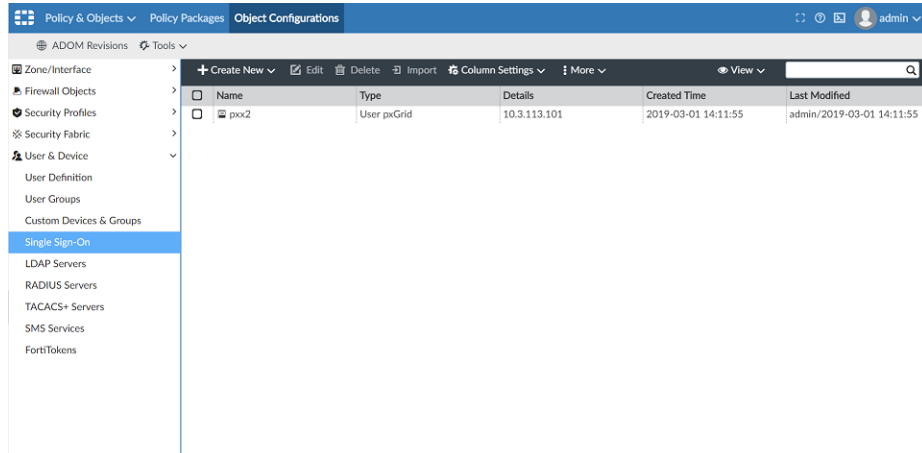
You must approve the pending FortiManager in Cisco ISE by going to *Administrator > pxGrid Services > Clients* and selecting and approving the FortiManager.

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](#).

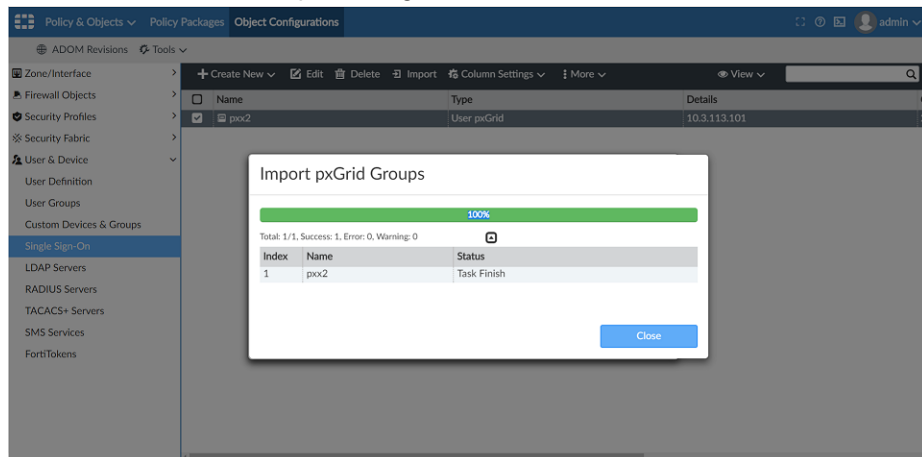


5. Go to *Policy & Objects* > *Object Configuration* > *Single Sign-On*.
6. Select the connector and click *Import*.

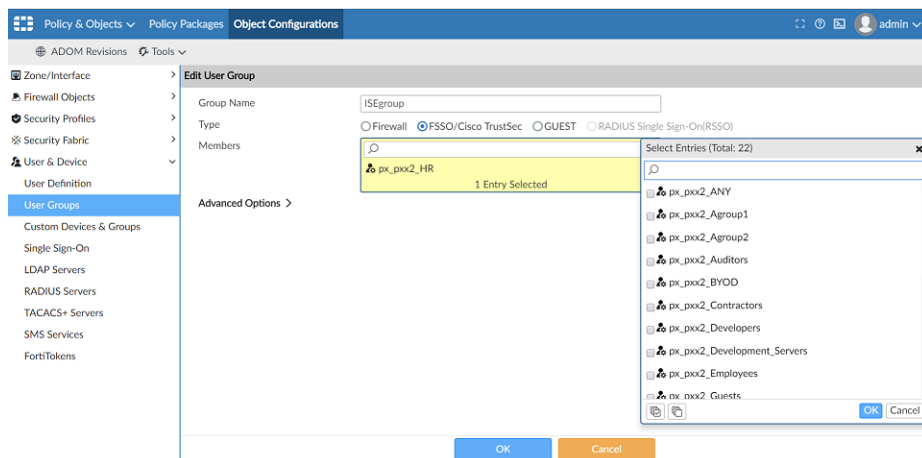


The pxGrid connector is imported.

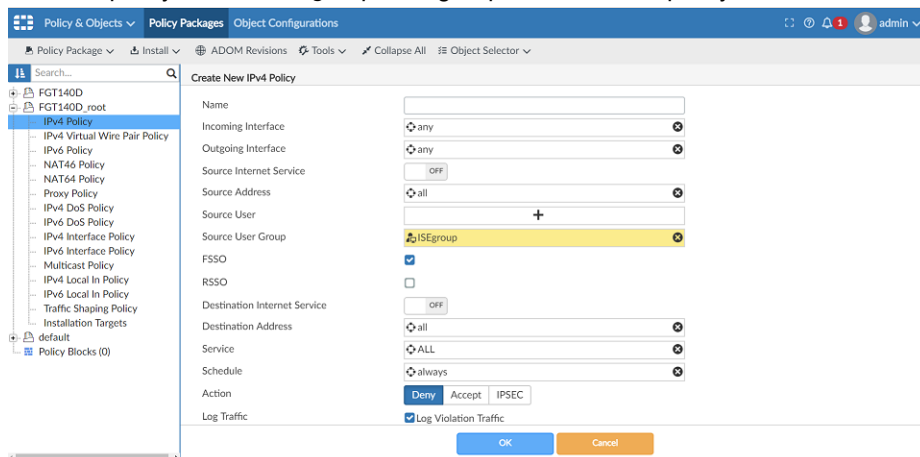
7. Click *Close* to close the import dialog.



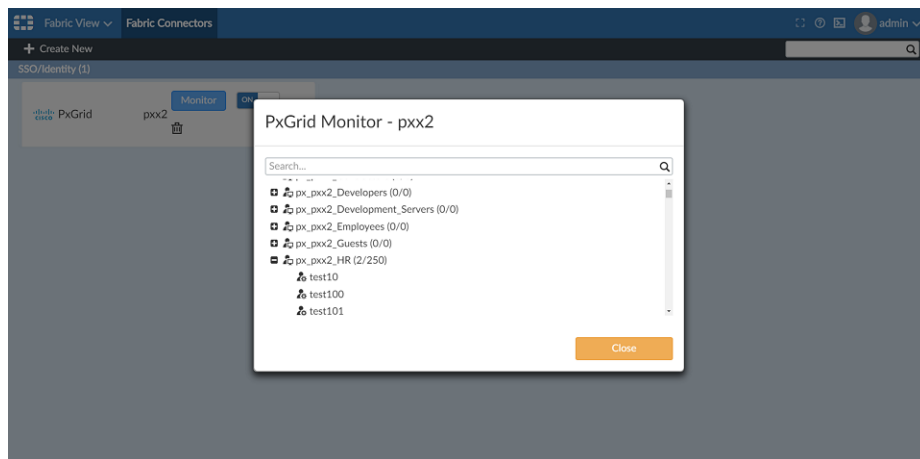
8. Click *User Groups* and create a new group. Set the type as *FSSO/Cisco TrustSec*, and select *pxGrid* user as a member.



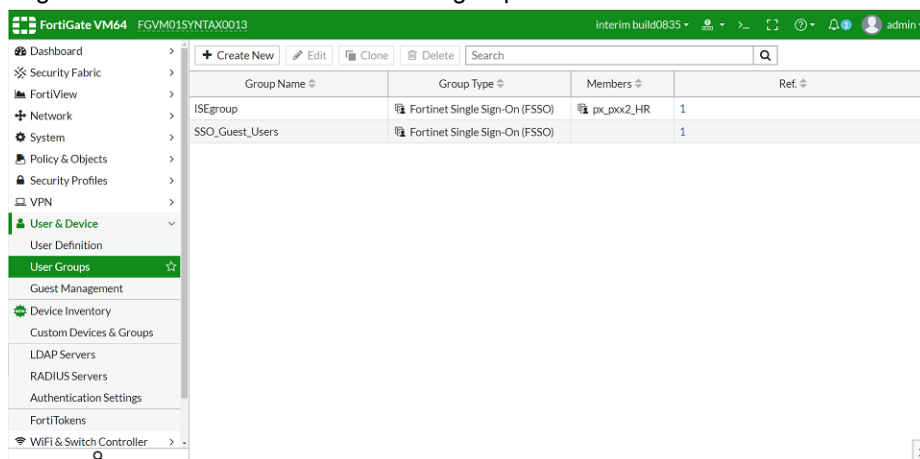
9. Create a policy with the *ISEgroup* user group and install the policy to FortiGate.



10. Go to *Fabric View > Fabric > 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 fssolist` 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-refresh-interval pxGrid refresh interval (60 - 1800 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_fcl_security_grp1 Workstation: MemberOf: fscs1
IP: 192.168.1.20 User: test2 Groups: px_fcl_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.

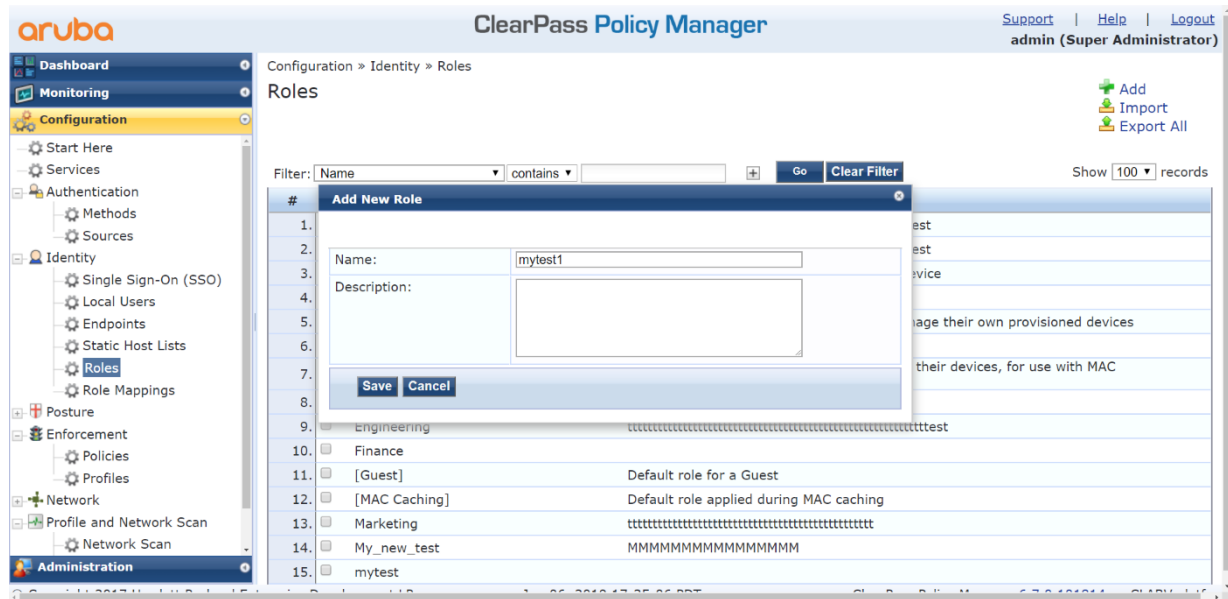
### Requirements:

- 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.

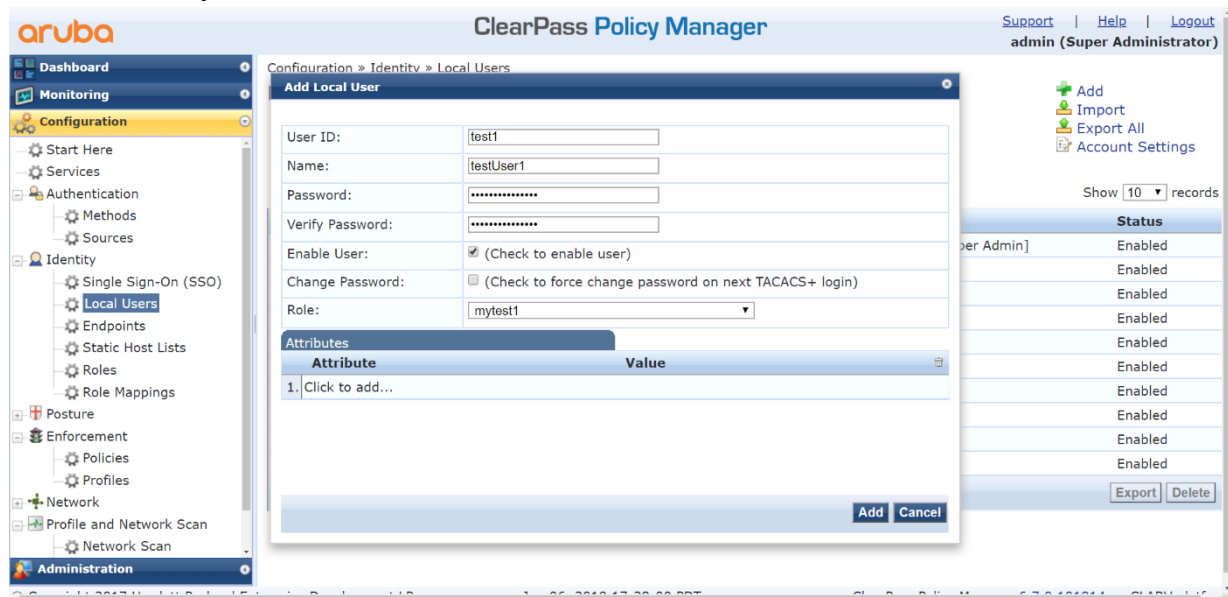
The *Description* field is optional.



d. Click Save.

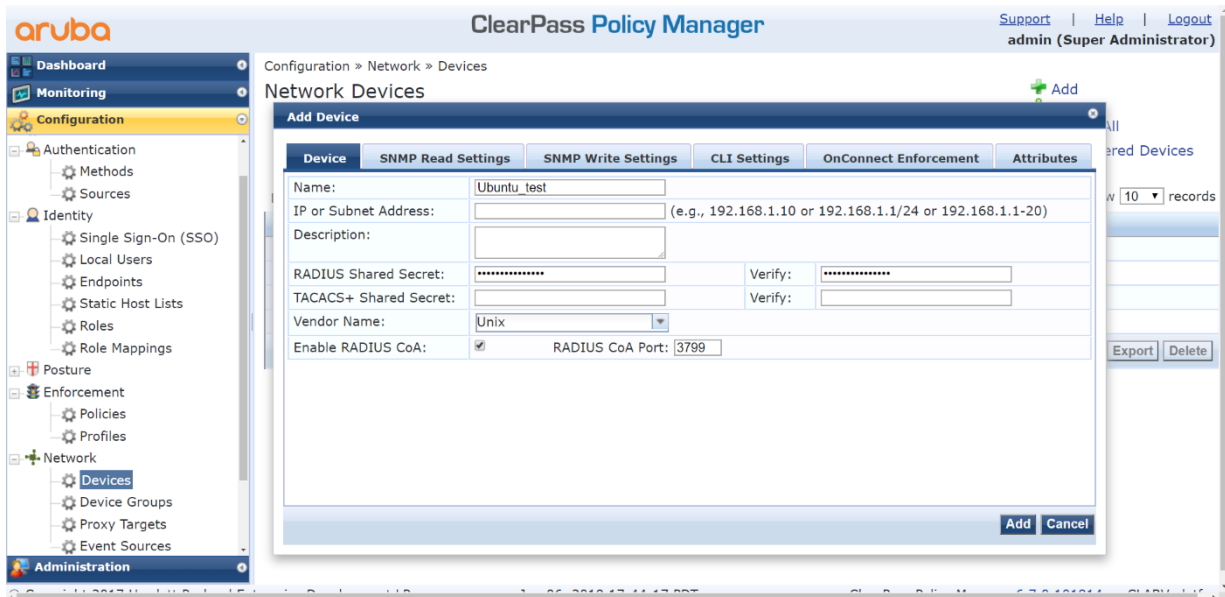
3. Create local users:

- 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*

Aruba ClearPass Policy Manager

Support | Help | Logout  
admin (Super Administrator)

11. Generic HTTP Copy\_of\_Check Point Login - AD POST Inform Check Point that user logged in.

Endpoint Context Server Details

Action Header Content Attributes

Server Type: Generic HTTP

Server Name: 10.3.113.57

Action Name: Frank-FMG-login

Description:

HTTP Method: POST

Authentication Method: Basic

URL: /jsonrpc/connector/user/login

Save Cancel

29. Juniper Networks SRX Juniper Networks SRX Logout POST This is the Endpoint Context Server Action to send user or device logout context to Juniper SRX server

30. MaaS360 Locate Device POST Get current or last known location of the device

iv. On the *Header* tab, configure the following:

- Set *Header Name* to *Content-Type*.
- Set *Header Value* to *application/json*.

Aruba ClearPass Policy Manager

Support | Help | Logout  
admin (Super Administrator)

11. Generic HTTP Copy\_of\_Check Point Login - AD POST Inform Check Point that user logged in.

Endpoint Context Server Details

Action Header Content Attributes

Specify the key-value pairs to be included in the HTTP Header -

#	Header Name	Header Value
1.	Content-Type	= application/json
2.	Click to add...	

Save Cancel

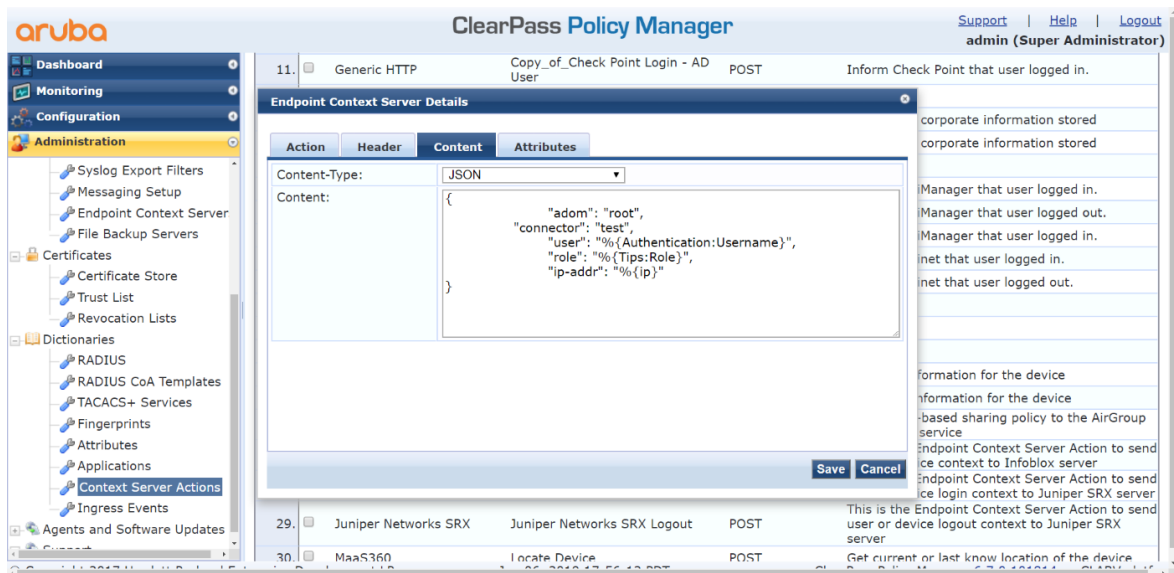
29. Juniper Networks SRX Juniper Networks SRX Logout POST This is the Endpoint Context Server Action to send user or device logout context to Juniper SRX server

30. MaaS360 Locate Device POST Get current or last known location of the device

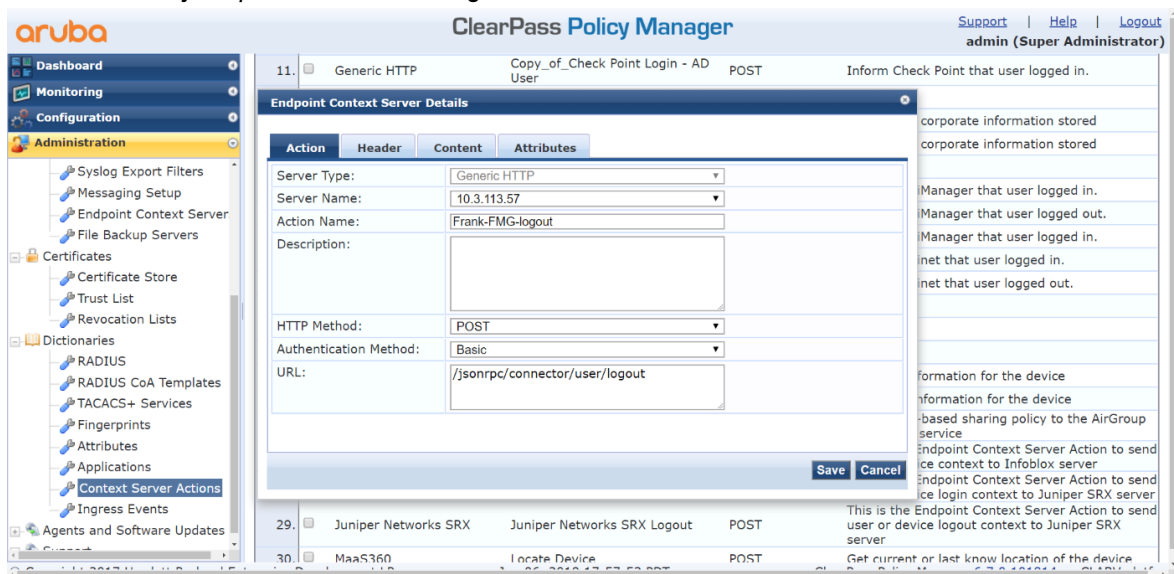
v. On the *Content* tab, configure the following:

- 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:

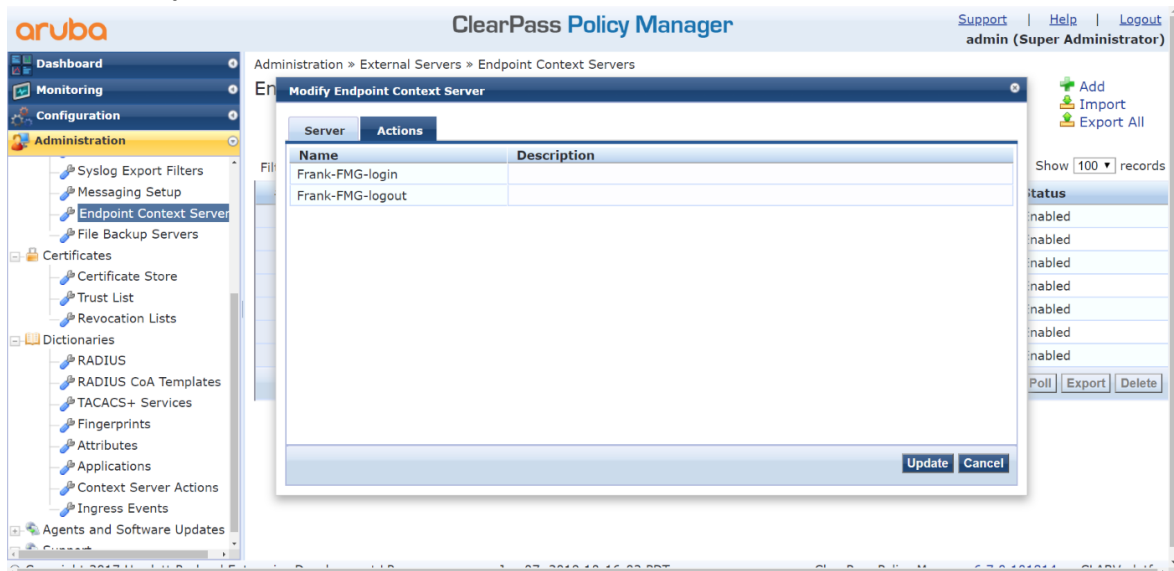
- Set *Content-Type* to *JSON*.
- Set *Content* to:

```
{
  "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:

- Go to *Administration > External Servers > Endpoint Context Servers > 10.3.113.57 > Actions*.
- Locate the two just created actions.



## 6. Create a profile:

- Go to *Configuration > Enforcement > Profiles*.
- Click **Add**.
- 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*.



**aruba** ClearPass Policy Manager [Support](#) | [Help](#) | [Logout](#)  
admin (Super Administrator)

Configuration » Enforcement » Profiles » Add Enforcement Profile

### Enforcement Profiles

Profile | Attributes | Summary

Template: Session Notification Enforcement

Name: [FortiManager - Login and Logout]

Description: FortiManager- Initial SSO integration testing

Type: Post\_Authentication

Action: ☒ Accept ☐ Reject ☐ Drop

Device Group List:

[Add new Device Group](#)

[Remove](#) [View Details](#) [Modify](#)

[Back to Enforcement Profiles](#) [Next >](#) [Save](#) [Cancel](#)

© Copyright 2017 Hewlett Packard Enterprise Development LP Jun 07, 2019 11:21:22 PDT ClearPass Policy Manager 6.7.0.101814 on CLABV platform

- 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

**aruba** ClearPass Policy Manager [Support](#) | [Help](#) | [Logout](#)  
admin (Super Administrator)

Configuration » Enforcement » Profiles » Add Enforcement Profile

### Enforcement Profiles

Profile | Attributes | Summary

Type	Name	Value
1. Session-Notify	Server Type	= Generic HTTP
2. Session-Notify	Login Action	= Frank-FMG-login
3. Session-Notify	Logout Action	= Frank-FMG-logout
4. Session-Notify	Server IP	= 10.3.113.57
5. Click to add...		

[Back to Enforcement Profiles](#) [Next >](#) [Save](#) [Cancel](#)

© Copyright 2017 Hewlett Packard Enterprise Development LP Jun 07, 2019 10:28:12 PDT ClearPass Policy Manager 6.7.0.101814 on CLABV platform

- e. Click **Save**.

7. Create a policy:

- Go to **Configuration > Enforcement > Policies**.
- 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*.

aruba ClearPass Policy Manager

Support | Help | Logout  
admin (Super Administrator)

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement Rules Summary

Name: fortimanager testing

Description:

Enforcement Type: ☒ RADIUS ☐ TACACS+ ☐ WEBAUTH (SNMP/Agent/CLI/CoA) ☐ Application ☐ Event

Default Profile: [Allow Access Profile] [View Details](#) [Modify](#) [Add new Enforcement Profile](#)

[Back to Enforcement Policies](#) [Next >](#) [Save](#) [Cancel](#)

© Copyright 2017 Hewlett Packard Enterprise Development LP Jun 07, 2019 10:31:04 PDT ClearPass Policy Manager 6.7.0.101814 on CLABV platform

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]*.

aruba ClearPass Policy Manager

Support | Help | Logout  
admin (Super Administrator)

Configuration » Enforcement » Policies » Add

Rules Editor

Conditions

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Date	Date-Time	EXISTS	
2. Click to add...			

Enforcement Profiles

Profile Names: [Post Authentication][FortiManager - Login and Logout] [Move Up](#) [Move Down](#) [Remove](#)

[Add new Enforcement Profile](#)

[Back to Enforcement Policies](#) [Next >](#) [Save](#) [Cancel](#)

© Copyright 2017 Hewlett Packard Enterprise Development LP Jun 07, 2019 10:32:58 PDT ClearPass Policy Manager 6.7.0.101814 on CLABV platform

e. Click *Save*.

8. Create services:

- Go to *Configuration > Services*.
- 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*.

aruba ClearPass Policy Manager

Support | Help | Logout  
admin (Super Administrator)

Configuration > Services > Edit - API Test Access OAuth2 API User Access

Services - API Test Access OAuth2 API User Access

Summary Service Authentication Roles Enforcement

Name: API Test Access OAuth2 API User Access

Description: Authentication service for API access using OAuth2

Type: Aruba Application Authentication

Status: Enabled

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization

Service Rule

Matches ☒ ANY or ☐ ALL of the following conditions:

Type	Name	Operator
1. Application	Name	EQUALS
2. Click to add...		

Back to Services

Disable Copy Save Cancel

© Copyright 2017 Hewlett Packard Enterprise Development LP Aug 23, 2019 10:56:11 PDT ClearPass Policy Manager 6.7.0.101814 on CLABV platform

- d. On the *Authentication* tab, set *Authentication Sources* to:

[Local User Repository] [Local SQL DB]  
[Admin User Repository] [Local SQL DB]

aruba ClearPass Policy Manager

Support | Help | Logout  
admin (Super Administrator)

Configuration > Services > Edit - API Test Access OAuth2 API User Access

Services - API Test Access OAuth2 API User Access

Summary Service Authentication Roles Enforcement

Name: API Test Access OAuth2 API User Access

Description: Authentication service for API access using OAuth2

Type: Aruba Application Authentication

Status: Enabled

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization

Service Rule

Matches ☒ ANY or ☐ ALL of the following conditions:

Type	Name	Operator
1. Application	Name	EQUALS
2. Click to add...		

Back to Services

Disable Copy Save Cancel

© Copyright 2017 Hewlett Packard Enterprise Development LP Aug 23, 2019 10:56:11 PDT ClearPass Policy Manager 6.7.0.101814 on CLABV platform

- 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]

- Click **Save**.
- Click **Add** again to add another service.
- 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

- On the **Authentication** tab, configure the following:
  - Set *Authentication Methods* to *[PAP]*.
  - Set *Authentication Sources* to *[Local User Repository] [Local SQL DB]*.
- 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]

The screenshot shows the ClearPass Policy Manager web interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Services, Authentication, Identity, Posture, Enforcement, Policies, Profiles, Network, Profile and Network Scan, and Policy Simulation. The main content area is titled 'ClearPass Policy Manager' and shows the configuration for 'AuthN user for FortiManager Testing'. The 'Configuration' tab is selected, and the 'Service' sub-tab is active. The 'Service' configuration includes fields for Name, Description, Type, Status, Monitor Mode, and More Options. Below these is a 'Service Rule' section with a table of conditions. The 'Authentication' section includes fields for Authentication Methods, Authentication Sources, Strip Username Rules, and Service Certificate. The 'Roles' section includes a Role Mapping Policy. The 'Enforcement' section includes fields for Use Cached Results and Enforcement Policy. At the bottom, there are buttons for 'Back to Services', 'Disable', 'Copy', 'Save', and 'Cancel'.

Configuration » Services » Edit - AuthN user for FortiManager Testing

Services - AuthN user for FortiManager Testing

Summary Service Authentication Roles Enforcement

**Service:**

Name: AuthN user for FortiManager Testing

Description: Authorization service for AirGroup device access

Type: RADIUS Enforcement ( Generic )

Status: Enabled

Monitor Mode: Disabled

More Options: -

**Service Rule**

Match ANY of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-IP-Address	EQUALS	10.0.0.1

**Authentication:**

Authentication Methods: [PAP]

Authentication Sources: [Local User Repository]

Strip Username Rules: -

Service Certificate: -

**Roles:**

Role Mapping Policy: -

**Enforcement:**

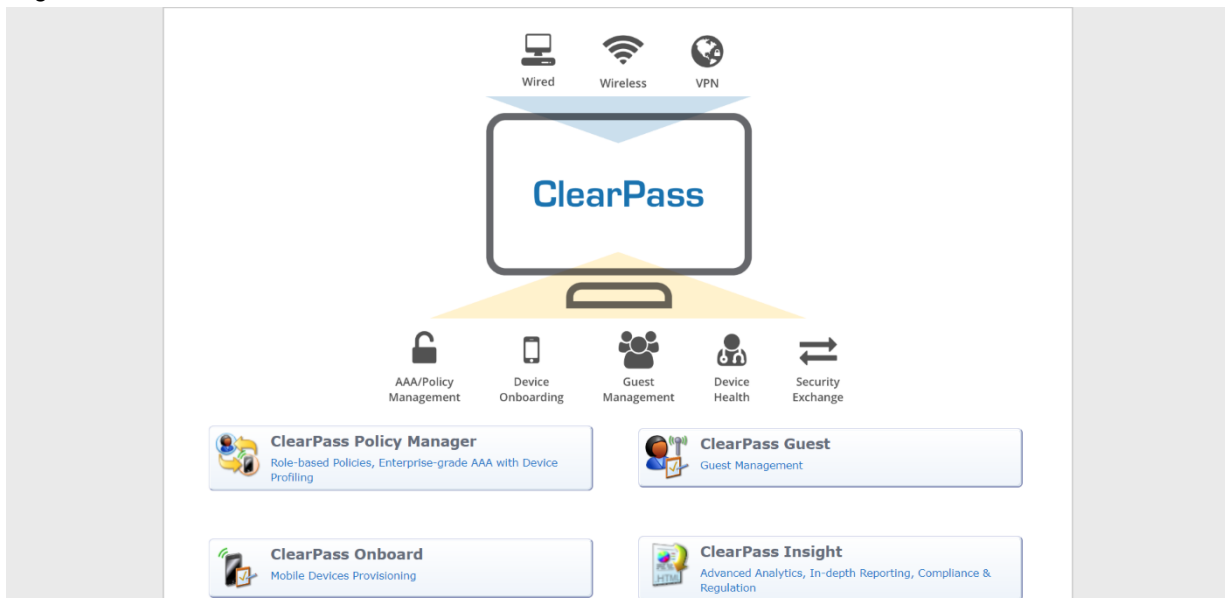
Use Cached Results: Disabled

Enforcement Policy: fortimanager testing

© Copyright 2017 Hewlett Packard Enterprise Development LP Aug 23, 2019 10:59:28 PDT ClearPass Policy Manager 6.7.0.101814 on CLABV platform

- 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 *Description* to *FMG login from it*.
- Select *Enable API client*.
- Set *Operator Profile* to *Super Administrator*.
- Set *Grant 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*.

The screenshot shows the 'Create API Client' form in the ClearPass Guest interface. The form is titled 'Create API Client' and includes the following fields and options:

- \* Client ID:** test
- Description:** FMG login from it
- Enabled:** ☒ Enable API client
- \* Operator Profile:** Super Administrator
- \* Grant Type:** Username and password credentials (grant\_type=password)
- Public Client:** ☒ This client is a public (trusted) client
- Refresh Token:** ☒ Allow the use of refresh tokens for this client
- Access Token Lifetime:** 8 hours
- Refresh Token Lifetime:** 14 days

The form also includes a sidebar with navigation options: Guest, Onboard, Configuration, Administration, Start Here, AirGroup Services, API Services, API Explorer, SOAP Web Services, Data Retention, Extensions, Import Configuration, Operator Logins, Plugin Manager, and Support.

e. Click *Save*.

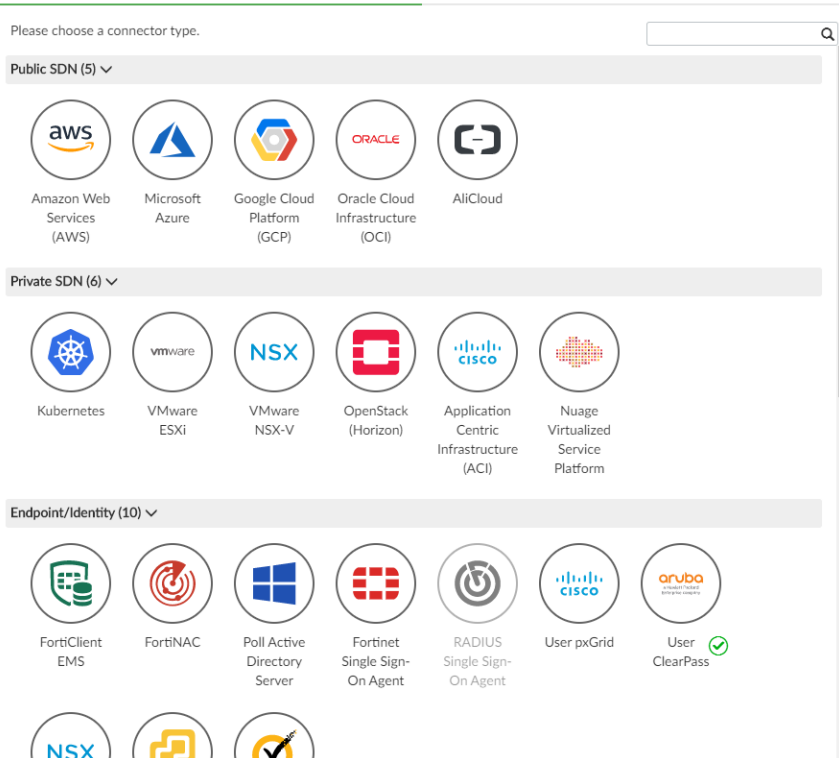
## To configure FortiManager:

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 > Fabric > External Connectors*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.

### Create New Fabric Connector



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).

## Create New Fabric Connector

Endpoint/Identity  
User ClearPass

## Connector Settings

Name	<input type="text"/>
Status	<input type="checkbox"/> OFF
Server	<input type="text"/>
Client	<input type="text"/>
User	<input type="text"/>
Password	<input type="password"/>

&lt; Back

Apply &amp; Refresh

OK

Cancel

6. Click **OK**.

7. Get the role and user from ClearPass:

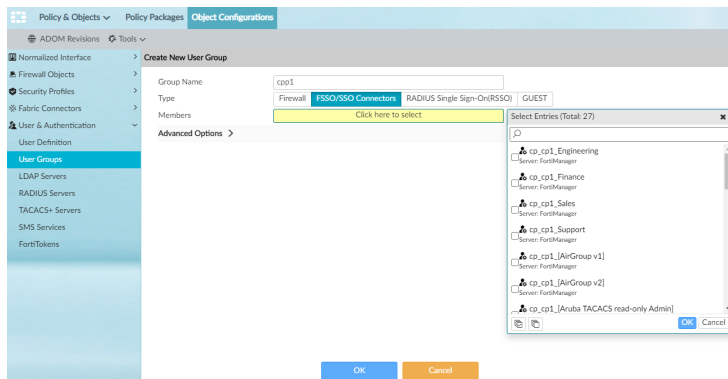
- Go to *Policy & Objects > Object Configurations > External Connectors > Endpoint/Identity*.
- Edit the ClearPass connector and click *Apply & Refresh*.

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:

- On the FortiManager, go to *Policy & Objects > Object Configurations > User & Authentication > User Groups*.
- Click *Create New*.
- 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: cppl
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 615](#)
2. [Creating a fabric connector for VMware NSX-T on page 616](#)
3. [Configure registered services on page 617](#)
4. [Configure the NSX-T Manager on page 618](#)
5. [Use the groups in a FortiManager policy on page 621](#)

## 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 > Admin > 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

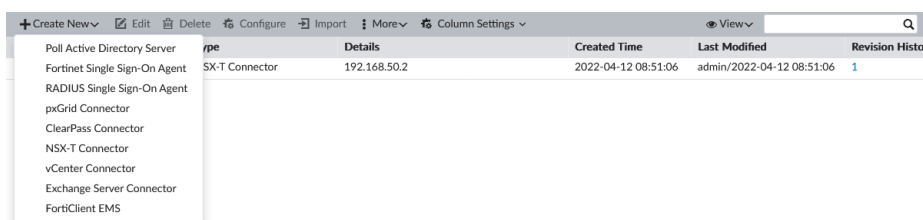
In FortiManager, create a fabric connector for VMware NSX-T.

### To configure an NSX-T connector on FortiManager:

1. Log into FortiManager.
2. Go to *Policy & Objects > Objects Configuration > External Connectors > 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**.

**Create New NSX-T Connector**

**Connector Settings**

Name:

Status: ☒

**NSX-T Manager Configurations**

Server:

User Name:

Password:

**FortiManager Configurations**

IP Address:

User Name:

Password:

**Revision**

Change Note:

Revision History

Revert	View Diff	Column Settings	Revisor	Changed by	Date/Time	Action	Change Note
No record found.							


Buttons: **Apply & Refresh** **OK** **Cancel**

**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.

<b>User Name</b>	Enter your NSX-T username.
<b>Password</b>	Enter your NSX-T password.
<b>FortiManager Configurations</b>	
<b>IP Address</b>	Enter the IP or FQDN for FortiManager.
<b>User Name</b>	Your FortiManager administrator password.
 <p>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.</p>	
<b>Password</b>	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.

Create New Service

Name	NSXTConnector		
Integration	EAST-WEST NORTH-SOUTH		
FortiGate Password	••••••••		
License Type	License File Flex-VM		
License URL Prefix	http://122312312/lics/		
Image Location	Type	Location	Action
	VM02	http://123123123/nsxt/FortiGate-VM64-1CPU.nsxt.ovf	✕ +

OK Cancel

<b>Name</b>	Enter the service name to register to NSX-T's partner service catalog.
<b>Integration</b>	Select the integration type as <i>East-West</i> or <i>North-South</i> .
<b>FortiGate Password</b>	Enter your FortiGate administrator password.
<b>License Type</b>	Select the license type as either <i>License File</i> or <i>Flex-VM</i> .
<b>License File</b>	<p>When using a <i>License File</i>:</p> <ol style="list-style-type: none"> <li>1. Enter the license URL prefix in <i>License URL Prefix</i>, for example: http://x.x.x.x/lics/.</li> <li>2. Click the Add icon to add a new image location, and configure the following:</li> </ol>

- **Type:** Select the VM type, for example *VM01*.
- **Location:** Enter the image location, for example: `http://x.x.x.x/FortiGate-VM64xCPU.nsxt.ovf`

**Flex-VM**

When using *Flex-VM*, select a previously configured FortiFlex Connector from which to obtain the license. See [Creating Flex-VM connectors on page 624](#).

3. Click *OK*, and save the NSX-T connector.
4. 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.

Select Members | Web-Servers



Add Compute Members either by creating or by directly adding them. You can also add Identity members separately. Identity members intersect with the Compute members to define effective membership of the group.

Membership Criteria (0)   Members (0)   **IP Addresses (1)**   MAC Addresses (0)   AD Groups (0)

**ACTIONS** ▾

Maximum: 4000

100.100.100.100/32 X

Enter IP Address

Format: 2001:0db8:85a3:0000:0000:8a2e:0370:7334 or 10.12.2.64/26 or 2001:1-5000:25

**CANCEL**   **APPLY**

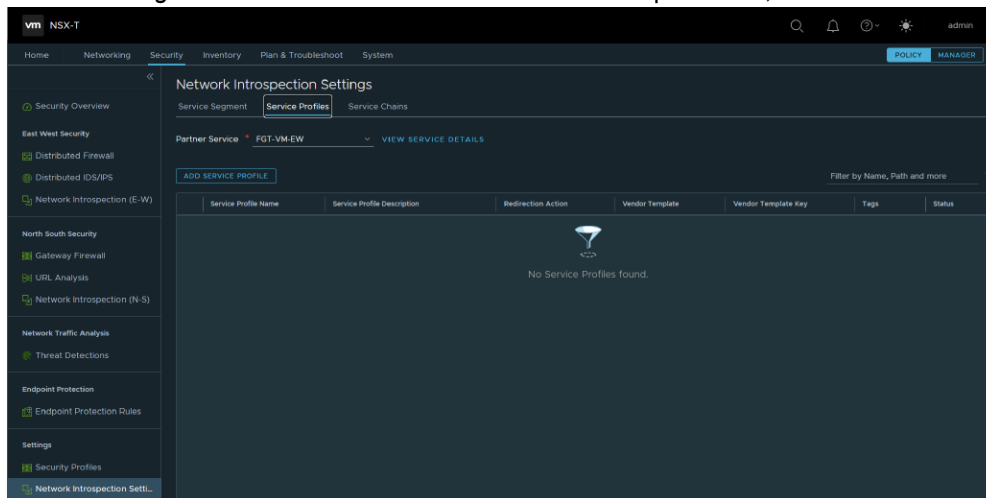
### 4. Save your changes, and repeat these steps until you have created all of the groups that you require.



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 > Object Configurations > External Connectors*.
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>`

### 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:

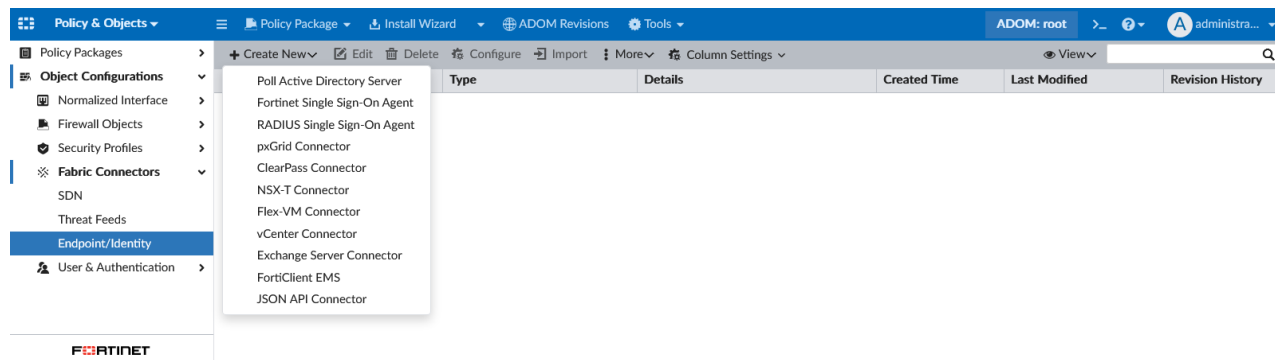
1. Create an SDN connector for VMware vCenter. See [Creating SDN connectors for VMware vCenter on page 622](#).
2. Create a dynamic address object that references the SDN connector for VMware vCenter. See [Creating dynamic addresses on page 623](#).
3. Create a firewall policy. See [Creating firewall policies on page 623](#).
4. Install the changes to FortiGate. See [Installing changes to FortiGate on page 624](#).  
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

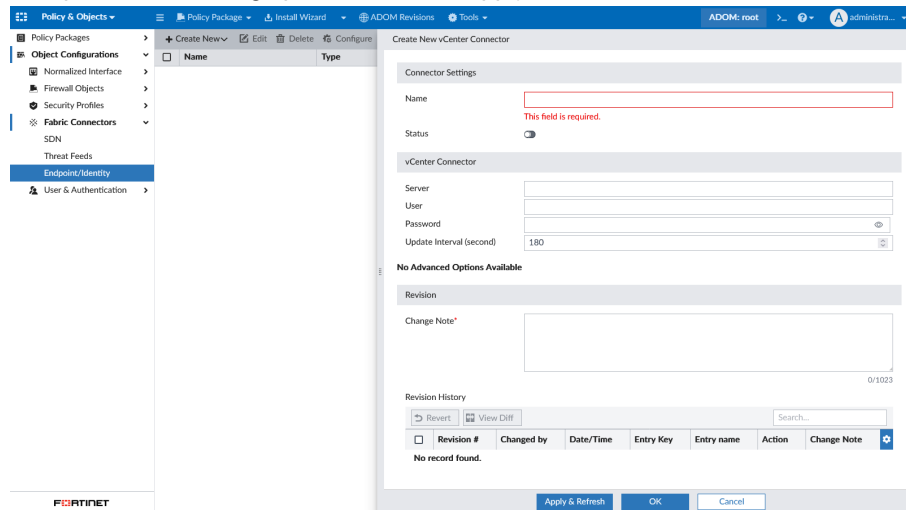
To create SDN connectors for VMware vCenter:

1. Go to *Policy & Objects > Object Configurations > External Connectors > 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**.

Create New Rule

Name: FGv6

Rule:  ✓ ✕ +

ip	name	vmuuid	vmid	nei
10.101.14.1	ms_tc7	503187c0-a86a-1b7a-ef05-f73092abaa56	34934	du
10.151.119.1	ms_tc7	503187c0-a86a-1b7a-ef05-f73092abaa56	34934	du
172.18.41.145	ms_tc7	503187c0-a86a-1b7a-ef05-f73092abaa56	34934	Vf
fe80::250:56ff:feb1:56ce::	ms_tc7	503187c0-a86a-1b7a-ef05-f73092abaa56	34934	Vf
fe80::344f:8997:36f2:3016::	ms_tc7	503187c0-a86a-1b7a-ef05-f73092abaa56	34934	du
fe80::b487:3a63:6245:e41d::	ms_tc7	503187c0-a86a-1b7a-ef05-f73092abaa56	34934	du

[Total: 6]

OK Cancel

FortiManager retrieves IP addresses from the VMware vCenter server.

## Creating dynamic addresses

### To create dynamic addresses:

1. Go to *Policy & Objects > Object Configurations > 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.

Type	Details	Interface	Visibility	Ref.
Subnet	0.0.0.0/0		Visible	0
Subnet	0.0.0.0/0		Hidden	0
IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel Interface (sslroot)	Visible	0
Dynamic (FSSO)	vc_fmng-stress_FGv6		Visible	1
Subnet	0.0.0.0/0		Visible	1

## Creating Flex-VM connectors

You can configure a Flex-VM connector to allow FortiManager to assign licenses to managed FortiGate devices through the device manager. See [Installing VM licenses on page 104](#).

**To create a Flex-VM connector:**

1. Go to *Policy & Objects > Object Configurations > External Connectors > Endpoint/Identity*.
2. Click *Create New*, and select *Flex-VM Connector*.  
The Create New Flex-VM Connector wizard opens.
3. Enter the following information:

<b>Name</b>	Enter a name for the Flex-VM connector.
<b>Status</b>	Toggle the slider on or off to enable or disable the connector.
<b>API User</b>	Enter the username for your Flex-VM API user.
<b>API Password</b>	Enter the password for your Flex-VM API user.
<b>Program SN</b>	Enter your Flex-VM 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 > Fabric > External Connectors* and click *Create New > JSON API connector*.  
You can also configure this connector at *Policy & Objects > Object Configurations > External Connectors > Endpoint/Identity*.  
Enter the following information:

<b>Name</b>	Enter a name for the JSON API connector.
<b>Status</b>	Toggle the slider on or off to enable or disable the connector.
<b>Tags</b>	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.

The screenshot shows the 'Edit JSON API Connector' dialog in the FortiManager interface. The 'Connector Settings' tab is active, displaying the following fields:

- Name:** test
- Status:** On
- Tags:** tag1, tag2, tag3

The 'JSON API Connectors' tab shows a list of connectors:

Name	Type	Details	Create
1	FortClient EMS	undefined:443	adm
2	FortClient EMS	undefined:443	adm
3	FortClient EMS	undefined:443	adm
4	FortClient EMS	undefined:443	adm
5	FortClient EMS	undefined:443	adm
test	JSON API Connector		adm

The 'Revision' tab shows a 'Change Note' field. The 'Revision History' tab shows a table of revisions:

Revision #	Changed by	Date/Time	Action	Change Note
4	admin	2022-07-06 14:54:35	Modify	test
3	admin	2022-07-06 14:54:35	Modify	test
2	admin	2022-07-06 14:54:35	Modify	create
1	admin	2022-07-06 14:54:35	Create	create

At the bottom of the dialog, there are 'OK' and 'Cancel' buttons.

## 3. The tags that you created in the connector can now be used in a policy as the FSSO group (adgrp).

The screenshot shows the 'Edit Firewall Policy' dialog in the FortiManager interface. The 'Policy Settings' tab is active, displaying the following fields:

- Name:** 1
- Incoming Interface:** any
- Outgoing Interface:** any
- Source Internet Service:** all
- IPv4 Source Address:** +
- IPv6 Source Address:** +
- Source User:** +
- Source User Group:** +
- FSSO Groups:** test\_tag1
- Destination Internet Service:** all
- IPv4 Destination Address:** +
- IPv6 Destination Address:** +
- Service:** ALL
- Schedule:** always
- Action:** Deny

The 'Advanced Options' tab shows the following fields:

- Block Notification:** On
- Log Violation Traffic:** On
- Generate Logs when Session Starts:** On

The 'Revision' tab shows a 'Change Note' field. The 'Revision History' tab shows a table of revisions:

Revision #	Changed by	Date/Time	Action	Change Note
4	admin	2022-07-06 14:54:35	Modify	test
3	admin	2022-07-06 14:54:35	Modify	test
2	admin	2022-07-06 14:54:35	Modify	create
1	admin	2022-07-06 14:54:35	Create	create

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.

# 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.



FortiManager VM with a trial license does not support FortiGuard subscriptions and cannot act as a local FDS.

---

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

To view and configure these services, go to *FortiGuard > Settings*.

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.



To see a list of which updates are available per platform when FortiManager is acting as a local FDS, see the [FortiManager Release Notes](#).

---

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.
- 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 48](#).
- Enable and configure the FortiManager system's built-in FDS. For more information, see [Configuring network interfaces on page 739](#).

- 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 648](#).

- 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 51](#).

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.

This section contains the following topics:

- [Licensing status](#)
- [Package management](#)
- [Query server management](#)
- [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](#)



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>.

---

## Licensing status

On the *FortiGuard > Licensing Status* pane, you can view the status of all licenses for each managed device. This section includes the following topics:

- [View licensing status on page 628](#)

### 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 > Licensing Status*. This page displays the following columns of information:  
The following toolbar is displayed:

<b>Refresh</b>	Select the refresh icon to refresh the information displayed on this page.
<b>Push Update</b>	Push a license update to the selected device in the group.
<b>Show License Expired Devices / Show All Devices</b>	Toggle to hide and display only devices with an expired license.
<b>Check License</b>	<p>Click to check expiry dates for licenses. The <i>Check License</i> 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.</p> <p>The <i>FortiGuard Subscription</i> 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).</p>
<b>Export</b>	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.
<b>Column Settings</b>	Click to choose what columns to display on the <i>Licensing Status</i> page.
<b>Search</b>	Use the search field to find a specific device in the table.

The following columns of information are displayed:

<b>Device Name</b>	The device name or host name. You can change the order that devices are listed by clicking the column title.
<b>Serial Number</b>	The device serial number
<b>Platform</b>	The device type or platform.
<b>ADOM</b>	The name of the ADOM that contains the device. You can change the order that ADOMs are listed by clicking the column title.
<b>Firmware Version</b>	Displays the version of firmware installed on the device.
<b>Support Contract</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• N/A: No support contract</li> <li>• 24/7: Support contract level that provides support 24 hours per day and 7 days per week</li> <li>• 8/5: Support contract level</li> </ul>
<b>FortiGuard Subscription</b>	<p>Displays the license status of the FortiGuard subscription.</p> <p>The status reflects the worst license status of the individual components of the FortiGuard license.</p> <p>Hover over the license status to display details about the following components: IPS &amp; Application Control, Antivirus, Web Filtering, and Email Filtering. License status can include:</p> <ul style="list-style-type: none"> <li>• All valid</li> <li>• Expires in &lt;time&gt;</li> <li>• Expired</li> </ul>

	<ul style="list-style-type: none"> <li>Unknown</li> </ul>
<b>Service Status</b>	<p>License status of antivirus and IPS service. FortiManager calculates the status based on the FortiGate's last update request.</p> <p>Hover the mouse over the cell to display details about the service status.</p> <p>Licenses status can include:</p> <ul style="list-style-type: none"> <li>Update Available</li> <li>Up to Date</li> <li>Expired</li> <li>Unknown</li> </ul>
<b>Virtual Domains</b>	<p>Number of virtual domains. Click the cart icon to go to the Fortinet support site (<a href="https://support.fortinet.com">https://support.fortinet.com</a>)</p>

## Package management

When FortiManager is acting as a local FDS, antivirus and IPS signature packages are managed in *FortiGuard > Package Management*. 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 > Package Management > Receive Status*. This page lists received packages, grouped by platform.

The following information is displayed:

<b>Refresh</b>	Select to refresh the table.
<b>Show Used Object Only</b>	Clear to show all package information. Select to show only relevant package information.
<b>Export</b>	Select a package, and click <i>Export</i> . The package is compressed and downloaded to your management computer. You can import the package into another FortiManager.
<b>Import</b>	Click <i>Import</i> to select a package exported from another FortiManager and import it into this FortiManager.
<b>Search</b>	Use the search field to find a specific object in the table.
<b>Package Name</b>	The name of the package downloaded from FortiGuard.
<b>Product</b>	<p>The name of the product supported by the package, such as FortiGate.</p> <p>Click the <i>Filter</i> icon to display the filter options. When a filter is active, the <i>Filter</i> icon is green. When the <i>Filter</i> icon is gray, no filter is applied.</p>
<b>Version</b>	The package version.



	Click the <i>Filter</i> icon to display the filter options. When a filter is active, the <i>Filter</i> icon is green. When the <i>Filter</i> icon is gray, no filter is applied.
<b>Service Entitlement</b>	The name of the service entitlement that includes the package support.
<b>Latest Version (Release Date/Time)</b>	The package version.
<b>Size</b>	The size of the package.
<b>To Be Deployed Version</b>	The package version that is to be deployed. By default, the latest version is deployed. Select <i>Change</i> to change the version.  When you export a package, only one version is exported. The <i>To Be Deployed Version</i> identifies what version is exported. See also <a href="#">Exporting packages example on page 634</a> .
<b>Update History</b>	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 > Package Management > 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:

<b>Push Pending</b>	Select the device or devices in the list, then click <i>Push Pending</i> in the toolbar to push pending updates to the device or devices.
<b>Push All Pending</b>	Select <i>Push All Pending</i> in the toolbar to push pending updates to all of the devices in the list.
<b>Refresh</b>	Select to refresh the list.
<b>Column Settings</b>	Select which fields are included in the service status table.
<b>Display Options</b>	Displays the available display options including <i>Show Pending Device Only</i> and <i>Group by ADOMs</i> .  This option is only available while viewing service status <i>By Device</i> .
<b>By ADOM</b>	Displays the service status information for all devices in the selected ADOM(s). By default, this is set to <i>All ADOMs</i> .

	This option is only available while viewing service status <i>By Device</i> .
<b>By Package</b>	Displays the service status information by installed package name.
<b>By Device</b>	Displays the service status information by device name.
<b>Search</b>	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.

<b>Device</b>	The device serial number or host name is displayed.
<b>Status</b>	<p>The service update status. A device's status can be one of the following:</p> <ul style="list-style-type: none"> <li>• <i>Up to Date</i>: The latest package has been received by the FortiGate unit.</li> <li>• <i>Never Updated</i>: The FortiGate unit has never requested or received the package.</li> <li>• <i>Pending</i>: 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.</li> <li>• <i>Problem</i>: The FortiGate unit missed the scheduled query, or did not correctly receive the latest package.</li> <li>• <i>Unknown</i>: The FortiGate unit's status is not currently known.</li> </ul>
<b>Last Update Time</b>	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:

<b>Installed Packages Name</b>	The name of the installed package.
<b>Applicable Firmware Version</b>	The firmware version of the device for which the installed package is created.
<b>Package Version</b>	The version of the installed package.
<b>Installed Devices</b>	The package installation progress for the devices. Click the <i>&lt;number&gt; of &lt;number&gt;</i> link to view the installed device list.

#### To view the installed device list:

1. Go to *FortiGuard > Package Management > 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.

<b>Device Name</b>	The name of the device.
<b>Current Version</b>	The version of the package.
<b>Status</b>	The device update status.
<b>Last Update Time</b>	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.

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 download of IoT packages:
 

```
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 > Package Management > Receive Status**.
2. In the **Search** box, type the name of the product, and press **Enter**.

The search results are displayed. In the following example, only FortiSandbox packages are displayed.

Package Name	Product	Version	Service Entitlement	Type	Latest Version (Release Date/Time)	Size	To Be Deployed Version	Update History
03000003SBEN00700	FortiSandbox			03000003SBEN00700	3000.00010 (2019-03-29 14:25:00)	3.63 MB	Latest	<a href="#">Change</a>
03000003SBEN00900	FortiSandbox			03000003SBEN00900	3000.00092 (2019-02-14 16:04:00)	29.18 MB	Latest	<a href="#">Change</a>
03000003SBEN01000	FortiSandbox			03000003SBEN01000	3000.00108 (2019-03-08 19:52:00)	23.89 MB	Latest	<a href="#">Change</a>
03000004SBEN00500	FortiSandbox			03000004SBEN00500	6.00019 (2018-10-25 21:32:00)	1.81 MB	Latest	<a href="#">Change</a>
030010005SBEN00200	FortiSandbox			030010005SBEN00200	16.00934 (2020-09-30 18:30:00)	99.16 KB	Latest	<a href="#">Change</a>
030010005SBEN00100	FortiSandbox			030010005SBEN00100	80.00858 (2020-10-05 04:23:00)	14.97 MB	Latest	<a href="#">Change</a>
030010005SBEN00200	FortiSandbox			030010005SBEN00200	80.00728 (2020-09-29 18:24:00)	49.08 MB	Latest	<a href="#">Change</a>
030010005SBEN00300	FortiSandbox			030010005SBEN00300	80.00752 (2020-09-30 18:48:00)	233.42 MB	Latest	<a href="#">Change</a>
030010005SBEN00400	FortiSandbox			030010005SBEN00400	2.03146 (2020-09-30 18:34:00)	41.81 MB	Latest	<a href="#">Change</a>
AntiVirus Signature Database	FortiSandbox	3.1.0+	AntiVirus	030010005SBEN010100	80.00858 (2020-10-05 04:23:00)	20.26 KB	Latest	<a href="#">Change</a>
AntiVirus Signature Database	FortiSandbox	3.1.0+	AntiVirus	030010005SBEN010200	80.00728 (2020-09-29 18:25:00)	766.16 KB	Latest	<a href="#">Change</a>
AntiVirus Signature Database	FortiSandbox	3.1.0+	AntiVirus	030010005SBEN010300	80.00752 (2020-09-30 18:50:00)	62.07 KB	Latest	<a href="#">Change</a>
AntiVirus Engine (64bit)	FortiSandbox	3.1.0+	AntiVirus	030010005SBEN00500	6.00147 (2020-04-17 17:50:00)	2.12 MB	Latest	<a href="#">Change</a>
Tracer Tool Engine (Android)	FortiSandbox	3.1.0+	AntiVirus	030010005SBEN00600	3001.00003 (2019-03-27 01:27:00)	3.40 MB	Latest	<a href="#">Change</a>
Rating Tool Engine (Android)	FortiSandbox	3.1.0+	AntiVirus	030010005SBEN00700	3001.00001 (2018-11-29 21:21:00)	3.63 MB	Latest	<a href="#">Change</a>
Tracer Tool Engine	FortiSandbox	3.1.0+	AntiVirus	030010005SBEN00900	3001.00154 (2019-09-24 23:19:00)	36.17 MB	Latest	<a href="#">Change</a>
Rating Tool Engine	FortiSandbox	3.1.0+	AntiVirus	030010005SBEN01000	3001.00065 (2019-09-25 23:38:00)	100.70 MB	Latest	<a href="#">Change</a>
Tracer Tool Engine (Linux)	FortiSandbox	3.1.0+	AntiVirus	030010005SBEN01300	3001.00005 (2019-05-21 22:14:00)	17.43 KB	Latest	<a href="#">Change</a>
Tracer Tool Engine (Linux)	FortiSandbox	3.1.0+	AntiVirus	030010005SBEN01400	3001.00006 (2019-05-29 18:16:00)	78.18 KB	Latest	<a href="#">Change</a>
030010025SBEN00500	FortiSandbox			030010025SBEN00500	6.00147 (2020-04-17 17:50:00)	2.12 MB	Latest	<a href="#">Change</a>
030010025SBEN00600	FortiSandbox			030010025SBEN00600	3001.00003 (2019-10-23 19:54:00)	3.40 MB	Latest	<a href="#">Change</a>
030010025SBEN00700	FortiSandbox			030010025SBEN00700	3001.00001 (2019-10-23 19:11:00)	3.63 MB	Latest	<a href="#">Change</a>
030010025SBEN00900	FortiSandbox			030010025SBEN00900	3001.00196 (2020-04-28 17:07:00)	36.17 MB	Latest	<a href="#">Change</a>
030010025SBEN01000	FortiSandbox			030010025SBEN01000	3001.00092 (2020-05-08 19:10:00)	111.39 MB	Latest	<a href="#">Change</a>
030010025SBEN01300	FortiSandbox			030010025SBEN01300	3001.00005 (2019-10-24 17:03:00)	17.41 KB	Latest	<a href="#">Change</a>
030010025SBEN01400	FortiSandbox			030010025SBEN01400	3001.00006 (2019-10-24 00:13:00)	78.18 KB	Latest	<a href="#">Change</a>

### 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.

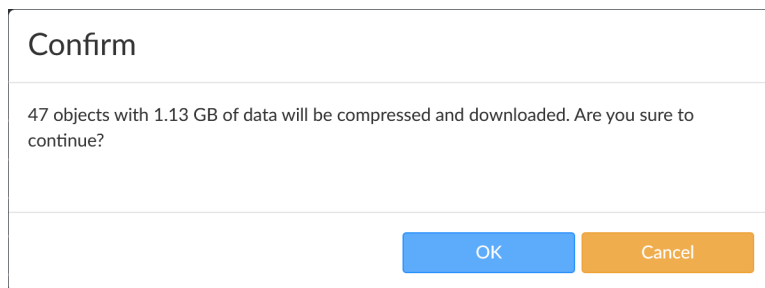
image

- b. In the **Change to Version** box, select the version to deploy, and click **OK**.

The *To Be Deployed* column displays the selected version.

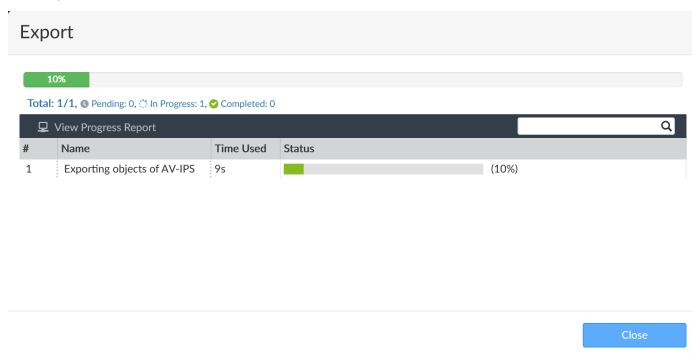
### 4. Select one or more packages, and click **Export**.

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.

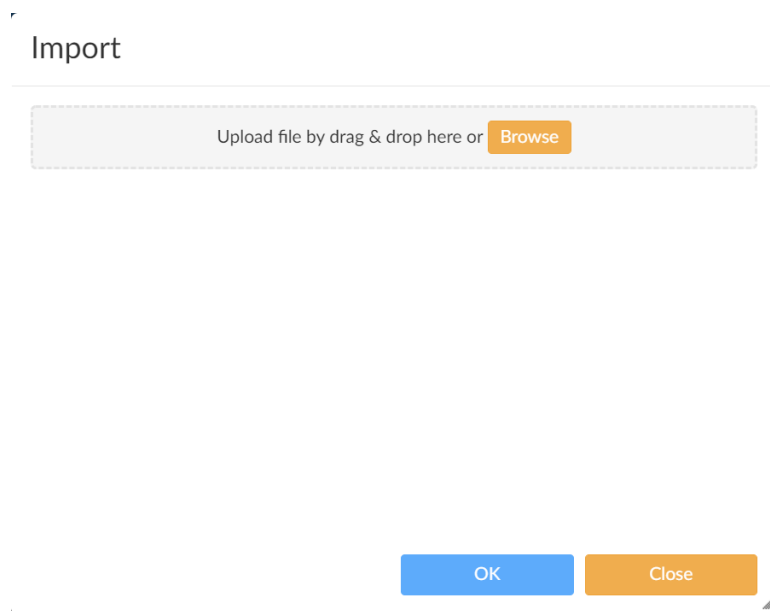
## Importing packages - example

You can import packages that you exported from another FortiManager.

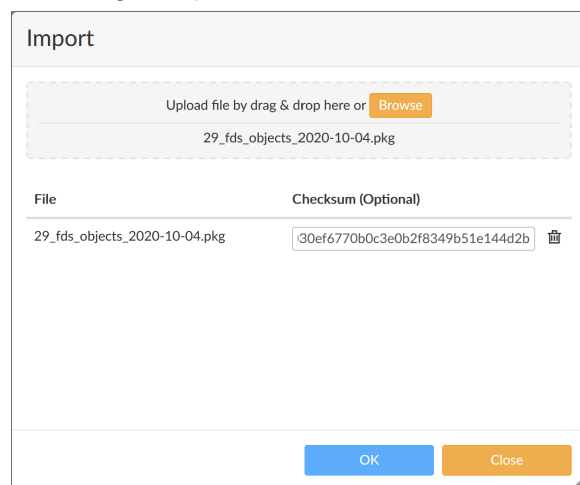
### To import packages:

1. Go to *FortiGuard > Package Management > Receive Status*.
2. Click *Import* box.

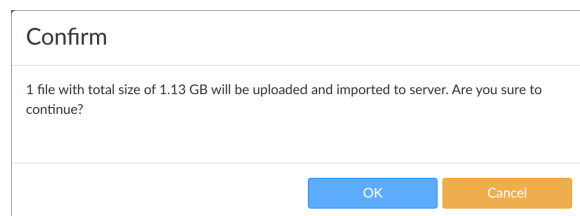
The Import dialog box is displayed.



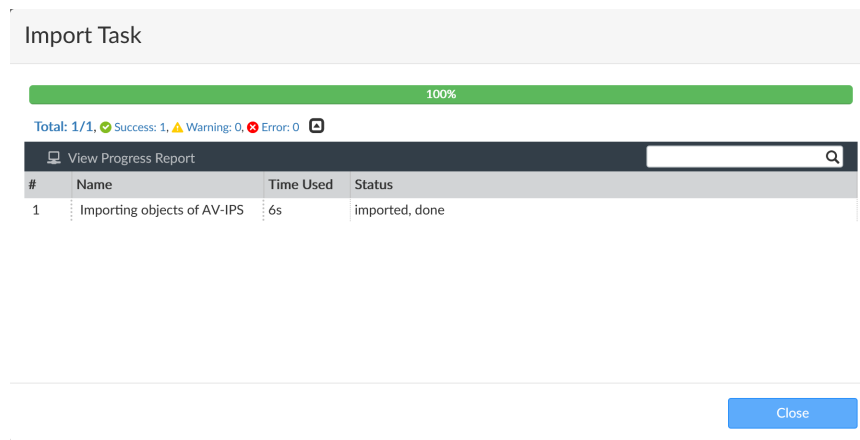
3. Drag and drop the exported package onto the dialog box.  
The dialog box updates.



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*.

## Query server management

The query server manager 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

To view the received packages, go to *FortiGuard > Query Server Management > Receive Status*.

The following information is displayed:

<b>Refresh</b>	Select to refresh the table.
<b>Export</b>	Select a package, and click <i>Export</i> . The package is compressed and downloaded to your management computer. You can import the package into another FortiManager.
<b>Import</b>	Click <i>Import</i> to select a package exported from another FortiManager and import it into this FortiManager.
<b>Search</b>	Use the search field to find a specific entry in the table.
<b>History</b>	The record of received packages.
<b>Package Received</b>	The name of the received package.
<b>Latest Version (Release Date/Time)</b>	The latest version of the received package.
<b>Size</b>	The size of the package.
<b>Update History</b>	Click to view the package update history.

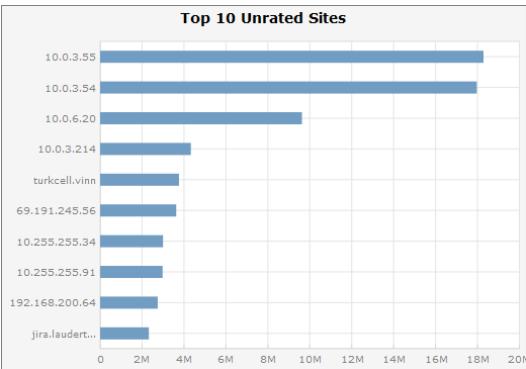
Update history

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 Server Management > 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.

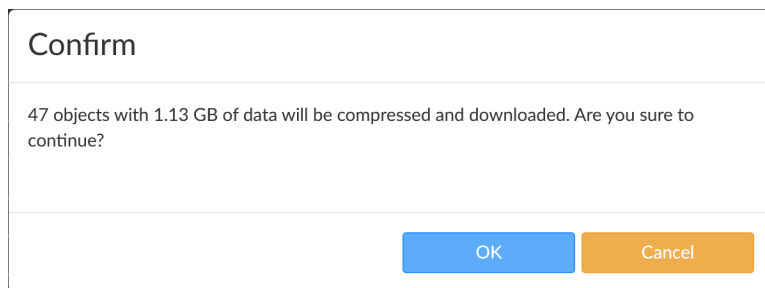
Exporting web filter databases - example

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:

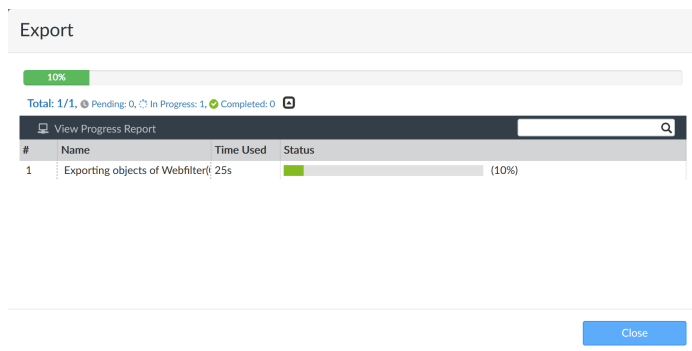
1. Go to *FortiGuard > Query Server Management > Receive Status*.
2. Select *Webfilter*, and click *Export*.  
The *Confirm* dialog box is displayed.





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.

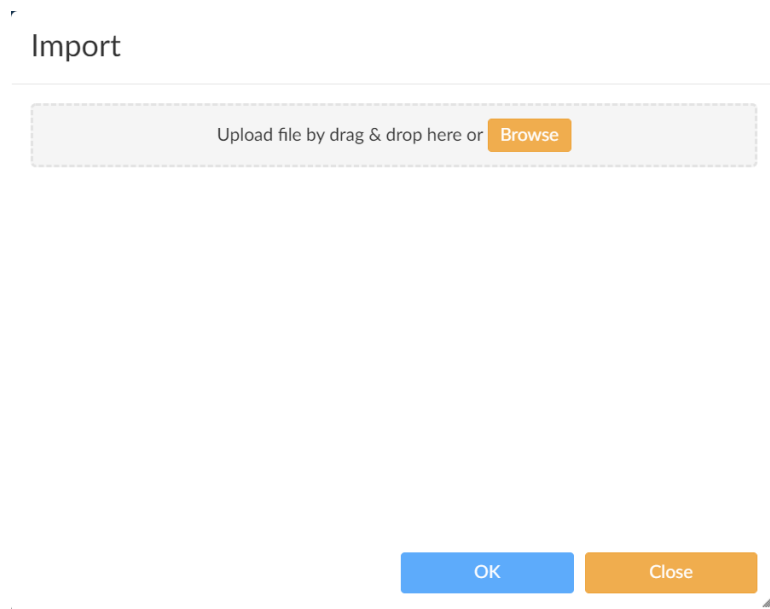
## Importing web filter databases - example

You can import web filter databases that you exported from another FortiManager.

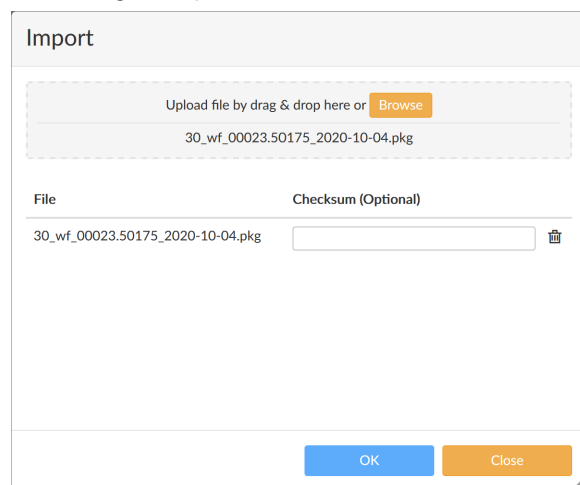
### To import web filter databases:

1. Go to *FortiGuard > Query Server Management > Receive Status*.
2. Click *Import* box.

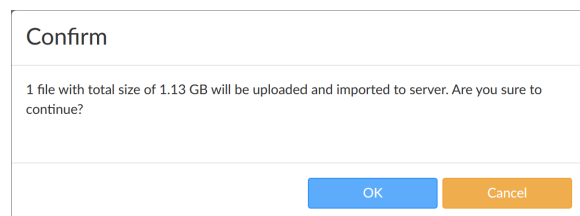
The Import dialog box is displayed.



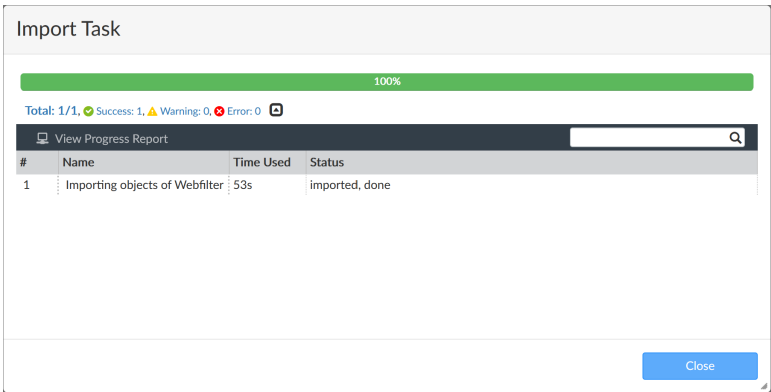
3. Drag and drop the exported package onto the dialog box.  
The dialog box updates.



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*.

## Firmware images

Go to *FortiGuard > Firmware Images* to manage the firmware images stored on the FortiManager device. You can import firmware images for FortiGate, FortiCarrier, FortiAnalyzer, FortiManager, FortiAP, FortiExtender, FortiSwitch, and FortiClient.

You can download only those images that are needed from the FDS systems, and customize which firmware images are available for deployment.

The following information and settings are available:

Import Images	Select to open the firmware image import list.
Models	From the dropdown list, select <i>All</i> to show all the available models on the FortiGuard server, or select <i>Managed</i> 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 <i>Change</i> to open the <i>Change Version</i> dialog box, then select the desired version from the dropdown list and select <i>OK</i> 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 643](#).

**Enable by Package**

Toggle *ON* to enable download prioritization by package. See [Package download prioritization on page 644](#).

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

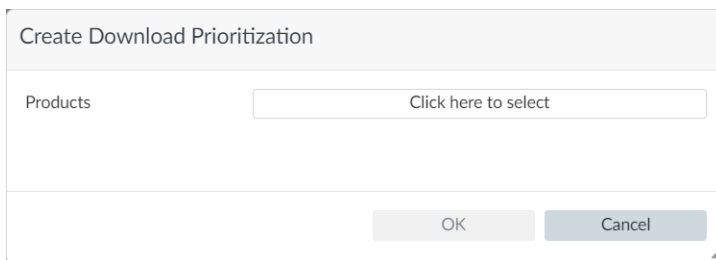
You can add products and versions to the download prioritization list, and then specify the download priority for the selected products and versions. Top priority is number 1.

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.



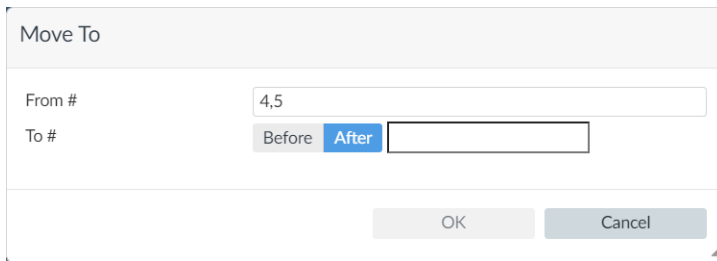
The dialog box titled "Create Download Prioritization" has a "Products" label and a text input field with the placeholder "Click here to select". At the bottom right, there are "OK" and "Cancel" buttons.

- 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.

Enable By Product <input checked="" type="checkbox"/>		
<div> <span>+ Create New</span> <span>🗑 Delete</span> <span>📁 Move To</span> <span>⚙ Column Settings</span> </div>		
<input type="checkbox"/> #	Product	Version
<input type="checkbox"/> 1	FortiClient	5.2
<input type="checkbox"/> 2	FortiGate	6.0
<input type="checkbox"/> 3	FortiMail	5.1
<input type="checkbox"/> 4	FortiDeceptor	3.1
<input type="checkbox"/> 5	FortiMail	5.3
<input type="checkbox"/> 6	FortiManager	6.2

3. Specify the download priority for products:
  - a. Select one or more products, and click *Move To*.  
The *Move To* dialog box is displayed.



Move To

From # 4,5

To # Before After

OK Cancel

- 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 644](#).

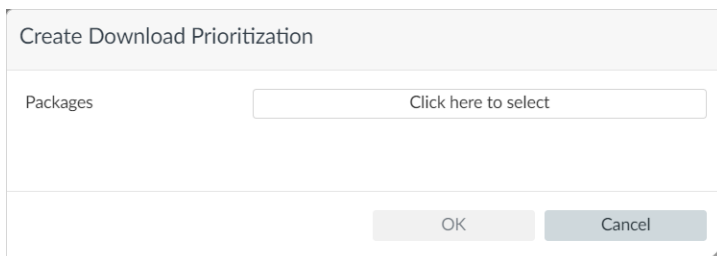
## Package download prioritization

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.



Create Download Prioritization

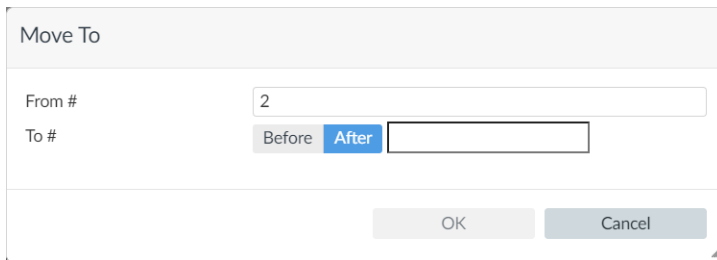
Packages

OK Cancel

- 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.

Enable By Package <input checked="" type="checkbox"/>							
+ Create New <input type="checkbox"/> Delete <input type="checkbox"/> Move To <input type="checkbox"/> Column Settings <input type="checkbox"/>							
<input type="checkbox"/> #	Package Name	Product	Version	Service Entitlement	Type	Latest Version (Release Date/Time)	Size
<input type="checkbox"/> 1	AntiVirus Signature Dat	FortiClient	6.0.0+	EMS	06000000FVDB00000	NA	NA
<input type="checkbox"/> 2	00000000FCNI00000	FortiGate			00000000FCNI00000	NA	NA
<input type="checkbox"/> 3	Internet Service DB	FortiManager	6.0.0+	Internet Service DB	06000000FFDB00305	7.01711 (2021-07-14 13:31:00)	6.91 KB

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.



The *Move To* dialog box is shown. It has a title bar 'Move To'. Below it, there are two input fields: 'From #' with the value '2' and 'To #' with a dropdown menu showing 'Before' and 'After' (selected). At the bottom, there are 'OK' and 'Cancel' buttons.

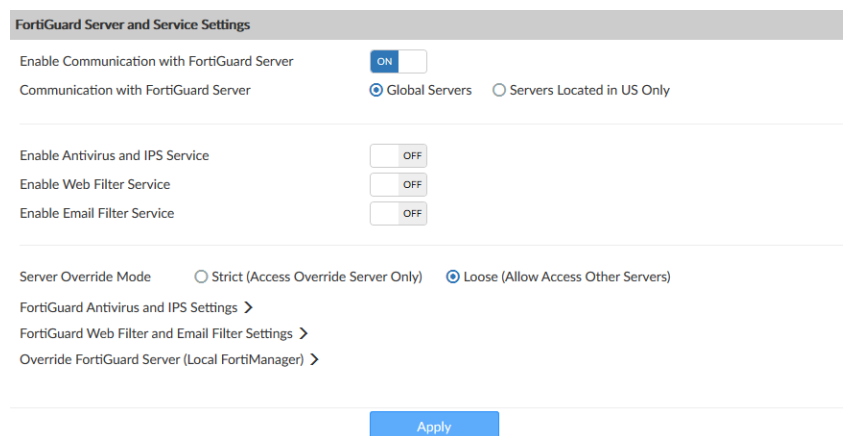
- b. Beside *To #*, select *Before* or *After*, and click the box to use the up and down arrows to position the selected packages in the priority list.
  - c. Click *OK*.  
The packages are moved, and the updated priority list is displayed.  
You can remove packages from the priority list. Select one or more packages, and click *Delete*.
4. (Optional) Add products and versions to the priority list. See [Product download prioritization on page 643](#).

## 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 649](#).



The *FortiGuard Server and Service Settings* page is shown. It includes the following settings:

- Enable Communication with FortiGuard Server:** ☒ ON
- Communication with FortiGuard Server:** ☒ Global Servers ☐ Servers Located in US Only
- Enable Antivirus and IPS Service:** ☐ OFF
- Enable Web Filter Service:** ☐ OFF
- Enable Email Filter Service:** ☐ OFF
- Server Override Mode:** ☐ Strict (Access Override Server Only) ☒ Loose (Allow Access Other Servers)
- FortiGuard Antivirus and IPS Settings >**
- FortiGuard Web Filter and Email Filter Settings >**
- Override FortiGuard Server (Local FortiManager) >**

An **Apply** button is located at the bottom.

### 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 649](#).

<b>Communication with FortiGuard Server</b>	Select <i>Servers Located in the US Only</i> to limit communication to FortiGuard servers located in the USA. Select <i>Global Servers</i> to communicate with servers anywhere.
<b>Enable Antivirus and IPS Service</b>	Toggle <i>ON</i> to enable antivirus and intrusion protection service. When on, select what versions of <i>FortiGate</i> , <i>FortiMail</i> , <i>FortiSandbox</i> , <i>FortiClient</i> , <i>FortiDeceptor</i> , and <i>FortiTester</i> to download updates for.
<b>Enable Web Filter and Service</b>	Toggle <i>ON</i> to enable web filter services. When uploaded to FortiManager, the Web Filter database version is displayed.
<b>Enable Email Filter Service</b>	Toggle <i>ON</i> to enable email filter services. When uploaded to FortiManager, the Email Filter databases versions are displayed.
<b>Server Override Mode</b>	Select <i>Strict (Access Override Server Only)</i> or <i>Loose (Allow Access Other Servers)</i> override mode.
<b>FortiGuard Antivirus and IPS Settings</b>	Configure antivirus and IPS settings. See <a href="#">FortiGuard antivirus and IPS settings on page 646</a> .
<b>FortiGuard Web Filter and Email Filter Settings</b>	Configure web and email filter settings. See <a href="#">FortiGuard web and email filter settings on page 647</a> .
<b>Override FortiGuard Server (Local FortiManager)</b>	Configure web and email filter settings. See <a href="#">Override FortiGuard server (Local FortiManager) on page 648</a> .

## FortiGuard antivirus and IPS settings

In this section you can enable settings for FortiGuard Antivirus and IPS settings. The following settings are available:

<b>Use Override Server Address for FortiClient</b>	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 <a href="#">Overriding default IP addresses and ports on page 662</a> .
<b>Use Override Server Address for FortiGate/FortiMail</b>	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 <a href="#">Overriding default IP addresses and ports on page 662</a> .
<b>Allow Push Update</b>	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 <a href="#">Enabling push updates on page 660</a> .
<b>Use Web Proxy</b>	Configure the FortiManager system's built-in FDS to connect to the FDN through a web proxy.  To enable updates using a web proxy, see <a href="#">Enabling updates through a web proxy on page 662</a> .



**Scheduled Regular Updates**

Configure when packages are updated without manually initiating an update request.

To schedule regular service updates, see [Scheduling updates on page 663](#).

**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.

FortiGuard Web Filter and Email Filter Settings ▾

Connection to FDS Server(s)

☐ OFF

Use Override Server Address for FortiClient

☐ OFF

Use Override Server Address for FortiGate/FortiMail

☐ OFF

Use Web Proxy

Polling Frequency

Poll Every

0

Hour

10

Minute

Log Settings

☒ ON

Log FortiGuard Server Update Events

FortiGuard Web Filtering

☐ Log URL disabled ☒ Log non-uri events ☐ Log all URL lookups

FortiGuard Anti-spam

☐ Log Spam disabled ☒ Log non-spam events ☐ Log all Spam lookups

FortiGuard Anti-virus Query

☐ Log Virus disabled ☒ Log non-virus events ☐ Log all Virus lookups

Override FortiGuard Server (Local FortiManager) >

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 662](#).

To enable web filter and email filter service updates using a web proxy server, see [Enabling updates through a web proxy on page 662](#).

**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 662](#).

**Use Web Proxy**

Configure the FortiManager system's built-in FDS to connect to the FDN through a web proxy. IPv4 and IPv6 are supported.

To enable updates using a web proxy, see [Enabling updates through a web proxy on page 662](#).

**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 664](#).

## 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 739](#).

## 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 660](#).
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 739](#).  
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 support, and then uploaded to the FortiManager.



As databases can be large, we recommend uploading them using the CLI. See [Uploading packages with the CLI on page 651](#).

---

Go to *FortiGuard > Settings* to configure FortiManager as a local FDS server and to upload update packages and license.

## FortiGuard Server and Service Settings

Enable Communication with FortiGuard Server

---

Enable AntiVirus and IPS Service

FortiGate ☐ 5.4 ☐ 5.6 ☐ 6.0 ☐ 6.2 ☐ 6.4

FortiMail ☐ All v4 ☐ All v5 ☐ All v6

FortiSandbox ☐ All v1 ☐ All v2 ☐ All v3

FortiClient ☐ All v4 ☐ 5.0 ☐ 5.2 ☐ 5.4 ☐ 5.6 ☐ 6.0

☐ 6.2 ☐ 6.4

FortiSwitch ☐ 5.4 ☐ 5.6 ☐ 6.0 ☐ 6.2

Enable Web Filter Service

Enable Email Filter Service

---

Upload Options for FortiGate/FortiMail

Packages and Database

Service License

Upload Options for FortiClient

AntiVirus/IPS Packages

**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. When on, select what versions of *FortiGate*, *FortiClient*, *FortiAnalyzer*, and *FortiMail* to download updates for.

**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.

**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 Customer Service & Support portal on your management computer, or drag and drop the file onto the dialog box.

Click *OK* to upload the package to FortiManager.

As the database can be large, uploading with the CLI is recommended. See [Uploading packages with the CLI on page 651](#).

**Service License**

Select to import the FortiGate or FortiSOAR license. Browse for the file on your management computer, or drag and drop the file onto the dialog box.

Click *OK* to upload the package to FortiManager.

A license file can be obtained from support by requesting your account entitlement for the device. See [Requesting account entitlement files on page 655](#).

### Upload Options for FortiClient

#### AntiVirus/IPS Packages

Select to upload the FortiClient AntiVirus/IPS packages. Browse for the file you downloaded from the Customer Service & Support portal on your management computer, or drag and drop the file onto the dialog box.

Click **OK** to upload the package to FortiManager.

## 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 CLI.



When internet access is restricted by a web proxy, you can establish a connection to FortiGuard for the FortiCare registration information or status using the following commands in the CLI:

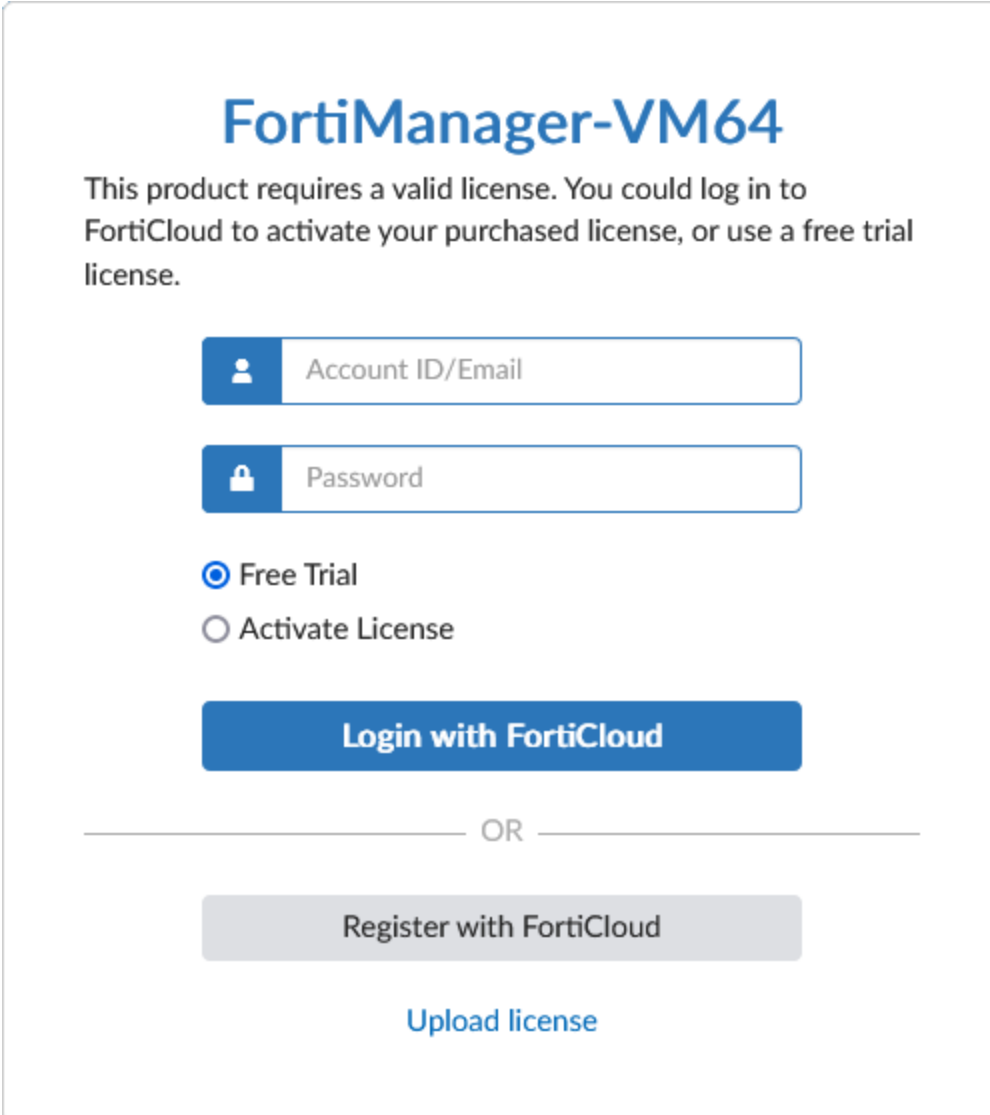
```
config fmupdate av-ips web-proxy
  set address <enter the web proxy address>
  set port <enter the port number of the web proxy (1 - 65535,
    default = 80)>
  set status enable
end
```

### 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:

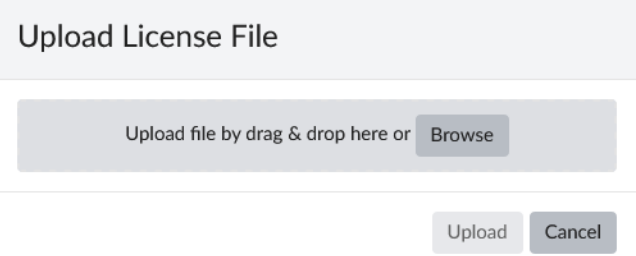
```
config fmupdate publicnetwork
  set status disable
end
```

2. Connect to the FortiManager GUI, and on the FortiManager login screen, click *Upload License*.



The screenshot shows the FortiManager-VM64 login interface. At the top, the title 'FortiManager-VM64' is displayed in blue. Below it, a message states: 'This product requires a valid license. You could log in to FortiCloud to activate your purchased license, or use a free trial license.' There are two input fields: 'Account ID/Email' with a person icon and 'Password' with a lock icon. Below these fields are two radio buttons: 'Free Trial' (selected) and 'Activate License'. A blue button labeled 'Login with FortiCloud' is positioned below the radio buttons. A horizontal line with the word 'OR' in the center separates this section from the next. Below the line is a gray button labeled 'Register with FortiCloud'. At the bottom of the form is a blue link labeled 'Upload license'.

3. Click *Browse* to select your FortiManager license or drag-and-drop the license file, and click *Upload*.



The screenshot shows the 'Upload License File' dialog box. It has a title bar that says 'Upload License File'. Below the title bar is a gray area with the text 'Upload file by drag & drop here or' followed by a 'Browse' button. At the bottom of the dialog are two buttons: 'Upload' and 'Cancel'.

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.

**FortiManager Setup - Welcome (1/4)**

**Welcome**

Perform the following steps to complete the setup of this FortiManager.

1. Register and SSO with FortiCare

☐ Import the Entitlement File

2. Specify Hostname

3. Change Your Password

4. Upgrade Firmware

Begin

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.

**FortiManager Setup - Welcome (1/4)**

**Welcome**

Perform the following steps to complete the setup of this FortiManager.

1. Register and SSO with FortiCare

☒ Import the Entitlement File

Add files by drag & drop here or [Add Files](#)

2. Specify Hostname

3. Change Your Password ✓

4. Upgrade Firmware ✓

Begin

b. *Command line interface:*

- i. Open the FortiManager CLI.
- ii. Upload the entitlement file using the following command.
 

```
execute fupdate <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:

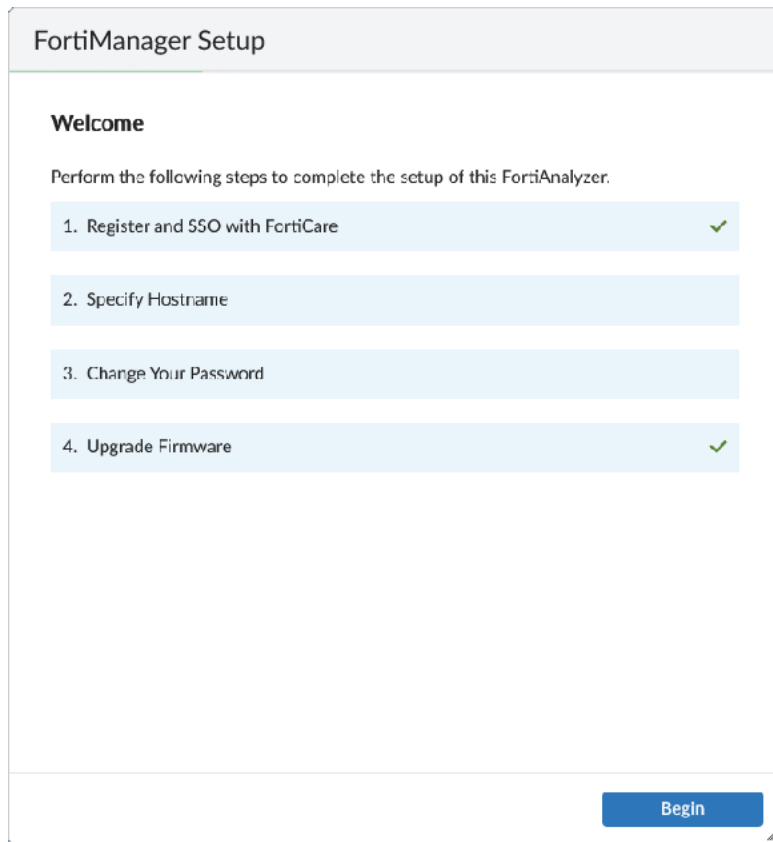
```
execute fupdate ftp import license entitlement-file 172.10.1.10 /pub/place
user1 password1
This operation will replace the current package!
Do you want to continue? (y/n)y

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.

You can request an entitlement file from Fortinet Customer Service & Support by creating a support ticket.

For example, you can request an account entitlement file for FortiSOAR units, and then upload the license file to the FortiGuard panel. See [Uploading account entitlement files on page 657](#).

### To request account entitlement files:

1. Log in to the Fortinet Customer Service & Support site (<https://support.fortinet.com/>).
2. Go to *Support > Create a Ticket*.

The *Ticket Wizard* is displayed, starting at the *1 Request Type* page.

**Ticket Wizard** Create Ticket

1 Request Type > 2 > 3 > 4

Specify Request Ticket Type

**Technical Support Ticket**  
You can create technical support tickets for technical issues with your Fortinet product. You require a Fortinet product with an active support contract to create this type of ticket. You will need to input the product serial number.

**Customer Service**  
You can create customer service tickets for questions related to contracts and account management.

3. In the *Specify Request Ticket Type* list, expand *Customer Service*, and click *Submit Ticket*.

**Ticket Wizard** Create Ticket

1 Request Type > 2 > 3 > 4

Specify Request Ticket Type

**Technical Support Ticket**  
You can create technical support tickets for technical issues with your Fortinet product. You require a Fortinet product with an active support contract to create this type of ticket. You will need to input the product serial number.

**Customer Service**  
You can create customer service tickets for questions related to contracts and account management.

**Submit Ticket**

**Start Web Chat**  
You can talk to our customer service representatives via online web chat.

The wizard moves to the *2 Basic Info* page, where you can specify ticket information.

4. On the *Specify Ticket Information* page, complete the following options, and click *Next*.
- In the *Serial Number* box, add the serial number for the device for which you want an entitlement file.
  - In the *Subject* box, type *Entitlement file*.
  - In the *Category* list, select *Contract/License*.

**Ticket Wizard** CS Ticket  
Serial Number: N/A

1 Request Type > 2 Basic Info > 3 Comment > 4 Completion

Specify Ticket Information

Serial Number:

**Contact Information**

Name:

Email:

Telephone:

Mobile Phone:

**Ticket Information**

Subject:

Category:

Previous Next

The wizard moves to the *3 Comment* page, where you can add a comment.

5. In the *Add Comment* box, request the entitlement file, and click *Next*.  
The request is complete.
6. Monitor your email to receive the entitlement file, and download it to your computer.

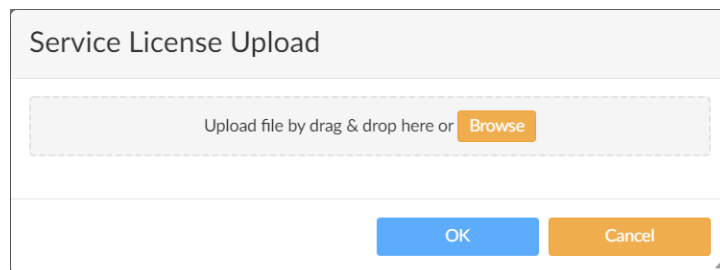
## Uploading account entitlement files

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 655](#).
2. Ensure that FortiManager is configured to work in a closed network. See [Operating as an FDS in a closed network on page 649](#).
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.

Procedures for configuring devices to use the built-in FDS vary by device type. See the documentation for your device for more information.



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 738](#) for details.

## 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 7.0 Ports and Protocols Guide](#).

## 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. Go to the *CLI Console* widget in the *System Settings > Dashboard* pane. For information on widget settings, see [Customizing the dashboard on page 720](#).
2. Click inside the console to connect.
3. To configure the system to add unauthorized devices and allow service requests, type the following CLI command lines:

```
config system admin setting
    set unreg_dev_opt add_allow_service
end
```

4. To configure the system to add unauthorized devices but deny service requests, type the following CLI command lines:

```
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 649](#).

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](#)

## 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 662](#).

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 646](#).
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
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.

### To enable updates to the FortiManager system through a proxy:

1. Go to *FortiGuard > Settings*.
2. If configuring a web proxy server to enable web and email filtering updates, expand *FortiGuard Web Filter and Email Filter Settings*.
3. If configuring a web proxy to enable antivirus and IPS updates, expand *FortiGuard Antivirus and IPS Settings*.
4. Toggle **ON** beside *Use Web Proxy* and enter the IP address and port number of the proxy.
5. If the proxy requires authentication, enter the user name and password.
6. Click *Apply*.

If the FDN connection status is *Disconnected*, the FortiManager system is unable to connect through the web proxy.

## 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 648](#).



## 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 646](#).
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 665](#).

---

## 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*.

## 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 646](#).
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, then click *Apply*:

Log Settings	
<b>Log FortiGuard Server Update Events</b>	Enable or disable logging of FortiGuard server update events.
FortiGuard Web Filtering	
<b>Log URL disabled</b>	Disable URL logging.
<b>Log non-URL events</b>	Logs only non-URL events.
<b>Log all URL lookups</b>	Logs all URL lookups (queries) sent to the FortiManager system's built-in FDS by FortiGate devices.
FortiGuard Anti-spam	
<b>Log Spam disabled</b>	Disable spam logging.
<b>Log non-spam events</b>	Logs email rated as non-spam.
<b>Log all Spam lookups</b>	Logs all spam lookups (queries) sent to the FortiManager system's built-in FDS by FortiGate devices.
FortiGuard Anti-virus Query	
<b>Log Virus disabled</b>	Disable virus logging.
<b>Log non-virus events</b>	Logs only non-virus events.
<b>Log all Virus lookups</b>	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:

- Central management of managed switches
- Per-device management of managed switches

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:

<b>Device &amp; Groups on page 666</b>	Displays unauthorized and authorized FortiSwitch devices. You can view, authorize, and edit authorized switches, as well as apply templates to switches.
<b>FortiSwitch Templates</b>	View, create, and edit FortiSwitch templates, VLANs, security policies, and custom commands. Templates can also be imported.

When [per-device management](#) is enabled, the *FortiSwitch Manager* module includes the following in the tree menu:

<b>Device &amp; Groups on page 666</b>	Displays unauthorized and authorized FortiSwitch devices. You can view, authorize, and edit authorized switches as well as configure ports for each managed switch in the <i>Managed Switches</i> tab.  View, create, and edit VLANs, security policies, LLDP profiles, QoS policies, and custom commands for each managed switch in the <i>FortiSwitch Profiles</i> tab.  Use the CLI to configure switches in the <i>CLI Configurations</i> tab.
--	--

## Device & Groups

On the *FortiSwitch Manager* pane, use the *Device & Groups* tree menu to access options for managing FortiSwitch devices and creating templates and profiles.

When [central management](#) is enabled, use *Device & Groups* to view and manage the following:

<b>Managed Switches</b>	<i>Managed FortiGate</i> displays managed FortiGate devices in the tree menu. Select a managed FortiGate device or VDOM to view its FortiSwitch devices in the <i>Managed FortiSwitch</i> pane. You can view, authorize, and edit authorized switches, as well as apply templates to switches.
-------------------------	--

When [per-device management](#) is enabled, use *Device & Groups* to view and manage the following:

<b>Managed Switches</b>	Displays unauthorized and authorized FortiSwitch devices. You can view, authorize, and edit authorized switches as well as configure ports for each managed switch.
-------------------------	---

**FortiSwitch Profiles**

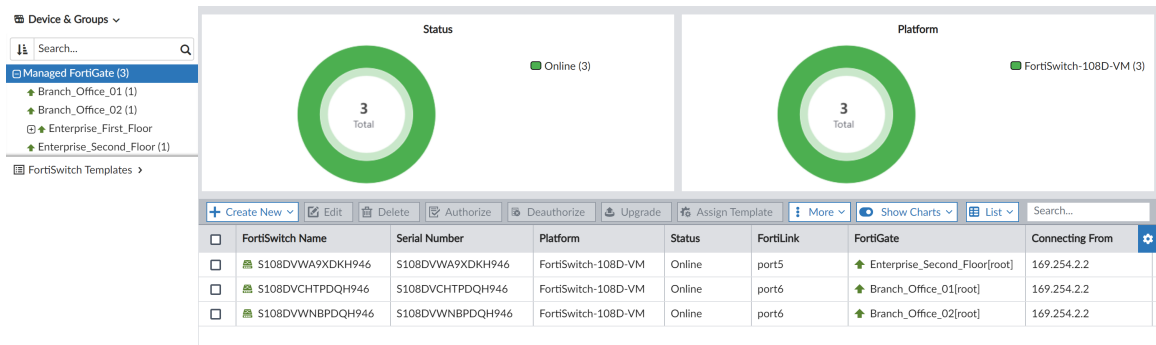
View, create, and edit VLANs, security policies, LLDP profiles, QoS policies, and custom commands for each managed switch.

**CLI Configurations on page 705**

You can use the CLI to configure switches.

Managed Switches

Go to *FortiSwitch Manager > Device & Groups* 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 770](#).

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:

- Managed FortiSwitch
- Online
- Offline
- Unauthorized
- Unknown

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 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 > Devices & Groups*. 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 > Device & Groups* pane when *Managed FortiSwitch* is selected.

<div> <span>+ Create New</span> <span>Edit</span> <span>Delete</span> <span>Authorize</span> <span>Deauthorize</span> <span>Upgrade</span> <span>Assign Template</span> <span>More</span> <span>Show Charts</span> <span>List</span> <span>Search...</span> </div>									
<input type="checkbox"/>	FortiSwitch Name	Serial Number	Platform	Status	FortiLink	FortiGate	Connecting From	OS Version	
<input type="checkbox"/>	 S108DVWA9XDKH946	S108DVWA9XDKH946	FortiSwitch-108D-VM	Online	port5	 Enterprise_Second_Floor[root]	169.254.2.2	S108DV-v7.0.0-buil	
<input type="checkbox"/>	 S108DVCHTPDQH946	S108DVCHTPDQH946	FortiSwitch-108D-VM	Online	port6	 Branch_Office_01[root]	169.254.2.2	S108DV-v7.0.0-buil	
<input type="checkbox"/>	 S108DVWNBPDQH946	S108DVWNBPDQH946	FortiSwitch-108D-VM	Online	port6	 Branch_Office_02[root]	169.254.2.2	S108DV-v7.0.0-buil	

The following options are available from the toolbar and right-click menu:

<b>Create New</b>	<p>From the dropdown, add a FortiSwitch device using the model device wizard or add a new FortiSwitch group.</p> <p>For adding FortiSwitch devices, see <a href="#">Using zero-touch deployment for FortiSwitch on page 674</a>.</p> <p>For adding FortiSwitch groups, see <a href="#">Creating a FortiSwitch group on page 675</a>.</p>
<b>Edit</b>	Edit the selected FortiSwitch.
<b>Delete</b>	Delete the selected FortiSwitch or FortiSwitches.
<b>Authorize</b>	Authorize a switch. See <a href="#">Authorizing and deauthorizing FortiSwitch devices on page 673</a> .
<b>Deauthorize</b>	Deauthorize a switch. See <a href="#">Authorizing and deauthorizing FortiSwitch devices on page 673</a> .
<b>Upgrade</b>	Upgrade the switch. The FortiSwitch must already be authorized.

	Before upgrading FortiSwitch, you can optionally go to <i>FortiGuard &gt; Firmware Images &gt; Product: FortiSwitch</i> , and click the download icon to manually download the firmware images.
<b>Assign Template</b>	Available when central management is enabled for <i>FortiSwitch Manager</i> . Assign a template to the FortiSwitch. Only applicable templates will be listed. See <a href="#">Assigning templates to FortiSwitch devices on page 699</a> .
<b>More</b>	Select <i>More</i> from the toolbar to view additional options. These options are also available from the right-click menu.
<b>View Ports</b>	Available when per-device management is enabled for <i>FortiSwitch Manager</i> . View and configure ports for the selected FortiSwitch. See <a href="#">Configuring a port on a single FortiSwitch on page 706</a> .
<b>Faceplates</b>	View the faceplate monitor. See <a href="#">Monitors on page 680</a> .
<b>Replace</b>	Replace a FortiSwitch device. Selecting this option allows you to enter a new FortiSwitch Serial Number for the selected device. See <a href="#">Replacing switches on page 672</a> .
<b>Restart</b>	Restart the FortiSwitch.
<b>Refresh</b>	Refresh the FortiSwitch list.
<b>Factory Reset</b>	Reset the FortiSwitch to factory settings.
<b>Register</b>	View the registration status and/or register the FortiSwitch to a FortiCloud account.
<b>Export to Excel/CSV</b>	Export the selected device details to an Excel or CSV file.
<b>Diagnostics and Tools</b>	View additional diagnostic and tool information, including device summary and cable tests. See <a href="#">Diagnostics and tools on page 677</a> . See <a href="#">Run a cable test on FortiSwitch ports from FortiManager on page 679</a> .
<b>LED Blink</b>	Start LED blink on the selected FortiSwitch for the specified period of time. This option is only available in the right-click menu.
<b>Show Charts</b>	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 <a href="#">Quick status bar on page 667</a> .
<b>List/Group/Topology</b>	Use the dropdown to toggle between the following views: <i>List</i> : Display the individual FortiSwitches in the list chart. This is the default. <i>Group</i> : Display the FortiSwitch groups in a list chart. <i>Topology</i> : Display the topology monitor. To return to the list view, click <i>Back to Managed Switches</i> . See <a href="#">Monitors on page 680</a>
<b>Search</b>	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:

<b>FortiSwitch Name</b>	The name assigned to the switch.
<b>Serial Number</b>	The serial number of the switch.
<b>Platform</b>	The FortiSwitch model.
<b>Status</b>	The online status of the switch.
<b>FortiLink</b>	The FortiLink of the switch.
<b>FortiGate</b>	The FortiGate that the FortiSwitch is connected to.
<b>Connecting From</b>	The IP address of the switch.
<b>OS Version</b>	The OS version on the switch.
<b>Join Time</b>	The date and time that the switch joined.
<b>Comments</b>	User entered comments.
<b>Template</b>	The FortiSwitch template assigned to the device, if any.

## Editing switches

FortiSwitch devices can be edited from the *FortiSwitch Manager > Device & Groups* 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.



Edit Managed FortiSwitch

Serial Number
S108DVWA9XDVG54

Name
S108DVWA9XDVG54

Description
0/63

Template
None

Managed Switch Status

Status
Online
View Ports
Restart

Connecting From
169.254.2.2

Join Time
Mon Mar 1 15:14:20 2021

Authorize State
Authorized
Deauthorize

Firmware

FortiSwitch OS Version
S108DV-v6.6.0-build5756,201009 (Interim) [Upgrade]

Enforce Firmware Version
OFF

OK
Cancel

- Edit the following options, then click *Apply* to apply your changes.

<b>Serial Number</b>	The device's serial number. This field cannot be edited.
<b>Name</b>	The name of the FortiSwitch.
<b>Description</b>	A description of the FortiSwitch, such as its model.
<b>Template</b>	Available when central management is enabled for <i>FortiSwitch Manager</i> . Select the template that will be applied to the FortiSwitch from the dropdown list. Only applicable templates are available.
<b>Custom Command Entry</b>	Available when per-device management is enabled for <i>FortiSwitch Manager</i> . Click <i>Create New</i> to create a new custom command entry that will be applied to the FortiSwitch. See <a href="#">Creating custom commands on page 704</a> .
<b>Status</b>	The status of the FortiSwitch, such as <i>Online</i> . Click <i>Restart</i> to restart the switch. Click <i>View Ports</i> to view the switches configured ports.
<b>Connecting From</b>	The IP address of the switch.
<b>Join Time</b>	The date and time that the switch joined.
<b>Authorized State</b>	The state of the AP, such as <i>Authorized</i> . If the switch is authorized, click <i>Deauthorize</i> to deauthorize the switch. If the switch is not authorized, click <i>Authorize</i> to authorize it. See <a href="#">Authorizing and deauthorizing FortiSwitch devices on page 673</a> .
<b>FortiSwitch OS Version</b>	The OS version on the switch. Click <i>Upgrade</i> to upgrade the firmware to a newer version if you have one available.
<b>Enforce Firmware Version</b>	Toggle the switch to the <i>On</i> position to enable enforced firmware versioning.

## Deleting switches

FortiSwitch devices can be deleted from the *FortiSwitch Manager > Device & Groups* pane.

### To delete FortiSwitch devices:

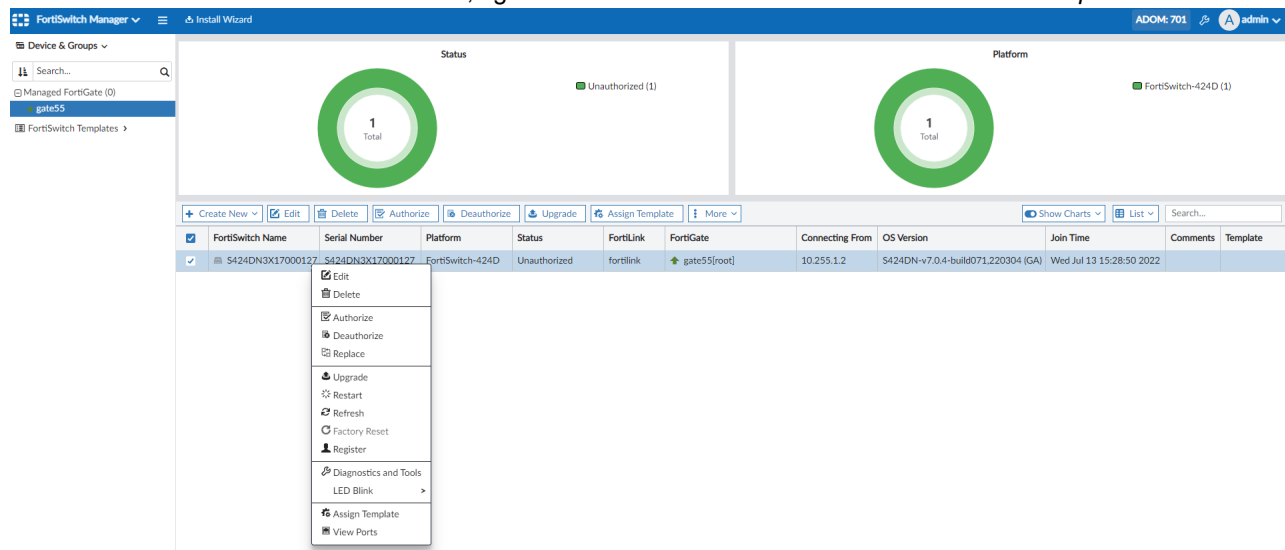
1. In the tree menu, select the FortiGate that contains the switch or switches to be deleted, or select *Managed FortiGate* to list all of the switches.
2. In the content pane, select the switch or switches, and click *Delete* from the toolbar, or right-click and select *Delete*.
3. Click *OK* in the 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 120](#).

### Replacing switches

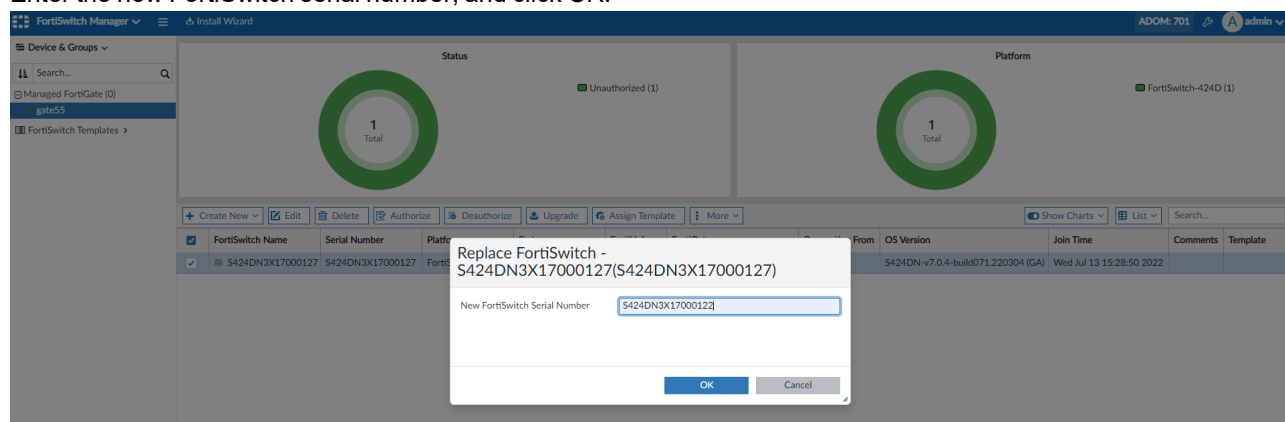
FortiSwitch devices can be replaced from the *FortiSwitch Manager > Device & Groups* pane.

### To replace a FortiSwitch device:

1. Go to *FortiSwitch Manager > Device & Groups*, and select a managed FortiGate.
2. Right-click on a FortiSwitch device in the table and click *Deauthorize*.
3. When the device's status is *Unauthorized*, right-click on the same FortiSwitch device and click *Replace*.



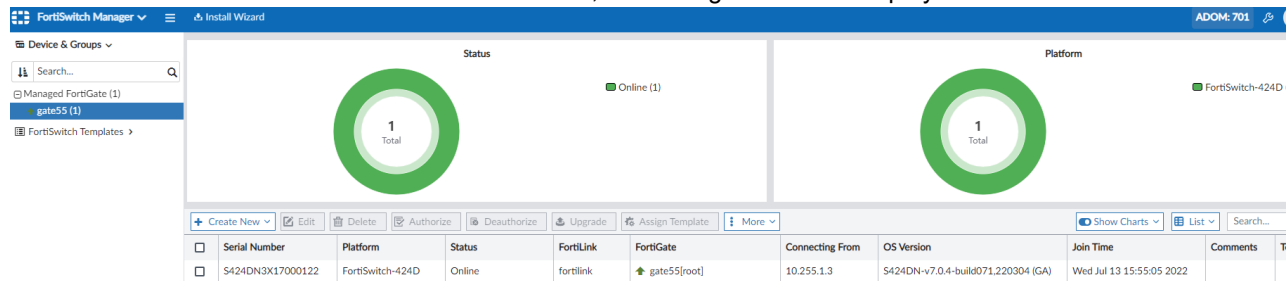
4. Enter the new FortiSwitch serial number, and click *OK*.



After the FortiSwitch has been replaced successfully, refresh the page and the new FortiSwitch is displayed as *Unauthorized*.

5. Authorize the FortiSwitch device, then connect the FortiSwitch to the FortiGate.

6. Power on the FortiSwitch device. After a few minutes, the managed switch is displayed as *Online*.



## Authorizing and deauthorizing FortiSwitch devices

FortiSwitch devices can be authorized and deauthorized from the *Managed Switches* pane, or from the *Edit Managed FortiSwitch* pane (see [Editing switches on page 670](#)).

### 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.

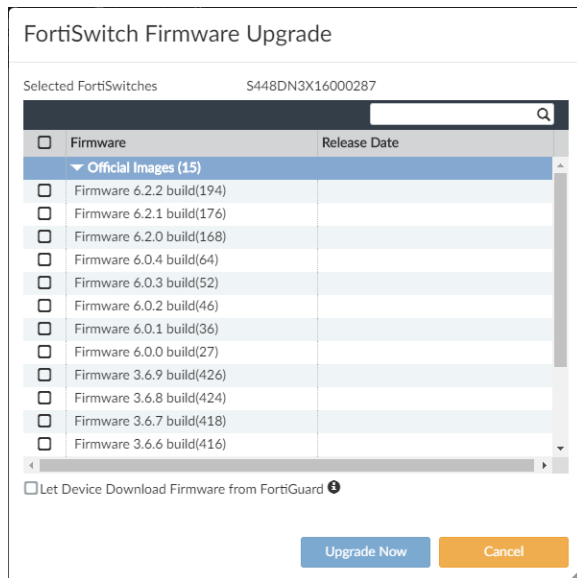
## Upgrading firmware for managed switches

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 > Device & Groups*
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.



FortiSwitch Firmware Upgrade

Selected FortiSwitches S448DN3X16000287

☐ Firmware Release Date

▼ Official Images (15)

<input type="checkbox"/>	Firmware 6.2.2 build(194)	
<input type="checkbox"/>	Firmware 6.2.1 build(176)	
<input type="checkbox"/>	Firmware 6.2.0 build(168)	
<input type="checkbox"/>	Firmware 6.0.4 build(64)	
<input type="checkbox"/>	Firmware 6.0.3 build(52)	
<input type="checkbox"/>	Firmware 6.0.2 build(46)	
<input type="checkbox"/>	Firmware 6.0.1 build(36)	
<input type="checkbox"/>	Firmware 6.0.0 build(27)	
<input type="checkbox"/>	Firmware 3.6.9 build(426)	
<input type="checkbox"/>	Firmware 3.6.8 build(424)	
<input type="checkbox"/>	Firmware 3.6.7 build(418)	
<input type="checkbox"/>	Firmware 3.6.6 build(416)	

☐ Let Device Download Firmware from FortiGuard ⓘ

Upgrade Now Cancel

4. Select the firmware, and click *Upgrade Now*.

## Using zero-touch deployment for FortiSwitch

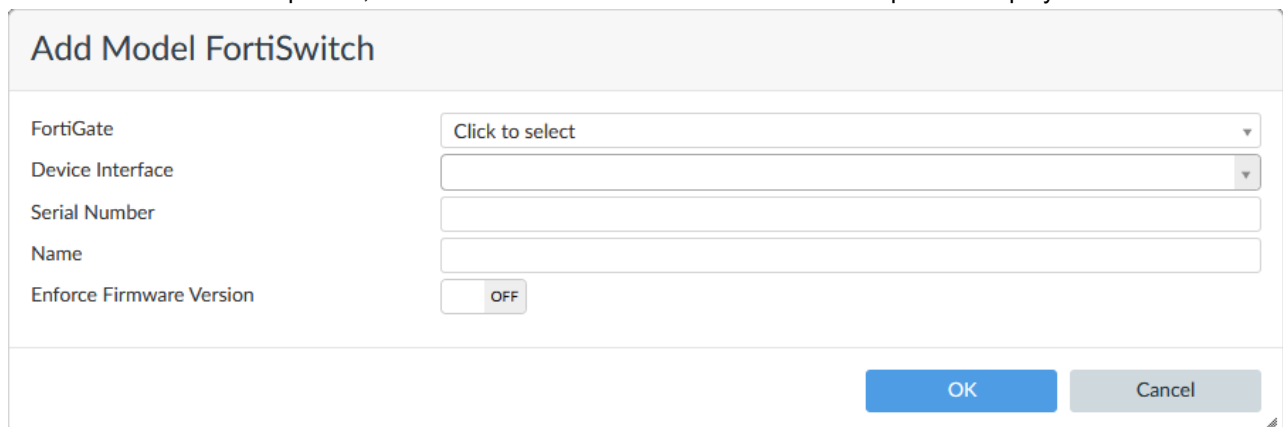
Configure FortiSwitch on FortiManager using its serial number and deploy FortiSwitch devices across the network using zero touch deployment. After configuring FortiSwitch on FortiManager, you can deploy remote FortiSwitch devices by just plugging them into remote FortiGate devices.

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 > Device & Groups*.
2. From the *Create New* dropdown, select *FortiSwitch*. The *Add Model FortiSwitch* pane is displayed.



Add Model FortiSwitch

FortiGate Click to select

Device Interface

Serial Number

Name

Enforce Firmware Version OFF

OK Cancel

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

<b>FortiGate</b>	Select the FortiGate device or VDOM from the drop-down.
<b>Device Interface</b>	Select the port where the FortiSwitch will be connected.
<b>Serial Number</b>	Specify the FortiSwitch serial number.
<b>Name</b>	Specify a name.
<b>Enforce Firmware Version</b>	Toggle <b>ON</b> to enforce a firmware version and select the firmware version from the drop-down menu. Toggle <b>OFF</b> 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 699](#).
  - For FortiSwitch Manager with per-device management enabled, see [Configuring a port on a single FortiSwitch on page 706](#).

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 62](#).

## 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 > Device & Groups*.
2. From the *Create New* dropdown, click *FortiSwitch Group*.  
The *Create New FortiSwitch Group* dialog displays.

### 3. Configure the following options:

Option	Description
<b>Name</b>	Enter a name for the FortiSwitch group.
<b>FortiGate</b>	Select the FortiGate device that controls the FortiSwitches.
<b>Switch FortiLink</b>	Select the port.
<b>FortiSwitches</b>	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 668](#)

### To edit a FortiSwitch group:

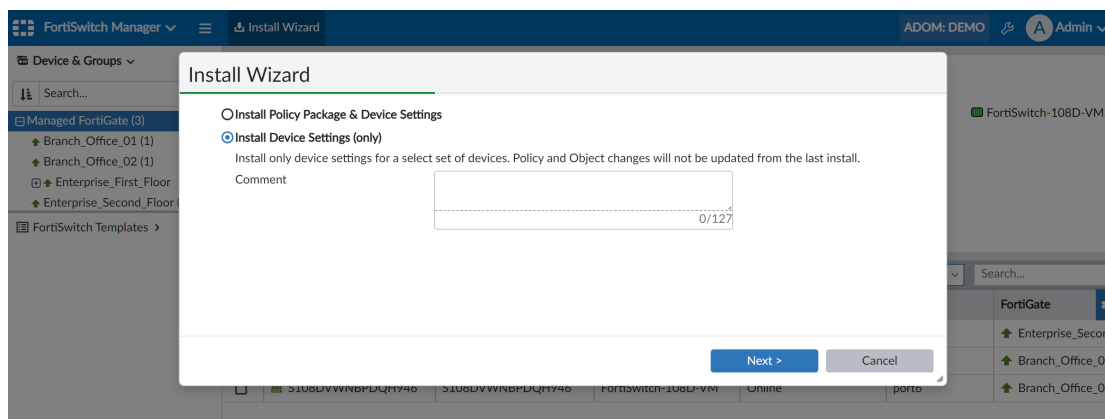
1. Go to *FortiSwitch Manager > Device & Groups*.
2. From the *List/View/Topology* dropdown, select *Group*.
3. Select the checkbox for the FortiSwitch group.
4. To edit the group, click *Edit*.  
Alternatively, you can delete the group by clicking *Delete*.

## 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 > Device & Groups*.
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.

Install Wizard - Device Settings only

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

<input checked="" type="checkbox"/>	▲ Device Name	IP Address	Platform
<input checked="" type="checkbox"/>	FortiGate-300D	10.2.172.133	FortiGate-300D
<input checked="" type="checkbox"/>	root [NAT] (Management)		vdom

< Back   Next >   Cancel

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

Install Wizard - Device Settings

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

<input checked="" type="checkbox"/>	▲ Device Name	Status	Action
<input checked="" type="checkbox"/>	FortiGate-300D	Connection Up	Install Preview

Install   Cancel

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 678](#).

Diagnostics and Tools ✕

Summary	Cable Test	
S424DN3K17000110		General Health <span>Good</span>
Name	S424DN3K17000110	16% CPU Usage
Serial Number	S424DN3K17000110	18% Memory Usage
Version	S424DN-v6.4.5-build461.201215 (GA)	9 day(s) Connection Uptime
Model	S424DN	42°C Temperature
FortiLink Interface	port24	
IP Address	169.254.1.5	
Join Time	Wed Jun 9 14:34:03 2021	
Status	Online	
Registration	Registered	
Actions <span>▼</span>		

### To view the Diagnostics and Tools form:

1. Go to *FortiSwitch Manager > Device & Groups > Managed FortiGate*.
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 *FortiSwitch Manager*, 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 > Device & Groups > Managed FortiGate*.
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 > Diagnostics and Tools* from the toolbar, or right-click the FortiSwitch and select *Diagnostics and Tools*. The *Diagnostics and Tools* form opens.
4. Click *Cable Test*.

Diagnostics and Tools ✕

Summary Cable Test

**S424DN3K17000110**

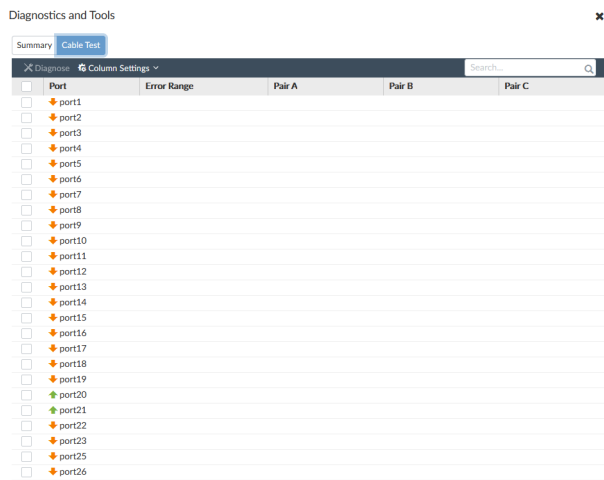
Name	S424DN3K17000110
Serial Number	S424DN3K17000110
Version	S424DN-v6.4.5-build461.201215 (GA)
Model	S424DN
FortiLink Interface	port24
IP Address	169.254.1.5
Join Time	Wed Jun 9 14:34:03 2021
Status	Online
Registration	Registered

Actions ▾

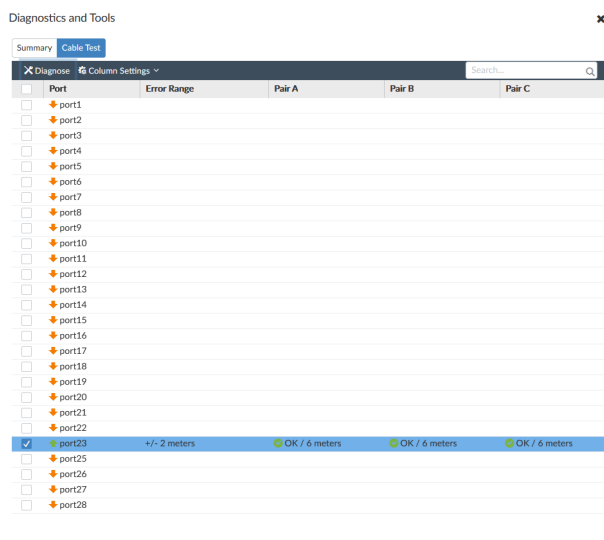
**General Health** Good

16%	CPU Usage
18%	Memory Usage
9 day(s)	Connection Uptime
42°C	Temperature

5. In the *Cable Test* pane, select the FortiSwitch ports you want to test, and click *Diagnose*.



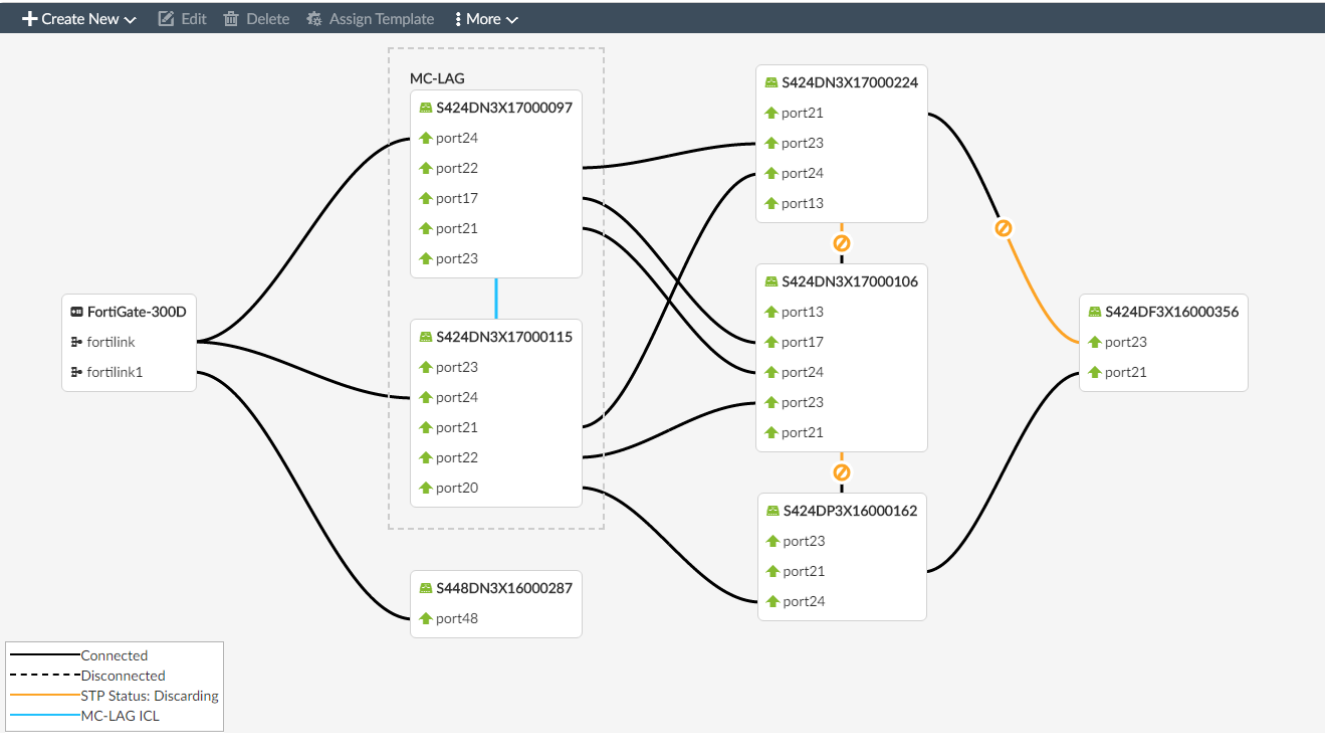
Once the cable test is run, the results are displayed



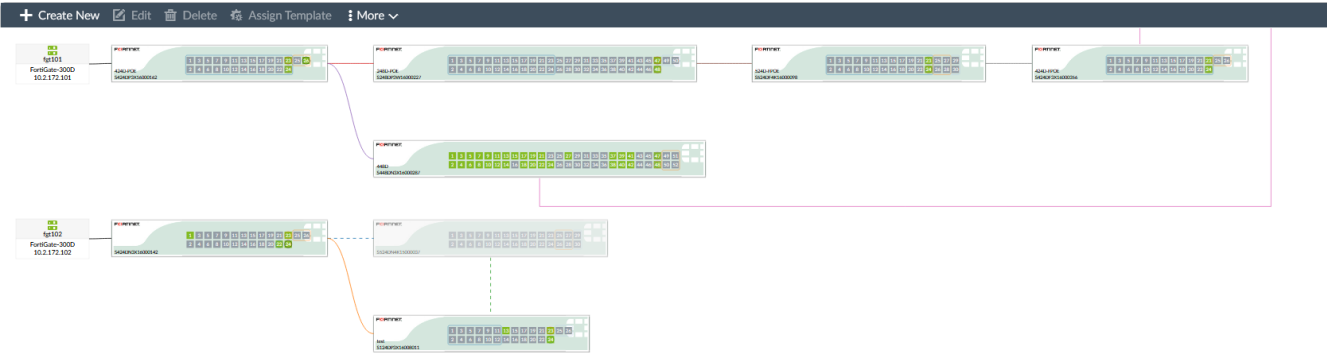
## Monitors

The *FortiSwitch Manager > Device & Groups* 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 > Device & Groups*. 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 > Device & Groups* 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.

<b>Link</b>	The state of the link, either <i>up</i> or <i>down</i> .
<b>Native VLAN</b>	The native VLAN of the port.
<b>Speed</b>	The speed of the port, such as <i>1000Mbps/Full Duplex</i> . The value is <i>0Mbps</i> if the link is down.
<b>Bytes Sent</b>	The total number of bytes sent by the port.
<b>Bytes Received</b>	The total number of bytes received by the port.

## FortiSwitch Templates for 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 682](#).
2. Create FortiSwitch VLANs. See [Creating FortiSwitch VLANs on page 688](#).
3. Create or import FortiSwitch templates. See [FortiSwitch Templates on page 683](#).
4. Assign templates to FortiSwitch devices. See [Assigning templates to FortiSwitch devices on page 699](#).
5. Install the templates to the devices. See [Installing changes to managed switches on page 676](#).

### 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 > All ADOMs*.
2. Double-click the ADOM to open it for editing.

3. Beside *Central Management*, select the *FortiSwitch* checkbox, and click *OK*.

**Edit ADOM**

Name: root

Type: FortiGate 6.4 7.0

Comments: 0/128

Devices

+ Select Device

Name	IP Address	Platform
Branch_Office_01		FortiGate-VM64
Branch_Office_02		FortiGate-VM64
EnterpriseCore		FortiGate-VM64
Enterprise_First_Floor		FortiGate-VM64

Mode: ☐ Normal ☐ Backup

Central Management: ☐ VPN ☒ FortiAP ☒ FortiSwitch

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

Perform Policy Check Before Every Install: OFF

Auto-Push Policy Packages When Device Back Online: ☐ Enable ☒ Disable

OK Cancel

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 119](#).

## 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*, and select *FortiSwitch Templates* in the tree menu.

+ Create New Edit Clone Delete Where Used Import Column Settings					
<input type="checkbox"/>	Name	Description	Platform	Last Modified	Created Time
<input type="checkbox"/>	124-poe		FortiSwitch-124D-POE	administrator/2021-03-16 09:54:17	2021-03-16 09:51:22
<input type="checkbox"/>	248-poe		FortiSwitch-248D-POE	administrator/2021-03-16 09:54:20	2021-03-16 09:51:38
<input type="checkbox"/>	switch-124D		FortiSwitch-124D	administrator/2021-03-16 09:54:22	2021-03-16 09:51:58

The following options are available in the toolbar and right-click menu:

<b>Create New</b>	Create a new FortiSwitch template. See <a href="#">Creating FortiSwitch templates on page 684</a> .
<b>Edit</b>	Edit the selected template.
<b>Clone</b>	Create a copy of an existing template.
<b>Delete</b>	Delete the selected template or templates.
<b>Where Used</b>	View where the selected template is used.
<b>Import</b>	Import a FortiSwitch template. See <a href="#">Importing FortiSwitch templates on page 687</a> .
<b>Column Settings</b>	Adjust the visible columns.
<b>Search</b>	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*, and select *FortiSwitch Templates* in the tree menu.
2. In the content pane, click *Create New* in the toolbar. The *Create New FortiSwitch Template* window opens.

Create New FortiSwitch Template

Template Name

Description

Platforms

Switch VLAN Assignments

Port	Description	Access Mode	Enabled Features	Native VLAN	Allowed VLAN	POE	DHCP Bl
<input type="checkbox"/> port1		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled	Untrust
<input type="checkbox"/> port2		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled	Untrust
<input type="checkbox"/> port3		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled	Untrust
<input type="checkbox"/> port4		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled	Untrust
<input type="checkbox"/> port5		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled	Untrust
<input type="checkbox"/> port6		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled	Untrust
<input type="checkbox"/> port7		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled	Untrust

3. Enter the following information, then click *OK* to create the new template.

<b>Template Name</b>	Type a name for the template.
<b>Description</b>	Optionally, enter a description.
<b>Platforms</b>	Select the platform that the template will apply to from the dropdown list.
<b>Switch VLAN Assignments</b>	<p>Configure VLAN assignments. A platform must be selected before VLAN assignments can be configured.</p> <p>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 <i>Native VLAN</i>, <i>Allowed VLAN</i>, <i>Security Policy</i>, <i>QoS Policy</i>, and <i>LLDP profiles</i> while multiple ports are selected.</p>
<b>Create</b>	Create a physical port or trunk group. See <a href="#">Creating ports and trunk groups on page 686</a> .
<b>Edit</b>	Edit the selected port or trunk.
<b>Delete</b>	Delete the selected ports or trunks.
<b>Column Settings</b>	Select which columns are visible or hidden in the Switch VLAN Assignments table.
<b>Custom Command Entry</b>	<p>Create a new custom command entry.</p> <p>Enter a name, and select a previously configured custom command. See <a href="#">Creating custom commands on page 697</a>.</p> <p>If a custom command has not yet been created, click the add icon in the <i>Custom Command</i> selection box to create one.</p>

## 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.	<b>Port Name</b>	Enter the name of the port.
	<b>Description</b>	Optionally, enter a description.
	<b>Access Mode</b>	Select the access mode from <i>dynamic</i> , <i>nac</i> , or <i>normal</i> .
	<b>Port Policy</b>	Select the dynamic port policy from the available port policy objects. See <a href="#">Creating FortiSwitch dynamic port policies on page 694</a> . This setting is only available when the access mode is dynamic.
	<b>Native VLAN</b>	Select the native VLAN from the available VLAN objects. See <a href="#">Creating FortiSwitch VLANs on page 688</a> . This setting is only available when the access mode is normal.
	<b>Allowed VLAN</b>	Select the allowed VLAN from the available VLAN objects. See <a href="#">Creating FortiSwitch VLANs on page 688</a> .
	<b>Security Policy</b>	Select the security policies from the available switch controller security policies. See <a href="#">FortiSwitch security policies on page 695</a> .
	<b>LLDP Profile</b>	Select an LLDP profile.
	<b>QoS Policy</b>	Select a QoS policy.
	<b>DHCP Blocking</b>	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.
	<b>Loop Guard</b>	Enable or disable Loop Guard for the port. Loop Guard cannot be applied to trunks, or ports that are in trunks.
	<b>STP</b>	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.
	<b>Edge Port</b>	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.
	<b>STP BPDU Guard</b>	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.
	<b>STP Root Guard</b>	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.



- 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.

<b>POE</b>	Right-click to enable or disable PoE for the port where applicable.
<b>IGMP Snooping</b>	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:

- On the *Create New FortiSwitch Template* pane, click **Create** in the *Switch VLAN Assignments* toolbar. The *Add VLAN Assignment* dialog box opens.
- Select *trunk* as the type.
- Enter a name for the trunk group in the *Trunk Name* field.
- In the *Members* field, select all the ports that will be in the group from the dropdown list.
- Select the mode: *lacp-active* (active link aggregation), *lacp-passive* (passive link aggregation), or *static*.
- 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:

- Go to *FortiSwitch Manager > FortiSwitch Templates*.
- In the tree menu, select *FortiSwitch Template*.
- In the content pane, click **Import** in the toolbar. The *Import* window opens.

- Select a FortiGate from the drop-down list.
- Select the FortiSwitch whose template will be imported from the drop-down list.
- (Optional) Enter a name for the template in the *New Name* field.
- 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 119](#).

## 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 on the Fortinet Document Library](#).
2. Authorize the FortiSwitch device on FortiGate, and add the FortiGate device to FortiManager. See [Add devices on page 51](#).
3. Import the FortiSwitch template using the *Import* feature in *FortiSwitch Manager > FortiSwitch Templates*. See [Importing FortiSwitch templates on page 687](#).
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 668](#).

+ Create Edit Delete Column Settings						
<input type="checkbox"/>	Port	Description	Access Mode	Enabled Features	Native VLAN	Allowed VLAN
<input type="checkbox"/>	port48		Normal	Edge Port Spanning Tree Protocol	default	quarantine
<input type="checkbox"/>	port49		Normal	Edge Port Spanning Tree Protocol	default	quarantine
<input type="checkbox"/>	port50		Normal	Edge Port Spanning Tree Protocol	default	quarantine
<input type="checkbox"/>	port51		Normal	Edge Port Spanning Tree Protocol	default	quarantine
<input type="checkbox"/>	port52		Normal	Edge Port Spanning Tree Protocol	default	quarantine
<input type="checkbox"/>	port53.1		Normal	Edge Port Spanning Tree Protocol	default	quarantine
<input type="checkbox"/>	port53.2		Normal	Edge Port Spanning Tree Protocol	default	quarantine
<input type="checkbox"/>	port53.3		Normal	Edge Port Spanning Tree Protocol	default	quarantine
<input type="checkbox"/>	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 706](#).

## Creating FortiSwitch VLANs

### To create a FortiSwitch VLAN:

1. Go to *FortiSwitch Manager > FortiSwitch Templates*.
2. In the tree menu, select *VLANs*.

3. In the content pane, click *Create New* in the toolbar. The *Create New VLAN Definition* window opens.

Create New VLAN Definition

Interface Name

VLAN ID

0

Role

DMZ LAN UNDEFINED WAN

Estimated Bandwidth

0 Kbps Upstream 0 Kbps Downstream

Address

Manual

0.0.0.0/0.0.0.0

IPv6 Addressing mode

Manual DHCP

IPv6 Address/Prefix

::/0

Restrict Access

Administrative Access

☐ CAPWAP
☐ DNP
☐ FGFM

☐ FTM
☐ HTTP
☐ HTTPS

☐ PING
☐ PROBE-RESPONSE
☐ RADIUS-ACCT

☐ SNMP
☐ SSH
☐ TELNET

IPv6 Administrative Access

☐ CAPWAP
☐ FGFM
☐ HTTP

☐ HTTPS
☐ PING
☐ SNMP

☐ SSH
☐ TELNET

DHCP Server

ON

Address Range

+ Create Edit Delete

Starting IP

End IP

No records found...

Netmask

0.0.0.0

Default Gateway

Same as Interface IP Specify 0.0.0.0

DNS Server

Same as System DNS Same as Interface IP Specify

Advanced...

Mode

Server Relay

NTP Server

Local Same as System NTP Specify 0.0.0.0

Time Zone

Disable Same as System Specify

Next Bootstrap Server

0.0.0.0

Additional DHCP Options

Lease Time

604800

+ Create Edit Delete

Option Code

Value

No records found...

MAC Reservation + Access Control

Unknown MAC Address Action

assign block

+ Create Edit Delete

MAC Address

Action or IP

Description

No records found...

Type

Regular IPsec

Networked Devices

Device Detection

OFF

Admission Control

Security Mode

CAPTIVE-PORTAL NONE

Authentication Portal

Local External example.com/captive

User Access

Restricted to Groups Allow all

Exempt Sources

+

Device

+

Exempt Destinations

+

Exempt Services

+

Miscellaneous

Scan Outgoing Connections to Botnet Sites

BLOCK DISABLE MONITOR

Secondary IP Address

ON

+ Create New Edit Delete

IP/Network Mask

Administrative Access

Status

Comments

0/255

Interface State

Enabled Disabled

Advanced Options

Per-Device Mapping

ON

+ Create New Edit Delete

Name

VDOM

Details

OK Cancel

FortiManager 7.2.3 Administration Guide  
Fortinet Inc.

689

4. Enter the following information, then click **OK** to add the new VLAN.

<b>Interface Name</b>	Enter a name for the interface.
<b>VLAN ID</b>	Enter the VLAN ID
<b>Role</b>	Select the role for the interface: <i>DMZ</i> , <i>LAN</i> , <i>UNDEFINED</i> , or <i>WAN</i> .
<b>Estimated Bandwidth</b>	Enter the estimated upstream and downstream bandwidths. This option is only available when <i>Role</i> is <i>WAN</i> .
<b>Address</b>	
<b>Addressing mode</b>	The addressing mode.
<b>IP/Network Mask</b>	Enter the IP address and netmask.
<b>IPv6 Addressing mode</b>	Select the IPv6 addressing mode: <i>Manual</i> or <i>DHCP</i> .
<b>IPv6 Address/Prefix</b>	Enter the IPv6 address. This option is only available when <i>IPv6 Addressing mode</i> is <i>Manual</i> .
<b>Restrict Access</b>	
<b>Administrative Access</b>	Select the allowed administrative service protocols from: <i>CAPWAP</i> , <i>DNP</i> , <i>FGFM</i> , <i>FTM</i> , <i>HTTP</i> , <i>HTTPS</i> , <i>PING</i> , <i>PROBE-RESPONSE</i> , <i>RADIUS-ACCT</i> , <i>SNMP</i> , <i>SSH</i> , and <i>TELNET</i> .
<b>IPv6 Administrative Access</b>	Select the allowed administrative service protocols from: <i>CAPWAP</i> , <i>FGFM</i> , <i>HTTP</i> , <i>HTTPS</i> , <i>PING</i> , <i>SNMP</i> , <i>SSH</i> , and <i>TELNET</i> .
<b>DHCP Server</b>	Turn the DHCP server on or off. This option is only available when <i>Role</i> is <i>LAN</i> or <i>UNDEFINED</i> .
<b>DHCP Server IP</b>	Enter the DHCP server IP address. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Relay</i> .
<b>Address Range</b>	Configure address ranges for DHCP. Click <i>Create</i> to create a new range. Ranges can also be edited and deleted as required. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i> .
<b>Netmask</b>	Enter the netmask. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i> .
<b>Default Gateway</b>	Configure the default gateway: <i>Same as Interface IP</i> , or <i>Specify</i> . If set to <i>Specify</i> , enter the gateway IP address in the field. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i> .

<b>DNS Server</b>	<p>Configure the DNS server: <i>Same as System DNS</i>, <i>Same as Interface IP</i>, or <i>Specify</i>.</p> <p>This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i>.</p>
<b>DNS Server 1 - 3</b>	<p>Enter the DNS server IP addresses.</p> <p>This option is only available when <i>DHCP Server</i> is <i>ON</i>, <i>Mode</i> is <i>Server</i>, and <i>DNS Server</i> is <i>Specify</i>.</p>
<b>Mode</b>	<p>Select the DHCP mode: <i>Server</i> or <i>Relay</i>.</p> <p>This option is only available when <i>DHCP Server</i> is <i>ON</i>.</p>
<b>NTP Server</b>	<p>Configure the NTP server: <i>Local</i>, <i>Same as System NTP</i>, or <i>Specify</i>. If set to <i>Specify</i>, enter the NTP server IP address in the field.</p> <p>This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i>.</p>
<b>Time Zone</b>	<p>Configure the timezone: <i>Disable</i>, <i>Same as System</i>, or <i>Specify</i>. If set to <i>Specify</i>, select the timezone from the dropdown list.</p> <p>This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i>.</p>
<b>Next Bootstrap Server</b>	<p>Enter the IP address of the next bootstrap server.</p> <p>This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i>.</p>
<b>Additional DHCP Options</b>	<p>In the <i>Lease Time</i> field, enter the lease time, in seconds. Default: 604800 seconds (7 days).</p> <p>Add DHCP options to the table. See <a href="#">To add additional DHCP options: on page 693</a> for details. Options can also be edited and deleted as required.</p> <p>This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i>.</p>
<b>MAC Reservation + Access Control</b>	<p>Select the action to take with unknown MAC addresses: <i>assign</i> or <i>block</i>.</p> <p>Add MAC address actions to the table. See <a href="#">To add a MAC address reservation: on page 693</a> for details. Reservations can also be edited and deleted as required.</p> <p>This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i>.</p>
<b>Type</b>	<p>Select the type: <i>Regular</i>, or <i>IPsec</i>.</p> <p>This option is only available when <i>DHCP Server</i> is <i>ON</i>.</p>
<b>Networked Devices</b>	<p>These options are only available when <i>Role</i> is <i>DMZ</i>, <i>LAN</i>, or <i>UNDEFINED</i>.</p>
<b>Device Detection</b>	<p>Turn device detection on or off.</p>
<b>Active Scanning</b>	<p>Turn active scanning on or off.</p>

	This option is only available when <i>Device Detection</i> is on.
<b>Admission Control</b>	These options are only available when <i>Role</i> is <i>LAN</i> or <i>UNDEFINED</i> .
<b>Security Mode</b>	Select the security mode: <i>CAPTIVE-PORTAL</i> , or <i>NONE</i> .
<b>Authentication Portal</b>	Configure the authentication portal: <i>Local</i> or <i>External</i> . If <i>External</i> is selected, enter the portal in the field. This option is only available when <i>Security Mode</i> is <i>CAPTIVE-PORTAL</i> .
<b>User Access</b>	Select <i>Restricted to Groups</i> or <i>Allow All</i> . This option is only available when <i>Security Mode</i> is <i>CAPTIVE-PORTAL</i> .
<b>User Groups</b>	Select user groups from the available groups. This option is available when <i>Security Mode</i> is <i>CAPTIVE-PORTAL</i> and <i>User Access</i> is <i>Restricted to Groups</i> .
<b>Exempt Sources</b>	Select sources that are exempt from the available firewall addresses. This option is only available when <i>Security Mode</i> is <i>CAPTIVE-PORTAL</i> .
<b>Device</b>	Select user devices, device categories, and/or device groups. This option is only available when <i>Security Mode</i> is <i>CAPTIVE-PORTAL</i> .
<b>Exempt Destinations</b>	Select destinations that are exempt from the available firewall addresses. This option is only available when <i>Security Mode</i> is <i>CAPTIVE-PORTAL</i> .
<b>Exempt Services</b>	Select services that are exempt from the available firewall services. This option is only available when <i>Security mode</i> is <i>CAPTIVE-PORTAL</i> .
<b>Miscellaneous</b>	
<b>Scan Outgoing Connections to Botnet Sites</b>	Select <i>Block</i> , <i>Disable</i> , or <i>Monitor</i> .
<b>Secondary IP Address</b>	Turn secondary IP addresses on or off. Add IP addresses to the table. See <a href="#">To add a secondary IP address: on page 693</a> for details. Addresses can also be edited and deleted as required.
<b>Status</b>	
<b>Comments</b>	Optionally, enter comments.
<b>Interface State</b>	Select if the interface is <i>Enabled</i> or <i>Disabled</i> .

**Advanced Options****color**

Change the color of the interface to one of the 32 options.

**Per-Device Mapping**

Enable per-device mapping.

Add mappings to the table. See [To add per device mapping: on page 694](#) for details. Mappings can also be edited and deleted as required.

**To add additional DHCP options:**

1. Click *Create* in the *Additional DHCP Options* table toolbar. The *Additional DHCP Options* dialog box opens.

2. Enter the *Option Code*.
3. Select the *Type*: *hex*, *ip*, or *string*.
4. Enter the corresponding value.
5. Click *OK* to create the option.

**To add a MAC address reservation:**

1. Click *Create* in the *MAC Reservation + Access Control* table toolbar. The *MAC Reservation + Access Control* dialog box opens.

2. Enter the *MAC Address*.
3. Select the *End IP*: *Assign IP*, *Block*, or *Reserve IP*. If reserving the IP address, enter it in the field.
4. Optionally, enter a description.
5. Click *OK* to create the reservation.

**To add a secondary IP address:**

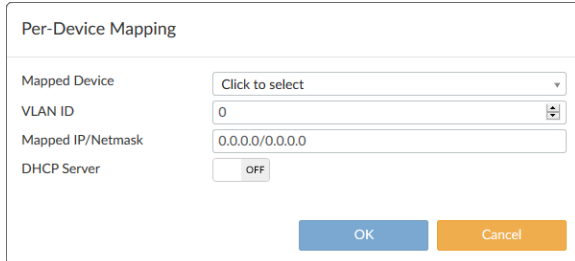
1. Click *Create New* in the *Secondary IP address* table toolbar. A dialog box opens.
2. Enter the IP address and netmask in the *IP/Network Mask* field.
3. Select the allowed administrative service protocols from: *CAPWAP*, *DNP*, *FGFM*, *FTM*, *HTTP*, *HTTPS*, *PING*,

*PROBE-RESPONSE, RADIUS-ACCT, SNMP, SSH, and TELNET.*

- Click **OK** to add the address.

### To add per device mapping:

- Click **Create New** in the *Per-Device Mapping* table toolbar. The *Per-Device Mapping* dialog box opens.



The *Per-Device Mapping* dialog box contains the following fields:

- Mapped Device:** A drop-down menu with the text "Click to select".
- VLAN ID:** A text input field containing the value "0".
- Mapped IP/Netmask:** A text input field containing the value "0.0.0.0/0.0.0.0".
- DHCP Server:** A toggle switch currently set to "OFF".

At the bottom right, there are two buttons: **OK** (blue) and **Cancel** (orange).

- Select the device to be mapped from the *Mapped Device* drop-down list.
- Enter the VLAN ID.
- Enter the mapped IP address and netmask in the *Mapped IP/Netmask* field.
- If required, enable *DHCP Server* and configure the options (options are the same as when creating a new VLAN definition).
- Click **OK** to add the device mapping.

## Creating FortiSwitch dynamic port policies

### To create a FortiSwitch dynamic port policy:

- Go to *FortiSwitch Manager > FortiSwitch Templates*.
- In the tree menu, select *Dynamic Port Policy*.
- Click **Create New**. The *Create New Dynamic Port Policy* pane opens.
- Enter a name for the dynamic port policy.
- In the *Policy Information* section, click **Create New**. The *Create New Dynamic Port Policy Rule* pane opens.
- Enter the following information, and click **OK** to save the dynamic port policy rule.

<b>Name</b>	Enter a unique name for the dynamic port policy rule.
<b>Status</b>	Set the rule to Enabled or Disabled.
<b>Description</b>	Optionally, enter a description for the rule.
<b>Device Patterns</b>	
<b>MAC Address</b>	Enable or disable matching a MAC address, then enter a MAC address.
<b>Host</b>	Enable or disable matching a host address, then enter a host address.
<b>Hardware Vendor</b>	Enable or disable matching a hardware vendor, then enter a hardware vendor name.
<b>Device Family</b>	Enable or disable matching a device family, then enter a device family name.
<b>Type</b>	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.

- 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 684](#).

## FortiSwitch security policies

### To view FortiSwitch security policies:

- Ensure that you are in the correct ADOM.
- Go to *FortiSwitch Manager > FortiSwitch Templates*.
- In the tree menu, select *Security Policies*.



FortiSwitch Security Policies are not available in version 5.4 ADOMs.

+ Create New Edit Clone Delete Where Used Import Column Settings					
<input type="checkbox"/>	Name	User Groups	Last Modified	Created Time	
<input type="checkbox"/>	802-1X-policy-default	SSO_Guest_Users	administrator/2021-03-16 13:00:57	2021-03-01 07:57:47	
<input type="checkbox"/>	Policy01	Guest-group	administrator/2021-03-16 13:02:09	2021-03-16 13:02:09	
<input type="checkbox"/>	Policy02	SSO_Guest_Users	administrator/2021-03-16 13:02:18	2021-03-16 13:02:18	

The following options are available in the toolbar and right-click menu:

<b>Create New</b>	Create a new FortiSwitch security policy. See <a href="#">Creating FortiSwitch security policies on page 696</a> .
<b>Edit</b>	Edit the selected policy.
<b>Clone</b>	Create a copy of the selected security policy.
<b>Delete</b>	Delete the selected policy or policies.
<b>Where Used</b>	See where the security policy is being used.
<b>Import</b>	Import security policies from a managed FortiGate device.
<b>Column Settings</b>	Select which columns are hidden or displayed in the security policy table.
<b>Search</b>	Enter a search string into the search field to search the policy list.

### To edit a security policy:

- 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.
- 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.

**Creating FortiSwitch security policies****To create a FortiSwitch security policy:**

1. Go to *FortiSwitch Manager > FortiSwitch Templates*.
2. In the tree menu, select *Security Policies*.
3. In the content pane, click *Create New* in the toolbar. The *Create New Security Policies* window opens.

Create New Security Policies

Name	<input type="text"/>
Security mode	<input checked="" type="radio"/> Port-based <input type="radio"/> MAC-based
User groups	<input type="text" value="Click here to select"/>
Guest VLAN	<input type="button" value="OFF"/>
Guest authentication delay second(s)	<input type="text" value="30"/>
Authentication fail VLAN	<input type="button" value="OFF"/>
MAC authentication bypass	<input type="button" value="OFF"/>
EAP pass-through	<input checked="" type="button" value="ON"/>
Override RADIUS timeout	<input type="button" value="OFF"/>

OK

Cancel

4. Enter the following information, then click *OK* to create the new security policy.

<b>Name</b>	Type a name for the template.
<b>Security mode</b>	Select the security mode, <i>Port-based</i> or <i>MAC-based</i> .
<b>User groups</b>	Select the user groups that the security policy will apply to.
<b>Guest VLAN</b>	Enable a guest VLAN, and select the VLAN from the available VLAN objects. See <a href="#">Creating FortiSwitch VLANs on page 688</a> .
<b>Guest authentication delay second(s)</b>	Set the guest authentication delay, in seconds (1 - 900, default = 30).
<b>Authentication fail VLAN</b>	Enable an authentication failure VLAN, and select the VLAN from the available VLAN objects. See <a href="#">Creating FortiSwitch VLANs on page 688</a> .

This option is not available when *Security mode* is *MAC-based*.

<b>MAC authentication bypass</b>	Enable MAC Authentication Bypass (MAB).
<b>EAP pass-through</b>	Enable EAP pass-through.
<b>Override RADIUS timeout</b>	Enable overriding the RADIUS timeout.

## Creating 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 > FortiSwitch Templates*.
2. In the tree menu, select *Custom Command*.
3. In the content pane, click *Create New* in the toolbar. The *Create New Custom Command* window opens. Below is an example custom command.

Create New Custom Command

Name: script-stp-age-10

Description:

Command: config switch stp setting  
set max-age 10  
end

44/4095

OK Cancel

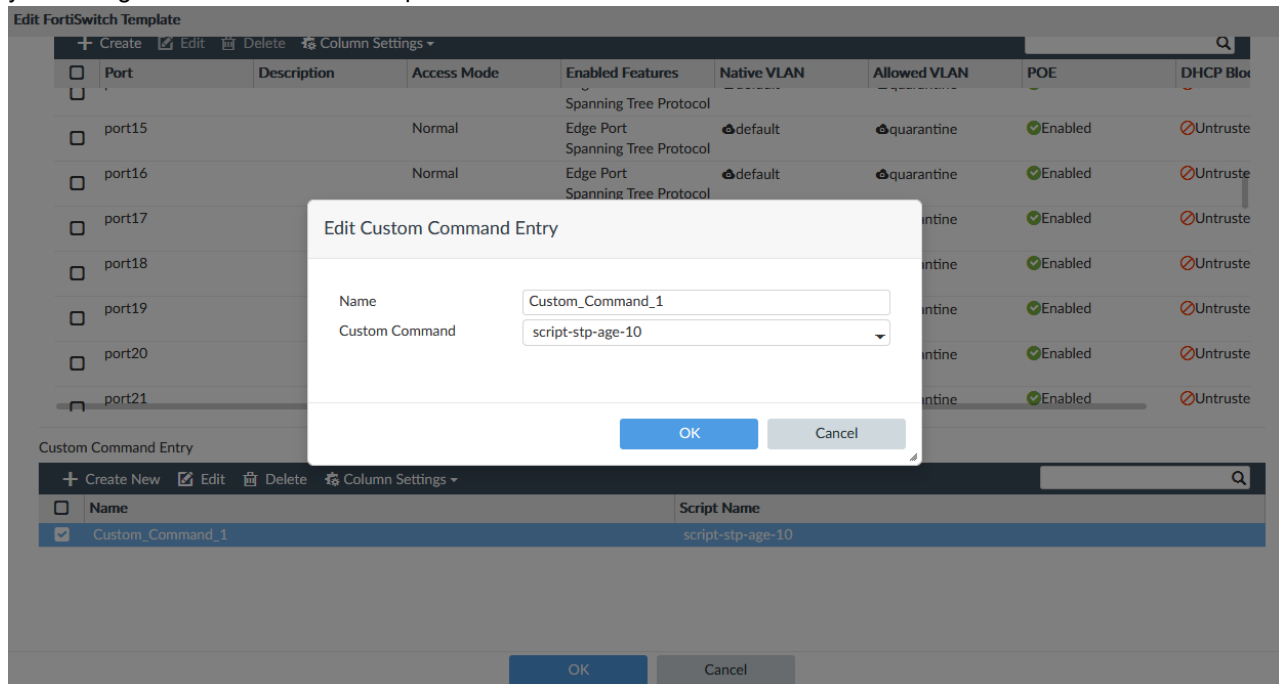
4. Enter the following information, then click *OK* to create the new custom command.

<b>Name</b>	Type a name for the custom command template.
<b>Description</b>	Optionally, type a description.
<b>Command</b>	Enter the CLI commands.

You can now add the custom command to a FortiSwitch template.

5. Go to *FortiSwitch Manager > FortiSwitch Templates > FortiSwitch Template*, and edit an existing template or create a new one.
6. In the *Custom Command Entry* table, click *Create New*. The *Create New Custom Command Entry* dialog appears.

7. Enter a name for the command entry and select your previously configured custom command. Click **OK**, and save your changes to the FortiSwitch template.

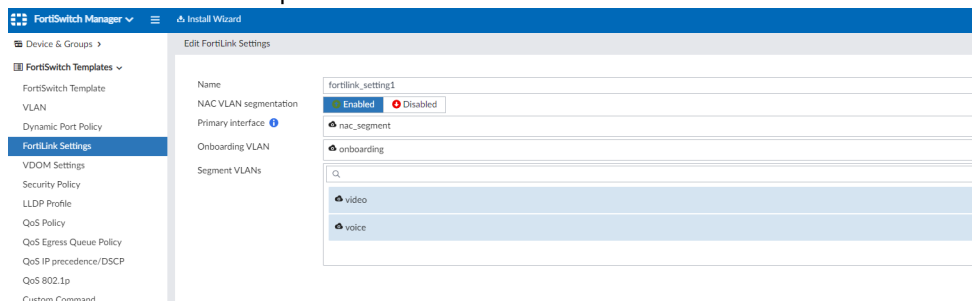


You can now install the custom command using the Install Wizard. See [Installing changes to managed switches on page 676](#).

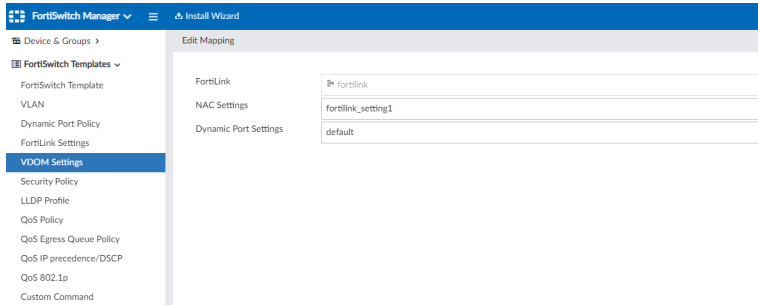
## Configuring a FortiLink settings template

To create a new FortiLink Setting template:

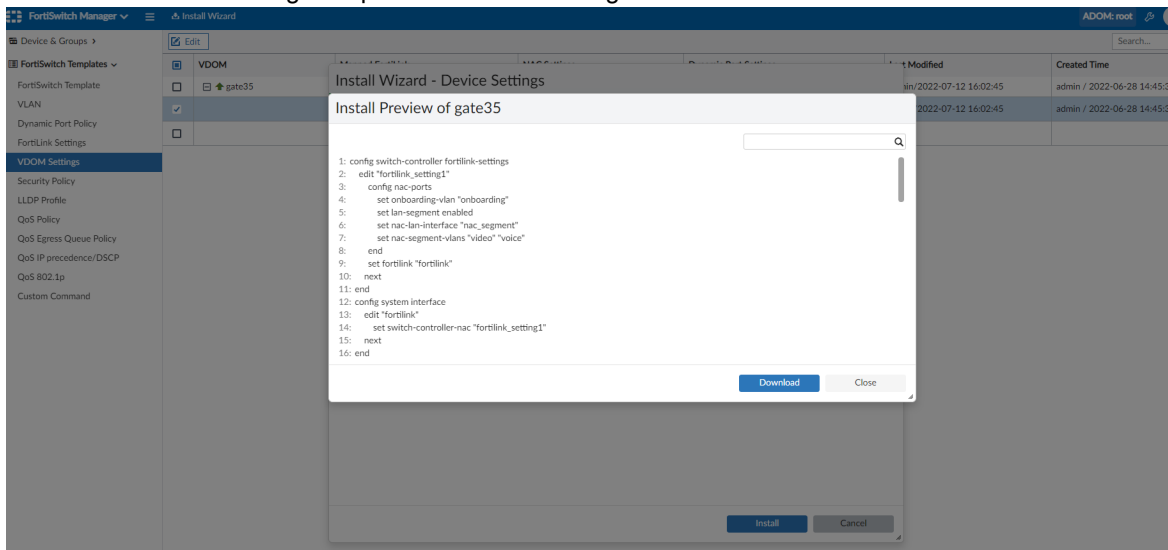
1. Go to *FortiSwitch Manager > FortiSwitch Templates > FortiLink Settings*, and click *Create New*.
2. Configure the details of the FortiLink Settings template including the *Name*, *NAC VLAN Segmentation*, *Primary Interface*, *Onboarding VLAN*, and *Segment VLANs*.
3. Click **OK** to save the template.



4. Go to *FortiSwitch Manager > FortiSwitch Templates > 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 683](#).

### To assign a templates:

1. Go to *FortiSwitch Manager > Device & Groups > Managed Switches*.
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 676](#).



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 670](#).

## FortiSwitch Profiles for 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 700](#).
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. See [FortiSwitch profiles on page 701](#).  
NAC policies can be created in both per-device management and central management. See [Create a new NAC policy on page 393](#).
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 706](#).
4. Install changes to managed switches. See [Installing changes to managed switches on page 676](#).

## 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 > All ADOMs*.
2. Double-click the ADOM to open it for editing.
3. Beside *Central Management*, clear the *FortiSwitch* checkbox, and click *OK*.  
Central management is disabled, and per-device management is enabled for FortiSwitch.

4.

Device & Groups

Search...

Managed FortiGate (3)

- Branch\_Office\_01 (1)
- Branch\_Office\_02 (1)
- Enterprise\_First\_Floor
- Enterprise\_Second\_Floor (1)

Managed Switches

FortiSwitch Profiles

CLI Configurations

Status

Platform

1 Total

Online (1)

FortiSwitch-108D-VM (1)

Create New

Edit

Delete

Authorize

Deauthorize

Upgrade

Show Charts

List

Search...

	FortiSwitch Name	Serial Number	Platform	Status	FortiLink	FortiGate	Connecting From	OS Version
<input type="checkbox"/>	S108DVCHTPDQH94	S108DVCHTPDQH94	FortiSwitch-108D-V	Online	port6	Branch_Office_01[root]	169.254.2.2	S108DV-v7.0.0-build4062.210

## FortiSwitch profiles

The *FortiSwitch Manager > Device & Groups > FortiSwitch Profiles* tab is available when per-device management is enabled for FortiSwitch Manager. You can use the *FortiSwitch Profiles* tab to create and manage VLANs, security policies, LLDP profiles, QoS profiles, and custom commands that you can assign to individual switches.

### Creating VLANs

#### To create VLANs:

1. Go to *FortiSwitch Manager > Device & Groups*, and select *VLAN* from the *FortiSwitch Profiles* 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 security policies

#### To create security policies:

1. Go to *FortiSwitch Manager > Device & Groups*, and select *Security Policy* from the *FortiSwitch Profiles* tab.
  2. In the tree menu, select a FortiGate.
- The security policies are displayed.

Managed Switches FortiSwitch Profiles : Security Policy CLI Configurations			
+ Create New Edit Delete Where Used Column Settings			
<input type="checkbox"/> Name	User Groups	Last Modified	Created Time
<input type="checkbox"/> 802-1X-policy-default	SSO_Guest_Users	administrator/2021-04-16 10:49:51	2021-04-14 09:40:45
<input type="checkbox"/> Policy_01	Guest-group	administrator/2021-04-16 10:49:51	2021-04-16 10:49:51
<input type="checkbox"/> Policy_02	Guest-group	administrator/2021-04-16 10:50:02	2021-04-16 10:50:02

- 3.
  4. Click *Create New*.
- The *Create New Security Policies* pane opens.
5. 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 > Device & Groups*, and select *LLDP Profile* from the *FortiSwitch Profiles* tab.
  2. In the tree menu, select a FortiGate.
- The *VLAN* profiles are displayed.

Managed Switches FortiSwitch Profiles : LLDP Profile CLI Configurations		
+ Create New Edit Delete Where Used Column Settings		
<input type="checkbox"/> Name	Last Modified	Created Time
<input type="checkbox"/> default	administrator/2021-04-16 10:53:24	2021-04-14 09:40:45
<input type="checkbox"/> default-auto-isl	administrator/2021-04-16 10:53:24	2021-04-14 09:40:45
<input type="checkbox"/> default-auto-mclag-isl	administrator/2021-04-16 10:53:24	2021-04-14 09:40:45
<input type="checkbox"/> fortivoice.port6	administrator/2021-04-16 10:53:24	2021-04-14 09:40:45

- 3.
  4. Click *Create New*.
- The *Create New FortiSwitch LLDP Profiles* pane opens.

Managed Switches FortiSwitch Profiles : LLDP Profile CLI Configurations

Create New FortiSwitch LLDP Profiles

Name

Transmitted LLDP-MED TLVs ☐ inventory-management ☐ location-identification  
☐ network-policy ☐ power-management

Transmitted IEEE 802.1 TLVs ☐ port-vlan-id

Transmitted IEEE 802.3 TLVs ☐ max-frame-size ☐ power-negotiation

Auto inter-switch LAG ☒

Auto isl hello timer duration

Auto isl port group ID

Auto isl receive timeout

Custom TLV Entry

+	Create New	✎ Edit	✖ Delete	Column Settings	Search
<input type="checkbox"/>	Name	OUI (3 hex bytes)	OUI Subtype	Information String	
No record found.					

Create & Refresh OK Cancel

5. 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 > Device & Groups*, and select *QoS Policy* from the *FortiSwitch Profiles* tab.
2. In the tree menu, select a FortiGate.  
The QoS policies are displayed in the content pane.
3. Click *Create New*.  
The *Create New QoS Policy* pane opens.

Create New QoS Policy

Name

Default COS Queue

Queue policy

Trust 802.1p map

Trust IP DSCP map

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 > Device & Groups*, and select *QoS Egress Queue Policy* from the *FortiSwitch Profiles* 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.

Create New QoS Egress Queue Policy

Name

Schedule

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 > Device & Groups*, and select *QoS IP precedence/DSCP* from the *FortiSwitch Profiles* 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.

Create New QoS IP precedence/DSCP

Name

Description

Maps between IP-DSCP value to COS Queue

+ Create New Edit Delete Column Settings					
<input type="checkbox"/>	Name	COS Queue Number	Differentiated Service	IP Precedence	Raw Values of DSC
No record found.					

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 > Device & Groups*, and select *QoS 802.1p* from the *FortiSwitch Profiles* 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.

## Create New QoS 802.1p

Name	<input type="text"/>
Description	<div><div></div><div>0/63</div></div>
COS queue mapped to dot1p priority number	
Priority-0	<div>queue-0</div>
Priority-1	<div>queue-0</div>
Priority-2	<div>queue-0</div>
Priority-3	<div>queue-0</div>
Priority-4	<div>queue-0</div>
Priority-5	<div>queue-0</div>
Priority-6	<div>queue-0</div>
Priority-7	<div>queue-0</div>

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 *FortiSwitch Profiles* tab. Once created, the custom command can be added to a managed FortiSwitch by editing the device in *Managed Switches* and selecting the custom command in the *Custom Command Entry* table. Once selected, use the Install Wizard to deploy the changes to FortiGate.

### To create a custom command:

1. Go to *FortiSwitch Manager > Device & Groups*. Select the *FortiSwitch Profile* tab and click *Custom Command* from the dropdown menu.
2. In the content pane, click *Create New* in the toolbar. The *Create New Custom Command* window opens.

## Create New Custom Command

Name	<input type="text" value="script-stp-age-10"/>
Description	<div><div></div><div>0/35</div></div>
Command	<div><div>config switch stp setting set max-age 10 end</div><div>44/4095</div></div>

OK

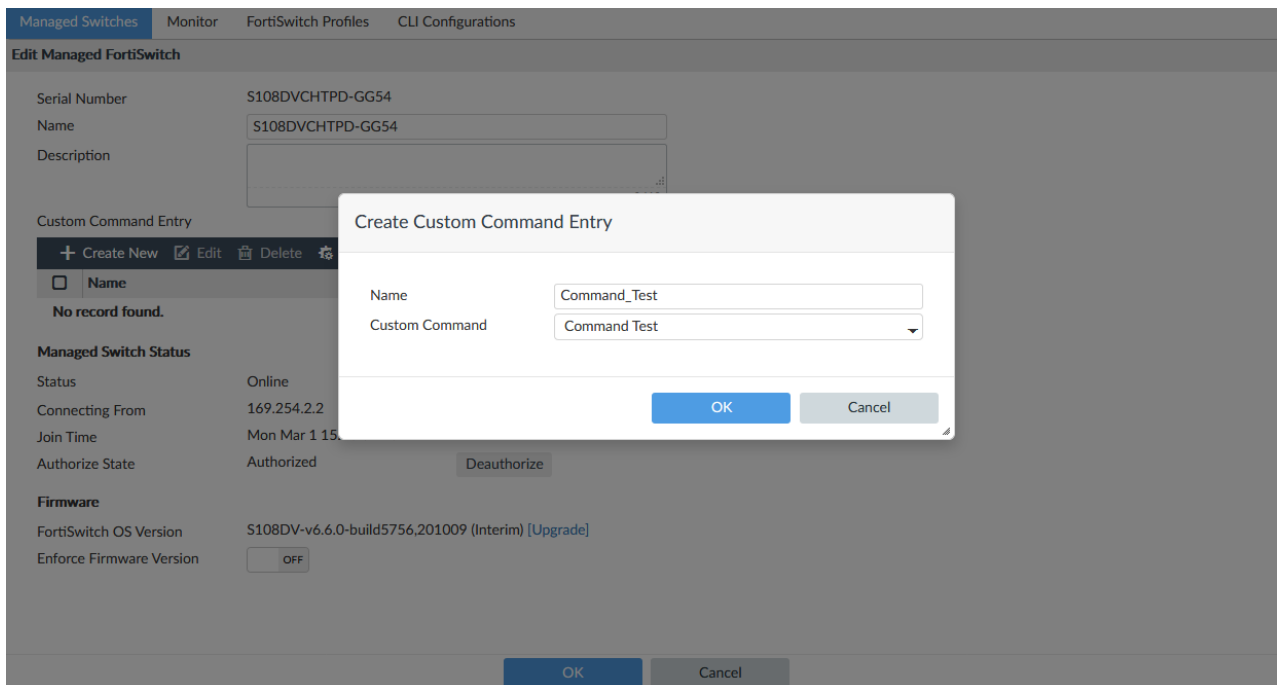
Cancel

- Enter the following information, then click *OK* to create the new custom command.

<b>Name</b>	Type a name for the custom command template.
<b>Description</b>	Optionally, type a description.
<b>Command</b>	Enter the CLI commands.

You can now add the custom command to a managed FortiSwitch device. See [Editing switches on page 670](#).

- Go to *FortiSwitch Manager > Device & Groups* and select a FortiGate, then edit a managed FortiSwitch.
- In the *Edit Managed FortiSwitch* pane, select *Create New* under *Custom Command Entry*.
- 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 676](#).

## 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:

- Go to *FortiSwitch Manager > Device & Groups*, and select the *CLI Configurations* tab.
- In the tree menu, select a FortiGate.  
The commands are displayed in the content pane.
- Use the tree menu to navigate between the commands.  
The options display in the content pane.

Managed Switches FortiSwitch Profiles CLI Configurations

switch-controller 802-1X-settings

link-down-auth: set-unauth (0 - 15, default: 3)

max-reauth-attempt: 3 (0 - 1440, default: 60)

reauth-period: 60 (4 - 60, default: 30)

tx-period: 30

Apply

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 > Device & Groups > Managed Switches*.
2. In the tree menu, select a FortiGate.  
The list of managed switches is displayed in the content pane.
3. Double-click a switch.  
The *FortiSwitch Ports* pane opens.

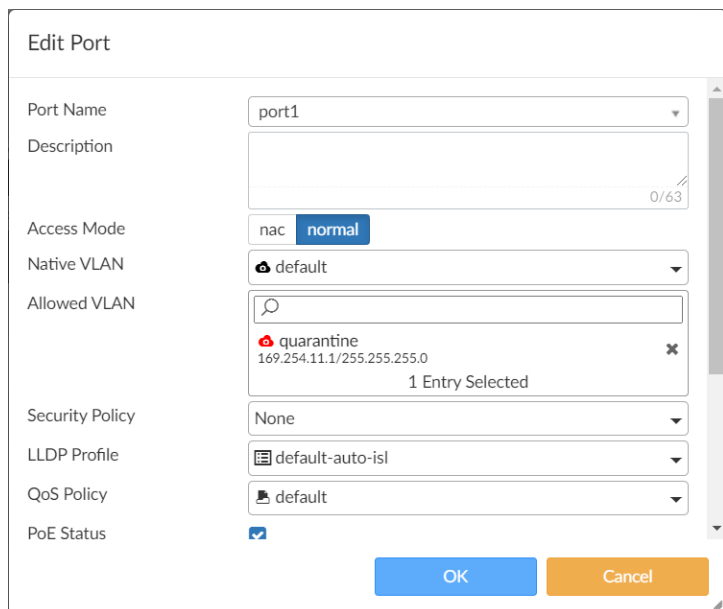
FortiSwitch Ports

MGMT PoE+ SFP

S248DF3X17000116

Port	Description	Access Mode	Enabled Features	Native VLAN	Allowed VLAN	POE	Device Information	DHCP
port1		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		Disabled
port2		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		Disabled
port3		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		Disabled
port4		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		Disabled
port5		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		Disabled
port6		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		Disabled
port7		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		Disabled
port8		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		Disabled
port9		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		Disabled

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.

# Extender Manager

The *Extender Manager* module allows you to managed connected FortiExtender. You can use the Extender Manager to create custom templates, SIM profiles, and data plans for up to two modems.

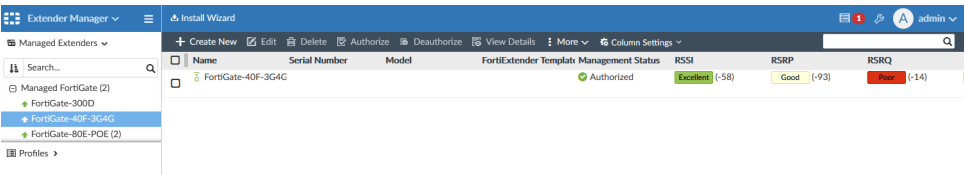
This section contains the following topics:

- [Managed extenders on page 708](#)
- [FortiExtender profiles on page 711](#)

## 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:

<b>Name</b>	The name of the FortiGate device that is managing the FortiExtender.
<b>Serial Number</b>	The serial number of the FortiExtender.
<b>Model</b>	The FortiExtender model.
<b>FortiExtender Template</b>	The FortiExtender template name.
<b>Management Status</b>	The FortiExtender management status, either <i>Authorized</i> or <i>Deauthorized</i> .
<b>RSSI</b>	The Received Signal Strength Indicator status, either <i>Excellent</i> , <i>Good</i> , or <i>Poor</i> .
<b>RSRP</b>	The Reference Signal Received Power status, either <i>Excellent</i> , <i>Good</i> , or <i>Poor</i> .
<b>RSRQ</b>	The Reference Signal Received Quality status, either <i>Excellent</i> , <i>Good</i> , or <i>Poor</i> .
<b>SINR</b>	The Signal-to-Interference-plus-Noise Ratio status, either <i>Excellent</i> , <i>Good</i> , or <i>Poor</i> .
<b>Network</b>	The FortiExtender network status and carrier name.

<b>Data Usage</b>	The current data usage.
<b>ENSI IMEI</b>	The FortiExtender electronic serial number (ESN) and international mobile equipment identity (IMEI).
<b>Phone Number</b>	The FortiExtender phone number.
<b>IMSI</b>	The FortiExtender international mobile subscriber identity (IMSI) number.
<b>ICCID</b>	The FortiExtender integrated circuit card identity (ICCID) number.
<b>Temperature</b>	The temperature information of FortiExtender. If temperature value is not available the value in the column will be empty.
<b>Version</b>	The FortiExtender firmware version.
<b>IP</b>	The FortiExtender IP address.

The right-click menu and toolbar options include:

<b>Refresh</b>	Select a FortiExtender in the list, right-click, and select <i>Refresh</i> in the menu to refresh the information displayed.
<b>Edit</b>	Select a FortiExtender in the list, right-click, and select <i>Edit</i> in the menu to edit the FortiExtender modem settings, PPP authentication, general, GSM/LTE, and CDMA settings.
<b>View Details</b>	Select a FortiExtender in the list, right-click, and select <i>View Details</i> in the menu to view the system status, modem status, and data usage.
<b>Upgrade</b>	Select a FortiExtender in the list, right-click, and select <i>Upgrade</i> in the menu to upgrade the FortiExtender firmware.
<b>Authorize</b>	Select a FortiExtender in the list, right-click, and select <i>Authorize</i> in the menu to authorize the unit for management.
<b>Deauthorize</b>	Select a FortiExtender in the list, right-click, and select <i>Deauthorize</i> in the menu to deauthorize the unit for management.
<b>Restart</b>	Select a FortiExtender in the list, right-click, and select <i>Restart</i> in the menu to restart the unit.
<b>Export to Excel</b>	Click to export the configuration as an Excel file.
<b>Export to CSV</b>	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*.
2. In the toolbar, click *Create New*. The *Create New Model FortiExtender* dialog is displayed.
3. Configure the model device.

<b>FortiGate</b>	Click the dropdown and select a device from the list.
<b>Serial Number</b>	Enter the serial number for the FortiExtender.
<b>Name</b>	Enter the device name.
<b>FortiExtender Template</b>	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*.
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*.
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*.
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*.
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*.

## FortiExtender 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 templates on page 711](#)
- [SIM Profiles on page 713](#)
- [Data plans on page 715](#)

## FortiExtender templates

You can create custom FortiExtender templates, assign a template to a device, and view where a template is used.

**To create a FortiExtender template:**

1. Go to *FortiExtender*.
2. In the tree menu, click *Profiles > FortiExtender Templates*.
3. In the toolbar click *Create New*. The *Create New FortiExtender Template* page opens.

## 4. Configure the template settings.

<b>Name</b>	Enter a name for the template.	
<b>Description</b>	(Optional) Enter a description of the template.	
<b>Modem (1 &amp; 2)</b>	<b>Normalized Interface</b>	Select an interface from the dropdown list.
	<b>SIM Profile</b>	Select a profile from the dropdown list, or click <i>Add</i> to create new profile.
<b>Dataplan</b>	Select a dataplan from the list, or click <i>Add</i> to create new dataplan, and click <i>OK</i> .	

5. Click *OK*.**To edit a FortiExtender template:**

1. In the tree menu, click *Profiles > FortiExtender Templates*.
2. Select a template, and do one of the following:
  - Double-click the template to open it.
  - In the toolbar, click *Edit*.
  - Right-click the template, and select *Edit* from the menu.

The *Edit FortiExtender Template* window opens.

3. Edit the template details, and click *OK*.**To clone a FortiExtender template:**

1. In the tree menu, click *Profiles > FortiExtender Templates* and select a template.
2. In the toolbar, click *Clone*, or right-click the template and select *Clone* from the menu. The *Clone FortiExtender Template* window opens.
3. Edit the template *Name* and settings as required.
4. Click *OK*.

**To assign a FortiExtender template to a device:**

1. In the tree menu, click *Profiles > FortiExtender Templates* and select a template.
2. In the toolbar, click *Assign to Device*, or right-click the template and select *Assign to Device* from the menu. The *Assign to Device* window opens.
3. Click the *FortiExtenders* field, and select a device(s) from the list.
4. Click *OK*.
5. Click *OK*.

**To view where a FortiExtender template is used:**

1. In the tree menu, click *Profiles > FortiExtender Templates* and select a template.
2. In the toolbar, click *Where Used*, or right-click the template and select *Where Used* from the menu. The *Where <template\_name> is used* window opens.
3. (Optional) Click *Edit* to edit the device.
4. (Optional) Click *View*, to view the device.
5. Click *Close*.

**To import a FortiExtender template:**

1. In the tree menu, click *Profiles > FortiExtender Templates*.
2. In the toolbar, click *Import*. The *Import FortiExtender Template* window opens.
3. Configure the template settings.

<b>FortiExtender</b>	Select a device from the dropdown list.
<b>Template Name</b>	Enter a name for the template.
<b>Interface Mapping Type</b>	Select <i>Per-Device</i> or <i>Per-Platform</i> .

4. Click *OK*.

**To delete a FortiExtender template:**

1. In the tree menu, click *Profiles > FortiExtender Templates* and select a template.
2. In the toolbar click *Delete*, or right-click the template and select *Delete* from the menu. The *Confirm Delete* window opens.
3. Click *OK*.

## SIM Profiles

The *SIM Profile* pane allows you to create and import SIM profiles. You can also view where a profile is used.

**To create a SIM profile:**

1. Go to *Extender Manager*.
2. In the tree-menu, click *Profiles > SIM Profile*. The *SIM Profile* pane opens.
3. In the toolbar, click *Create New*. The *Create New SIM Profile* window opens.
4. Enter a name for the profile.

5. For the Default SIM settings, select either *SIM1*, *SIM2*, *Carrier*, or *Lowest Cost*.

**Create New SIM Profile**

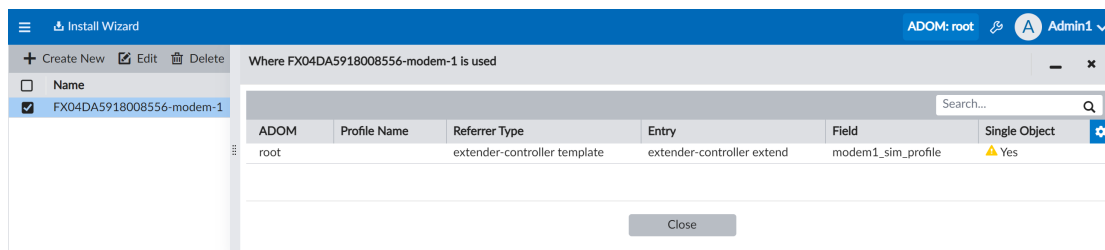
Name	<input style="width: 90%;" type="text"/>
Description	<div style="border: 1px solid #ccc; height: 60px; width: 90%;"></div> <div style="text-align: right; font-size: small;">0/4096</div>
Default SIM	<div style="display: flex; gap: 5px;"> <div style="background-color: #007bff; color: white; padding: 2px 10px; border: 1px solid #007bff;">SIM1</div> <div style="padding: 2px 10px; border: 1px solid #ccc;">SIM2</div> <div style="padding: 2px 10px; border: 1px solid #ccc;">Carrier</div> <div style="padding: 2px 10px; border: 1px solid #ccc;">Lowest Cost</div> </div>
SIM1 PIN	<input type="checkbox"/> OFF
SIM2 PIN	<input type="checkbox"/> OFF
GPS	<input checked="" type="checkbox"/> ON
Auto SIM switch	<input checked="" type="checkbox"/> ON
By disconnecting	<input type="checkbox"/> OFF
By signal	<input type="checkbox"/> OFF
By data plan	<input type="checkbox"/> OFF
Switch back	<input type="checkbox"/> Time <input type="checkbox"/> Timer
<b>Advanced Options</b> <span style="float: right;">▼</span>	
conn-status	<input style="width: 90%;" type="text" value="0"/>
modem-id	<input style="width: 90%;" type="text" value="0"/>
redundant-intf	<input style="width: 90%;" type="text"/>
redundant-mode	<input type="checkbox"/> OFF
status	<input checked="" type="checkbox"/> ON

6. Configure the other settings as required, and click **OK**.

To install the SIM profile on a device, click *Install Wizard*.

**To view where a profile is used:**

1. Go to *Extender Manager*.
2. In the tree menu, click *Profiles > SIM 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 displays.



4. Click *Close*.

### To delete a SIM profile:

1. Go to *Extender Manager*.
2. In the tree menu, click *Profiles > SIM profile*.
3. In the toolbar, click *Delete*, or right-click the profile and select *Delete* from the menu. The *Confirm Deletion* dialog is displayed.
4. Click *OK*.



You cannot delete a SIM profile that is in use.

## 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*.
2. In the tree menu, click *Profiles > Data Plan*. The *Data Plan* pane opens.
3. In the toolbar, click *Create New*. The *Create New Data Plan* dialog is displayed.
4. Enter a name and ensure the *Status* is enabled.
5. 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*).

6. Click **OK**.

To install the data plan on a device, click *Install Wizard*.

**To assign a plan to a device:**

**To view where a data plan is used:**

1. Go to *Extender Manager*.
2. In the tree menu, click *Profiles > Data Plan*. The *Data Plan* pane opens.
3. Select a data plan in the list, and click *Where Used*. The *Where <data\_plan\_name> is used* window displays.

ADOM	Profile Name	Referrer Type	Entry	Field	Single Object
root	extender-controller template	extender-controller extend	dataplan	Yes	

4. Click *Close*.

**To clone a data plan:**

1. Go to *Extender Manager*.
2. In the tree menu, click *Profiles > Data Plan*. The *Data Plan* pane opens.
3. In the toolbar, click *Clone*, or right-click a profile and select *Clone* from the menu. The *Clone Data Plan* window opens.
4. Edit the Data Plan name and other settings as required.
5. Click **OK**.

**To delete a data plan:**

1. Go to *Extender Manager*.
2. In the tree menu, click *Profiles > Data Plan*. The *Data Plan* pane opens.
3. In the toolbar, click *Delete*, or right-click a profile and select *Delete* from the menu. The *Confirm Deletion* dialog is

displayed.

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.

---

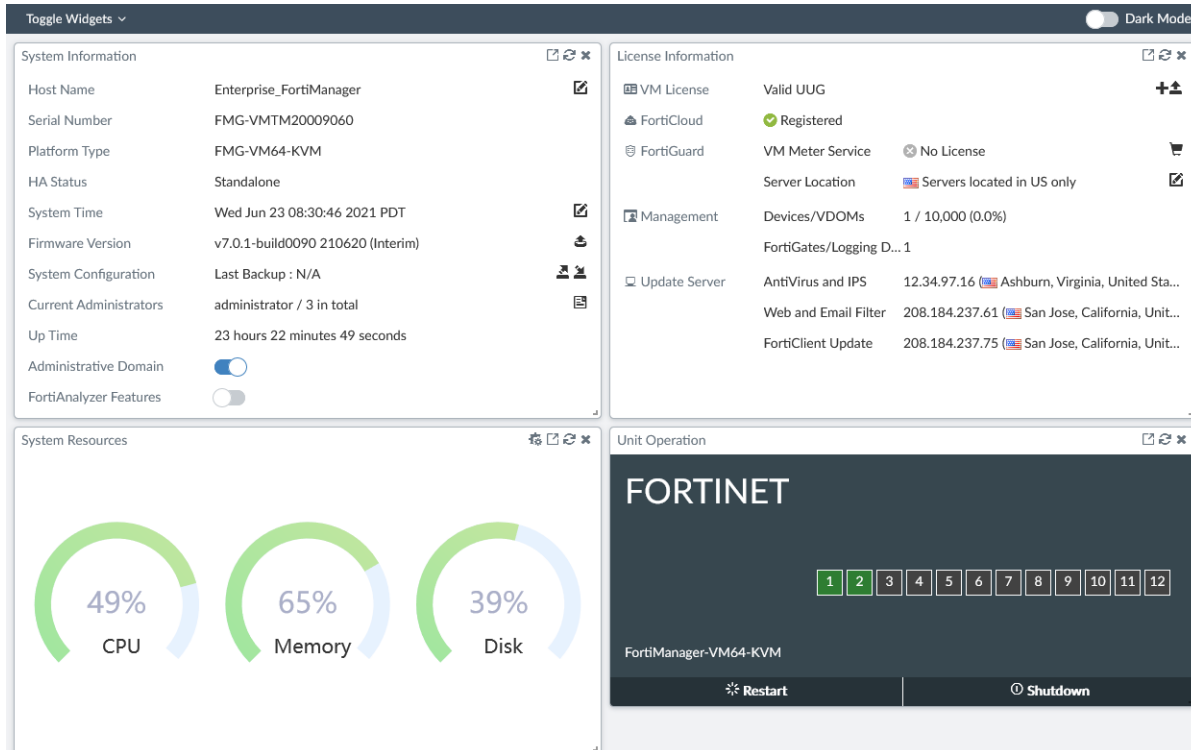
This section contains the following topics:

- [Dashboard on page 719](#)
- [Logging Topology on page 737](#)
- [Network on page 738](#)
- [RAID Management on page 744](#)
- [Administrative Domains \(ADOMs\) on page 750](#)
- [Certificates on page 777](#)
- [Event Log on page 782](#)
- [Task Monitor on page 785](#)
- [SNMP on page 786](#)
- [Mail Server on page 795](#)
- [Syslog Server on page 797](#)
- [Meta Fields on page 798](#)
- [Device logs on page 800](#)
- [File Management on page 804](#)
- [Advanced Settings on page 804](#)



## Dashboard

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



The following widgets are available:

Widget	Description
<b>System Information</b>	<p>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 <a href="#">System Information widget on page 721</a>.</p> <p>From this widget you can manually update the FortiManager firmware to a different release. For more information, see <a href="#">Updating the system firmware on page 723</a>.</p> <p>The widget fields will vary based on how the FortiManager is configured, for example, if ADOMs are enabled.</p>
<b>System Resources</b>	<p>Displays the real-time and historical usage status of the CPU, memory and hard disk. For more information, see <a href="#">System Resources widget on page 729</a>.</p>
<b>License Information</b>	<p>Displays whether the unit license is registered to FortiCloud.</p> <p>Displays the devices being managed by the FortiManager unit and the maximum numbers of devices allowed. For more information, see <a href="#">License Information widget on page 729</a>.</p>

Widget	Description
	From this widget you can add a license or manually upload a license for VM systems.
<b>Unit Operation</b>	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 <a href="#">Unit Operation widget on page 734</a> .
<b>Alert Message Console</b>	Displays log-based alert messages for both the FortiManager unit and connected devices. For more information, see <a href="#">Alert Messages Console widget on page 734</a> .
<b>Log Receive Monitor</b>	Displays a real-time monitor of logs received. You can view data per device or per log type. For more information, see <a href="#">Log Receive Monitor widget on page 735</a> . The <i>Log Receive Monitor</i> widget is available when <i>FortiAnalyzer Features</i> is enabled.
<b>Insert Rate vs Receive Rate</b>	Displays the log insert and receive rates. For more information, see <a href="#">Insert Rate vs Receive Rate widget on page 735</a> . The <i>Insert Rate vs Receive Rate</i> widget is available when <i>FortiAnalyzer Features</i> is enabled.
<b>Log Insert Lag Time</b>	Displays how many seconds the database is behind in processing the logs. For more information, see <a href="#">Log Insert Lag Time widget on page 736</a> . The <i>Log Insert Lag Time</i> widget is available when <i>FortiAnalyzer Features</i> is enabled.
<b>Receive Rate vs Forwarding Rate</b>	Displays the <i>Receive Rate</i> , 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 <a href="#">Receive Rate vs Forwarding Rate widget on page 736</a> . The <i>Receive Rate vs Forwarding Rate</i> widget is available when <i>FortiAnalyzer Features</i> is enabled.
<b>Disk I/O</b>	Displays the disk utilization, transaction rate, or throughput as a percentage over time. For more information, see <a href="#">Disk I/O widget on page 737</a> . The <i>Disk I/O</i> widget is available when <i>FortiAnalyzer Features</i> is enabled.

## 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
<b>Move a widget</b>	Move the widget by clicking and dragging its title bar, then dropping it in its new location
<b>Add a widget</b>	Select <i>Toggle Widgets</i> from the toolbar, then select the name widget you need to add.
<b>Delete a widget</b>	Click the <i>Close</i> icon in the widget's title bar.

Action	Steps
<b>Customize a widget</b>	For widgets with an edit icon, you can customize the widget by clicking the Edit icon and configuring the settings.
<b>Reset the dashboard</b>	Select <i>Toggle Widgets &gt; Reset to Default</i> 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:

<b>Host Name</b>	The identifying name assigned to this FortiManager unit. Click the edit host name button to change the host name. For more information, see <a href="#">Changing the host name on page 722</a> .
<b>Serial Number</b>	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.
<b>Platform Type</b>	Displays the FortiManager platform type, for example <i>FMGVM64</i> (virtual machine).
<b>HA Status</b>	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 <a href="#">High Availability on page 889</a> .
<b>System Time</b>	The current time on the FortiManager internal clock. Click the edit system time button to change system time settings. For more information, see <a href="#">Configuring the system time on page 722</a> .
<b>Firmware Version</b>	<p>The version number and build number of the firmware installed on the FortiManager unit.</p> <p>You can access the latest firmware version available on FortiGuard from FortiManager.</p> <p>Alternately you can manually download the latest firmware from the Customer Service &amp; Support website at <a href="https://support.fortinet.com">https://support.fortinet.com</a>. Click the update button, then select the firmware image to load from the local hard disk or network volume. For more information, see <a href="#">Updating the system firmware on page 723</a>.</p>
<b>System Configuration</b>	<p>The date of the last system configuration backup. The following actions are available:</p> <ul style="list-style-type: none"> <li>Click the backup button to backup the system configuration to a file; see <a href="#">Backing up the system on page 726</a>.</li> <li>Click the restore to restore the configuration from a backup file; see <a href="#">Restoring the configuration on page 728</a>. You can also migrate the configuration to a different FortiManager model by using the CLI. See <a href="#">Migrating the configuration on page 728</a>.</li> </ul>

<b>Current Administrators</b>	The number of administrators currently logged in. Click the current session list button to view the session details for all currently logged in administrators.
<b>Up Time</b>	The duration of time the FortiManager unit has been running since it was last started or restarted.
<b>Administrative Domain</b>	Displays whether ADOMs are enabled. Toggle the switch to change the Administrative Domain state. See <a href="#">Enabling and disabling the ADOM feature on page 753</a> .
<b>FortiAnalyzer Features</b>	Displays whether FortiAnalyzer features are enabled. Toggle the switch to change the FortiAnalyzer features state. <i>FortiAnalyzer Features</i> are not available on the FortiManager 100C or when FortiManager HA is enabled. See <a href="#">FortiAnalyzer Features on page 29</a> 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 *System Settings > 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 *System Settings > 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:

<b>System Time</b>	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 <i>Refresh</i> button.
<b>Time Zone</b>	Select the time zone in which the FortiManager unit is located and whether or not the system automatically adjusts for daylight savings time.
<b>Update Time By</b>	Select <i>Set time</i> to manually set the time, or <i>Synchronize with NTP Server</i> to automatically synchronize the time.
<b>Set Time</b>	Manually set the data and time.
<b>Select Date</b>	Set the date from the calendar or by manually entering it in the format: YYYY/MM/DD.
<b>Select Time</b>	Select the time.
<b>Synchronize with NTP Server</b>	Automatically synchronize the date and time.
<b>Server</b>	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 <a href="http://www.ntp.org">http://www.ntp.org</a> .
<b>Min</b>	Minimum poll interval in seconds as power of 2 (e.g. 6 means 64 seconds, default = 6).
<b>Max</b>	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 *System Settings* module 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 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 726](#).



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.



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 627](#).

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:

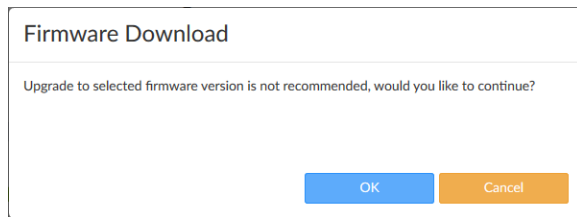
1. Go to *System Settings*.
2. In the *System Information* widget, beside *Firmware Version*, click *Update Firmware*.  
The *Firmware Management* dialog box opens.

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.

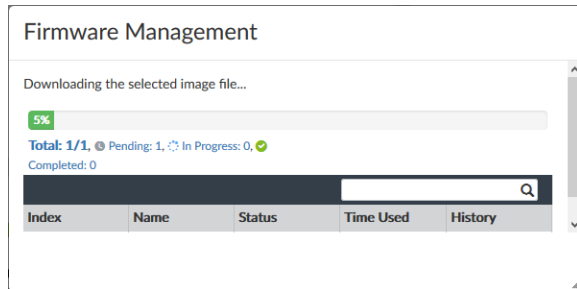
If you want to encrypt the backup file, enable *Encryption*, then type and confirm the password you want to use. The password can be a maximum of 63 characters.

4. From the *FortiGuard Firmware* box, select the version of FortiManager for the upgrade, and click *OK*.  
The *FortiGuard Firmware* box displays all FortiManager firmware images available for upgrade. A green checkmark displays beside the recommended image for FortiManager upgrade.

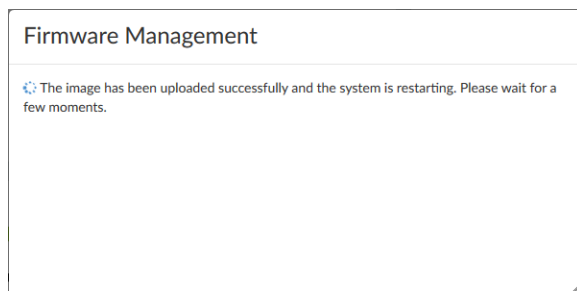
If you select an image without a green checkmark, a confirmation dialog box is displayed. Click *OK* to continue.



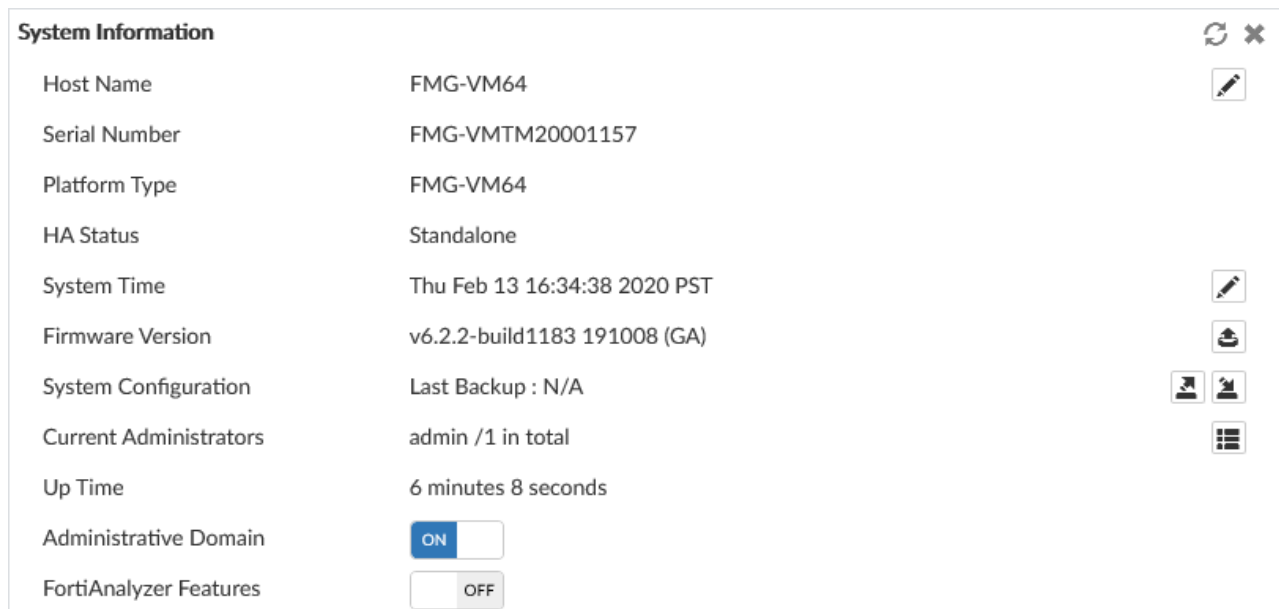
FortiManager downloads the firmware image from FortiGuard.



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 *System Settings > 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.  
If you want to encrypt the backup file, enable *Encryption*, then type and confirm the password you want to use. 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 noting that the upgrade was successful.



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. Launch the *Device Manager* module and make sure that all formerly added devices are still listed.
9. Launch 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 641](#).

## 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.

If any management extensions are enabled, the backup file includes the configuration for each enabled management extension.

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 448](#).

Fortinet recommends backing up all configuration settings from your FortiManager unit before upgrading the FortiManager firmware. See [Updating the system firmware on page 723](#).

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.



**To back up the FortiManager configuration:**

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, click the backup button next to *System Configuration*. The *Backup System* dialog box opens
3. If you want to encrypt the backup file, select the *Encryption* box, then type and confirm the password you want to use. The password can be a maximum of 63 characters.
4. Select *OK* and save the backup file on your management computer.

**Configuring automatic backups**

You can configure FortiManager to automatically backup your configuration on a set schedule. This feature can only be configured through the CLI.

**To schedule automatic backup of the FortiManager configuration:**

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](#).

**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.

## 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.

If your FortiManager has management extensions enabled, the configuration for the enabled management extension is restored too.



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 *System Settings > 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*.

<b>Choose Backup File</b>	Select <i>Browse</i> to find the configuration backup file you want to restore, or drag and drop the file onto the dialog box.
<b>Password</b>	Type the encryption password, if applicable.
<b>Overwrite current IP, routing and HA settings</b>	Select the checkbox to overwrite the current IP, routing, and HA settings.
<b>Restore in Offline Mode</b>	Informational checkbox. Hover over the help icon for more information.

## Migrating the configuration

You can back up the system of one FortiManager model, and then use the CLI and the FTP, SCP, or SFTP protocol to migrate the settings to another FortiManager model.

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.



The `execute migrate all-settings` command migrates all configurations except the CLI system settings. These system settings must be manually copied from the original FortiManager model to the other FortiManager model.

### To migrate the FortiManager configuration:

1. In one FortiManager model, go to *System Settings > Dashboard*.
2. Back up the system. See [Backing up the system on page 726](#).
3. In the other FortiManager model, go to *System Settings > 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>
[crpytpasswd]
```
6. After migrating, update the CLI system settings, as needed.
7. Re-establish the FGFM tunnels. See [Appendix C - Re-establishing the FGFM tunnel after VM license migration on page 909](#).

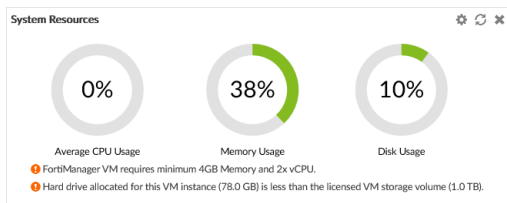


If the original FortiManager has databases from FortiGuard (antivirus, antispam, webfilter, etc.), they will not be included in the configuration file. After migrating, export the packages from the original FortiManager and import them to the other FortiManager. For example, see [Exporting web filter databases example on page 638](#) and [Importing web filter databases example on page 639](#).

## 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 25](#)). 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.

License Information			 
 VM License	Valid UUG	 	
 FortiCloud	 Registered		
 FortiGuard	VM Meter Service	 No License	
	Server Location	 Servers located in US only	
 Management	Devices/VDOMs	0 of 10,000 (0.0%)	
	FortiAPs	3	
	FortiSwitches	3	
 Update Server	AntiVirus and IPS	12.34.97.16  Ashburn, Virginia, United S...	
	Web and Email Filter	96.45.33.64  Sunnyvale, California, Unit...	
	FortiClient Update	96.45.33.106  Sunnyvale, California, Uni...	

**VM 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 731](#).

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.

**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 731](#).

**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.

<b>FortiGates/Logging Devices</b>	The number of connected FortiGates and other logging devices.
<b>FortiAPs</b>	The number of connected FortiAPs.
<b>FortiSwitches</b>	The number of connected FortiSwitches.
<b>Logging</b>	This section is only shown when <i>FortiAnalyzer Features</i> is enabled. For more information, see <a href="#">FortiAnalyzer Features on page 29</a> .
<b>Device/VDOMs</b>	The total number of devices and VDOMs connected to the FortiManager and the total number of device and VDOM licenses.
<b>GB/Day</b>	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. The GB/Day log volume can be viewed per ADOM through the CLI using: <code>diagnose fortilogd logvol-adom &lt;name&gt;</code> .
<b>Update Server</b>	
<b>AntiVirus and IPS</b>	The IP address and physical location of the Antivirus and IPS update server.
<b>Web and Email Filter</b>	The IP address and physical location of the web and email filter update server.
<b>FortiClient Update</b>	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 21](#).

### To register a FortiManager device:

1. Go to *System Settings > 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.

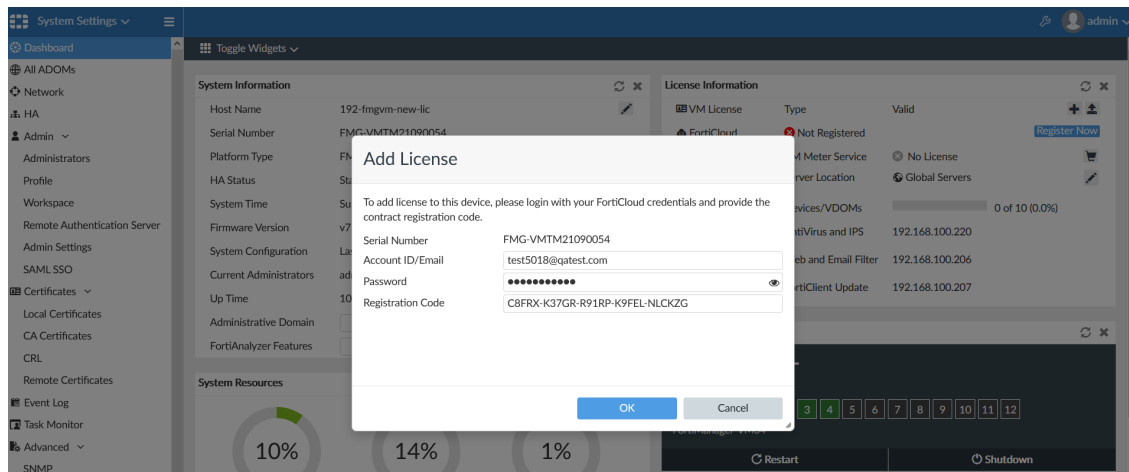
**To purchase a new license:**

1. Go to the Fortinet Technical Support site at <https://support.fortinet.com/>.
2. Log in by using your FortiCloud account credentials.
3. Purchase a license.

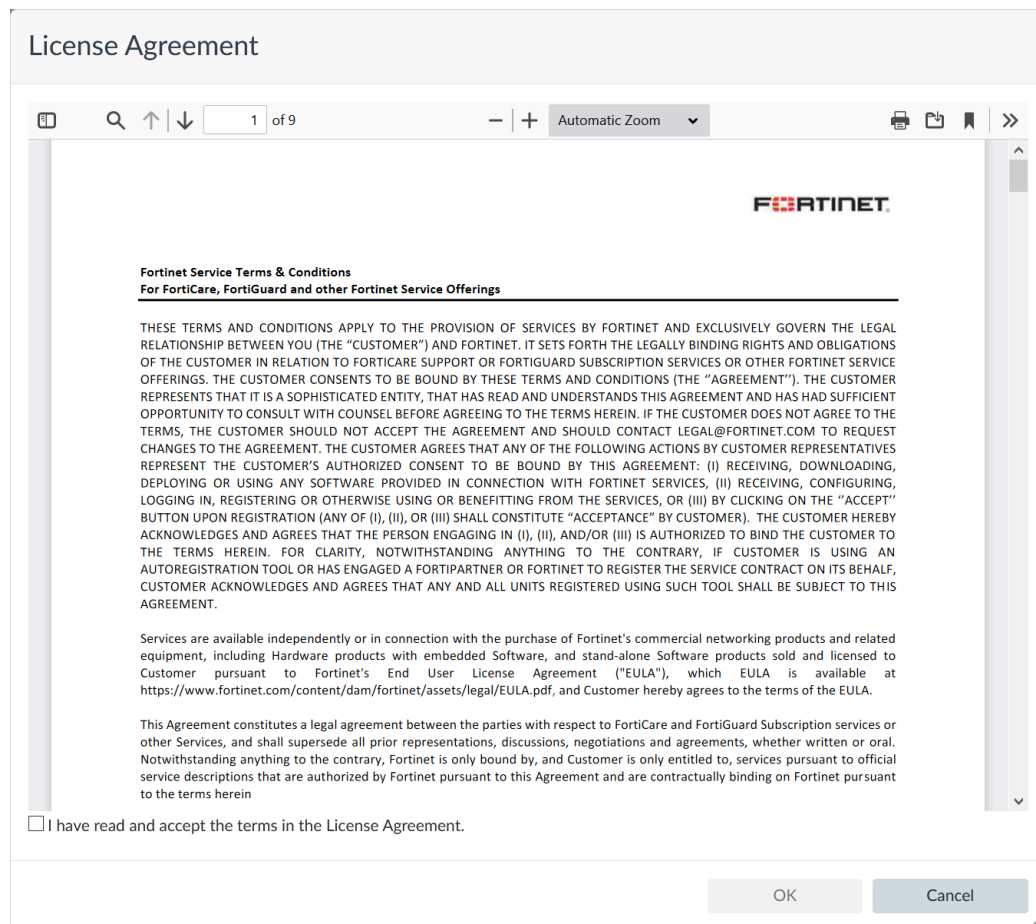
You will receive an email from Fortinet with a PDF attachment that includes a contract registration code.

**To add a license:**

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

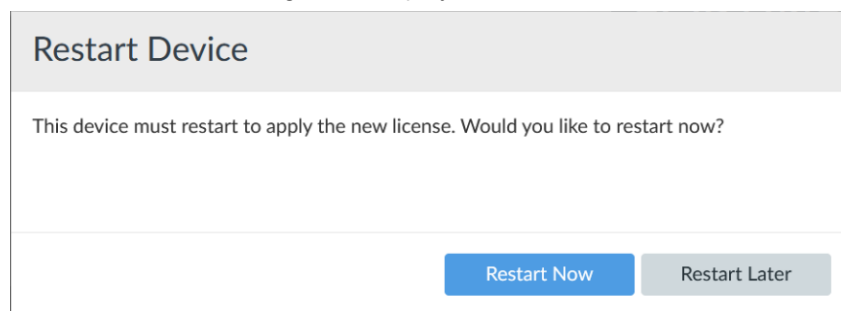


3. Complete the following options, and click **OK**:
  - a. In the *Account ID/Email* box, type the email for your FortiCloud account.
  - b. In the *Password* box, type the password for your FortiCloud account.
  - c. In the *Registration Code* box, enter the contract registration code for the add-on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



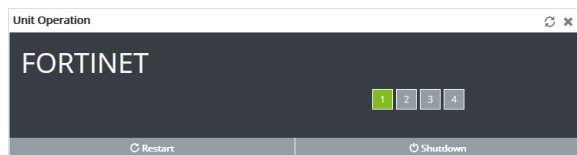
FortiAP, FortiSwitch, and FortiExtender are not included in the license count. For more information see the [Fortinet Product Matrix](#).

---

## 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.

---



Alert Message Console	
Time	Message
May 31, 09:59:02	Disk usage for Adom FortiMail is approaching the delete threshold 90% of total 102400 MB.
May 31, 09:57:26	Disk usage for Adom FortiSandbox is approaching the delete threshold 90% of total 102400 MB.
May 31, 09:41:48	Disk usage for Adom root is approaching the delete threshold 90% of total 3145728 MB.
May 31, 08:58:59	Disk usage for Adom FortiMail is approaching the delete threshold 90% of total 102400 MB.
May 31, 08:57:25	Disk usage for Adom FortiSandbox is approaching the delete threshold 90% of total 102400 MB.
May 31, 08:41:37	Disk usage for Adom root is approaching the delete threshold 90% of total 3145728 MB.
May 31, 07:58:59	Disk usage for Adom FortiMail is approaching the delete threshold 90% of total 102400 MB.
May 31, 07:57:25	Disk usage for Adom FortiSandbox is approaching the delete threshold 90% of total 102400 MB.
May 31, 07:41:32	Disk usage for Adom root is approaching the delete threshold 90% of total 3145728 MB.
May 31, 06:58:53	Disk usage for Adom FortiMail is approaching the delete threshold 90% of total 102400 MB.

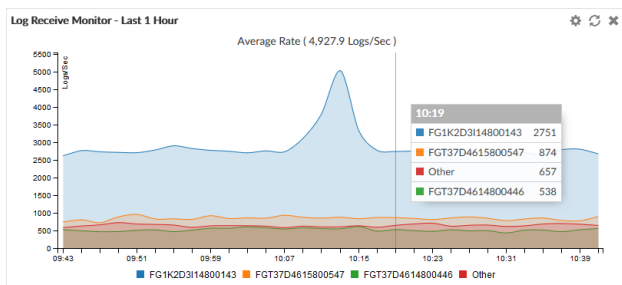
Click *Edit* from the widget toolbar to view the *Alert Message Console Settings*, where you can adjust the number of entries that are visible in the widget, and the refresh interval.

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 29](#).

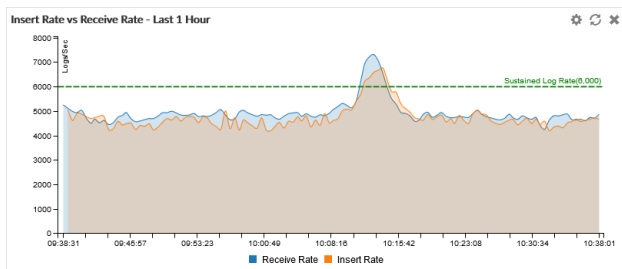
## Insert Rate vs Receive Rate widget

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.

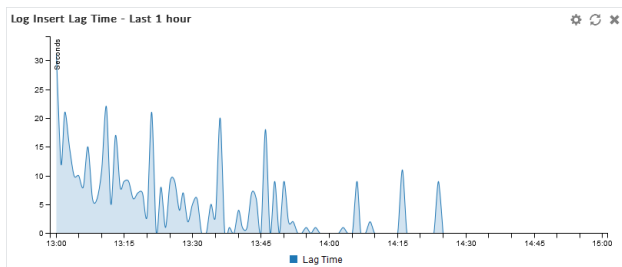


This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 29](#).

## 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.

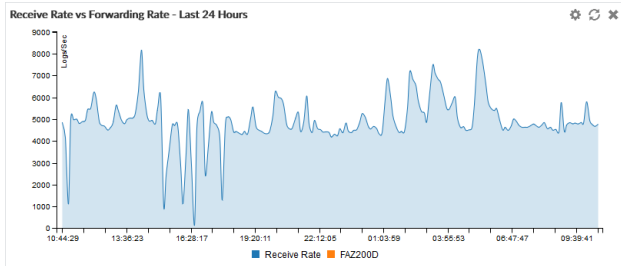


This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 29](#).

## 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.

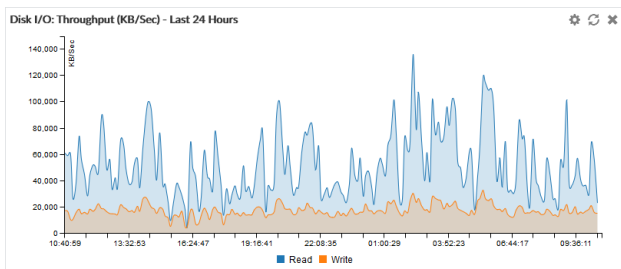


This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 29](#).

## 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.



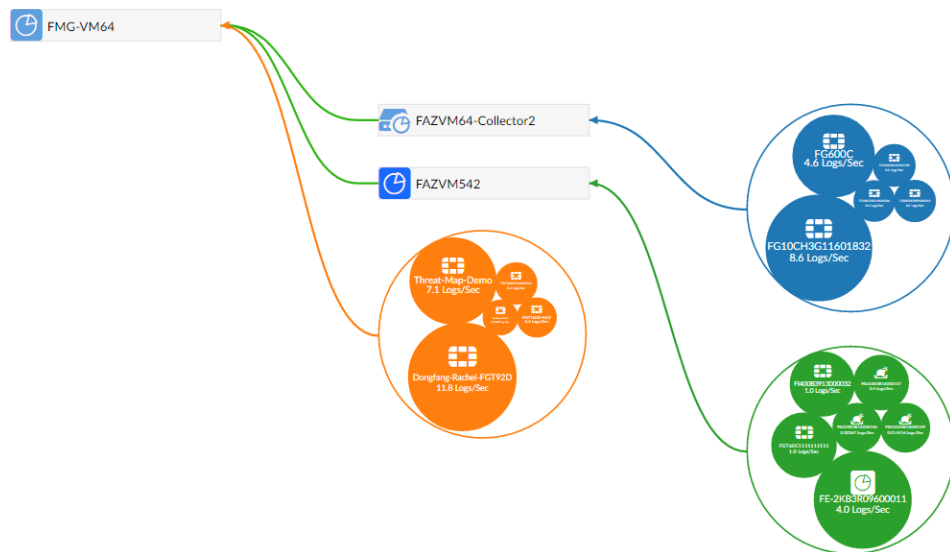
This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 29](#).

## Logging Topology

The *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 29](#).

## 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 808](#) and [Managing administrator accounts on page 809](#).

## 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.

Name	IP/Netmask	IPv6 Address	Description	Administrative Access	IPv6 Administrative Access	Service Access	Enable
port1	10.100.55.2/255.255.255.0	:::0		HTTPS, HTTP, PING, SSH			<input checked="" type="checkbox"/>
port2	10.100.88.2/255.255.255.0	:::0		HTTPS, HTTP, PING, SSH			<input checked="" type="checkbox"/>
port3	0.0.0.0/0.0.0.0	:::0					<input checked="" type="checkbox"/>
port4	0.0.0.0/0.0.0.0	:::0					<input checked="" type="checkbox"/>
port5	0.0.0.0/0.0.0.0	:::0					<input checked="" type="checkbox"/>
port6	0.0.0.0/0.0.0.0	:::0					<input checked="" type="checkbox"/>
port7	0.0.0.0/0.0.0.0	:::0					<input checked="" type="checkbox"/>
port8	0.0.0.0/0.0.0.0	:::0					<input checked="" type="checkbox"/>
port9	0.0.0.0/0.0.0.0	:::0					<input checked="" type="checkbox"/>
port10	0.0.0.0/0.0.0.0	:::0					<input checked="" type="checkbox"/>
port11	0.0.0.0/0.0.0.0	:::0					<input checked="" type="checkbox"/>
port12	0.0.0.0/0.0.0.0	:::0					<input checked="" type="checkbox"/>

DNS

Primary DNS Server: 8.8.8.8

Secondary DNS Server: 208.91.112.53

Apply

2. In the *Interface* pane, double-click *Port1*. The *Edit System Interface* pane is displayed.

Edit System Interface

Name: port1

Alias:

IP Address/Netmask: 10.100.55.12/255.255.255.0

IPv6 Address: :::0


Administrative Access: ☒ HTTPS ☒ HTTP ☒ PING ☒ SSH ☐ SNMP ☐ Web Service

IPv6 Administrative Access: ☐ HTTPS ☐ HTTP ☐ PING ☐ SSH ☐ SNMP ☐ Web Service

Service Access: ☐ FortiGate Updates ☐ Web Filtering

Status: ☒ Enable ☐ Disable

3. Configure the following settings for *port1*, then click *OK* to apply your changes.

<b>Name</b>	Displays the name of the interface.
<b>IP Address/Netmask</b>	The IP address and netmask associated with this interface.
<b>IPv6 Address</b>	The IPv6 address associated with this interface.
<b>Administrative Access</b>	Select the allowed administrative service protocols from: HTTPS, HTTP, PING, SSH, SNMP, and Web Service.
<b>IPv6 Administrative Access</b>	Select the allowed IPv6 administrative service protocols from: HTTPS, HTTP, PING, SSH, SNMP, and Web Service.
<b>Service Access</b>	<p>Select the Fortinet services that are allowed access on this interface. These include <i>FortiGate Updates</i> and <i>Web Filtering</i>. By default all service access is enabled on port1, and disabled on port2.</p> <p>Select <i>Bind to IP Address</i> and specify the IP address. The IP address specified in Bind to IP address must be on the same subnet as the IP address of the interface. This IP address is only for FortiGate 443 requests.</p> <hr/> <div>  <p>Specifying the IP address is optional. If you do not change the default IP address (0.0.0.0), the interface IP address is used.</p> </div> <hr/>
<b>Status</b>	Select <i>Enable</i> or <i>Disable</i> .

4. Configure the DNS settings, and click *Apply*.

<b>Primary DNS Server</b>	The primary DNS server IP address.
<b>Secondary DNS Server</b>	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, and Web Service.

**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.

## 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 network 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 <a href="#">Configuring network interfaces on page 739</a> .
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 <i>Host(s)</i> , <i>Port(s)</i> , <i>VLAN(s)</i> , and <i>Protocol</i> .

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 Address/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*.

After the aggregate links are configured, log into FortiGate and go to *Network > Interfaces*, and configure an aggregation interface. For information, see [Aggregation and redundancy](#) in the *FortiOS Administration Guide*.

**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 741](#).

## 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 rebuild 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 *System Settings > Dashboard*, provides detailed information about RAID array failures. For more information see [Alert Messages Console widget on page 734](#).

---

## Summary



RAID Level

Status

Disk Space Usage

Raid-10 [\[Change\]](#)

System is functioning normally.

1890GB Used / 5442GB Free / 7332GB Total

25% Used

## Disk Management

Disk Number	Disk Status	Size(GB)	Disk Model
0	✓	1862	ST2000NM0033-9ZM175
1	✓	1862	ST2000NM0033-9ZM175
2	✓	1862	ST2000NM0033-9ZM175
3	✓	1862	ST2000NM0033-9ZM175
4	✓	1862	ST2000NM0033-9ZM175
5	✓	1862	ST2000NM0033-9ZM175
6	✓	1862	ST2000NM0033-9ZM175
7	✓	1862	ST2000NM0033-9ZM175

<b>Summary</b>	Shows summary information about the RAID array.
<b>Graphic</b>	Displays the position and status of each disk in the RAID array. Hover the cursor over each disk to view details.
<b>RAID Level</b>	Displays the selected RAID level. Click <i>Change</i> to change the selected RAID level. When you change the RAID settings, all data is deleted.
<b>Status</b>	Displays the overall status of the RAID array.
<b>Disk Space Usage</b>	Displays the total size of the disk space, how much disk space is used, and how much disk space is free.
<b>Disk Management</b>	Shows information about each disk in the RAID array.
<b>Disk Number</b>	Identifies the disk number for each disk.
<b>Disk Status</b>	Displays the status of each disk in the RAID array. <ul style="list-style-type: none"> <li><i>Ready</i>: The hard drive is functioning normally.</li> <li><i>Rebuilding</i>: 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.</li> <li><i>Initializing</i>: The FortiManager unit is writing to all the hard drives in the device in order to make the array fault tolerant.</li> <li><i>Verifying</i>: The FortiManager unit is ensuring that the parity data of a redundant drive is valid.</li> <li><i>Degraded</i>: The hard drive is no longer being used by the RAID controller.</li> <li><i>Inoperable</i>: 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.</li> </ul>
<b>Size (GB)</b>	Displays the size, in GB, of each disk.
<b>Disk Model</b>	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 734](#).



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 734](#) for information.
4. Configure the RAID level. See [Configuring the RAID level on page 747](#).
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 808](#).



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 85](#).

## 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 751](#).

## 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 > All ADOMs* pane.

## ADOM types

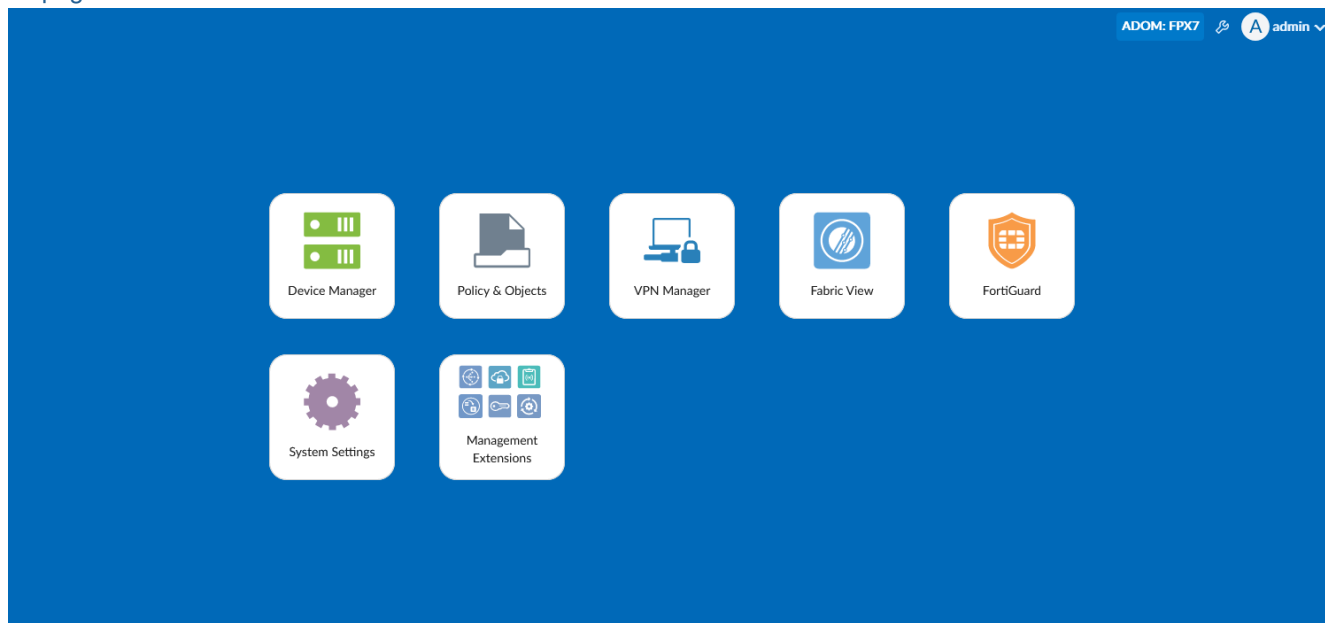
When ADOMs are enabled, you can create ADOMs and select a type. The type of ADOM determines what types of devices you can add to the ADOM. FortiManager supports the following types of ADOMs:

<b>Fabric</b>	You can add FortiGate and other types of devices from a Security Fabric to an ADOM with <i>Fabric</i> type selected.
<b>FortiGate</b>	You can add only FortiGate devices to an ADOM with <i>FortiGate</i> type selected.
<b>FortiCarrier</b>	You can add only FortiCarrier devices to an ADOM with <i>FortiCarrier</i> type selected.
<b>FortiFirewall</b>	You can add only FortiFirewall devices to an ADOM with <i>FortiFirewall</i> type selected.
<b>FortiFirewallCarrier</b>	You can add only FortiFirewall Carrier devices to an ADOM with <i>FortiFirewallCarrier</i> type selected.
<b>FortiProxy</b>	You can only add FortiProxy devices to an ADOM with <i>FortiProxy</i> type selected. See <a href="#">FortiProxy ADOMs on page 752</a> .

See [Creating ADOMs on page 759](#).

## FortiProxy ADOMs

You can create FortiProxy ADOMs to centrally manage FortiProxy devices using FortiManager. See [Creating ADOMs on page 759](#).



The following FortiManager modules are available in FortiProxy ADOMs:

FortiManager Module	Features available in FortiProxy ADOM
<b>Device Manager on page 48</b>	Use the <i>Device Manager</i> 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 <i>Device Manager</i> pane. Using the device database, you can configure managed FortiProxy devices. For more information, see <a href="#">Device Manager on page 48</a> .
<b>Policy &amp; Objects on page 304</b>	Configure policies and objects for FortiProxy devices, including: <ul style="list-style-type: none"> <li>• <a href="#">Create a new FortiProxy firewall policy on page 395</a></li> <li>• <a href="#">Create a new FortiProxy proxy auto-configuration (PAC) policy on page 397</a></li> <li>• <a href="#">FortiProxy content analysis objects on page 446</a></li> </ul> For more information, see <a href="#">Policy &amp; Objects on page 304</a> .
<b>VPN Manager on page 511</b>	Use the <i>VPN Manager</i> 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 <a href="#">VPN Manager on page 511</a> .
<b>Fabric View on page 556</b>	The <i>Fabric View</i> module enables you to view and create fabric connectors. For more information, see <a href="#">Fabric View on page 556</a> .
<b>FortiGuard on page 627</b>	View and manage FortiGuard services for FortiProxy devices. For more information, see <a href="#">FortiGuard on page 627</a> .
<b>System Settings on page 718</b>	Configure FortiManager system settings.

FortiManager Module	Features available in FortiProxy ADOM
	For more information, see <a href="#">System Settings on page 718</a> .
<a href="#">Management Extensions on page 900</a>	Configure FortiManager management extension applications. For more information, see <a href="#">Management Extensions on page 900</a> .

## 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*, *FortiSoC*, 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 28](#).

### To enable the ADOM feature:

1. Log in to the FortiManager as a super user administrator.
2. Go to *System Settings > 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 763](#).  
Only after removing all the non-root ADOMs can ADOMs be disabled.
3. Go to *System Settings > 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

When creating an ADOM in Backup Mode, the ADOM is considered *Read Only*, where you cannot make changes to the ADOM and managed devices from FortiManager. Changes are made via scripts, which are run on the managed device, or through the device's GUI or CLI directly. Revisions are sent to the FortiManager when 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.

When you add a device to an ADOM in backup mode, you can import firewall address and service objects to FortiManager, and FortiManager stores the objects in the Device Manager database. You can view the objects on the *Policy & Objects* pane. Although you can view the objects on the *Policy & Objects* pane, the objects are not stored in the central database. This lets you maintain a repository of objects used by all devices in the backup ADOM that is separate from the central database.

All devices that are added to the ADOM will only have their configuration backed up. Configuration changes cannot be made to the devices in a backup ADOM. You can push any existing revisions to managed devices. You can still monitor and review the revision history for these devices, and scripting is still allowed for pushing scripts directly to FortiGate units.

## 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:

- *Device Manager*
- *Policy & Objects*
- *FortiGuard*
- *FortiView*
- *System Settings*

### To create backup ADOMs:

1. Go to *System Settings > All 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 <i>Add Device</i> wizard.
Mode	Select <i>Backup</i> .

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. The wizard also lets you import Firewall address and service objects. Policies are not imported. Alternately, you can import objects after adding devices by using the *Import Configuration* button on the *Device Manager* pane.

All imported objects are stored in the device database. They are not stored in the central database, which is used to store objects used in policies.

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 757](#).

### Importing FortiGate objects

#### To import FortiGate objects when adding devices:

1. Go to *Device Manager > Device & Groups*, and click *Add Device*.
2. Follow the *Add Device* wizard, until the *Import* button is displayed.
3. Click *Import* to import firewall address and service objects to the Device Manager database.  
The objects are imported into the Device Manager database.  
Alternately you can import the objects after you add the device.
4. Go to the *Policy & Objects* pane to view the objects.  
You can also create, edit, and delete objects.

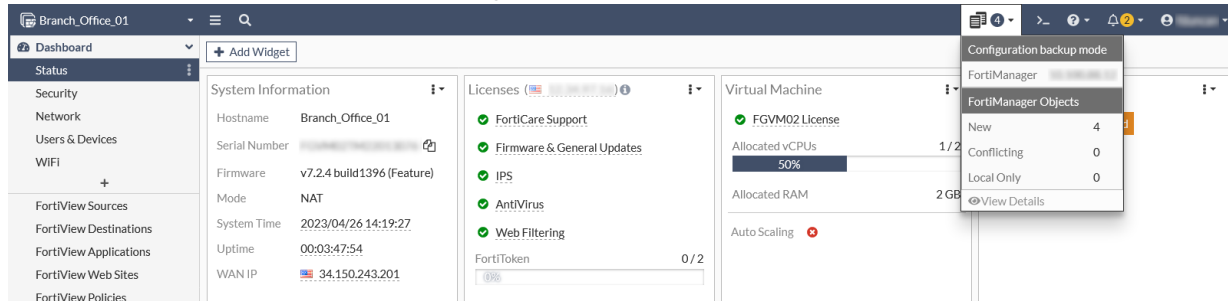
#### To import FortiGate objects after adding devices:

1. Go to *Device Manager > Device & Groups*.
2. Select a device and click *Import Policy*.  
The objects are imported into the Device Manager 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:

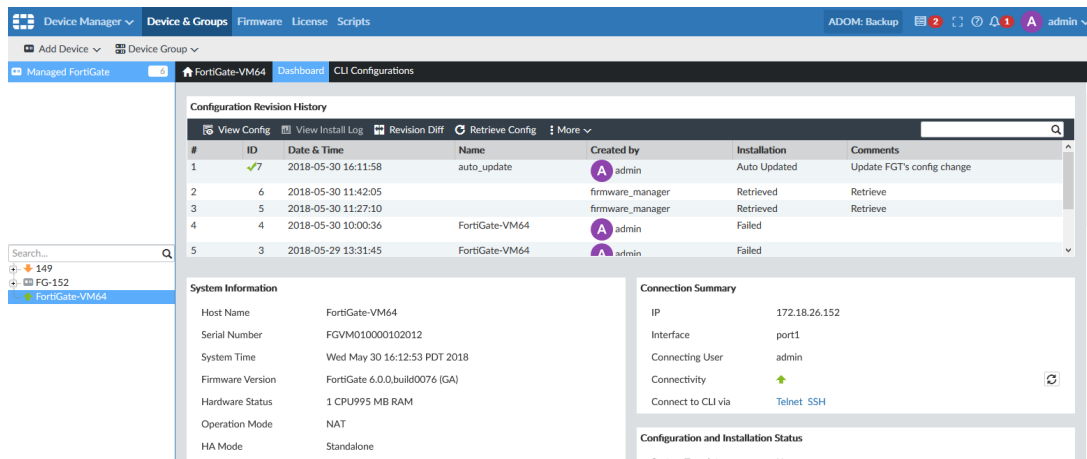
<b>New</b>	Objects stored on the FortiManager backup ADOM that are not available locally. To import new objects to the local FortiGate, select them and click <i>Import</i> or <i>Import All</i> .
<b>Conflicting</b>	Local and FortiManager objects that are in conflict. To view a comparison of the objects, click <i>View Properties</i> . To replace a local object with the FortiManager object, select the object and click <i>Update</i> .
<b>Local Only</b>	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 <a href="#">Importing FortiGate objects on page 756</a> .

## Viewing read-only policies in backup ADOMs

When an ADOM is in backup mode, you can view information about read-only policies

To view read-only policies:

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 137](#).



5. In the dashboard toolbar, click *CLI Configurations* to view information about policies. The policies are read-only.

## Managing ADOMs

The ADOMs feature must be enabled before ADOMs can be created or configured. See [Enabling and disabling the ADOM feature on page 753](#).

To create and manage ADOMs, go to *System Settings > All ADOMs*.

<div><div><div>+ Create New</div><div>Edit</div><div>Delete</div><div>Enter ADOM</div><div>Disable ADOM</div><div>Lock</div><div>Unlock</div><div>More</div><div>Column Settings</div></div><div>Search...</div></div>						
<input type="checkbox"/>	▲ Name	Firmware Version	Central Management			Devices
Security Fabric (2)						
<input type="checkbox"/>	ADOM_7	Fabric 7.0	VPN	FortiAP	FortiSwitch	1 Device (including 1 VDOM)
<input type="checkbox"/>	root	Fabric 6.4	VPN	FortiAP	FortiSwitch	1 Device (including 1 VDOM)
Central Management (9)						
<input type="checkbox"/>	ADOM7	FortiGate 7.0	VPN	FortiAP	FortiSwitch	1 Device (including 1 VDOM)
<input type="checkbox"/>	FortiCarrier	FortiCarrier 6.4	VPN	FortiAP	FortiSwitch	
<input type="checkbox"/>	FortiDeceptor	FortiFirewall 3.1	VPN	FortiAP	FortiSwitch	
<input type="checkbox"/>	FortiFirewall	FortiFirewall 6.2	VPN	FortiAP	FortiSwitch	
<input type="checkbox"/>	FortiFirewallCarrier	FortiFirewallCarrier 6.2	VPN	FortiAP	FortiSwitch	
<input type="checkbox"/>	FortiProxy	FortiProxy 1.2	VPN	FortiAP	FortiSwitch	
<input type="checkbox"/>	ManagedFAZ	FortiGate 7.0	VPN	FortiAP	FortiSwitch	1 Device (including 1 VDOM)
<input type="checkbox"/>	TEST	FortiGate 7.2	VPN	FortiAP	FortiSwitch	1 Device (including 1 VDOM)
<input type="checkbox"/>	Global Database	Global 6.4	VPN	FortiAP	FortiSwitch	
Other Device Types (12)						
<input type="checkbox"/>	FortiAnalyzer	FortiAnalyzer	-	-	-	
<input type="checkbox"/>	FortiAuthenticator	FortiAuthenticator	-	-	-	
<input type="checkbox"/>	FortiCache	FortiCache	-	-	-	
<input type="checkbox"/>	FortiClient	FortiClient	-	-	-	
<input type="checkbox"/>	FortiDDoS	FortiDDoS	-	-	-	
<input type="checkbox"/>	FortiMail	FortiMail	-	-	-	
<input type="checkbox"/>	FortiManager	FortiManager	-	-	-	
<input type="checkbox"/>	FortiNAC	FortiNAC	-	-	-	
<input type="checkbox"/>	FortiSandbox	FortiSandbox	-	-	-	
<input type="checkbox"/>	FortiWeb	FortiWeb	-	-	-	
<input type="checkbox"/>	Syslog	Syslog	-	-	-	
<input type="checkbox"/>	Chassis	-	-	-	-	

### Create New

Create a new ADOM. See [Creating ADOMs on page 759](#).

### Edit

Edit the selected ADOM. This option is also available from the right-click menu. See [Editing an ADOM on page 763](#).



<b>Delete</b>	Delete the selected ADOM or ADOMs. You cannot delete default ADOMs. This option is also available from the right-click menu. See <a href="#">Deleting ADOMs on page 763</a> .
<b>Enter ADOM</b>	Switch to the selected ADOM. This option is also available from the right-click menu.
<b>Disable ADOM</b>	Disable the selected ADOM. This option is also available from the right-click menu.
<b>More</b>	<p>Select <i>Expand Devices</i> to expand all of the ADOMs to show the devices in each ADOM.</p> <p>Select <i>Collapse Devices</i> to collapses the device lists.</p> <p>Select <i>ADOM Health Check</i> to generate a report that identifies whether any ADOMs contain problematic devices. See <a href="#">Checking ADOM health on page 764</a>.</p> <p>Select an ADOM, and click <i>Clone</i> to make a copy of the ADOM. Devices are not cloned to the new ADOM.</p> <p>Select an ADOM, and click <i>Upgrade</i> to upgrade the ADOM. See also <a href="#">ADOM versions on page 766</a>.</p> <p>Some of these options are also available from the right-click menu.</p>
<b>Search</b>	Enter a search term to search the ADOM list.
<b>Name</b>	<p>The name of the ADOM.</p> <p>ADOMs are listed in the following groups: <i>Security Fabric</i>, <i>Central Management</i>, <i>Backup Mode</i> (if there are any backup mode ADOMs), and <i>Other Device Types</i>. A group can be collapsed or expanded by clicking the triangle next to its name.</p>
<b>Firmware Version</b>	<p>The firmware version of the ADOM. Devices in the ADOM should have the same firmware version.</p> <p>See <a href="#">ADOM versions on page 766</a> for more information.</p>
<b>Central Management</b>	Whether or not central management for VPN, FortiAP, or FortiSwitch is enabled for the ADOM.
<b>Devices</b>	<p>The number of devices and VDOMs that the ADOM contains.</p> <p>The device list can be expanded or by clicking the triangle.</p>

## 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 754](#).
- 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:

- Ensure that ADOMs are enabled. See [Enabling and disabling the ADOM feature on page 753](#).
- Go to *System Settings > All ADOMs*.
- Click *Create New* in the toolbar. The *Create New ADOM* pane is displayed.

**Create New ADOM**

Name:

Type: FortiGate (6.2, 6.4, 7.0)

Comments:

Devices

+ Select Device

Name	IP Address	Platform
No Device.		

Mode: ☒ Normal ☐ Backup

Central Management: ☐ VPN ☒ FortiAP ☒ FortiSwitch

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

Perform Policy Check Before Every Install:

Auto-Push Policy Packages When Device Back Online: ☐ Enable ☒ Disable

OK Cancel

- Configure the following settings, then click *OK* to create the ADOM.

<b>Name</b>	Type a name that allows you to distinguish this ADOM from your other ADOMs. ADOM names must be unique.
<b>Type</b>	Select <i>Fabric</i> , <i>FortiCarrier</i> , <i>FortiFirewall</i> , <i>FortiFirewall Carrier</i> , <i>FortiGate</i> , or <i>FortiProxy</i> 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.
<b>Version</b>	Select the version of the devices in the ADOM. The ADOM version cannot be edited.

<b>Devices</b>	Add a device or devices with the selected versions to the ADOM. The search field can be used to find specific devices. See <a href="#">Assigning devices to an ADOM on page 762</a> .
<b>Mode</b>	Select <i>Normal</i> mode if you want to manage and configure the connected devices from the FortiManager GUI. Select <i>Backup</i> mode if you want to backup the configurations to the FortiManager, but configure each device locally. See <a href="#">ADOM modes on page 754</a> for more information.
<b>Central Management</b>	Select the <i>VPN</i> checkbox to enable central VPN management. Select the <i>FortiAP</i> checkbox to enable central FortiAP management. This checkbox is selected by default. Select the <i>FortiSwitch</i> checkbox to enable central FortiSwitch management. This option is only available when the <i>Mode</i> is <i>Normal</i> .
<b>Default Device Selection for Install</b>	Select either <i>Select All</i> or <i>Deselect All</i> . This option is only available when the <i>Mode</i> is <i>Normal</i> .
<b>Perform Policy Check Before Every Install</b>	Turn <i>On</i> to perform a policy consistency check before every install. Only added or modified policies are checked. See <a href="#">Perform a policy consistency check on page 320</a> .
<b>Action When Conflicts Occur During Policy Check</b>	Select an action to take when a conflict occurs during the automatic policy consistency check, either <i>Continue Installation</i> or <i>Stop Installation</i> .
<b>Auto-Push Policy Packages When Device Back Online</b>	Automatically push policy package updates to currently offline managed devices when the devices come back online.
<b>Data Policy</b>	Specify how long to keep logs in the indexed and compressed states. This section is only available when FortiAnalyzer features are enabled. See <a href="#">FortiAnalyzer Features on page 29</a> .
<b>Keep Logs for Analytics</b>	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 <i>FortiView</i> , <i>Incidents &amp; Events/FortiSoC</i> , and <i>Reports</i> modules. After the specified length of time expires, Analytics logs are automatically purged from the SQL database.
<b>Keep Logs for Archive</b>	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 <i>FortiView</i> , <i>Incidents &amp; Events/FortiSoC</i> , or <i>Reports</i> modules. After the specified length of time expires, Archive logs are automatically deleted from the FortiManager unit.
<b>Disk Utilization</b>	Specify how much disk space to use for logs. This section is only available when FortiAnalyzer features are enabled. See <a href="#">FortiAnalyzer Features on page 29</a> .

<b>Maximum Allowed</b>	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.
<b>Analytics : Archive</b>	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 <i>Modify</i> checkbox to change the setting.
<b>Alert and Delete When Usage Reaches</b>	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 > All 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 754](#)). VDOMs cannot be assigned to multiple ADOMs.

### To assign VDOMs to an ADOM:

1. Go to *System Settings > All 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 759](#).

---

### 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 > Admin > Administrator*.
  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 > All 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 839](#)), 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 762](#).

### To delete an ADOM:

1. Go to *System Settings > All 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 > All 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:

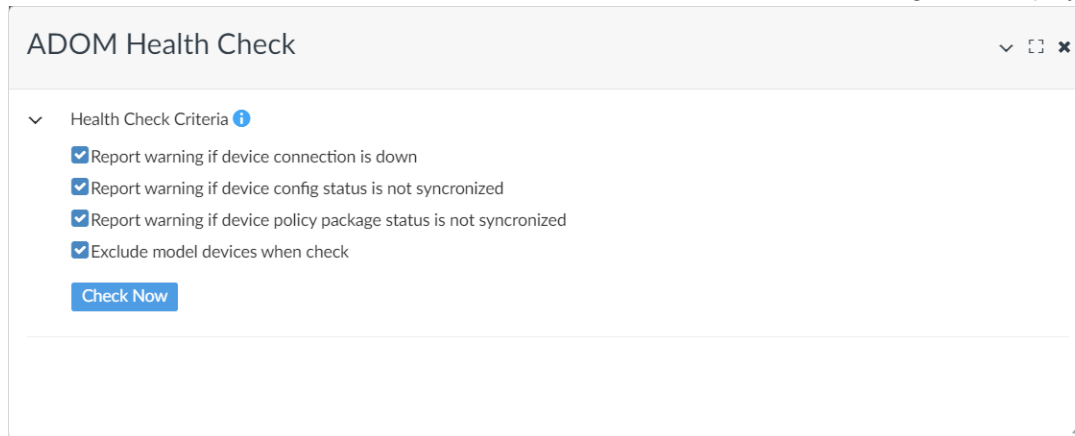
- Device connection is down.
- Device configuration status is not synchronized.
- Device policy package status is not synchronized.

You can also choose whether to exclude model devices from the health check.

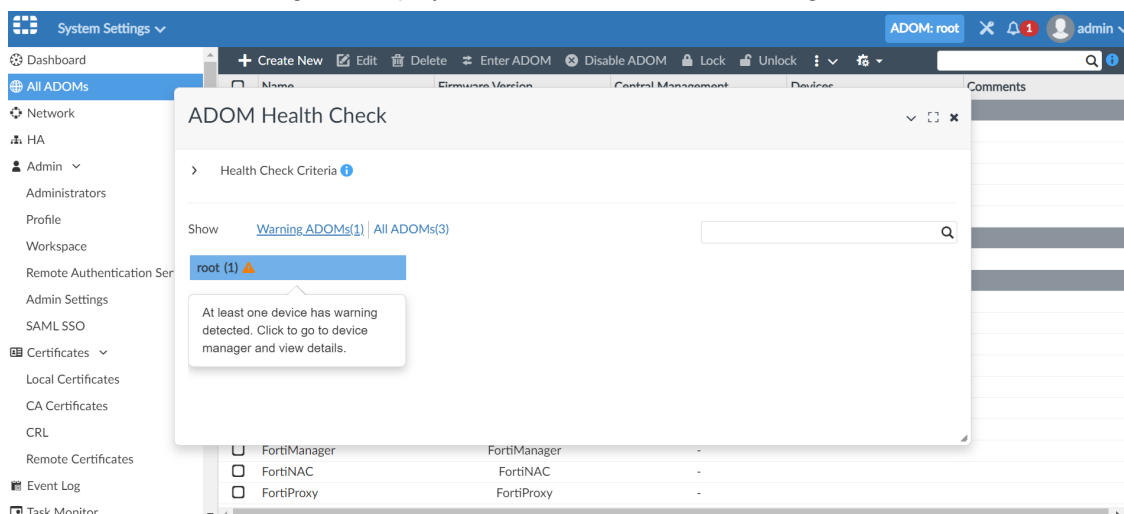
When the health check status is displayed, you can view what ADOMs contain problematic devices, and go directly to the *Device Manager* pane in the ADOM with problematic devices. You can also return to the *ADOM Health Check* dialog box, and continue checking ADOM statuses.

**To check ADOM health:**

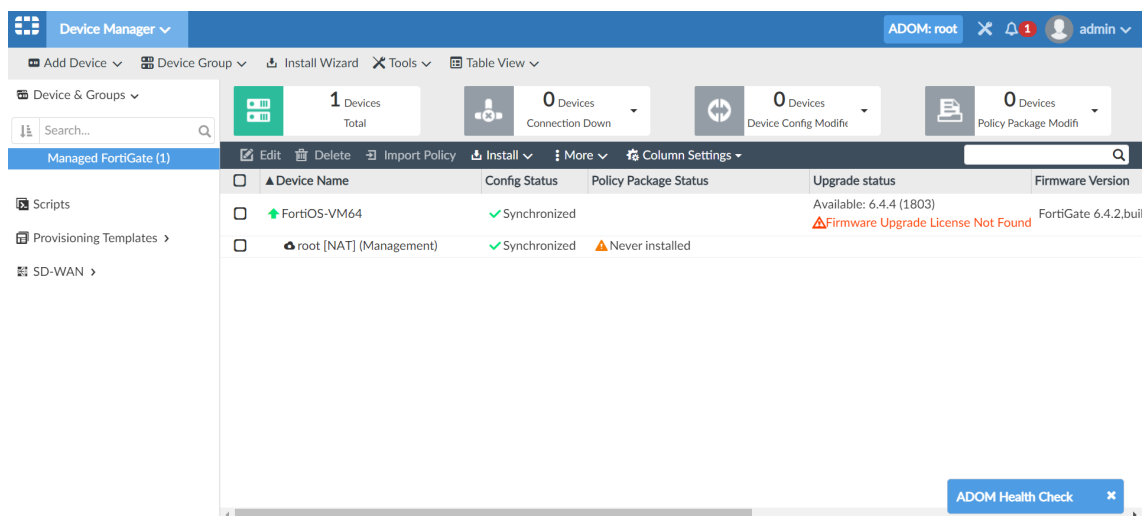
1. Go to *System Settings > All ADOMs*.
2. From the *More* menu, select *ADOM Health Check*. The *ADOM Health Check* dialog box is displayed.



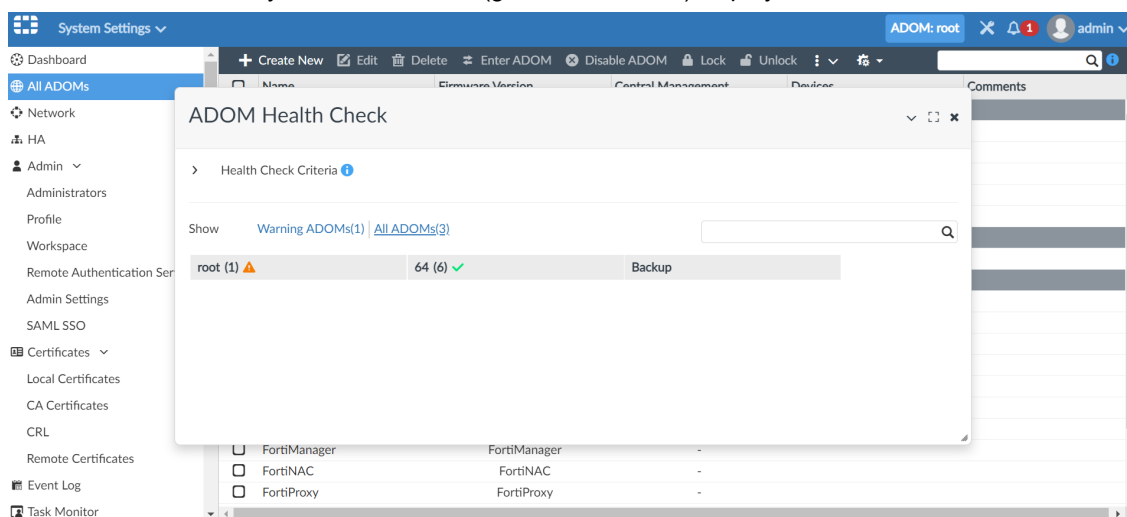
3. In the *Health Check Criteria* section, select what items to check, and click *Check Now*. The results of the check are displayed. In the following example, *Warning ADOMs <number>* is selected, and the list of ADOMs with warnings are displayed. The *root* ADOM has a warning.



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 is associated with a specific firmware version, based on the firmware version of the devices that are in that ADOM. This version is selected when creating a new ADOM. See [Creating ADOMs on page 759](#).

ADOM version N can manage devices with firmware version N. For example, ADOM version 6.4 can manage devices with firmware version 6.4.

When upgrading firmware for managed devices, ADOM version N can tolerate to manage devices with firmware version N+1. This is sometimes called mixed mode or migration mode. For example, ADOM version 7.0 can manage devices with firmware 7.0 and 7.2. This allows you to continue to manage an ADOM as normal while upgrading the devices within



that ADOM. Generally, you should upgrade the ADOM version from N to N+1 after all of the devices within the ADOM have been updated to firmware version N+1.



You can upgrade some ADOM versions without first updating all FortiGate units in the ADOM. For more information, see [Using mixed versions in ADOMs on page 771](#).

---

When adding a new FortiGate unit to an ADOM, the FortiGate unit should have the same FortiOS version as the ADOM.



You can use this feature to facilitate upgrading managed devices to new firmware. It is not recommended to permanently leave the ADOM with devices that contain a mix of firmware versions because of restrictions.

For example, you cannot use features from the higher firmware version, such as templates that reference syntax from the higher version. You also cannot import policies from devices that are running higher firmware versions than the ADOM version.

However installation to devices running higher firmware versions is supported.



For a complete list of supported devices and firmware versions, see the FortiManager Release Notes.

---

The general steps for upgrading an ADOM containing multiple devices running FortiOS 7.0 from 7.0 to 7.2 are as follows:

1. In the ADOM, upgrade one of the FortiGate units to FortiOS 7.2, and then resynchronize the device.  
All of the ADOM objects, including Policy Packages, remain as 7.0 objects.
2. Upgrade the rest of the FortiGate units in the ADOM to FortiOS 7.2.
3. Upgrade the ADOM to 7.2. See [Upgrading an ADOM on page 770](#) for more information.  
All of the database objects will be converted to 7.2 format, and the GUI content for the ADOM will change to reflect 7.2 features and behavior.



An ADOM can only be upgraded after all the devices within the ADOM have been upgraded.

---

## Global database version

The global database ADOM supports its own version plus one version. For example, if the global database ADOM version is 7.0, the global database ADOM can manage version 7.0 and 7.2, but not 6.4.

The global database is reset when the database version is edited. The database is not reset when the global database ADOM is upgraded using the *Upgrade* command.



The global database ADOM should only be upgraded after all the ADOMs that are using a global policy package have been upgraded.

**To upgrade the global database ADOM:**

1. Go to *System Settings > All 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:**

Editing the global database version will reset the database. All global policy packages will be lost. This should only be used when starting to use the global database for the first time, or when resetting the database is required.

---

1. Go to *System Settings > All 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 770](#)

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 848](#).

---

**To enable workspace mode, and disable concurrent ADOM access:**

1. Go to *Systems Settings > All 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*.

**Edit ADOM**

Name: FDS\_Update  
 Type: Fabric 6.4  
 Comments: 0/128

Devices: + Select Device [Search]

Name	IP Address	Platform
No Device.		

Mode: ☒ Normal ☐ Backup

Central Management: ☐ VPN ☒ FortiAP ☐ SD-WAN

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

Perform Policy Check Before Every Install: OFF

Auto-Push Policy Packages When Device Back Online: ☐ Enable ☒ Disable

Status: OK

Workspace Mode:

4. Click **OK**. Concurrent mode is disabled.

### To disable workspace mode, and enable concurrent ADOM access:

1. Go to *Systems Settings > All 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*.

**Edit ADOM**

Name: root  
 Type: FortiGate 6.4  
 Comments: 0/128

Devices: + Select Device [Search]

Name	IP Address	Platform
No Device.		

Mode: ☐ Normal ☐ Backup

Central Management: ☐ VPN ☒ FortiAP ☐ SD-WAN

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

Perform Policy Check Before Every Install: OFF

Auto-Push Policy Packages When Device Back Online: ☐ Enable ☒ Disable

Status: OK

Workspace Mode:

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 performing device-level changes to it, such as upgrading firmware for a device. If you are making changes at the ADOM level, you can leave the ADOM unlocked and lock policy packages or objects independently.

The padlock icon, shown next to the ADOM name on the banner and in the *All ADOMs* list, will turn from gray to green when you lock an ADOM. If it is red, it means that another administrator has locked the ADOM.

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 an ADOM:

- Ensure that you are in the specific ADOM that you will be editing (top right corner of the GUI), then select *Lock* from the banner.
- Or, go to *System Settings > All ADOMs*, right-click on an ADOM, and select *Lock* from the right-click menu.

The ADOM will now be locked, allowing you to make changes to it and preventing other administrators from making changes unless lock override is enabled. The lock icon will turn into a green locked padlock. For other administrators

### To unlock an ADOM:

- Ensure you have saved any changes you may have made to the ADOM then select *Unlock ADOM* from the banner.
- Or, go to *System Settings > All ADOMs*, right-click on an ADOM, and select *Lock* from the right-click menu.

If there are unsaved changes to the ADOM, a dialog box will give you the option of saving or discarding your changes before unlocking the ADOM. The ADOM will now be unlocked, allowing any administrator to lock the ADOM and make changes.

### To enable or disable ADOM lock override:

Enter the following CLI commands:

```
config system global  
    set lock-preempt {enable | disable}  
end
```

## Upgrading an ADOM

To upgrade an ADOM, you must be logged in as a super user administrator.



Typically, ADOMs are upgraded after all the devices within the ADOM have been upgraded. For information on upgrading an ADOM before all devices within the ADOM are upgraded, see [ADOM versions on page 766](#) and [Using mixed versions in ADOMs on page 771](#).

---



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 726](#).

### To upgrade an ADOM:

1. Go to *System Settings > All 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.

## Using mixed versions in ADOMs

FortiManager 7.2.3 supports mixed version ADOMs, allowing you to upgrade an ADOM's version without first being required to update the firmware of all devices in the ADOM.

See the table below for device firmware versions that are supported by each ADOM version:

ADOM Version	Device management support
6.4	Manage devices with firmware version 6.4, and 7.0.
7.0	Manage devices with firmware 6.4, 7.0, and 7.2.
7.2	Manage devices with firmware 7.0 and 7.2

You can upgrade the ADOM version before all of the devices within the ADOM have been updated.

The general steps for upgrading ADOM versions are as follows:

1. In the ADOM, update one or more of the FortiGate units to the new firmware version.  
For example, update the FortiGate from version 6.4 to 7.0, and then resynchronize the device. All of the ADOM objects, including Policy Packages, remain as 6.4 objects.
2. Upgrade the ADOM to the new ADOM version. See [Upgrading an ADOM on page 770](#) for more information.  
For example, upgrade the ADOM from version 6.4. to 7.0. All of the database objects will be converted to 7.0 format, and the GUI content for the ADOM will change to reflect 7.0 features and behavior.

After the ADOM is upgraded, you can install configuration changes to FortiGates running the same version or one version earlier. FortiManager ADOM versions 6.4 and 7.0 support mixed FortiOS versions by automatically downgrading the CLI syntax to the same version as the device when you install configuration changes to FortiGates running an earlier version of FortiOS.

Automatic downgrade of CLI syntax is handled as follows:

- New CLI syntax that does not exist in the previous version is discarded during downgrade and isn't used.
- Modified CLI syntax is reverted to the previous version's CLI syntax and used.
- Deleted CLI syntax is converted to the previous version's CLI syntax and uses the default values from that version.



Although you can install configuration changes to FortiGates running an earlier firmware version than the ADOM, the best practice is to install configuration changes to devices that are on the same version as the ADOM.



You cannot import configurations from devices on different firmware versions than the ADOM version. For example, the configuration of a FortiGate device on 7.0.x cannot be imported into a FortiManager 7.2 ADOM.

## 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* contain packages created with the objects from *Object Configurations*. You can also define firewall and traffic shaping header and footer policies. For more information, see [Creating policy packages on page 776](#).
  - *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 774](#).
  - *Object Configurations* contain all the pre-configured objects. You can also create new objects. For more information, see [Creating object configurations on page 772](#).

## 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 object configurations in Global Database:

1. Change the ADOM to *Global Database*.
2. Click *Object Configurations*. The Object Configuration pane shows the following object categories.
3. Click *Create New* to create new objects in each category.
  - Normalized Interface
    - Normalized Interface
    - Virtual Wire Pair
  - Firewall Objects
    - Addresses
    - Wildcard FQDN Addresses
    - Services
    - Schedules
    - Virtual IPs
    - IP Pools
    - Traffic Shapers
    - Shaping Profile

- Security Profiles
  - AntiVirus
  - Web Filter
  - Application Control
  - Intrusion Prevention
  - SSL/SSH Inspection
  - Application Signatures
  - IPS Signatures
- Fabric Connectors
  - SDN
  - Threat Feeds
  - Endpoint/Identity
- User & Authentication
  - User Definition
  - User Groups
  - LDAP Servers
  - RADIUS Servers
  - TACACS+ Servers
  - SMS Services
  - FortiTokens
- Script
  - Scripts

4. Click **OK** after creating the objects in each category.

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

## 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:

<b>Create New</b>	Create a new IPS header/footer.
<b>Edit</b>	Edit an existing IPS header/footer.
<b>Delete</b>	Delete an existing IPS header/footer.
<b>ADOM Assignments</b>	Specify to which ADOM(s) an IPS header/footer can be assigned.
<b>Assign/Un-assign</b>	Assign the IPS header/footer to one or more ADOMs. ADOMs will not appear in the <i>Assign/Un-assign</i> list unless they have first been specified using <i>ADOM Assignment</i> .  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.
<b>Column Settings</b>	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:

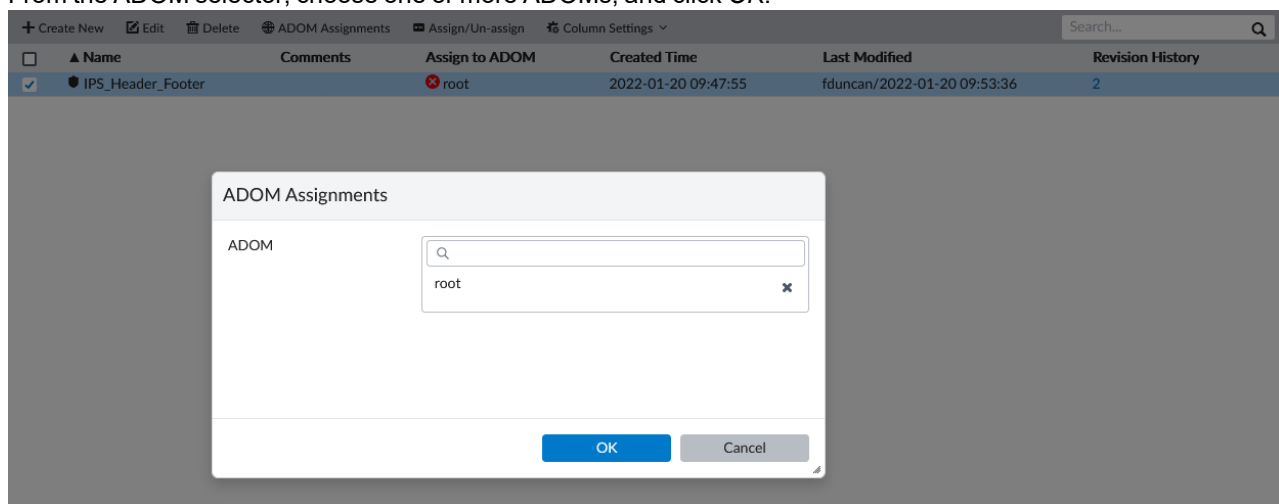
<b>Name</b>	Enter a name.
<b>Comments</b>	Optionally, enter comments about the IPS header/footer.
<b>IPS Signatures and Filters</b>	Click <i>Create new</i> , and select <i>Header IPS</i> or <i>Footer IPS</i> to create new IPS signatures and filters.
<b>Filters</b>	When creating filters, the following settings are available: <i>Action (Allow, Monitor, Block, Reset, Default, Quarantine)</i> , <i>Packet Logging</i> , <i>Status</i> , and <i>Filter</i> . Click the edit filter icon to create a new filter.  For information on hold-time and CVE filter options, see <a href="#">Intrusion prevention hold-time and CVE filtering on page 829</a> .



<b>Signatures</b>	When selecting signatures, the following settings are available: <i>Action (Allow, Monitor, Block, Reset, Default, Quarantine), Packet Logging, Status, Rate-based Setting, Exempt IPs, and Signatures</i> . Click <i>Add Signature</i> to select a new signature.
<b>Revision</b>	Enter a change note for any changes made to the IPS header/footer sensor. Previous changes are displayed under <i>Revision History</i> .

### To assign an IPS header/footer to an ADOM:

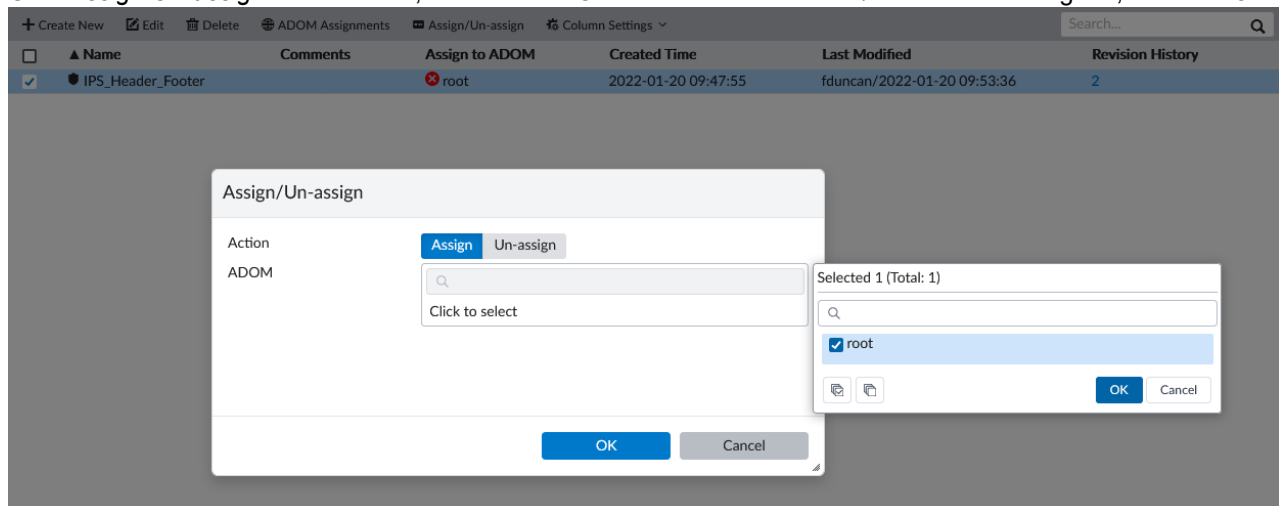
1. Change the ADOM to *Global Database*.
2. Click *Header/Footer IPS* from the navigation menu, and click *ADOM Assignments*. *ADOM Assignments* determines to which ADOM(s) an IPS header/footer can be assigned.
3. From the ADOM selector, choose one or more ADOMs, and click *OK*.



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.

+	Create New	Edit	Delete	ADOM Assignments	Assign/Un-assign	Column Settings	Search...
<input type="checkbox"/>	▲ Name	Comments	Assign to ADOM	Created Time	Last Modified	Revision History	
<input checked="" type="checkbox"/>	● IPS_Header_Footer		✖ root	2022-01-20 09:47:55	fduncan/2022-01-20 09:53:36	2	

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.

<div><div><div><div><div></div><div>Create New</div></div><div><div></div><div>Edit</div></div><div><div></div><div>Delete</div></div><div><div></div><div>ADOM Assignments</div></div><div><div></div><div>Assign/Un-assign</div></div><div><div></div><div>Column Settings</div></div></div><div><div>Search...</div><div></div></div></div></div>						
<input type="checkbox"/>	<div><div></div><div>Name</div></div>	Comments	Assign to ADOM	Created Time	Last Modified	Revision History
<input type="checkbox"/>	<div><div></div><div>IPS_Header_Footer</div></div>		<div><div></div><div>root</div></div>	2022-01-20 09:47:55	fduncan/2022-01-20 09:53:36	<div><div></div><div>2</div></div>

5. Navigate to the ADOM where the IPS header/footer was installed, and go to *Policy & Objects > Object Configurations > Intrusion Prevention*.

All new and existing Intrusion Prevention objects within this ADOM include the IPS headers and footers that were assigned to the ADOM.

**Edit IPS Sensor**

Name:

Comments:

Block malicious URLs: ☒

**IPS Signatures and Filters**

+ Create New Edit Delete Up Down Filter Search...					
<input type="checkbox"/>	Details	Exempt IPs	Action	Packet Logging	Status
<input type="checkbox"/>	Header IPS (1)				
<input type="checkbox"/>	Application: Ipswitch	0	Default	Disabled	Default
<input type="checkbox"/>	Local ADOM IPS (2)				
<input type="checkbox"/>	Severity: <span>medium</span> <span>high</span> <span>critical</span>	0	Block	Disabled	Enabled
<input type="checkbox"/>	Severity: <span>low</span>	0	Default	Disabled	Default
<input type="checkbox"/>	Footer IPS (1)				
<input type="checkbox"/>	2Wire.Wireless.Router.XSRF.Password.Reset 1024CMS.Standard.PHP.File.Inclusion	0	Default	Disabled	Default

**Botnet C&C**

Scan Outgoing Connections to Botnet Sites: Block Disable Monitor

**Advanced Options >**

OK Cancel

### 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 401](#).



NGFW 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 329](#).
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 329](#).

**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 313](#).

**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 121](#)

## 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 > Local 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 > Local Certificates*.
2. Click *Create New* 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:

<b>Certificate Name</b>	The name of the certificate.
<b>Subject Information</b>	Select the ID type from the dropdown list: <ul style="list-style-type: none"> <li>• <i>Host IP</i>: Select if the unit has a static IP address. Enter the public IP address of the unit in the <i>Host IP</i> field.</li> <li>• <i>Domain Name</i>: 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 <i>Domain Name</i> field.</li> <li>• <i>Email</i>: Select to use an email address. Enter the email address in the <i>Email Address</i> field.</li> </ul>
<b>Optional Information</b>	
<b>Organization Unit (OU)</b>	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.
<b>Organization (O)</b>	Legal name of the company or organization.
<b>Locality (L)</b>	Name of the city or town where the device is installed.
<b>State/Province (ST)</b>	Name of the state or province where the FortiGate unit is installed.
<b>Country (C)</b>	Select the country where the unit is installed from the dropdown list.
<b>E-mail Address (EA)</b>	Contact email address.

<b>Subject Alternative Name</b>	<p>Optionally, enter one or more alternative names for which the certificate is also valid. Separate names with a comma.</p> <p>A name can be:</p> <ul style="list-style-type: none"> <li>• e-mail address</li> <li>• IP address</li> <li>• URI</li> <li>• DNS name (alternatives to the Common Name)</li> <li>• directory name (alternatives to the Distinguished Name)</li> </ul> <p>You must precede the name with the name type. Examples:</p> <ul style="list-style-type: none"> <li>• IP:1.1.1.1</li> <li>• email:test@fortinet.com</li> <li>• email:my@other.address</li> <li>• URI:http://my.url.here/</li> </ul>
<b>Key Type</b>	The key type can be <i>RSA</i> or <i>Elliptic Curve</i> .
<b>Key Size</b>	Select the key size from the dropdown list: <i>512 Bit</i> , <i>1024 Bit</i> , <i>1536 Bit</i> , or <i>2048 Bit</i> . This option is only available when the key type is <i>RSA</i> .
<b>Curve Name</b>	Select the curve name from the dropdown list: <i>secp256r1</i> (default), <i>secp384r1</i> , or <i>secp521r1</i> . This option is only available when the key type is <i>Elliptic Curve</i> .
<b>Enrollment Method</b>	The enrollment method is set to <i>File Based</i> .

## Importing local certificates

### To import a local certificate:

1. Go to *System Settings > Certificates > Local Certificates*.
2. Click *Import* in the toolbar or right-click and select *Import*. The *Import* dialog box opens.
3. Enter the following information as required, then click *OK* to import the local certificate:

<b>Type</b>	Select the certificate type from the dropdown list: <i>Local Certificate</i> , <i>PKCS #12 Certificate</i> , or <i>Certificate</i> .
<b>Certificate File</b>	Click <i>Browse...</i> and locate the certificate file on the management computer, or drag and drop the file onto the dialog box.
<b>Key File</b>	<p>Click <i>Browse...</i> and locate the key file on the management computer, or drag and drop the file onto the dialog box.</p> <p>This option is only available when <i>Type</i> is <i>Certificate</i>.</p>
<b>Password</b>	<p>Enter the certificate password.</p> <p>This option is only available when <i>Type</i> is <i>PKCS #12 Certificate</i> or <i>Certificate</i>.</p>
<b>Certificate Name</b>	<p>Enter the certificate name.</p> <p>This option is only available when <i>Type</i> is <i>PKCS #12 Certificate</i> or <i>Certificate</i>.</p>

## Deleting local certificates

To delete a local certificate or certificates:

1. Go to *System Settings > Certificates > Local 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 > Local 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.

View Local Certificate	
Certificate Name	Fortinet_Local
Issuer	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress = support@fortinet.com
Subject	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiManager, CN = FMG-VM0000000000, emailAddress = support@fortinet.com
Valid From	2011-11-08 23:12:50 GMT
Valid To	2038-01-09 03:14:07 GMT
Version	3
Serial Number	71:cc:97
Extension	Name: X509v3 Basic Constraints Critical: no Content: CA:FALSE

OK

3. Click *OK* to return to the local certificates list.

## Downloading local certificates

To download a local certificate:

1. Go to *System Settings > Certificates > Local 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 > CA Certificates*.
2. Click *Import* in the toolbar, or right-click and select *Import*. The *Import* dialog box opens.
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 > CA 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 > CA 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 > CA 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 > CRL*.
2. Click *Import* in the toolbar, or right-click and select *Import*. The *Import* dialog box opens.
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 > CRL*.
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 > CRL*.
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.

Last 1 Day ▾		Add Filter		Apr 25 To Apr 26		Download		Raw Log		Historical Log	
#	Date Time	Level	User	Sub Type	Description	Operation	Performed On	Changes			
7	2021-04-26 12:27:39	notice	 admin	objcfg	cdb event log for object changed	edit	dev=global,ado...	type=fsp_managi 3.key=S108DVCI Apr 14 09:12:07			
8	2021-04-26 12:24:07	notice	 admin	objcfg	cdb event log for object changed	edit	dev=global,ado...	type=fsp_managi 3.key=S108DVVA Apr 14 09:12:48			
9	2021-04-26 12:24:07	notice	 admin	objcfg	cdb event log for object changed	edit	dev=global,ado...	type=fsp_managi 3.key=S108DVCI Apr 14 16:12:07			
10	2021-04-26 12:24:07	notice	 admin	objcfg	cdb event log for object changed	edit	dev=global,ado...	type=fsp_managi 3.key=S108DVVA Apr 14 16:27:32			
11	2021-04-26 12:21:10	notice	 admin	objcfg	cdb event log for object changed	edit	dev=global,ado...	type=fsp_managi 3.key=S108DVVA Apr 14 16:12:48			
12	2021-04-26 12:19:55	information	update_manager	fgd	Package update response from FortiGuard server received	Update Response	12.34.97.16	Receive an updat fds(00000.0000C 01000000ALCI0 version:00000.0C			
13	2021-04-26 12:09:41	information	update_manager	fgd	Package update response from FortiGuard server received	Update Response	12.34.97.16	Receive an updat fds(00000.0000C 01000000ALCI0 version:00000.0C			

The following options are available:

<b>Last...</b>	Select the amount of time to show from the available options, or select a custom time span or any time.
<b>Add Filter</b>	Filter the event log list based on the log level, user, sub type, or message. See <a href="#">Event log filtering on page 784</a> .
<b>Download</b>	Download the event logs in either CSV or the normal format to the management computer.
<b>Raw Log / Formatted Log</b>	Click on <i>Raw Log</i> to view the logs in their raw state. Click <i>Formatted Log</i> to view them in the formatted into a table.
<b>Historical Log</b>	Click to view the historical logs list.
<b>Back</b>	Click the back icon to return to the regular view from the historical view.
<b>View</b>	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.
<b>Delete</b>	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.
<b>Clear</b>	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.
<b>Type</b>	Select the type from the dropdown list: <ul style="list-style-type: none"> <li>Event Log</li> <li>FDS Upload Log: Select the device from the dropdown list.</li> <li>FDS Download Log: Select the service (FDS or FCT) from the <i>Service</i></li> </ul>

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:

<b>#</b>	The log number.
<b>Date/Time</b>	The date and time that the log file was generated.
<b>Level</b>	The severity level of the message. For a description of severity levels, see the <a href="#">Log Message Reference</a> .
<b>User</b>	The user that the log message relates to.
<b>Sub Type</b>	The event log subtype. For a description of the subtypes for event logs, see the <a href="#">Log Message Reference</a> .
<b>Description</b>	A description of the event.
<b>Operation</b>	The change or operation that triggered the event.
<b>Performed On</b>	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.
<b>Changes</b>	Details of the change.
<b>Message</b>	Log message details. A <i>Session ID</i> is added to each log message. The <i>username</i> 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:

- 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.
- 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 [Advanced Settings on page 804](#).

To filter the information in the monitor, enter a text string in the search field.

<div> <span>+</span> Group Error Devices           <span>🗑️</span> Delete           <span>🔍</span> View Task Detail           <span>📄</span> Show Status           <span>⚙️</span> Column Settings         </div> <div></div>									
<input type="checkbox"/>	ID	Source	Description	User	Status	Time Used	ADOM	Start Time	End Time
<input type="checkbox"/>	37	Install Configuration	Push config to device.	admin	<div><div></div></div> (80%)	14s	root	Tue Jan 28 2020 3:16:40 PM	N/A
<input type="checkbox"/>	36	Install Package	Install Package 'default'	admin	Success: 1	2s	root	Tue Jan 28 2020 3:16:37 PM	Tue Jan 28 2020 3:16:39 PM
<input type="checkbox"/>	35	Firmware Manager	Device Image Upgrade	admin	Success: 1	4m 1s	root	Tue Jan 28 2020 3:12:31 PM	Tue Jan 28 2020 3:16:32 PM
<input type="checkbox"/>	34	Device Manager	Add/delete Unauthorized Devices	Auto link	<div><div></div></div> (50%)	4m 40s	root	Tue Jan 28 2020 3:12:14 PM	N/A
<input type="checkbox"/>	33	Device Manager	pm devprof adom root default scope member	admin	Success: 1	4s	root	Tue Jan 28 2020 3:10:59 PM	Tue Jan 28 2020 3:11:03 PM
<input type="checkbox"/>	32	Device Manager	Add Device	admin	Success: 1	6s	root	Tue Jan 28 2020 3:10:52 PM	Tue Jan 28 2020 3:10:58 PM
<input type="checkbox"/>	31	Device Manager	Delete Device	admin	Success: 1	3s	root	Tue Jan 28 2020 3:10:12 PM	Tue Jan 28 2020 3:10:15 PM
<input type="checkbox"/>	30	Install Configuration	Push config to device.	admin	Success: 1	22s	root	Tue Jan 28 2020 2:55:17 PM	Tue Jan 28 2020 2:55:39 PM
<input type="checkbox"/>	29	Device Manager	Add/delete Unauthorized Devices	Auto link	Success: 1	43s	root	Tue Jan 28 2020 2:54:56 PM	Tue Jan 28 2020 2:55:39 PM
<input type="checkbox"/>	28	Device Manager	Add Device	admin	Success: 1	5s	root	Tue Jan 28 2020 2:54:18 PM	Tue Jan 28 2020 2:54:23 PM
<input type="checkbox"/>	27	Device Manager	Add/delete Unauthorized Devices	admin	Success: 1	2s	root	Tue Jan 28 2020 2:54:02 PM	Tue Jan 28 2020 2:54:04 PM
<input type="checkbox"/>	26	Device Manager	Delete Device	admin	Success: 1	3s	root	Tue Jan 28 2020 2:49:23 PM	Tue Jan 28 2020 2:49:26 PM
<input type="checkbox"/>	25	Install Configuration	Push config to device.	admin	Error: 1	32s	root	Tue Jan 28 2020 2:46:09 PM	Tue Jan 28 2020 2:46:41 PM
<input type="checkbox"/>	24	Install Package	Install Package 'default'	admin	Success: 1	2s	root	Tue Jan 28 2020 2:46:06 PM	Tue Jan 28 2020 2:46:08 PM

The following options are available:

<b>Group Error Devices</b>	Create a group of the failed devices, allowing for re-installations to be done only on the failed devices.
<b>Delete</b>	Remove the selected task or tasks from the list. This changes to <i>Cancel Running Task(s)</i> when <i>View</i> is <i>Running</i> .
<b>View Task Detail</b>	View the task <i>Index</i> , <i>Name</i> , <i>Status</i> , <i>Time Used</i> , and <i>History</i> , in a new window. Click the icons in the <i>History</i> column to view the following information: <ul style="list-style-type: none"> <li>History</li> <li>Promotion of device in FortiManager with autolink</li> <li>Upgrade remote device firmware</li> <li>Retrieve remote device configuration</li> <li>Installation of device templates</li> <li>Installation of policy packages</li> <li>Execution of additional scripts</li> </ul> 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.
<b>Show Status</b>	Select which tasks to view from the dropdown list, based on their status. The available options are: <i>All</i> , <i>Pending</i> , <i>Running</i> , <i>Canceling</i> , <i>Canceled</i> , <i>Done</i> , <i>Error</i> , <i>Aborting</i> , <i>Aborted</i> , and <i>Warning</i> .
<b>Column Settings</b>	Select the columns you want to display from the dropdown.

The following information is available:

<b>ID</b>	The identification number for a task.
<b>Source</b>	The platform from where the task is performed.
<b>Description</b>	The nature of the task. Double-click the task to display the specific actions taken under this task.
<b>User</b>	The user or users who performed the tasks.
<b>Status</b>	<p>The status of the task:</p> <ul style="list-style-type: none"> <li>• <i>Success</i>: Completed with success.</li> <li>• <i>Error</i>: Completed without success.</li> <li>• <i>Canceled</i>: User canceled the task.</li> <li>• <i>Canceling</i>: User is canceling the task.</li> <li>• <i>Aborted</i>: The FortiManager system stopped performing this task.</li> <li>• <i>Aborting</i>: The FortiManager system is stopping performing this task.</li> <li>• <i>Running</i>: Being processed. In this status, a percentage bar appears in the Status column.</li> <li>• <i>Pending</i></li> <li>• <i>Warning</i></li> </ul>
<b>Time Used</b>	The number of seconds to complete the task.
<b>ADOM</b>	The ADOM associated with the task.
<b>Start Time</b>	The time that the task was started.
<b>End Time</b>	The time that the task was completed.

## 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 > Advanced > SNMP* to configure the SNMP agent.

**SNMP**

SNMP Agent ☒ Enable

Description

Location

Contact

**Apply**

---

**SNMP v1/v2c**

+ Create New ☒ Edit ☐ Delete

Community Name	Queries	Traps	Enable
<input type="checkbox"/> Solara			<input checked="" type="checkbox"/>
<input type="checkbox"/> Terminus			<input checked="" type="checkbox"/>
<input type="checkbox"/> Trantor			<input checked="" type="checkbox"/>

---

**SNMP v3**

+ Create New ☒ Edit ☐ Delete

User Name	Security Level	Notification Hosts	Queries
<input type="checkbox"/> Bliss	No Authentication, No Privacy		
<input type="checkbox"/> Daneel	Authentication, No Privacy		
<input type="checkbox"/> Fallom	Authentication, Privacy		
<input type="checkbox"/> Golan	No Authentication, No Privacy		

The following information and options are available:

<b>SNMP Agent</b>	Select to enable the SNMP agent. When this is enabled, it sends FortiManager SNMP traps.
<b>Description</b>	Optionally, type a description of this FortiManager system to help uniquely identify this unit.
<b>Location</b>	Optionally, type the location of this FortiManager system to help find it in the event it requires attention.
<b>Contact</b>	Optionally, type the contact information for the person in charge of this FortiManager system.
<b>SNMP v1/2c</b>	The list of SNMP v1/v2c communities added to the FortiManager configuration.
<b>Create New</b>	Select <i>Create New</i> to add a new SNMP community. If SNMP agent is not selected, this control will not be visible. For more information, see <a href="#">SNMP v1/v2c communities on page 788</a> .
<b>Edit</b>	Edit the selected SNMP community.
<b>Delete</b>	Delete the selected SNMP community or communities.
<b>Community Name</b>	The name of the SNMP community.
<b>Queries</b>	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.
<b>Traps</b>	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.

<b>Enable</b>	Enable or disable the SNMP community.
<b>SNMP v3</b>	The list of SNMPv3 users added to the configuration.
<b>Create New</b>	Select <i>Create New</i> to add a new SNMP user. If SNMP agent is not selected, this control will not be visible. For more information, see <a href="#">SNMP v3 users on page 791</a> .
<b>Edit</b>	Edit the selected SNMP user.
<b>Delete</b>	Delete the selected SNMP user or users.
<b>User Name</b>	The user name for the SNMPv3 user.
<b>Security Level</b>	The security level assigned to the SNMPv3 user.
<b>Notification Hosts</b>	The notification host or hosts assigned to the SNMPv3 user.
<b>Queries</b>	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 > Advanced > SNMP* and ensure the SNMP agent is enabled.
2. In the *SNMP v1/v2c* section, click *Create New* in the toolbar. The *New SNMP Community* pane opens.

**New SNMP Community**

Protocol	Port	Enable
v1	161	<input checked="" type="checkbox"/>
v2c	161	<input checked="" type="checkbox"/>


Traps:

Protocol	Port	Enable
v1	162	<input checked="" type="checkbox"/>
v2c	162	<input checked="" type="checkbox"/>

SNMP Event	Enable
Interface IP changed	<input checked="" type="checkbox"/>
Log Disk Space Low	<input checked="" type="checkbox"/>
CPU Overuse	<input checked="" type="checkbox"/>
Memory Low	<input checked="" type="checkbox"/>
System Restart	<input checked="" type="checkbox"/>
CPU usage exclude NICE threshold	<input checked="" type="checkbox"/>
HA Failover	<input checked="" type="checkbox"/>
RAID Event	<input checked="" type="checkbox"/>
Power Supply Failed	<input checked="" type="checkbox"/>
Fan Speed Out Of Range	<input checked="" type="checkbox"/>
Temperature Out Of Range	<input checked="" type="checkbox"/>
Voltage Out Of Range	<input checked="" type="checkbox"/>

OK Cancel

3. Configure the following options, then click *OK* to create the community.

<b>Name</b>	Enter a name to identify the SNMP community. This name cannot be edited later.
<b>Hosts</b>	<p>The list of hosts that can use the settings in this SNMP community to monitor the FortiManager system.</p> <p>When you create a new SNMP community, there are no host entries. Select <i>Add</i> to create a new entry that broadcasts the SNMP traps and information to the network connected to the specified interface.</p>
<b>IP Address/Netmask</b>	<p>Enter the IP address and netmask of an SNMP manager.</p> <p>By default, the IP address is 0.0.0.0 so that any SNMP manager can use this SNMP community.</p>
	<div>  <p>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)</p> </div>

<b>Interface</b>	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.
<b>Delete</b>	Click the delete icon to remove this SNMP manager entry.
<b>Add</b>	Select to add another entry to the Hosts list. Up to eight SNMP manager entries can be added for a single community.
<b>Queries</b>	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.
<b>Traps</b>	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.
<b>SNMP Event</b>	<p>Enable the events that will cause SNMP traps to be sent to the community.</p> <ul style="list-style-type: none"> <li>• <i>Interface IP changed</i></li> <li>• <i>Log disk space low</i></li> <li>• <i>CPU Overuse</i></li> <li>• <i>Memory Low</i></li> <li>• <i>System Restart</i></li> <li>• <i>CPU usage exclude NICE threshold</i></li> <li>• <i>HA Failover</i></li> <li>• <i>RAID Event</i> (only available for devices that support RAID)</li> <li>• <i>Power Supply Failed</i> (only available on supported hardware devices)</li> <li>• <i>Fan Speed Out of Range</i></li> <li>• <i>Temperature Out of Range</i></li> <li>• <i>Voltage Out of Range</i></li> </ul> <p>FortiAnalyzer feature set SNMP events:</p> <ul style="list-style-type: none"> <li>• <i>High licensed device quota</i></li> <li>• <i>High licensed log GB/day</i></li> <li>• <i>Log Alert</i></li> <li>• <i>Log Rate</i></li> <li>• <i>Data Rate</i></li> </ul>

#### To edit an SNMP community:

1. Go to *System Settings > Advanced > SNMP*.
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 > Advanced > SNMP*.
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 > Advanced > SNMP* and ensure the SNMP agent is enabled.
2. In the *SNMP v3* section, click *Create New* in the toolbar. The *New SNMP User* pane opens.

**New SNMP User**

User Name:

Security Level: No Authentication, No Privacy ▼

Queries: ☐ Enable Port:

Notification Hosts:  +

SNMP Event	Enable
Interface IP changed	<input checked="" type="checkbox"/>
Log Disk Space Low	<input checked="" type="checkbox"/>
CPU Overuse	<input checked="" type="checkbox"/>
Memory Low	<input checked="" type="checkbox"/>
System Restart	<input checked="" type="checkbox"/>
CPU usage exclude NICE threshold	<input checked="" type="checkbox"/>
HA Failover	<input checked="" type="checkbox"/>
RAID Event	<input checked="" type="checkbox"/>
Power Supply Failed	<input checked="" type="checkbox"/>
Fan Speed Out Of Range	<input checked="" type="checkbox"/>
Temperature Out Of Range	<input checked="" type="checkbox"/>
Voltage Out Of Range	<input checked="" type="checkbox"/>

OK Cancel

3. Configure the following options, then click *OK* to create the community.

<b>User Name</b>	The name of the SNMP v3 user.
<b>Security Level</b>	<p>The security level of the user. Select one of the following:</p> <ul style="list-style-type: none"> <li>• <i>No Authentication, No Privacy</i></li> <li>• <i>Authentication, No Privacy</i>: Select the <i>Authentication Algorithm</i> (SHA1, MD5) and enter the password.</li> <li>• <i>Authentication, Privacy</i>: Select the <i>Authentication Algorithm</i> (SHA1, MD5), the <i>Private Algorithm</i> (AES, DES), and enter the passwords.</li> </ul>
<b>Queries</b>	Select to enable queries then enter the port number. The default port is 161.
<b>Notification Hosts</b>	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 > Advanced > SNMP*.
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 > Advanced > SNMP*.
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.

## 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.

MIB file name or RFC	Description
<b>FORTINET-CORE-MIB.mib</b>	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.
<b>FORTINET-FORTIMANAGER-MIB.mib</b>	The proprietary FortiManager MIB includes system information and trap information for FortiManager units.
<b>RFC-1213 (MIB II)</b>	The Fortinet SNMP agent supports MIB II groups with the following exceptions. <ul style="list-style-type: none"> <li>• No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10).</li> <li>• 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.</li> </ul>
<b>RFC-2665 (Ethernet-like MIB)</b>	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.

Trap message	Description
<b>ColdStart, WarmStart, LinkUp, LinkDown</b>	Standard traps as described in RFC 1215.
<b>CPU usage high (fnTrapCpuThreshold)</b>	CPU usage exceeds the set percent. This threshold can be set in the CLI using the following commands: <pre>config system snmp sysinfo     set trap-high-cpu-threshold &lt;percentage value&gt; end</pre>
<b>CPU usage excluding NICE processes (fmSysCpuUsageExcludedNice)</b>	CPU usage excluding NICE processes exceeds the set percentage. This threshold can be set in the CLI using the following commands: <pre>config system snmp sysinfo     set trap-cpu-high-exclude-nice-threshold &lt;percentage value&gt; end</pre>
<b>Memory low</b>	Memory usage exceeds 90 percent. This threshold can be set in the CLI using the following commands:

Trap message	Description
<b>(fnTrapMemThreshold)</b>	<pre>config system snmp sysinfo   set trap-low-memory-threshold &lt;percentage value&gt; end</pre>
<b>Log disk too full (fnTrapLogDiskThreshold)</b>	Log disk usage has exceeded the configured threshold. Only available on devices with log disks.
<b>Temperature too high (fnTrapTempHigh)</b>	A temperature sensor on the device has exceeded its threshold. Not all devices have thermal sensors. See manual for specifications.
<b>Voltage outside acceptable range (fnTrapVoltageOutOfRange)</b>	Power levels have fluctuated outside of normal levels. Not all devices have voltage monitoring instrumentation.
<b>Power supply failure (fnTrapPowerSupplyFailure)</b>	Power supply failure detected. Available on some devices that support redundant power supplies.
<b>Interface IP change (fnTrapIpChange)</b>	The IP address for an interface has 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.
<b>HA switch (fnTrapHASwitch)</b>	FortiManager HA cluster has been re-arranged. A new primary has been selected and asserted.

## 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
<b>fnSysSerial</b>	Fortinet unit serial number.

### Administrator accounts:

MIB field	Description
<b>fnAdminNumber</b>	The number of administrators on the Fortinet unit.

MIB field	Description
<b>fnAdminTable</b>	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
<b>fnMessages</b>	The number of custom messages on the Fortinet unit.

**MIB fields and traps**

MIB field	Description
<b>fmModel</b>	A table of all FortiManager models.
<b>fmTrapHASwitch</b>	The FortiManager HA cluster has been re-arranged. A new primary has been selected and asserted.

## Mail Server

A mail server allows the FortiManager to send 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.

<b>SMTP Server Name</b>	Enter a name for the SMTP server.
<b>Mail Server</b>	Enter the mail server information.
<b>SMTP Server Port</b>	Enter the SMTP server port number. The default port is 25.
<b>Enable Authentication</b>	Enable or disable authentication.
<b>Email Account</b>	Enter an email account. This option is only accessible when authentication is enabled.
<b>Password</b>	Enter the email account password. This option is only accessible when authentication is enabled.

**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 798](#).



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.

Create New Syslog Server Settings

Name	<input type="text"/>
IP address (or FQDN)	<input type="text"/>
Syslog Server Port	<input type="text" value="514"/>
Reliable Connection	<input type="checkbox"/>

OK Cancel

3. Configure the following settings and then select *OK* to create the syslog server.

<b>Name</b>	Enter a name for the syslog server.
<b>IP address (or FQDN)</b>	Enter the IP address or FQDN of the syslog server.
<b>Syslog Server Port</b>	Enter the syslog server port number. The default port is 514.
<b>Reliable Connection</b>	Enable or disable a reliable connection with the syslog server. The default is <i>disable</i> .
<b>Secure Connection</b>	Enable/disable connection secured by TLS/SSL. The default is <i>disable</i> . This option is only available when <i>Reliable Connection</i> is enabled.
<b>Local Certificate CN</b>	Enter one of the available local certificates used for secure connection: <i>Fortinet_Local</i> or <i>Fortinet_Local2</i> . The default is <i>Fortinet_Local</i> . This option is only available when <i>Secure Connection</i> is enabled.
<b>Peer Certificate CN</b>	Enter the certificate common name of syslog server. Null means no certificate CN for the syslog server. This option is only available when <i>Secure Connection</i> is enabled.

### To enable sending FortiManager local logs to 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 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 797](#).

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 437](#).

---



+ Create New Edit Delete Collapse All Expand All Column Settings				
<input type="checkbox"/> Meta Fields	Length	Importance	Status	
▼ System Administrator (2)				
<input type="checkbox"/> Contact Email	50	Optional	Enabled	
<input type="checkbox"/> Contact Phone	50	Optional	Enabled	
▼ Device (5)				
<input type="checkbox"/> Company/Organization	50	Optional	Enabled	
<input type="checkbox"/> Contact Email	50	Optional	Enabled	
<input type="checkbox"/> Contact Phone Number	50	Optional	Enabled	
<input type="checkbox"/> Address	150	Optional	Enabled	
<input type="checkbox"/> storenumber	20	Required	Enabled	
▼ Device Group (0)				
▼ Device VDOM (0)				
▼ Administrative Domain (0)				
▼ Firewall Address (0)				
▼ Firewall Address Group (0)				
▼ Central NAT (0)				
▼ Firewall Service (0)				
▼ Firewall Service Group (0)				
▼ Firewall Policy (0)				



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.

Create New Meta Fields

Object

System Administrator

Name

test

Length

20

Importance

☐ Optional
 ☒ Required

Status

☐ Disabled
 ☒ Enabled

Variable

\$(test)

OK

Cancel

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*.

<b>Importance</b>	Select <i>Required</i> to make the field compulsory; otherwise, select <i>Optional</i> .
<b>Status</b>	Select <i>Disabled</i> to disable this field. The default selection is <i>Enabled</i> . This field is only available for non-firewall objects.

- Click *OK*.  
The meta field is created.

#### To edit a meta field:

- Go to *System Settings > Advanced > Meta Fields*.
- 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.
- 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:

- Go to *System Settings > Advanced > Meta Fields*.
- Select the field or fields you need to delete.
- Click *Delete* in the toolbar, or right-click and select *Delete*.
- 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.gz
```

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 29](#).

## 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	
<b>Roll log file when size exceeds</b>	Enter the log file size, from 10 to 500MB. Default: 200MB.
<b>Roll log files at scheduled time</b>	Select to roll logs daily or weekly. <ul style="list-style-type: none"> <li><i>Daily</i>: select the hour and minute value in the dropdown lists.</li> <li><i>Weekly</i>: select the day, hour, and minute value in the dropdown lists.</li> </ul>
<b>Upload logs using a standard file transfer protocol</b>	Select to upload logs and configure the following settings.
<b>Upload Server Type</b>	Select one of <i>FTP</i> , <i>SFTP</i> , or <i>SCP</i> .

<b>Upload Server IP</b>	Enter the IP address of the upload server.
<b>User Name</b>	Enter the username used to connect to the upload server.
<b>Password</b>	Enter the password used to connect to the upload server.
<b>Remote Directory</b>	Enter the remote directory on the upload server where the log will be uploaded.
<b>Upload Log Files</b>	Select to upload log files when they are rolled according to settings selected under <i>Roll Logs</i> , or daily at a specific hour.
<b>Upload rolled files in gzip file format</b>	Select to gzip the logs before uploading. This will result in smaller logs and faster upload times.
<b>Delete files after uploading</b>	Select to remove device log files from the FortiManager system after they have been uploaded to the Upload Server.
<b>Local Device Log</b>	
<b>Send the local event logs to FortiAnalyzer / FortiManager</b>	Select to send local event logs to another FortiAnalyzer or FortiManager device.
<b>IP Address</b>	Enter the IP address of the FortiAnalyzer or FortiManager.
<b>Upload Option</b>	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.
<b>Severity Level</b>	Select the minimum log severity level from the dropdown list. This option is only available when <i>Upload Option</i> is <i>Realtime</i> .
<b>Reliable log transmission</b>	Select to use reliable log transmission.
<b>Secure connection</b>	Select to use a secure connection for log transmission. This option is only available when <i>Reliable log transmission</i> is selected.

## 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
```

## File Management

FortiManager allows you to configure automatic deletion of device log files, quarantined files, reports, and content archive files after a set period of time.

Go to *System Settings > Advanced > File Management* to configure file management settings.

**File Management**

**Automatically Delete**

<input type="checkbox"/> Device log files older than	365	Days	Scheduled daily at time	00:00
<input type="checkbox"/> Reports older than	365	Days	Scheduled daily at time	00:00
<input type="checkbox"/> Content archive files older than	365	Days	Scheduled daily at time	00:00
<input type="checkbox"/> Quarantined files older than	365	Days	Scheduled daily at time	00:00

Apply

Configure the following settings, and then select *Apply*:

<b>Device log files older than</b>	Select to enable automatic deletion of compressed log files. Enter a value in the text field, select the time period ( <i>Days</i> , <i>Weeks</i> , or <i>Months</i> ), and choose a time of day.
<b>Reports older than</b>	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.
<b>Content archive files older than</b>	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.
<b>Quarantined files older than</b>	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.

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.




This pane is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 29](#).

## Advanced Settings

Go to *System Settings > Advanced > Advanced Settings* to view and configure advanced settings and download WSDL files.

Configure the following settings and then select *Apply*:

<b>Offline Mode</b>	Enabling <i>Offline Mode</i> 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.
<b>ADOM Mode</b>	<p>Select the ADOM mode, either <i>Normal</i> or <i>Advanced</i>.</p> <p>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.</p> <hr/> <div>  <p>Advanced ADOM mode cannot be enabled when a remote FortiAnalyzer is being managed by FortiManager.</p> </div> <hr/>
<b>Download WSDL file</b>	<p>Select the required WSDL functions then click the <i>Download</i> button to download the WSDL file to your management computer.</p> <p>When selecting <i>Legacy Operations</i>, no other options can be selected.</p> <p>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.</p>
<b>Chassis Management</b>	Enable chassis management, then enter the chassis update interval, from 4 to 1440 minutes. Default: 15 minutes.
<b>Configuration Changes Received from FortiGate</b>	Select to either automatically accept changes (default) or to prompt the administrator to accept the changes.
<b>Task List Size</b>	Set a limit on the size of the task list. Default: 2000.
<b>Verify Installation</b>	Select to preview the installation before proceeding.
<b>Allow Install Interface Policy Only</b>	Select to manage and install only interface based policies, instead of all device and policy configuration.
<b>Display Policy &amp; Objects in Dual Pane</b>	Enable to display both the <i>Policy Packages</i> and <i>Object Configurations</i> tabs on a single pane in the <i>Policy &amp; Objects</i> module. See <a href="#">Feature visibility on page 309</a> .
<b>Display Device/Group tree view in Device Manager</b>	Enable to display devices and groups within a single tree menu and include <i>Add Device</i> and <i>Install Wizard</i> commands in the right-click menu.

## 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 *System Settings > 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 *System Settings > 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. <ul style="list-style-type: none"><li>• &lt;adom&gt;: The ADOM name.</li><li>• &lt;version&gt;: The ADOM version.</li><li>• &lt;mr&gt;: The major release number.</li><li>• &lt;ostype&gt;: Supported OS type.</li></ul>



Variable	Description
<code>all-except-ip</code>	Reset all settings except the current IP address and route information.
<code>all-settings</code>	Reset to factory default settings.
<code>all-shutdown</code>	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.

# Administrators

The *System Settings > Admin* menu enables 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 877](#) for more information.

In workflow mode, approval matrices can be create and managed on the *Approval Matrix* pane. See [Workflow approval on page 857](#) for more information.

This section contains the following topics:

- [Trusted hosts on page 808](#)
- [Monitoring administrators on page 809](#)
- [Disconnecting administrators on page 809](#)
- [Managing administrator accounts on page 809](#)
- [Administrator profiles on page 839](#)
- [Authentication on page 864](#)
- [Global administration settings on page 877](#)
- [Two-factor authentication on page 883](#)

## 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 *System Settings > 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:

<b>User Name</b>	The name of the administrator account. Your session is indicated by <i>(current)</i> .
<b>IP Address</b>	The IP address where the administrator is logging in from. This field also displays the logon type (GUI, jsconsole, or SSH).
<b>Start Time</b>	The date and time the administrator logged in.
<b>Time Out (mins)</b>	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 *System Settings > 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 > Admin > Administrator* 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.

+ Create New Edit Clone Delete Table View Column Settings							
Seq.#	Name	Type	Profile	ADOMs	Policy Packages	Trusted IPv4 Hosts	
1	123456	LOCAL	Super_User	All ADOMs	All Packages	0.0.0.0/0.0.0.0	
2	Blue	Restricted Admin LOCAL	qwer	FG60		0.0.0.0/0.0.0.0	
3	PKI	PKI	Standard_User	All ADOMs	52to56:default FG60:default FG60:Root/FortiGate-VM64_root	0.0.0.0/0.0.0.0	
4	Restrict	LOCAL	Restricted_User	All ADOMs	All Packages	0.0.0.0/0.0.0.0	
5	admin	LOCAL	Super_User	All ADOMs	All Packages	0.0.0.0/0.0.0.0	
6	dap	LDAP Wildcard	Standard_User	FG60 fg56 fg54 root	fg54:default root:default fg56:default FG60:Packages/FortiGate-VM64	0.0.0.0/0.0.0.0	
7	new	LOCAL	Package_User	Exclude: FG60	root:FortiGate-VM64_root root:Model1 Global:default	0.0.0.0/0.0.0.0	
8	red	LOCAL	Super_User	All ADOMs	All Packages	0.0.0.0/0.0.0.0	
9	riemann	LDAP Wildcard	Restricted_User	All ADOMs	All Packages	0.0.0.0/0.0.0.0	
10	test	LOCAL	Super_User	All ADOMs	All Packages	0.0.0.0/0.0.0.0	

The following options are available:

<b>Create New</b>	Create a new administrator. See <a href="#">Creating administrators on page 811</a> .
<b>Edit</b>	Edit the selected administrator. See <a href="#">Editing administrators on page 816</a> .
<b>Clone</b>	Clone the selected administrator.
<b>Delete</b>	Delete the selected administrator or administrators. See <a href="#">Deleting administrators on page 816</a> .
<b>Table View/Tile View</b>	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.
<b>Column Settings</b>	Change the displayed columns.
<b>Search</b>	Search the administrators.
<b>Change Password</b>	Change the selected administrator's password. This option is only available from the right-click menu. See <a href="#">Editing administrators on page 816</a> .

The following information is shown:

<b>Seq.#</b>	The sequence number.
<b>Name</b>	The name the administrator uses to log in.
<b>Type</b>	The user type, as well as if the administrator uses a wildcard.
<b>Profile</b>	The profile applied to the administrator. See <a href="#">Administrator profiles on page 839</a> If a profile is applied per-ADOM for the administrator, they are listed as <i>ADOM:profile</i> .
<b>ADOMs</b>	The ADOMs the administrator has access to or is excluded from.
<b>Policy Packages</b>	The policy packages the administrator can access.

<b>Comments</b>	Comments about the administrator account. This column is hidden by default.
<b>Trusted IPv4 Hosts</b>	The IPv4 trusted host(s) associated with the administrator. See <a href="#">Trusted hosts on page 808</a> .
<b>Trusted IPv6 Hosts</b>	The IPv6 trusted host(s) associated with the administrator. See <a href="#">Trusted hosts on page 808</a> . This column is hidden by default.
<b>Contact Email</b>	The contact email associated with the administrator. This column is hidden by default.
<b>Contact Phone</b>	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 864](#) for details.

---

**To create a new administrator:**

1. Go to *System Settings > Admin > Administrators*.
2. In the toolbar, click *Create New* to display the *New Administrator* pane.

## Create New Administrator

User Name	<input type="text"/>
Avatar	<input type="button" value="+ Add Photo"/> <input type="button" value="- Remove Photo"/>
Description	<div></div>
Admin Type	LOCAL <input type="button" value="v"/>
New Password	<input type="password"/> <input type="button" value="v"/>
Confirm Password	<input type="password"/> <input type="button" value="v"/>
FortiToken Cloud	<input checked="" type="button" value="Disable"/> <input type="button" value="FortiToken Mobile"/> <input type="button" value="Email"/> <input type="button" value="SMS"/>
Administrative Domain	<input checked="" type="button" value="All ADOMs"/> <input type="button" value="All ADOMs except specified ones"/> <input type="button" value="Specify"/>
Admin Profile	Restricted_User <input type="button" value="v"/>
Policy Package	<input checked="" type="button" value="All Packages"/> <input type="button" value="Specify"/>
JSON API Access	None <input type="button" value="v"/>
Theme Mode	<input checked="" type="button" value="Use Global Theme"/> <input type="button" value="Use Own Theme"/>
Trusted Hosts	<input type="checkbox"/>

## Meta Fields &gt;

## Advanced Options v

change-password	enable <input type="button" value="v"/>
ext-auth-accprofile-override	disable <input type="button" value="v"/>
ext-auth-adom-override	disable <input type="button" value="v"/>
ext-auth-group-match	undefined <input type="button" value="v"/>
fingerprint	undefined <input type="button" value="v"/>
first-name	undefined <input type="button" value="v"/>
last-name	undefined <input type="button" value="v"/>
login-max	32 <input type="button" value="v"/>
pager-number	undefined <input type="button" value="v"/>

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.

<b>Avatar</b>	<p>Apply a custom image to the administrator.</p> <p>Click <i>Add Photo</i> to select an image already loaded to the FortiManager, or to load an new image from the management computer.</p> <p>If no image is selected, the avatar will use the first letter of the user name.</p>
<b>Comments</b>	<p>Optionally, enter a description of the administrator, such as their role, location, or the reason for their account.</p>
<b>Admin Type</b>	<p>Select the type of authentication the administrator will use when logging into the FortiManager unit. One of: <i>LOCAL</i>, <i>RADIUS</i>, <i>LDAP</i>, <i>TACACS+</i>, <i>PKI</i>, <i>Group</i>, or <i>SSO</i>. See <a href="#">Authentication on page 864</a> for more information.</p>
<b>Server or Group</b>	<p>Select the RADIUS server, LDAP server, TACACS+ server, or group, as required.</p> <p>The server must be configured prior to creating the new administrator.</p> <p>This option is not available if the <i>Admin Type</i> is <i>LOCAL</i> or <i>PKI</i>.</p>
<b>Match all users on remote server</b>	<p>Select this option to automatically add all users from a LDAP server specified in <i>Admin&gt;Remote Authentication Server</i>. All users specified in the <i>Distinguished Name</i> field in the LDAP server will be added as FortiManager users with the selected Admin Profile.</p> <p>Select this option when the <i>Admin Type</i> is <i>SSO</i> 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 <a href="#">SAML admin authentication on page 872</a>.</p> <p>If this option is not selected, the <i>User Name</i> specified must exactly match the LDAP user specified on the LDAP server.</p> <p>This option is not available if the <i>Admin Type</i> is <i>LOCAL</i> or <i>PKI</i>.</p>
<b>Subject</b>	<p>Enter a comment for the PKI administrator.</p> <p>This option is only available if the <i>Admin Type</i> is <i>PKI</i>.</p>
<b>CA</b>	<p>Select the CA certificate from the dropdown list.</p> <p>This option is only available if the <i>Admin Type</i> is <i>PKI</i>.</p>
<b>Required two-factor authentication</b>	<p>Select to enable two-factor authentication.</p> <p>This option is only available if the <i>Admin Type</i> is <i>PKI</i>.</p>
<b>New Password</b>	<p>Enter the password.</p> <p>This option is not available if <i>Match all users on remote server</i> is selected.</p> <p>If the <i>Admin Type</i> is <i>PKI</i>, this option is only available when <i>Require two-factor authentication</i> is selected.</p> <p>If the <i>Admin Type</i> is <i>RADIUS</i>, <i>LDAP</i>, or <i>TACACS+</i>, the password is only used when the remote server is unreachable.</p>
<b>Confirm Password</b>	<p>Enter the password again to confirm it.</p> <p>This option is not available if <i>Match all users on remote server</i> is selected.</p>

	If the <i>Admin Type</i> is <i>PKI</i> , this option is only available when <i>Require two-factor authentication</i> is selected.
<b>Force this administrator to change password upon next log on.</b>	<p>Force the administrator to change their password the next time that they log in to the FortiManager.</p> <p>This option is only available if <i>Password Policy</i> is enabled in <i>Admin Settings</i>. See <a href="#">Password policy on page 880</a>.</p>
<b>FortiToken Cloud</b>	<p>Enable or disable two-factor authentication with FortiToken Cloud, then select the token delivery method from the following options:</p> <ul style="list-style-type: none"> <li>• <i>FortiToken Mobile</i>: 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.</li> <li>• <i>Email</i>: Receive the token by email.</li> <li>• <i>SMS</i>: Receive the token by SMS message.</li> </ul> <p>This option is not available if Admin Type is set to <i>PKI</i> or <i>SSO</i>. See <a href="#">Two-factor authentication on page 883</a>.</p>
<b>Administrative Domain</b>	<p>Choose the ADOMs this administrator will be able to access.</p> <ul style="list-style-type: none"> <li>• <i>All ADOMs</i>: The administrator can access all the ADOMs.</li> <li>• <i>All ADOMs except specified ones</i>: The administrator cannot access the selected ADOMs.</li> <li>• <i>Specify</i>: The administrator can access the selected ADOMs. Specifying the ADOM shows the <i>Specify Device Group to Access</i> check box. Select the <i>Specify Device Group to Access</i> 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.</li> </ul> <p>If the <i>Admin Profile</i> is <i>Super_User</i>, then this setting is <i>All ADOMs</i>.</p> <p>This field is available only if ADOMs are enabled. See <a href="#">Administrative Domains (ADOMs) on page 750</a>.</p>
<b>Admin Profile</b>	<p>Select an administrator profile from the list. The profile selected determines the administrator's access to the FortiManager unit's features. See <a href="#">Administrator profiles on page 839</a>.</p> <p>If the <i>Administrative Domain</i> is <i>Specify</i>, you can select <i>Single</i> or <i>Per-ADOM</i>.</p> <ul style="list-style-type: none"> <li>• <i>Single</i> (default): Select one profile to apply for all ADOMs the administrator can access.</li> <li>• <i>Per-ADOM</i>: Select a 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.</li> </ul>
<b>Policy Package</b>	<p>Choose the policy packages this administrator will have access to.</p> <ul style="list-style-type: none"> <li>• <i>All Packages</i>: The administrator can access all the packages.</li> <li>• <i>Specify</i>: 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.</li> </ul> <p>This option is only available when the <i>Admin Profile</i> is not a <i>Restricted Admin</i> profile. See <a href="#">Restricted administrators on page 818</a>.</p>



<b>JSON API Access</b>	Select the permission for JSON API Access. Select <i>Read-Write</i> , <i>Read</i> , or <i>None</i> . The default is <i>None</i> .
<b>Web Filter Profile</b>	Select the web filter profiles that the restricted administrator will be able to edit. This option is only available when the <i>Admin Profile</i> is set to a <i>Restricted Admin</i> profile. Security profiles can be configured by going to <i>Policy &amp; Objects &gt; Object Configuration</i> . See <a href="#">Managing objects and dynamic objects on page 402</a> .
<b>IPS Sensor</b>	Select the IPS profiles that the restricted administrator will be able to edit. This option is only available when the <i>Admin Profile</i> is set to a <i>Restricted Admin</i> profile. Security profiles can be configured by going to <i>Policy &amp; Objects &gt; Object Configuration</i> . See <a href="#">Managing objects and dynamic objects on page 402</a> .
<b>Application Sensor</b>	Select the application control profiles that the restricted administrator will be able to edit. This option is only available when the <i>Admin Profile</i> is set to a <i>Restricted Admin</i> profile. Security profiles can be configured by going to <i>Policy &amp; Objects &gt; Object Configuration</i> . See <a href="#">Managing objects and dynamic objects on page 402</a> .
<b>Trusted Hosts</b>	Optionally, turn on trusted hosts, then enter their IP addresses and netmasks. Up to ten IPv4 and ten IPv6 hosts can be added. See <a href="#">Trusted hosts on page 808</a> for more information.
<b>Theme Mode</b>	Select <i>Use Global Theme</i> to apply a theme to all administrator accounts. Select <i>Use Own Theme</i> to allow administrators to select their own theme.
<b>Meta Fields</b>	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 <a href="#">Workflow mode on page 854</a> .
<b>Advanced Options</b>	Configure advanced options, see <a href="#">Advanced options</a> below. For more information on advanced options, see the <i>FortiManager CLI Reference</i> .

### Advanced options

Option	Description	Default
<b>change-password</b>	Enable or Disable changing password.	disable
<b>ext-auth-accprofile-override</b>	Enable or Disable overriding the account profile by administrators configured on a Remote Authentication Server.	disable
<b>ext-auth-adom-override</b>	Enable or Disable overriding the ADOM by administrators configured on a Remote Authentication Server. This will also override the <i>Admin Profile</i> configured for each ADOM.	disable
<b>ext-auth-group-match</b>	Specify the group configured on a Remote Authentication Server.	-

Option	Description	Default
<b>fingerprint</b>	Specify the user certificate fingerprint based on MD5, SHA-1, or SHA-256 hash function. This option is only available if the <i>Admin Type</i> is <i>PKI</i> .	-
<b>first-name</b>	Specify the first name.	-
<b>last-name</b>	Specify the last name.	-
<b>mobile-number</b>	Specify the mobile number.	-
<b>pager-number</b>	Specify the pager number.	-
<b>restrict-access</b>	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 > Admin > 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 > Admin > 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 25](#) 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 > Admin > 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 > Admin > 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 > Admin > 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.

## Edit Administrator

User Name	<input type="text" value="TestAdmin"/>		
Avatar	<div>T</div> <div>+ Add Photo</div> <div>- Remove Photo</div>		
Description	<div></div>		
Admin Type	LOCAL <span>▼</span>		
Admin Profile	test <span>▼</span>		
Administrative Domain	<div>All ADOMs</div> <div>All ADOMs except specified ones</div> <div>Specify</div>		
Policy Package	<div>All Packages</div> <div>Specify</div>		
JSON API Access	Read-Write <span>▼</span>		
Theme Mode	<div>Use Global Theme</div> <div>Use Own Theme</div>		
Trusted Hosts	<div><input checked="" type="checkbox"/></div>		
Trusted IPv4 Host 1	<input type="text" value="10.2.116.0/255.255.255.0"/>		
Trusted IPv4 Host 2	<input type="text" value="255.255.255.255/255.255.255.255"/>		
Trusted IPv4 Host 3	<input type="text" value="255.255.255.255/255.255.255.255"/> <div>+</div>		
Trusted IPv6 Host 1	<input "::="" 0"="" type="text" value=""/>		
Trusted IPv6 Host 2	<input "ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff="" 128"="" type="text" value=""/>		
Trusted IPv6 Host 3	<input "ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff="" 128"="" type="text" value=""/> <div>+</div>		
Meta Fields >			
Advanced Options >			

OK

Cancel

## 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 838](#).

When a restricted administrator 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.

The screenshot displays the 'Restricted Admin Mode' interface. On the left is a navigation menu with options: Web Filter, Profiles, Rating Overrides, URL Filter, Content Filter, Local Category, Intrusion Prevention, and Application Control. The main area is titled 'Edit Web Filter Profile'. It includes a 'Name' field with 'default' and a 'Comment' field with 'Default web filtering.'. Below these is a 'FortiGuard Category Based Filter' section with a table of categories and their authentication status. Further down is a 'Category Usage Quota' section with a table for creating or editing quotas. At the bottom is a 'File Filter' section with a table for file filter rules. The interface concludes with 'OK' and 'Cancel' buttons.

Category	Authenticate
Local Categories	
Potentially Liable	
Adult/Mature Content	
Bandwidth Consuming	
Security Risk	
General Interest - Personal	
General Interest - Business	
Unrated	

Category	Quota

Name	Comments	Protocols	File Types	Action	Direction	Match Encrypted Files
No record found.						

### 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 843](#).
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 811](#)



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 823](#) and [Application control restricted administrator on page 834](#).

# 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*.

Edit Web Filter Profile

Name

default

Comment

Default web filtering.

Advanced Options >

Inspection Mode

Proxy

Flow Based

☐ Log all URLs

☒ FortiGuard Categories

Expand All

Collapse All

All

<input type="checkbox"/>	Category	Authenticate
<input type="checkbox"/>	Local Categories	
<input type="checkbox"/>	Potentially Liable	
<input type="checkbox"/>	Adult/Mature Content	
<input type="checkbox"/>	Bandwidth Consuming	
<input type="checkbox"/>	Security Risk	
<input type="checkbox"/>	General Interest - Personal	
<input type="checkbox"/>	General Interest - Business	
<input type="checkbox"/>	Unrated	

Static URL Filter

☐ URL Filter

☐ Block malicious URLs discovered by FortiSandbox

☐ Web Content Filter

Rating Options

☐ Allow Websites When a Rating Error Occurs

☐ Rate URLs by Domain and IP Address

Apply

Name	The profile name.
Comment	Optionally, enter a description of the profile.
Advanced Options	Configure advanced options, including:

	<ul style="list-style-type: none"> <li>• <i>https-replacemsg</i>: enable/disable</li> <li>• <i>replacemsg-group</i>: select a group from the list</li> <li>• <i>web-filter-activex-log</i>: enable/disable</li> <li>• <i>web-filter-command-block-log</i>: enable/disable</li> <li>• <i>web-filter-cookie-removal-log</i>: enable/disable</li> <li>• <i>web-filter-js-log</i>: enable/disable</li> <li>• <i>web-filter-jscript-log</i>: enable/disable</li> <li>• <i>web-filter-referer-log</i>: enable/disable</li> <li>• <i>web-filter-unknown-log</i>: enable/disable</li> <li>• <i>web-filter-vbs-log</i>: enable/disable</li> <li>• <i>wisp</i>: enable/disable</li> <li>• <i>wisp-algorithm</i>: <i>auto-learning</i>, <i>primary-secondary</i>, or <i>round-robin</i></li> </ul>
<b>Inspection Mode</b>	Select <i>Proxy</i> or <i>Flow Based</i> .
<b>Log all URLs</b>	Select to log all URLs.
<b>FortiGuard Categories</b>	<p>Select FortiGuard categories.</p> <p>Right-click on a category to change the action: <i>Allow</i>, <i>Block</i>, <i>Warning</i>, <i>Monitor</i>, <i>Authenticate</i>, or, if available, <i>Disable</i>.</p> <p>Use the filter drop-down menu to filter the categories shown in the table based on the action.</p>
<b>Allow Users to override blocked categories</b>	<p>Select to allow users to override blocked categories.</p> <p>This option is only available if <i>Inspection Mode</i> is <i>Proxy</i>.</p>
<b>Override Permit</b>	Select the override permits: <i>bannedword-override</i> , <i>contenttype-check-override</i> , <i>fortiguard-wf-override</i> , and <i>urlfilter-override</i> .
<b>Groups that can override</b>	Select groups that can override blocked categories.
<b>Profile can switch to</b>	Select profiles that the user can switch to.
<b>Switch applies to</b>	Select what the switch applies to: <i>ask</i> , <i>browser</i> , <i>ip</i> , <i>user</i> , or <i>user-group</i> .
<b>Switch Duration</b>	Select the switch duration, either <i>ask</i> or <i>constant</i> .
<b>Duration</b>	<p>Enter the duration of the switch.</p> <p>This option is only available if <i>Switch Duration</i> is <i>constant</i>.</p>
<b>Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex</b>	<p>Select to enforce <i>Safe Search</i>.</p> <p>This option is only available if <i>Inspection Mode</i> is <i>Proxy</i>.</p>
<b>Log all search keywords</b>	<p>Select to log all search keywords.</p> <p>This option is only available if <i>Inspection Mode</i> is <i>Proxy</i>.</p>
<b>Block Invalid URLs</b>	<p>Select to block invalid URLs.</p> <p>This option is only available if <i>Inspection Mode</i> is <i>Proxy</i>.</p>
<b>URL Filter</b>	Select to enable URL filters.

	Select URL filters from the dropdown list, and/or create and manage filters in the table.
<b>Block malicious URLs discovered by FortiSandbox</b>	Select to block URLs that FortiSandbox deems malicious.
<b>Web Content Filter</b>	Select to apply web content filters. Click <i>Add</i> to add filters to the table. Edit and delete filters as required.
<b>Allow Websites When a Rating Error Occurs</b>	Select to allow access to websites if a rating error occurs.
<b>Rate URLs by Domain and IP Address</b>	Select to rate URLs by both their domain and IP address.
<b>Block HTTP Redirects by Rating</b>	Select to block HTTP redirects based on the site's rating. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
<b>Rate Images by URL (Blocked images will be replaced with blanks)</b>	Select to rate images based on the URL. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
<b>Restrict Google account usage to specific domains</b>	Select to restrict Google account usage to specific domains. Click <i>Add</i> to add the domains to the table. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
<b>Provide Details for Blocked HTTP 4xx and 5xx Errors</b>	Select to receive details about blocked HTTP errors. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
<b>HTTP POST Action: Block</b>	Select to set the HTTP POST action to block. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
<b>Remove Java Applet Filter</b>	Select to remove the Java applet filter. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
<b>Remove ActiveX Filter</b>	Select to remove the ActiveX filter. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
<b>Remove Cookie Filter</b>	Select to remove the cookie filter. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .

#### 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 837](#).

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 840](#).

### To create an IPS restricted administrator:

1. Go to *System Settings > Admin > Profile*, 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 843](#).
2. Optionally, toggle *Allow to Install* if you want this administrator to be able to install changes to FortiGate devices.

**New Profile**

Profile Name: IPS\_Admin

Description: Restricted profile for intrusion prevention administrators. 59/1023

Type: ☐ System Admin ☒ Restricted Admin

Permission: ☐ Web Filter ☐ Application Control ☒ Intrusion Prevention


Allow to Install: ☒ ON

OK Cancel

3. Go to *System Settings > Admin > 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 811](#).  
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.

**Edit Administrator**

User Name	IPSAAdmin
Avatar	 + Add Photo - Remove Photo
Description	<div></div>
Admin Type	LOCAL
Admin Profile	IPSAAdmin
Administrative Domain	<div> All ADOMs All ADOMs except specified ones Specify </div> <div> <input type="text"/> <div> FabricADOM ✕ 700 ✕ root ✕ </div> </div>
Web Filter	<div> All Web Filters Specify </div> <div> <input type="text"/> <div>None</div> </div>
Application Control	<div> All Application Controls Specify </div>
Intrusion Prevention	<div> All Intrusion Preventions Specify </div>
JSON API Access	None
Theme Mode	<div> Use Global Theme Use Own Theme </div>
Trusted Hosts	<input type="checkbox"/>
Meta Fields >	
Advanced Options >	

OK Cancel



For more information about restricted administrator profiles, see [Restricted administrators on page 818](#).

To configure IPS settings as a restricted administrator, see:

- [Intrusion prevention profiles on page 824](#)
- [Intrusion prevention signatures on page 827](#)
- [Intrusion prevention diagnostics on page 828](#)
- [Intrusion prevention hold-time and CVE filtering on page 829](#)
- [Intrusion prevention FortiGuard packages on page 829](#)
- [Intrusion prevention licenses and services on page 831](#)
- [Intrusion prevention templates on page 832](#)
- [Intrusion prevention global headers and footers on page 833](#)

## 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*.

Edit IPS Sensor

Name

all\_default

Comments

All predefined signatures with default setting.

47/255

Block malicious URLs

OFF

IPS Signatures and Filters

+ Create New

Edit

Delete

Move Up

Move Down

Column Settings

☐

Details

Exempt IPs

Action

Packet Logging

☐

0

default

disable

Botnet C&C

Scan Outgoing Connections to Botnet Sites

Block

Disable

Monitor

Advanced Options

Revision

Change Note

0/1023

Revision History

Revert

View Diff

Column Settings

☐

Revision #

Changed by

Date/Time

Action

Change Note

No record found.

OK

Cancel

<b>Name</b>	The profile name.
<b>Comment</b>	Optionally, enter a description of the profile.
<b>IPS Signatures and Filters</b>	Click <i>Create New</i> and select the <i>Type</i> as either <i>Filter</i> or <i>Signature</i> 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.
<b>Filters</b>	When creating filters, the following settings are available: <i>Action</i> ( <i>Allow</i> , <i>Monitor</i> , <i>Block</i> , <i>Reset</i> , <i>Default</i> , <i>Quarantine</i> ), <i>Packet Logging</i> , <i>Status</i> , and <i>Filter</i> . Click the edit filter icon to create a new filter.

FortiManager 7.2.3 Administration Guide  
Fortinet Inc.

825

For information on hold-time and CVE filter options, see [Intrusion prevention hold-time and CVE filtering on page 829](#).

<b>Signatures</b>	When selecting signatures, the following settings are available: <i>Action (Allow, Monitor, Block, Reset, Default, Quarantine), Packet Logging, Status, Rate-based Setting, Exempt IPs, and Signatures</i> . Click <i>Add Signature</i> to select a new signature. As a restricted administrator, custom IPS signatures can be created by navigating to <i>Intrusion Prevention &gt; IPS Signatures</i> in the tree menu. See <a href="#">Intrusion prevention signatures on page 827</a> .
<b>Botnet C&amp;C</b>	Enable Botnet C&C to scan outgoing connections to botnet sites. Botnet C&C can be set to <i>Block, Disable, or Monitor</i> .
<b>Advanced Options</b>	Enable or disable extended logging.
<b>Revision</b>	Enter a change note that includes details about the change made to the IPS profile.
<b>Revision History</b>	View the revision history for this profile. Select <i>View Diff</i> in the toolbar to compare two versions in revision history. Select <i>Revert</i> in the toolbar to revert to a previous version based on revision history.



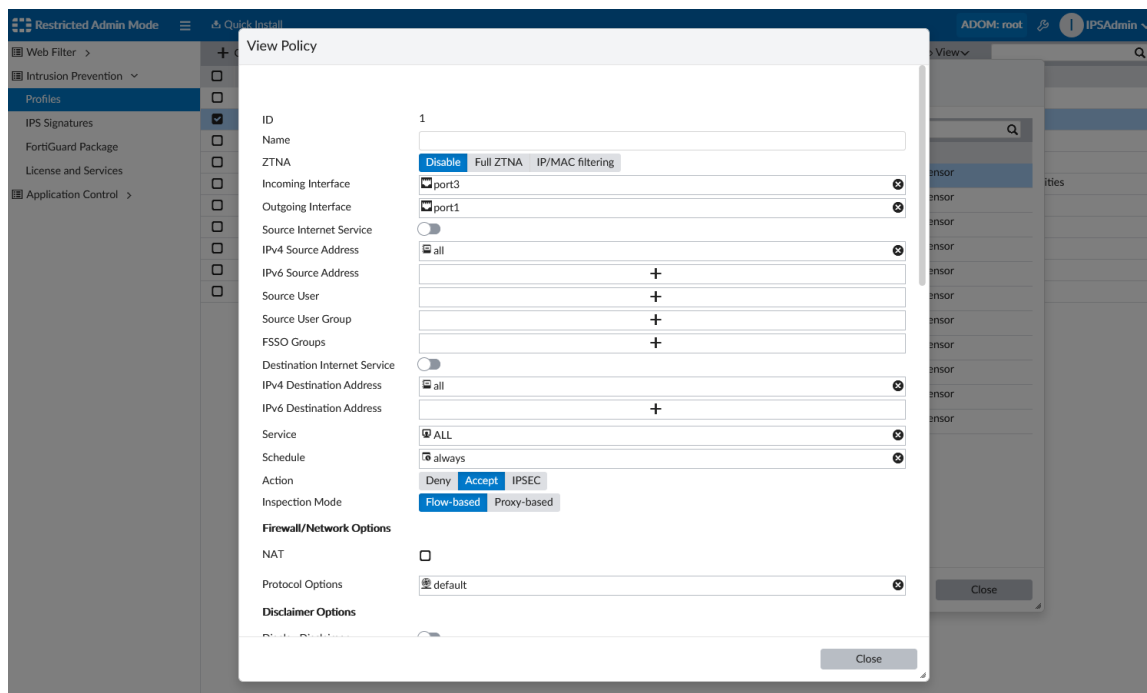
To clone an existing profile, right-click the profile in the content pane, and select *Clone*.

### 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.

Create New Custom Signature

Name

Signature

Status ☒ ON

Revision

Change Note

Revision History

Revert View Diff Column Settings

Revision #	Changed by	Date/Time	Action	Change Note
No record found.				

OK Cancel

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 [IPS Signatures](#) on page 435 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:

Restricted Admin Mode Install Wizard ADOM: root IPSADMIN

Device Name	CPU% (IPS)	MEM% (IPS)	Decoder Packets
Branch_Office_01	-	3	-
Branch_Office_02	-	3	-
Enterprise_First_Floor	-	8	-
Enterprise_Second_Floor	-	7	-
fduncan-tech72	-	4	-

<b>Device Name</b>	The name of the FortiGate device.
<b>CPU% (IPS)</b>	The CPU used by IPS processes as a percentage for the device.

<b>MEM% (IPS)</b>	The memory used by IPS processes as a percentage for the device.
<b>Decoder Packets</b>	The number of transmitted decoder packets.
<b>Session Packets</b>	The number of transmitted session packets.
<b>Protocol Packets</b>	The number of transmitted protocol packets.
<b>Application Packets</b>	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 433](#) 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 433](#) 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.

Restricted Admin Mode										Quick Install		ADOM: root		IPAdmin											
Web Filter										Refresh		Show Used Object Only		Export		Import		Column Settings		Search...					
Intrusion Prevention										Package Name		Product		Version		Service Entitlement		Type		Latest Version (Release Date/Time)		Size		To Be Deployed	
Profiles										<input type="checkbox"/>	▲ Package Name	FortiManager	6.0.12+	IPS	06000000NIDS02603	19.00223 (2021-12-21 06:01:00)	1.29 MB	Latest	Char						
IPS Signatures										<input type="checkbox"/>	Signature Database (Extended)	FortiManager	5.4.0+	FortiCare	05004000NIDS02300	19.00223 (2021-12-21 06:02:00)	84.46 KB	Latest	Char						
FortiGuard Package										<input type="checkbox"/>	Signature Meta Data (Application Control)	FortiManager	6.0.9+6.2.0	FortiCare	05006000APDB00100	19.00220 (2021-12-16 02:08:00)	57.86 KB	Latest	Char						
License and Services										<input type="checkbox"/>	Signature Meta Data (Application Control)	FortiManager	6.2.1-6.2.8.6+	FortiCare	06000000APDB00100	19.00220 (2021-12-16 02:08:00)	57.86 KB	Latest	Char						
Application Control										<input type="checkbox"/>	Signature Meta Data (Application Control)	FortiManager	6.2.9+	FortiCare	06002000APDB00100	19.00220 (2021-12-16 02:08:00)	63.94 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (Application Control)	FortiManager	6.4.2+	FortiCare	06004000APDB00100	19.00220 (2021-12-16 02:08:00)	64.05 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (Application Control)	FortiManager	7.0.1+	FortiCare	07000000APDB00100	19.00220 (2021-12-16 02:08:00)	64.02 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (Industrial)	FortiManager	6.0.9+6.2.0	FortiCare	05006000ISDB00100	19.00217 (2021-12-13 20:02:00)	39.49 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (Industrial)	FortiManager	6.2.1-6.2.8.6+	FortiCare	06000000ISDB00100	19.00217 (2021-12-13 20:02:00)	40.70 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (Industrial)	FortiManager	6.2.9+	FortiCare	06002000ISDB00100	19.00217 (2021-12-13 20:02:00)	43.08 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (Industrial)	FortiManager	6.4.2+	FortiCare	06004000ISDB00100	19.00217 (2021-12-13 20:02:00)	43.24 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (Industrial)	FortiManager	7.0.1+	FortiCare	07000000ISDB00100	19.00217 (2021-12-13 20:02:00)	43.84 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (IPS Extended)	FortiManager	6.0.9+6.2.0	FortiCare	05006000NIDS02500	19.00223 (2021-12-21 06:02:00)	397.13 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (IPS Extended)	FortiManager	6.2.1-6.2.8.6+	FortiCare	06000000NIDS02500	19.00223 (2021-12-21 06:02:00)	446.98 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (IPS Extended)	FortiManager	6.2.9+	FortiCare	06002000NIDS02500	19.00223 (2021-12-21 06:02:00)	447.19 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (IPS Extended)	FortiManager	6.4.7+	FortiCare	06004000NIDS02500	19.00223 (2021-12-21 06:02:00)	447.19 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (IPS Extended)	FortiManager	7.0.1+	FortiCare	07000000NIDS02500	19.00223 (2021-12-21 06:02:00)	447.17 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (IPS Regular)	FortiManager	6.0.9+6.2.0	FortiCare	05006000NIDS02400	19.00223 (2021-12-21 06:02:00)	253.69 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (IPS Regular)	FortiManager	6.2.1-6.2.8.6+	FortiCare	06000000NIDS02400	19.00223 (2021-12-21 06:02:00)	253.95 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (IPS Regular)	FortiManager	6.2.9+	FortiCare	06002000NIDS02400	19.00223 (2021-12-21 06:02:00)	254.21 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (IPS Regular)	FortiManager	6.4.7+	FortiCare	06004000NIDS02400	19.00223 (2021-12-21 06:02:00)	254.21 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (IPS Regular)	FortiManager	7.0.1+	FortiCare	07000000NIDS02400	19.00223 (2021-12-21 06:02:00)	254.48 KB	Latest	Char						
										<input type="checkbox"/>	Signature Meta Data (IPS)	FortiManager	5.4.0+	FortiCare	05004000NIDS02200	19.00223 (2021-12-21 06:02:00)	353.59 KB	Latest	Char						

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 Labs

Fortinet

NEWS / RESEARCH

SERVICES

THREAT LOOKUP

PSIRT

RESOURCES

Search FortiGuard

Home / App Control

Update: 19.218

Updated: Dec 14, 2021 - 10:05

Modified (3)

Latest Versions

19.220

19.218

19.217

19.211

19.210

Anti-Virus

89.07972

38 minutes ago

Mobile Service

89.07972

39 minutes ago

Intrusion Protection

19.223

2 hours ago

App Control

19.220

4 days ago

App Control

Name	Status	Update
SkyVPN.	Ⓢ	Modified
Pinterest	Ⓢ	*Sig Added
Xbox.HTTP	Ⓢ	*Sig Added

FortiGuard packages can be imported or exported.

To import a FortiGuard package:

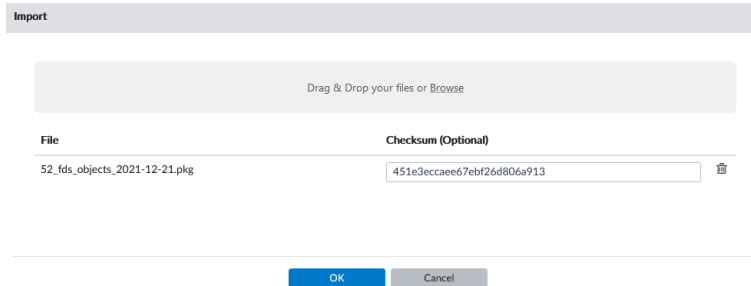
- As a restricted administrator, go to *Intrusion Prevention > FortiGuard Package*.
- Click *Import* in the toolbar.
- Drag and drop the file or browse to the location of the file and select it.

FortiManager 7.2.3 Administration Guide  
Fortinet Inc.

830



- (Optional) Enter the checksum value obtained when exporting the package to verify the file's integrity.



Import

Drag & Drop your files or Browse

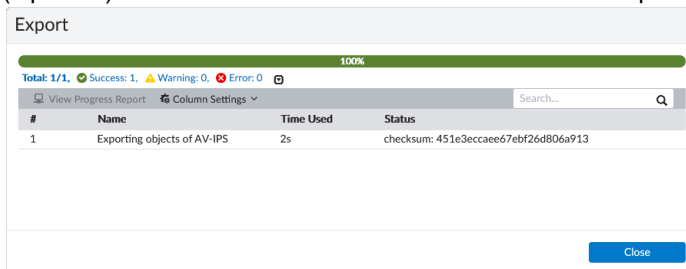
File	Checksum (Optional)
52_fds_objects_2021-12-21.pkg	451e3eccae67ebf26d806a913

OK Cancel

- Click **OK**.

### To export a FortiGuard package:

- As a restricted administrator, go to *Intrusion Prevention > FortiGuard Package*.
- Click *Export* in the toolbar.  
A dialog appears to confirm the number and size of the objects you have selected to export.
- Click **OK**, and the *Export* window appears to confirm the status of the task.
- (Optional) Record the checksum value to include when importing this package in order to verify its integrity.



Export

100%

Total: 1/1, Success: 1, Warning: 0, Error: 0

View Progress Report Column Settings Search...

#	Name	Time Used	Status
1	Exporting objects of AV-IPS	2s	checksum: 451e3eccae67ebf26d806a913

Close

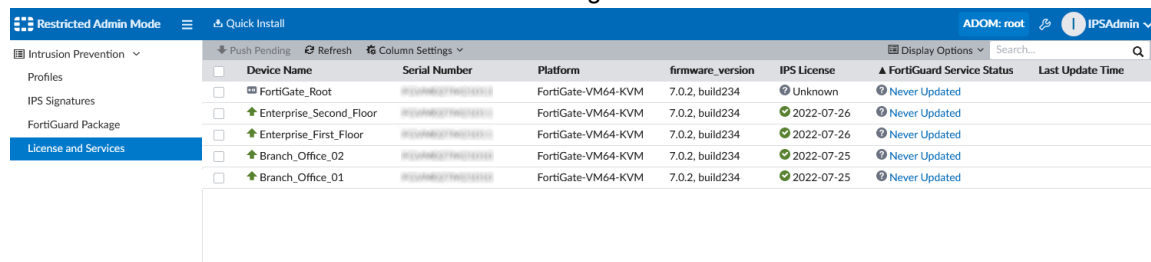
## Intrusion prevention licenses and services

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	Serial Number	Platform	firmware_version	IPS License	FortiGuard Service Status	Last Update Time
FortiGate_Root	FG240M6277960213102	FortiGate-VM64-KVM	7.0.2, build234	Unknown	Never Updated	
Enterprise_Second_Floor	FG240M6277960213102	FortiGate-VM64-KVM	7.0.2, build234	2022-07-26	Never Updated	
Enterprise_First_Floor	FG240M6277960213102	FortiGate-VM64-KVM	7.0.2, build234	2022-07-26	Never Updated	
Branch_Office_02	FG240M6277960213102	FortiGate-VM64-KVM	7.0.2, build234	2022-07-25	Never Updated	
Branch_Office_01	FG240M6277960213102	FortiGate-VM64-KVM	7.0.2, build234	2022-07-25	Never Updated	

<b>Device Name</b>	The FortiGate device's name.
<b>Serial Number</b>	The FortiGate device's serial number.
<b>Platform</b>	The FortiGate device's platform type.
<b>firmware_version</b>	The FortiGate device's firmware version.
<b>IPS License</b>	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.
<b>FortiGuard Service Status</b>	The status of the FortiGuard service for the FortiGate device. The status includes only IPS related objects.
<b>Last Update Time</b>	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 copied.

**Edit IPS Template**

Name: Temp2

Description:

**IPS Global** ☒

Database: Extended **Regular**

Engine Count: 0 (0 - 255, default: 0)

Exclude Signatures: **Industrial** None

Fail Open: ☐

Packet Log Queue Depth: 128 (128 - 4096, default: 128)

Socket Size: 0

Traffic Submit: ☐

**System IPS** ☒

Override Signature Hold By Id: ☒

Signature Hold Time: 0h (day range: 0 - 7, hour range: 0 - 23, max hold time: 7d0h, default hold time: 0d0h)

**IPS Settings** ☒

IPS Packet Quota: 0 (0 - 4294967295, default: 0)

Packet Log History: 1 (1 - 255)

Packet Log Memory: 256 (64 - 8192 kB)

Packet Log Post Attack: 0 (0 - 255)

OK Cancel

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**.

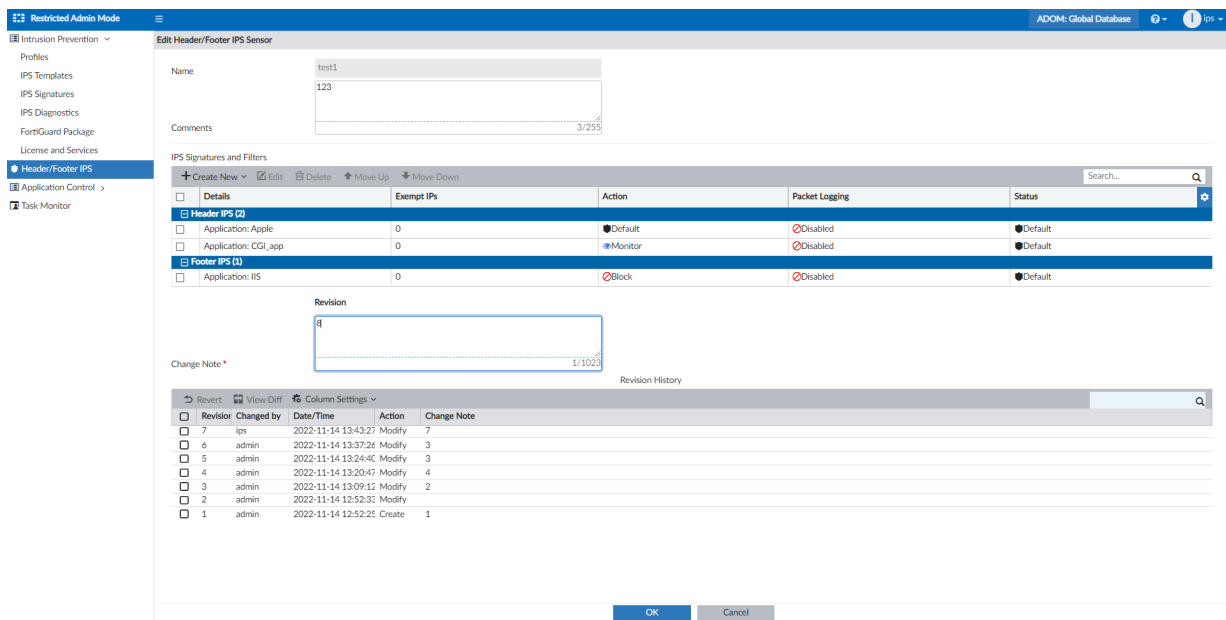
## Intrusion prevention global headers and footers

Restricted IPS admins can manage the IPS headers and footers and perform IPS installations in the *Global Database ADOM*.

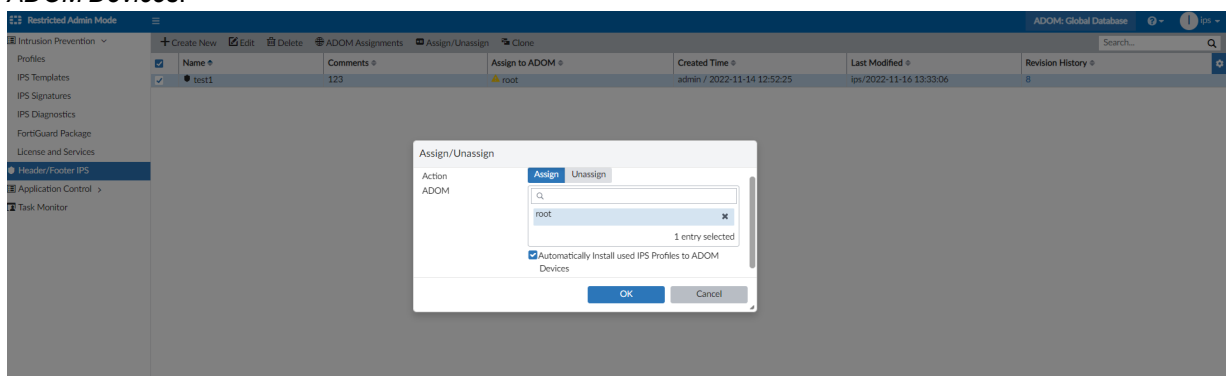
For more information, see [Global Database on page 772](#) and [Header/Footer IPS on page 774](#).

### 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*.



## 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:

- Log on as a Restricted Administrator.
- Go to *Application Control > Custom Signatures*.

3. Click *Create New*. The *Create New Custom Application Signature* screen appears.

Create New Custom Application Signature

Name

Signature

Comment

0/1023

0/63

OK

Cancel

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.

**Edit Application Control Profile**

Name: default

Comments: Monitor all applications. 25/255

**Categories**

<input type="button" value="Monitor"/> Botnet	<input type="button" value="Monitor"/> Game	<input type="button" value="Monitor"/> Proxy	<input type="button" value="Monitor"/> Video/Audio
<input type="button" value="Monitor"/> Business	<input type="button" value="Monitor"/> General.Interest	<input type="button" value="Monitor"/> Remote.Access	<input type="button" value="Monitor"/> VoIP
<input type="button" value="Monitor"/> Cloud.IT	<input type="button" value="Monitor"/> Mobile	<input type="button" value="Monitor"/> Social.Media	<input type="button" value="Monitor"/> Industrial
<input type="button" value="Monitor"/> Collaboration	<input type="button" value="Monitor"/> Network.Service	<input type="button" value="Monitor"/> Storage.Backup	<input type="button" value="Monitor"/> Web.Client
<input type="button" value="Monitor"/> Email	<input type="button" value="Monitor"/> P2P	<input type="button" value="Monitor"/> Update	<input checked="" type="button" value="Allow"/> Unknown Applications

**Application Overrides**

+ Add Signatures ☒ Edit Parameters

Application Signature	Category	Action
-----------------------	----------	--------

**Filter Overrides**

+ Add Filter ☒ Edit

Filter Details	Action
----------------	--------

**Options**

☒ Deep Inspection of Cloud Applications

☒ Allow and Log DNS Traffic

☒ Replacement Messages for HTTP-based Applications

☐ Logging of Other Applications

☐ Logging of Unknown Applications

**Advanced Options** >

**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 *bittorrent, 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 843](#).

---

**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*.

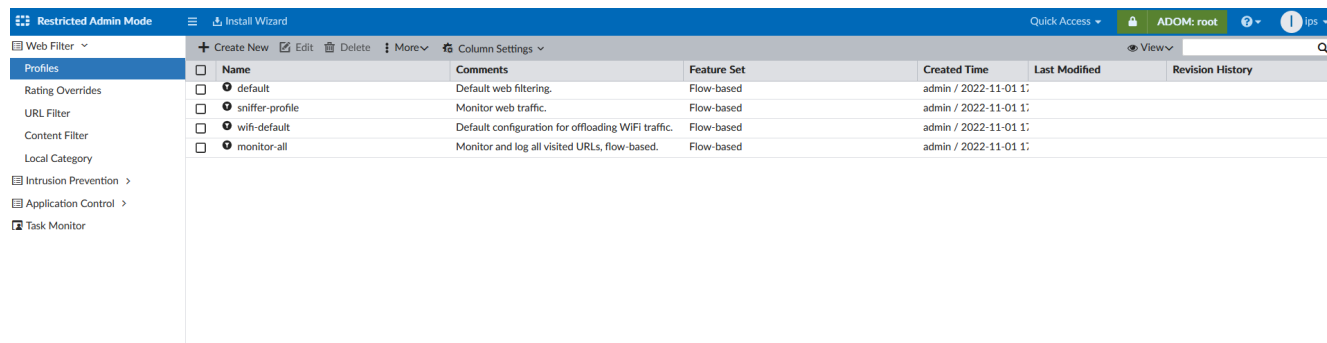
**To install IPS profiles:**

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 847](#).

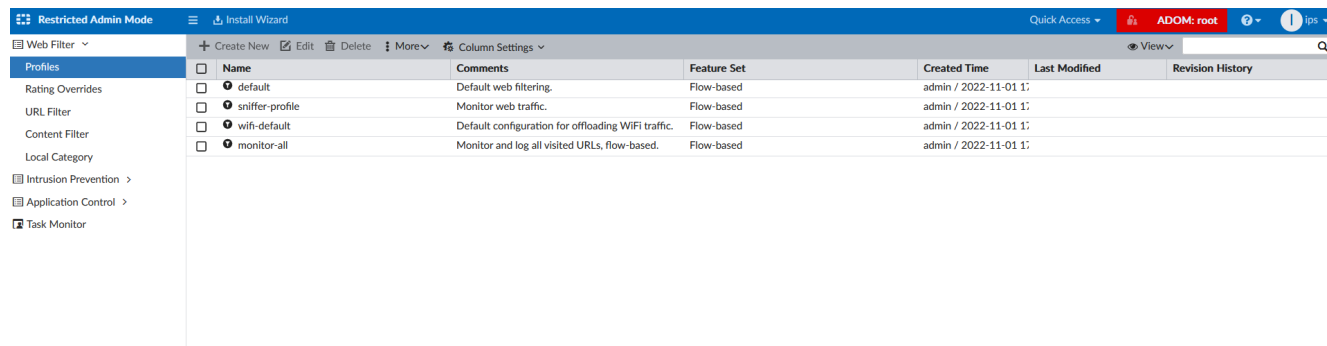
When Workspace mode is enabled on an ADOM (or all ADOMs), a lock icon appears next to the ADOM name for the restricted administrator.



Restricted Admin Mode		Quick Access		ADOM: root		ips	
Web Filter		Create New	Edit	Delete	More	Column Settings	View
Profiles	<input type="checkbox"/> Name	Comments		Feature Set	Created Time	Last Modified	Revision History
Rating Overrides	<input type="checkbox"/> default	Default web filtering.		Flow-based	admin / 2022-11-01 11		
URL Filter	<input type="checkbox"/> sniffer-profile	Monitor web traffic.		Flow-based	admin / 2022-11-01 11		
Content Filter	<input type="checkbox"/> wif-default	Default configuration for offloading WiFi traffic.		Flow-based	admin / 2022-11-01 11		
Local Category	<input type="checkbox"/> monitor-all	Monitor and log all visited URLs, flow-based.		Flow-based	admin / 2022-11-01 11		

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 Admin Mode		Quick Access		ADOM: root		ips	
Web Filter		Create New	Edit	Delete	More	Column Settings	View
Profiles	<input type="checkbox"/> Name	Comments		Feature Set	Created Time	Last Modified	Revision History
Rating Overrides	<input type="checkbox"/> default	Default web filtering.		Flow-based	admin / 2022-11-01 11		
URL Filter	<input type="checkbox"/> sniffer-profile	Monitor web traffic.		Flow-based	admin / 2022-11-01 11		
Content Filter	<input type="checkbox"/> wif-default	Default configuration for offloading WiFi traffic.		Flow-based	admin / 2022-11-01 11		
Local Category	<input type="checkbox"/> monitor-all	Monitor and log all visited URLs, flow-based.		Flow-based	admin / 2022-11-01 11		



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 854](#).



## 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:

<b>Restricted_User</b>	Restricted user profiles have no system privileges enabled, and have read-only access for all device privileges.
<b>Standard_User</b>	Standard user profiles have no system privileges enabled, and have read/write access for all device privileges.
<b>Super_User</b>	Super user profiles have all system and device privileges enabled. It cannot be edited.
<b>Package_User</b>	Package user profile have read/write policy and objects privileges enabled, and have read-only access for system and other privileges.

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 > Profile* to view and manage administrator profiles.

<div> <span>+</span> Create New           <span>✎</span> Edit           <span>📄</span> Clone           <span>🗑️</span> Delete           <input type="text"/> </div>				
<input type="checkbox"/>	#	Name	Type	Description
<input type="checkbox"/>	1	Restricted_User	System Admin	Restricted user profiles have no System Privileges enabled, and have read-only access for all Device Privileges.
<input type="checkbox"/>	2	Standard_User	System Admin	Standard user profiles have no System Privileges enabled, but have read/write access for all Device Privileges.
<input type="checkbox"/>	3	Super_User	System Admin	Super user profiles have all system and device privileges enabled.
<input type="checkbox"/>	4	Package_User	System Admin	Package user profile have read/write policy package and objects privileges enabled, and have read-only access for system and others privileges.
<input type="checkbox"/>	5	qwer	Restricted Admin	
<input type="checkbox"/>	6	Restrict_Admin	Restricted Admin	
<input type="checkbox"/>	7	Restrict 2	Restricted Admin	
<input type="checkbox"/>	8	admin	System Admin	

The following options are available:

<b>Create New</b>	Create a new administrator profile. See <a href="#">Creating administrator profiles on page 843</a> .
<b>Edit</b>	Edit the selected profile. See <a href="#">Editing administrator profiles on page 846</a> .
<b>Clone</b>	Clone the selected profile. See <a href="#">Cloning administrator profiles on page 846</a> .
<b>Delete</b>	Delete the selected profile or profiles. See <a href="#">Deleting administrator profiles on page 846</a> .
<b>Search</b>	Search the administrator profiles list.

The following information is shown:

<b>Name</b>	The name the administrator uses to log in.
<b>Type</b>	The profile type, either <i>System Admin</i> or <i>Restricted Admin</i> .
<b>Description</b>	A description of the system and device access permissions allowed for the selected profile.

## Permissions

The below table lists the default permissions for the predefined 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*, *FortiSOC*, *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 29](#).

Setting	Predefined Administrator Profile			
	Super User	Standard User	Restricted User	Package User
<b>System Settings</b> system-setting	Read-Write	None	None	Read-Only
<b>Administrative Domain</b> adom-switch	Read-Write	Read-Write	None	Read-Write
<b>FortiGuard Center</b> fgd_center	Read-Write	None	None	Read-Only
<b>License Management</b> fgd-center-licensing	Read-Write	None	None	Read-Only
<b>Firmware Management</b> fgd-center-fmw-mgmt	Read-Write	None	None	Read-Only
<b>Settings</b> fgd-center-advanced	Read-Write	None	None	Read-Only
<b>Device Manager</b> device-manager	Read-Write	Read-Write	Read-Only	Read-Write

Setting	Predefined Administrator Profile			
	Super User	Standard User	Restricted User	Package User
<b>Add/Delete/Edit Devices/Groups</b> device-op	Read-Write	Read-Write	None	Read-Write
<b>Retrieve Configuration from Devices</b> config-retrieve	Read-Write	Read-Write	Read-Only	Read-Only
<b>Revert Configuration from Revision History</b> config-revert	Read-Write	Read-Write	Read-Only	Read-Only
<b>Delete Device Revision</b> device-revision-deletion	Read-Write	Read-Write	Read-Only	Read-Write
<b>Terminal Access</b> term-access	Read-Write	Read-Write	Read-Only	Read-Only
<b>Manage Device Configurations</b> device-config	Read-Write	Read-Write	Read-Only	Read-Write
<b>Provisioning Templates</b> device-profile	Read-Write	Read-Write	Read-Only	Read-Write
<b>SD-WAN</b> device-wan-link-load-balance	Read-Write	Read-Write	Read-Only	Read-Write
<b>Script Access</b> script-access	Read-Write	Read-Write	None	Read-Write
<b>Policy &amp; Objects</b> policy-objects	Read-Write	Read-Write	Read-Only	Read-Write
<b>Global Policy Packages &amp; Objects</b> global-policy-packages	Read-Write	Read-Write	None	Read-Write
<b>Assignment</b> assignment	Read-Write	None	None	Read-Only
<b>Policy Packages &amp; Objects</b>	Read-Write	Read-Write	Read-Only	Read-Write

Setting	Predefined Administrator Profile			
	Super User	Standard User	Restricted User	Package User
<b>adom-policy-packages</b>				
<b>Policy Check</b> consistency-check	Read-Write	Read-Write	Read-Only	Read-Only
<b>Edit Installation Targets</b> set-install-targets	Read-Write	Read-Write	Read-Only	Read-Write
<b>Install Policy Package or Device Configuration</b> deploy-management	Read-Write	Read-Write	Read-Only	Read-Write
<b>Import Policy Package</b> import-policy-packages	Read-Write	Read-Write	Read-Only	Read-Write
<b>Interface Mapping</b> intf-mapping	Read-Write	Read-Write	Read-Only	Read-Write
<b>AP Manager</b> device-ap	Read-Write	Read-Write	Read-Only	Read-Write
<b>FortiSwitch Manager</b> device-fortiswitch	Read-Write	Read-Write	Read-Only	Read-Write
<b>VPN Manager</b> vpn-manager	Read-Write	Read-Write	Read-Only	Read-Write
<b>Extension Access</b> extension-access	Read-Write	Read-Write	None	Read-Only
<b>FortiView</b> log-viewer	Read-Write	Read-Write	Read-Only	Read-Only
<b>Log View/FortiView</b> log-viewer	Read-Write	Read-Write	Read-Only	Read-Only
<b>FortiSOC</b> event-management	Read-Write	Read-Write	Read-Only	Read-Only
<b>Create &amp; Update Incidents</b> update-incidents	Read-Write	Read-Write	None	None
<b>Triage Event</b> triage-events	Read-Write	Read-Write	None	None
<b>Reports</b> report-viewer	Read-Write	Read-Write	Read-Only	Read-Only

Setting	Predefined Administrator Profile			
	Super User	Standard User	Restricted User	Package User
<b>Run Report</b> <code>run-report</code>	Read-Write	Read-Write	None	None
<b>Fabric View</b> <code>fabric-viewer</code>	Read-Write	Read-Write	Read-Only	Read-Only
<b>CLI only settings</b>				
<code>device-forticlient</code>	Read-Write	Read-Write	Read-Only	Read-Write
<code>realtime-monitor</code>	Read-Write	Read-Write	Read-Only	Read
<code>adom-lock</code>	Read-Write	Read-Write	Read-Only	Read-Write
<code>device-policy-package-lock</code>	Read-Write	Read-Write	Read-Only	Read-Write
<code>read-passwd</code>	Read-Write	None	None	Read-Only
<code>ips-objects</code>	Read-Write	Read-Write	Read	Read-Write

## 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 > Profile*.
2. Click *Create New* in the toolbar. The *New Profile* pane is displayed.

New Profile

Profile Name

This field is required.

Description

0/1023

Type

☒ System Admin
 ☐ Restricted Admin


Read-Write

Read-Only

None

System Settings	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Administrative Domain	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
FortiGuard Center	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
License Management	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Firmware Management	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Settings	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Device Manager	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Add/Delete/Edit Devices/Groups	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Retrieve Configuration from Devices	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Revert Configuration from Revision History	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Delete Device Revision	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Terminal Access	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Manage Device Configurations	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Provisioning Templates	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
SD-WAN	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Script Access	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Policy & Objects	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Global Policy Packages & Objects	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Assignment	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Policy Package & Objects	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Policy Check	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Edit Installation Targets	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Install Policy Package or Device Configuration	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Import Policy Package	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Interface Mapping	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
AP Manager	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
FortiSwitch Manager	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
VPN Manager	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Extension Access	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
FortiView	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

## 3. Configure the following settings:

<b>Profile Name</b>	Enter a name for this profile.
<b>Description</b>	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.
<b>Type</b>	Select the type of profile, either <i>System Admin</i> or <i>Restricted Admin</i> .
<b>Permission</b>	Select which permissions to enable from <i>Web Filter</i> , <i>Application Control</i> , and <i>Intrusion Prevention</i> .  This option is only available when <i>Type</i> is <i>Restricted Admin</i> . See <a href="#">Restricted administrators on page 818</a> for information.
<b>Allow to Install</b>	Allows restricted administrators to install Web Filters, Intrusion Prevention, and Application Control profiles. See <a href="#">Installing profiles as a restricted administrator on page 837</a> .
<b>Permissions</b>	Select <i>None</i> , <i>Read Only</i> , or <i>Read-Write</i> access for the categories as required.  This option is only available when <i>Type</i> is <i>System Admin</i> .
<b>Privacy Masking</b>	Enable/disable privacy masking.  This option is only available when FortiAnalyzer features are enabled.
<b>Masked Data Fields</b>	Select the fields to mask: <i>Destination Name</i> , <i>Source IP</i> , <i>Destination IP</i> , <i>User</i> , <i>Source Name</i> , <i>Email</i> , <i>Message</i> , and/or <i>Source MAC</i> .
<b>Data Mask Key</b>	Enter the data masking encryption key. You need the <i>Data Mask Key</i> to see the original data.
<b>Data Unmasked Time(0-365 Days)</b>	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 <i>Log View</i> toolbar is greater than the number of days in the <i>Data Masked Time</i> field.
<div>  <ul style="list-style-type: none"> <li>Only integers between 0-365 are supported.</li> <li>Time frame masking does not apply to real time logs.</li> <li>Time frame masking applies to custom view and drill-down data.</li> </ul> </div>	

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 > Profile*.
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 > Profile*.
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 > Profile*.
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 854](#).

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 848](#).

## To enable or disable workspace in the GUI:

1. Go to *System Settings > All 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 754](#)).



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 170](#).

---

## Enable workspace mode

Workspace mode can be enabled per ADOM or in all ADOMs.

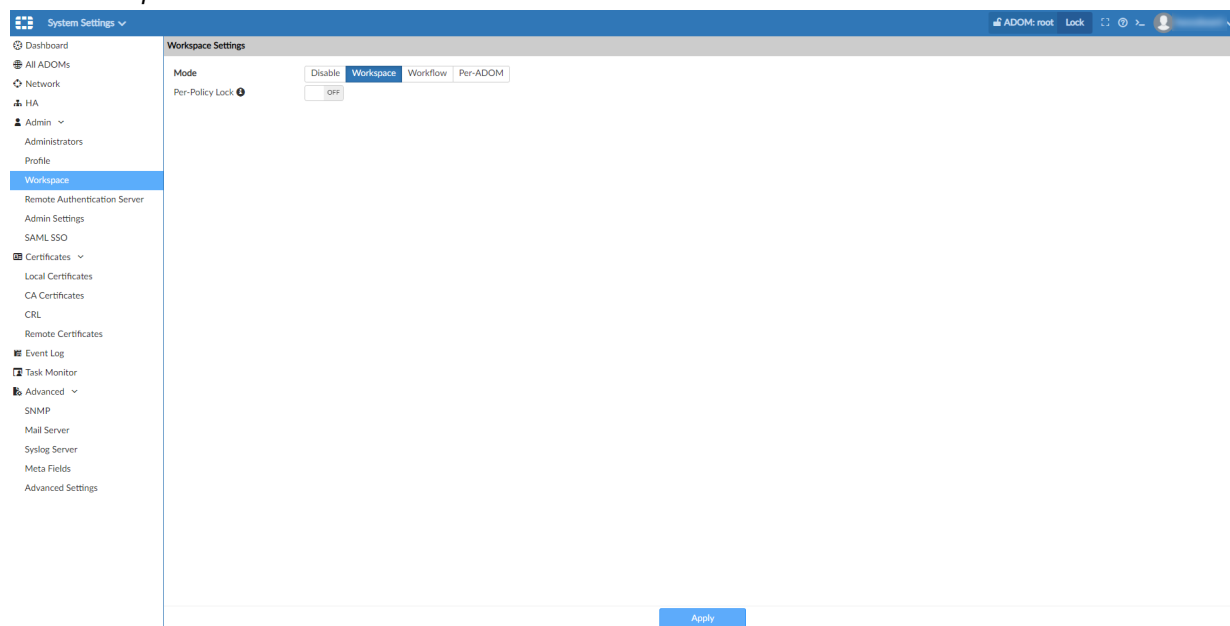


After changing the workspace mode, your session will end, and you will be required to log back into the FortiManager.

---

## To enable workspace mode on all ADOMs in the GUI:

1. Go to *System Settings > Admin > Workspace*.
2. Click *Workspace*.



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
```

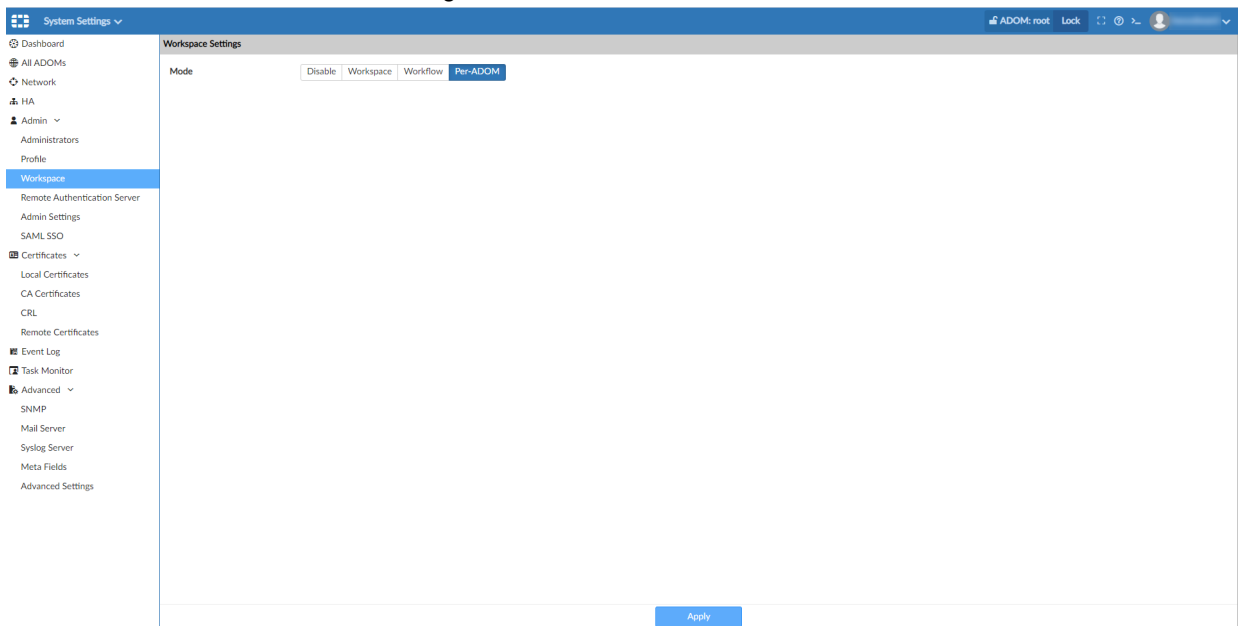


When workspace mode is enabled, *Device Manager* and *Policy & Objects* are read-only. You must lock the ADOM, a device, or a policy package before you can make any changes.

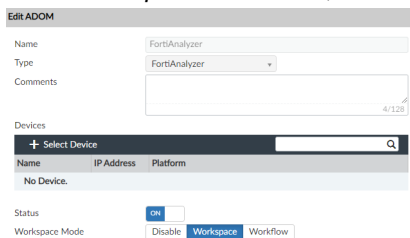
## To enable workspace mode per ADOM in the GUI:

1. Ensure ADOMs are enabled.
2. Go to *System Settings > Admin > Workspace*.

3. Click *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 > All 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

In workspace mode, an ADOM must be locked before you can make changes to it or add devices, policy packages, or objects.

When an ADOM is locked, other administrators are unable to make changes to devices, policies, and objects in that ADOM until you either unlock the ADOM, or log out of the FortiManager.



Policy packages and devices can also be locked individually. See [Locking a device on page 852](#) and [Locking a policy package on page 852](#).

---

#### 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 > All 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.

If another administrator has locked devices or policy packages within the ADOM, you will be given the option of forcibly disconnecting them, thus removing the locks, before you can lock the ADOM.

---

#### 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 > All 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.

---

---

## 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 754](#)).

---

### 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 > Admin > 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.

---

## 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 > Workspace*.
2. Click *Workflow*.
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 > Admin > Workspace*.
  - b. Click *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 > All 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 # 1* 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 > 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:

1. Go to *System Settings > Dashboard*.
2. In the *CLI Console* widget enter the following CLI commands in their entirety:

```
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 795](#), and each administrator must have a contact email address configured, see [Managing administrator accounts on page 809](#).



This menu is only available when `workspace-mode` is set to `workflow`.

### To create a new approval matrix:

1. Go to *System Settings > Admin > Approval Matrix*.
2. Click *Create New*.

The screenshot shows the 'New Approval Matrix' dialog box. It has the following fields and values:

- ADOM: fgt54-2
- Approval Group # 1: TLeela, PJFry
- Approval Group # 2: BBRodriguez, HConrad
- Send an Email Notification to: admin
- Mail Server: localMail

At the bottom, there are 'OK' and 'Cancel' buttons.

3. Configure the following settings:

<b>ADOM</b>	Select the ADOM from the dropdown list.
<b>Approval Group</b>	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.
<b>Send an Email Notification to</b>	Select to add administrators to send email notifications to.
<b>Mail Server</b>	Select the mail server from the dropdown list. A mail server must already be configured. See <a href="#">Mail Server on page 795</a> .

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 configured for the ADOM to which the session applies before a workflow session can be started. See [Workflow approval on page 857](#).

---

## 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 862](#).
5. Click *Create New Session*.

Create New Session

Session Name

Comments

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 304](#).

## 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 859](#).
2. Click *Sessions > View Diff*. The *Revisions Diff* dialog box opens.

Revision Diffs Between 1 and 2

Summary

**Global Policy -**  
Have no difference on global policy package.

**Policy Package - changed (4)**

Policy Package	Install On	User	Update Time	Change Summary	
FortiGate-VM64_CDOMm		admin	2018-02-21 08:18:25	changed	<a href="#">[Details]</a>
FortiGate-VM64_CDOMm_1		admin	2018-02-21 08:41:08	changed	<a href="#">[Details]</a>
FortiGate-VM64_root		admin	2018-02-21 08:40:12	changed	<a href="#">[Details]</a>
Model1		admin	2018-02-21 08:39:39	changed	<a href="#">[Details]</a>

**Policy Object - added (1) [\[Details\]](#)**

Category	User	Update Time	Change Summary
system virtual-wire-pair	admin	2018-02-21 08:40:35	added (1)

Download

Close

3. Select *Details* to view specific changes within a policy package or the policy objects.

Revision Diffs Between 1 and 2

Summary Policy Objects **FortiGate-VM64\_CDOMm\_1** FortiGate-VM64\_root

firewall policy - added (1)

	Seq.#	Policy ID	Name	From	To	Source	Destination	Schedule	Service	Action	Log	Status	Security Profiles	Policy Section	Install On	Others
Added	1	1	VpairO	"port1"	"port10"	"all"	"all"	"always"	"ALL"							

firewall multicast-policy - added (1)

	Seq.#	Policy ID	Source Interface	Source	Destination Interface	Destination	Protocol	Source NAT	Destination NAT	Action	Log	Policy Section	Install On	Others
Added	1	1	"any"	"all"	"any"	"all"	0	1	0.0.0.0					

firewall local-in-policy - added (1)

	Seq.#	Policy ID	Source	Destination	Service	Schedule	Interface	Action	Policy Section	Install On	Others
Added	1	1	"all"	"all"	"ALL"	"always"	"vpnmgmt_tet_spoke2hub"				

firewall DoS-policy - added (1)

	Seq.#	Policy ID	Interface	Source	Destination	Service	Policy Section	Install On	Others
Added	1	1	"vpnmgmt_tet_mesh"	"test_local_subnet_1"	"test_local_subnet_2"	"AH"			

firewall shapoin-policy - added (1)

Download Close

4. Click *Download* to download a CSV file of the changes to your management computer.
5. 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 857](#)), 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:

<b>Comments</b>	Enter a comment describing the changes that have been made in this session.
<b>Attach configuration change details</b>	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. 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 862](#).
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 862](#).
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 862](#).
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 862](#).
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.

Session List

✓ Approve

✗ Reject

🗑 Discard

🔍 View Diff

<input type="checkbox"/>	ID	Name	User	Date Submi...	Approved/...	Comments
<input type="checkbox"/>	3	Session-...	admin		0/1	It didn't wor...
<input checked="" type="checkbox"/>	2	Session-...	HConrad	2016-04-19...	0/1	bureaucrati...
<input type="checkbox"/>	1	Session-9	admin	2016-04-19...	0/1	This is a test...

+ Add Comment

[HConrad] - 2016-04-19 05:53:08

bureaucratic stuff

[HConrad] - 2016-04-19 12:52:46

bureaucratic stuff

Continue Session In Progress

Continue Without Session



The following options and information are available:

<b>Approve</b>	Approve the selected session. Enter comments in the <i>Approve Session</i> dialog box as required.
<b>Reject</b>	Reject the selected session. Enter comments in the <i>Reject Session</i> dialog box as required. A rejected session must be repaired before the next session in the list can be approved.
<b>Discard</b>	Discard the selected session. If a session is discarded, all later sessions are also discarded.
<b>Repair</b>	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.
<b>Revert</b>	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.
<b>View Diff</b>	View the changes that were made prior to approving or rejecting the session. Select <i>Details</i> to view specific changes within a policy package.
<b>ID</b>	A unique number to identify the session.
<b>Name</b>	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.
<b>User</b>	The administrator who created the session.
<b>Date Submitted</b>	The date and time the session was submitted for approval.
<b>Approved/...</b>	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.
<b>Comments</b>	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.
<b>Create New Session</b>	Select to create a new workflow session. This option is not available when a session has been saved or is already in progress.
<b>Continue Session in Progress</b>	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.
<b>Continue Without Session</b>	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.

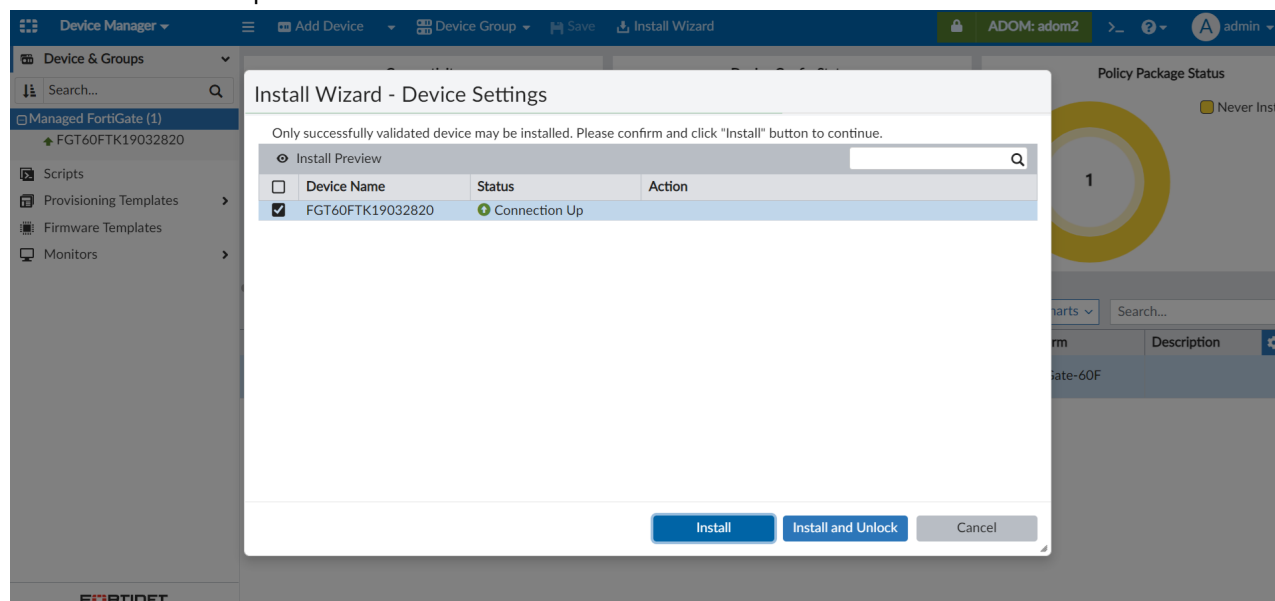
This setting is helpful for ensuring that ADOMs do not remain locked after the administrator has completed their work.

This setting can only be configured in the CLI.

## To enable the install and unlock setting in Workspace mode:

1. In the FortiManager CLI, enter the following commands:  

```
config system global
set workspace-mode workspace-unlock-after-install
```
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 864](#) 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 867](#), [RADIUS servers on page 869](#), [TACACS+ servers on page 871](#), and [Remote authentication server groups on page 871](#) 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 778](#).

#### 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 PKCS#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 > CA Certificates*.
3. Click *Import*, 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 > Admin > Administrator*.
2. Click *Create New*. The *New Administrator* dialog box opens.  
See [Creating administrators on page 811](#) 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 867](#), [RADIUS servers on page 869](#), and [TACACS+ servers on page 871](#) for more information.

Remote authentication servers can be added, edited, deleted, and added to authentication groups (CLI only).

Go to *System Settings > Admin > Remote Authentication Server* to manage remote authentication servers.

+ Create New ▾ Edit Delete				
<input type="checkbox"/>	▲ Name	Type	ADOM	Details
<input type="checkbox"/>	ActTack	TACACS+		10.10.10.15 CHAP
<input type="checkbox"/>	Dapple	LDAP	All ADOMs	10.10.10.11:389/cn:
<input type="checkbox"/>	Lapper	LDAP	Syslog, FortiAuthenticator, FortiCache, FortiMail, FortiWeb	10.10.10.55:389/cn:
<input type="checkbox"/>	Rader	RADIUS		10.10.10.13 PAP
<input type="checkbox"/>	Radium	RADIUS		10.11.10.10 10.11.11.10 MSv2

The following options are available:

<b>Create New</b>	Add an LDAP, RADIUS, or TACACS+ remote authentication server. See <a href="#">LDAP servers on page 867</a> , <a href="#">RADIUS servers on page 869</a> , and <a href="#">TACACS+ servers on page 871</a> .
<b>Edit</b>	Edit the selected remote authentication server. See <a href="#">Editing remote authentication servers on page 867</a> .
<b>Delete</b>	Delete the selected remote authentication server or servers. See <a href="#">Deleting remote authentication servers on page 867</a> .

The following information is displayed:

<b>Name</b>	The name of the server.
<b>Type</b>	The server type: <i>LDAP</i> , <i>RADIUS</i> , or <i>TACACS+</i> .
<b>ADOM</b>	The administrative domain(s) which are linked to the remote authentication server.
<b>Details</b>	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 > Admin > 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 867](#), [RADIUS servers on page 869](#), and [TACACS+ servers on page 871](#) 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 > Admin > 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.

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 > Admin > Remote Authentication Server*.
2. Select *Create New > LDAP Server* from the toolbar. The *New LDAP Server* pane opens.


**New LDAP Server**

Name

Server Name/IP

Port

Common Name Identifier

Distinguished Name  

Bind Type

User DN

Password

Secure Connection ☒ Enable

Protocol

Certificate

Administrative Domain

**Advanced Options >**

3. Configure the following settings, and then click *OK* to add the LDAP server.

<b>Name</b>	Enter a name to identify the LDAP server.
<b>Server Name/IP</b>	Enter the IP address or fully qualified domain name of the LDAP server.
<b>Port</b>	Enter the port for LDAP traffic. The default port is 389.
<b>Common Name Identifier</b>	The common name identifier for the LDAP server. Most LDAP servers use <i>cn</i> . However, some servers use other common name identifiers such as <i>uid</i> .
<b>Distinguished Name</b>	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 <i>query distinguished name</i> icon will query the LDAP server for the name and open the <i>LDAP Distinguished Name Query</i> window to display the results.
<b>Bind Type</b>	Select the type of binding for LDAP authentication: <i>Simple</i> , <i>Anonymous</i> , or <i>Regular</i> .
<b>User DN</b>	When the <i>Bind Type</i> is set to <i>Regular</i> , enter the user DN.
<b>Password</b>	When the <i>Bind Type</i> is set to <i>Regular</i> , enter the password.
<b>Secure Connection</b>	Select to use a secure LDAP server connection for authentication.
<b>Protocol</b>	When <i>Secure Connection</i> is enabled, select either LDAPS or STARTTLS.
<b>Certificate</b>	When <i>Secure Connection</i> is enabled, select the certificate from the dropdown list.
<b>Administrative Domain</b>	Choose the ADOMs that this server will be linked to for reporting: <i>All ADOMs</i> (default), or <i>Specify</i> for specific ADOMs.
<b>Advanced Options</b>	
<b>adom-attr</b>	Specify an attribute for the ADOM.

<b>attributes</b>	Specify the attributes such as <i>member</i> , <i>uniquemember</i> , or <i>memberuid</i> .
<b>connect-timeout</b>	Specify the connection timeout in millisecond.
<b>filter</b>	Specify the filter in the format (objectclass=*)
<b>group</b>	Specify the name of the LDAP group.
<b>memberof-attr</b>	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 <i>memberof-attr</i> will inherit the administrative permissions specified for this group.
<b>profile-attr</b>	Specify the attribute for this profile.
<b>secondary-server</b>	Specify a secondary server.
<b>tertiary-server</b>	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 > Admin > Remote Authentication Server*.
2. Select *Create New > RADIUS Server* from the toolbar. The *New RADIUS Server* pane opens.

Name	<input type="text" value="test-Radius"/>
Server Name/IP	<input type="text" value="10.2.0.159"/>
Port	<input type="text" value="1812"/>
Server Secret	<input type="password" value="*****"/>
Connection Status	<span>✔ Successful</span>
	<span>Test Connectivity</span> <span>Test User Credentials</span>
Secondary Server Name/IP	<input type="text"/>
Secondary Server Secret	<input type="password" value="*****"/>
	<span>Test Connectivity</span> <span>Test User Credentials</span>
Authentication Type	<span>ANY ▾</span>
Advanced Options >	

OK Cancel

3. Configure the following settings, and then click *OK* to add the RADIUS server.

<b>Name</b>	Enter a name to identify the RADIUS server.
<b>Server Name/IP</b>	Enter the IP address or fully qualified domain name of the RADIUS server.
<b>Port</b>	Enter the port for RADIUS traffic. The default port is 1812. Some RADIUS servers use port 1645.
<b>Server Secret</b>	Enter the RADIUS server secret. Click the eye icon to Show or Hide the server secret.
<b>Test Connectivity</b>	Click <i>Test Connectivity</i> to test the connectivity with the RADIUS server. Shows success or failure.
<b>Test User Credentials</b>	Click <i>Test User Credentials</i> to test the user credentials. Shows success or failure.
<b>Secondary Server Name/IP</b>	Enter the IP address or fully qualified domain name of the secondary RADIUS server.
<b>Secondary Server Secret</b>	Enter the secondary RADIUS server secret.
<b>Authentication Type</b>	Select the authentication type the RADIUS server requires. If you select the default <i>ANY</i> , FortiManager tries all authentication types.
<b>Advanced Options</b>	
nas-ip	Specify the IP address for the Network Attached Storage (NAS).



## TACACS+ servers

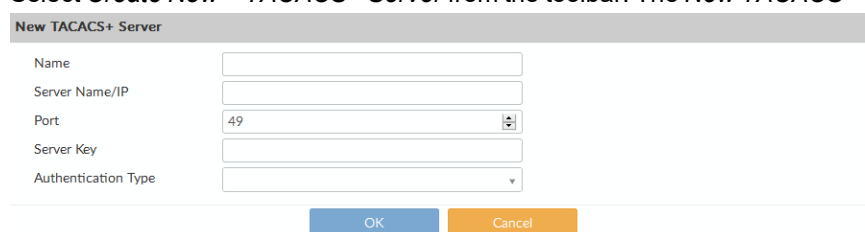
Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol that provides access control for routers, network access servers, and other network computing devices via one or more centralized servers. It allows a client to accept a user name and password and send a query 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 > Admin > 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.

<b>Name</b>	Enter a name to identify the TACACS+ server.
<b>Server Name/IP</b>	Enter the IP address or fully qualified domain name of the TACACS+ server.
<b>Port</b>	Enter the port for TACACS+ traffic. The default port is 49.
<b>Server Key</b>	Enter the key to access the TACACS+ server. The server key can be a maximum of 16 characters in length.
<b>Authentication Type</b>	Select the authentication type the TACACS+ server requires. If you select the default <i>ANY</i> , 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 875](#).



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 > Admin > 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:

<b>Name</b>	Enter a name for the service provider.
<b>IdP Prefix</b>	Copy the IdP prefix. This will be required when configuring your service providers.
<b>SP Type</b>	Select <i>Fortinet</i> as the <i>SP Type</i> . If the SP is not a Fortinet product, select <i>Custom</i> as the <i>SP Type</i> and copy the <i>SP Entity ID</i> , <i>SP ACS (Login) URL</i> , and <i>SP SLS (Logout) URL</i> from your SPs configuration page.
<b>SP Address</b>	Enter the IP address of the service provider.
<b>SAML Attributes</b>	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: <ul style="list-style-type: none"><li>• Type: <i>Username</i>, Attribute: <i>username</i></li><li>• Type: <i>Profile Name</i>, Attribute: <i>profilename</i></li><li>• Type: <i>ADOM</i>, Attribute: <i>adoms</i></li></ul>

### SAML SSO Wildcard users



As long as the SP has the same user profile and ADOM names 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 811](#).

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:

Go to **System Settings > SAML SSO**.

Select **Service Provider (SP)**.

Enter the **Server Address** which is the browser accessible address for this device.

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.
- **Require Assertions Signed from IdP:** Enable this setting to require that all assertions received from the IdP are signed.

Configure the IdP Settings:

1. Select the IdP type as **Fortinet** or **Custom**.
2. Enter the **IdP Address** and the **Prefix** that you obtained while configuring the IdP device.
3. 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.

Confirm that the information is correct and select **Apply**.

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: <pre>&lt;Attribute Name="username"&gt;   &lt;AttributeValue&gt;user1&lt;/AttributeValue&gt; &lt;/Attribute&gt;</pre>

SAML Attribute	Description
profilename	<p>The <i>Profile</i> assigned to the user. If a matching profile exists on the FortiManager, it will be assigned to the user. This attribute is optional.</p> <p>Example:</p> <pre>&lt;Attribute Name="profilename"&gt;   &lt;AttributeValue&gt;SSOPROFILE&lt;/AttributeValue&gt; &lt;/Attribute&gt;</pre>
adoms	<p>The <i>ADOM(s)</i> 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.</p> <p>Example:</p> <pre>&lt;Attribute Name="adoms"&gt;   &lt;AttributeValue&gt;ADOM1&lt;/AttributeValue&gt;   &lt;AttributeValue&gt;ADOM2&lt;/AttributeValue&gt; &lt;/Attribute&gt;</pre>

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 876](#).

### To enable login with FortiCloud:

- 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 *System Settings > Dashboard* in the *License Information* widget.
- Go to *System Settings > Admin > SAML SSO*, and enable *Allow admins to login with FortiCloud*.

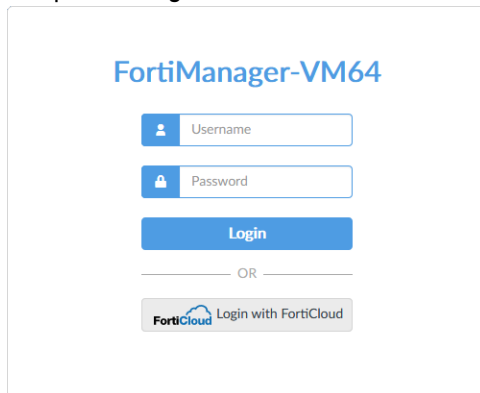
Single Sign-On Settings

Server Address: 192.168.50.243

Allow admins to login with FortiCloud: ☒ ON

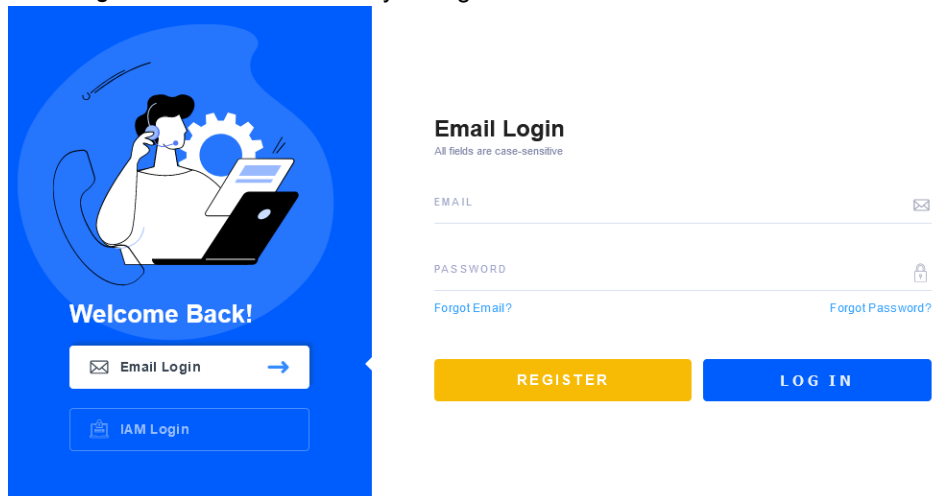
Single Sign-On Mode: Disabled Identity Provider (IdP) Service Provider (SP)

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.



The image shows the FortiManager-VM64 login page. It features a blue header with the text "FortiManager-VM64". Below the header, there are two input fields: "Username" and "Password", each with a corresponding icon (a person for username and a lock for password). Below these fields is a blue "Login" button. Underneath the button is a horizontal line with the text "OR" in the center. At the bottom, there is a button labeled "Login with FortiCloud" with the FortiCloud logo to its left.

4. Click *Login with FortiCloud*. Enter your login credentials from FortiCloud and click *LOGIN*.



The image shows the "Email Login" page. On the left, there is a blue sidebar with a white illustration of a person talking on a phone and working on a laptop. Below the illustration, it says "Welcome Back!". There are two buttons: "Email Login" with an envelope icon and a right arrow, and "IAM Login" with a person icon. On the right, the "Email Login" form has the title "Email Login" and a note "All fields are case-sensitive". It has two input fields: "EMAIL" and "PASSWORD", each with a corresponding icon (an envelope for email and a lock for password). Below the "EMAIL" field is a link "Forgot Email?". Below the "PASSWORD" field is a link "Forgot Password?". At the bottom, there are two buttons: a yellow "REGISTER" button and a blue "LOG IN" button.

You are signed in with your FortiCloud user account.

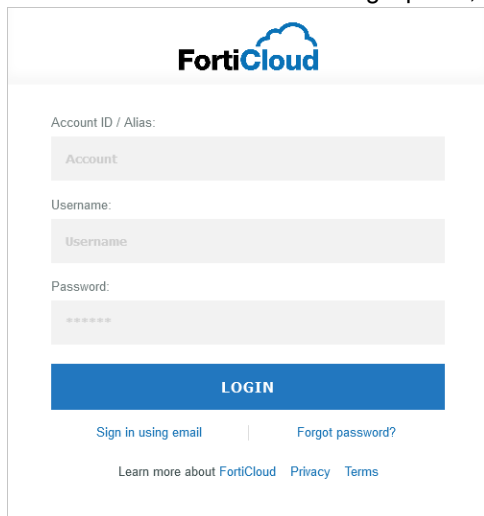
## IAM user account login

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 \(IAM\)](#).
2. 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*.

A screenshot of the FortiCloud login portal. At the top is the FortiCloud logo. Below it are three input fields: 'Account ID / Alias:' with a placeholder 'Account', 'Username:' with a placeholder 'Username', and 'Password:' with a placeholder '\*\*\*\*\*'. Below these fields is a blue 'LOGIN' button. At the bottom, there are two links: 'Sign in using email' and 'Forgot password?'. At the very bottom, there are three links: 'Learn more about FortiCloud', 'Privacy', and 'Terms'.

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, HTTPS, or SSH, 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 *Blueberry*. 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 > Admin > Admin Settings*.

**Admin Settings**

Language: Auto Detect

High Contrast Theme: OFF

Other Themes:

Blueberry	Kiwi	Cherry	Plum
Spring	Summer	Autumn	Winter
Circuit Board	Calla Lily	Binary Tunnel	Mars
Blue Sea	Technology	Landscape	Twilight
Canyon	Northern Light	Astronomy	Fish
Penguin	Mountain	Panda	Parrot
Cave	Zebra		

Password Policy: OFF

Display Options on GUI >

Fabric Authorization ⓘ

Authorization Address: lwoodward-test-sf700-mar31.fortidemo.fortinet.com

Authorization Port: 10406

Apply

2. Configure the following settings as needed, then click *Apply* to save your changes to all administrator accounts:

Administration Settings	
<b>HTTP Port</b>	Enter the TCP port to be used for administrative HTTP access. Default: 80. Select <i>Redirect to HTTPS</i> to redirect HTTP traffic to HTTPS.
<b>HTTPS Port</b>	Enter the TCP port to be used for administrative HTTPS access. Default: 443.
<b>HTTPS &amp; Web Service Server Certificate</b>	Select a certificate from the dropdown list.
<b>Idle Timeout</b>	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 <a href="#">Idle timeout on page 881</a> for more information.
<b>Idle Timeout (API)</b>	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.



<b>Idle Timeout (GUI)</b>	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.
<b>View Settings</b>	
<b>Language</b>	Select a language from the dropdown list. See <a href="#">GUI language on page 881</a> for more information.
<b>High Contrast Theme</b>	Toggle <i>ON</i> 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.
<b>Other Themes</b>	Select a theme for the GUI. The selected theme is not applied until you click <i>Apply</i> , allowing to you to sample different themes. Default: Blueberry.
<b>Password Policy</b>	Click to enable administrator password policies. See <a href="#">Password policy on page 880</a> and <a href="#">Password lockout and retry attempts on page 880</a> for more information.
<b>Minimum Length</b>	Select the minimum length for a password, from 8 to 32 characters. Default: 8.
<b>Must Contain</b>	Select the types of characters a password must contain.
<b>Admin Password Expires after</b>	Select the number of days a password is valid for, after which it must be changed.
<b>Display Options on GUI</b>	Click to expand the display options.
<b>Show Script</b>	Display the <i>Script</i> menu item. This menu is located on the <i>Device Manager</i> pane. This is an advanced FortiManager feature.
<b>Show Add Multiple Button</b>	Display the <i>Add Multiple Devices</i> option. This option is located on the <i>Device Manager &gt; Devices &amp; Groups</i> pane, under the <i>More</i> option in the toolbar. This is an advanced FortiManager feature.
<b>Show Device List Import/Export</b>	Select to display the <i>Import Device List</i> and <i>Export Device List</i> buttons. This option is located on the <i>Device Manager &gt; Devices &amp; Groups</i> pane, under the <i>More</i> option in the toolbar. This is an advanced FortiManager feature.
<b>Fabric Authorization</b>	<p>Specifies the accessible management IP of FortiManager for FortiOS to retrieve and use for authorization of a Security Fabric connection to FortiManager.</p> <p>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.</p> <p>Without this information, the browser popup window cannot connect to FortiManager in certain topologies, such as when NAT is used.</p> <p>See also <a href="#">Security Fabric authorization information for FortiOS on page 882</a>.</p>

<b>Authorization Address</b>	Type the accessible management IP for FortiManager.
<b>Authorization Port</b>	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.

<b>Minimum Length</b>	Specify the minimum number of characters that a password must be, from 8 to 32. Default: 8.
<b>Must Contain</b>	Specify the types of characters a password must contain: uppercase and lowercase letters, numbers, and/or special characters.
<b>Admin Password Expires after</b>	Specify the number of days a password is valid for. When the time expires, an administrator will be prompted to enter a new password.

## 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 > Admin > Admin 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.

### To change the idle timeout:

1. Go to *System Settings > Admin > Admin Settings*.
2. Change the *Idle Timeout* period as required.
3. Click *Apply*.

## 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 > Admin > Admin Settings*.
2. Under *Fabric Authorization*, set the following options:

<b>Authorization Address</b>	Type the GUI-accessible URL for FortiManager.
<b>Authorization Port</b>	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.
protocol Traffic protocol.
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.
  protocol Traffic protocol.
  src Source IP and mask.
```

## Two-factor authentication

FortiManager supports the following two methods for two-factor authentication:

- [FortiAuthenticator](#)
- [FortiToken Cloud](#)

### Two-factor authentication with FortiAuthenticator

To configure two-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:

<b>Username</b>	Enter a user name for the local user.
<b>Password creation</b>	Select Specify a password from the dropdown list.
<b>Password</b>	Enter a password. The password must be a minimum of 8 characters.
<b>Password confirmation</b>	Re-enter the password. The passwords must match.

<b>Allow RADIUS authentication</b>	Enable to allow RADIUS authentication.
<b>Role</b>	Select the role for the new user.
<b>Enable account expiration</b>	Optionally, select to enable account expiration. For more information see the <i>FortiAuthenticator Administration Guide</i> .

4. Click **OK** to continue to the *Change local user* page.

5. Configure the following settings, then click **OK**.

<b>Disabled</b>	Select to disable the local user.
<b>Password-based authentication</b>	Leave this option selected. Select <i>[Change Password]</i> to change the password for this local user.
<b>Token-based authentication</b>	Select to enable token-based authentication.
<b>Deliver token code by</b>	Select to deliver token by FortiToken, email, or SMS. Click <i>Test Token</i> to test the token.
<b>Allow RADIUS authentication</b>	Select to allow RADIUS authentication.
<b>Enable account expiration</b>	Optionally, select to enable account expiration. For more information see the <i>FortiAuthenticator Administration Guide</i> .
<b>User Role</b>	
<b>Role</b>	Select either <i>Administrator</i> or <i>User</i> .
<b>Full Permission</b>	Select to allow Full Permission, otherwise select the admin profiles to apply to the user. This option is only available when <i>Role</i> is <i>Administrator</i> .
<b>Web service</b>	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 <i>Role</i> is <i>Administrator</i> .
<b>Restrict admin login from trusted management subnets only</b>	Select to restrict admin login from trusted management subnets only, then enter the trusted subnets in the table. This option is only available when <i>Role</i> is <i>Administrator</i> .
<b>Allow LDAP Browsing</b>	Select to allow LDAP browsing. This option is only available when <i>Role</i> is <i>User</i> .

### 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*.

<b>Name</b>	Enter a name for the RADIUS client entry.
<b>Client name/IP</b>	Enter the IP address or Fully Qualified Domain Name (FQDN) of the FortiManager.
<b>Secret</b>	Enter the server secret. This value must match the FortiManager RADIUS server setting at <i>System Settings &gt; Admin &gt; Remote Authentication Server</i> .
<b>First profile name</b>	See the <i>FortiAuthenticator Administration Guide</i> .
<b>Description</b>	Enter an optional description for the RADIUS client entry.
<b>Apply this profile based on RADIUS attributes</b>	Select to apply the profile based on RADIUS attributes.
<b>Authentication method</b>	Select <i>Enforce two-factor authentication</i> from the list of options.
<b>Username input format</b>	Select specific user name input formats.
<b>Realms</b>	Configure realms.
<b>Allow MAC-based authentication</b>	Optional configuration.
<b>Check machine authentication</b>	Select to check machine based authentication and apply groups based on the success or failure of the authentication.
<b>Enable captive portal</b>	Enable various portals.
<b>EAP types</b>	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 > Admin > Remote Authentication Server*.
2. Click *Create New > RADIUS Server* in the toolbar.
3. Configure the following settings, then click *OK*.

<b>Name</b>	Enter a name to identify the FortiAuthenticator.
-------------	--

<b>Server Name/IP</b>	Enter the IP address or fully qualified domain name of your FortiAuthenticator.
<b>Port</b>	Enter the port for FortiAuthenticator traffic.
<b>Server Secret</b>	Enter the FortiAuthenticator secret.
<b>Secondary Server Name/IP</b>	Enter the IP address or fully qualified domain name of the secondary FortiAuthenticator, if applicable.
<b>Secondary Server Secret</b>	Enter the secondary FortiAuthenticator secret, if applicable.
<b>Authentication Type</b>	Select the authentication type the FortiAuthenticator requires. If you select the default <i>ANY</i> , FortiManager tries all authentication types. <b>Note:</b> RADIUS server authentication for local administrator users stored in FortiAuthenticator requires the <i>PAP</i> authentication type.

#### To create the administrator:

1. Go to *System Settings > Admin > Administrator*.
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 811](#).
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.

## Two-factor authentication with FortiToken Cloud

To use two-factor authentication with FortiToken Cloud, you must have an active FortiToken Cloud license registered on FortiCloud. For more information about this process, see the [FortiToken Cloud Admin Guide](#).

#### To configure two-factor authentication for administrators with FortiToken Cloud:

1. In FortiManager, go to *System Settings > Admin > Administrators* and click *Create New* or edit an existing administrator.
2. 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 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.



Create New Administrator

User Name

test

Avatar

T

+ Add Photo

- Remove Photo

Description

Admin Type

LOCAL

New Password

Confirm Password

FortiToken Cloud

Disable

FortiToken Mobile

Email

SMS

Email

test@fortinet.com

Country Dial Code

United States Canada

Mobile Number

1234567890

Administrative Domain

All ADOMs

All ADOMs except specified ones

Specify

Admin Profile

Restricted\_User

Policy Package

All Packages

Specify

JSON API Access

None

Theme Mode

Use Global Theme

Use Own Theme

Trusted Hosts

Meta Fields

Advanced Options

OK

Cancel

3. Enter the appropriate contact information.

4. Edit other fields as needed and click **OK**.

When the administrator logs in, they are prompted to enter the token code from their email, SMS, or FortiToken Mobile.

---

Please input FortiToken code:

# 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 891](#).

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.



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
- FortiCloud
- FortiGuard database downloaded by FortiManager
- Network
- HA
- Local certificates
- SNMP
- Mail server
- Syslog server
- 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 891](#).

## **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 890](#).

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 75](#).

This is not required when using *VRRP Failover Mode*.

**Cluster Status**

Refresh Column Settings Search...

SN	Mode	IP	Enable	Module Data Synchronized	Pending Module Data
FMG-VM0A16000566	Primary	10.3.106.63		0.0 KB	0.0 KB
FMG-VM0A17002226	Secondary	10.3.106.64		0.0 KB	0.0 KB

**Cluster Settings**

Failover Mode: **Manual** VRRP

Operation Mode: Standalone **Primary** Secondary

Peer IP and Peer SN: IP Type: IPv4 Peer IP: 10.3.106.64 Peer SN: FMG-VM0A17002226

Cluster ID: 1 (1-64)

Group Password: (2048-20480) MB

File Quota: 4096

Heart Beat Interval: 10 Seconds

Failover Threshold: 30 (1-255)

VIP: Click to select

VRRP Interface: Click to select

Priority: 1 (1-253)

Unicast: ☐

Monitored IP: IP: Interface: Click to select

Download Debug Log: Download

Apply

Configure the following settings:

<b>Cluster Status</b>	Monitor FortiManager HA status. See <a href="#">Monitoring HA status on page 897</a> .
<b>SN</b>	The serial number of the device.
<b>Mode</b>	The high availability mode, either <i>Primary</i> or <i>Secondary</i> .
<b>IP</b>	The IP address of the device.
<b>Enable</b>	Shows if the peer is currently enabled.
<b>Module Data Synchronized</b>	Module data synchronized in bytes.
<b>Pending Module Data</b>	Pending module data in bytes.
<b>Cluster Settings</b>	

<b>Failover Mode</b>	<p>Select <i>Manual</i> 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.</p> <p>Select <i>VRRP</i> 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.</p>
<b>Operation Mode</b>	<p>Select <i>Primary</i> to configure the FortiManager unit to be the primary unit in a cluster.</p> <p>Select <i>Secondary</i> to configure the FortiManager unit to be a backup unit in a cluster.</p> <p>Select <i>Standalone</i> to stop operating in HA mode.</p>
<b>Peer IP</b>	<p>Select the peer IP version from the dropdown list, either <i>IPv4</i> or <i>IPv6</i>. 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.</p> <p>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.</p>
<b>Peer SN</b>	Type the serial number of the FortiManager unit corresponding to the entered IP address.
<b>Cluster ID</b>	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.
<b>Group Password</b>	<p>A password for the HA cluster. All members of the HA cluster must have the same password.</p> <p>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.</p>
<b>File Quota</b>	<p>Enter the file quota, from 2048 to 20480 MB (default: 4096 MB).</p> <p>You cannot configure the file quota for backup units.</p>
<b>Heart Beat Interval</b>	<p>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.</p> <p>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.</p>
<b>Failover Threshold</b>	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.

<b>VIP</b>	Enter the VIP of the FortiManager-HA. This setting can only be configured when the <i>Failover Mode</i> is <i>VRRP</i> .
<b>VRRP Interface</b>	Select the VRRP interface. This setting can only be configured when the <i>Failover Mode</i> is <i>VRRP</i> .
<b>Priority</b>	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 <i>Failover Mode</i> is <i>VRRP</i> .
<b>Unicast</b>	Optionally, toggle this setting <i>ON</i> to use Unicast for the VRRP message. This setting can only be configured when the <i>Failover Mode</i> is <i>VRRP</i> .
<b>Monitored IP</b>	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 <i>Failover Mode</i> is <i>VRRP</i> .
<b>Download Debug Log</b>	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.



## GUI configuration steps

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:

<b>Failover Mode</b>	Manual
<b>Operation Mode</b>	Primary
<b>Peer IP</b>	172.20.120.23
<b>Peer SN</b>	<serial_number>
<b>Peer IP</b>	192.268.34.23
<b>Peer SN</b>	<serial_number>
<b>Cluster ID</b>	15
<b>Group Password</b>	password
<b>File Quota</b>	4096
<b>Heartbeat Interval</b>	5 (Keep the default setting.)
<b>Failover Threshold</b>	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:

<b>Failover Mode</b>	Manual
<b>Operation Mode</b>	Secondary
<b>Priority</b>	5 (Keep the default setting.)
<b>Peer IP</b>	172.20.120.45
<b>Peer SN</b>	<serial_number>
<b>Cluster ID</b>	15

<b>Group Password</b>	password
<b>File Quota</b>	4096
<b>Heartbeat Interval</b>	5 (Keep the default setting.)
<b>Failover Threshold</b>	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:

<b>Failover Mode</b>	Manual
<b>Operation Mode</b>	Secondary
<b>Priority</b>	5 (Keep the default setting.)
<b>Peer IP</b>	192.168.20.23
<b>Peer SN</b>	<serial_number>
<b>Cluster ID</b>	15
<b>Group Password</b>	password
<b>File Quota</b>	4096
<b>Heartbeat Interval</b>	5 (Keep the default setting.)
<b>Failover Threshold</b>	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.

## 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:

<b>Cluster Status</b>	The cluster status can be <i>Up</i> if this unit is received HA heartbeat packets from all of its configured peers. The cluster status will be <i>Down</i> if the cluster unit is not receiving HA heartbeat packets from one or more of its configured peers.
<b>Mode</b>	The role of the FortiManager unit in the cluster. The role can be: <ul style="list-style-type: none"> <li>• <i>Primary</i>: for the primary unit.</li> <li>• <i>Secondary</i>: for the backup units.</li> </ul>
<b>Module Data Synchronized</b>	The amount of data synchronized between this cluster unit and other cluster units.
<b>Pending Module Data</b>	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](#).

## FortiManager support for FortiAnalyzer HA

You can manage FortiAnalyzer HA via FortiManager. FortiManager retrieves the cluster member list and updates the information whenever it changes, including FortiAnalyzer HA failover or a change in members.

### To enable support for FortiAnalyzer HA:

1. Go to *Device Manager > Device and Groups*.
2. Click the down arrow next to *Add Devices*. Select *Add FortiAnalyzer*.

The Add FortiAnalyzer dialog opens.

**Add FortiAnalyzer**

**Discover**

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

IP Address: 10.3.121.202

Username: admin

Password: [masked]

Next > Cancel

3. From the *Add FortiAnalyzer* box, add FortiAnalyzer HA to FortiManager DVM by HA cluster's VIP, and click *Next*. The FortiAnalyzer HA is discovered with its HA status information. Click *Next* to continue.

**Add FortiAnalyzer**

The following information has been discovered from the device:

IP Address	10.3.121.202
Host Name	FAZVM64-HA
SN	FAZ-VMTM20001379
Model	FortiAnalyzer-VM64
Firmware Version	6.4.0, build5792 (GA)
HA Status	Active - Passive
Administrator	admin

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

Name: FAZVM64-HA

Description: [empty]

Next > Cancel

FortiAnalyzer HA is added successfully. Click *Finish*.

### Add FortiAnalyzer

Status:

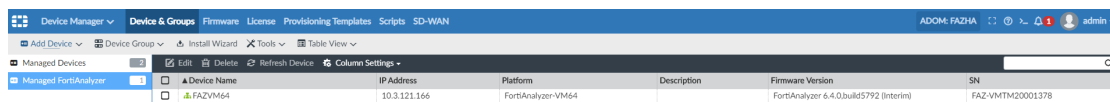
✓ FortiAnalyzer Added Successfully

Finish

4. 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.

Device Name	IP Address	Platform	Description	Firmware Version	SN
FAZVM64	10.3.121.202	FortiAnalyzer-VM64		FortiAnalyzer 6.4.0, build5792 (Interim)	FAZ-VMTM20001379

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".



Device Name	IP Address	Platform	Description	Firmware Version	SN
FAZVM64	10.3.121.166	FortiAnalyzer-VM64		FortiAnalyzer 6.4.0.build5792 (interim)	FAZ-VM64M20001378



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.

# Management Extensions

The *Management Extensions* pane allows you to enable licensed applications that are released and signed by Fortinet. The applications are installed and run on FortiManager.



The *Management Extensions* pane is only displayed in the GUI after at least one management extension application (MEA) is enabled and running on FortiManager.

You must enable your first MEA using the CLI; subsequent MEAs can be enabled using the GUI.

A number of management extension applications (MEAs) are available. The following table identifies the available applications and any ADOM requirements needed to access the application:

Management Extension Application	ADOM Requirements for Access
<a href="#">FortiAIOPS MEA on page 900</a>	ADOM version 7.0 or later
<a href="#">FortiPortal MEA on page 901</a>	ADOM version 6.4 or later
<a href="#">FortiSigConverter MEA on page 901</a>	ADOM version 6.4 or later
<a href="#">FortiSOAR MEA on page 901</a>	ADOM version 6.4 or later
<a href="#">FortiWLM MEA on page 901</a>	ADOM version 6.4 or later
<a href="#">Policy Analyzer MEA on page 902</a>	ADOM version 7.0 or later
<a href="#">Universal Connector MEA on page 902</a>	ADOM version 7.0 or later

See also [Enabling management extension applications on page 902](#).

For information on how to access event logs for a management extension, see [Accessing management extension logs on page 904](#).

## FortiAIOPS MEA

FortiAIOPS management extension application (MEA) aims at diagnosing and troubleshooting network issues by analyzing potential problems and suggesting remedial steps based on the Artificial Intelligence (AI) and Machine Learning (ML) architecture that it is built upon. FortiAIOPS learns from your network data to report statistics on a comprehensive and simple dashboard, providing network visibility and deep insight into your network. Thus, enabling you to effectively manage your connected devices and resolve network issues swiftly with the help of AI/ML.

FortiAIOPS MEA is hosted on FortiManager.

For details about using FortiAIOPS MEA, see the *FortiAIOPS MEA User Guide* on the [Document Library](#).

## FortiPortal MEA

You can use FortiPortal management extension application (MEA) to operate a cloud-based hosted security management and log retention service. For details about using FortiPortal MEA, see the *FortiPortal MEA Administration Guide* on the [Document Library](#).

When FortiPortal is enabled, you can use it to provide a self-service management interface for customers to monitor and configure security instances without direct FortiManager access.

FortiPortal provides a comprehensive set of security management and analytics within a multi-tenant, multi-tier management framework. This enables Managed Security Service Providers (MSSPs) to give their customers controlled access to configuration and analytics. Enterprises and educational institutions can use FortiPortal to delegate a limited set of management and analytic capabilities to business units, departments, colleges, and so on.

## FortiSigConverter MEA

FortiSigConverter management extension application (MEA) imports Snort rules directly into FortiManager and converts them to Fortinet supported IPS signatures. Snort is a popular open source Network Intrusion Detection System (NIDS). For details about using FortiSigConverter MEA, see the *FortiSigConverter MEA Administration Guide* on the [Document Library](#).

When FortiSigConverter is enabled, you can import Snort signature files and convert them into IPS signatures. After the signature files are converted, you can use the application to select rules you want to push to FortiManager. To view the signatures in FortiManager, go to *Policy & Objects > Object Configurations*.

## FortiSOAR MEA

You can enable the Fortinet Security Orchestration, Automation, and Response (FortiSOAR) management extension application (MEA) on FortiManager, and use it to manage the entire lifecycle of a threat or breach within your organization. For details about using FortiSOAR MEA, see the *FortiSOAR MEA Administration Guide* on the [Document Library](#).

## FortiWLM MEA

You can use FortiWLM management extension application (MEA) to monitor, operate, and administer wireless networks on FortiGates that are managed by FortiManager. For details about using FortiWLM MEA, see the *FortiWLM MEA Administration Guide* on the [Document Library](#).

When FortiWLM is enabled, the FortiManager configuration backup includes the configuration for FortiWLM too. See [Backing up the system on page 726](#).

When FortiWLM is enabled, you can use it to monitor your wireless network. You must configure the wireless network by using the *Device Manager* and *AP Manager* modules of FortiManager.

## Policy Analyzer MEA

Policy Analyzer management extension application (MEA) is used to learn about FortiGate traffic from logs, and present you with several policy options, based on the needs of the analyzed traffic. You can choose a policy option, and Policy Analyzer MEA adds a policy block to the policy, and triggers installation of the updated policy package to FortiGate.

In order to use Policy Analyzer MEA, you must have the following products:

- FortiGate running FortiOS 7.0.2
- FortiAnalyzer 7.0.2
- FortiManager 7.0.2
  - ADOM version 7.0
  - FortiManager must manage FortiGate.
  - FortiManager must be able to communicate with FortiAnalyzer by its IP address, and the FortiManager administrator requires valid FortiAnalyzer credentials to authorize access to the logs.

For details about configuring devices for Policy Analyzer MEA and using Policy Analyzer MEA, see the *Policy Analyzer 1.0.0 Administration Guide* on the [Document Library](#).

## Universal Connector MEA

Universal Connector management extension application (MEA) lets you configure fabric connectors to external applications, such as Guardicore Centra. Fabric connectors let you retrieve information from external applications to FortiManager, and use the information in FortiManager to create objects for use in policies that are installed to FortiGates.

FortiManager hosts Universal Connector, and Universal Connector hosts fabric connectors to external applications.

For details about using Universal Connector MEA, see the *Universal Connector 1.0.0 Administration Guide* on the [Document Library](#).

## Enabling management extension applications



Some management extension applications require a minimum amount of memory or a minimum number of CPU cores.

Before you enable a management extension application, review the requirements in the [FortiManager 7.0.2 Release Notes](#).

---

FortiManager provides access to applications that are released and signed by Fortinet.



Only administrators with a *Super\_User* profile can enable management extensions.

A CA certificate is required to install management extensions on FortiManager. See [CA certificates on page 780](#).

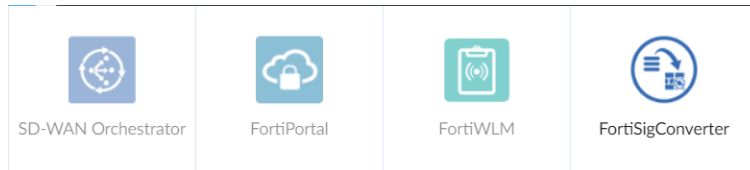
Some management extension applications, such as FortiAI Ops, require read-write JSON API access to be enabled. See [Enabling read-write JSON API access on page 615](#).

---



**To enable management extensions:**

1. Go to *Management Extensions*.
  - The first MEA used on FortiManager must be enabled using the CLI. After it is enabled and running, *the Management Extensions* pane is displayed in the GUI and subsequent MEAs can be enabled in the GUI following the steps below. For instructions on enabling your first MEA, see [CLI for management extensions on page 903](#).
  - Some management applications are only available in the root ADOM or in specific ADOM versions.
2. Click a grayed out tile to enable the application.  
Grayed out tiles represent disabled applications. In the following example, FortiSigConverter is enabled, and the other management applications are disabled.



3. Click **OK** in the dialog that appears. It might take some time to install the application.

**CLI for management extensions**

You can use the CLI console to enable, disable, update, debug, and check the management extension.

**To enable management extensions:**

1. Enable the production registry:
 

```
FMG-VM64 # config system docker
(docker)# set status
enable Enable production registry.
```
2. Enable the management application.
 

```
(docker)# set
fortiaioops Enable/disable container.
fortiportal Enable/disable container.
fortisigconverter Enable/disable container.
fortisoar Enable/disable container.
fortiwlrm Enable/disable container.
policyanalyzer Enable/disable container.
universalconnector Enable/disable container.
```

**To disable management extensions:**

```
config system docker
(docker)# get
(docker)# set {fortiaioops | fortiportal | fortisigconverter | fortisoar | fortiwlrm |
policyanalyzer | universalconnector} disable
```

**To debug management extensions:**

```
diagnose debug application docker
```

**To clean up or check management extensions:**

```
diagnose docker {cleanup|status}
```

**To limit CPU and RAM resources for management extensions:**

```
config system docker
  (docker)# set cpu <integer> #Set the maximum % of CPU usage (10 - 50, default = 50).
  (docker)# set mem <integer> #Set the maximum % of RAM usage (10 - 50, default = 50).
```



- The CLI commands allow you to set the resource limit globally for all management extension applications.
- If management extension applications reach the limit of allocated FortiManager resource, a warning appears in the *Alert Message Console* widget.

See also [Checking for new versions and upgrading on page 904](#).

## Accessing management extension logs

Event logs generated by a management extension are available in the local event log of FortiManager. They are displayed in the following locations in *System Settings*:

- *Alert Message Console* widget
- *Event log* pane

**To access management extension logs in the *Alert Message Console* widget:**

1. Go to *System Settings > Dashboard*.
2. In the *Dashboard* pane, locate the *Alert Message Console* widget.  
The recently generated management extension local logs are displayed in the *Alert Message Console* widget.

**To access management extension logs in the *Event Log* pane:**

1. Go to *System Settings > Event Log* to view the local log list.  
The recently generated management extension local logs are displayed in the *Event Log* pane.

## Checking for new versions and upgrading

You can check whether a new version of an enabled management extension application is available on the Fortinet registry by using the CLI.

When the latest version of an enabled management extension application is running on FortiManager, the version is reported as *(up to date)*. When a new image is available on the Fortinet registry for an enabled management extension application, the output displays *(new image available)*.

In the example below, FortiSOAR MEA is enabled and a new version is available for installation. You can upgrade FortiSOAR MEA by using the CLI.

### To check for new versions of enabled management extensions:

```
diagnose docker status
  fortiaioops: disabled
  fortiportal: running (up to date)
  fortisigconverter: running (up to date)
  fortisoar: running (new image available)
  fortiwlm: running (up to date)
  universalconnector: disabled
```

### To upgrade enabled management extensions:

```
diagnose docker upgrade {fortiaioops | fortiportal | fortisigconverter | fortisoar | fortiwlm
  | universalconnector}
```

# 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  $\geq 1071741825$  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 909](#)
- [FGFM connection established through FortiGate on page 909](#)

### 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-establish 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 909](#).

### 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 910](#)

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 911](#).

## 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.

**Edit Device**

Name: Branch\_Office\_01

Description: 0/128

IP Address: 10.0.11.2

Serial Number: FGVM02TM21010944 (FortiGate-VM64-KVM)

Firmware Version: FortiGate 7.0.2, build0234

Admin User: admin

Password: [Masked]

Connected Interface: To-HQ-B

HA Mode: Stand-Alone

**Meta Fields**

Company/Organization: [Optional]

Contact Email: [Optional]

Contact Phone Number: [Optional]

Address: [Optional]

Geographic Coordinate: 37.338207 (Latitude) -121.88633 (Longitude)

OK Cancel

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](http://www.fortinet.com)

Copyright© 2023 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 General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. 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.