



# FortiManager - Administration Guide

Version 6.2.1

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

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

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



December 2, 2019

FortiManager 6.2.1 Administration Guide

02-621-476230-20190819

# TABLE OF CONTENTS

<b>Setting up FortiManager</b>	<b>12</b>
Connecting to the GUI	12
Security considerations	13
Restricting GUI access by trusted host	13
Other security considerations	13
GUI overview	14
Panels	16
Color themes	17
Full-screen mode	17
Switching between ADOMs	17
Using the right-click menu	17
Avatars	17
Showing and hiding passwords	18
FortiAnalyzer Features	18
Enable or disable FortiAnalyzer features	19
Configuring FortiManager appliances	20
Adding devices	20
Installing to managed devices	21
Enabling central management	21
Monitoring managed devices	22
Restarting and shutting down	22
<b>FortiManager Key Concepts</b>	<b>24</b>
FortiManager modules	24
Modules for FortiAnalyzer feature set	25
Object database and FortiManager modules	25
Inside the FortiManager system	26
Communication protocols and devices	26
Object database and devices	27
ADOMs and devices	29
Operations	30
Key features of the FortiManager system	31
Security Fabric	31
Configuration revision control and tracking	32
Centralized management	32
Administrative domains	32
Local FortiGuard service provisioning	32
Firmware management	32
Scripting	32
Logging and reporting	32
Fortinet device life cycle management	32
<b>Firewall Devices</b>	<b>34</b>
ADOMs	35
Adding devices	35
Adding devices using the wizard	36

Authorizing devices .....	43
Hiding unauthorized devices .....	43
Add a VDOM to a device .....	45
Adding a Security Fabric group .....	46
Import policy wizard .....	47
Adding FortiAnalyzer devices .....	49
Adding FortiAnalyzer devices with the wizard .....	50
Viewing policy rules .....	53
Importing devices .....	53
Importing detected devices .....	54
Importing and exporting device lists .....	54
Configuring devices .....	55
Configuring a device .....	56
Out-of-Sync device .....	57
Configuring VDOMs .....	57
Using the device dashboard .....	60
View system dashboard for managed/logging devices .....	60
View system interfaces .....	62
CLI-Only Objects menu .....	62
System dashboard widgets .....	63
Installing to devices .....	66
Using the Install Wizard to install policy packages and device settings .....	66
Using the Install Wizard to install device settings only .....	67
View a policy package diff .....	68
Managing devices .....	69
Using the quick status bar .....	69
Customizing columns .....	70
Refreshing a device .....	70
Editing device information .....	70
Deleting a device .....	72
Replacing a managed device .....	72
Setting unauthorized device options .....	73
Using the CLI console for managed devices .....	73
Displaying Security Fabric topology .....	74
Manage Devices from Map View .....	74
Managing device configurations .....	78
View configurations for device groups .....	79
Checking device configuration status .....	81
Managing configuration revision history .....	82
Device groups .....	86
Default device groups .....	86
Add device groups .....	86
Manage device groups .....	86
Firmware .....	87
View firmware for device groups .....	87
Upgrade firmware for device groups .....	87
Firmware Management .....	88
License .....	89



View licenses for device groups .....	89
License Management .....	90
Add-on license .....	91
Provisioning Templates .....	91
System templates .....	92
Threat Weight templates .....	93
Certificate templates .....	94
Scripts .....	96
Enabling scripts .....	96
Configuring scripts .....	97
CLI script group .....	102
Script syntax .....	103
Script history .....	107
Script samples .....	107
SD-WAN .....	128
Enabling central SD-WAN management .....	128
Interface members .....	129
SD-WAN templates .....	131
Health-Check Servers .....	138
Assigned devices .....	140
Monitor SD-WAN .....	140
IPsec VPN Wizard .....	142
Configure BGP Neighbor .....	144
FortiExtender .....	145
FortiMeter .....	147
Overview .....	147
Points .....	148
Authorizing metered VMs .....	149
Monitoring VMs .....	150
FortiGate chassis devices .....	150
Viewing chassis dashboard .....	151
<b>Firewall Policy &amp; Objects .....</b>	<b>156</b>
About policies .....	157
Policy theory .....	158
Global policy packages .....	159
Policy workflow .....	159
Provisioning new devices .....	159
Day-to-day management of devices .....	160
Display options .....	160
Managing policy packages .....	161
Create new policy packages .....	161
Create new policy package folders .....	163
Edit a policy package or folder .....	163
Clone a policy package .....	163
Remove a policy package or folder .....	164
Assign a global policy package .....	164
Install a policy package .....	165
Reinstall a policy package .....	165

Schedule a policy package install .....	167
Export a policy package .....	168
Policy package installation targets .....	168
Perform a policy consistency check .....	170
View logs related to a policy rule .....	172
Find and replace objects .....	172
Managing policies .....	173
Policy Lookup .....	175
Creating policies .....	176
Editing policies .....	176
Creating Policy Blocks .....	182
IP policies .....	184
Create New Firewall Policy .....	190
Create New Security Policy .....	193
Virtual wire pair policy .....	196
NAT policies .....	198
Proxy policy .....	199
Central SNAT .....	202
Central DNAT .....	203
DoS policies .....	209
Interface policies .....	211
Multicast policy .....	212
Local in policies .....	213
Traffic shaping policy .....	214
Managing objects and dynamic objects .....	215
Create a new object .....	216
Creating an IPv6 Address Template .....	218
Promote an Object to Global Database .....	220
Map a dynamic ADOM object .....	220
Map a dynamic device object .....	221
Map a dynamic device group .....	224
Remove an object .....	224
Edit an object .....	224
Push to device .....	225
Clone an object .....	226
Search objects .....	226
Find unused objects .....	226
Find and merge duplicate objects .....	227
Export signatures to CSV file format .....	227
CLI-Only objects .....	228
FortiToken configuration example .....	228
FSSO user groups .....	229
Interface mapping .....	231
VIP mapping .....	232
Modify existing interface-zone mapping .....	232
Create a new shaping profile .....	233
ADOM revisions .....	234
<b>Fabric View .....</b>	<b>237</b>
Security Fabric Topology .....	237

Physical Topology .....	238
Logical Topology .....	239
Filter Topology Views .....	240
Search Topology Views .....	241
Security Rating .....	241
Enabling the Security Rating tab .....	242
Viewing Security Fabric Ratings .....	242
Fabric Connectors .....	243
SDN .....	243
Threat Feeds .....	261
SSO/Identity .....	262
<b>SOC Monitoring .....</b>	<b>283</b>
Monitors .....	283
Device Status .....	283
Using the Monitors dashboard .....	285
Customizing the Monitors dashboard .....	286
<b>VPN .....</b>	<b>287</b>
Overview .....	287
Enabling central VPN management .....	288
DDNS support .....	289
IPsec VPN Communities .....	290
Managing IPsec VPN communities .....	290
Creating IPsec VPN communities .....	290
VPN community settings .....	292
Monitoring IPsec VPN tunnels .....	298
Map View .....	299
IPsec VPN gateways .....	300
Managing VPN gateways .....	300
Creating managed gateways .....	300
Creating external gateways .....	305
VPN security policies .....	306
Defining policy addresses .....	307
Defining security policies .....	307
SSL VPN .....	308
Manage SSL VPNs .....	308
Portal profiles .....	311
Monitor SSL VPNs .....	316
<b>Access Points .....</b>	<b>318</b>
Managed APs .....	318
Quick status bar .....	319
Managing APs .....	320
FortiAP groups .....	325
Authorizing and deauthorizing FortiAP devices .....	326
Assigning profiles to FortiAP devices .....	326
Rogue APs .....	327
Connected clients .....	328
Monitor .....	329

Clients Monitor .....	329
Health Monitor .....	330
Map view .....	331
Google map .....	331
Floor map .....	332
WiFi profiles .....	334
AP profiles .....	334
SSIDs .....	340
WIDS profiles .....	348
Bluetooth profiles .....	352
QoS profiles .....	354
Bonjour profiles .....	356
<b>FortiSwitch Manager .....</b>	<b>359</b>
Managed Switches .....	359
Quick status bar .....	360
Managing FortiSwitches .....	360
Zero Touch Deployment for FortiSwitch .....	362
Authorizing and deauthorizing FortiSwitch devices .....	366
Assigning templates to FortiSwitch devices .....	367
Monitor .....	367
FortiSwitch Templates .....	368
FortiSwitch templates .....	368
FortiSwitch VLANs .....	371
FortiSwitch security policies .....	378
<b>Endpoint Compliance .....</b>	<b>381</b>
How FortiManager fits into endpoint compliance .....	382
FortiTelemetry .....	382
Viewing devices .....	383
Enabling FortiTelemetry on interfaces .....	383
Enabling endpoint control on interfaces .....	384
Assigning FortiClient profile packages to devices .....	384
Monitor .....	384
Monitoring FortiClient endpoints .....	385
Monitoring FortiClient endpoints by compliance status .....	386
Monitoring FortiClient endpoints by interface .....	386
Exempting non-compliant FortiClient endpoints .....	386
FortiClient profiles .....	387
Viewing profile packages .....	387
Viewing FortiClient profiles .....	387
Creating FortiClient profile packages .....	388
Creating FortiClient profiles .....	389
Editing FortiClient profiles .....	393
Deleting FortiClient profiles .....	393
Importing FortiClient profiles .....	393
Assigning profile packages .....	393
<b>Device Firmware and Security Updates .....</b>	<b>394</b>
Settings .....	395

Connecting the built-in FDS to the FDN .....	398
Operating as an FDS in a closed network .....	399
Configuring devices to use the built-in FDS .....	401
Matching port settings .....	402
Handling connection attempts from unauthorized devices .....	402
Configure a FortiManager without Internet connectivity to access a local FortiManager as FDS .....	402
Configuring FortiGuard services .....	403
Enabling push updates .....	403
Enabling updates through a web proxy .....	405
Overriding default IP addresses and ports .....	405
Scheduling updates .....	406
Accessing public FortiGuard web and email filter servers .....	406
Logging events related to FortiGuard services .....	407
Logging FortiGuard antivirus and IPS updates .....	407
Logging FortiGuard web or email filter events .....	407
Restoring the URL or antispam database .....	408
Licensing status .....	409
Package management .....	409
Receive status .....	410
Service status .....	410
Query server management .....	412
Receive status .....	412
Query status .....	413
Firmware images .....	413
<b>Locks for Restricting Configuration Changes .....</b>	<b>415</b>
Normal mode .....	415
Enable normal mode .....	416
Locking an ADOM .....	416
Locking a device .....	417
Locking a policy package .....	418
Workflow mode .....	419
Enable workflow mode .....	419
Workflow approval .....	420
Workflow sessions .....	421
<b>System Settings .....</b>	<b>428</b>
Dashboard .....	429
Customizing the dashboard .....	430
System Information widget .....	431
System Resources widget .....	436
License Information widget .....	436
Unit Operation widget .....	437
Alert Messages Console widget .....	438
Log Receive Monitor widget .....	438
Insert Rate vs Receive Rate widget .....	439
Log Insert Lag Time widget .....	439
Receive Rate vs Forwarding Rate widget .....	440

Disk I/O widget .....	440
Logging Topology .....	440
Network .....	441
Configuring network interfaces .....	441
Disabling ports .....	443
Changing administrative access .....	443
Static routes .....	443
RAID Management .....	444
Supported RAID levels .....	444
Configuring the RAID level .....	447
Monitoring RAID status .....	447
Checking RAID from command line .....	448
Swapping hard disks .....	449
Adding hard disks .....	450
Administrative Domains .....	450
Enabling and disabling the ADOM feature .....	451
ADOM device modes .....	452
ADOM modes .....	452
Managing ADOMs .....	455
Deleting ADOMs .....	460
ADOM versions .....	461
Concurrent ADOM access .....	462
Locking an ADOM .....	463
Upgrading an ADOM .....	464
Certificates .....	464
Local certificates .....	464
CA certificates .....	467
Certificate revocation lists .....	468
Fetcher Management .....	469
Fetching profiles .....	470
Fetch requests .....	471
Synchronizing devices and ADOMs .....	473
Fetch monitoring .....	474
Event Log .....	474
Event log filtering .....	476
Task Monitor .....	476
SNMP .....	478
SNMP agent .....	478
SNMP v1/v2c communities .....	480
SNMP v3 users .....	483
SNMP MIBs .....	484
SNMP traps .....	485
Fortinet & FortiManager MIB fields .....	486
Mail Server .....	487
Syslog Server .....	489
Meta Fields .....	490
Device logs .....	491
Configuring rolling and uploading of logs using the GUI .....	492

Configuring rolling and uploading of logs using the CLI .....	494
File Management .....	495
Advanced Settings .....	496
<b>Administrators .....</b>	<b>497</b>
Trusted hosts .....	497
Monitoring administrators .....	498
Disconnecting administrators .....	498
Managing administrator accounts .....	498
Creating administrators .....	500
Editing administrators .....	504
Deleting administrators .....	504
Restricted administrators .....	505
Administrator profiles .....	513
Permissions .....	514
Creating administrator profiles .....	517
Editing administrator profiles .....	519
Cloning administrator profiles .....	519
Deleting administrator profiles .....	520
Authentication .....	520
Public Key Infrastructure .....	520
Managing remote authentication servers .....	522
LDAP servers .....	523
RADIUS servers .....	525
TACACS+ servers .....	526
Remote authentication server groups .....	527
SAML admin authentication .....	528
Global administration settings .....	529
Password policy .....	531
Password lockout and retry attempts .....	531
GUI language .....	532
Idle timeout .....	532
Two-factor authentication .....	533
Configuring FortiAuthenticator .....	533
Configuring FortiManager .....	535
<b>High Availability .....</b>	<b>537</b>
Configuring HA options .....	539
General FortiManager HA configuration steps .....	540
GUI configuration steps .....	541
Monitoring HA status .....	543
Upgrading the FortiManager firmware for an operating cluster .....	544
<b>Change Log .....</b>	<b>545</b>

# 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 12](#)
- [Security considerations on page 13](#)
- [GUI overview on page 14](#)
- [FortiAnalyzer Features on page 18](#)
- [Configuring FortiManager appliances on page 20](#)
- [Adding devices on page 20](#)
- [Installing to managed devices on page 21](#)
- [Enabling central management on page 21](#)
- [Monitoring managed devices on page 22](#)
- [Restarting and shutting down on page 22](#)

## 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.

### 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`.
4. Type `admin` in the *Name* field, leave the *Password* field blank, and click *Login*.  
The *Change Password* dialog box is displayed.
5. Change the default password now, or click *Later* to change the password later:
  - a. In the *New Password* box, type a new password.
  - b. In the *Confirm Password* box, type the new password again, and click *OK*.



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 14](#).



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 441](#).

---



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 443](#).

---



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 498](#) for information.

## 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 13](#)
- [Other security considerations on page 13](#)

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

### Other security considerations

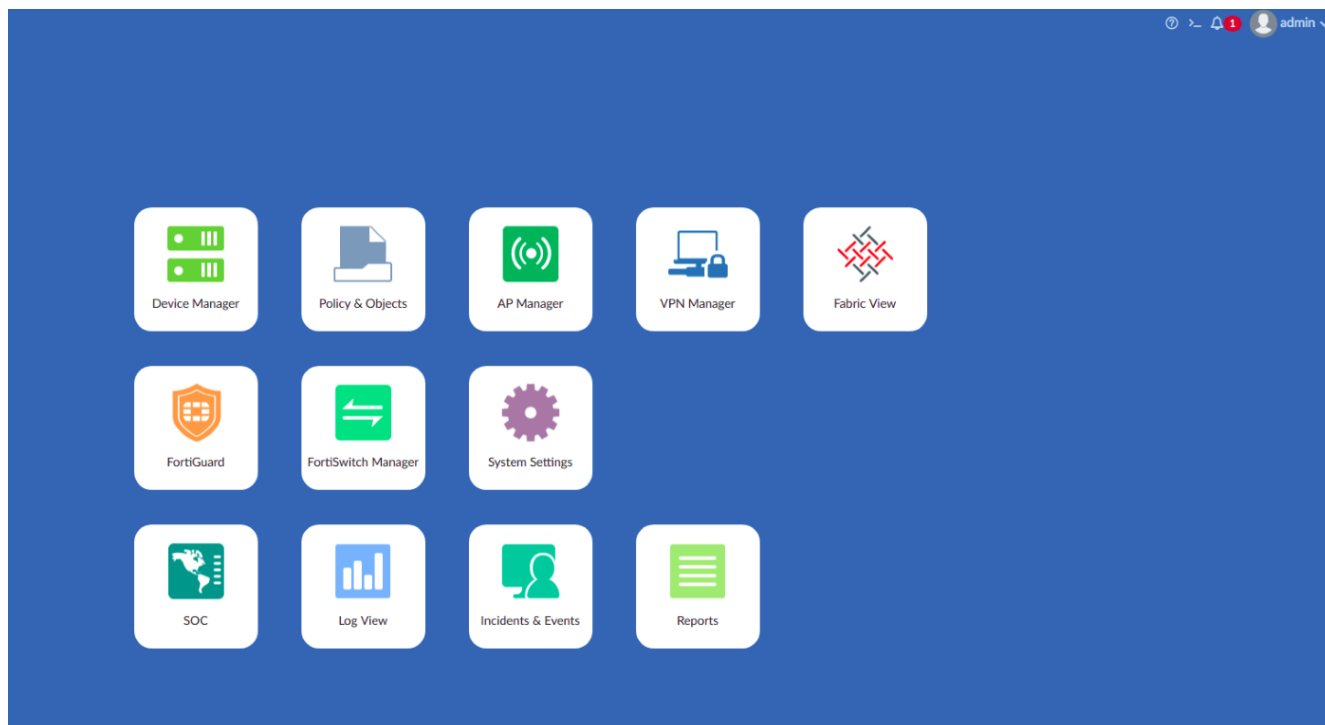
Other security consideration for restricting access to the FortiManager GUI include the following:

- 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.

## 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>	Manage devices, VDOMs, groups, firmware images, device licenses, and scripts. You can also configure system, threat weight, and Certificate templates, and view real-time monitor data. See <a href="#">Firewall Devices on page 34</a> .
<b>Policy &amp; Objects</b>	Configure policy packages and objects. For more information, see <a href="#">Firewall Policy &amp; Objects on page 156</a> .
<b>AP Manager</b>	Configure and manage FortiAP access points. For more information, see <a href="#">Access Points on page 318</a> .
<b>FortiClient Manager</b>	Manage FortiClient profiles and monitor FortiClient endpoints that are registered to FortiGate devices. See <a href="#">Endpoint Compliance on page 381</a> .
<b>VPN Manager</b>	Configure and manage VPN connections. You can create VPN topologies and managed/external gateways. For more information, see <a href="#">VPN on page 287</a> .

<b>Fabric View</b>	Configure fabric connectors and view Security Fabric Ratings. See <a href="#">Fabric View on page 237</a> .
<b>FortiGuard</b>	Manage communication between devices and the FortiManager using the FortiGuard protocol. See <a href="#">Device Firmware and Security Updates on page 394</a> .
<b>FortiSwitch Manager</b>	Configure and manage FortiSwitch devices. For more information, see <a href="#">FortiSwitch Manager on page 359</a> .
<b>SOC</b>	View device status information in real-time. When FortiAnalyzer features are enabled, FortiView and additional predefined SOC Monitor dashboards are available. See <a href="#">SOC Monitoring on page 283</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>Incidents &amp; Events</b>	Configure and view events for logging devices. 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 428</a> .

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>	If ADOMs are enabled, the required ADOM can be selected from the dropdown list. If enabled, ADOMs can also be locked or unlocked. The ADOMs available from the ADOM menu will vary depending on the privileges of the current user.
<b>Full Screen</b>	Click to view only the content pane in the browser window. See <a href="#">Full-screen mode on page 17</a> .
<b>Help</b>	Click to open the FortiManager online help, or view the <i>About</i> information for your device (Product, Version, and Build Number).
<b>CLI Console</b>	Click the <i>CLI Console</i> icon on the right side of the banner on any page. The CLI console is a terminal window that enables you to configure the FortiManager unit using CLI commands directly from the GUI, without making a separate SSH, or local console connection to access the CLI. When using the CLI console, you are logged in with the same administrator account that you used to access the GUI. You can enter commands by typing them, or you can copy and paste commands into or out of the console. Click <i>Detach</i> in the CLI Console toolbar to open the console in a separate window. <b>Note:</b> The <i>CLI Console</i> requires that your web browser support JavaScript.

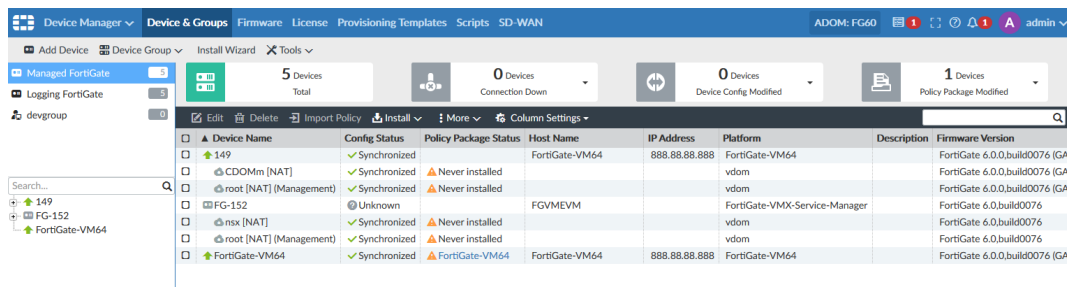
<b>Notification</b>	Click to display a list of notifications. Select a notification from the list to take action on the issue.
<b>admin</b>	Click to change the password or log out of the GUI.

## Panes

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

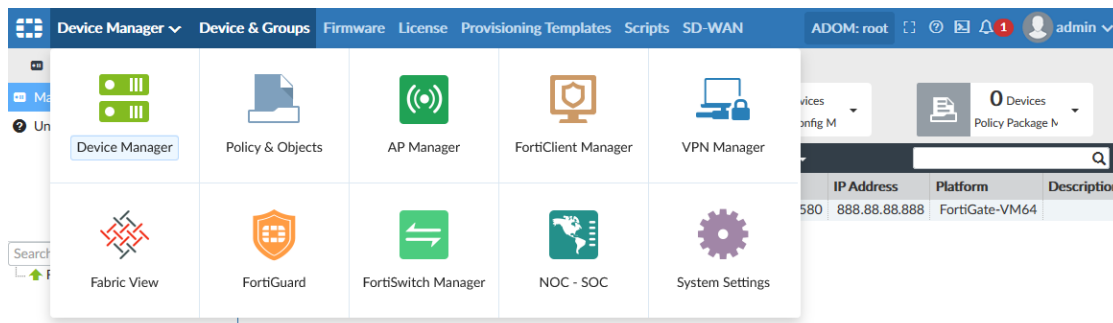
<b>Banner</b>	Along the top of the page; includes the home button (Fortinet logo), tile menu, ADOM menu (when enabled), admin menu, notifications, help button, and CLI console button.
<b>Tree menu</b>	On the left side of the screen; includes the menus for the selected pane.
<b>Content pane</b>	Contains 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> .

The *Device Manager* pane includes a quick status bar on the top of the content pane that provides quick information on the state of the devices in the current device group. Clicking a status updates the content pane to display the relevant devices. See [Firewall Devices on page 34](#) for more information.



Device Name	Config Status	Policy Package Status	Host Name	IP Address	Platform	Description	Firmware Version
149	Synchronized	Never installed	FortiGate-VM64	888.88.88.888	FortiGate-VM64		FortiGate 6.0.0.build0076 (GA)
CDOMm [NAT]	Synchronized	Never installed			vdom		FortiGate 6.0.0.build0076 (GA)
root [NAT] (Management)	Synchronized	Never installed			vdom		FortiGate 6.0.0.build0076 (GA)
FG-152	Unknown		FGVMEVM		FortiGate-VMX-Service-Manager		FortiGate 6.0.0.build0076
nsx [NAT]	Synchronized	Never installed			vdom		FortiGate 6.0.0.build0076
root [NAT] (Management)	Synchronized	Never installed			vdom		FortiGate 6.0.0.build0076
FortiGate-VM64	Synchronized	FortiGate-VM64	FortiGate-VM64	888.88.88.888	FortiGate-VM64		FortiGate 6.0.0.build0076 (GA)

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.



Device Manager	Policy & Objects	AP Manager	FortiClient Manager	VPN Manager
Fabric View	FortiGuard	FortiSwitch Manager	NOC - SOC	System Settings

## 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 529](#).

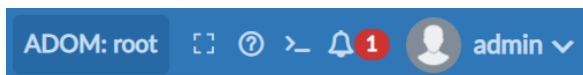
## Full-screen mode

You can view several panes in full-screen mode. When a pane is in full-screen mode, the tree menu on the left side of the screen is hidden.

Click the *Full Screen* button in the toolbar to enter full-screen mode, and press the *Esc* key on your keyboard to exit full-screen mode.

## Switching between ADOMs

When ADOMs are enabled, you can move between ADOMs by selecting an ADOM from the *ADOM* menu in the banner.

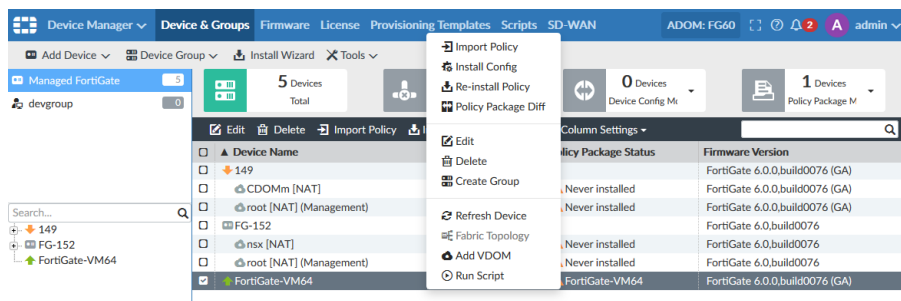


ADOM access is controlled by administrator accounts and the profile assigned to the administrator account. Depending on your account privileges, you might not have access to all ADOMs. See [Managing administrator accounts on page 498](#) for more information.

## 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 *Install Config*, *Import Policy*, *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 *SOC > FortiView* and *Log View* panes. FortiManager can display an avatar when

the following requirements are met:

- FortiClient is managed by FortiGate or FortiClient EMS with logging to FortiManager enabled.
- FortiClient sends logs and a picture of each user to FortiManager.

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 500](#).

## 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 enabled either for a FortiManager unit or for managed FortiAnalyzer units, but not for both at the same time. The 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, 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 [Adding FortiAnalyzer devices on page 49](#).

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

<b>SOC</b>	Enables <i>FortiView</i> and additional SOC <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 429</a> .
<b>Logging Topology</b>	View the logging topology. See <a href="#">Logging Topology on page 440</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>Fetcher Management</b>	Configure log fetching. See <a href="#">Fetcher Management on page 469</a> .
<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 491</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 495</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 a FortiAnalyzer units to the FortiManager. If a FortiAnalyzer is added to the FortiManager, FortiAnalyzer features are automatically enabled to support the managed FortiAnalyzer unit, and cannot be disabled.

See [Adding FortiAnalyzer devices on page 49](#) 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
```



The FortiAnalyzer feature set is not available on the FortiManager 100C.

## Configuring FortiManager appliances

Following is an overview of how to configure a FortiManager appliance.

### To configure FortiManager appliances:

1. Connect to the GUI. See [Connecting to the GUI on page 12](#).
2. Configure IP addresses. See [Configuring network interfaces on page 441](#).
3. Configure the RAID level, if the FortiManager unit supports RAID. See [RAID Management on page 444](#).

## Adding devices

After you configure the FortiManager device, you should plan the network topology, configure ADOMs, configure administrative accounts, and then add the devices that you want to manage.

The number of devices that can be managed depends on the device model and license. An add-on license can be purchased for some high end devices to increase that number of device that can be managed. See [Add-on license on page 91](#) for more information.

It is recommended that you import the policy from the device when you add the device to FortiManager. FortiManager uses the imported policy to automatically create a policy package for that device.

### To add devices:

1. Plan your network topology.
2. Configure administrative domains. See [Administrative Domains on page 450](#).
3. Configure administrator accounts. See [Managing administrator accounts on page 498](#).
4. Add devices to FortiManager. See [Adding devices on page 35](#).
5. If not done when you added the device, import the policy from each online device to FortiManager. See [Import policy wizard on page 47](#).  
A policy package is automatically created for the device based on the policy. You can view the policy package on the *Policy & Objects* pane.



After initially importing policies from the device, all changes related to policies and objects should be made in *Policy & Objects* on the FortiManager.

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

---

When initially adding a device to a FortiManager, there are several steps that should be followed before the FortiGate is considered synchronized.

### To synchronize FortiGate with FortiManager:

1. Ensure a policy package is assigned to this device using *Import Policy*.
2. Perform an *Install Policy Package* to ensure that FortiGate and FortiManager are properly synchronized.



As a result, the Config Status and Policy Package Status will show as *Synchronized*.



The above procedure does not apply to the Backup Mode.

---

Ensuring that a FortiGate is synchronized sets a good foundation for future configuration changes to be pushed to the FortiGate.

## Installing to managed devices

After you add devices to FortiManager, you can configure objects and policies, and use policy packages to install the objects and policies to one or more devices.

If you imported a policy from a device, you can edit and create policies for the imported policy package, and then install the updated policy package back to the device. Alternately you can create and configure a new policy package. You can install a policy package to multiple devices.

If you want to install device-specific settings, you can configure the settings by using the device dashboard on the *Device Manager* pane. When you install to the device, the device-specific settings are pushed to the device.

### To install to devices:

1. Create or edit objects. See [Create a new object on page 216](#) or [Edit an object on page 224](#).
2. Create or edit policies in a policy package to select the objects. See [Creating policies on page 176](#) or [Editing policies on page 176](#).  
You can create or edit policies in the policy package that was automatically created for the device when you imported its policy. Alternately, you can create a new policy package in which to define policies. See [Create new policy packages on page 161](#).
3. Ensure that the installation targets for the policy package include the correct devices. See [Policy package installation targets on page 168](#).
4. Edit device-specific settings by using the device dashboard on the *Device Manager* pane. See [Using the device dashboard on page 60](#).
5. Install the policy package and device settings to devices by using the Installation Wizard. See [Installing to devices on page 66](#).

## Enabling central management

FortiManager includes the option to enable central management for each of the following elements:

- SD-WAN: see [SD-WAN on page 128](#)
- VPN: see [VPN on page 287](#)
- AP: see [Access Points on page 318](#)

When central management is enabled, you can configure settings once, and then install the settings to one or more devices.

When central management is disabled, you must configure the settings for each device, and then install the settings to each device.

**To use central management:**

1. Enable central management for SD-WAN, VPN, and/or AP.
2. Configure the settings.
3. Install the settings to one or more devices.

## Monitoring managed devices

FortiManager includes many options for monitoring managed devices. Following is a sample of panes that you can use to monitor managed devices:

- Quick status bar—see [Using the quick status bar on page 69](#)
- Device dashboard—see [Using the device dashboard on page 60](#)
- Device configurations—see [Managing device configurations on page 78](#)
- Policy packages—see [Managing policy packages on page 161](#)
- *AP Manager* pane—see [Monitor on page 329](#)
- *FortiClient Manager* pane—see [Monitoring FortiClient endpoints on page 385](#)
- *FortiSwitch Manager* pane—see [Monitor on page 367](#)

When optional centralized features are enabled, you can also use the following panes to monitor the centralized features for managed devices:

- *SD-WAN* pane—see [SD-WAN on page 128](#)
- *VPN Manager* pane—see [VPN on page 287](#)

When FortiAnalyzer features are enabled on the FortiManager device, you can also view and analyze log messages from managed devices by using the *SOC > FortiView*, *Log View*, *Event Management*, and *Reports* panes. See [FortiAnalyzer Features on page 18](#).

## 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.

**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.

**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.

**To reset the FortiManager unit:**

1. From the CLI, or in the *CLI Console* menu, enter the following command:  

```
execute reset all-settings
```

This operation will reset all settings to factory defaults  
Do you want to continue? (y/n)
2. Enter *y* to continue. The device will reset to factory default settings and restart.

**To reset logs and re-transfer all SQL logs to the database:**

1. From the CLI, or in the *CLI Console* menu, enter the following command:  

```
execute reset-sqllog-transfer
```

WARNING: This operation will re-transfer all logs into database.  
Do you want to continue? (y/n)
2. Enter *y* to continue. All SQL logs will be resent to the database.

# 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 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.

This section contains the following topics:

- [FortiManager modules on page 24](#)
- [Object database and FortiManager modules on page 25](#)
- [Inside the FortiManager system on page 26](#)
- [Key features of the FortiManager system on page 31](#)

## FortiManager modules

The FortiManager feature set includes the following modules:

- Device Manager
- Policy & Objects
- AP Manager
- FortiClient Manager
- VPN Manager
- Fabric View
- FortiGuard
- FortiSwitch Manager
- SOC
- System Settings

## Modules for FortiAnalyzer feature set

When the FortiAnalyzer feature set is enabled in FortiManager, additional modules are available. The FortiAnalyzer feature set includes the following modules:

- SOC (*FortiView* and additional SOC *Monitors* become available in this module)
- Log View
- Incidents & Events
- Reports



The FortiAnalyzer feature set is disabled by default. To enable the features, turn it on from the dashboard (see [System Information widget on page 431](#)), or use the following CLI commands:

```
config system global
    set faz-status enable
end
```

Changing faz status will affect FAZ feature in FMG. If you continue, system will reboot to add/remove FAZ feature.

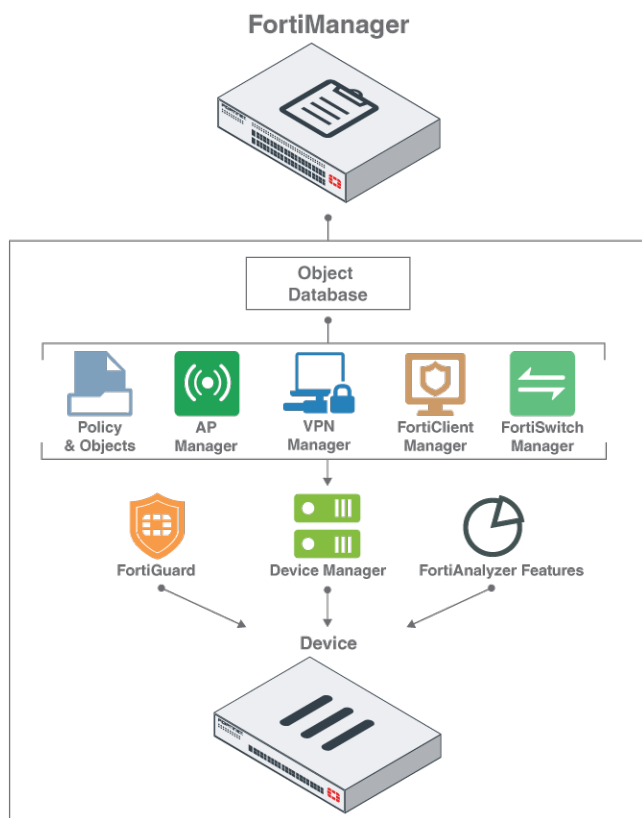
```
Do you want to continue? (y/n) y
```

The FortiAnalyzer feature set is also enabled when you use the Device Wizard to add a FortiAnalyzer device to FortiManager.

---

## Object database and FortiManager modules

Following is a diagram that shows an overview of the main FortiManager modules: Device Manager, FortiGuard, and FortiAnalyzer features. FortiManager includes a central database that stores elements for Policy & Objects, AP Manager, VPN Manager, FortiClient Manager, and FortiSwitch Manager, and you can install these elements to devices through Device Manager.

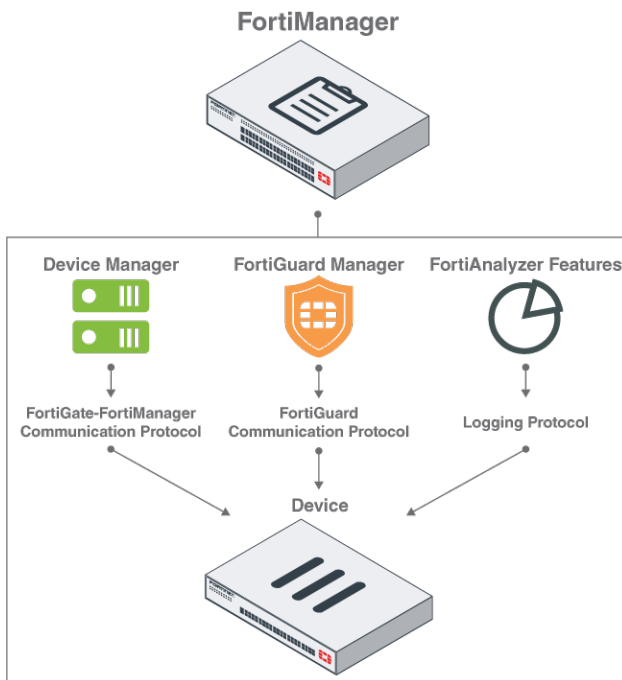


## Inside the FortiManager system

FortiManager is a robust system with multiple communication protocols and layers to help you effectively manage your Fortinet security infrastructure.

### Communication protocols and devices

FortiManager communicates with managed devices by using several protocols. *Device Manager*, *FortiGuard Manager*, and *FortiAnalyzer Features* each use a different protocol to communicate with managed devices.



## Device Manager

*Device Manager* contains all devices that are managed by the FortiManager unit. You can create new device groups, provision and add devices, and install policy packages and device settings. *Device Manager* communicates with devices by using the FortiGate-FortiManager (FGFM) protocol. See [Firewall Devices on page 34](#).

## FortiGuard Manager

*FortiGuard Manager* communicates with devices by using the FortiGuard protocol.

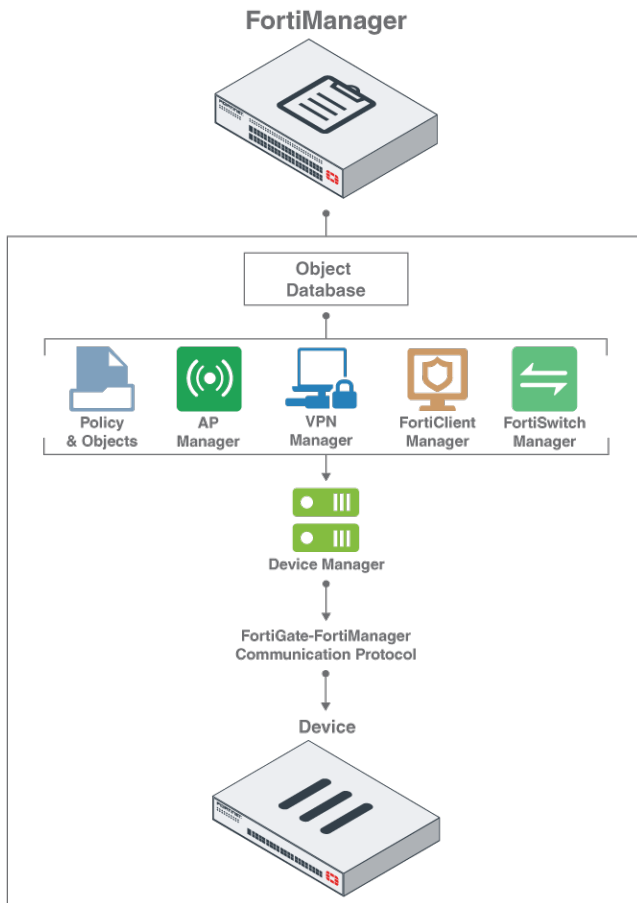
## FortiAnalyzer features

When FortiAnalyzer features are enabled for the FortiManager unit, the *SOC > FortiView*, *Log View*, *Incidents & Events*, and *Reports* panes are available. FortiAnalyzer features include tools for viewing and analyzing log messages, and the feature communicates with devices by using the logging protocol.

## Object database and devices

FortiManager includes an object database to store all of the objects that you create. You can use the objects in the following panes and apply the objects to devices:

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



## Policy & Objects

The *Policy & Objects* pane contains all of your global and local policy packages and objects as well as configuration revisions. Objects created for the *Policy & Objects* pane are stored in the objects database. See [Firewall Policy & Objects on page 156](#).

## AP Manager

The *AP Manager* pane lets you view and configure FortiAP access points as well as FortiExtender wireless WAN extenders. Objects created for the *AP Manager* pane are stored in the objects database. See [Access Points on page 318](#).

## VPN Manager

The *VPN Manager* pane lets you centrally manage IPsec VPN and SSL-VPN settings. Objects created for the *VPN Manager* pane are stored in the objects database. See [VPN on page 287](#).



## FortiClient Manager

The *FortiClient Manager* pane lets you manage FortiClient profiles and monitor FortiClient endpoints that are registered to FortiGate devices. Objects created for the *FortiClient Manager* pane are stored in the objects database. See [Endpoint Compliance on page 381](#).

## FortiSwitch Manager

The *FortiSwitch Manager* pane lets you manage and monitor FortiSwitch devices, and configure FortiSwitch templates and VLANs. Objects created for the *FortiSwitch Manager* pane are stored in the objects database. See [FortiSwitch Manager on page 359](#).

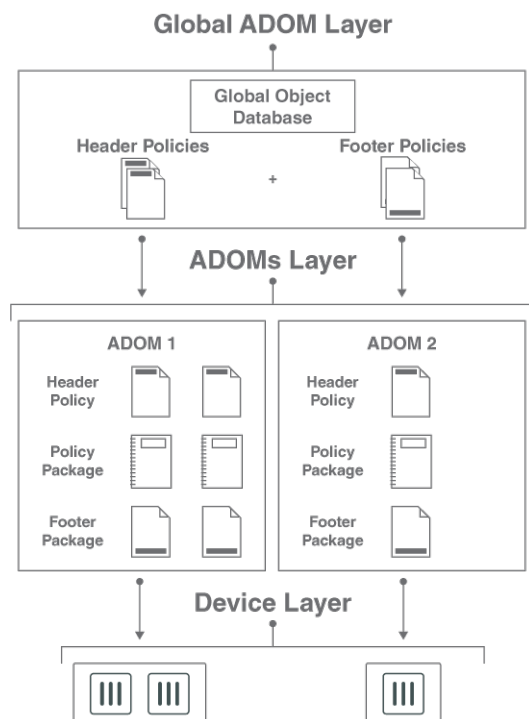
## ADOMs and devices

The *Device Manager* pane is used to install policy packages to devices. When ADOMs are enabled, the *Device Manager* pane is used to install policy packages to the devices in an ADOM.

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.



## Global ADOM layer

The global ADOM layer contains two key pieces: the global object database and 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 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 the FortiManager unit, 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

## Install

The install operation pushes device configuration from the FortiManager to a FortiGate device.

The 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 the FortiManager.

The install operation can include only device settings, or device settings and policy packages.

For more information, see [Installing to devices on page 66](#).

## Re-install

The re-install operation reinstalls a policy package on a FortiGate device. For more information, see [Reinstall a policy package on page 165](#).

## Import

The import operation copies policies and policy-related objects from the device database into the ADOM, creating a policy package that reflects the current configuration of the FortiGate device.

For more information, see [Import policy wizard on page 47](#).

## Retrieve

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

## Auto-Update

When there is a change on the FortiGate that is not initiated by an install operation, the FortiGate automatically sends the configuration changes to the FortiManager.

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 settings
    set auto-update disable
end
```

## 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 452](#).

## Auto-Retrieve

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

## Refresh

The FortiManager queries the FortiGate to update that FortiGate's current synchronization status. For more information, see [Refreshing a device on page 70](#).

## Revert

The revert operation loads a saved configuration revision into the device database. For more information, see [Managing configuration revision history on page 82](#).

# 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 46](#). You can also display the security fabric topology (see [Displaying Security Fabric topology on page 74](#)) and view Security Fabric Ratings (see [Fabric View on page 237](#)).

## 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 on page 450](#).

## 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 [Device Firmware and Security Updates on page 394](#).

## Firmware management

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

## Scripting

FortiManager supports CLI or Tcl based scripts to simplify configuration deployments. See [Scripts on page 96](#).

## 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.

# Firewall Devices

Use the *Device Manager* pane to add, configure, and manage devices.

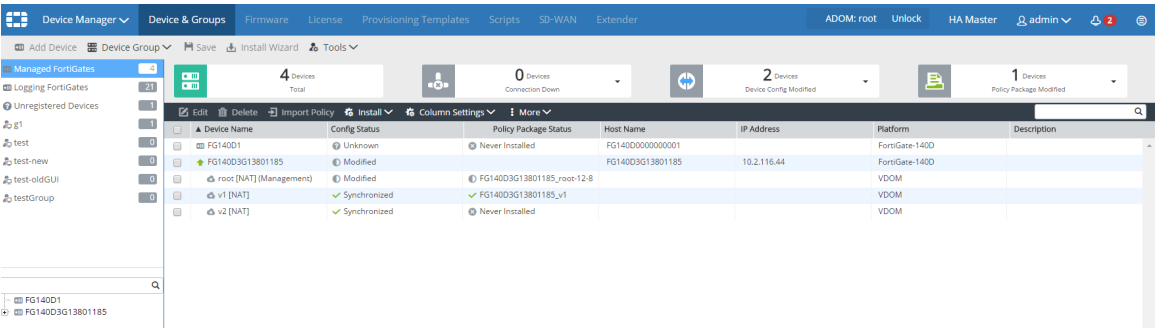
This topic covers navigating the *Device Manager* pane, adding devices, and managing devices. It also covers managing FortiExtender wireless WAN extenders.



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.



If workspace or workflow is enabled, the ADOM must be locked before changes can be made. See [Locking an ADOM on page 463](#).



The *Device Manager* pane includes the following tabs in the blue banner:

<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="#">Adding devices on page 35</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 69</a> .
<b>Firmware</b>	View information about firmware for devices as well as upgrade firmware. See <a href="#">Firmware on page 87</a> .
<b>License</b>	View license information for devices as well as push license updates to devices. See <a href="#">License on page 89</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 91</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 96</a> .

**SD-WAN**

Configure profiles for load balancing SD-WAN links and monitor load-balancing profiles. The *SD-WAN* tab is displayed only when central SD-WAN Link load balancing is enabled. See [SD-WAN on page 128](#).

**Extender**

View and configure FortiExtender. See [FortiExtender on page 145](#).

## ADOMs

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

- Firmware version: group all 6.0 devices into one ADOM, and all 6.2 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 on page 450](#).



For information on adding devices to an ADOM by using the *Add Device* wizard, see [Adding devices using the wizard on page 36](#).

## Adding devices

You must add devices to the FortiManager system to use FortiManager to manage the devices. You must also enable *Central Management* on the managed device by using FortiOS. You can add an existing, operational device or an unregistered device. You can also provision a new device.

You can add individual devices or multiple devices. Adding devices using the *Add Device* wizard gives you more configuration options than using *Add Multiple* devices.

For a device that is currently online, use the *Add Device* wizard, select *Discover*, and follow the steps in the wizard. Adding an existing device does not result in an immediate connection to the device. Device connection happens only when you successfully synchronize the device. To provision a new device which is not yet online, use the *Add Device* wizard and select *Add Model Device*.

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 a 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.

---

## Adding devices using the wizard

You can add devices to the FortiManager unit by using the *Add Device* wizard. You can use the wizard to discover devices or add model devices to your FortiManager unit.

---



You cannot use the *Add Device* wizard to add FortiAnalyzer to FortiManager. You must use the *Add FortiAnalyzer* wizard instead. See [Adding FortiAnalyzer devices on page 49](#).

---

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

Use the *Add Model Device* option to add a device that is not yet online. You can configure a model device to automatically complete authorization with FortiManager when the device is online.

---



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.

---



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

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

---

## Adding a device using Discover mode

The following steps will guide you through the *Add Device* wizard phases to add a device using *Discover* mode.

---



FortiManager will not be able to communicate with the FortiGate if offline mode is enabled. Enabling offline mode will prevent FortiManager from discovering devices.

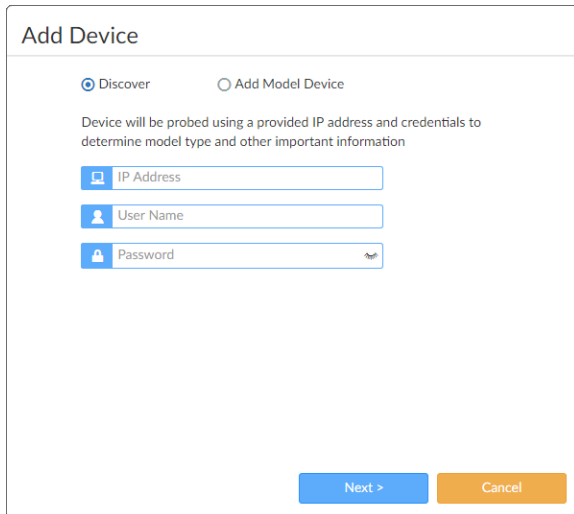
---

### 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.



The 'Add Device' wizard is shown with the 'Discover' option selected. It includes a text box for the IP address, a text box for the user name, and a password field with a toggle for visibility. A 'Next >' button is at the bottom right.

**Add Device**

☒ Discover ☐ Add Model Device

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

IP Address

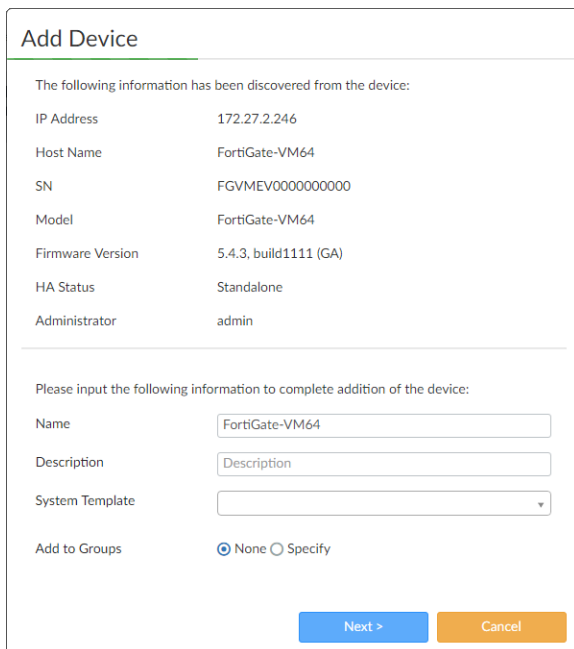
User Name

Password

Next > Cancel

4. Select **Discover**. Type the IP address, user name, and password for the device, then click **Next**. FortiManager probes the IP address on your network to discover device details, including:

- IP address
- Host name
- Serial number
- Device model
- Firmware version and build
- High Availability status
- Administrator user name



The 'Add Device' wizard shows the discovered information from the device. It includes a table with fields like IP Address, Host Name, SN, Model, Firmware Version, HA Status, and Administrator. Below the table, there are input fields for Name, Description, System Template, and Add to Groups. A 'Next >' button is at the bottom right.

**Add Device**

The following information has been discovered from the device:

IP Address	172.27.2.246
Host Name	FortiGate-VM64
SN	FGVMEV0000000000
Model	FortiGate-VM64
Firmware Version	5.4.3, build1111 (GA)
HA Status	Standalone
Administrator	admin

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

Name FortiGate-VM64

Description Description

System Template

Add to Groups ☒ None ☐ Specify

Next > Cancel

5. Configure the following settings:

<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 select to configure all settings per-device inside <i>Device Manager</i> . For more information, see <a href="#">Provisioning Templates on page 91</a> .
<b>Add to Groups</b>	Select to add the device to any predefined groups.

6. Click *Next*.

The wizard discovers the device, and performs some or all of the following checks:

- Discovering device
- Creating device database
- Initializing configuration database
- Retrieving configuration
- Retrieving support data
- Updating group membership
- Successfully add device
- Check device status

**Add Device**

Name: FortiGate-VM64

IP Address: 172.27.2.246

Status: 50%

- ✓ Discovering device
- ✓ Creating device database
- ✓ Initializing configuration database
- Retrieving configuration
- Retrieving support data
- Updating group membership
- Successfully add device
- Check Device Status

Cancel

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

7. 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 - FortiGate-VM64 [root]

Create a new policy package for import.

Policy Package Name: FortiGate-VM64\_root

Folder: root

Policy Selection: ☒ Import All (1)

☐ Select Policies and Profile Groups 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.

Searching for interface mappings on device ...

Next > Cancel

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

The list of objects that will be updated is displayed.

Import Device - FortiGate-VM64 [root]

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

Duplicates (4) ▼

Address (1)	all	
Recurring Schedule (1)	always	
Service (1)	ALL	
Service Category (1)	General	

Next >
Cancel

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.

Import Device - FortiGate-VM64 [root]

✓ 1 policies and objects are imported. [\[Download Import Report\]](#)

Import Summary

Firewall Policy	1 of 1
-----------------	--------

Finish

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

## Adding a model device

The following instructions will guide you through the *Add Device* wizard phases to add a device using *Add Model Device* mode.



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
```



When adding devices to product-specific ADOMs, you can only add that product type to the ADOM. When selecting to add 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 ☒ Add Model Device

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

Name	<input type="text" value="Name"/>
Link Device By	<input type="text" value="Serial Number"/>
Serial Number	<input type="text" value="Serial Number"/>
Device Model	<input type="text"/>
Enforce Firmware Version	<input type="checkbox"/>
Firmware Version	6.2
Assign Policy Package	<input type="checkbox"/>
Assign Device Provision Profile	<input type="checkbox"/>
Device Group	<input type="text" value="Click here to select"/>

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 device will be added, either <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 the model device is added.</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>	Type the device serial number or pre-shared key. This field is mandatory. If using a pre-shared key, each device must have a unique pre-shared key. You can change the pre-shared key after adding the model device. See <a href="#">Editing device information on page 70</a> .
<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>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>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>Assign Device Provisioning Profile</b>	Select the check box and select a device provisioning profile from the drop-down to assign a particular provisioning profile to the device.
<b>Device Group</b>	Click <i>Device Group</i> and select a group to assign the device to the group.

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.



A configuration file needs to be associated with the model device so that FortiManager will automatically install the configuration to the matching device when it connects to the FortiManager. FortiManager will 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 [Managing configuration revision history on page 82](#).

## 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.

### To authorize devices:

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

Device Name	Assign New Device Name
FGVM010000102012	FGVM010000102012

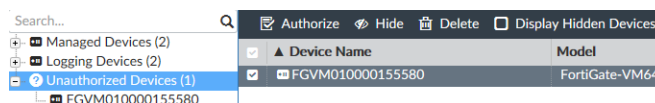
4. If ADOMs are enabled, select the ADOM in the *Add the following device(s) to ADOM* list. If ADOMs are disabled, select *root*.
5. Click *OK* to authorize the device or devices.  
The device or devices are authorized and FortiManager can start managing the device or devices.

## 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* and click the *Unauthorized Devices* tree menu. The content pane displays the unauthorized devices.



2. 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.

## Example of adding a model device by pre-shared key

This section describes how to add a FortiGate model by using the pre-shared key for FortiGate. 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. In the *Link Device By* list, 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 a model device by serial number

This section describes how to add a FortiGate model device to FortiManager by using the serial number for the FortiGate. 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. In the *Link Device By* list, 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 in device central management.

- a. Go to *System > Settings*.
- b. In the *Central Management* area, type the FortiManager IP address in the *IP/Domain Name* box, and click *Apply*.

FortiManager automatically links the model device to the real device, and installs configurations to the device.



## Add a VDOM to a device

To add a VDOM to a managed FortiGate device, right-click on the content pane for a particular device and select *Add VDOM* from the pop-up menu. There are 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](#).

---

### Split-Task VDOM Mode

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 tree menu, click the group. The devices in the group are displayed in the content pane.
3. In the content pane, right-click a device and select *Add VDOM*.
4. Click *Split-Task VDOM*.

### Multi VDOM Mode

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 tree menu, click the group. The devices in the group are displayed in the content pane.
3. In the content pane, right-click a device and select *Add VDOM*.
4. Click *Multi VDOM*.

5. The *Create New Virtual Domain* window opens.

Create New Virtual Domain

Enable VDOM

VDOM Name

Description

Enable

Operation Mode

Interface Members

Split-Task VDOM Multi VDOM

☒

NAT

Click here to select

OK

Cancel

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

<b>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>Operation Mode</b>	Select either <i>NAT</i> or <i>Transparent</i> .
<b>Interface Members</b>	Click to select each port one by one.



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 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 74](#).

### 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 a device using Discover mode on page 36](#). Alternatively, you can enable Central Management in the root FortiGate unit and specify the IP address of the FortiManager. See [Authorizing devices on page 43](#).  
All devices part of the Security Fabric group are automatically added in *Unauthorized Devices*.
4. Select all devices in *Unauthorized Devices* and click *Add*.
5. Specify the credentials for each device in the *Add Device* dialog and click *OK*.

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



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

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

Device Name	Config Status	Policy Package Status	Host Name	IP Address	Platform	Description
FG100D3G14811667	✓ Synchronized	✓ Never Installed	FG101E-L2	10.3.121.191	FortGate-101E	
FG101E-L2	✓ Synchronized	✓ Never Installed	FG101E-L3	10.3.121.192	FortGate-101E	
FGT100D-HA-root*	✓ Synchronized	✓ Never Installed	FGT100D-HA-root	10.3.121.100	FortGate-100D	
FGP200A414800316	✓ Auto-update	✓	FG280DPOE-L3	10.3.121.111	FortGate-280D-POE	
FG280DPOE-L3	✓ Auto-update	✓	FG81E-HA-L2	10.3.121.181	FortGate-81E-POE	
FG81E-HA-L2	✓ Auto-update	✓	FGT200DPOE-L1-root*	10.3.121.112	FortGate-200D-POE	
FGT200DPOE-L1-root*	✓ Auto-update	✓	FGVM-076-L2	10.3.121.76	FortGate-VM64	
FGVM-076-L2	✓ Auto-update	✓				

## Import policy wizard

On the *Device Manager > Device & Groups* pane, right-click a device, and select *Import Policy* to launch the *Import Device* wizard. This wizard allows you to import interface maps, policy databases, and objects. Default or per-device mapping must exist or the installation will fail.



After initially importing policies from the device, make all 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.

## Device Interface

The Device Interface page allows you to choose an ADOM interface for each device interface. When importing configuration from a device, all enabled interfaces require a mapping.

Interface maps will be created automatically for unmapped interfaces.

Import Device - FortiGate

[root]

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	ADOM Interface
port1	port1
port2	port2
port3	port3
port4	port4
port5	port5
port6	port6
port7	port7
port8	port8
port9	port9

☒ Add mappings for all unused device interfaces

Next >

Cancel

Select *Add mapping for all unused device interfaces* to automatically create interface maps for unused interfaces.

Policy

The policy page allows you to create a new policy package for import.

Select a folder from the dropdown menu, specify a policy package name, then configure the following options:

Policy Package Name	Type a name for the policy package.
Folder	Select a folder on the dropdown menu.
Policy Selection	Select to import all, or select specific policies and policies groups to import.
Object Selection	Select <i>Import only policy dependent objects</i> to import policy dependent objects only for the device. Select <i>Import all objects</i> to import all objects for the selected device.

Object

The object page will search 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 Details* to view details of each individual conflict, or you can download an HTML conflict file to view all the details about the conflicts. Duplicates will not be imported.

Click *Next* to view the objects that are ready to be imported, and then click *Next* again to proceed with importing.

Import

Objects are imported into the common database, and the policies are imported into the selected package. Click *Next* to continue to the summary.



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, or VPN console.

## Summary

The summary page allows you to download the import device summary results. It cannot be downloaded from anywhere else.

## Adding FortiAnalyzer devices

Adding a FortiAnalyzer device to FortiManager gives FortiManager visibility into the logs on the FortiAnalyzer, providing a Single Pane of Glass on the FortiManager. It also enables FortiAnalyzer features, such as *SOC > FortiView*, and *Log View*.

For information about FortiAnalyzer features, see [FortiAnalyzer Features on page 18](#). See also [Viewing policy rules on page 53](#) and [View logs related to a policy rule on page 172](#).



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



If FortiAnalyzer features are enabled, you cannot add a FortiAnalyzer unit to the FortiManager. See [FortiAnalyzer Features on page 18](#).

In addition, you cannot add a FortiAnalyzer unit to the FortiManager when ADOMs are enabled and ADOM mode is 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:

- You can add one FortiAnalyzer device to each ADOM, and the FortiAnalyzer device limit must be equal to or greater than the number of devices in the 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.
- You cannot add the same FortiAnalyzer device to multiple ADOMs.

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 92](#).

### Legacy FortiAnalyzer ADOM

The FortiAnalyzer ADOM supports FortiAnalyzer units added to FortiManager before upgrading to FortiManager 5.6 and later. If you want to use the new functionality, you must delete the FortiAnalyzer unit from FortiManager and add it by using the Add FortiAnalyzer wizard.

### 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: *SOC > 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 with the wizard

If the FortiAnalyzer unit 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.



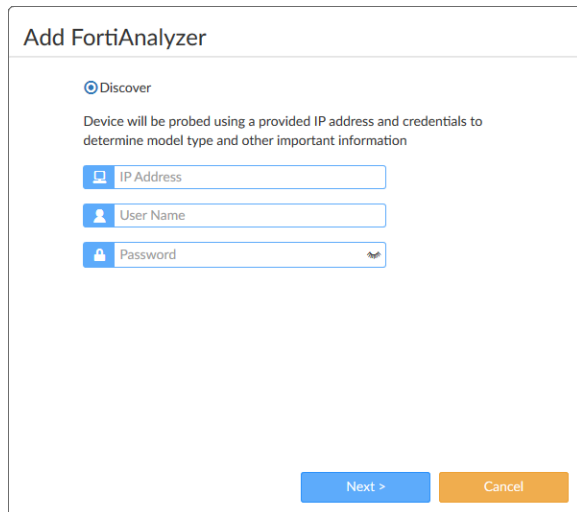
FortiManager and FortiAnalyzer must be running 5.6 or later, and the versions must be the same on both devices.

---

**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 *Add Device > Add FortiAnalyzer*. The wizard opens.

The *Add FortiAnalyzer* option is hidden if you've already added a FortiAnalyzer device.



5. 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

The following information has been discovered from the device:

IP Address	172.27.2.223
Host Name	FAZVM64
SN	FAZ-VM0000000001
Model	FortiAnalyzer-VM64
Firmware Version	5.6.0, build1530 (GA)
HA Status	Standalone
Administrator	admin

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

Name	<input type="text" value="FAZVM64"/>
Description	<input type="text" value="Description"/>

Next >
Cancel

6. 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

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

50%

Status	Device Name	Platform
Sync	FGVM01000092070	FortiGate-VM64

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.



Status	Description
<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.

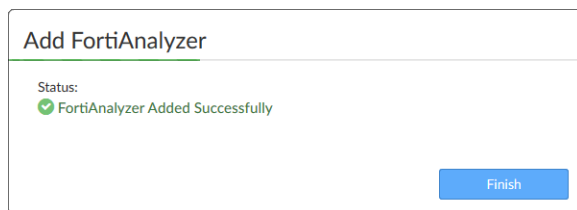
If the FortiManager ADOM does not exist on the FortiAnalyzer device, a warning is displayed. You can add the ADOM and devices to FortiAnalyzer by clicking the *Synchronize ADOM and Devices* button.

7. 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.

8. Click *Finish* to close the wizard.



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

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 92](#).

## 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 [Adding FortiAnalyzer devices on page 49](#).

**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.

## Importing devices

You can import devices using the following methods:

- [Importing detected devices](#)
- [Importing and exporting device lists](#)

## Importing detected devices

You can import detected devices for each device.

### To import detected devices:

1. Ensure that you are in the correct ADOM.
2. Go to the *Device Manager* tab, and from the *Tools* menu, click *Global Display Options*.
3. In the *Detected Devices* area, select *Detected Devices*, and click *OK*.
4. In the tree menu, select a device. The device dashboard is displayed.
5. Click *Detected Devices*. The *Detected Devices* pane is displayed.
6. 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.



The *Import and Export Device List* features are disabled by default. To enable, go to *System Settings > Admin > Admin Settings*, and select the *Show Device List Import/Export* checkbox under *Display Options on GUI*.



Proper logging must be implemented when importing a list. If any add or discovery operation fails, there must be appropriate event logs generated so you can trace what occurred.

### To export a device list to compressed JSON format:

1. Go to *Device Manager > Device & Groups*.
2. Select a device group, such as *Managed Devices*.
3. From the *More* menu, select *Export Device List*.  
The *Choose ADOM* dialog box is displayed.

Choose ADOM

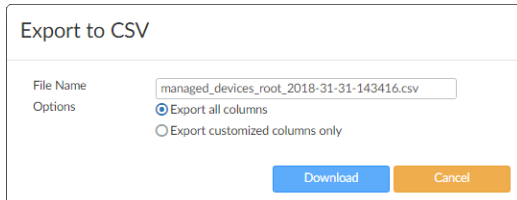
Please choose where to export device list from.

Current ADOM
All ADOM
Cancel

4. 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. Select a device group, such as *Managed Devices*.
3. From the *More* menu, select *Export to CSV*.  
The *Export to CSV* dialog box is displayed.

The image shows a dialog box titled "Export to CSV". It has two sections: "File Name" and "Options". In the "File Name" section, there is a text input field containing the value "managed\_devices\_root\_2018-31-31-143416.csv". In the "Options" section, there are two radio buttons. The first radio button is selected and is labeled "Export all columns". The second radio button is labeled "Export customized columns only". At the bottom of the dialog box, there are two buttons: "Download" (in blue) and "Cancel" (in orange).

4. (Optional) Change the file name.
5. Select whether to export all columns or only customized columns.
6. Click *Download*.

**To import a device list:**

1. Go to *Device Manager > Device & Groups*.
2. Select a device group, such as *Managed Devices*.
3. From the *More* menu, select *Import Device List*.
4. 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.
5. Click *OK*.

## Configuring devices

You can configure the FortiGate units in three ways:

- Per device, from the Device Manager dashboard toolbar.
- Per VDOM, from the Device Manager dashboard toolbar.
- Per provisioning template.

This section contains the following topics:

- [Configuring a device](#)
- [Out-of-Sync device](#)
- [Configuring VDOMs](#)

## Configuring a device

Configuring a FortiGate unit using the *Device Manager* dashboard toolbar is very similar to configuring FortiGate units using the FortiGate 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 configure a FortiGate unit:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, select a device group.
3. In the content pane, select a device.
4. From the *Install* menu, select *Install Config*.
5. When the installation configuration is complete, click *Finish*.

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.

---

## 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.

## 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 476](#).

## Configuring VDOMs

Virtual domains (VDOMs) enable you to partition and use your FortiGate unit as if it were multiple units.



VDOMs have their own dashboard and toolbar. You can configure the VDOM in the same way that you can configure a device.

<b>Delete</b>	Select to remove this virtual domain. This function applies to all virtual domains except the root.
<b>Create New</b>	Select to create a new virtual domain.
<b>Management Virtual Domain</b>	Select the management VDOM and select <i>Apply</i> .
<b>Name</b>	The name of the virtual domain and if it is the management VDOM.
<b>Virtual Domain</b>	Virtual domain type.
<b>IP/Netmask</b>	The IP address and mask. Normally used only for Transparent mode.
<b>Type</b>	Either VDOM Link or Physical.
<b>Access</b>	HTTP, HTTPS, SSH, PING, and/or SNMP.
<b>Resource Limit</b>	Select to configure the resource limit profile for this VDOM.

## Creating and editing virtual domains

Creating and editing virtual domains in the FortiManagersystem is very similar to creating and editing VDOMs using the FortiGate GUI.

You need to enable virtual domains before you can create one.

**To enable virtual domains:**

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, select a device group.
3. In the lower tree menu, select a device. The device dashboard displays.
4. In the *System Information* widget, select the *Enable* link in the *VDOM* field.

**To create a virtual domain:**

1. In the *Device Manager* tab, display the device dashboard for the unit you want to configure.
2. From the *System* menu, select *Virtual Domain*.
3. Click *Create New* to create a new VDOM.



The Virtual Domain tab may not be visible in the content pane tab bar. See [View system dashboard for managed/logging devices on page 60](#) for more information.

---

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. In the *Device Manager* pane, display the device dashboard for the device.
2. From the *System* menu, select *Interface*.

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

4. Enter the following information:

<b>Name</b>	Name of the VDOM link.
<b>Interface #x</b>	The interface number, either <i>1</i> or <i>0</i> .
<b>VDOM</b>	Select the VDOM
<b>IP/Netmask</b>	Type the IP address and netmask for the VDOM.
<b>Administrative Access</b>	Select the allowed administrative service protocols: <i>HTTPS</i> , <i>PING</i> , <i>FMG-Access</i> , <i>CAPWAP</i> , <i>SSH</i> , and <i>SNMP</i> . <b>Note:</b> HTTP traffic will be automatically redirected to HTTPS.
<b>Description</b>	Optionally, type a description for the link.

5. 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 161](#)). All objects related to the VDOM must also be removed, such as routes, VPNs, and admin accounts.

### To delete a VDOM:

1. In the *Device Manager* tab, display the device dashboard for the unit you want to configure.
2. From the *System* menu, select *Virtual Domain*.
3. Right-click on the VDOM and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the VDOM.

## Using the device dashboard

You can view the dashboard and related information of all managed/logging and provisioned devices.

This section contains the following topics:

- [View system dashboard for managed/logging devices](#)
- [View system interfaces on page 62](#)
- [CLI-Only Objects menu](#)
- [System dashboard widgets](#)

## View system dashboard for managed/logging devices

You can view information about individual devices in the *Device Manager* pane on the dashboard for each device. This section describes the dashboard for a FortiGate unit.

**To view the dashboard for managed/logging devices:**

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.



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.

3. In the bottom tree menu, select a device. The *System: Dashboard* for the device displays in the content pane.

**System Information**

Host Name	FortiGate-VM66
Serial Number	FGVM010000000000
System Time	Tue May 29 13:04:37 PDT 2018
Firmware Version	FortiGate 6.0.0.build0076 (GA)
Hardware Status	1 CPU/995 MB RAM
Operation Mode	NAT
HA Mode	Standalone
Session Information	<a href="#">View Session List</a>
Description	
Operation	<a href="#">Reboot</a> <a href="#">Shutdown</a>

**License Information**

**VM License**

License Status	Pending
VM Resources	1 CPU/1 allowed, 995 MB RAM/995 MB allowed

**Support Contract**

Registration	vancouver_support@fortinet.com
Hardware Version	
Firmware	✓ Web/Online Support (Expires 2018-07-02)
Enhanced Support	✓ 8x5 Support (Expires 2018-07-02)

**Connection Summary**

IP	172.88.26.852
Interface	port1
Connecting User	admin
Connectivity	✓
Connect to CLI via	<a href="#">Telnet</a> <a href="#">SSH</a>

**Configuration and Installation Status**

System Template	None
Database Configuration	<a href="#">View</a>
Total Revisions	2
Sync Status	Synchronized
Warning	None
Installation Tracking	
Device Settings Status	Unmodified
Installation Preview	<a href="#">Preview</a>
Last Installation	None
Scheduled Installation	None
Script Status	
Last Script Run	None <a href="#">View History</a>
Scheduled Script	None

4. In the dashboard toolbar, click the tabs to display different options that you can configure for the device. See [Dashboard toolbar on page 61](#).
5. You can control what tabs are displayed by clicking *Display Options*. See [Display Options on page 61](#).



## Dashboard toolbar

The dashboard toolbar displays tabs that you can use to configure the device. The available tabs depends on the device. You can choose what tabs to display by clicking display options.



The options available on the dashboard toolbar varies depending on what feature set the device supports. If a feature is not enabled on the device the corresponding tab is not available on the toolbar.

## Display Options

You can customize panels at both the ADOM and device levels. Select *Tools > Display Options* to open the *Display Options* dialog box to customize the available content at the ADOM level. Alternatively, you can select a device, and then select *Display Options* to customize device tabs. You can select to inherit from ADOM or customize.

Display Options

<input checked="" type="checkbox"/> Policy	<input checked="" type="checkbox"/> Firewall Policy <input checked="" type="checkbox"/> IPv4 Policy <input checked="" type="checkbox"/> IPv6 Policy <input checked="" type="checkbox"/> Security Policy <input checked="" type="checkbox"/> NAT64 Policy <input checked="" type="checkbox"/> IPv4 DoS Policy <input checked="" type="checkbox"/> IPv4 Interface Policy <input checked="" type="checkbox"/> Multicast Policy <input checked="" type="checkbox"/> IPv6 Local In Policy <input checked="" type="checkbox"/> Authentication Rules	<input checked="" type="checkbox"/> Virtual Wire Pair Policy <input checked="" type="checkbox"/> IPv4 Virtual Wire Pair Policy <input checked="" type="checkbox"/> IPv6 Virtual Wire Pair Policy <input checked="" type="checkbox"/> NAT46 Policy <input checked="" type="checkbox"/> Proxy Policy <input checked="" type="checkbox"/> IPv6 DoS Policy <input checked="" type="checkbox"/> IPv6 Interface Policy <input checked="" type="checkbox"/> IPv4 Local In Policy <input checked="" type="checkbox"/> Traffic Shaping Policy <input checked="" type="checkbox"/> Installation Targets
<input checked="" type="checkbox"/> Policy Block	<input checked="" type="checkbox"/> Policy Block	
<input checked="" type="checkbox"/> Zone/Interface	<input checked="" type="checkbox"/> Interface	
<input checked="" type="checkbox"/> Firewall Objects	<input checked="" type="checkbox"/> Addresses <input checked="" type="checkbox"/> Multicast Addresses <input checked="" type="checkbox"/> Services <input checked="" type="checkbox"/> Virtual IPs <input checked="" type="checkbox"/> Traffic Shapers <input checked="" type="checkbox"/> Virtual Servers <input checked="" type="checkbox"/> Web Proxy Forwarding Server	<input checked="" type="checkbox"/> Internet Service <input checked="" type="checkbox"/> Wildcard FQDN Addresses <input checked="" type="checkbox"/> Schedules <input checked="" type="checkbox"/> IP Pools <input checked="" type="checkbox"/> Shaping Profile <input checked="" type="checkbox"/> Health Check <input checked="" type="checkbox"/> Authentication Scheme
<input checked="" type="checkbox"/> Security Profiles	<input checked="" type="checkbox"/> AntiVirus <input checked="" type="checkbox"/> Web Application Firewall <input checked="" type="checkbox"/> Application Control <input checked="" type="checkbox"/> Email Filter <input checked="" type="checkbox"/> VoIP <input checked="" type="checkbox"/> Protocol Options <input checked="" type="checkbox"/> Profile Group <input checked="" type="checkbox"/> Web URL Filter <input checked="" type="checkbox"/> Web Filter Local Category <input checked="" type="checkbox"/> ICAP Servers <input checked="" type="checkbox"/> Application Group <input checked="" type="checkbox"/> Email List	<input checked="" type="checkbox"/> DNS Filter <input checked="" type="checkbox"/> Web Filter <input checked="" type="checkbox"/> Intrusion Prevention <input checked="" type="checkbox"/> Data Leak Prevention <input checked="" type="checkbox"/> ICAP <input checked="" type="checkbox"/> SSL/SSH Inspection <input checked="" type="checkbox"/> Web Rating Overrides <input checked="" type="checkbox"/> Web Content Filter <input checked="" type="checkbox"/> File Filter <input checked="" type="checkbox"/> Application Signatures <input checked="" type="checkbox"/> IPS Custom Signature
<input checked="" type="checkbox"/> Fabric Connectors	<input checked="" type="checkbox"/> SDN <input checked="" type="checkbox"/> SSO/Identity	<input checked="" type="checkbox"/> Threat Feeds
<input checked="" type="checkbox"/> User & Device	<input checked="" type="checkbox"/> User Definition <input checked="" type="checkbox"/> Custom Devices & Groups <input checked="" type="checkbox"/> RADIUS Servers <input checked="" type="checkbox"/> POP3 Users <input checked="" type="checkbox"/> SMS Services	<input checked="" type="checkbox"/> User Groups <input checked="" type="checkbox"/> LDAP Servers <input checked="" type="checkbox"/> TACACS+ Servers <input checked="" type="checkbox"/> PKI <input checked="" type="checkbox"/> FortTokens
<input checked="" type="checkbox"/> WAN Optimize	<input checked="" type="checkbox"/> Profile <input checked="" type="checkbox"/> Authentication Group	<input checked="" type="checkbox"/> Peer
<input checked="" type="checkbox"/> Dynamic Object	<input checked="" type="checkbox"/> Local Certificate	<input checked="" type="checkbox"/> VPN Tunnel
<input checked="" type="checkbox"/> Advanced	<input checked="" type="checkbox"/> Replacement Message Group	<input checked="" type="checkbox"/> CA Certificates
<input checked="" type="checkbox"/> CLI Only Objects	<input checked="" type="checkbox"/> CLI Only Objects	



The options available when customizing device tabs at the ADOM level will vary based on the ADOM version.

To select all of the content panels in a particular category, select the checkbox beside the category name. To reset a category selection, clear the checkbox.

To select all of the content panels, select *Check All* at the bottom of the window. To reset all of the selected panels, select *Reset to Default* at the bottom of the window.



The available device tabs are dependent on the device model and settings configured for that model. The following tables provide an overview and descriptions of common dashboard toolbar panels, and content options.

---

## View system interfaces

You can view interface information about individual devices in the *Device Manager* tab.

### To view interfaces for a device:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, select the device group, for example, *Managed Devices*. The list of devices is displayed in the content pane and in the bottom tree menu.
3. In the bottom tree menu, select a device. The dashboard for the device displays in the content pane.
4. From the *System* menu, select *Interface*. The *System: Interface* dashboard is displayed.

## CLI-Only Objects menu

FortiManager includes a *CLI-Only Objects* menu in the *Device Manager* pane that allows you to configure device settings that are normally configured via the CLI on the device, as well as settings that are not available in the FortiManager GUI.

### To access the CLI-only objects menu:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, select a device group.
3. In the lower tree menu, select a device. The device dashboard is displayed in the content pane.
4. Click *Display Options*. The *Display Options* dialog box is displayed.
5. Select the *CLI-Only Objects* checkbox, and click *OK*. The *CLI-Only Objects* menu is displayed in the toolbar.
6. Click *CLI-Only Objects*.



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.

---

## System dashboard widgets

The system dashboard widgets provide quick access to device information, and device connectivity with the FortiManager system. The following widgets are available in FortiManager:

- [Configuration Revision History](#) (available when the ADOM is in backup mode)
- [System Information](#)
- [License Information](#)
- [Connection Summary](#)
- [Configuration and Installation Status](#)

The following table provide a description of these dashboard widgets. Note that not all of the listed options will be available on every 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.
System Information	
<b>Host Name</b>	The host name of the device.
<b>Serial Number</b>	The device serial number.
<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>Firmware Version</b>	The device firmware version and build number.
<b>System Configuration</b>	Displays the Last Backup. You can backup or restore.

System Information	
<b>Current Administrators</b>	Displays the number of administrators configured on this device.
<b>Hardware Status</b>	The number of CPUs and the amount of RAM for the device.
<b>Up Time</b>	Displays the duration the device has been up.
<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>Support Contract</b>	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.
<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.
Connection Summary	
<b>IP</b>	The IP address of the device.
<b>Interface</b>	The port used to connect to the FortiManager system.
<b>Connecting User</b>	The user name for logging in to the device.
<b>Connectivity</b>	<p>The device connectivity status and the time it was last checked. A green arrow means that the connection between the device and the FortiManager system is up; a red arrow means that the connection is down.</p> <p>Select <i>Refresh</i> to test the connection between the device and the FortiManager system.</p>
<b>Connect to CLI via</b>	Select SSH.
Configuration and Installation Status	
<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 a model device on page 40</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 a model device on page 40</a>.</p>

Configuration and Installation Status	
<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 a model device on page 40</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>Sync 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.



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

## Installing to devices

- To use the *Install Wizard* to install policy packages and device settings to one or more FortiGate devices, see [Using the Install Wizard to install policy packages and device settings on page 66](#).
- To use the *Install Wizard* to install device settings only, see [Using the Install Wizard to install device settings only on page 67](#).
- To reinstall a policy package without using the *Install Wizard*, see [Reinstall a policy package on page 165](#).



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

## Using the Install Wizard to install 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:

- If using ADOMs, ensure that you are in the correct ADOM.
- In the toolbar, select *Install Wizard* or *Install > Install Wizard*.
- Select *Install Policy Package & Device Settings* and specify the policy package and other parameters. 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

default

Comment

Write a comment

☒ Create ADOM Revision

Revision Name

default\_2017-7-17-15-14-10

Revision Comments

Write a comment

☒ Schedule Install

2017/07/17

03

14

PM

☐ Install Device Settings (only)

Next >

Cancel

<b>Policy Package</b>	Select the policy package from the dropdown list.
<b>Comment</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.

4. 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 170](#)).

Install Wizard - Policy Package (default)

✓ Installation Preparation Total: 1/1, Success: 1, Error: 0, Warning: 0

✓ Interface Validation

✓ Policy and Object Validation

✓ Policy Consistency Check [View Results]

✓ Ready to Install

Device Name	Status	Action
FortiGate-VM64[1]	Connection Up	Install Preview Policy Package Diff

Install Cancel

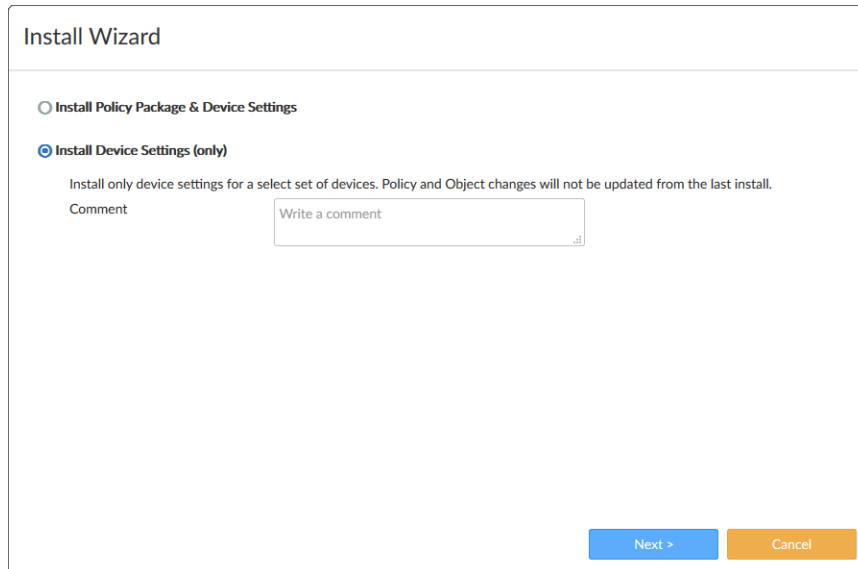
5. (Optional) Click the *Install Preview* button to view a preview of the installation and download a text file of the installation preview details. You can also download a text file of the installation preview details.
6. (Optional) Click the *Policy Package Diff* button to view the differences between the current policy and the policy in the device. See also [View a policy package diff on page 68](#).
7. 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.
8. Click *Finish* to close the wizard.

## Using the Install Wizard to 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.

## View 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. Right-click a device and select *Policy Package Diff*.  
The *Policy Package Diff* window is displayed after data is gathered.



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

4. Beside *Policy*, click the *Details* link to display details about the policy changes.
5. In the *Category* row, click the *Details* link to display details about the specific policy changes.
6. Beside *Policy Object*, click the *Details* link to display details about the policy object changes.
7. Click *Cancel* to close the window.

## Managing devices

Once a device has been added to the *Device Manager* pane, the configuration is available within other tabs in the FortiManager system, such as *Policy & Objects*.

This section includes the following topics:

- [Using the quick status bar](#)
- [Customizing columns](#)
- [Refreshing a device](#)
- [Editing device information](#)
- [Replacing a managed device](#)
- [Setting unauthorized device options](#)
- [Using the CLI console for managed devices](#)

### 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 information:

- Devices Total
- Devices Connection
- Devices Device Config
- Devices Policy Package

You can click each quick status to display only the devices referenced in the quick status.

#### To view the quick status bar:

1. Go to *Device Manager > Device & Groups*. The quick status bar is displayed.



2. In the tree menu, select a group. The devices for the group are displayed in the content pane, and the quick status bar updates.
3. Click the menu on each quick status to filter the devices displayed on the content pane.  
For example, click the menu for *Device Config* and select *Modified*. The content pane displays only devices in the selected group with modified configuration files.
4. Click *Devices Total* to return to the main view.

## 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. Click *Column Settings* and select the columns you want to display.

## 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. In the content pane, select a device.
2. Select *More > Refresh Device*. The *Update Device* dialog box opens to show the refresh progress.

## 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.

**Edit Device**

Name: fgt142

Description:

IP Address: 10.10.10.10

Serial Number: FGP2000000000000 (FortiGate-200D-POE)

Firmware Version: FortiGate 6.0, build76

Admin User: admin

Password: .....

Connected Interface: mgmt

HA Mode: Stand-Alone

**Device Location** ▾

Geographic Coordinate: 0.0 (Latitude) 0.0 (Longitude)

Show Map

Company/Organization: Optional

Country: Optional

Province/State: Optional

City: Optional

Contact: Optional

OK Cancel

4. Edit the device settings and click *OK*.

<b>Name</b>	The name of the device.
<b>Description</b>	Descriptive information about the device.
<b>IP Address</b>	Enter the IP address of the device.
<b>Pre-Shared Key</b>	<p>Enter the model device's pre-shared key. Select <i>Show Pre-shared Key</i> to see the key.</p> <p>This option is only available when editing a model device that was added with a pre-shared key.</p>
<b>Automatically link to real device</b>	<p>Select to automatically authorize the device to be managed by FortiManager when the device is online.</p> <p>This option is only available when editing a model device.</p>
<b>Serial Number</b>	<p>The serial number of the device.</p> <p>For model devices added with a pre-shared key, this will show the device model.</p>
<b>Firmware Version</b>	The firmware version.
<b>Admin User</b>	Enter the administrator user name.
<b>Password</b>	Enter the administrator user password.
<b>Connected Interface</b>	The connected interface, if the connection is up.
<b>HA Mode</b>	Displays whether the FortiGate unit is operating in standalone or high availability mode.

<b>Geographic Coordinates</b>	Identifies the latitude and longitude of the device location to support the interactive maps. Click <i>Show Map</i> to open a map showing the location of the device based on the coordinates. Click and drag the map marker to adjust the device's location.
<b>Company/Organization</b>	Optionally, enter the company or organization information.
<b>Country</b>	Optionally, enter the country where the device is located.
<b>Province/State</b>	Optionally, enter the province or state.
<b>City</b>	Optionally, enter the city.
<b>Contact</b>	Optionally, enter the contact information.

## 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 86](#)).
- If a template is assigned to the device, the template will remain with no device assignment ([Provisioning Templates on page 91](#)).
- 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 168](#)).
- 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 178](#)).
- If there are VDOMs in other ADOMs, they will be deleted with the device ([ADOM device modes on page 452](#)).

### 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 content pane, select a device and then click *Delete* in the toolbar, or right click on a device and select *Delete*.
4. 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 and re-deploy the configuration.



You can only reinstall a device that has a *Retrieve* button under the *Revision History* tab.

## 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.

## 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.

## Using the CLI console for managed devices

You can access the CLI console of managed devices.

**To use the CLI console:**

1. Go to *Device Manager*.
2. In the tree menu, select a device group, and in the bottom of the tree menu, select a device. The device dashboard displays.

- 3.** On the *Connection Summary* widget *Connect to CLI via line*, select *SSH*.

<b>Connect to:</b>	Shows the device that you are currently connected to. Select the dropdown menu to select another device.
<b>IP</b>	The IP address of the connected device.
<b>SSH</b>	Connect to the device via SSH.
<b>Connect   Disconnect</b>	Connect to the device you select, or terminate the connection.
<b>Close</b>	Exit the CLI console.

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*.

## Displaying Security Fabric topology

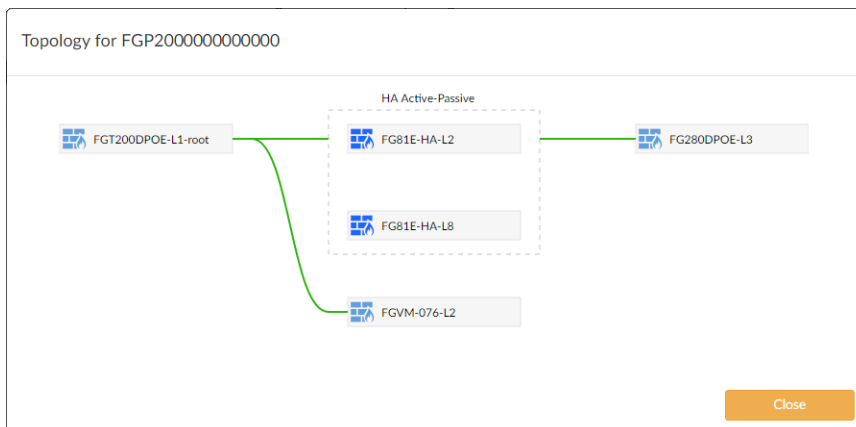
For Security Fabric devices, you can display the Security Fabric topology.

**To display the Security Fabric topology:**

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager* and click the *Devices Total* tab in the quick status bar.
3. 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.



## Manage Devices from Map View

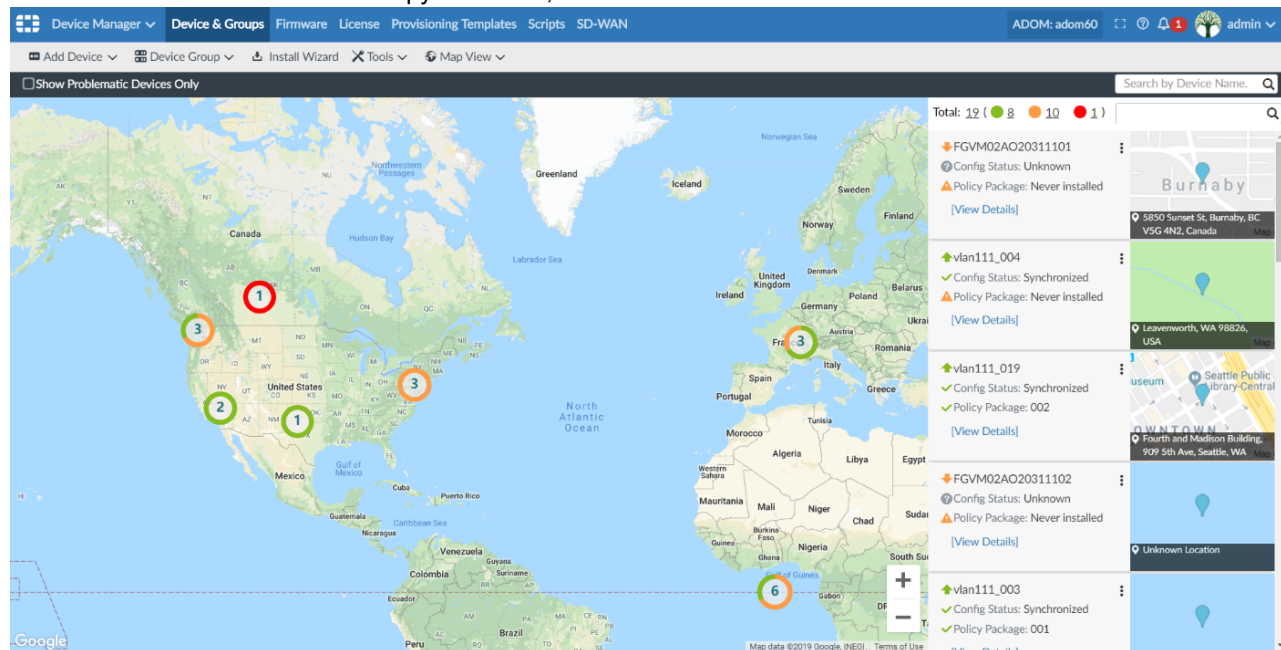
Automatically view the location of FortiGate devices on Google Maps using Map View. You can also manually configure the location of the FortiGate from FortiManager. Manage devices by performing various actions on the devices directly from the Map View.

## To Manage devices from Map View:

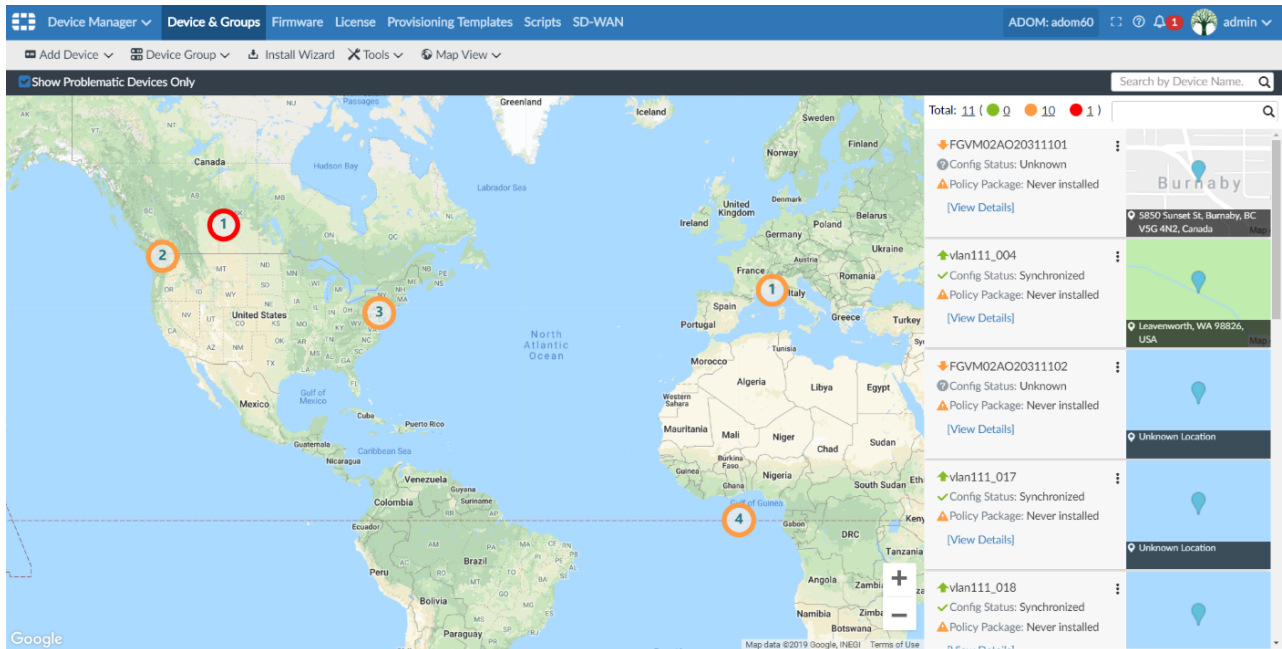
1. Go to Device Manager and select **Map View** from the menu options.

Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	IP Address	Platform	Description
FGVM02AO20311101	Unknown	Never installed	FortiGate 5.6.4.build1575 (GA)	FGVM02AO20311101	10.5.10.1	FortiGate-VM64	
FGVM02AO20311102	Unknown	Never installed	FortiGate 5.6.5.build1600 (GA)	FGVM02AO20311102	10.5.10.2	FortiGate-VM64	
vlan111_001	Modified	Never installed	FortiGate 6.0.3.build0200 (GA)	vlan111_001	10.5.11.1	FortiGate-VM64	
1 [NAT]	Synchronized	Never installed	FortiGate 6.0.3.build0200 (GA)			vdcom	
2 [NAT]	Synchronized	Never installed	FortiGate 6.0.3.build0200 (GA)			vdcom	
root [NAT] (Management)	Synchronized	Never installed	FortiGate 6.0.3.build0200 (GA)			vdcom	
vlan111_002	Synchronized	vlan111_002	FortiGate 6.0.3.build0200 (GA)	vlan111_002	10.5.11.2	FortiGate-VM64	
vlan111_003	Synchronized	001	FortiGate 6.0.3.build0200 (GA)	vlan111_003	10.5.11.3	FortiGate-VM64	
vlan111_004	Synchronized	Never installed	FortiGate 6.0.3.build0200 (GA)	vlan111_004	10.5.11.4	FortiGate-VM64	
vlan111_005	Synchronized	vlan111_005	FortiGate 6.0.3.build0200 (GA)	vlan111_005	10.5.11.5	FortiGate-VM64	
vlan111_006	Synchronized	vlan111_002	FortiGate 6.0.3.build0200 (GA)	vlan111_006	10.5.11.6	FortiGate-VM64	
vlan111_007	Synchronized	vlan111_007	FortiGate 6.0.3.build0200 (GA)	vlan111_007	10.5.11.7	FortiGate-VM64	
vlan111_008	Synchronized	vlan111_008	FortiGate 6.0.3.build0200 (GA)	vlan111_008	10.5.11.8	FortiGate-VM64	
vlan111_011	Synchronized	Never installed	FortiGate 6.0.3.build0200 (GA)	vlan111_011	10.5.11.11	FortiGate-VM64	
vlan111_013	Synchronized	Never installed	FortiGate 6.0.3.build0200 (GA)	vlan111_013	10.5.11.13	FortiGate-VM64	
vlan111_014	Synchronized	Never installed	FortiGate 6.0.3.build0200 (GA)	vlan111_014	10.5.11.14	FortiGate-VM64	
vlan111_015	Synchronized	Never installed	FortiGate 6.0.3.build0200 (GA)	vlan111_015	10.5.11.15	FortiGate-VM64	
vlan111_016	Synchronized	vlan111_016	FortiGate 6.0.3.build0200 (GA)	vlan111_016	10.5.11.16	FortiGate-VM64	
vlan111_017	Synchronized	Never installed	FortiGate 6.0.3.build0200 (GA)	vlan111_017	10.5.11.17	FortiGate-VM64	
vlan111_018	Synchronized	Never installed	FortiGate 6.0.3.build0200 (GA)	vlan111_018	10.5.11.18	FortiGate-VM64	
vlan111_019	Synchronized	002	FortiGate 6.0.3.build0200 (GA)	vlan111_019	10.5.11.19	FortiGate-VM64	
vlan111_020	Synchronized	Never installed	FortiGate 6.0.3.build0200 (GA)	vlan111_020	10.5.11.20	FortiGate-VM64	

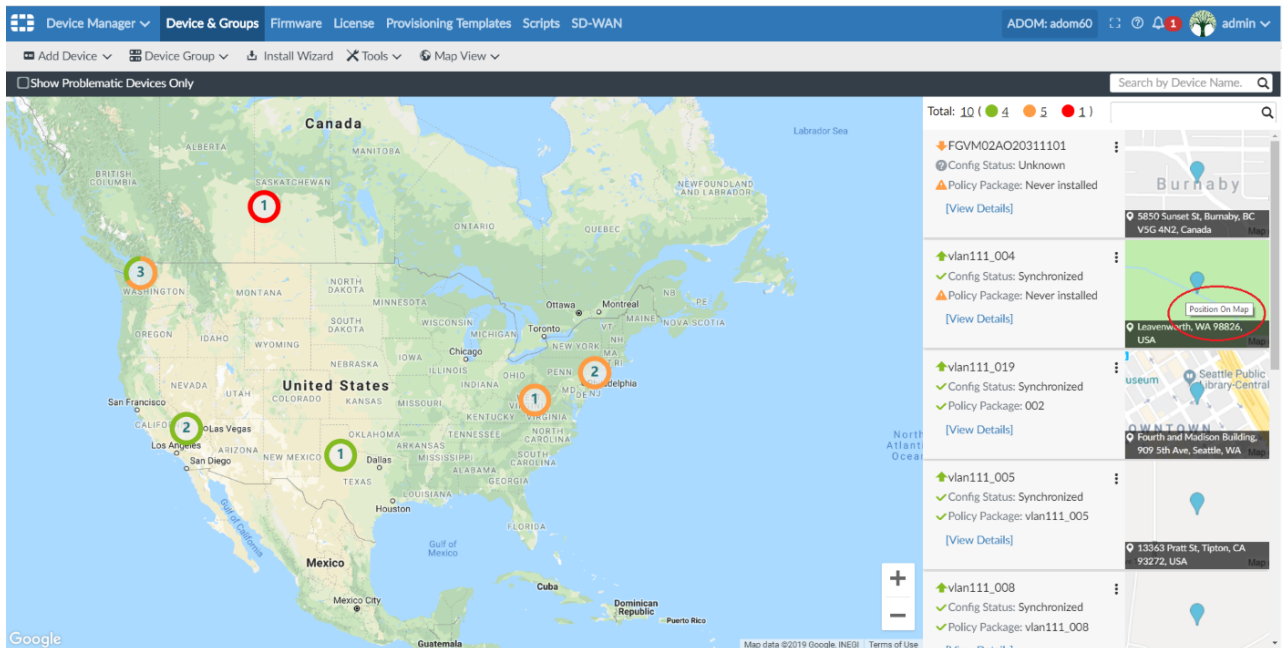
2. Map view shows device location on Google Maps and a combined status in Green, Orange, and Red colors.
  - Green - Shows devices are healthy. The policy package configuration and device configuration are in sync.
  - Orange - Shows a warning status. The device configuration status or policy package 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.



3. Select **Show Problematic Devices Only** to filter devices on the map and show it on the right pane with **Orange** or **Red** status.



- To manually position a device, click the device shown on the smaller map on the right pane.





5. Enter the location of the device manually. You can drag the device to the accurate position.

The screenshot shows the FortiManager 6.2.1 Device Manager interface. The 'Device & Groups' tab is selected. A table lists devices with their names, geographic coordinates, cities, and countries. The 'vlan111\_004' device is highlighted. To the right, a map view shows the location of Sunnyvale, CA, USA, with a red pin indicating the device's position. The map includes labels for various streets and districts like Sunnyvale West, Heritage District, and Cherry Orchard.

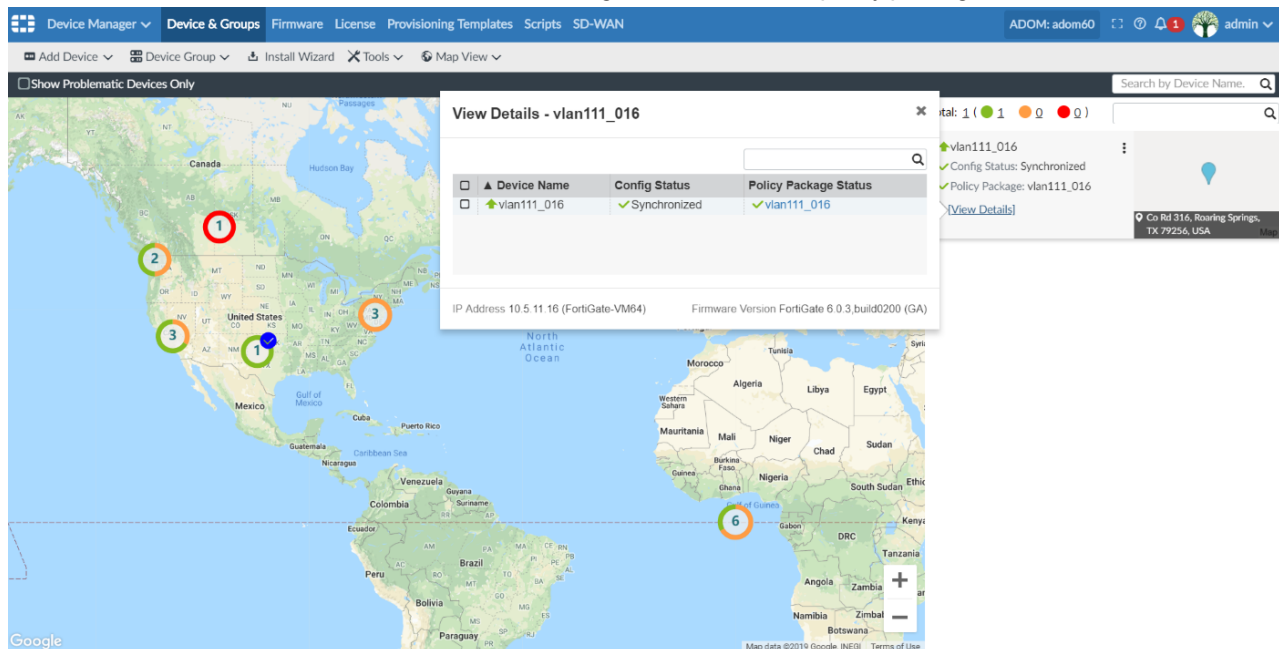
Device Name	Geographic Coordinate	City	Country
FGVM02AO20311101	49.2488091, -122.9805104	Burnaby	Canada
FGVM02AO20311102	0, 0	Unknown Location	Democratic Republic of the Congo
vlan111_001	38.5481654230466, -80.33203125	Webster Springs	United States
vlan111_002	45.089035564831, 0.87890625	Saint-Pierre-de-Chignac	France
vlan111_003	0, 0	Alexandria	United States
vlan111_004	37.36883, -122.0363496	Sunnyvale	United States
vlan111_005	36.0313317763319, -119.35546875	Tipton	United States
vlan111_006	0, 0	Sunnyvale	United States
vlan111_007	50.9584267233599, 8.61328125	Battenberg (Eder)	Germany
vlan111_008	36.2088230928372, -115.0048828125	Las Vegas	United States
vlan111_011	52.7259844176303, -108.9613773	Cut Knife	Canada
vlan111_013	43.6158017, 7.05424770000002	Valbonne	France
vlan111_014	40.7511838, -73.9921394	New York	United States
vlan111_015	40.7511838, -73.9921394	New York	United States
vlan111_016	33.8704155509418, -100.8984375	Roaring Springs	United States
vlan111_017	0, 0	Unknown Location	Unknown Location
vlan111_018	0, 0	Unknown Location	Unknown Location
vlan111_019	47.6062095, -122.3320708	Seattle	United States
vlan111_020	0, 0	Unknown Location	Unknown Location

6. Click *Show Unpositioned Devices* to filter devices that do not have any location.

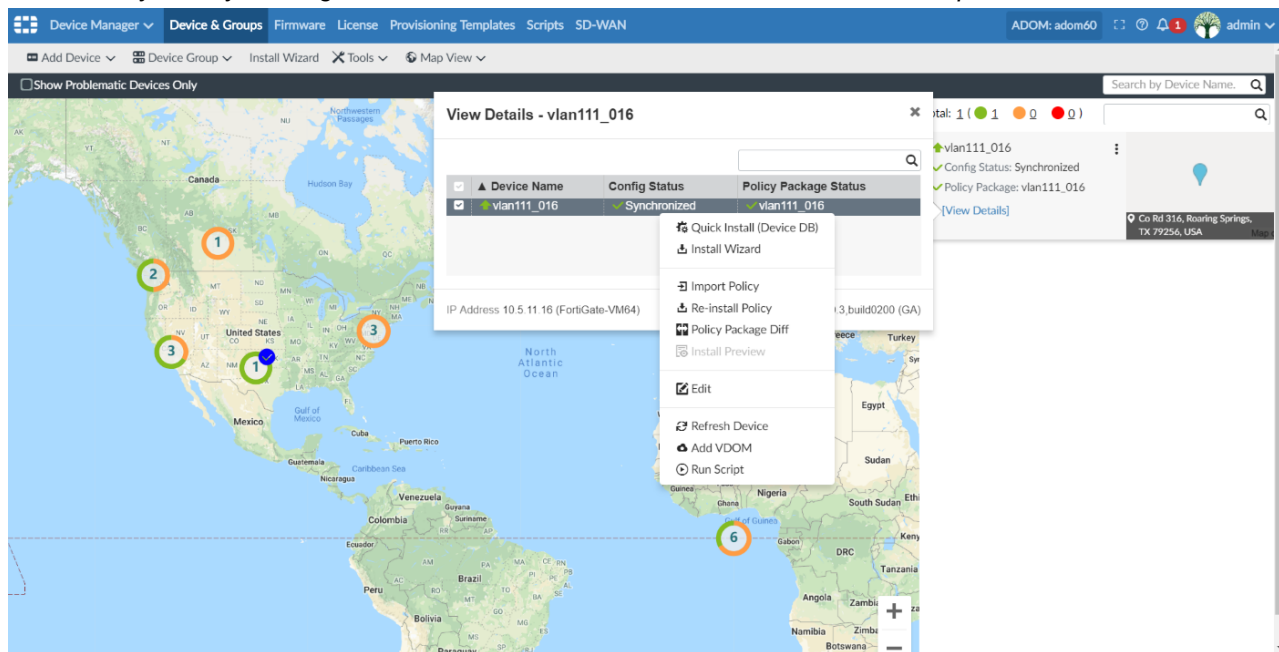
The screenshot shows the FortiManager 6.2.1 Device Manager interface. The 'Device & Groups' tab is selected. A table lists devices with their names, geographic coordinates, cities, and countries. The 'vlan111\_017', 'vlan111\_018', and 'vlan111\_020' devices are highlighted. To the right, a world map view shows the entire globe, indicating that the devices are unpositioned. The map includes labels for various continents and oceans like North Atlantic Ocean, South Atlantic Ocean, Indian Ocean, and Southern Ocean.

Device Name	Geographic Coordinate	City	Country
vlan111_017	0, 0	Unknown Location	Unknown Location
vlan111_018	0, 0	Unknown Location	Unknown Location
vlan111_020	0, 0	Unknown Location	Unknown Location

7. Click *View Details* for the device to show device configuration status and policy package status.



8. Right-click the device menu to 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*.



## Managing device configurations

The FortiManager system 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:

- [View configurations for device groups](#)
- [Checking device configuration status](#)
- [Managing configuration revision history](#)

## View configurations for device groups

You can view configuration information for devices in a group on the *Device Manager* tab.

### To view configurations:

1. Go to *Device Manager > Device & Groups*.
2. 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>	See the table below for config status details.
<b>Policy Package Status</b>	See the table below for policy package status details. Click on the policy package name to go to view and manage the package (see <a href="#">Managing policy packages on page 161</a> ).
<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>Firmware Version</b>	The firmware version.
<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>Country</b>	The country where the device is located.
<b>Province/State</b>	The province or state.
<b>City</b>	The city.
<b>Contact</b>	The contact information.

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.
<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.

Policy Package Status	Icon	Description
<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 	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.

## 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 *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.

The *Configuration and Installation Status* widget shows the following information:

<b>System Template</b>	Displays the name of the selected system template. Click <i>Change</i> to change the system template.
<b>Database Configuration</b>	Click <i>View</i> to display the database configuration file of the FortiGate unit.
<b>Total Revisions</b>	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="#">Managing configuration revision history on page 82</a> . Click <i>Revision Diff</i> to compare revisions. For details, see <a href="#">Comparing different configuration files on page 85</a> .
<b>Sync Status</b>	The synchronization status with the FortiManager. <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>

Click *Refresh* to update the synchronization status.

#### Warning

Displays any warnings related to configuration and installation status.

- *None*: No warning.
- *Unknown configuration version running on FortiGate: FortiGate configuration has been changed!*: The FortiManager system cannot detect which revision (in revision history) is currently running on the device.
- *Unable to detect the FortiGate version*: Connectivity error.
- *Aborted*: The FortiManager system cannot access the device.

#### Installation Tracking

##### Device Settings Status

- *Modified*: Some configuration on the device has changed since the latest revision in the FortiManager database. Click *Save Now* to install and save the configuration.
- *UnModified*: All configuration displayed on the device is saved as the latest revision in the FortiManager database.

##### Installation Preview

Click *Preview* to preview an actual device configuration installation, including any errors and warnings.

##### Last Installation

Displays the last installation's date, time, revision number, and the person who did the installation.

##### Scheduled Installation

Displays the data and time when a new configuration will be installed on the device.

#### Script Status

##### Last Script Run

Displays the date and time when the last script was run. Click *View History* to see the script execution history.

##### Scheduled Script

Displays the date and time when the next script is scheduled to run.

## Managing 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 *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*.

In the *Configuration Revision History* dialog box, the following buttons are in the toolbar:

#### View Config

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 85</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> </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.

#### To view the configuration settings on a FortiGate unit:

1. Go to *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*.
5. 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.

**To add a tag (name) to a configuration version on a FortiGate unit:**

1. Go to *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*.
5. 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 and importing a configuration file**

You can download a configuration file and a factory default configuration file. You can also 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 download a configuration file:**

1. Go to *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*.
5. Select the revision you want to download.
6. Click *View Config > Download*.
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 *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*.
5. In the toolbar, click *Download Factory Default*.

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

1. Go to *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*.



5. 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 *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*.
5. Select a revision, and click *Revision Diff* in the toolbar.
6. 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.

### To revert to another configuration file:

1. Go to *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*.

5. Right-click the revision to which you want to revert, and click *Revert*.  
The system immediately reverts to the selected revision.

## Device groups

On the *Device Manager > Device & Groups* pane, you can create, edit, and delete device groups.

### 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 groups.

### Add device groups

You can create a group and add devices to the group.

#### To add 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*.

### Manage 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.

---

## Firmware

On the *Device Manager > Firmware* pane, you can view the firmware installed on managed devices. You can also view whether a firmware upgrade is available and the upgrade history for devices.

### View firmware for device groups

You can view firmware information for devices in a group.

**To view firmware:**

1. Go to *Device Manager*.
2. In the tree menu, select the device group name, for example, *Managed Devices*.
3. Click the *Firmware* tab.

For a description of the options, see [Firmware Management on page 88](#).

### Upgrade firmware for device groups

The firmware of the devices within a group can also be updated as a group.

**To update device group firmware:**

1. Go to *Device Manager*.
2. In the tree menu, select the device group name, for example, *Managed Devices*.
3. Click the *Firmware* tab.
4. Locate an applicable firmware image in the *Available Upgrade* list, then click *Upgrade* to upgrade all of the devices in the group to that image.

The upgrade history is also shown and you can view more details by clicking *All History*.

## Firmware Management

FortiGate device firmware can be updated from the *Device Manager > Firmware* pane. Upgrades can also be scheduled to occur at a later date.

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.

In the *Device Manager* pane, select the *Managed Devices* group, then click the *Firmware* tab.

Device Manager > Device & Groups > Firmware					
Upgrade View Release Note Imported Images Refresh Column Settings					
#	Device Name	Platform	Current Build	Upgrade Available	Status
5.6.2 (1)					
1	FortiGate-VM64	FortiGate-VM64	1486	6.0.0 (76) Upgrade	
6.0.0 (2)					
1	Igt142	FortiGate-200D-POE	76	Running Latest Release	
2	Igt148	FortiGate-80E-POE	119	6.0.0 (76) Upgrade	

The following information and options are available:

<b>Upgrade</b>	Select to upgrade the selected device if the device can be upgraded.
<b>View Release Notes</b>	Select to view the release notes for the FortiOS version of the selected device.
<b>Imported Images</b>	Select to display the imported images where you can import or delete images.
<b>Refresh</b>	Refresh the list.
<b>Column Settings</b>	Click to select which columns to display or select <i>Reset to Default</i> to display the default columns.
<b>Device Name</b>	The names of the FortiGate devices in the group, organized by firmware version.
<b>Platform</b>	The device platform.
<b>Current Build</b>	The build installed in the device.
<b>Upgrade Available</b>	The current firmware version and build number of the firmware on the device. If an update is available and can be applied to the device, Upgrade can be selected to open the <i>Upgrade Firmware</i> dialog box.
<b>Status</b>	The status of the device's license. If the license has expired, the firmware cannot be upgraded.
<b>Upgrade History</b>	Right-click a device and select <i>Show Upgrade History</i> to view the device's upgrade history.

### To upgrade a device's firmware:

1. Go to *Device Manager*.
2. In the tree menu, select a device group, and then click the *Firmware* tab.
3. Select a device or device group with an upgrade available that is licensed for firmware upgrades, then click *Upgrade* in either the toolbar or in the *Upgrade Available* column. The *Upgrade Firmware* dialog box opens.

Upgrade Firmware

Devices

FortiGate-VM64

Upgrade to

5.6.2 (1486)

☒ Schedule Upgrade
 

2017/12/05

08:16

If scheduled upgrade fails

☒ Cancel Upgrade
 

☐ Retry
 

2

 times, retry interval 

2

 minutes.

☐ Boot From Alternate Partition After Upgrade
 

OK

Cancel

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

<b>Upgrade to</b>	Select a firmware version from the dropdown list.
<b>Schedule Upgrade</b>	Select to schedule the upgrade, then enter the date and time for the upgrade, and select an action to take if the update fails: <ul style="list-style-type: none"> <li>Cancel Upgrade</li> <li>Retry: enter the number of times to retry and the time between retries.</li> </ul>
<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.



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.

## License

On the *Device Manager > License* pane, you can view license information for managed devices.

## View licenses for device groups

You can view license information for devices in a group.

**To view licenses:**

1. Go to *Device Manager*.
2. In the tree menu, select a device group, and then click the *License* tab.

For a description of the options, see [License Management on page 90](#).

## License Management

You can check FortiGate device licenses in *Device Manager > License*.

In the *Device Manager* pane, select the *Managed Devices* group, then click the *License* tab.

#	Device Name	Serial Number	Firmware Version	Support Contract	FortiGuard Subscription	Service Status	Virtual Domains
1	149	FGVM160000000000	6.0.0, build76	24x7	All Valid	Unknown	3/10
2	FG-152	FGVMEV0000000000	6.0.0, build76	24x7	All Valid	Unknown	2/10
3	FortiGate-VM64	FGVM010000000000	6.0.0, build76	8x5	All Valid	Unknown	1/10

The following columns are displayed. You can filter columns that have a *Filter* icon.

<b>Device Name</b>	Name of the device
<b>Serial Number</b>	Serial number for the device
<b>Firmware Version</b>	Firmware version for 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>License status of FortiGuard. The status reflects the worst license status of the individual components of the FortiGuard license. Hover over the license status to display details about the following components: IPS &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> <li>• Unknown</li> </ul>
<b>Service Status</b>	<p>License status of antivirus and IPS service. Hover the mouse over the cell to display details about the service status. 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>

The following buttons are available on the toolbar:

<b>Push Update</b>	Push a license update to the selected device in the group.
<b>Refresh</b>	Refresh the list of devices in the group.
<b>Export</b>	Click to export the device list, device update details, and license details to a PDF or CSV file format. A file in the selected format is downloaded to the management computer.
<b>Column Settings</b>	Click to select which columns display on the License pane.

## Add-on license

Add-on licenses can be purchased for high end FortiManager devices to increase the number of device that can be managed. An add-on license can only be added using the CLI.

The below table lists the device that can have add-on licenses added, the number of devices the FortiManager can manage by default, and the maximum number of devices that can be managed by adding add-on licenses.

Model	Normal license	With add-on license
FMG-3900E	10000	100000
FMG-3000F	4000	8000
FMG-4000E	4000	8000

### To add an add-on license:

1. Purchase an add-on license (<https://support.fortinet.com>).
2. Open the license file in a text editor.
3. Connect to the CLI and run the following command:  

```
execute add-on-license <license>
```

Where **<license>** is the license text, copied and pasted from the text editor.
4. After the system automatically reboots, check the *License Information* widget to confirm that the number of *Devices/VODMs* that can be managed has increased. See [License Information widget on page 436](#).

## Provisioning Templates

Go to *Device Manager > Provisioning Templates* to access configuration options for the following templates:

- [System templates](#)
- [Threat Weight templates](#)
- [Certificate templates](#)

## 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
DNS	Primary DNS Server, Secondary DNS Server, Local Domain Name.



Widget	Description
<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.
<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.

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 to be associated with the template by selecting *Assign to Device*.

#### To assign a system template to a device:

1. Go to *Device Manager > Provisioning Templates > System Templates*.
2. In the content pane, select a template and click *Assign to Device*.
3. Select devices to assign to and click *OK*.  
The devices assigned to the template are shown in the *Assign to Device* column.

## 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.

## 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.

## 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 DB. 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 for you to be able to 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 102](#) for information.

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 529](#).
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 97</a> .
<b>Schedule Script</b>	Schedule when the selected script will run. See <a href="#">Schedule a script on page 101</a> .
<b>Create New / New</b>	Create a new script. See <a href="#">Add a script on page 98</a> .
<b>Edit</b>	Edit the selected script. See <a href="#">Edit a script on page 99</a> .
<b>Delete</b>	Delete the selected script. See <a href="#">Delete a script on page 100</a> .
<b>Clone</b>	Clone the selected script. See <a href="#">Clone a script on page 100</a> .
<b>Import CLI Script / Import</b>	Import a script from your management computer. See <a href="#">Import a script on page 100</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 100</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 101](#)).

**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 107](#) 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* ([Display options on page 160](#)).
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*, or right-click anywhere in the script list and select *New* from the menu. The *Create Script* dialog box.

Create New Script

Script Name

[\[View Sample Script\]](#)

Comments

0/255

Type

CLI Script

Run script on

Device Database

Script details

Advanced Device Filters

OK

Return

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.
<b>Script Detail</b>	Type the script itself, either manually using a keyboard, or by copying and pasting from another editor.
<b>Advanced Device Filters</b>	Select to adjust the advanced filters for the script. The options include: <ul style="list-style-type: none"><li>• <i>Platform</i> (select from the dropdown list)</li><li>• <i>Build</i></li><li>• <i>Device</i> (select from the dropdown list)</li><li>• <i>Host name</i></li><li>• <i>SN</i></li></ul> These options are not available for Global Database ADOM scripts, or if <i>Run script on</i> is set to <i>Policy Package or ADOM Database</i> .

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

Scripts can be exported to text files on your local computer.

### 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*.
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

Scripts can be imported as text files from your local computer.



**To import a 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 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.

## 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 group will run.</li> <li>• <i>Monthly</i> - Set the day of the month and the time of day that the script or group will run.</li> </ul>

## 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 > CLI Script Group*.

The following information is displayed:

<b>Name</b>	The user-defined script group name.
<b>Members</b>	The scripts that are included in the script group.
<b>Target</b>	The script group target.
<b>Comments</b>	User defined comment for the 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 *Policy Package* or *ADOM Database*, select the policy package from the drop-down list, then click *Run Now*.

**Search** Enter a search term in the search field to search the script groups.

### To create a new CLI script group:

1. Go to *Device Manager > Scripts > CLI Script Group*.
2. Select *Create New* 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.
<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>
<b>Members</b>	Use the directional arrows to move available scripts to member scripts.

## Script syntax

Most script syntax is the same as that used by FortiOS. For information see the *FortiOS CLI Reference*, available in the [Fortinet Document Library](#).

Some special syntax is required by the FortiManager to run CLI scripts on devices.

### Syntax applicable for address and address6

```
config firewall address
edit xxxx

...regular FOS command here...

config dynamic_mapping
edit "<dev_name>"-"<vdom_name>"
set subnet x.x.x.x x.x.x.x
next
end
```

### Syntax applicable for ippool and ippool6

```
config firewall ippool
edit xxxx

...regular FOS command here...

config dynamic_mapping
```

```
edit "<dev_name>"-"<vdom_name>"
    set startip x.x.x.x
    set endip x.x.x.x
next
end
```

### Syntax applicable for vip, vip6, vip46, and vip64

```
config firewall vip
edit xxxx

...regular FOS command here...

config dynamic_mapping
edit "<dev_name>"-"<vdom_name>"
    set extintf "any"
    set extip x.x.x.x-x.x.x.x
    set mappedip x.x.x.x-x.x.x.x
    set arp-reply enable|disable
next
end
```

### Syntax applicable for dynamic zone

```
config dynamic interface
edit xxxx
    set single-intf disable
    set default-mapping enable|disable
    set defmap-intf xxxx
    config dynamic_mapping
        edit "<dev_name>"-"<vdom_name>"
            set local-intf xxxx
            set intrazone-deny enable|disable
        next
    end
next
end
```

### Syntax applicable for dynamic interface

```
config dynamic interface
edit xxxx
    set single-intf enable
    set default-mapping enable|disable
    set defmap-intf xxxx
    config dynamic_mapping
        edit "<dev_name>"-"<vdom_name>"
            set local-intf xxxx
            set intrazone-deny enable|disable
        next
    end
next
end
```

**Syntax applicable for dynamic multicast interface**

```
config dynamic multicast interface
  edit xxx
    set description xxx
    config dynamic_mapping
      edit "fgtname"-"vdom"
        set local-intf xxx
      next
    end
  next
end
```

**Syntax applicable for local certificate (dynamic mapping)**

```
config dynamic certificate local
  edit xxxx
    config dynamic_mapping
      edit "<dev_name>"-"global"
        set local-cert xxxx
      next
    end
```

**Syntax applicable for vpn tunnel**

```
config dynamic vpntunnel
  edit xxxx
    config dynamic_mapping
      edit "<dev_name>"-"<vdom_name>"
        set local-ipsec "<tunnel_name>"
      next
    end
```

**Syntax applicable for vpn console table**

```
config vpnmgr vpntable
  edit xxxx
    set topology star|meshed|dial
    set psk-auto-generate enable|disable
    set psksecret xxxx
    set ike1proposal 3des-sha1 3des-md5 ...
    set ike1dhgroup XXXX
    set ike1keylifeseq 28800
    set ike1mode aggressive|main
    set ike1dpd enable|disable
    set ike1nat traversal enable|disable
    set ike1nat keepalive 10
    set ike2proposal 3des-sha1 3des-md5
    set ike2dhgroup 5
    set ike2keylifetype seconds|kbyte|both
    set ike2keylifeseq 1800
    set ike2keylifekbs 5120
    set ike2keepalive enable|disable
    set replay enable|disable
    set pfs enable|disable
    set ike2autonego enable|disable
```

```
    set fcc-enforcement enable|disable
    set localid-type auto|fqdn|user-fqdn|keyid|addressasn1dn
    set authmethod psk|signature
    set inter-vdom enable|disable
    set certificate XXXX
  next
end
```

### Syntax applicable for vpn console node

```
config vpnmgr node
  edit "1"
    set vpntable "<table_name>"
    set role hub|spoke
    set iface xxxx
    set hub_iface xxxx
    set automatic_routing enable|disable
    set extgw_p2_per_net enable|disable
    set banner xxxx
    set route-overlap use-old|use-new|allow
    set dns-mode manual|auto
    set domain xxxx
    set local-gw x.x.x.x
    set unity-support enable|disable
    set xauthtype disable|client|pap|chap|auto
    set authusr xxxx
    set authpasswd xxxx
    set authusrgrp xxxx
    set public-ip x.x.x.x
    config protected_subnet
      edit 1
        set addr xxxx xxxx ...
      next
    end
  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 97](#).
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 476](#).

## 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 112](#).

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 112](#).

## 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>	This script does not work when run on a policy package.



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:

```
config global
    show system interface port1
end
```

Since running on device database does not yield any useful information.

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

```
----- 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 -----
```

The script should be run on the FortiGate Directly (via CLI).

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

```
----- Executing time: 2013-10-15 13:52:02 -----
Starting log (Run on device)
FortiGate-VM64 $ config global
FortiGate-VM64 (global) $ show system interface port1
config system interface
    edit "port1"
        set vdom "root"
        set ip 10.2.66.181 255.255.0.0
        set allowaccess ping https ssh snmp http fgfm auto-ipsec radius-acct
            probe-response capwap
        set type physical
        set snmp-index 1
    next
end
FortiGate-VM64 (global) $ end
----- The end of log -----
```

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   next end </pre>
<b>Variations</b>	none

#### View information about all the configured FDN servers on this device:

<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 </pre>

```
-- Server List (Tue Oct 3 09:34:46 2006) --

IP Weight Round-time TZ Packets Curr Lost Total Lost
** None **
```

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       set sysgrp read     next   end end</pre>
<b>Output</b>	<p>View the log of script running on device:FortiGate-VM64</p> <pre>----- 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 -----</pre>

<b>Variations</b>	<p>This profile is read-only to allow a policy administrator to monitor this device's configuration and traffic.</p> <p>Variations may include enabling other areas as read-only or write permissions based on that account type's needs.</p>
-------------------	---

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
```

- **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 differvcode\_forward 000011 entry - if its not found lines 12-15 are executed, otherwise they are skipped
- line 12 opens the policy determined by the loop counter
- line 13-14 enable diffserv\_forward, and set it to 000011
- line 15 saves this entry and prepares for the next one
- line 16 closes the if statement
- line 17 closes the for each loop
- line 18 saves all the updated firewall policy entries

## Additional Tcl Scripts

### Example: Get and display state information about the FortiGate device:

Script:

```

#!
#Run on FortiOS 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>	<pre>puts [exec_ondb "/adom/./pkg/&lt;pkg_fullpath&gt;" "embedded cli commands" "# "] or puts [exec_ondb "/pkg/&lt;pkg_fullpath&gt;" "embedded cli commands" "# "]</pre>
<b>Usage</b>	<pre>puts [exec_ondb "/adom/./pkg/default" " config firewall address edit port5_address next end " "# "]</pre>

**Example 3:**

Run Tcl script on a specific device in an ADOM:

<b>Syntax</b>	<pre>puts [exec_ondb "/adom/&lt;adom_name&gt;/device/&lt;dev_name&gt;" "embedded cli commands" "# "]</pre>
<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>	<pre>puts [exec_ondb "/adom/&lt;adom_name&gt;/device/." "embedded cli commands" "# "]</pre>
<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.

## SD-WAN

Go to *Device Manager* > *SD-WAN* to configure SD-WAN templates and assign FortiGate devices to the templates.

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.

Using SD-WAN templates consists of the following steps:

1. Specify the ports where the SD-WAN settings will be applied. See [Interface members on page 129](#).
2. Specify the health-check servers that will monitor the network parameters. See [Health-Check Servers on page 138](#).
3. Create an SD-WAN template that includes the following:
  - a. Add Interface Members - add the Interface Members created in step 1.
  - b. Performance SLA - create a Performance SLA. Add the Interface Member and Health Check Servers.
  - c. SD-WAN Rules - create rules and configure advanced options on network traffic management.See [SD-WAN templates on page 131](#).
4. Assign a FortiGate device to the SD-WAN template. See [Assigned devices on page 140](#).
5. Install device settings using the *Install Wizard*. See [Using the Install Wizard to install device settings only on page 67](#).
6. Go to *SD-WAN* > *Monitor* to monitor the FortiGate devices. See [Monitor SD-WAN on page 140](#).



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 using the *Install Wizard* to be in sync with the settings on the FortiGate.

## Enabling central SD-WAN management

Central SD-WAN management can be enabled per ADOM. When enabled, the *SD-WAN* tab shows the following items on the left pane:

- Assigned Devices
- SD-WAN Templates
- Interface Members
- Health-Check Servers
- Monitor

**To enable central SD-WAN management:**

1. Go to *System Settings > All ADOMs*.
2. Select the ADOM and click *Edit* in the toolbar, or right-click the ADOM and select *Edit* from the pop-up menu. The *Edit ADOM* window opens. (See [Editing an ADOM on page 460](#).)
3. Next to *Central Management*, select the *SD-WAN* check box.
4. Click *OK*.

## Interface members

Create new WAN interface members.

**To create a new interface member:**

1. Ensure that you are in the correct ADOM and that central SD-WAN management is enabled.
2. Go to *Device Manager > SD-WAN > Interface Members*.
3. Click *Create New* in the content pane toolbar, or right-click and select *Create New*. The *Create New WAN Interface* page opens.

4. Enter the following information, then click *OK* to create the new WAN interface:

<b>Name</b>	Enter the name of the WAN detect server.
<b>Description</b>	Enter a description of the server.
<b>Default Interface</b>	Specify the default interface for the WAN link.
<b>Gateway</b>	The default gateway for this interface. Usually the default gateway of the Internet service provider that this interface is connected to.
<b>Weight</b>	Weight of this interface for weighted load balancing (0 - 255). More traffic is directed to interfaces with higher weights.
<b>Volume Ratio</b>	Measured volume ratio (this value / sum of all values = percentage of link volume, 0 - 255).
<b>Per-Device Mapping</b>	Enable per-device mapping. See <a href="#">Per-device mapping on page 130</a> .
<b>Advanced Options</b>	

<b>gateway6</b>	IPv6 gateway address.
<b>ingress-spillover-threshold</b>	Ingress spillover threshold for this interface (0 - 16776000 kbit/s). When this traffic volume threshold is reached, new sessions spill over to other interfaces in the SD-WAN.
<b>priority</b>	Priority of the interface (0 - 4294967295). Used for SD-WAN rules or priority rules.
<b>source</b>	Source IPv4 address.
<b>source6</b>	Source IPv6 address.
<b>spillover-threshold</b>	Egress spillover threshold for this interface (0 - 16776000 kbit/s). When this traffic volume threshold is reached, new sessions spill over to other interfaces in the SD-WAN.
<b>status</b>	Enable/disable the interface.

#### To edit an interface member:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN > Interface Members*.
3. Select the interface member from the list and click *Edit* in the toolbar, or right-click the interface then select *Edit*. The *Edit WAN Interface* page opens.
4. Edit the interface as required, and click *OK* to apply your changes.

#### To delete an interface member or members:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN > Interface Members*.
3. Select the interface or interfaces from the list and click *Delete* in the toolbar, or right-click the interface and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the interface or interfaces.

## Per-device mapping

#### To add WAN interface per-device mapping:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN > Interface Members*.
3. Click *Create New* in the content pane toolbar, or right-click and select *Create New*. The *Create New WAN Interface* page opens.
4. Enable *Per-Device Mapping*.

5. Click *Create New* in the per-device mapping toolbar. The *Create New Interface Member* dialog-box opens.

6. Select a *Mapped Device* then an *Interface* from the drop-down lists.
7. Enter the *Gateway* IP address, *Weight*, *Volume*, and *Advanced Options*.
8. Click *OK*.

#### To edit WAN interface per-device mapping:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN > Interface Members*.
3. Click *Create New* in the content pane toolbar, or right-click and select *Create New*. The *Create New WAN Interface* page opens.
4. Select a per device mapping then click *Edit* in the per-device mapping toolbar. The *Edit Interface Member* dialog-box opens.
5. Edit the settings as required, then click *OK*.

#### To delete WAN interface per-device mappings:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN > Interface Members*.
3. Click *Create New* in the content pane toolbar, or right-click and select *Create New*. The *Create New WAN Interface* page opens.
4. Select one or more per device mapping, then click *Delete* in the per-device mapping toolbar.
5. Click *OK* in the confirmation dialog box to delete the mapping or mappings.

## SD-WAN templates

Create an SD-WAN template with the required network parameters. Create the interface member and health-check servers before adding them to the SD-WAN template. See [Interface members on page 129](#) and [Health-Check Servers on page 138](#).

#### To create a new SD-WAN template:

1. Ensure that you are in the correct ADOM and that central SD-WAN management is enabled.
2. Go to *Device Manager > SD-WAN > SD-WAN Template*.

3. Click *Create New* in the content pane toolbar, or right-click and select *Create New*. The *Create New* page opens.

**Create New**

Name

Description  0/4096

SD-WAN Status

**Interface Members**

+ Create New ☐ Edit ☐ Delete

<input type="checkbox"/>	#	ID	Port
--------------------------	---	----	------

**Performance SLA**

+ Create New ☐ Edit ☐ Delete

<input type="checkbox"/>	#	Name	Detect Server	Detect Protocol	Failure Threshold	Recovery Threshold
--------------------------	---	------	---------------	-----------------	-------------------	--------------------

**SD-WAN Rules**

+ Create New ☐ Edit ☐ Delete

<input type="checkbox"/>	#	Name	Source	Destination	Criteria	Members
<input type="checkbox"/>	1	sd-wan	ALL	ALL	Source IP Based	ALL

**Advanced Options** ▾

fail-alert-interfaces

fail-detect

4. Enter the following information and click *OK* to create the new SD-WAN template:

<b>Name</b>	Enter the name of the template.
<b>Description</b>	Enter a description of the template.
<b>SD-WAN Status</b>	Select <i>On</i> or <i>Off</i> .
<b>Interface Members</b>	Interface members can be added, edited, and removed. An interface member must be created before it can be added to a template, see <a href="#">Interface members on page 129</a> .
<b>Performance SLA</b>	See <a href="#">Performance SLA on page 133</a> .
<b>SD-WAN Rules</b>	See <a href="#">SD-WAN rules on page 135</a> .
<b>Advanced Options</b>	
<b>fail-alert-interfaces</b>	Names of the FortiGate interfaces from which the link failure alert is sent for this interface.
<b>fail-detect</b>	Enable/disable fail detection features for this interface.

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

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN > SD-WAN Template*.
3. Select the template from the list and click *Edit* in the toolbar, or right-click the template and select *Edit*. The *Edit* page opens.
4. Edit the template as required, and click *OK* to apply your changes.



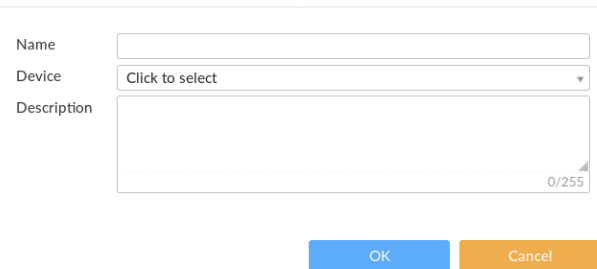
**To delete an SD-WAN template:**

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN > SD-WAN Template*.
3. Select the template from the list and click *Delete* in the toolbar, or right-click the template and select *Delete*.
4. Click OK in the confirmation dialog box to delete the template or templates.

**To import an SD-WAN template or templates:**

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN > SD-WAN Template*.
3. Click *Import*. The Import SD-WAN templates screen is shown.

Import SD-WAN templates



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 and now visible in *Device Manager > SD-WAN > SD-WAN Template*.



A prefix *Import* is automatically added to SD-WAN templates that are imported from the FortiGate devices.

## Performance SLA

Create a Performance SLA in FortiManager that can be used to monitor the SD-WAN performance in FortiGate devices. You can also create a Performance SLA in FortiManager. 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. Ensure that you are in the correct ADOM and that central SD-WAN management is enabled.
2. Go to *Device Manager > SD-WAN > SD-WAN Template*.
3. Click *Create New* in the content pane toolbar, or right-click and select *Create New*. The *Create New* page 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>Detect 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>
<b>Detect Server</b>	Enter the IP address of the WAN interface that you want to monitor.
<b>Member</b>	Select available interface members. The interfaces must already be added to the template.
<b>SLA</b>	Click <i>Create New</i> to create a new SLA. Enable and enter the <i>Jitter Threshold</i> (in milliseconds), <i>Latency Threshold</i> (in milliseconds), and <i>Packet Loss Threshold</i> (in percent), then click <i>OK</i> to create the SLA. SLAs can also be edited and deleted as required.
<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>	
<b>addr-mode</b>	Address mode (IPv4 or IPv6).
<b>http-get</b>	URL used to communicate with the server if the protocol is HTTP.
<b>http-match</b>	Response string expected from the server if the protocol is HTTP.
<b>interval</b>	Status check interval, or the time between attempting to connect to the server, in seconds (1 - 3600, default = 5).
<b>packet-size</b>	Packet size of a TWAMP test session (64 - 1024).
<b>threshold-alert-jitter</b>	Alert threshold for jitter (ms, default = 0), range [0-4294967295].
<b>threshold-alert-latency</b>	Alert threshold for latency, in milliseconds (0 - 4294967295, default = 0).
<b>threshold-alert-packetloss</b>	Alert threshold for packet loss, in percent (0 - 100, default = 0).
<b>threshold-warning-jitter</b>	Warning threshold for jitter, in milliseconds (0 - 4294967295, default = 0).
<b>threshold-warning-latency</b>	Warning threshold for latency, in milliseconds (0 - 4294967295, default = 0).
<b>threshold-warning-packetloss</b>	Warning threshold for packet loss, in percent (0 - 100, default = 0).

## 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. Ensure that you are in the correct ADOM and that central SD-WAN management is enabled.
2. Go to *Device Manager > SD-WAN > SD-WAN Template*.
3. Click *Create New* in the content pane toolbar, or right-click and select *Create New*. The *Create New* page opens.

4. In the SD-WAN Rules toolbar, click *Create New*. The *Create New SD-WAN Rule* dialog-box opens.

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

<b>Name</b>	Enter the name of the rule.
<b>Source</b>	
<b>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>Internet Service</b>	Select a service or services from the drop-down 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 drop-down 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 drop-down 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 drop-down 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 drop-down 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 drop-down list. This option is only available when <i>Destination</i> is <i>Internet Service</i> .
<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. This option is only available the protocol is set to <i>Specify</i> .
<b>Outgoing Interface</b>	Select <i>Best Quality</i> or <i>Minimum Quality (SLA)</i> .
<b>Interface Members</b>	Select interface members.
<b>Status Check</b>	This option is only available when the outgoing interface is <i>Best Quality</i> .
<b>Require SLA Target</b>	This option is only available when the outgoing interface is <i>Minimum Quality (SLA)</i> .
<b>Advanced Options</b>	
<b>addr-mode</b>	Address mode (IPv4 or IPv6).
<b>bandwidth-weight</b>	Coefficient of reciprocal of available bidirectional bandwidth in the formula of custom-profile-1, range [0-10000000].
<b>dscp-forward</b>	Enable/disable forward traffic DSCP tag.
<b>dscp-forward-tag</b>	Forward traffic DSCP tag.
<b>dscp-reverse</b>	Enable/disable reverse traffic DSCP tag.
<b>dscp-reverse-tag</b>	verse traffic DSCP tag.
<b>dst-negate</b>	Enable/disable negation of destination address match.
<b>dst6</b>	Destination IPv6 address name.
<b>input-device</b>	Source interface name.
<b>internet-service-ctrl</b>	Control-based Internet Service ID list.
<b>internet-service-ctrl-group</b>	Control-based Internet Service ID, range [0-4294967295].
<b>internet-service-custom-group</b>	Custom Internet Service group list.
<b>internet-service-group</b>	Internet Service group list.
<b>jitter-weight</b>	Coefficient of jitter in the formula of custom-profile-1, range [0-10000000].
<b>latency-weight</b>	Coefficient of latency in the formula of custom-profile-1, range[0-10000000].
<b>link-cost-threshold</b>	Percentage threshold change of link cost values that will result in policy route regeneration (0 - 10000000, default = 10).
<b>packet-loss-weight</b>	Coefficient of packet-loss in the formula of custom-profile-1, range[0-10000000].
<b>route-tag</b>	IPv4 route map route-tag, range [0-4294967295].

<b>src-negate</b>	Enable/disable negation of source address match.
<b>src6</b>	Source IPv6 address name.
<b>status</b>	Enable/disable SD-WAN service.

## Health-Check Servers

Configure health-check servers for the FortiGate unit to verify that real servers are able respond to network connection attempts. If a real server responds to connection attempts, the load balancer continues to send sessions to it. If a real server stops responding to connection attempts, the load balancer assumes that the server is down and does not send sessions to it. The health-check servers configuration determines how the load balancer tests the real servers. You can use a single health-check servers for multiple load balancing configurations.

### To add a health-check server:

1. Ensure that you are in the correct ADOM and that central SD-WAN management is enabled.
2. Go to *Device Manager > SD-WAN > Health-Check Servers*.
3. Click *Create New* in the content pane toolbar. The *Create New WAN Detect Server* page opens.

4. Enter the following information, then click *OK* to add the server:

<b>Name</b>	Enter the name of the WAN detect server.
<b>Description</b>	Enter a description of the server.
<b>Detect Server</b>	Enter the IP address of the WAN interface that you want to monitor. Click the plus icon to add more interfaces.
<b>Per-Device Mapping</b>	Enable per-device mapping. See <a href="#">Per-device mapping on page 139</a> .

### To edit a health-check server:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN > Health-Check Servers*.
3. Select the server from the list and click *Edit* in the toolbar, or right-click the server then select *Edit*. The *Edit WAN Detect Server* page opens.
4. Edit the server as required, then click *OK* to apply your changes.

**To delete a health-check server or servers:**

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN > Health-Check Servers*.
3. Select the server or servers from the list and click *Delete* in the toolbar, or right-click the server then select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the server or servers.

**Per-device mapping**

Adding a Health-Check Server makes it the default server for all VDOMs on the FortiGate device. With per-device mapping, you can add a different Health-Check Server for each VDOM on the FortiGate device.

**To add health-check per-device mapping:**

1. Ensure that you are in the correct ADOM and that central SD-WAN management is enabled.
2. Go to *Device Manager > SD-WAN > Health-Check Servers*.
3. Click *Create New* in the content pane toolbar. The *Create New WAN Detect Server* page opens.
4. Enable *Per-Device Mapping*.
5. Click *Create New* in the per-device mapping toolbar.

Create New Health-Check Server

Mapped Device: Click to select

Detect Server	Seq#	IP
	1	IP

OK Cancel

6. Select a *Mapped Device* from the drop-down list.
7. Enter the *Detect Server* IP address, and add additional detect servers as needed.
8. Click *OK*.

**To edit health-check per-device mapping:**

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN > Health-Check Servers*.
3. Click *Create New* in the content pane toolbar, or right-click and select *Create New*. The *Create New WAN Detect Server* page opens.
4. Select a per device mapping then click *Edit* in the per-device mapping toolbar.
5. Edit the settings as required, then click *OK*.

**To delete health-check per-device mappings:**

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN > Health-Check Servers*.
3. Click *Create New* in the content pane toolbar, or right-click and select *Create New*. The *Create New WAN Detect Server* page opens.

4. Select one or more per device mapping, then click *Delete* in the per-device mapping toolbar.
5. Click *OK* in the confirmation dialog box to delete the mapping or mappings.

## Assigned devices

Assign a FortiGate device to an SD-WAN template. 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 a FortiGate device to the SD-WAN template:

1. Ensure that you are in the correct ADOM and that central SD-WAN management is enabled.
2. Go to *Device Manager > SD-WAN > Assigned Devices*.
3. Click *Create New* in the content pane toolbar, or right-click and select *Create New*.  
The *Create New* page opens.

The screenshot shows the 'Create New' dialog box. It has a title bar 'Create New'. Below it are two dropdown menus: 'FortiGate' and 'WAN Template'. Under these is a section titled 'Interface Mapping' which contains a table with three columns: 'ID', 'SD-WAN Member', and 'Mapped Interface'. At the bottom of the dialog are two buttons: 'OK' (blue) and 'Cancel' (orange).

4. Select a *FortiGate* and *WAN Template* from the drop-down lists.  
The *Interface Mapping* table will be populated with the interface members that are in the selected template.
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 > SD-WAN > Assigned Devices*.
3. Select the assigned device from the list, and click *Edit* in the toolbar, or right-click the device and select *Edit*.  
The *Edit* page opens.
4. Edit the FortiGate and WAN template as required, and click *OK* to apply your changes.

### To delete an assigned device or devices:

1. If using ADOMs, ensure that you are in the correct ADOM..
2. Go to *Device Manager > SD-WAN > Assigned Devices*.
3. Select the assigned device or devices from the list and click *Delete* in the toolbar, or right-click the device and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the assigned device or devices.

## Monitor SD-WAN

After adding the Interface Members, Health-Check Servers, creating SD-WAN templates, and assigning devices to the SD-WAN template, go to *SD-WAN > Monitor* to monitor the FortiGate devices.

The FortiGate devices can be monitored from two views, *Map View* and *Table View*.



## Map View

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

1. Click *Map View* to view the SD-WAN link on Google Maps.
2. Hover over the SD-WAN icon. The following information is shown:

#### <Name of the FortiGate device> (<Model>)

<b>Interface</b>	Interface members.
<b>Performance SLA</b>	Shows whether the interface is meeting the performance SLA criteria.
<b>Jitter (ms)</b>	Actual value of Jitter.
<b>Latency (ms)</b>	Actual value of Latency.
<b>Packet Loss (ms)</b>	Actual value of Packet loss.
<b>Bandwidth (TX/RX)</b>	Bandwidth of data transmitted and received.
<b>Volume (TX/RX)</b>	Volume of data transmitted and received.
<b>Session</b>	Number of active sessions.



Select *Show Unhealthy Devices only* to show only the devices that do not meet the Performance SLA criteria.

## Table View

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

1. Click *Table View* to view the SD-WAN parameters for each device.  
The following information is shown for each device:

<b>Device</b>	Name of the device.
<b>SD-WAN</b>	Interface members.
<b>Internet Services</b>	Add or remove the <i>Internet Services</i> from the <i>Services Settings</i> drop-down. The data is shown for the selected Internet Services. The Internet Services are specified in <i>SD-WAN Rules &gt; Destination type &gt; Internet Service</i> in FortiGate.
<b>Applications</b>	Add or remove the <i>Applications</i> from the <i>Services Settings</i> drop-down. The data is shown for the selected applications. The applications are specified in <i>SD-WAN Rules &gt; Destination type &gt; Internet Service</i> in FortiGate.
<b>Upload</b>	Volume of data transmitted up stream
<b>Download</b>	Volume of data transmitted down stream.

**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*. Alternatively, 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.

## SD-WAN Monitoring History

FortiManager provides an option to collect and store SD-WAN Monitor data. Go to *SD-WAN > Monitor > Table View* to view the following drill-down data:

- Click each FortiGate device to view drill-down values for the particular device. The graphs available are Bandwidth Overview, Traffic Overview, Jitter, Latency, and Packet Loss.
- Click each application to view drill-down values for the particular application. The graphs available are Jitter, Latency, and Packet Loss.

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
end
```

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 24, 12, 6, 1, and N hours.
- SD-WAN Monitoring history is stored in FortiManager for 8 days.

## IPsec VPN Wizard

The SD-WAN Interface page in FortiManager now includes an IPsec VPN creation wizard. Administrators can configure a VPN using a wizard when configuring the SD-WAN.

### To configure the IPsec VPN in SD-WAN:

1. Go to *System Settings > All ADOMs* and edit the ADOM. Disable *SD-WAN* in Central Management. Click *OK*.
2. Go to *Device Manager > SD-WAN*. Select any device or VDOM and click *Edit*. If no device is available, click *Create New*.

3. Click *Create VPN* under *Interface Members* in the *Create New SD-WAN* or *Edit SD-WAN* page.

Device: FGVM020000155864 (root)

SD-WAN Status: ☒ ON

Interface Members

+ Create New Edit Delete Move Up Move Down

<input type="checkbox"/>	#	ID	Port	Status	Weight	Gateway	Ingress Spillover	Spillover
<input type="checkbox"/>	1	4	port2	Enable	0	11.1.1.200	0	0
<input type="checkbox"/>	2	5	port3	Enable	0	12.1.1.200	0	0

Create VPN

Performance SLA

+ Create New Edit Delete

<input type="checkbox"/>	#	Name	Detect Server	Detect Protocol	Failure Threshold	Recovery Threshold
--------------------------	---	------	---------------	-----------------	-------------------	--------------------

SD-WAN Rules

+ Create New Edit Delete Move Up Move Down

<input type="checkbox"/>	#	Name	Source	Destination	Criteria	Members
<input type="checkbox"/>	1	sd-wan	ALL	ALL	Source IP Based	ALL

Advanced Options >

OK Cancel

4. Configure the following settings and click *OK* to auto-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> )

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

The screenshot shows the 'Edit SD-WAN' configuration window in FortiManager. The 'Interface Members' table is as follows:

#	ID	Port	Status	Weight	Gateway	Ingress Spillover	Spillover
1	4	port2	Enable	0	11.1.1.200	0	0
2	5	port3	Enable	0	12.1.1.200	0	0
3	1	vpn_dc1	Enable		0.0.0.0		

Below the table is a 'Create VPN' button. The 'Performance SLA' and 'SD-WAN Rules' sections are also visible.

6. Edit the VPN in Interface Members to configure *Gateway IP*, *Estimated Upstream Bandwidth (Kbps)*, and *Estimated Downstream Bandwidth (Kbps)*.

## Configure BGP Neighbor

Create SD-WAN rules to include Border Gateway Protocol (BGP) neighbors that are added in FortiGate devices.

### To configure BGP Neighbor:

1. Go to *Device Manager* > [FortiGate] > Router > BGP.
2. Under *Neighbors*, click *Create New*.
3. In the *Create New Neighbor* screen, specify the *IP* and *Remote AS*. Click *OK*. Repeat this step to add multiple neighbors.
4. Go to *System Settings* > All ADOMs.
5. Double-click [ADOM\_Name].
6. In *Central Management*, clear the *SD-WAN* check box. Click *OK*.
7. Go to *Device Manager* > Device & Groups.
8. Click the FortiGate device to view the device database.
9. Go to *Device Manager* > SD-WAN.
10. Click *Create New*.
11. In the *Create New SD-WAN* screen, select the FortiGate from the *Device* drop-down. The BGP Neighbors added in the FortiGate (Device Manager) automatically appear under *Neighbor*.

**Create New SD-WAN**

Device: FGVMO0TM19002130 (root)

**Detect Servers**

#	Name	Detect Server	Detect Protocol	Failure Threshold	Recovery Threshold
1	Default_AWS	aws.amazon.com	HTTP	5	10
2	Default_FortiGuard	fortiguard.com	HTTP	5	10
3	Default_Gmail	gmail.com	Ping	5	10
4	Default_Google Search	www.google.com	HTTP	5	10
5	Default_Office_365	www.office.com	HTTP	5	10

**Neighbors**

#	IP	Role	Member	Health Check	SLA
1	10.21.2.201	primary	@port1	Default_AWS	
2	10.21.2.202	standalone	@port1	Default_Gmail	1

**SD-WAN Rules**

#	Name	Source	Destination	Criteria	Members
1	sd-wan	ALL	ALL	Source IP Based	ALL

**Advanced Options**

fail-alert-interfaces: port1 (1 Entry Selected)

fail-detect: disable

neighbor-hold-boot-time: 500

neighbor-hold-down: disable

neighbor-hold-down-time: 0

Buttons: OK, Cancel

12. Toggle the SD-WAN Status to *ON*.

13. Configure the following *Advanced Options*:

<b>fail-alert-interfaces</b>	Select the port from the drop-down.
<b>fail-detect</b>	Select <i>enable</i> or <i>disable</i> .
<b>neighbor-hold-boot-time</b>	Specify in <i>seconds</i> .
<b>neighbor-hold-down</b>	Select <i>enable</i> or <i>disable</i> .
<b>neighbor-hold-down-time</b>	Specify in <i>seconds</i> .

14. Click *OK*.



The BGP Neighbor feature is only available for Per-Device Management. This feature is not available in Central Management and SD-WAN templates.

## FortiExtender

FortiExtender is centrally managed from the *Device Manager* pane. When a FortiGate in the ADOM has managed FortiExtender devices, they are listed in an *All FortiExtender* group.

To view managed FortiExtender devices, go to *Device Manager > Extender*.

The following information is displayed:

<b>Device Name</b>	The name of the FortiGate device that is managing the FortiExtender.
<b>Serial Number</b>	The serial number of the FortiExtender.
<b>Priority</b>	The FortiExtender priority, either <i>Primary</i> or <i>Secondary</i> .
<b>Model</b>	The FortiExtender model.
<b>Management Status</b>	The FortiExtender management status, either <i>Authorized</i> or <i>Deauthorized</i> .
<b>Status</b>	The FortiExtender status, either <i>Up</i> or <i>Down</i> .
<b>Network</b>	The FortiExtender network status and carrier name.
<b>Current Usage</b>	The current data usage.
<b>Last Month Usage</b>	The data usage for the last month.
<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>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>Set Primary</b>	Select a FortiExtender in the list, right-click, and select <i>Set Primary</i> in the menu to set the unit as the primary device.
<b>Status</b>	Select a FortiExtender in the list, right-click, and select <i>Status</i> in the menu to view status information including system status, modem status, and data usage.

#### To edit a FortiExtender:

1. Go to *Device Manager > Extender*.
2. Select a FortiExtender and click *Edit* in the toolbar, or right-click the FortiExtender device, and select *Edit*. The *Edit*

*FortiExtender* page opens.

3. Configure the following settings, then click *OK* to save the setting:

<b>Modem Settings</b>	Configure the dial mode, redial limit, and quota limit.
<b>PPP Authentication</b>	Configure the user name, password, and authentication protocol.
<b>General</b>	Configure the usage cycle reset day, AT dial script, modem password, and enable/disable allowing network initiated updates to modem setting.
<b>GSM / LTE</b>	Configure the access point name (APN), SIM PIN, and LTE multiple mode.
<b>CDMA</b>	Configure the NAI, AAA shared secret, HA shared secret, primary HA, secondary HA, AAA SPI, and HA SPI.

## 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-vX-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

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 148](#).
6. Ensure that the VM is authorized for central management by FortiManager. See [Adding devices on page 35](#).
7. Authorize the metered VMs in FortiManager. See [Authorizing metered VMs on page 149](#).



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 [Adding devices on page 35](#).

#### To authorize metered FortiOS VMs:

1. Ensure that the VM is authorized for central management by FortiManager. See [Adding devices on page 35](#).
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 43](#).

#### To authorize metered FortiWeb VMs:

1. Ensure that the FortiWeb VM is authorized for central management by FortiManager. See [Adding devices on page 35](#).

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 496](#) 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>OK: 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>• <i>OK</i>: All monitored voltages are within acceptable ranges.</li> <li>• <i>Below lower critical</i>: 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.

# Firewall 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 513](#).

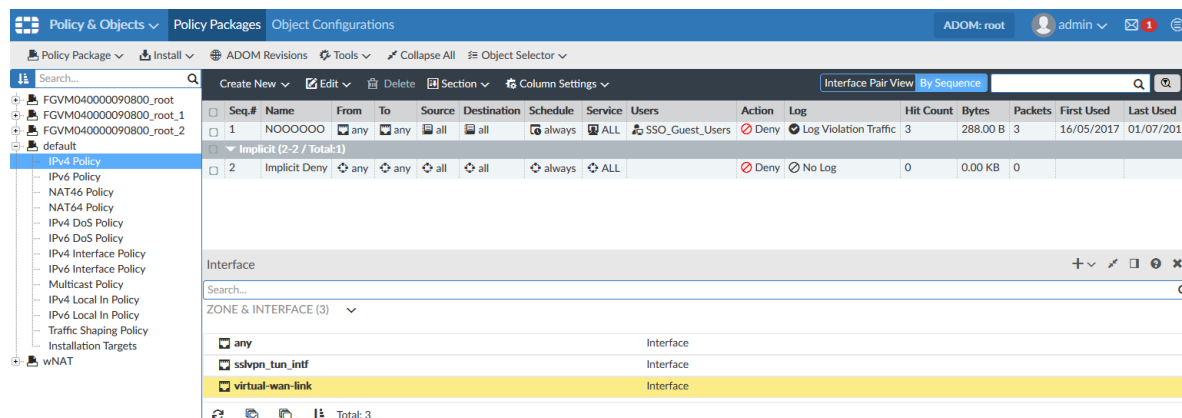


If *Display Policy & Objects in Dual Pane* is enabled, the *Policy Packages* and *Object Configurations* tabs will be shown on the same pane, with *Object Configurations* on the lower half of the screen. See [Display options on page 160](#).



If workspace is enabled, the ADOM must be locked before changes can be made. See [Locking an ADOM on page 463](#).

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 419](#).



The following tabs are available on the *Policy & Objects* pane by default:

**Policy Packages** Click to display the *Policy Packages* pane.

**Object Configurations** Click to display the *Object Configurations* pane.

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 Wizard</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>Display Options</i> , <i>Find Unused Objects</i> , or <i>Find Duplicate Objects</i> .
<b>Collapse/Expand All</b>	Collapse or expand all the categories in the policy list.
<b>Object Selector</b>	Open the object selector pane on the bottom or right side of the content pane. This option is not available when dual pane is enabled.
<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>Display Options</i> , <i>Find Unused Objects</i> , or <i>Find Duplicate Objects</i> .

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 explicitly assigned to specific 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.

Display options for policies and objects can be configured in *Policy & Objects > Tools > Display Options*.



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.

---

## 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.

## Display options

The policy and objects that are displayed on the *Policy & Objects* pane can be customized, and the *Policy Packages* and *Object Configurations* tabs can be combined onto a single pane.

To adjust the policies and objects that are displayed, go to *Tools > Display Options*.

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 display 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 convert the module to 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 be a single pane that includes both tabs.

Policy & Objects													
ADOM: root													
Policy Package													
Create New													
View Mode													
Seq.#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profiles	Log	NAT	Hit Count
1	NOOOOOO	virtual-wan-link	any	all	all	always	ALL	SSO_Guest_Users	Deny		Log Violation Traffic		0
2	Test any interface	virtual-wan-link	any	all	all	always	ALL		Accept	default	Log All Sessions	Disabled	0
Implicit (3-3 / Total:1)													
3	Implicit Deny	any	any	all	all	always	ALL		Deny		No Log		0
Zone/Interface													
Create New													
More													
Interface													
Default Mapping													
Per-Device Mapping													
Description													
Interface (5)													
	any												> 0 out of 2
	sslvpn_tun_intf												> 0 out of 2
	virtual-wan-link												> 0 out of 2
	Linkob1												> 0 out of 2
	Meshow1												> 0 out of 2
Zone (6)													
	vpnmgr_test_hub2spoke												> 0 out of 2
	vpnmgr_test_mesh												> 0 out of 2
	vpnmgr_test_spoke2hub												> 0 out of 2
	vpnmgr_test_hub2spoke												> 0 out of 2
	vpnmgr_test_mesh												> 0 out of 2
	vpnmgr_test_spoke2hub												> 0 out of 2

## 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 > Display Options* 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 > Policy Packages*.

3. From the *Policy Package* menu select *New Package* or right-click in the tree menu and select *New Package*. 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 > Policy Packages*.
3. From the *Policy Package* menu select *New Package* or right-click in the tree menu and select *New Package*. The *Create New Policy Package* window opens.

Create New Policy Package

The screenshot shows the 'Create New Policy Package' dialog box. It has the following fields and controls:

- Name:** A text input field.
- In Folder:** A text input field with a folder icon button to its right.
- Central NAT:** A checkbox.
- NGFW Mode:** Two buttons: 'Profile-based' (selected) and 'Policy-based'.
- Consolidated Firewall Mode:** A button labeled 'OFF'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

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>In Folder</b>	Optionally, click the <i>In Folder</i> button to select a folder for the 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> .



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 > Policy Packages*.
3. From the *Policy Package* menu select *New Folder* or right-click in the tree menu 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.

### 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, then click *OK* to apply 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 Package* from the toolbar, or right-click on the package or folder and select *Clone Package* 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 specific ADOMs.

Only ADOMs of the same version as the global database or the next higher major release are presented as options for assignment.



The central NAT setting must be consistent between the global policy package and the ADOM to which you are assigning the policy package. Because central NAT is not supported at the global level, you should disable central NAT in all ADOMs to which you are assigning a global policy package.

The inspection-mode setting must also match in the global policy package and the ADOM to which you are assigning the policy package.

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.

Add ADOM Edit ADOM Delete Select All Assign Selected			
ADOMs	Status	ADOM Policy Packages	Action
Gat	Pending changes	All Policy Packages	[Assign]
Got	Up to date	All Policy Packages	[Unassign]
root	Pending changes	All Policy Packages	[Assign]

4. If required, select *Add ADOM* to add an ADOM to the assignment list.
5. In the assignment list, select an ADOM, or click *Select All*.
6. Click *Assign Selected* from the content toolbar. The *Assign* dialog box opens.
7. Select whether you want to assign only used objects or all objects, and if policies will be automatically installed to ADOM devices.
8. Click *OK* to assign the policy package to the selected ADOM or ADOMs.





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 178](#).

---

### 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. Select a policy package and from the *Install* menu or right-click menu 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 [Using the Install Wizard to install policy packages and device settings on page 66](#). For more information on editing the installation targets, see [Policy package installation targets on page 168](#).

## 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.

3. In the toolbar, select *Install > Re-install Policy*.

After data is gathered, the *Re-install Policy Package* window is displayed.

Re-install Policy Package

✓ Policy Consistency Check

Device	Policy Package	Policy Check	Validation
FortiGate-VM64			
root	FortiGate-VM64_root	Policy Check Succeed	OK Install Preview Policy Package Diff
CDOMm	FortiGate-VM64_CDOMm	Policy Check Succeed	OK Install Preview Policy Package Diff

Next > Cancel

4. (Optional) View policy consistency check results (see [Perform a policy consistency check on page 170](#)).

- 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

any -> port8									
#	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		

any -> any									
#	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)

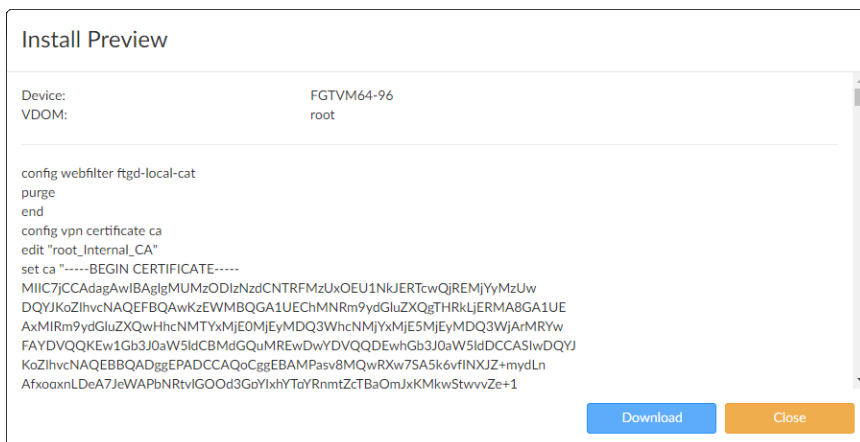
Close

- b. Click the *Close* button to close the page and return to the wizard.

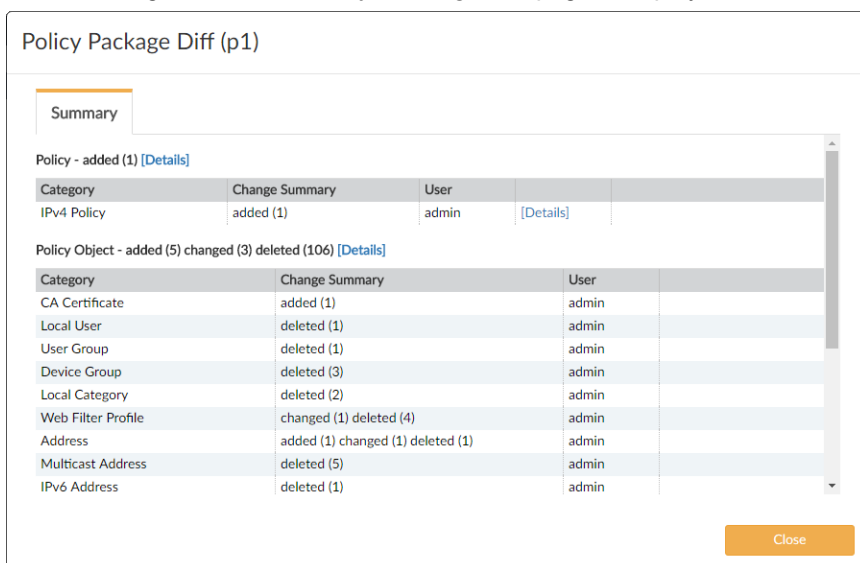
5. (Optional) View a preview of the installation.

- a. Click the *Install Preview* button.

After data is gathered, the *Install Preview* page is displayed.



- b. Click the *Download* button to download a text file of the preview information.
  - c. Click the *Close* button to close the page and return to the wizard.
6. (Optional) View the difference between the current policy package and the policy in the device.
- a. Click the *Policy Package Diff* button.
- After data is gathered, the *Policy Package Diff* page is displayed.



- b. Click the *Details* links to view details about the changes to the policy, specific policies, and policy objects.
  - c. Click *Close* to close the page and return to the wizard.
7. Click *Next*.
8. Click *Install*.
- The policy package is reinstalled to the target devices.

## Schedule a policy package install

In FortiManager you can create, edit, and delete install schedules for policy packages. The *Schedule Install* menu option has been added to the *Install* wizard when selecting to install policy package and device settings. You can specify the date and time to install the latest policy package changes.

Select the clock icon which is displayed beside the policy package name to create an install schedule. Select this icon to

edit or cancel the schedule. When a scheduled install has been configured and is active, hover the mouse over the icon to view the scheduled date and time.

#### To schedule the install of a policy package to a target device:

1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects > Policy Packages*.
3. From the *Install* menu, select *Install Wizard*. The *Install Wizard* opens.
4. Select *Schedule Install*, and set the install schedule date and time.
5. Select *Next*. In the device selection screen, edit the installation targets as required.
6. Select *Next*. In the interface validation screen, edit the interface mapping as required.
7. Select *Schedule Install* to continue to the policy and object validation screen. In the ready to install screen you can copy the log and download the preview text file.

#### To edit or cancel an install schedule:

1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects > Policy Packages*.
3. Click the clock icon next to the policy package name in the *Policy Package* tree. The *Edit Install Schedule* dialog box is displayed.
4. Select *Cancel Schedule* to cancel the install schedule, then select *OK* in the confirmation dialog box to cancel the schedule. Otherwise, edit the install schedule as required and select *OK* to save your changes.

## Export a policy package

You can export a policy package as a Microsoft Excel or CSV file.

#### To export a policy package:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. Select a policy package or folder then, from the *Policy Package* menu, select *Export to Excel* or *Export to CSV*. The policy package is downloaded to your management computer.

## Policy package installation targets

The *Installation Targets* pane allows you to view the installation target, config status, policy package status, and schedule install status, as well as edit installation targets for policy package installs.

To view installation targets, go to *Policy & Objects > Policy Packages*. In the tree menu for the policy package, select *Installation Targets*.

The following information is displayed:

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

**Policy Package Status** See the table below for policy package status details.

The following table identifies the different available config statuses.

Config Status	Icon	Description
<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>

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.

Policy Package Status	Icon	Description
<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 fsso-polling* is *Modified*. This is because FortiManager sends all fsso-polling objects to all devices that are using agentless FSSO.

The following options are available:

<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 460](#)).

### 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.

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

any -> port8

#	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	

any -> any

#	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

### 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 [Adding FortiAnalyzer devices on page 49](#).

### 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



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.

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 display options. See [Display options on page 160](#) for more information.

Seq.#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profiles	Log
1	test	any	port9	all	all	always	ALL		Deny		Lo
2	badbuild	port8	port9	auth.gfx.ms	all	always	ALL		Deny		Lo
3	shadowing	port7	port6	auth.gfx.ms	google-play	always	ALL_ICMP ALL_TCP ALL_ICMP6 ALL_UDP FTP		Accept	certificate-inspection	Lo
4	matching	any	port5	all	all	always	ALL		Deny		Lo
5	malade	any	port3	all	all	always	ALL		Accept	certificate-inspection	Lo
▼ Implicit (6-6 / Total:1)											
6	Implicit Deny	any	any	all	all	always	ALL		Deny		N

You can configure the following policies for a policy package:

IP policies	Central SNAT	Multicast policy
Virtual wire pair policy	Central DNAT	Local in policies
NAT policies	DoS policies	Traffic shaping policy
Proxy policy	Interface policies	

Various options are also available from column specific right-click menus, for more information see [Column options on page 174](#).



If workspace or workflow is enabled, the ADOM must be locked before changes can be made. See [Locking an ADOM on page 463](#).



Not all policy and object options are enabled by default. To configure the enabled options, from the *Tools* menu, select *Display Options*.



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.

The default *Simple Search* will highlight text that matches the string entered in the search field.

### To add column filters:

1. Select *Column Filter* from the search field dropdown menu.
2. Do either of the following:
  - a. Right-click on a specific value in any column and select *Add Filter* (equals or not equals) from the menu.  
or
  - a. Click *Add Filter*, then select a column heading from the list.
  - b. Select from the available values in the provided list. Select *Or* to add multiple values, or select *Not* to remove any policies that contain the selected value from the results.  
Multiple filters can be added.
3. Click *Go* to filter the list.

## Policy hit count

You can use FortiManager to view FortiGate policy hit counters. You must enable policy hit counts before you can view the information.

In FortiManager, the policy hit counts are aggregated across all managed FortiGate units for the policy.

The hit count is collected from managed FortiGate units every 300 seconds (5 minutes) by default. You can configure the frequency by using the `config system global` command with the `hitcount_interval` variable and the `hitcount_concurrent` variable. For more information, see the *FortiManager CLI Reference* available on the [Fortinet Document Library](#).

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

The hit count information is excluded from the FortiManager event log, but it's included in the debug log for troubleshooting purposes.

#### To enable policy hits:

1. Go to *System Settings > Advanced Settings*.
2. Beside *Policy Hit Count*, select *Enable*.

#### To view policy hit counts:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Package*.
3. In the tree menu for a policy package, select a policy. The content pane for the policy is displayed.
4. View the *Hit Count*, *Bytes*, *Packets*, *First Used*, and *Last Used* columns.
5. Hover the mouse over the cells in the columns to view the *Session Count*, *Session First Used*, and *Session Last Used* fields of information.

The *Session Count* field reports the total number of completed sessions from the FortiGate. The *Session Count* field excludes incomplete sessions, such as sessions where TCP three-way handshakes are incomplete, UDP sessions are pending replies, and SCTP sessions that have not reached an established state.

The *Session First Used* and *Session Last Used* fields are session aware and triggered when return traffic is generated. They indicate when a policy rule is being used not just hit.

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

Generic policies can be inserted above or below the currently selected policy. From the *Create New* menu, select *Insert Above* or *Insert Below*. By default, new policies will be inserted at the bottom of the list.

## Editing policies

Policies can be edited in a variety of different way, often directly on the policy list.

### 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 177](#) and [Drag and drop objects on page 178](#).

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.

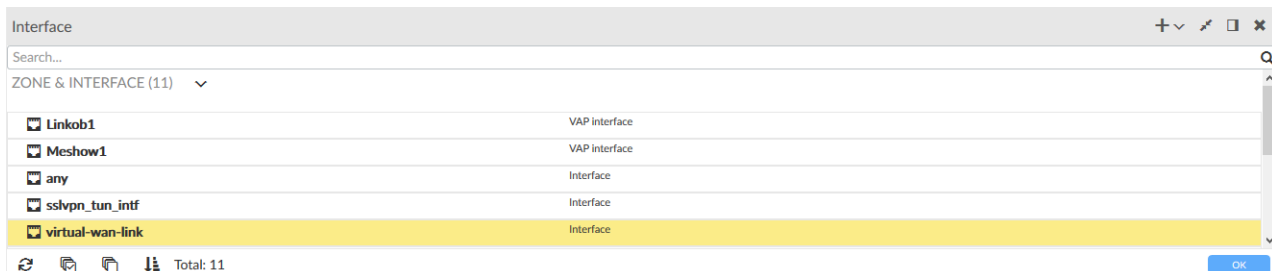
## Object selector

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 [Display options on page 160](#).

---



<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 216</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 224](#) and [Clone an object on page 226](#).

## 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. The *Install On* column is not shown by default.
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 168](#)), 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.

- Click *OK* to close the *Object Selector* frame.

#### To edit a policy service with dual pane enabled:

- Ensure you are in the correct ADOM.
- Go to *Policy & Objects*.
- In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
- In the object pane, go to *Firewall Objects > Services*. The services objects are displayed in the content pane.
- 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:

- Go to *Policy & Objects > Object Configuration*.
- In the tree menu, go to *Firewall Objects > Services*. The services objects are displayed in the content pane.
- Select a services object, and click *Edit*. The *Edit Service* dialog box is displayed.
- 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>	Configure ICMP error message verification. <ul style="list-style-type: none"> <li><b>disable</b>: The FortiGate unit does not validate ICMP error messages.</li> <li><b>strict</b>: If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B)   TCP(C,D) header, then if FortiManager</li> </ul>



can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. If it is enabled, the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the `anti-replay` option checks packets.

- default: Use the global setting defined in `system global`.

This field is available when *Protocol* is *TCP/UDP/SCTP*.

This field is not available if *explicit-proxy* is enabled.

<b>Color</b>	Click the icon to select a custom, colored icon to display next to the service name.
<b>session-ttl</b>	Type the default session timeout in seconds. 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. This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i> .
<b>tcp-halfclose-timer</b>	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> . This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i> .
<b>tcp-halfopen-timer</b>	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> . This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i> .
<b>tcp-timewait-timer</b>	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." Reducing the length of the TIME-WAIT state means the FortiGate unit can close terminated sessions faster, which means that more new sessions can be opened before the session limit is reached. The valid range is 0 to 300 seconds. A value of 0 sets the TCP TIME-WAIT to 0 seconds. Type 0 to use the global setting defined in <code>system global</code> . This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i> .
<b>udp-idle-timer</b>	Type the number of seconds before an idle UDP connection times out. The valid range is from 1 to 86400 seconds. Type 0 to use the global setting defined in <code>system global</code> . This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i> .

**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.

---

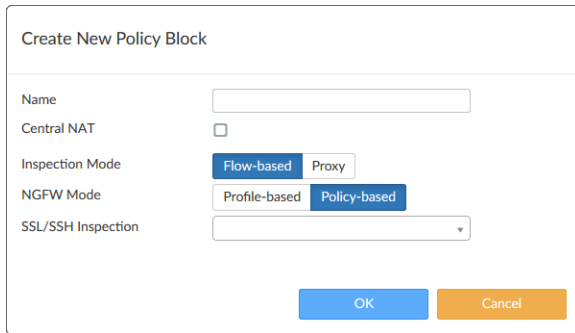
## Creating Policy Blocks

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.

**To create a new Policy Block:**

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects*.

- Right-click *Policy Blocks* and click *New*. The *Create New Policy Block* window opens.



The 'Create New Policy Block' dialog box contains the following fields and controls:

- Name:** A text input field.
- Central NAT:** A checkbox.
- Inspection Mode:** Two buttons: 'Flow-based' (selected) and 'Proxy'.
- NGFW Mode:** Two buttons: 'Profile-based' and 'Policy-based' (selected).
- SSL/SSH Inspection:** A dropdown menu.
- Buttons:** 'OK' (blue) and 'Cancel' (orange) at the bottom right.

- 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>	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> .

## 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:

- Ensure that you are in the correct ADOM.
- Go to *Policy & Objects*.
- Go to *Policy Blocks > [Policy\_Block\_Name] > IPv4 or IPv6*.
- Click *Create New*. See [IP policies on page 184](#) on how to create an IPv4 or IPv6 policy.

### To copy a policy into a Policy Block:

- Ensure that you are in the correct ADOM.
- Go to *Policy & Objects*.
- Click *[Policy\_Package\_Name]*. For example, click *Default*.
- Click *IPv4 or IPv6*.
- Select one or more policies.
- Right-click and select *Copy*.
- Go to *Policy Blocks > [Policy\_Block\_Name] > IPv4 or IPv6*.
- 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.

## Appending a Policy Block to a Policy Package

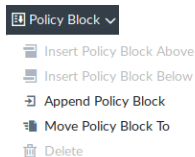
Once a Policy Block is created, it can be appended to a Policy Package. After appending the Policy Block to a Policy Package, assigning installation targets and installing the Policy Package to the installation targets, all the policies in the Policy Block are installed to the target.



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

OK Cancel



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.

## IP policies

The section describes how to create new IPv4 and IPv6 policies.

IPv6 security policies are created both for an IPv6 network and a transitional network. A transitional network is a network that is transitioning over to IPv6, but must still have access to the Internet or must connect over an IPv4 network. IPv6 policies allow for this specific type of traffic to travel between the IPv6 and IPv4 networks.



On the *Policy & Objects* tab, from the *Tools* menu, select *Display Options*. In the *Policy* section, select the *IPv6 Policy* checkbox to display this option.

### To create a new IPv4 or IPv6 policy:

1. 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 Policy* or *IPv6 Policy*. If you are in the Global Database ADOM, select *IPv4 Header Policy*, *IPv4 Footer Policy*, *IPv6 Header Policy*, or *IPv6 Footer Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list, but above the implicit policy. The *Create New Policy* pane opens.

Create New IPv4 Policy

Name	<input type="text"/>
Incoming Interface	<input type="text" value="any"/>
Outgoing Interface	<input type="text" value="any"/>
Source Internet Service	<input type="button" value="OFF"/>
Source Address	<input type="text" value="all"/>
Source User	<input type="text"/>
Source User Group	<input type="text"/>
Source Device	<input type="text"/>
Destination Internet Service	<input type="button" value="OFF"/>
Destination Address	<input type="text" value="all"/>
Service	<input type="text" value="ALL"/>
Schedule	<input type="text" value="always"/>
Action	<input type="button" value="Deny"/> <input type="button" value="Accept"/> <input type="button" value="IPSEC"/>
Log Traffic	<input checked="" type="checkbox"/> Log Violation Traffic
	<input type="checkbox"/> Generate Logs when Session Starts
Comments	<input type="text"/>

Meta Fields >  
Advanced Options >

5. Enter the following information:

<b>Name</b>	Enter a unique name for the policy. Each policy must have a unique name.
<b>Incoming Interface</b>	<p>Click the field then select interfaces from the <i>Object Selector</i> frame, or drag and drop the address from the object pane.</p> <p>Select the remove icon to remove values.</p> <p>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 216</a> for more information.</p>

<b>Outgoing Interface</b>	Select outgoing interfaces.
<b>Source Internet Service</b>	Turn source internet service on or off, then select services. This option is only available for IPv4 policies.
<b>Source Address</b>	Select source addresses. 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>Source Device</b>	Select source devices, device groups, and device categories. 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. This option is only available for IPv4 policies.
<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>Service</b>	Select services and service groups. This option is only available when <i>Destination Internet Service</i> is off.
<b>Schedule</b>	Select schedules, one time or recurring, and schedule groups.
<b>Application</b>	Select applications. This option is only available when <i>NGFW Mode</i> is <i>Policy-based</i> for the policy package; see <a href="#">Create new policy packages on page 161</a> .
<b>URL Category</b>	Select URL categories. This option is only available when <i>NGFW Mode</i> is <i>Policy-based</i> for the policy package; see <a href="#">Create new policy packages on page 161</a> .
<b>Action</b>	Select an action for the policy to take: <i>ACCEPT</i> , <i>DENY</i> , or <i>IPSEC</i> . <i>IPSEC</i> is not available for IPv6 policies.
<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> or <i>IPSEC</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>
<b>Generate Logs when Session Starts</b>	Select to generate logs when the session starts.
<b>Capture Packets</b>	Select to capture packets. This option is available when the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> , and <i>Log Security Events</i> or <i>Log All Sessions</i> is selected
<b>NAT</b>	Select to enable NAT.

	<p>If enabled, select <i>Use Destination Interface Address</i> or <i>Dynamic IP Pool</i>, and select <i>Fixed Port</i> if required. If <i>Dynamic IP Pool</i> is selected, select pools. This option is available when the <i>Action</i> is <i>ACCEPT</i>, and when <i>NGFW Mode</i> is <i>Profile-based</i>; see <a href="#">Create new policy packages on page 161</a>.</p>
<b>VPN Tunnel</b>	<p>Select a VPN tunnel dynamic object from the dropdown list. Select to allow traffic to be initiated from the remote site.</p> <p>This option is available when the <i>Action</i> is <i>IPSEC</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> or <i>IPSEC</i>.</p> <p>The following profile types can be added:</p> <ul style="list-style-type: none"> <li>• AntiVirus Profile</li> <li>• Web Filter Profile</li> <li>• Application Control</li> <li>• IPS Profile</li> <li>• Email Filter Profile</li> <li>• DLP Sensor</li> <li>• VoIP Profile</li> <li>• ICAP Profile</li> <li>• SSL/SSH Inspection</li> <li>• Web Application Firewall</li> <li>• DNS Filter</li> <li>• Proxy Options</li> <li>• Profile Group (available when <i>Use Security Profile Group</i> is selected)</li> </ul>
<b>Shared Shaper</b>	<p>Select traffic shapers.</p> <p>This option is available if the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i>.</p>
<b>Reverse Shaper</b>	<p>Select traffic shapers.</p> <p>This option is available if the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> and at least one forward traffic shaper is selected.</p>
<b>Per-IP Shaper</b>	<p>Select per IP traffic shapers.</p> <p>This option is available if the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i>.</p>
<b>Comments</b>	<p>Add a description of the policy, such as its purpose, or the changes that have been made to it.</p>
<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 <i>FortiOS CLI Reference</i>.</p>

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.

### Advanced options

Option	Description	Default
auth-cert	HTTPS server certificate for policy authentication (IPv4 only).	none

Option	Description	Default
<b>auth-path</b>	Enable or disable authentication-based routing (IPv4 only).	disable
<b>auth-redirect-addr</b>	HTTP-to-HTTPS redirect address for firewall authentication (IPv4 only).	none
<b>auto-asic-offload</b>	Enable or disable policy traffic ASIC offloading.	enable
<b>block-notification</b>	Enable or disable block notification (IPv4 only).	disable
<b>captive-portal-exempt</b>	Enable or disable exemption of captive portal (IPv4 only).	disable
<b>custom-log-fields</b>	Select the custom log fields from the dropdown list.	none
<b>delay-tcp-npu-session</b>	Enable or disable TCP NPU session delay in order to guarantee packet order of 3-way handshake (IPv4 only).	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.	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>	Type 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>	Type 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>disclaimer</b>	Enable or disable user authentication disclaimer (IPv4 only).	disable
<b>dscp-match</b>	Enable or disable DSCP check.	disable
<b>dscp-negate</b>	Enable or disable negate DSCP match.	disable
<b>dscp-value</b>	Enter the DSCP value.	000000
<b>dsri</b>	Enable or disable DSRI (Disable Server Response Inspection) to ignore HTTP server responses.	disable
<b>dstaddr-negate</b>	Enable or disable negated destination address match.	disable
<b>firewall-session-dirty</b>	Packet session management, either <i>check-all</i> or <i>check-new</i> .	check-all
<b>fsso-agent-for-ntlm</b>	Select the FSSO agent for NTLM from the dropdown list (IPv4 only).	none
<b>identity-based-route</b>	Name of identity-based routing rule (IPv4 only).	none
<b>internet-service-negate</b>	When enabled, Internet services match against any Internet service EXCEPT the selected Internet service (IPv4 only).	disable
<b>internet-service-src-negate</b>	Enables or disables the use of Internet Services in source for this policy. If enabled, <code>internet-service-src</code> specifies what the service must NOT be (IPv4 only).	disable
<b>learning-mode</b>	Enable or disable learning mode for policy (IPv4 only).	disable



Option	Description	Default
<b>match-vip</b>	Enable or disable match DNATed packet (IPv4 only).	disable
<b>natinbound</b>	Enable or disable policy NAT inbound.	disable
<b>natip</b>	Type the NAT IP address in the text field (IPv4 only).	0.0.0.0
<b>natoutbound</b>	Enable or disable policy NAT outbound.	disable
<b>np-acceleration</b>	Enable or disable UTM Network Processor acceleration.	enable
<b>ntlm</b>	Enable or disable NTLM authentication (IPv4 only).	disable
<b>ntlm-enabled-browsers</b>	Type a value in the text field (IPv4 only).	none
<b>ntlm-guest</b>	Enable or disable NTLM guest (IPv4 only).	disable
<b>outbound</b>	Enable or disable policy outbound.	disable
<b>permit-any-host</b>	Enable to accept UDP packets from any host (IPv4 only).	disable
<b>permit-stun-host</b>	Enable to accept UDP packets from any STUN host (IPv4 only).	disable
<b>radius-mac-auth-bypass</b>	Enable MAC authentication bypass. The bypassed MAC address must be received from RADIUS server.	disable
<b>redirect-url</b>	URL redirection after disclaimer/authentication (IPv4 only).	none
<b>replacemsg-override-group</b>	Specify authentication replacement message override group.	none
<b>rtp-addr</b>	Select the RTP address from the dropdown list (IPv4 only).	none
<b>rtp-nat</b>	Enable to apply source NAT to RTP packets received by the firewall policy (IPv4 only).	disable
<b>scan-botnet-connections</b>	Enable or disable scanning of connections to Botnet servers (IPv4 only).	disable
<b>schedule-timeout</b>	Enable to force session to end when policy schedule end time is reached (IPv4 only).	disable
<b>send-deny-packet</b>	Enable to send a packet in reply to denied TCP, UDP or ICMP traffic.	disable
<b>service-negate</b>	Enable or disable negated service match.	disable
<b>session-ttl</b>	Type a value for the session time-to-live (TTL) from 300 to 604800, or type 0 for no limitation.	0
<b>srcaddr-negate</b>	Enable or disable negated source address match.	disable
<b>ssh-filter-profile</b>	Select an SSH filter profile from the dropdown list.	None
<b>ssl-mirror</b>	Enable or disable SSL mirror.	disable
<b>ssl-mirror-intf</b>	Mirror interface name.	none
<b>tcp-mss-receiver</b>	Type a value for the receiver's TCP MSS.	0
<b>tcp-mss-sender</b>	Type a value for the sender's TCP MSS.	0

Option	Description	Default
<b>tcp-session-without-syn</b>	Enable or disable creation of TCP session without SYN flag. <ul style="list-style-type: none"> <li>all - Enable TCP session without SYN.</li> <li>data-only - Enable TCP session data only.</li> <li>disable - Disable TCP session without SYN.</li> </ul>	disable
<b>timeout-send-rst</b>	Enable sending a TCP reset when an application session times out.	disable
<b>vlan-cos-fwd</b>	Type the VLAN forward direction user priority.	255
<b>vlan-cos-rev</b>	Type the VLAN reverse direction user priority.	255
<b>vlan-filter</b>	Set VLAN filters.	
<b>wanopt</b>	Enable or disable WAN optimization (IPv4 only).	disable
<b>wanopt-detection</b>	WAN optimization auto-detection mode (IPv4 only).	active
<b>wanopt-passive-opt</b>	WAN optimization passive mode options. This option decides what IP address will be used to connect server (IPv4 only).	default
<b>wanopt-peer</b>	WAN optimization peer (IPv4 only).	none
<b>wanopt-profile</b>	WAN optimization profile (IPv4 only).	none
<b>wccp</b>	Enable or disable Web Cache Communication Protocol (WCCP) (IPv4 only).	disable
<b>webcache</b>	Enable or disable web cache (IPv4 only).	disable
<b>webcache-https</b>	Enable or disable web cache for HTTPS (IPv4 only).	disable
<b>wssso</b>	Enable or disable WiFi Single Sign-On (IPv4 only).	enable

## Create New Firewall Policy

The 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's processed, if it's processed, and even whether or not it's allowed to pass through the FortiGate.



The Firewall Policy is visible only if the *NGFW Mode* is selected as *Policy-based* in the policy package.

### To create a new Firewall Policy:

1. 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*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list, but above the implicit policy. The *Create New Firewall Policy* pane opens.

Create New Firewall Policy

Name	<input type="text"/>
Incoming Interface	<input type="button" value="⊕"/> any <input type="button" value="✕"/>
Outgoing Interface	<input type="button" value="⊕"/> any <input type="button" value="✕"/>
Source Internet Service	<input type="button" value="OFF"/>
IPv4 Source Address	<input type="button" value="⊕"/> all <input type="button" value="✕"/>
IPv6 Source Address	<input type="button" value="⊕"/> all <input type="button" value="✕"/>
Source User	<input type="button" value="⊕"/>
Source User Group	<input type="button" value="⊕"/>
Destination Internet Service	<input type="button" value="OFF"/>
IPv4 Destination Address	<input type="button" value="⊕"/> all <input type="button" value="✕"/>
IPv6 Destination Address	<input type="button" value="⊕"/> all <input type="button" value="✕"/>
Service	<input type="button" value="⊕"/> ALL <input type="button" value="✕"/>

Firewall / Network Options

**i** Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.

Security Profiles

SSL/SSH Inspection  no-inspection

Comments

0/1023

Advanced Options >

OK Cancel

5. Enter the following information:

<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 from the <i>Object Selector</i> frame, or drag and drop the address from the object pane. Select the remove icon to remove values. 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 216</a> for more information.
<b>Outgoing Interface</b>	Select outgoing interfaces.
<b>Source Internet Service</b>	Turn source internet service on or off, then select services. This option is only available for IPv4 policies.
<b>IPv4 Source Address</b>	Select the IPv4 source addresses. This option is only available when <i>Source Internet Service</i> is off.
<b>IPv6 Source Address</b>	Select the IPv6 source addresses. 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>Source Device</b>	Select source devices, device groups, and device categories. 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. This option is only available for IPv4 policies.
<b>IPv4 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>IPv6 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>Service</b>	Select services and service groups. This option is only available when <i>Destination Internet Service</i> is off.
<b>Firewall / Network Options</b>	Central NAT is enabled by default so NAT settings from matching Central SNAT policies will be applied.
<b>Security Profiles</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> 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 216</a> for more information.
<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 <i>FortiOS CLI Reference</i> .

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.

### Advanced options

Option	Description	Default
<b>auto-asic-offload</b>	Enable or disable policy traffic ASIC offloading.	enable
<b>cifs-profile</b>	Enable or disable authentication-based routing (IPv4 only).	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.	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

Option	Description	Default
<b>diffservcode-forward</b>	Type 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>	Type 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>http-policy-redirect</b>	Select the custom log fields from the dropdown list.	none
<b>inspection-mode</b>	Enable or disable TCP NPU session delay in order to guarantee packet order of 3-way handshake (IPv4 only).	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>session-ttl</b>	Type a value for the session time-to-live (TTL) from 300 to 604800, or type 0 for no limitation.	0
<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>	Type a value for the receiver's TCP MSS.	0
<b>tcp-mss-sender</b>	Type a value for the sender's TCP MSS.	0
<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>	WAN optimization passive mode options. This option decides what IP address will be used to connect server (IPv4 only).	default
<b>wanopt-peer</b>	WAN optimization peer (IPv4 only).	none
<b>wanopt-profile</b>	WAN optimization profile (IPv4 only).	none
<b>webcache</b>	Enable or disable web cache (IPv4 only).	disable
<b>webcache-https</b>	Select the FSSO agent for NTLM from the drop-down list (IPv4 only).	none
<b>webproxy-forward-server</b>	Name of identity-based routing rule (IPv4 only).	none
<b>webproxy-profile</b>	When enabled, Internet services match against any Internet service except the selected Internet service (IPv4 only).	disable

## Create New Security Policy

The section describes how to create a new Security Policy. A Security Policy consists of rules related to proxy, antivirus, IPS, Email, and DLP sensor.



The Security Policy is visible only if the *NGFW Mode* is selected as *Policy-based* in the policy package.



On the *Policy & Objects* tab, from the *Tools* menu, select *Display Options*. In the *Policy* section, select the *Security Policy* check box to display this option.

**To create a new Security Policy:**

1. 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*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list, but above the implicit policy. The *Create New Security Policy* pane opens.

Create New Security Policy

Name	<input type="text"/>
Incoming Interface	<input type="text" value="any"/>
Outgoing Interface	<input type="text" value="any"/>
Source	<input type="text" value="all"/>
Destination	<input type="text" value="all"/>
Service	<input type="button" value="App Default"/> <input type="button" value="Specify"/>
Schedule	<input type="text" value="always"/>
Application	<input type="text" value="+"/>
URL Category	<input type="text" value="+"/>
Action	<input checked="" type="radio"/> Accept <input type="radio"/> Deny
Log Violation Traffic	<input checked="" type="checkbox"/>
Comments	<input type="text" value=""/> 0/1023

Advanced Options >

5. Enter the following information:

<b>Name</b>	Enter a unique name for the policy. Each policy must have a unique name.
<b>Incoming Interface</b>	<p>Click the field then select interfaces from the <i>Object Selector</i> frame, or drag and drop the address from the object pane.</p> <p>Select the remove icon to remove values.</p> <p>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 216</a> for more information.</p>
<b>Outgoing Interface</b>	Select outgoing interfaces.

<b>Source</b>	Select source addresses.
<b>Destination Address</b>	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
<b>Service</b>	Select the service. Select <i>App Default</i> or <i>Specify</i> . Select the Service from the <i>Objector Selector</i> if <i>Specify</i> is selected.
<b>Schedule</b>	Select schedules, one time or recurring, and schedule groups.
<b>Application</b>	Select applications.
<b>URL Category</b>	Select URL categories.
<b>Action</b>	Select an action for the policy to take: <i>ACCEPT</i> or <i>DENY</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> or <i>IPSEC</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>
<b>Generate Logs when Session Starts</b>	Select to generate logs when the session starts.
<b>Security Profiles</b>	Select to add security profiles or profile groups. This option is available when the <i>Action</i> is <i>ACCEPT</i> . The following profile types can be added: <ul style="list-style-type: none"> <li>• Proxy Options</li> <li>• AntiVirus Profile</li> <li>• IPS Profile</li> <li>• Email Filter Profile</li> <li>• DLP Sensor</li> </ul>
<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 <i>FortiOS CLI Reference</i> .

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.

### Advanced options

Option	Description	Default
<b>application-list</b>	Select from the drop-down list.	None
<b>cifs-profile</b>	Enable or disable authentication-based routing (IPv4 only).	None
<b>dnsfilter-profile</b>	Select from the drop-down list.	None
<b>icap-profile</b>	Select from the drop-down list.	None

Option	Description	Default
<b>custom-log-fields</b>	Select the custom log fields from the drop-down list.	none
<b>internet-service-negate</b>	When enabled, Internet services match against any Internet service except the selected Internet service (IPv4 only).	disable
<b>internet-service-src-negate</b>	Enables or disables the use of Internet Services in source for this policy. If enabled, <code>internet-service-src</code> specifies what the service must NOT be (IPv4 only).	disable
<b>service-negate</b>	Enable or disable negated service match.	disable
<b>ssh-filter-profile</b>	Select an SSH filter profile from the drop-down list.	None
<b>ssl-ssh-profile</b>	Select an SSL SSH profile from the drop-down list.	no-inspection
<b>utm-status</b>	Enable or disable the Unified Threat Management status.	disable
<b>voip-profile</b>	Select the VOIP profile.	None
<b>webfilter-profile</b>	Select the web filter profile.	None

## Virtual wire pair policy

The 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 252](#).



You must display the option before you can set it. On the *Policy & Objects* pane, from the *Tools* menu, select *Display Options*, and then select the *IPv4 Virtual Wire Pair Policy* checkbox to display this option.

### To create a 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 *IPv4 Virtual Wire Pair Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Policy* pane opens.
5. Enter the following information, then click *OK* to create the policy:

<b>Name</b>	Enter a unique name for the policy. Each policy must have a unique name.
<b>Virtual Wire Pair Interface</b>	Select an interface. You can type the name of the interface to search for it in the list.
<b>Virtual Wire Pair</b>	Select an arrow to indicate the flow of traffic between ports.



<b>Source Internet Service</b>	Turn source internet service on or off, then select services from the <i>Object Selector</i> frame, or drag and drop them from the object pane.
<b>Source Address</b>	Select source addresses. 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>Source Device</b>	Select source devices, device groups, and device categories. This option is only available when <i>Source Internet Service</i> is off.
<b>Internet Service</b>	Toggle <i>ON</i> to enable Internet service. Toggle <i>OFF</i> to disable Internet service.
<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 available when <i>Destination Internet Service</i> is <i>OFF</i> .
<b>Service</b>	Select services and service groups. This option is available when <i>Destination Internet Service</i> is <i>OFF</i> .
<b>Schedule</b>	Select schedules, one time or recurring, and schedule groups.
<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>
<b>Generate Logs when Session Starts</b>	Select to generate logs when the session starts.
<b>Capture Packets</b>	Select to capture packets. This option is available when the <i>Action</i> is <i>ACCEPT</i> and <i>Log Security Events</i> or <i>Log All Sessions</i> is selected
<b>Security Profiles</b>	Select to add security profiles or profile groups. This option is available when <i>Action</i> is <i>Accept</i> . The following profile types can be added: <ul style="list-style-type: none"> <li>• Antivirus Profile</li> <li>• Web Filter Profile</li> <li>• Application Control</li> <li>• IPS Profile</li> <li>• Email Filter Profile</li> <li>• DLP Sensor</li> <li>• VoIP Profile</li> </ul>

	<ul style="list-style-type: none"> <li>• ICAP Profile</li> <li>• SSL/SSH Inspection</li> <li>• Web Application Firewall</li> <li>• DNS Filter</li> <li>• Proxy Options</li> <li>• Profile Group (available when <i>Use Security Profile Group</i> is selected)</li> </ul>
<b>Shared Shaper</b>	Select traffic shapers. This option is available if the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> .
<b>Reverse Shaper</b>	Select traffic shapers. This option is available if the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> and at least one forward traffic shaper is selected.
<b>Per-IP Shaper</b>	Select per IP traffic shapers. This option is available if the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> .
<b>Description</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 on page 187</a> . For more information on advanced option, see the <i>FortiOS CLI Reference</i> .

## NAT policies

Use NAT46 policies for IPv6 environments where you want to expose certain services to the public IPv4 Internet. You will need to configure a virtual IP to permit the access.

Use NAT64 policies to perform network address translation (NAT) between an internal IPv6 network and an external IPv4 network.

The NAT46 Policy tab allows you to create, edit, delete, and clone NAT46 policies. The NAT64 Policy tab allows you to create, edit, delete, and clone NAT64 policies.



On the *Policy & Objects* pane, from the *Tools* menu, select *Display Options*, and then select the *NAT46 Policy* and *NAT64 Policy* checkboxes to display these options.

### To create a NAT46 or NAT64 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 *NAT46 Policy* or *NAT64 Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be

added to the bottom of the list. The *Create New Policy* pane opens.

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

<b>Incoming Interface</b>	Click the field then select interfaces from the <i>Object Selector</i> frame, or drag and drop the address from the object pane.
<b>Outgoing Interface</b>	Select outgoing interfaces.
<b>Source Address</b>	Select source addresses.
<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 schedules, one time or recurring, and schedule groups.
<b>Action</b>	Select an action for the policy to take: <i>ACCEPT</i> , or <i>DENY</i> .
<b>Log Allowed Traffic</b>	Select to log allowed traffic.
<b>NAT</b>	NAT is enabled by default for this policy type when the <i>Action</i> is <i>ACCEPT</i> . <i>Use Destination Interface Address</i> is selected by default. Select <i>Fixed Port</i> if required.
<b>Dynamic IP Pool</b>	Select to use dynamic IP pools. Select <i>Fixed Port</i> if required, and the <i>IP Pool Name</i> from the available IP pool objects. This option is only available for NAT64 policies.
<b>Traffic Shaping</b>	Select traffic shapers. This option is available if the <i>Action</i> is <i>ACCEPT</i> .
<b>Reverse Traffic Shaping</b>	Select traffic shapers. This option is available if at least one forward traffic shaper is selected.
<b>Per-IP Traffic Shaping</b>	Select per IP traffic shapers. This option is available if the <i>Action</i> is <i>ACCEPT</i> .
<b>Description</b>	Add a description of the policy, such as its purpose, or the changes that have been made to it.
<b>Advanced Options</b>	
<b>ippool</b>	Enable IP pools. This option is only available for NAT46 policies.
<b>permit-any-host</b>	Enable to accept UDP packets from any host.
<b>poolname</b>	Select a firewall IP pool from the dropdown list (default = None). This option is only available for NAT46 policies.
<b>tcp-mss-receiver</b>	Enter a value for the receiver's TCP MSS.
<b>tcp-mss-sender</b>	Enter a value for the sender's TCP MSS.

## Proxy policy

The section describes how to create web, FTP, and WAN Opt proxy policies.



On the *Policy & Objects* pane, go to *Tools > Display Options*, and then select the *Explicit Proxy Policy* checkbox in the *Policy* section to display this option.

### 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 *Explicit Proxy Policy*.
3. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Policy* pane opens.

**Create New Proxy Policy**

Explicit Proxy Type	<input checked="" type="radio"/> Explicit Web <input type="radio"/> Transparent Web <input type="radio"/> FTP <input type="radio"/> WAN Optimize
Outgoing Interface	<input type="text" value="any"/>
Source	<input type="text"/>
Destination	<input type="text"/>
Service	<input type="text"/>
Schedule	<input checked="" type="radio"/> always
Action	<input checked="" type="radio"/> Accept <input type="radio"/> Deny <input type="radio"/> Redirect
Log Traffic	<input type="radio"/> No Log <input type="radio"/> Log Security Events <input checked="" type="radio"/> Log All Sessions <input checked="" type="checkbox"/> Generate Logs when Session Starts
<b>Disclaimer Options</b>	
Display Disclaimer	<input checked="" type="radio"/> Disable <input type="radio"/> By Domain <input type="radio"/> By Policy <input type="radio"/> By User
<b>Security Profiles</b>	
Web Proxy Forwarding Server	<input type="text"/>
Comments	<input type="text"/>
Advanced Options >	

OK Cancel

4. Enter the following information, then click *OK* to create the policy:

<b>Explicit Proxy Type</b>	Select the explicit proxy type: <i>Explicit Web</i> , <i>Transparent Web</i> , <i>FTP</i> , or <i>WAN Optimize</i> .
<b>Incoming Interface</b>	Select incoming interfaces from the <i>Object Selector</i> frame, or drag and drop the address from the object pane. This option is only available when the proxy type is set to <i>Transparent Web</i> .
<b>Outgoing Interface</b>	Select outgoing interfaces.
<b>Source</b>	Select source addresses.
<b>Destination</b>	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
<b>Service</b>	Select services and service groups from the object selector pane.
<b>Schedule</b>	Select schedules, one time or recurring, and schedule groups.

<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 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> When <i>Log All Sessions</i> is selected, you can select to generate logs when the session starts. 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>Disclaimer Options</b>	Set the Display Disclaimer: <i>Disable</i> , <i>By Domain</i> , <i>By Policy</i> , or <i>By User</i> . Optionally, select a custom message in the <i>Customize Messages</i> field if not disabled. These options are available when the <i>Action</i> is <i>Accept</i> .
<b>Security Profiles</b>	Select to add security profiles or profile groups. 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>• 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>• DLP Sensor</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> <li>• Proxy Options</li> <li>• SSL/SSH Inspection</li> <li>• Profile Group (available when <i>Use Security Profile Group</i> is selected)</li> </ul> This option is available when the <i>Action</i> is <i>Accept</i> .
<b>Redirect URL</b>	Enter the redirect URL. This option is only available when the <i>Action</i> is <i>Redirect</i> .
<b>Web Proxy Forwarding Server</b>	Select a web proxy forwarding server from the dropdown list. 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 <i>FortiOS CLI Reference</i> .

**Advanced options**

Option	Description	Default
<b>dstaddr-negate</b>	Enable or disable negated destination address match.	disable
<b>global-label</b>	Enter a global label.	-
<b>http-tunnel-auth</b>	Enable or disable HTTP tunnel authentication	disable
<b>internet-service-negate</b>	Enable or disable negated internet service.	disable
<b>label</b>	Enter a label	-
<b>poolname</b>	Select a firewall IP pool from the dropdown list.	None
<b>scan-botnet-connections</b>	Enable or disable scanning of connections to Botnet servers.	disable
<b>service-negate</b>	Enable or disable negated service match.	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 negated source address match.	disable
<b>ssh-filter-profile</b>	Name of an existing SSH filter profile.	None
<b>transparent</b>	Use IP address of client to connect to server.	disable
<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 from the dropdown list.	None

**Central SNAT**

The Central SNAT (Secure NAT) table 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.

The Central SNAT table allows you to create, edit, delete, and clone central SNAT entries.



Central SNAT does not support *Section View*.



*Central NAT* must be enabled, or *NGFW Mode* must be set to *Policy-based*, when creating or editing the policy package for this option to be available in the tree menu. See [Create new policy packages on page 161](#).

#### To create a new central SNAT entry:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package, click *Central SNAT*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Central SNAT* pane opens.
5. Configure the following settings, then click *OK* to create the policy:

<b>Incoming Interface</b>	Click the field then select interfaces from the <i>Object Selector</i> frame, or drag and drop the address from the object pane. Select the remove icon to remove values.
<b>Outgoing Interface</b>	Select outgoing interfaces.
<b>Source Address</b>	Select source addresses.
<b>Destination Address</b>	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
<b>NAT</b>	Select to enable NAT.
<b>IP Pool Configuration</b>	Select either <i>Use Outgoing Interface Address</i> , or <i>Use Dynamic IP Pool</i> . If using a dynamic IP pool, select the pool from the <i>Object Selector</i> frame. This option is only available when <i>NAT</i> is selected.
<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>Comments</b>	Add a description of the policy, such as its purpose, or the changes that have been made to it.
<b>Meta Fields</b>	If configured, enter values for the required meta fields, and optionally for the optional fields. See <a href="#">Meta Fields on page 490</a> .
<b>Advanced Options</b>	Enable or disable <i>nat</i> .

## Central DNAT

The FortiGate unit checks the NAT table and determines if the destination IP address for incoming traffic must be changed using DNAT. 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. DNAT means the actual address of the internal network is hidden from the Internet. This step determines whether a route to the destination address actually exists.

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 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 selected *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 from 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.



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 161](#).

#### To create a new central DNAT entry:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package, click *Central DNAT*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Virtual IP* pane opens.
5. Configure the following settings, then click *OK* to create the VIP:

<b>Name</b>	Enter a unique name for the DNAT.
<b>Comments</b>	Optionally, enter comments about the DNAT, such as its purpose, or the changes that have been made to it.
<b>Color</b>	Select a color.
<b>Interface</b>	Select an interface.
<b>Network Type</b>	Select the network type: <i>Static NAT</i> , <i>DNS Translation</i> , or <i>FQDN</i> .
<b>External IP Address/Range</b>	Enter the start and end external IP addresses in the fields. If there is only one address, enter it in both fields. This option is not available when the network type is <i>FQDN</i> .
<b>Mapped IP Address/Range</b>	Enter the mapped IP address. This option is not available when the network type is <i>FQDN</i> .
<b>External IP Address</b>	Enter the external IP address. This option is only available when the network type is <i>FQDN</i> .
<b>Mapped Address</b>	Select the mapped address.



	This option is only available when the network type is <i>FQDN</i> .
<b>Source Interface Filter</b>	Select a source interface filter.
<b>Optional Filters</b>	Enable or disable optional filters.
<b>Source Address</b>	Add source IP, range, or subnet filters. Multiple filters can be added using the <i>Add</i> icon.
<b>Services</b>	Enable and add services.
<b>Port Forwarding</b>	Enable or disable port forwarding.
<b>Protocol</b>	Select the protocol: <i>TCP</i> , <i>UDP</i> , <i>SCTP</i> , or <i>ICMP</i> .
<b>External Service Port</b>	Enter the external service port. This option is not available when <i>Protocol</i> is <i>ICMP</i> .
<b>Map to Port</b>	Enter the map to port. This option is not available when <i>Protocol</i> is <i>ICMP</i> .
<b>Enable ARP Reply</b>	Select to enable ARP reply.
<b>Add To Groups</b>	Optionally, select groups to add the virtual IP to from the list.
<b>Advanced Options</b>	Configure advanced options, see <a href="#">Advanced options</a> . For more information on advanced option, see the <i>FortiOS CLI Reference</i> .
<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.

#### To import VIPs from the Virtual IP object table:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package, click *Central DNAT*.
4. Click *Import* in the toolbar. The *Import* dialog box will open.
5. Select the VIP object or objects that need to be imported. If necessary, use the search box to locate specific objects.
6. Click *OK* to import the VIPs to the *Central DNAT* table.

#### Advanced options

Option	Description	Default
<b>dns-mapping-ttl</b>	Enter time-to-live for DNS response, from 0 to 604 800. 0 means use the DNS server's response time.	0
<b>extaddr</b>	Select an address.	None

Option	Description	Default
<b>gratuitous-arp-interval</b>	Set the time interval between sending of gratuitous ARP packets by a virtual IP. 0 disables this feature.	0
<b>http-cookie-age</b>	Set how long the browser caches cooking, from 0 to 525600 seconds.	60
<b>http-cookie-domain</b>	Enter the domain name to restrict the cookie to.	none
<b>http-cookie-domain-from-host</b>	If enabled, when the unit adds a SetCookie to the HTTP(S) response, the Domain attribute in the SetCookie is set to the value of the Host: header, if there is one.	disable
<b>http-cookie-generation</b>	The exact value of the generation is not important, only that it is different from any generation that has already been used.	0
<b>http-cookie-path</b>	Limit the cookies to a particular path.	none
<b>http-cookie-share</b>	Configure HTTP cookie persistence to control the sharing of cookies across more than one virtual server. The default setting means that any cookie generated by one virtual server can be used by another virtual server in the same virtual domain. Disable to make sure that a cookie generated for a virtual server cannot be used by other virtual servers.	same-ip
<b>http-ip-header-name</b>	Enter a name for the custom HTTP header that the original client IP address is added to.	none
<b>https-cookie-secure</b>	Enable or disable using secure cookies for HTTPS sessions.	disable
<b>id</b>	Custom defined ID.	0
<b>max-embryonic-connections</b>	The maximum number of partially established SSL or HTTP connections, from 0 to 100000.	1000
<b>nat-source-vip</b>	Enable to prevent unintended servers from using a virtual IP. Disable to use the actual IP address of the server (or the destination interface if using NAT) as the source address of connections from the server that pass through the device.	disable
<b>outlook-web-access</b>	If enabled, the <code>Front-End-Https: on</code> header is inserted into the HTTP headers, and added to all HTTP requests.	disable
<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-client-fallback</b>	Enable to prevent Downgrade Attacks on client connections.	enable
<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> </ul>	allow

Option	Description	Default
	<ul style="list-style-type: none"> <li>secure: require secure renegotiation.</li> </ul>	
<b>ssl-client-session-state-max</b>	The maximum number of SSL session states to keep for the segment of the SSL connection between the client and the unit, from 0 to 100000.	1000
<b>ssl-client-session-state-timeout</b>	The number of minutes to keep the SSL session states for the segment of the SSL connection between the client and the unit, from 1 to 14400.	30
<b>ssl-client-session-state-type</b>	<p>The method to use to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate.</p> <ul style="list-style-type: none"> <li>both: 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>count: expire SSL session states when <code>ssl-client-session-state-max</code> is exceeded.</li> <li>disable: expire all SSL session states.</li> <li>time: expire SSL session states when <code>ssl-client-session-state-timeout</code> is exceeded.</li> </ul>	both
<b>ssl-dh-bits</b>	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 response.	disable
<b>ssl-hpkp-age</b>	The number of seconds that the client should honor the HPKP setting (60 - 157680000).	5184000
<b>ssl-hpkp-backup</b>	Certificate to generate the backup HPKP pin from (size = 35, datasource(s) = vpn.certificate.local.name, vpn.certificate.ca.name).	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>	Certificate to generate the primary HPKP pin from (size = 35, datasource(s) = vpn.certificate.local.name, vpn.certificate.ca.name).	None
<b>ssl-hpkp-report-uri</b>	URL to report HPKP violations to (size = 255).	
<b>ssl-hsts</b>	Enable or disable including HSTS header in response.	disable
<b>ssl-hsts-age</b>	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 Location HTTP header field.	disable
<b>ssl-http-match-host</b>	Enable to apply Location conversion to the reply's HTTP header only if the host name portion of Location matches the request's Host field or, if the Host field does not exist, the host name portion of the request's URI.	disable

Option	Description	Default
<b>ssl-max-version</b>	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> , or <code>tls-1.2</code> .	<code>tls-1.2</code>
<b>ssl-min-version</b>	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> , or <code>tls-1.2</code> .	<code>tls-1.0</code>
<b>ssl-pfs</b>	Select the handling of Perfect Forward Secrecy (PFS) by controlling the cipher suites that can be selected. <ul style="list-style-type: none"> <li><code>allow</code>: allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.</li> <li><code>deny</code>: allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.</li> <li><code>require</code>: allow only Diffie-Hellman cipher-suites, so PFS is applied.</li> </ul>	<code>allow</code>
<b>ssl-send-empty-frags</b>	Enable to precede the record with empty fragments to thwart attacks on CBC IV.  Disable this option if SSL acceleration will be used with an old or buggy SSL implementation which cannot properly handle empty fragments.	<code>enable</code>
<b>ssl-server-algorithm</b>	Set the permitted encryption algorithms for SSL server 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>	<code>client</code>
<b>ssl-server-max-version</b>	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> , or <code>tls-1.2</code> .	<code>client</code>
<b>ssl-server-min-version</b>	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> , or <code>tls-1.2</code> .	<code>client</code>
<b>ssl-server-session-state-max</b>	The maximum number of SSL session states to keep for the segment of the SSL connection between the client and the unit, from 0 to 100000.	<code>100</code>
<b>ssl-server-session-state-timeout</b>	The number of minutes to keep the SSL session states for the segment of the SSL connection between the client and the unit, from 1 to 14400.	<code>60</code>
<b>ssl-server-session-state-type</b>	The method to use to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate. <ul style="list-style-type: none"> <li><code>both</code>: 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><code>count</code>: expire SSL session states when <code>ssl-client-session-state-max</code> is exceeded.</li> <li><code>disable</code>: expire all SSL session states.</li> <li><code>time</code>: expire SSL session states when <code>ssl-client-session-state-timeout</code> is exceeded.</li> </ul>	<code>both</code>

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

## DoS policies

The *IPv4 DoS Policy* and *IPv6 DoS Policy* panes allow you to create, edit, delete, and clone DoS policies.



On the *Policy & Objects* pane, from the *Tools* menu, select *Display Options*, and then select the *IPv4 DoS Policy* and *IPv6 DoS Policy* checkboxes to display these option.

### To create a DoS 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 *IPv4 DoS Policy* or *IPv6 DoS Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Policy* pane opens.
5. Configure the following settings, then click *OK* to create the policy:

<b>Incoming Interface</b>	Select the incoming interface from the <i>Object Selector</i> frame, or drag and drop the address from the object pane.
<b>Source Address</b>	Select the source address.
<b>Destination Address</b>	Select the destination address.
<b>Service</b>	Select the service.
<b>L3 Anomalies</b>	
<b>ip_src_session</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
<b>ip_dst_session</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
<b>L4 Anomalies</b>	
<b>tcp_syn_flood</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 2000.

<b>tcp_port_scan</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 1000.
<b>tcp_src_session</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
<b>tcp_dst_session</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
<b>udp_flood</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 2000.
<b>udp_scan</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 2000.
<b>udp_src_session</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
<b>udp_dst_session</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
<b>icmp_flood</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 250.
<b>icmp_sweep</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 100.
<b>icmp_src_session</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 300.
<b>icmp_dst_session</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 1000.
<b>sctp_flood</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 2000.
<b>sctp_scan</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 1000.

<b>sctp_src_session</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
<b>sctp_dst_session</b>	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
<b>Advanced Options</b>	Optionally, add a description of the policy, such as its purpose, or the changes that have been made to it.

## Interface policies

The *IPv4 Interface Policy* and *IPv6 Interface Policy* panes allow you to create, edit, delete, and clone interface policies.



On the *Policy & Objects* pane, from the *Tools* menu, select *Display Options*, and then select the *IPv4 Interface Policy* and *IPv6 Interface Policy* check boxes to display these options.

### To create a new interface 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 *IPv4 Interface Policy* or *IPv6 Interface Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Policy* pane opens.
5. Configure the following settings, then click *OK* to create the policy:

<b>Source</b>	
<b>Interface</b>	Select the source zone from the <i>Object Selector</i> frame, or drag and drop the address from the object pane.
<b>Address</b>	Select the source address.
<b>Destination</b>	
<b>Address</b>	Select the destination address.
<b>Service</b>	Select the service.
<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>	Select to enable antivirus and select the profile from the dropdown list.
<b>Web Filter Profile</b>	Select to enable Web Filter and select the profile from the dropdown list.
<b>Application Control</b>	Select to enable Application Control and select the profile from the dropdown list.

<b>IPS Profile</b>	Select to enable IPS and select the profile from the dropdown list.
<b>Email Filter Profile</b>	Select to enable Email Filter and select the profile from the dropdown list.
<b>DLP Sensor</b>	Select to enable DLP Sensor and select the profile from the dropdown list.
<b>Advanced Options</b>	
<b>comments</b>	Add comments about the policy.
<b>dsri</b>	Enable or disable DSRI (default = disable).
<b>scan-botnet-connections</b>	Enable or disable scanning of connections to Botnet servers (default = disable).

## Multicast policy

Multicasting consists of using a single source to send data to many receivers simultaneously, while conserving bandwidth and reducing network traffic.



On the *Policy & Objects* pane, from the *Tools* menu, select *Display Options*, and then select the *Multicast Policy* checkbox to display this option.

### To create a new multicast 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 *Multicast Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Policy* pane opens.
5. Configure the following settings, then click *OK* to create the policy:

<b>Incoming Interface</b>	Click in the field and select incoming interfaces from the multicast interface list on the <i>Object Selector</i> frame, or drag and drop the interface from the object pane.  If no multicast interfaces are configured, click the <i>Create New Object</i> button to open the <i>Create New Dynamic Multicast Interface</i> window, and then create a new multicast interface.
<b>Outgoing Interface</b>	Click in the field and select outgoing interfaces from the multicast interface list.  If no multicast interfaces are configured, one must be created.
<b>Source Address</b>	Click the field and select the source firewall addresses.
<b>Source NAT</b>	Enable source NAT.
<b>Source NAT Address</b>	Enter the source NAT IP address.



<b>Destination Interface</b>	Click the field and select the destination firewall addresses.
<b>Destination NAT</b>	Enter the destination NAT IP address.
<b>Protocol Option</b>	Select a protocol option from the dropdown list: <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>	Select to log traffic.
<b>Advanced Options</b>	Enable or disable <i>auto-asic-offload</i> (default = enable).

## Local in policies

The section describes how to create new IPv4 and IPv6 Local In policies.



On the *Policy & Objects* pane, from the *Tools* menu, select *Display Options*, and then select the *IPv4 Local In Policy* and *IPv6 Local In Policy* checkboxes to display these options.

### To create a new Local In policy:

1. 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*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Policy* pane opens.
5. Enter the following information, then click *OK* to create the policy:

<b>Interface</b>	Click the field then select an interface from the object selector frame, or drag and drop the interface from the object pane.
<b>Source Address</b>	Select source addresses.
<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 schedules, one time or recurring, and schedule groups.
<b>Action</b>	Select an action for the policy to take: <i>ACCEPT</i> or <i>DENY</i> .
<b>HA Management Interface Only</b>	Select to enable. This option is only available for IPv4 policies.

## Traffic shaping policy

The section describes how to create new traffic shaping policies.



On the *Policy & Objects* pane, from the *Tools* menu, select *Display Options*, and then select the *Traffic Shaping Policy* checkbox to display this option.

### To create a traffic shaping policy:

1. 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*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Policy* pane opens.
5. Enter the following information, then click *OK* to create the policy:

<b>IP Version</b>	Select the IP address version: <i>IPv4</i> or <i>IPv6</i> .
<b>Matching Criteria</b>	
<b>Source Internet Service</b>	Turn source internet service on or off, then select services.
<b>Source Address</b>	Select source addresses from the <i>Object Selector</i> frame, or drag and drop them from the object pane. 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>Service</b>	Select services and service groups. This option is only available when <i>Destination Internet Service</i> is off.
<b>Application Category</b>	Select application categories.
<b>Application</b>	Select applications.
<b>URL Category</b>	Select URL categories.
<b>Users</b>	Select users.
<b>User Groups</b>	Select user groups.
<b>Apply Shaper</b>	

<b>Outgoing Interface</b>	Select outgoing interfaces.
<b>Traffic Shaping</b>	Select traffic shapers.
<b>Reverse Traffic Shaping</b>	Select traffic shapers.
<b>Per-IP Traffic Shaping</b>	Select per IP traffic shapers.
<b>Advanced Options</b>	
<b>class-id</b>	Set the class ID (2 - 31, default = 0).
<b>schedule</b>	Set the schedule (default = None).

## 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 [Display options on page 160](#).

Objects and dynamic objects are managed in the *Policy & Objects > Object Configurations* pane (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 in the *Policy & Objects > Policy Packages* pane (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 178](#).



On the *Policy & Objects > Object Configuration* pane, 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 > Address*.  
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.

**Create New Address**

Address Name

Type

IP/Netmask

Interface

Static Route Configuration

Comments

Add To Groups

Meta Fields >

Advanced Options >

Per-Device Mapping



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.



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-Only Objects > ips* or *Device Manager > [FortiGate\_Name] > CLI-Only Objects > 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.

---



For objects other than the Dynamic Interface and Zone, the color coding option is available in *Advanced Options*.

---

### 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 *Zone/Interface > Interface*.  
The interface list is displayed in the content pane. The available interfaces are selectable on the content pane toolbar.
4. From the *Create New* menu, select the type of interface. In this example, *Zone* was selected. The *Create New Zone* pane opens.

5. Select or specify the values for the following fields:

- Name - specify a name for the object.
- Description - enter a brief description.
- Color - select a color for this object from the drop-down.
- Default Mapping - select the check box to configure the default mapping for this object. See [Map a dynamic ADOM object on page 220](#)
- Per-Device Mapping - switch the slider to *ON* for mapping this interface to a FortiGate device. See [Interface mapping on page 231](#)

6. Click *OK*.



If a color code is not selected while creating an object, black is assigned as the default color. The color coding for Dynamic Interface and Zone cannot be installed to the FortiGate devices and can only be viewed in FortiManager. The color coding for other objects can be installed to FortiGate devices.

## 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	

OK Cancel

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 *Zone/Interface > 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.

## 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 96](#)



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

Delete

Clone

Where Used

Grouping

Promote to Global



```
        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 > Display Options*.
4. Select *Dynamic Object* and click *OK*.

The following device objects are available:

- [Create a Local Certificate on page 222](#)
- [Create a VPN Tunnel on page 222](#)
- [Create Multicast Interface on page 223](#)



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

+ Create New

Edit

Delete

Column Settings

OK

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 ☒ ON ☐

+ Create New ☒ Edit ☐ Delete ☐ Column Settings

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 <b>ON</b> . Click <i>Create New</i> . Select the <i>Mapped Device</i> and <i>VPN Tunnel</i> . Click <b>OK</b> .

## Create Multicast Interface

Create a Multicast Interface to sync with devices using per-device mapping.

**To create a Multicast Interface:**

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
3. Go to *Dynamic Object > Multicast Interface*.
4. Click *Create New*. The *Create New Dynamic Multicast Interface* pane opens.

**Create New Dynamic Multicast Interface**

Name

Description

Default Mapping ☐ OFF ☐

Per-Device Mapping ☒ ON ☐

+ Create New ☒ Edit ☐ Delete ☐ Column Settings

Name	VDOM	Details	Type	Addressing Mode	IP/Netmask

OK Cancel

5. Select or specify the values for the following and click **OK**:

<b>Name</b>	Specify the name for the Dynamic Multicast Interface.
<b>Description</b>	Specify a description.
<b>Default Mapping</b>	Toggle Per-Device Mapping to <b>ON</b> and specify the interface for default mapping.

**Per-Device Mapping**

Toggle Per-Device Mapping to *ON*. Click *Create New*. Select the *Mapped Device* and *Interface*. Click *OK*.

## 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>Managed 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 225](#).

**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, and 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.

---

## 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:

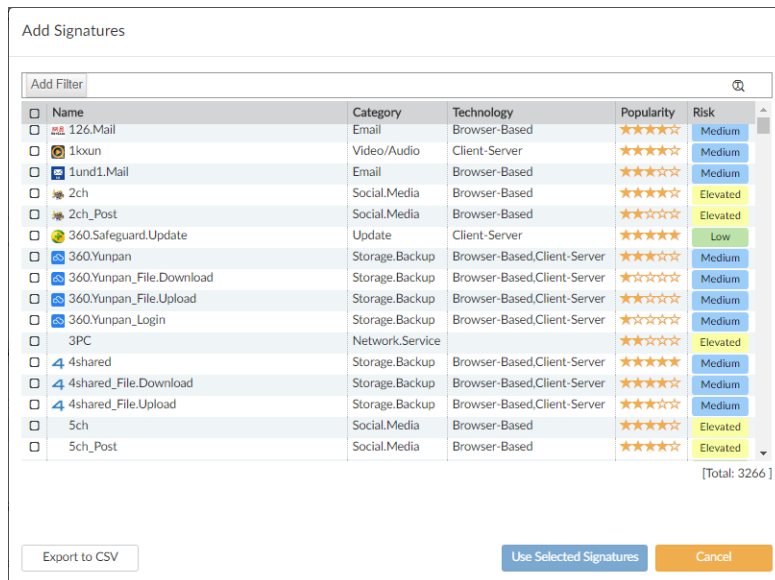
1. Go to *Policy & Objects*.
2. From the *Tools* menu, select *Find Duplicate Objects*. The *Duplicate Objects* dialog box is displayed.
3. Review the groups of duplicate objects.
4. Click *Merge* to merge a group of duplicate objects into one object.
5. When you are done, click *Close*.

## Export signatures to CSV file format

You can export Intrusion Prevention signatures (IPS) and Application Control signatures to a file CSV format.

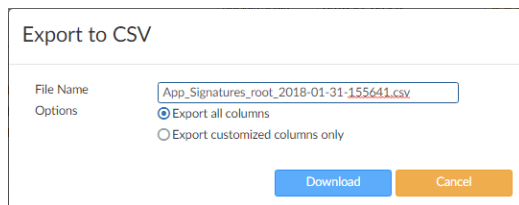
### To export signatures to CSV format:

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.



6. Click **Export to CSV**.

The **Export to CSV** dialog box is displayed.



7. (Optional) Change the file name.

8. Select whether to export all columns or only customized columns.

9. Click **Download**.

## CLI-Only objects

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 & Device > FortiTokens**.
4. Click **Create New**.
5. Type the serial number or serial numbers of the FortiToken unit or units and click **OK**. Up to ten serial numbers can be entered.
6. Go to **User & Device > 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 & Device > 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 165](#).
10. On the FortiGate, select *User > FortiToken*. Select one of the newly created FortiTokens, then select *OK* to activate the FortiToken unit.

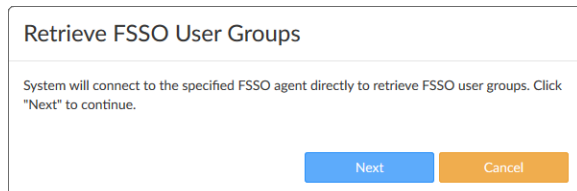
## FSSO user groups

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*. and select *User & Device > Single Sign-On*.
3. Click *Create New > Fortinet Single Sign-On Agent* from the dropdown list.
4. Enter a unique name for the agent in the *Name* field.
5. Enter the IP address or name, password, and port number of the FSSO servers in the FSSO Agent field. Add and remove servers as needed by clicking the *Add* and *Remove* icons at the end of the rows.
6. Select *From FSSO Agents* in the *Select FSSO Groups* field.
7. Click *Apply & Refresh*. The *Retrieve FSSO User Groups* dialog box will open.



8. Click *Next*. The groups are retrieved from the FSSO.
9. Click *OK*. The groups can now be used in user groups, which can then be used in policies.

### To get groups from an LDAP server:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*. and select *User & Device > Single Sign-On*.
3. Click *Create New > Fortinet Single Sign-On Agent* from the dropdown list.
4. Enter a unique name for the agent in the *Name* field.
5. Select an LDAP server from the dropdown list. LDAP Servers can be added and configured from *User & Device > LDAP Servers*.
6. Select groups from the *Groups* tab, then select *Add Selected* to add the groups.  
You can also select *Manually Specify* in the *Select LDAP Groups* field, and then manually enter the group names.
7. Select *OK*.

## 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 81](#).

1. Go to *Policy & Objects > Object Configurations*. and select *User & Device > Single Sign-On*.
2. Click *Create New > Fortinet Single Sign-On Agent* from the dropdown list. The *Create New Fortinet Single Sign-On Agent* window opens.

3. Enter a unique name for the agent in the *Name* field.
4. Enter the IP address or name, password, and port number of the FSSO servers in the FSSO Agent field. Add and remove servers as needed by clicking the *Add* and *Remove* icons at the end of the rows.
5. Select *Via FortiGate* in the *Select FSSO Groups* field.
6. Click *Apply & Refresh*. The *Retrieve FSSO User Groups* wizard will open.

7. Click *Next* to proceed with the wizard.
8. Select the device that the FSSO groups will be imported from. This device must be authorized for central management by FortiManager, its configuration must be synchronized, and it must be able to communicate with the FSSO server.
9. Click *Next*. The FSSO agent is installed on the FortiGate, the FortiGate retrieves the groups, and then the groups are imported to the FortiManager.

10. After the groups have been imported, click *Finish*. The imported groups will be listed in the *User Groups* field.

Create New Fortinet Single Sign-On Agent

Name	<input type="text" value="fssso1"/>		
FSSO Agent	IP/Name	Password	Port
	<input type="text" value="10.222.788.878"/>	<input type="password" value="••••••••"/>	<input type="text" value="8000"/> +
	<input type="text"/>	<input type="password"/>	<input type="text" value="8000"/> +
Select FSSO Groups	<input type="radio"/> From FSSO Agents <input checked="" type="radio"/> 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	<input type="text"/>		
Per-Device Mapping	<input type="button" value="OFF"/>		
Advanced Options	>		

11. Click *OK*. The groups can now be used in user groups, which can then be used in policies.



You must rerun the wizard to update the group list. It is not automatically updated.

### To get groups from AD:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*. and select *User & Device > Single Sign-On*.
3. Click *Create New > Poll Active Directory Server* from the dropdown list.
4. Configure the server name, local user, password, and polling.
5. Select an LDAP server from the dropdown list. LDAP Servers can be added and configured from *User & Device > LDAP Servers*.
6. Select groups from the *Groups* tab, then select *Add Selected* to add the groups.  
You can also select *Manually Specify* in the *Select LDAP Groups* field, and then manually enter the group names.
7. Select *OK*.

## 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 *Zone/Interface > Interface* and click *Create New > Dynamic interface*.
4. Enter a name and description for the dynamic interface.
5. Turn on *Per-Device Mapping*.
6. Click *Add*. 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. Go to *Policy & Objects > Object Configurations*.
5. Click *Create New > Zone*. Configure the settings and create a zone named *Zone\_One*. Enable Per-Device Mapping and select the *Mapped Device* and *Device Interface*.
6. Go to *Policy & Objects > Policy Packages*. Select *Create New* from the *Policy Package* drop-down.
7. In the *Create New Policy Package* dialog, specify the name as *New\_Policy\_Package*.
8. Click the *New\_Policy\_Package* and click *Create New*. Specify the name as *New\_IPv4\_Policy* and include *Zone\_One* in the policy.

9. Click *New\_IPv4\_Policy* and click *Installation Target*. Assign the FortiGate device to this policy.
10. Right-click *New Policy Package* and select *Install Wizard*. Select *Install Policy Package & Device Settings* and select the *New Policy Package* from the drop-down. Complete the installation as per the Install Wizard. *Zone\_One* is now available on the FortiGate device and mapped as specified in step 5.



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.

### 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> .



After creating the shaping profile, go to *Device Manager > Device & Groups > Managed Devices > [Device\_Name]*. In *System:Interface*, toggle *Shaping Profile* to *ON*. Select the newly created shaping profile and click *OK*.



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.

## 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>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>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>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:

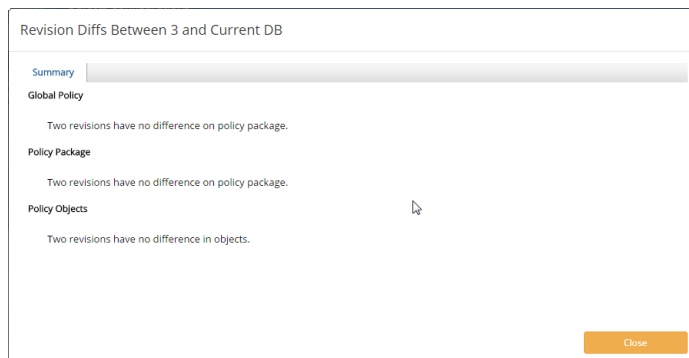
1. Open the *ADOM Revisions* window.
2. Select a revision, and click *Restore*. A confirmation dialog box will appear.
3. Click **OK** to continue.  
The *Restore Revision* dialog box opens. Restoring a revision will revert policy packages, objects and VPN console to the selected version.
4. Click **OK** 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.



# 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:

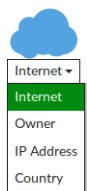
- [Security Fabric Topology on page 237](#)
- [Physical Topology on page 238](#)
- [Logical Topology on page 239](#)
- [Filter Topology Views on page 240](#)
- [Search Topology Views on page 241](#)
- [Security Rating on page 241](#)
- [Fabric Connectors on page 243](#)

## 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.

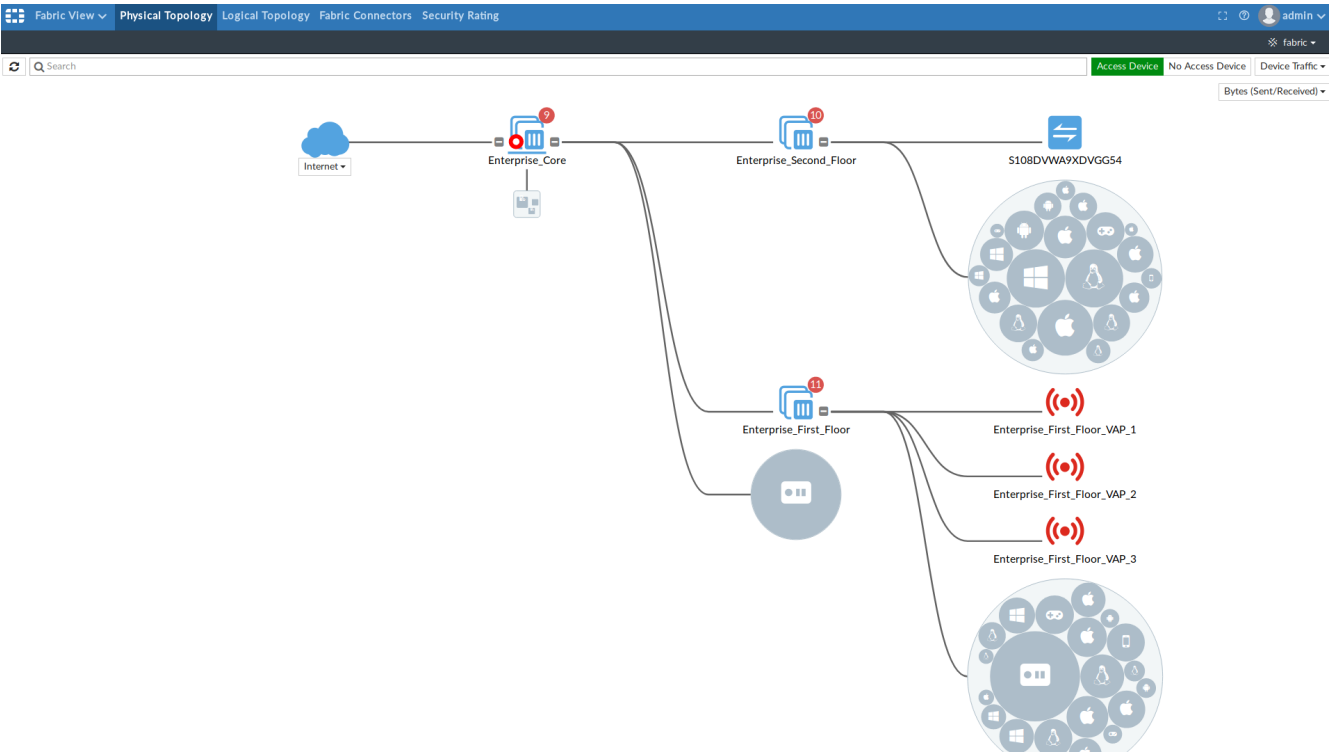
### Switch stacking

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.

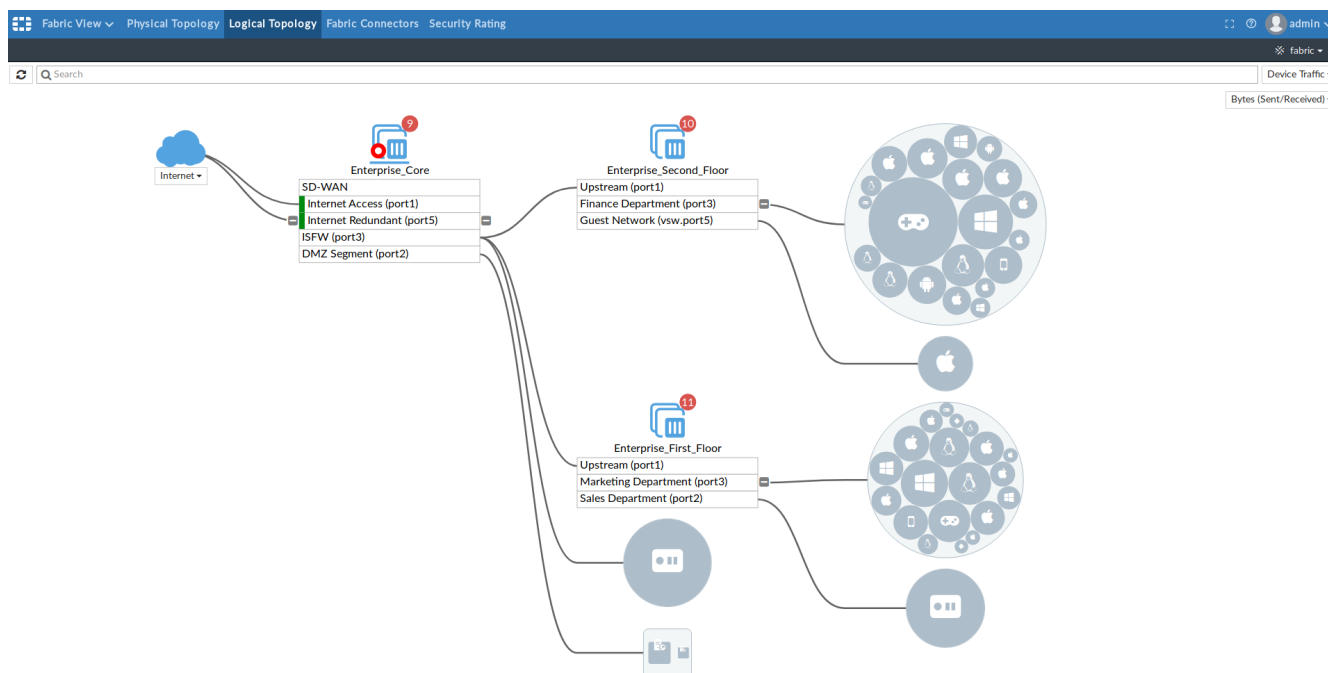
FortiGate	Enterprise_First_Floor
Hostname	Enterprise_First_Floor
Serial	FGVM010000154924
Model	FortiGate VM64-KVM
Version	v6.2.0 build0776
Operation Mode	NAT
Inspection Mode	Proxy-based
Topology	Enterprise_Core Enterprise_First_Floor 3 Downstream Fabric Devices
Management IP	10.100.88.101
CPU Usage	1%
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 screenshot shows the FortiManager interface with the 'Security Rating' pane selected. The top bar indicates 'Fabric View' and 'Security Rating'. The main area displays a 'Security Score: -595.4' with a progress bar showing 'Failed (32)' and 'All Results (96)'. Below the score, a table lists issues categorized by 'Issue', 'FortiGate', 'Result', and 'Recommendation'.

Issue	FortiGate	Result	Recommendation
Endpoint Management: 2 High, 2 Medium, 4 Critical			
Endpoint Registration Interfaces which are classified as "LAN" should have FortiTelemetry enabled.	FGT100DHA-CSF-root (FG100D3G14811667)	-30	All dependencies were not met in order for this test to run. Apply the recommendations of the following tests so that further auditing can take place: • Interface Classification
	FG101E-L3 (FG101E4Q17001278)	-30	audit_package::recommendation::EndpointRegistration 1. lan <b>Easy Apply</b>
FortiClient Compliance All registered FortiClient devices should be compliant with FortiClient compliance profile.	FGT100DHA-CSF-root (FG100D3G14811667)	-10	All dependencies were not met in order for this test to run. Apply the recommendations of the following tests so that further auditing can take place: • Endpoint Registration
	FG101E-L3 (FG101E4Q17001278)	-10	All dependencies were not met in order for this test to run. Apply the recommendations of the following tests so that further auditing can take place: • Endpoint Registration

The following information is available on the *Security Rating* pane:

### Tree menu

Displays the list of Security Fabric groups. Each group is identified by its root FortiGate unit.

<b>Security Score</b>	The results of the Security Fabric Rating. For information about each of the checks that are performed, see the <a href="#">Fortinet Recommended Security Best Practices</a> document.
<b>Failed &lt;number&gt;</b>	Click to filter the content pane to display only failed results. The number of failures is displayed in brackets.
<b>All Results &lt;number&gt;</b>	Click to filter the content pane to display all results. The total number of results is displayed in brackets.
<b>All FortiGates</b>	Click to view results for all FortiGate units in the selected Security Fabric group, or click individual FortiGate units to view only its results.
<b>Issues</b>	You can expand and contract the list of issues. For example, click <i>Fabric Security Hardening</i> to expand and contract the rows of information about that issue.
<b>FortiGate</b>	Displays the name of the FortiGate unit. Hover your mouse over the name to display more information about the device.
<b>Result</b>	Displays the result of the Security Fabric Rating for the specific issue.
<b>Recommendation</b>	Displays the recommended action for the issue.

## 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.

## Fabric Connectors

You can use FortiManager to create the following types of fabric connectors:

- [SDN](#)
- [Threat Feeds](#)
- [SSO/Identity](#)



You can create multiple fabric connectors of the same type in FortiManager. This is applicable only for ADOM version 6.2.

---

## SDN

You can use the *Fabric Connectors* tab to create SDN fabric connectors for the following products:

- Cisco Application Centric Infrastructure (ACI)
- Amazon Web Services (AWS)
- Microsoft Azure
- VMware NSX
- Nuage Virtualized Services Platform
- Horizon (OpenStack)
- Oracle Cloud Infrastructure
- VMWare ESXi

The fabric connectors in FortiManager define the type of connector and include information for FortiGate to communicate with and authenticate with the products. In some cases FortiGate units must communicate with products through the Fortinet SDN Connector, and in other cases FortiGate units communicate directly with the products.

FortiGate works with Fortinet SDN Connector to communicate with the following products:

- Cisco Application Centric Infrastructure (ACI)
- Nuage Virtualized Services Platform

For more information about Fortinet SDN Connector, see the [Fortinet Document Library](#).



You cannot import a policy package for Fortinet SDN Connector from FortiGate to FortiManager.

---

FortiGate works without Fortinet SDN Connector to communicate directly with the following products:

- Amazon Web Services (AWS)
- Microsoft Azure
- VMware NSX

- Horizon (OpenStack)
- Oracle Cloud Infrastructure
- VMWare ESXi

This section contains the following topics:

- [Creating ACI fabric connectors on page 244](#)
- [Creating AWS fabric connectors on page 245](#)
- [Creating Microsoft Azure fabric connectors on page 246](#)
- [Creating VMware NSX fabric connectors on page 247](#)
- [Creating Nuage fabric connectors on page 249](#)
- [Creating Horizon connector on page 253](#)
- [Creating Oracle Cloud Infrastructure \(OCI\) connector on page 254](#)
- [Creating VMWare ESXi connector on page 255](#)
- [Importing address names to fabric connectors on page 250](#)
- [Configuring dynamic firewall addresses for fabric connectors on page 251](#)
- [Configuring virtual wire pairs on page 252](#)

## 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 and Fortinet SDN Connector to communicate 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 through Fortinet SDN Connector. As a result, you are configuring communication and authentication information for Fortinet SDN Connector.

If ADOMs are enabled, you can create multiple fabric connectors per ADOM; however, each fabric connector requires a unique IP address.

Requirements:

- FortiManager version 5.6 ADOM or later  
The method described in this topic for creating fabric connectors requires version 6.0 ADOM or later.
- 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 Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.
3. Under *SDN*, select *ACI*, and click *Next*.
4. Configure the following options, and then click *OK*:

<b>Name</b>	Type a name for the fabric connector object.
<b>Type</b>	Displays Application Centric Infrastructure (ACI).



<b>IP</b>	Type the IP address for Fortinet SDN Connector.
<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.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.

#### To complete the fabric connector setup:

1. Import address names from ACI to the fabric connector object. See [Importing address names to fabric connectors on page 250](#).  
The address names are imported and converted to dynamic firewall address objects. The objects do not yet include IP addresses. The objects are displayed on the *Firewall Objects > Addresses* pane.
2. In the policy package in which you will be creating the new policy, create an IPv4 policy and include the firewall address objects for ACI. See [IP policies on page 184](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 165](#).  
FortiGate uses the information and Fortinet SDN Connector to communicate with ACI and dynamically populate the firewall address objects with IP addresses.

If the address names change in ACI after you import them to FortiManager, you must import the address names again.

## 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. Fortinet SDN Connector is not required for this configuration.

When you create a fabric connector for AWS, you are specifying how FortiGate can communicate directly with AWS.

If ADOMs are enabled, you can create one fabric connector per ADOM.

Requirements:

- FortiManager version 5.6 ADOM or later  
The method described in this topic for creating fabric connectors requires version 6.0 ADOM or later.
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with AWS.

Following is a high-level overview of the configuration procedure:

#### To create a fabric connector object for AWS:

1. Go to *Fabric View > Fabric Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.

3. Under *SDN*, select *AWS*, and click *Next*.
4. Configure the following options, and then click *OK*:

<b>Name</b>	Type a name for the fabric connector object.
<b>Type</b>	Displays <i>Amazon Web Services (AWS)</i> .
<b>AWS access key ID</b>	Type the access key ID from AWS.
<b>AWS secret access key</b>	Type the secret access key from AWS.
<b>AWS region name</b>	Type the region name from AWS.
<b>AWS VPC ID</b>	Type the AWS VPC ID.
<b>Update Interval (s)</b>	Specify how often in seconds that the dynamic firewall objects should be updated.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.

#### To complete the fabric connector setup:

1. Import address names from AWS to the fabric connector object. See [Importing address names to fabric connectors on page 250](#).  
The address names are imported and converted to firewall address objects. The objects do not yet include IP addresses. The objects are displayed on the *Firewall Objects > Addresses* pane.
2. In the policy package in which you will be creating the new policy, create an IPv4 policy and include the firewall address objects for AWS. See [IP policies on page 184](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 165](#).  
FortiGate communicates with AWS to dynamically populate the firewall address objects with IP addresses.

If the filter names change in AWS after you import them to FortiManager, you must modify the filter again.

## Creating Microsoft Azure fabric connectors

With FortiManager, you can create a fabric connector for Microsoft Azure. You cannot import address names from Microsoft Azure to the fabric connector. Instead you must manually create dynamic firewall 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. Fortinet SDN Connector is not required for this configuration.

When you create a fabric connector for Microsoft Azure, you are specifying how FortiGate can communicate directly with Microsoft Azure.

If ADOMs are enabled, you can create one fabric connector per ADOM.

Requirements:

- FortiManager version 5.6 ADOM or later  
The method described in this topic for creating fabric connectors requires version 6.0 ADOM or later.
- 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 Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.
3. Under *SDN*, select *Azure*, and click *Next*.
4. Configure the following options, and then click *OK*:

<b>Name</b>	Type a name for the fabric connector object.
<b>Type</b>	Displays Microsoft Azure.
<b>Azure tenant ID</b>	Type the tenant ID from Azure.
<b>Azure client ID</b>	Type the client ID from Azure.
<b>Azure client secret</b>	Type the client secret from Azure.
<b>Azure subscription ID</b>	Type the subscription ID for Azure.
<b>Azure resource group</b>	Type the resource group for Azure.
<b>Update Interval (s)</b>	Specify how often in seconds that the dynamic firewall objects should be updated.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
<b>Advanced Options</b>	Expand to specify advanced options for Azure.
<b>azure-region</b>	Select an Azure region.

**To complete the fabric connector setup:**

1. Create dynamic firewall address objects. See [Configuring dynamic firewall addresses for fabric connectors on page 251](#).  
You cannot import address names from Microsoft Azure to FortiManager.
2. In the policy package in which you will be creating the new policy, create an IPv4 policy and include the dynamic firewall address objects for Microsoft Azure. See [IP policies on page 184](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 165](#).  
FortiGate communicates with Microsoft Azure 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. Fortinet SDN Connector is not required for this configuration.

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:

- FortiManager version 5.6 ADOM or later  
The method described in this topic for creating fabric connectors requires version 6.0 ADOM or later.
- 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 Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.
3. Under *SDN*, select *NSX*, and click *Next*.
4. Configure the following options, and then click *OK*:

<b>Name</b>	Type a name for the fabric connector object.
<b>Type</b>	Displays <i>VMware NSX</i> .
<b>IP</b>	Type the IP address for VMware NSX.
<b>User Name</b>	Type the user name for VMware NSX.
<b>Password</b>	Type the password for VMware NSX.
<b>Update Interval (s)</b>	Specify how often in seconds that the dynamic firewall objects should be updated.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
<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 Mgmt and Sync.
<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.

#### To complete the fabric connector setup:

1. Import address names from VMware NSX to the fabric connector object. See [Importing address names to fabric connectors on page 250](#).

The address names are imported and converted to firewall address objects. The objects do not yet include IP addresses. The objects are displayed on the *Firewall Objects > Addresses* pane.

2. Create a virtual wire pair. See [Configuring virtual wire pairs on page 252](#).
3. In the policy package in which you will be creating the new policy, create an IPv4 virtual wire pair policy, select the virtual wire pair, and add the firewall address objects for the VMware NSX. See [Virtual wire pair policy on page 196](#).
4. Install the policy package to FortiGate or FortiGate VMX Service Manager. See [Install a policy package on page 165](#).

The FortiGate unit or FortiGate VMX Service Manager communicates with VMware NSX to dynamically populate the firewall address objects with IP addresses.

If the address names change in VMware NSX after you import them to FortiManager, you must import the address names again.

## Creating Nuage fabric connectors

With FortiManager, you can create a fabric connector for Nuage Virtualized Services Platform. You cannot import address names from Nuage Virtualized Services Platform to the fabric connector. Instead you must manually create dynamic firewall objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information and Fortinet SDN Connector to communicate with Nuage Virtualized Services Platform and dynamically populate the objects with IP addresses.

When you create a fabric connector for Nuage Virtualized Services Plan, you are specifying how FortiGate can communicate with Nuage through Fortinet SDN Connector. As a result, you are configuring communication and authentication information for Fortinet SDN Connector.

If ADOMs are enabled, you can create multiple fabric connectors per ADOM; however, each fabric connector requires a unique IP address.

Requirements:

- FortiManager version 5.6 ADOM or later  
The method described in this topic for creating fabric connectors requires version 6.0 ADOM or later.
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with Nuage Virtualized Services Platform.

### To create a fabric connector object for Nuage:

1. Go to *Fabric View > Fabric Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.
3. Under *SDN*, select *Nuage*, and click *Next*.
4. Configure the following options, and then click *OK*:

<b>Name</b>	Type a name for the fabric connector object.
<b>Type</b>	Displays Nuage Virtualized Services Platform.
<b>IP</b>	Type the IP address for Fortinet SDN Connector.
<b>Port</b>	Identify the port used for Fortinet SDN Connector.

Perform one of the following options:

- Click *Use Default* to use the default port.
- Click *Specify* and type the port number.

<b>User Name</b>	Type the user name for Fortinet SDN Connector.
<b>Password</b>	Type the password for Fortinet SDN Connector.
<b>Status</b>	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.

#### To complete the fabric connector setup:

1. Create dynamic firewall address objects. See [Configuring dynamic firewall addresses for fabric connectors on page 251](#).

You cannot import address names from Nuage Virtualized Services Platform to FortiManager.

2. In the policy package in which you will be creating the new policy, create an IPv4 policy and include the firewall address objects for Nuage Virtualized Services Platform. See [IP policies on page 184](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 165](#).

FortiGate communicates with Nuage Virtualized Services Platform 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 NSX and ACI, to the fabric connector, and dynamic firewall address objects are automatically created.

When you are importing address names from AWS, you must add filters to display the correct instances before importing address names.



You cannot import address names to fabric connectors created for Microsoft Azure and Nuage Virtualized Services Platform. You must manually create dynamic firewall address objects for these types of fabric connectors. See [Configuring dynamic firewall addresses for fabric connectors on page 251](#).

#### To import address names for NSX and ACI:

1. Go to *Policy & Objects > Object Configurations*.
2. In the tree menu, go to *Security Fabric > Fabric Connectors*.
3. In the content pane, right-click the fabric connector, and select *Import*.  
The *Import SDN Connector* dialog box is displayed.
4. Select the address names, and click *Import*.  
The address names are imported and converted to dynamic firewall address objects that are displayed on the *Firewall Objects > Addresses* pane.

#### To import address names for AWS:

1. Go to *Policy & Objects > Object Configurations*.
2. In the tree menu, go to *Security Fabric > Fabric Connectors*.

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 AWS 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: `AWS-<random identifier>`. Use the *Details* column and the instance ID to identify the object.

## Configuring dynamic firewall addresses for fabric connectors

You cannot import address names to fabric connectors created for Microsoft Azure and Nuage Virtualized Services Platform. Instead you must create dynamic firewall objects that can be dynamically populated when FortiGate communicates with Microsoft Azure and Nuage Virtualized Services Platform.

### To configure dynamic firewall addresses for Microsoft Azure 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. Complete the following options for Microsoft Azure fabric connectors:

<b>Address Name</b>	Type a name for the firewall address object.
<b>Type</b>	Select <i>Fabric Connector Address</i> .
<b>SDN</b>	Select the Microsoft Azure fabric connector.
<b>Filter</b>	Type the name of the filter for the AWS instance.

5. Set the remaining options as required, and click *OK*

#### To configure dynamic firewall addresses for Nuage 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. Complete the following options for Nuage fabric connectors:

<b>Address Name</b>	Type a name for the firewall address object.
<b>Type</b>	Select <i>Fabric Connector Address</i> .
<b>SDN</b>	Select the Nuage Virtualized Services Platform fabric connector.
<b>Organization</b>	Type the name of the organization for the Nuage Virtualized Services Platform.
<b>Subnet Name</b>	Type the name of the subnet for the Nuage Virtualized Services Platform.
<b>Policy Group</b>	Type the name of the policy group for the Nuage Virtualized Services Platform.

5. Set the remaining options as required, and click *OK*

## Configuring virtual wire pairs

Before you create an IPv4 virtual wire pair policy, you must create a virtual wire pair.



ADOM version 5.4, 5.6, or later is required. Earlier ADOM versions are not supported.

#### To configure virtual wire pairs:

1. Go to *Policy & Objects > Object Configurations*.
2. In the tree menu, go to *Zone/Interface > Interface*.
3. In the content pane, click *Create New* and select *Virtual Wire Pair*.
4. Complete the following options, and click *OK*.

<b>Name</b>	Type a name for the virtual wire pair.
-------------	--



**Interface Members**

Select two interface members.

**Wildcard VLAN**

Toggle **ON** to enable wildcard VLANs for the virtual wire pair. When enabled, all VLAN-tagged traffic can pass through the virtual wire pair, if allowed by the virtual wire pair firewall policies.

Toggle **OFF** to disable wildcard VLANs for the virtual wire pair.

## Creating 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 and Fortinet SDN Connector 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) through Fortinet SDN Connector. As a result, you are configuring communication and authentication information for Fortinet SDN Connector.


If ADOMs are enabled, you can create multiple fabric connectors per ADOM; however, each fabric connector requires a unique IP address.

Requirements:


- FortiManager version 6.0 ADOM or later.  
The method described in this topic for creating fabric connectors requires version 6.0 ADOM or later.
- 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):

- Go to *Fabric View > Fabric Connectors*.
- Click *Create New*. The *Create New Fabric Connector* wizard is displayed.
- Under *SDN*, select *Horizon*, and click *Next*. The *Horizon (OpenStack)* screen is displayed.

Create New Fabric Connector  OpenStack (Horizon)

---

Name	<input type="text"/>
Type	OpenStack (Horizon) ▼
Domain	<input type="text"/>
Server	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password"/> 
Update Interval (s) ⓘ	<input type="button" value="Use Default"/> <input type="button" value="Specify"/>
Status	<input checked="" type="checkbox"/> ON <input type="checkbox"/>

- Configure the following options, and then click **OK**:

<b>Name</b>	Type a name for the fabric connector object.
<b>Type</b>	Displays OpenStack (Horizon).

<b>Domain</b>	Type the Domain for Fortinet SDN Connector.
<b>Server</b>	Type the IP address for the SDN Connector.
<b>User Name</b>	Type the user name for Fortinet SDN Connector.
<b>Password</b>	Type the password for Fortinet SDN Connector.
<b>Update Interval (s)</b>	Specify the update interval for the Fortinet SDN Connector. 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.

5. Go to *Policy & Objects > Security Fabric > Fabric Connectors*. Select the connector and click *Import*.
6. The Horizon (OpenStack) connector is imported. Click *Close* to close the import dialog.
7. Create a Policy Package and install it to a FortiGate device. The Horizon (OpenStack) connector object is synced with the FortiGate device.

## Creating Oracle Cloud Infrastructure (OCI) connector

With FortiManager, you can create a fabric connector for Oracle (OCI), and then import address names from Oracle (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 and Fortinet SDN Connector to communicate with Oracle (OCI) and dynamically populate the objects with IP addresses.

When you create a fabric connector for Oracle (OCI), you are specifying how FortiGate can communicate with Oracle (OCI) through Fortinet SDN Connector. As a result, you are configuring communication and authentication information for Fortinet SDN Connector.

If ADOMs are enabled, you can create multiple fabric connectors per ADOM; however, each fabric connector requires a unique IP address.

Requirements:

- FortiManager with ADOM version 6.0 or later.  
The method described in this topic for creating fabric connectors requires ADOM version 6.0 or later.
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with Oracle (OCI).

### To create a fabric connector object for Oracle (OCI):

1. Go to *Fabric View > Fabric Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.

3. Under *SDN*, select *Oracle*, and click *Next*. The *Oracle Cloud Infrastructure (OCI)* screen is displayed.

Create New Fabric Connector ORACLE Oracle Cloud Infrastructure (OCI)

---

Name	<input type="text"/>
Type	Oracle Cloud Infrastructure (OCI) ▼
User ID	<input type="text"/>
OCI Tenant ID	<input type="text"/>
OCI Compartment ID	<input type="text"/>
OCI Server Region	US Phoenix Server ▼
OCI Certificate	None ▼
Update Interval (s) ⓘ	<input type="button" value="Use Default"/> <input type="button" value="Specify"/>
Status	<input checked="" type="checkbox"/> ON

4. Configure the following options, and then click *OK*:

<b>Name</b>	Type a name for the fabric connector object.
<b>Type</b>	Displays Oracle Cloud Infrastructure (OCI).
<b>User ID</b>	Type the User ID for the Fortinet SDN Connector.
<b>OCI Tenant ID</b>	Type the OCI Tenant ID.
<b>OCI Compartment ID</b>	Type the OCI Compartment ID.
<b>OCI Server Region</b>	Select the OCI Server Region from the drop-down.
<b>OCI Certificate</b>	Select the OCI Certificate from the drop-down.
<b>Update Interval (s)</b>	Specify the update interval for the Fortinet SDN Connector. 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.

5. Go to *Policy & Objects > Security Fabric > Fabric Connectors*. Select the connector and click *Import*.
6. The Oracle (OCI) connector is imported. Click *Close* to close the import dialog.
7. Create a Policy Package and install it to a FortiGate device. The Oracle (OCI) connector object is synced with the FortiGate device.

## 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 and Fortinet SDN Connector 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 with VMWare ESXi through Fortinet SDN Connector. As a result, you are configuring communication and authentication information for Fortinet SDN Connector.

If ADOMs are enabled, you can create multiple fabric connectors per ADOM; however, each fabric connector requires a unique IP address.

Requirements:

- FortiManager with ADOM version 6.2 or later.  
The method described in this topic for creating fabric connectors requires ADOM version 6.2 or later.
- 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 Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.
3. Under *SDN*, select *VMWare ESXi*, and click *Next*. The *VMWare ESXi* screen is displayed.

Create New Fabric Connector vmware VMWare ESXi

---

Name

Type VMWare ESXi

Server

User Name

Password

Update Interval (s) Use Default Specify

Status ON

< Back
OK
Cancel

4. Configure the following options, and then 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 the SDN Connector.
<b>User Name</b>	Type the user name for Fortinet SDN Connector.
<b>Password</b>	Type the password for Fortinet SDN Connector.
<b>Update Interval (s)</b>	Specify the update interval for the Fortinet SDN Connector. 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.

5. Go to *Policy & Objects > Security Fabric > Fabric Connectors*. Select the connector and click *Import*.
6. The VMWare ESXi connector is imported. Click *Close* to close the import dialog.

7. Create a Policy Package and install it to a FortiGate device. The VMWare ESXi connector object is synced with the FortiGate device.

## 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 and Fortinet SDN Connector 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 with Kubernetes through Fortinet SDN Connector. As a result, you are configuring communication and authentication information for Fortinet SDN Connector.

If ADOMs are enabled, you can create multiple fabric connectors per ADOM; however, each fabric connector requires a unique IP address.

Requirements:

- FortiManager with ADOM version 6.2 or later.  
The method described in this topic for creating fabric connectors requires ADOM version 6.2 or later.
- 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 Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.
3. Under *SDN*, select *Kubernetes*, and click *Next*. The *Kubernetes* screen is displayed.

#### Create New Fabric Connector



Name

Type  
Kubernetes ▼

IP

Port

Secret Token

Update Interval (s) ⓘ

Status  
☒ ON ☐

4. Configure the following options, and then click *OK*:

Name	Type a name for the fabric connector object.
------	--

<b>Type</b>	Displays Kubernetes.
<b>IP</b>	Type the IP address for the SDN Connector.
<b>Port</b>	Specify the port for the Fortinet SDN Connector. 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>
<b>Secret Token</b>	Specify a secret token for the Fortinet SDN Connector.
<b>Update Interval (s)</b>	Specify the update interval for the Fortinet SDN Connector. 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.

- Go to *Policy & Objects > Security Fabric > Fabric Connectors*. Select the connector and click *Import*.
- The Kubernetes connector is imported. Click *Close* to close the import dialog.
- Create a Policy Package and install it to a FortiGate device. The Kubernetes connector object is synced with the FortiGate device.



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 Alibaba Cloud Service connector

With FortiManager, you can create a fabric connector for Alibaba Cloud Service (ACS), and then import address names from Alibaba Cloud 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 and Fortinet SDN Connector to communicate with Alibaba Cloud Service and dynamically populate the objects with IP addresses.

When you create a fabric connector for Alibaba Cloud Service, you are specifying how FortiGate can communicate with Alibaba Cloud Service through Fortinet SDN Connector. As a result, you are configuring communication and authentication information for Fortinet SDN Connector.

If ADOMs are enabled, you can create multiple fabric connectors per ADOM; however, each fabric connector requires a unique IP address.

Requirements:

- FortiManager with ADOM version 6.2 or later.  
The method described in this topic for creating fabric connectors requires ADOM version 6.2 or later.
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with Alibaba Cloud Service.

### To create a fabric connector object for Alibaba Cloud Service:

1. Go to *Fabric View > Fabric Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.
3. Under *SDN*, select *Alibaba Cloud Service*, and click *Next*. The *Alibaba Cloud Service* screen is displayed.

#### Create New Fabric Connector



Name

Type  
Alibaba Cloud Service (ACS) ▼

AccessKey ID

AccessKey Secret

Region ID

Update Interval (s) ⓘ

Status  
☒ ON ☐ OFF

&lt; Back

OK

Cancel

4. Configure the following options, and then click *OK*:

<b>Name</b>	Type a name for the fabric connector object.
<b>Type</b>	Displays Alibaba Cloud Service (ACS).
<b>AccessKey ID</b>	Specify the AccessKey ID for the SDN Connector.
<b>AccessKey Secret</b>	Specify the AccessKey Secret for the SDN Connector.
<b>Region ID</b>	Specify the Region ID for the Fortinet SDN Connector.
<b>Update Interval (s)</b>	Specify the update interval for the Fortinet SDN Connector. 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.

5. Go to *Policy & Objects > Security Fabric > Fabric Connectors*. Select the connector and click *Import*.
6. The Alibaba Cloud Service connector is imported. Click *Close* to close the import dialog.
7. Create a Policy Package and install it to a FortiGate device. The Alibaba Cloud Service connector object is synced with the FortiGate device.

## Creating Google Cloud Platform connector

With FortiManager, you can create a fabric connector for Google Cloud Platform (GCP), and then import address names from Google Cloud Platform 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 and Fortinet SDN Connector to communicate with Google Cloud Platform and dynamically populate the objects with IP addresses.

When you create a fabric connector for Google Cloud Platform, you are specifying how FortiGate can communicate with Google Cloud Platform through Fortinet SDN Connector. As a result, you are configuring communication and authentication information for Fortinet SDN Connector.

If ADOMs are enabled, you can create multiple fabric connectors per ADOM; however, each fabric connector requires a unique IP address.

Requirements:

- FortiManager with ADOM version 6.2 or later.  
The method described in this topic for creating fabric connectors requires ADOM version 6.2 or later.
- 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 Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.
3. Under *SDN*, select *Google Cloud Platform*, and click *Next*. The *Google Cloud Platform* screen is displayed.

Create New Fabric Connector

Google Cloud Platform (GCP)

Name

Type

Google Cloud Platform (GCP)

Project Name

Service Account Email

Private Key

Update Interval (s) ⓘ

Use Default Specify

Status

ON

< Back OK Cancel

4. Configure the following options, and then click *OK*:

<b>Name</b>	Type a name for the fabric connector object.
<b>Type</b>	Displays Google Cloud Platform (GCP).
<b>Project Name</b>	Specify the Project Name for the SDN Connector.
<b>Service Account Email</b>	Specify the Service Account Email for the SDN Connector.
<b>Private Key</b>	Specify the Private Key for the Fortinet SDN Connector.
<b>Update Interval (s)</b>	Specify the update interval for the Fortinet SDN Connector.



Select one of the following options:

- Click *Use Default* to use the default interval.
- Click *Specify* and specify the interval.

**Status**

Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.

5. Go to *Policy & Objects > Security Fabric > Fabric Connectors*. Select the connector and click *Import*.
6. The Google Cloud Platform connector is imported. Click *Close* to close the import dialog.
7. Create a Policy Package and install it to a FortiGate device. The Google Cloud Platform connector object is synced with the FortiGate device.

## Threat Feeds

You can use the *Fabric Connectors* tab to create the following types of threat feed connectors:

- Category
- Address
- Domain

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 261](#)

## Creating threat feed connectors

You can create threat feed connectors for FortiGuard categories, firewall IP addresses, and domain names.

### To create threat feed connectors:

1. Go to *Fabric View > Fabric Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.
3. Under *Threat Feeds*, select *Category*, *Address*, or *Domain*, and click *Next*.
4. Configure the following options, and then click *OK*:

<b>Type</b>	Displays <i>URL List</i> if you selected <i>Category</i> . Displays <i>IP List</i> if you selected <i>Address</i> . Displays <i>Domain List</i> if you selected <i>Domain</i> .
<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>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.

## SSO/Identity

You can use the *Fabric Connectors* tab to create the following types of SSO/identity connectors:

- AD Polling
- FSSO
- RADIUS
- Cisco pxGrid
- Aruba ClearPass

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 262](#)
- [Creating FSSO connectors on page 263](#)
- [Creating RADIUS connectors on page 263](#)
- [Creating Cisco pxGrid connector on page 264](#)
- [Creating ClearPass connector on page 270](#)

## 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 Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.
3. Under *SSO/Identity*, select *AD Polling*, and click *Next*.
4. Configure the following options, and then 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.

**LDAP Server**

Select the LDAP server name from the list. The LDAP server name is used in LDAP connection strings.

## Creating FSSO connectors

You can create SSO/identity connectors for Fortinet single sign-on (FSSO) agents.

FSSO is the authentication protocol by which users can transparently authenticate to FortiGate, FortiClient EMS, FortiAuthenticator, and FortiCache devices.

### To create FSSO connectors:

1. Go to *Fabric View > Fabric Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.
3. Under *SSO/Identity*, select *FSSO*, and click *Next*.
4. Configure the following options, and then click *OK*:

<b>Name</b>	Type a name for the connector object.
<b>FSSO Agent</b>	Complete the <i>IP/Name</i> , <i>Password</i> , and <i>Port</i> options for each FortiAuthenticator unit that will act as an SSO agent.
<b>Select FSSO Groups</b>	Specify whether to get FSSO groups from FSSO agents or via FortiGate.
<b>User Groups LDAP Server</b>	Select the name of the LDAP server to be used to get group information from the Directory Service.
<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> .



To configure the FSSO connector as a FortiClient EMS Connector, select the *Type* as *FortiClient EMS*, *IP/Name* as the Windows Server's IP and turn *SSL* to *ON*. Click *Apply and Refresh*. The connector gets a list of tags from the EMS server and shows them as User Groups. This is similar to the Active Directory groups in Windows Server.

## 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 Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.

- Under *SSO/Identity*, select *RADIUS*, and click *Next*.
- Configure the following options, and then click *OK*:

Name	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.
<b>Advanced Options</b>	Expand to view and configure advanced options for RADIUS single sign-on agents. For details, see the <i>FortiOS CLI Reference</i> .

## Creating Cisco pxGrid connector

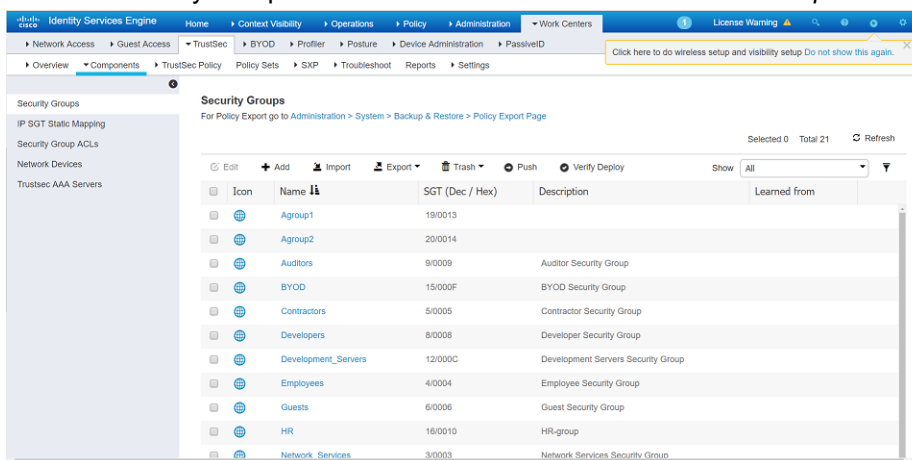
Cisco pxGrid for FortiManager centralizes the updates from pxGrid for all FortiGate devices, and leverages the efficient FSSO protocol to apply dynamic policy updates to FortiGate.

Requirements:

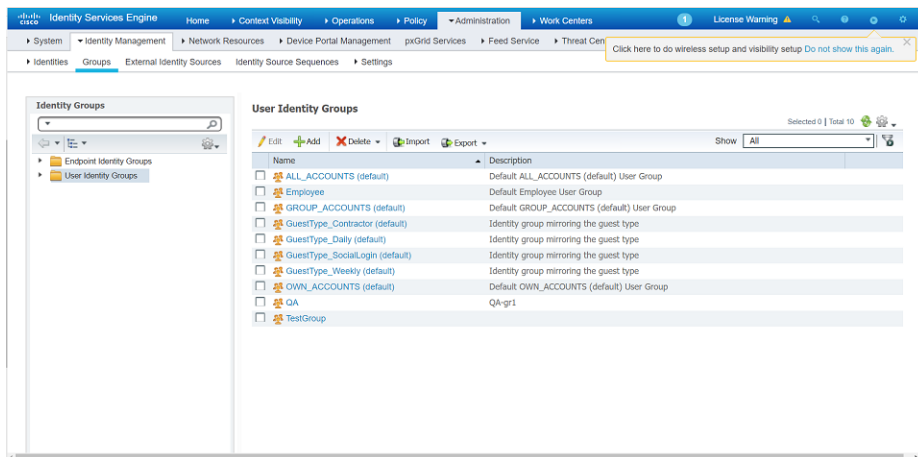
- FortiManager version 5.6 ADOM or later.  
The method described in this topic for creating fabric connectors requires version 6.0 ADOM or later.
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with Cisco pxGrid.
- Configure the Cisco ISE server and download the certificate.

### To configure Cisco ISE server:

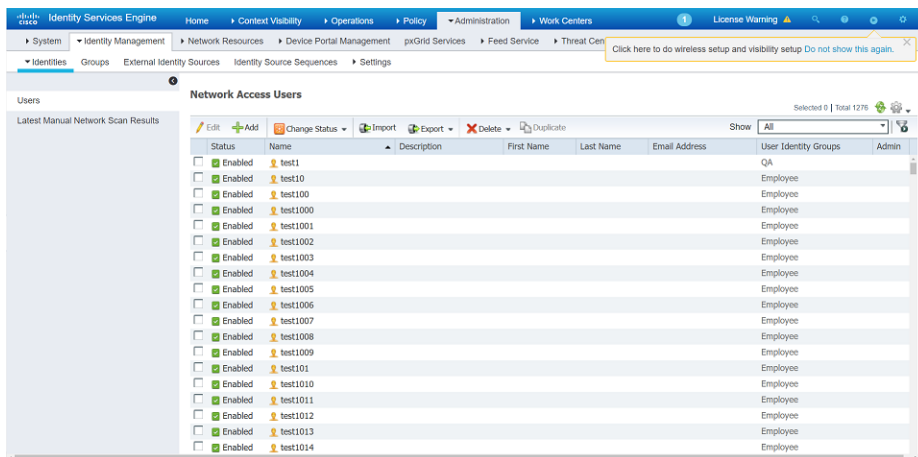
- Create a Security Group: Go to *ISE > Work Centers > TrustSec > Components > Security Groups*. Click *Add*.



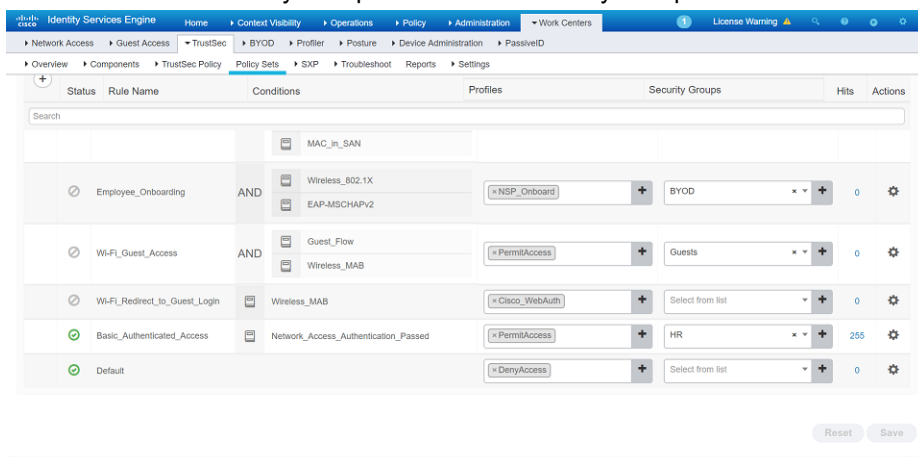
- Create a User Identity Group: Go to *ISE > Administration > Identity Management > Groups > User Identity Groups*. Click *Add*.



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**.

Identity Services Engine

Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

All Clients Web Clients Capabilities Live Log Settings Certificates Permissions

### Generate pxGrid Certificates

I want to \*

Common Name (CN) \*

Certificate Template PxGrid\_Certificate\_Template

Subject Alternative Name (SAN) \*

Certificate Download Format \*

Certificate Password \*

Confirm Password \*

Reset Create

Connected to pxGrid Ise-fmgga.fmgga.com

6. See log for current users: Go to *ISE > Operations > RADIUS > Live Logs*.

Identity Services Engine

Home Context Visibility Operations Policy Administration Work Centers

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client Stopped Responding 0 Repeat Counter 0

Refresh Never Show Latest 20 records Within Last 3 hours

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP A
Mar 01, 2019 02:52:32.196 PM	0		0	test2	00:11:22:33:44:55	Unknown	Default >> D...	Default >> B...	PermitAcces...	192.
Mar 01, 2019 02:52:03.737 PM				test2	00:11:22:33:44:55	Unknown	Default >> D...	Default >> B...	PermitAcces...	192.
Mar 01, 2019 02:44:06.881 PM				test2	00:11:22:33:44:55		Default >> D...	Default		192.

Last Updated: Fri Mar 01 2019 14:53:44 GMT-0800 (Pacific Standard Time) Records Shown: 3

7. See live sessions of current users: Go to *ISE > Operations > RADIUS > Live Sessions*.

Identity Services Engine

Home Context Visibility Operations Policy Administration Work Centers

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Live Logs Live Sessions

Refresh Every 1 minute Show Latest 20 records Within Last 24 hours

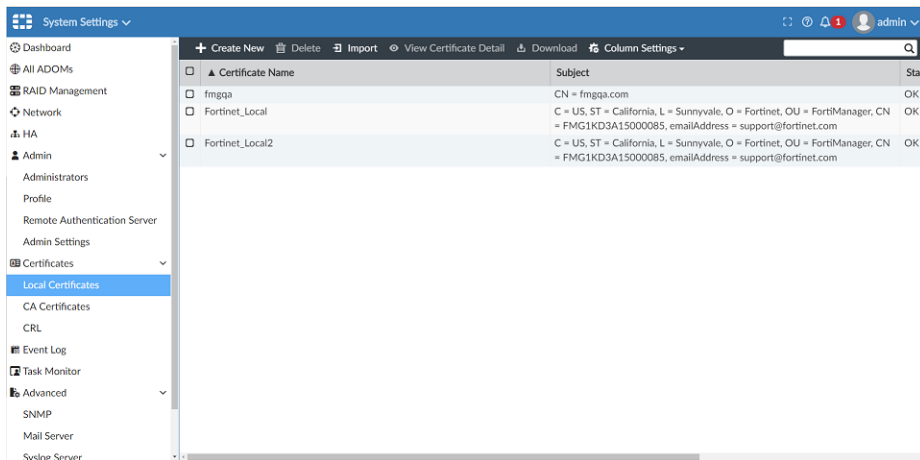
Refresh Export To Filter

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

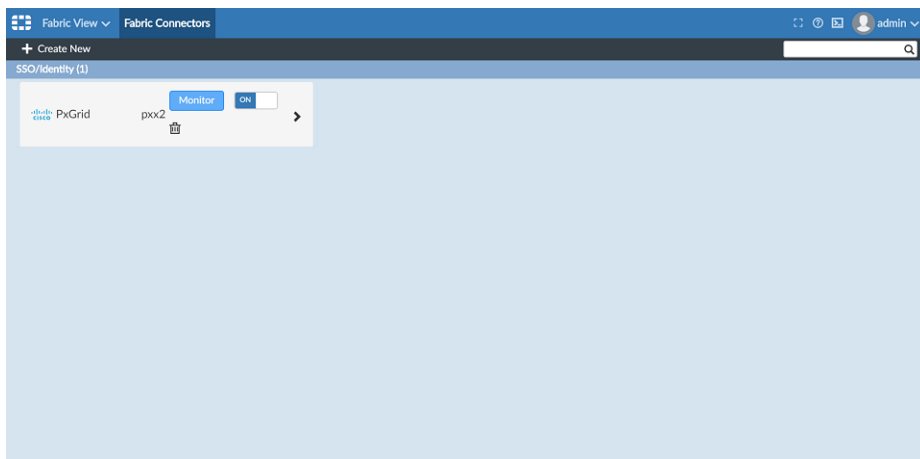
Last Updated: Fri Mar 01 2019 14:54:44 GMT-0800 (Pacific Standard Time) Records Shown: 1

## To configure FortiManager:

1. Go to *System Settings > Local Certificates > Import*. Import the downloaded certificate.



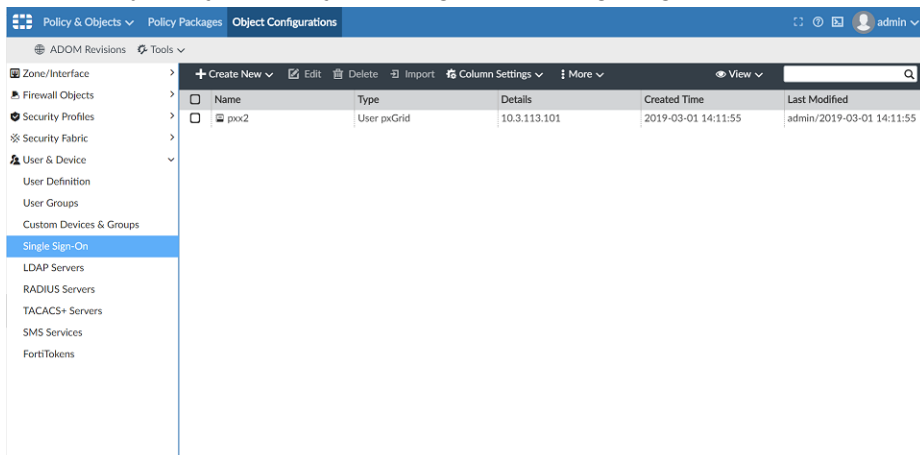
2. Go to *Fabric View > Fabric Connectors*.
3. Click *Create New*.
4. Select *Cisco pxGrid* and click *Next*.
5. Configure the following options and click *OK* to create the Cisco pxGrid connector:



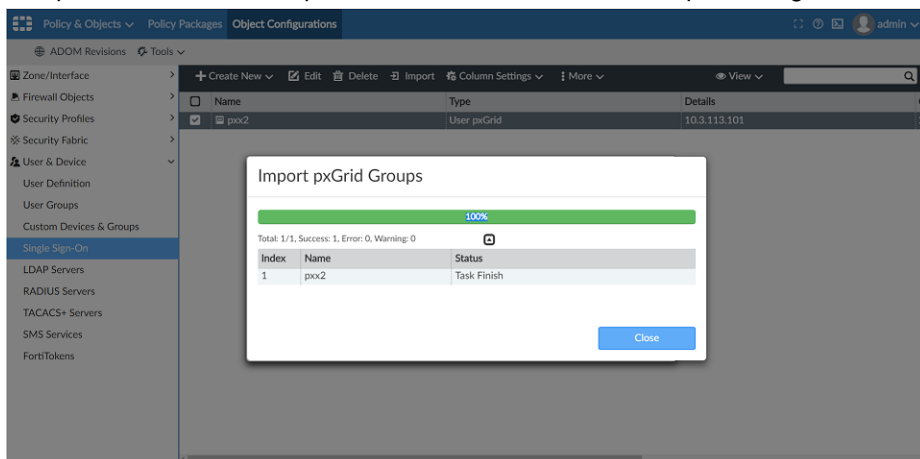
6.

<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.

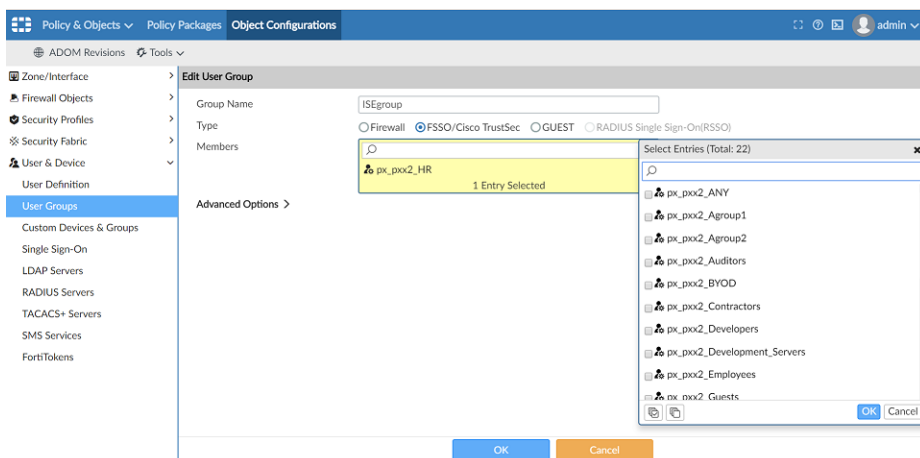
7. Go to **Policy & Objects > Object Configuration > Single Sign-On**. Select the connector and click **Import**.



8. The pxGrid connector is imported. Click **Close** to close the import dialog.

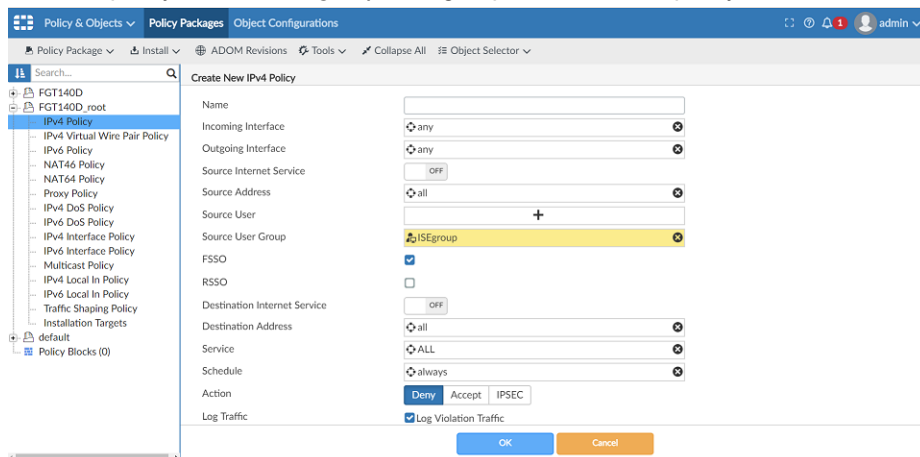


9. Click **User Groups** and create a new group. Set the type as **FSSO/Cisco TrustSec**, and select **pxGrid** user as a member.

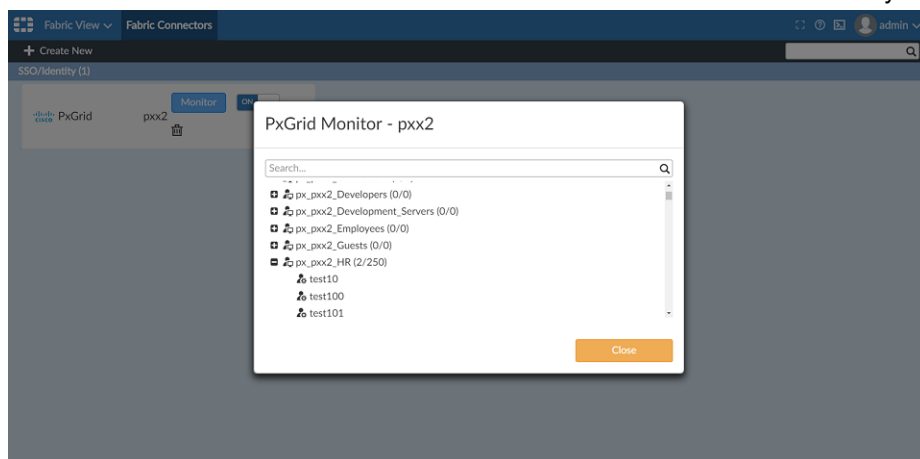




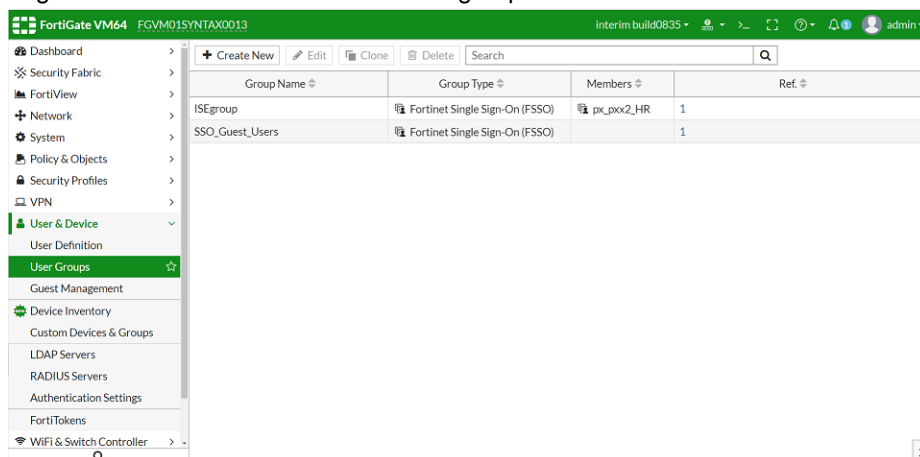
10. Create a policy with the *ISEgroup* user group and install the policy to FortiGate.



11. Go to *Fabric View > Fabric Connectors*. Click *Monitor* to see the users currently logged in.



12. Log on to FortiGate to view the ISE user group.



13. On the FortiGate command line, use the `diagnose debug authd fssolist` to monitor the current user list.

## CLI Commands for FortiManager and FortiGate

### Command line 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 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_grpl Workstation: MemberOf: fscs1
IP: 192.168.1.20 User: test2 Groups: px_fcl_security_grpl 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 connector

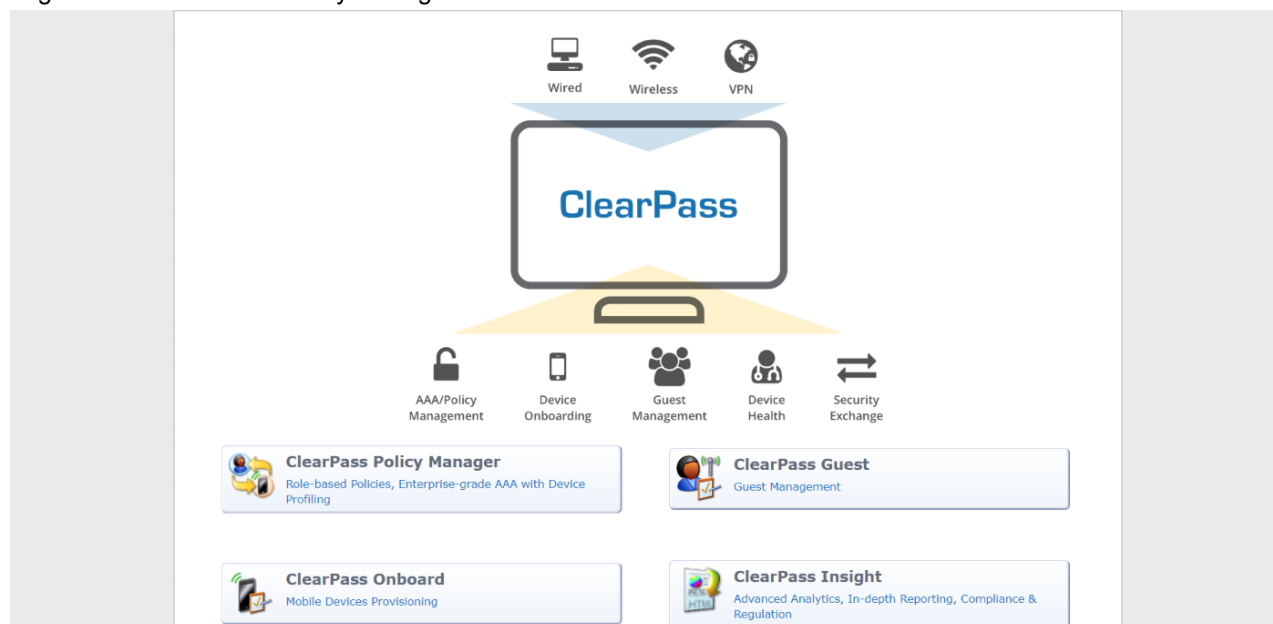
ClearPass connector for FortiManager centralizes the updates from ClearPass for all FortiGate devices, and leverages the efficient FSSO protocol to apply dynamic policy updates to FortiGate.

### Requirements:

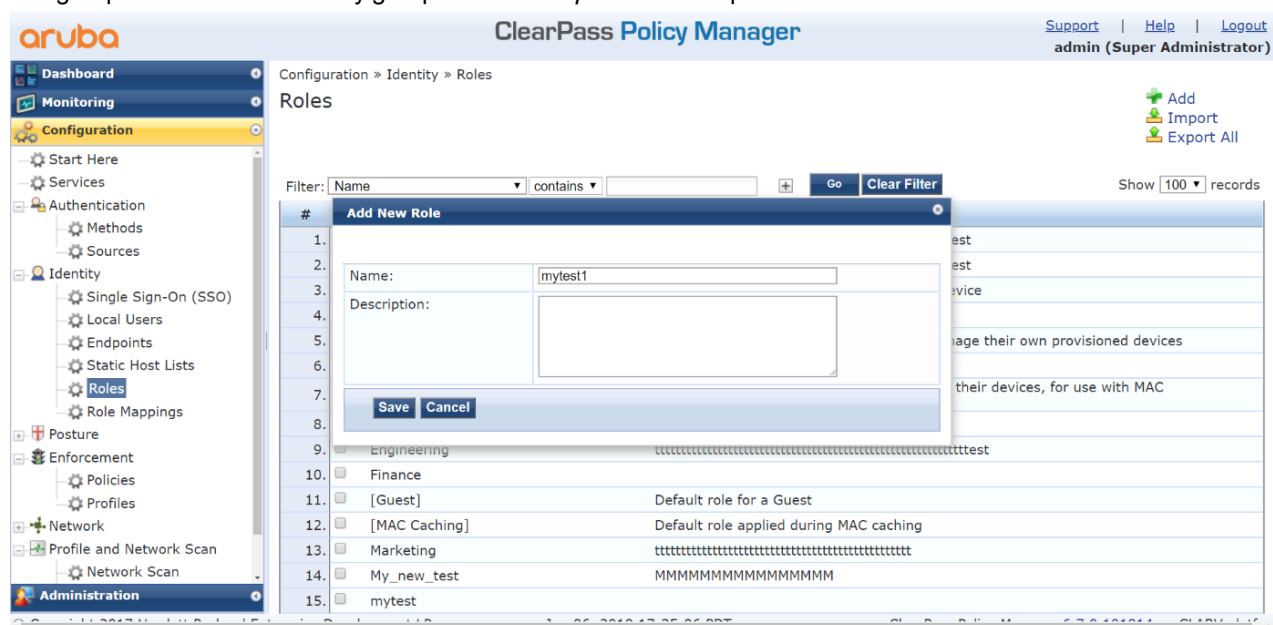
- FortiManager version 5.6 ADOM or later.  
The method described in this topic for creating fabric connectors requires version 6.0 ADOM or later.
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with ClearPass.
- Expose JSON API allowing ClearPass to call it.

### To configure ClearPass:

1. Log on to the ClearPass Policy Manager.



2. **Create Roles.** Go to *Configuration > Identity > Roles > Add*. Specify the name as *mytest1*. FortiManager will get this group as an Active Directory group. The *Description* field is optional.



3. Create local users. Go to *Configuration > Identity > Local Users > Add*. Configure the following:

The screenshot shows the 'Add Local User' form in the ClearPass Policy Manager. The form fields are as follows:

- User ID: test1
- Name: testUser1
- Password: (masked)
- Verify Password: (masked)
- Enable User: ☒ (Check to enable user)
- Change Password: ☐ (Check to force change password on next TACACS+ login)
- Role: mytest1

The 'Attributes' section is currently empty, showing a table with columns 'Attribute' and 'Value'.

- User ID - specify the user ID as *test1*.
- Name - specify the name as *testUser1*.
- Password - specify the password as *qa1234*.
- Enable - select the check box.
- Role - specify the role as *mytest1* (created in step 1).

4. Add Ubuntu Simulator. Go to *Configuration > Network > Devices > Add*. Configure the following settings:

The screenshot shows the 'Add Device' form in the ClearPass Policy Manager. The form fields are as follows:

- Name: Ubuntu\_test
- IP or Subnet Address: (empty)
- Description: (empty)
- RADIUS Shared Secret: (masked)
- TACACS+ Shared Secret: (masked)
- Vendor Name: Unix
- Enable RADIUS CoA: ☒ RADIUS CoA Port: 3799
- Verify: (masked)
- Verify: (empty)

- Name - specify the name as *Ubuntu\_test*.
- IP or Subnet Address - specify as 10.3.113.61.
- RADIUS Shared Secret - specify as *qa1234*.
- Vendor name - specify as *Unix*.

5. Configure FortiManager to get packet from ClearPass.
6. Create Endpoint Context Server Action for FortiManager. Go to *Administration > Dictionaries > Context Server Actions > Add*. Create a *Login* action.
7. Configure the following settings in the Action tab:

The screenshot shows the Aruba ClearPass Policy Manager web interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, and Administration. Under Administration, there are links for Syslog Export Filters, Messaging Setup, Endpoint Context Server, File Backup Servers, Certificates, Dictionaries, and Agents and Software Updates. The main content area is titled 'ClearPass Policy Manager' and shows a table of actions. The 'Endpoint Context Server Details' dialog is open, displaying the configuration for a new action.

Action	Header	Content	Attributes
11.	Generic HTTP	Copy_of_Check Point Login - AD User	POST
Inform Check Point that user logged in.			

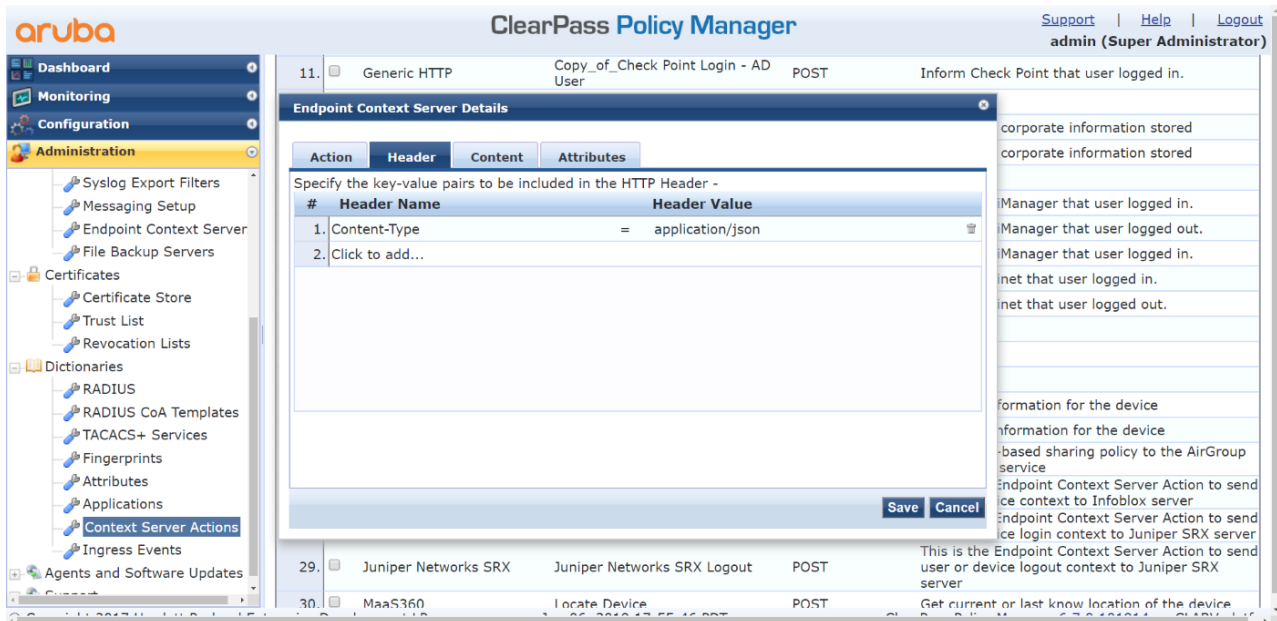
**Endpoint Context Server Details**

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

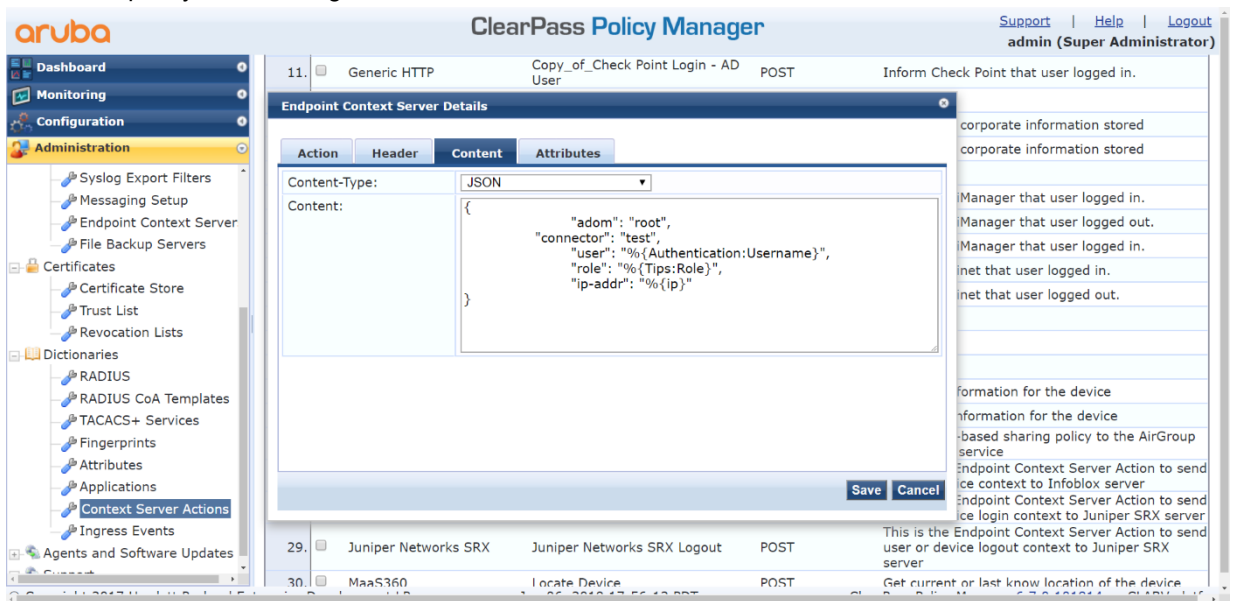
Save Cancel

- Server Type - select *Generic HTTP*.
- Server Name - specify *10.3.113.57*. This is the IP address of FortiManager.
- Action Name - specify as *Frank-FMG-login*.
- Description - inform FortiManager that the user logged on.
- HTTP Method- select *POST*.
- Authentication Method - select *Basic*.
- URL - specify */jsonrpc/connector/user/login*

## 8. Configure the following settings in the Header tab:



- Header Name - specify as *Content-Type*.
- Header Value - specify as *application/json*.
- Content-Type - select *JSON*.
- Content - specify the following:



```
{
  "adom": "root",
  "connector": "test", <-----this will be the connector name created on
  "user": "%{Authentication:Username}",
  "role": "%{Tips:Role}",
  "ip-addr": "%{ip}"
}
```

9. Create Endpoint Context Server Action for FortiManager. Go to *Administration > Dictionaries > Context Server Actions > Add*. Create a *Logout* action.

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-logout		
Description:			
HTTP Method:	POST		
Authentication Method:	Basic		
URL:	/jsonrpc/connector/user/logout		

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

10. Configure the following settings in the Action tab:

ClearPass Policy Manager

Support | Help | Logout  
admin (Super Administrator)

Administration » External Servers » Endpoint Context Servers

**Add Endpoint Context Server**

Server

Select Server Type:	Generic HTTP
Server Name:	10.3.113.57
Server Base URL:	https://10.3.113.57
Authentication Method:	Basic
Username:	admin
Password:	
Verify:	
Validate Server:	<input type="checkbox"/> Enable to validate the server certificate
Bypass Proxy:	<input type="checkbox"/> Enable to bypass proxy server

Save Cancel

Show 100 records

**Status**

Enabled
Enabled
Enabled
Enabled
Enabled
Enabled
Enabled

Export Delete

- Server Type - select *Generic HTTP*.
- Server Name - specify *10.3.113.57*. This is the IP address of FortiManager.
- Action Name - specify as *Frank-FMG-logout*.
- Description - inform FortiManager that user logged out.
- HTTP Method - select *POST*.
- Authentication Method - select *Basic*.
- URL - specify */jsonrpc/connector/user/logout*

11. Configure the following settings in the Header tab:

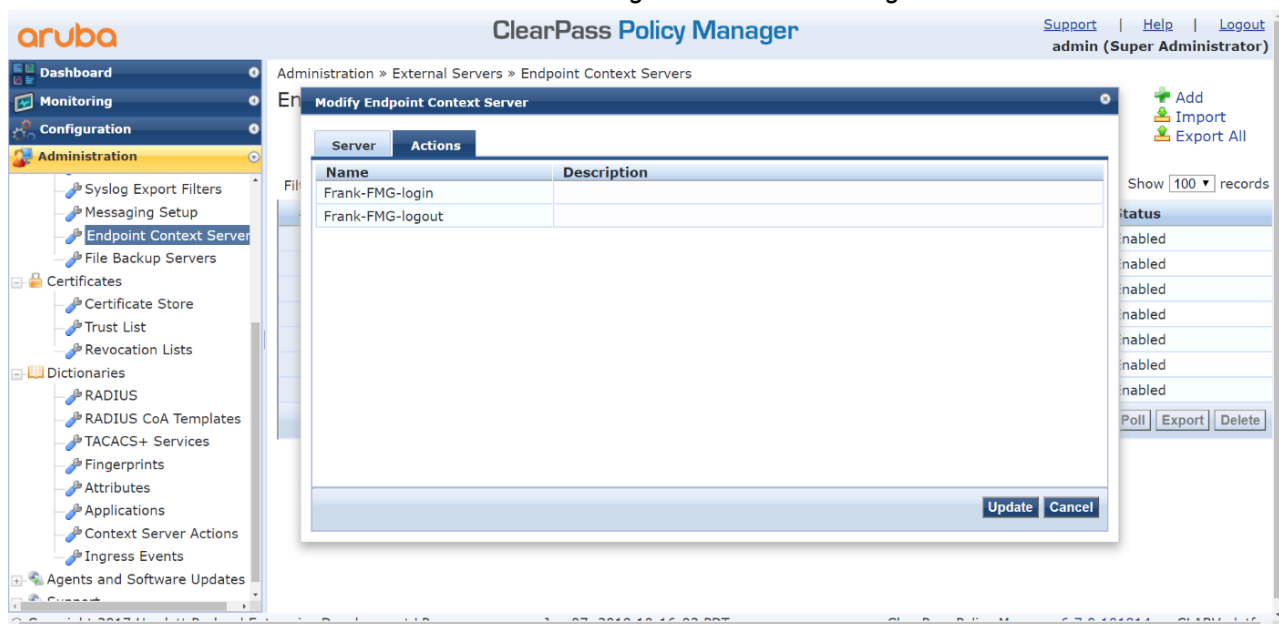
- Header Name - specify as *Content-Type*.
- Header Value - specify as *application/json*.
- Content-Type - select *JSON*.
- Content - specify the following:

```
{
    "adom": "root",
    "connector": "test", <--this will be the connector name created on FM
    "user": "%{Authentication:Username}",
    "role": "%{Tips:Role}",
    "ip-addr": "%{ip}"
}
```

12. Add FortiManager as the Endpoint Context Server. Go to *Administration > External Servers > Endpoint Context Servers > Add*. Configure the following settings:

- Server Type - select *Generic HTTP*.
- Server Name - specify *10.3.113.57*. This the FortiManager IP.
- Authentication Method - select *Basic*.
- Username - specify *admin*. This is the administrator on FortiManager.

13. Check Actions is added to the server. Go to *Administration > External Servers > Endpoint Context Servers > 10.3.113.57 > Actions*. You can now find *Frank-FMG-login* and *Frank-FMG-Logout*.



14. Create profile. Go to *Configuration > Enforcement > Profiles > Add*.



15. Configure the following settings in the *Profile* tab:

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](#)

[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

- Template - select *Session Notification Management*.
- Name - specify *FortiManager Login and Logout*.
- Description - specify *FortiManager - Initial SSO integration testing*.
- Type - select *Post\_Authentication*.

16. Configure the following settings in the *Attributes* tab.

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

Type	Name	Value
Session-Notify	Server Type	Generic HTTP
Session-Notify	Login Action	Frank-FMG-login

17.

Session-Notify	Logout Action	Frank-FMG-logout
Session-Notify	Server IP	10.3.113.57 (FortiManager IP)

18. Create a Policy. Go to *Configuration > Enforcement > Policies > Add*.

19. Configure the following settings in the *Enforcement* tab.

aruba ClearPass Policy Manager

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

- Name - specify *FortiManager testing*.
- Enforcement Type - select *RADIUS*.
- Default profile - *Allow Access Profile*.

20. Configure the following settings in the Rules tab:

aruba ClearPass Policy Manager

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...]

--Select to Add--

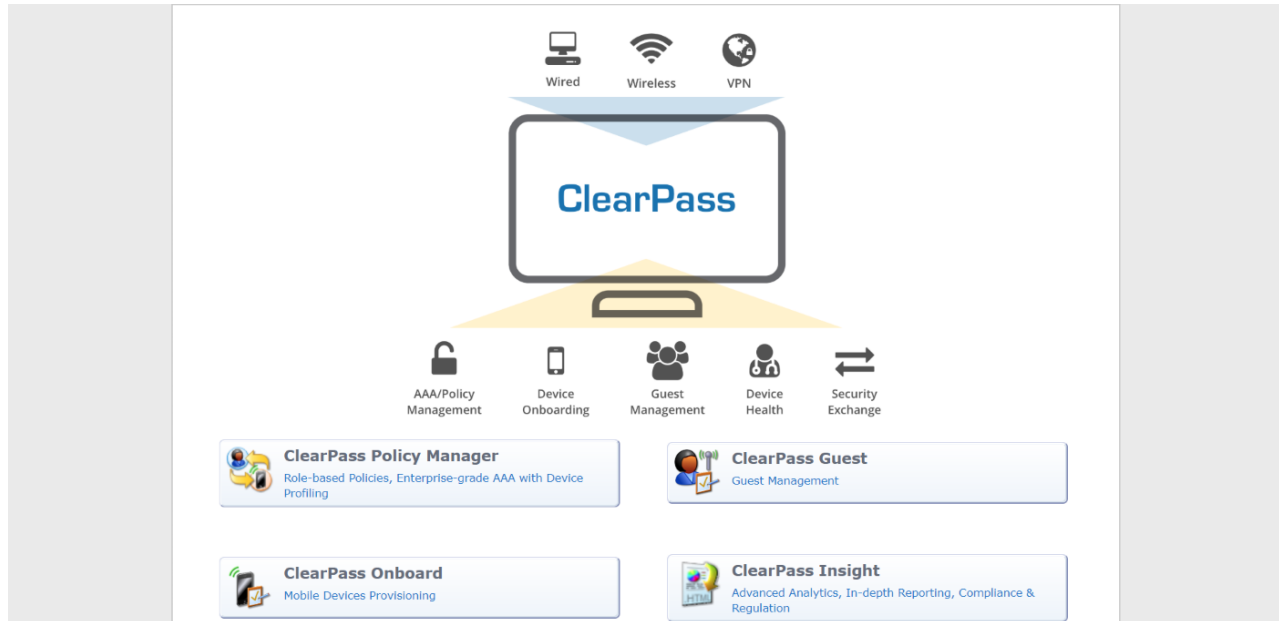
[Move Up](#) [Move Down](#) [Remove](#)

[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

- Type - select *Date*.
- Name - select *Date-Time*.
- Operation - select *EXISTS*.
- Profile Names: *[Post Authentication][FortiManager-Login and Logout]*

21. Create API Client. Log on from ClearPass Guest.



22. Go to *Administration > API Services > API Clients > Create API Client*. Configure the following:

The screenshot shows the 'Create API Client' form in the Aruba ClearPass Guest administration interface. The breadcrumb trail is 'Home > Administration > API Services > API Clients'. The form title is 'Create API Client' and it includes the instruction 'Use this form to create a new API client.' The form fields are as follows:

Create API Client	
* Client ID:	test <small>The unique string identifying this API client. Use this value in the OAuth2 "client_id" parameter.</small>
Description:	FM login from it <small>Use this field to store comments or notes about this API client.</small>
Enabled:	<input checked="" type="checkbox"/> Enable API client
* Operator Profile:	Super Administrator <small>The operator profile applies role-based access control to authorized OAuth2 clients. This determines what API objects and methods are available for use.</small>
* Grant Type:	Username and password credentials (grant_type=password) <small>Only the selected authentication method will be permitted for use with this client ID.</small>
Public Client:	<input checked="" type="checkbox"/> This client is a public (trusted) client <small>Public clients have no client secret.</small>
Refresh Token:	<input checked="" type="checkbox"/> Allow the use of refresh tokens for this client <small>An OAuth2 refresh token may be used to obtain an updated access token. Use grant_type=refresh_token for this.</small>
Access Token Lifetime:	8 hours <small>Specify the lifetime of an OAuth2 access token.</small>
Refresh Token Lifetime:	14 days <small>Specify the lifetime of an OAuth2 refresh token.</small>

© Copyright 2019 Hewlett Packard Enterprise Development LP ClearPass Guest 6.7.0.35289 on CLABV platform

- Client ID - specify as *test*.
- Description - FortiManager logs on from this client.
- Operator Profile - Select *Super Administrator*.
- Grand Type - select *Username and password credentials (grant type=password)*.

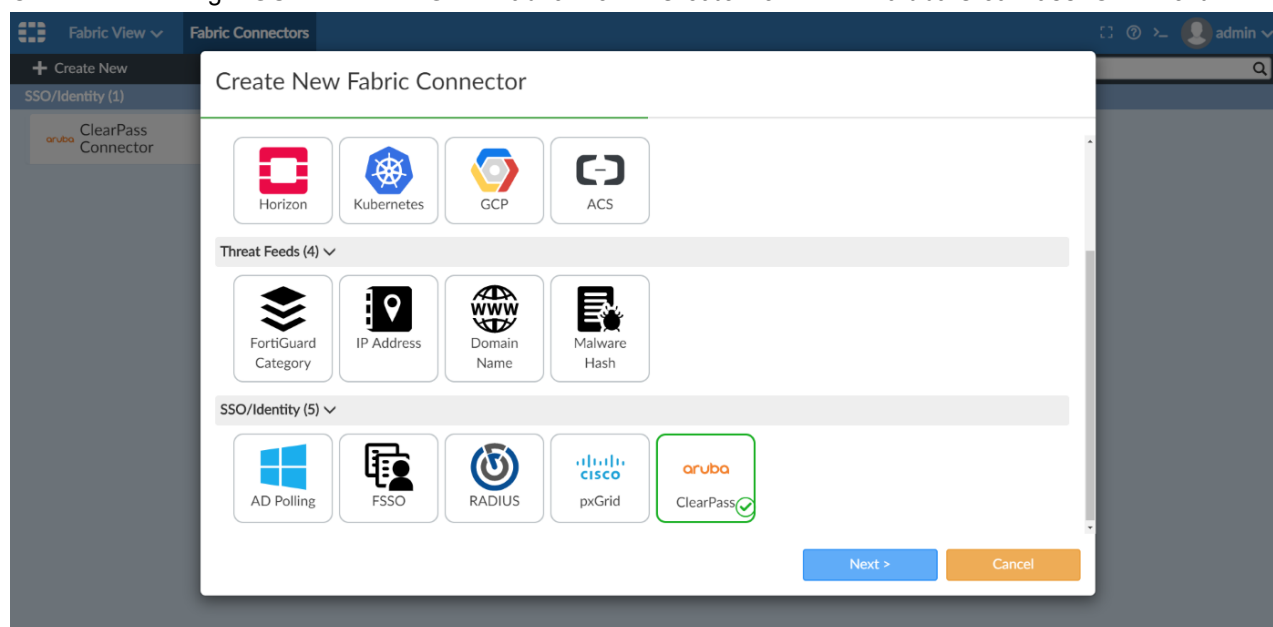
- Public Client - select the check box.
- Refresh Tokens - select the check box.

### To configure FortiManager:

1. Log on to FortiManager.
2. Launch the command line and execute the following:

```
config system admin user
edit admin
set rpc-permit read-write
end
```

3. Create FortiManager GUI connector. Go to *Fabric View > Create New*. Select *aruba ClearPass*. Click *Next*.



## 4. Configure the following settings:

aruba User ClearPass

Create New Fabric Connector

Name: test

Status: ☒ ON

Server: 10.3.113.102

Client: test

User: admin

Password: .....

< Back OK Cancel

- Name - specify the name as *test*. This name must be same as used in *ClearPass Endpoint Context Server Actions > Frank-FMG-login/Frank-FMG-logout > Content > "Connector": "test"*.
- Status - toggle to *ON*.
- Server - specify the IP as *10.3.113.102*. This is the ClearPass IP.
- Client - specify as *test*. This is the name of the API Client created.
- User - specify as *admin*. This is the ClearPass login name.
- Password - specify as *Qa1234*. This is the ClearPass password.

5. Get role and user from ClearPass. Go to *Policy & Objects > Object Configurations > Fabric Connectors > SSO/Identity*. Select the connector and click *Import*, or edit it then click *Apply & Refresh*. FortiManager then gets the roles and users from ClearPass. Green shows the user has logged on.

Policy & Objects Policy Packages Object Configurations

ADOM Revisions Tools

Zone/Interface Firewall Objects Security Profiles Fabric Connectors SDN Threat Feeds SSO/Identity User & Device WAN Optimize Dynamic Object Advanced CLI Only Objects

Edit ClearPass Connector

Name: test

Status: ☒ ON

Server: 10.3.113.102

Client: test

User: admin

Password: .....

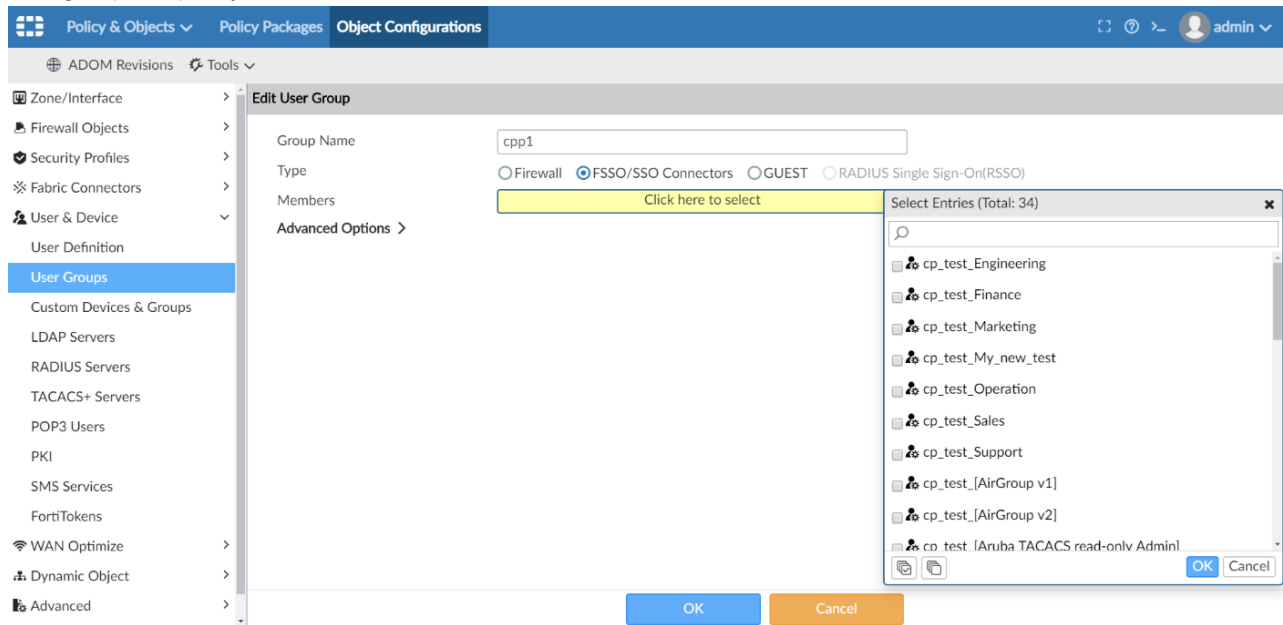
Connector Users

Search...

- cp\_test\_Engineering (0/2)
- cp\_test\_Finance (2/3)
- user1 (10.210.15.185)
- user2 (10.210.15.186)
- user5 (10.210.15.189)
- cp\_test\_Marketing (0/1)
- cp\_test\_My\_new\_test (0/0)
- cp\_test\_Operation (0/2)

Apply & Refresh OK Cancel

6. Install *adgrp* from ClearPass to FortiGate. *Policy & Objects > Object Configurations > User & Devices > User Groups*. Create user group with type as FSSO/SSO Connectors, and select members as *ClearPass adgrp*. Use the user group in a policy and install it to FortiGate.



# SOC Monitoring

Use the Security Operations Center (SOC) to view the configuration status of managed devices.

- [Monitors on page 283](#)

If FortiAnalyzer features are enabled, FortiView and additional monitors are available. For more information, see the *FortiAnalyzer Administration Guide*.

## Monitors

SOC *Monitors* include a predefined dashboard for *Device Status*.

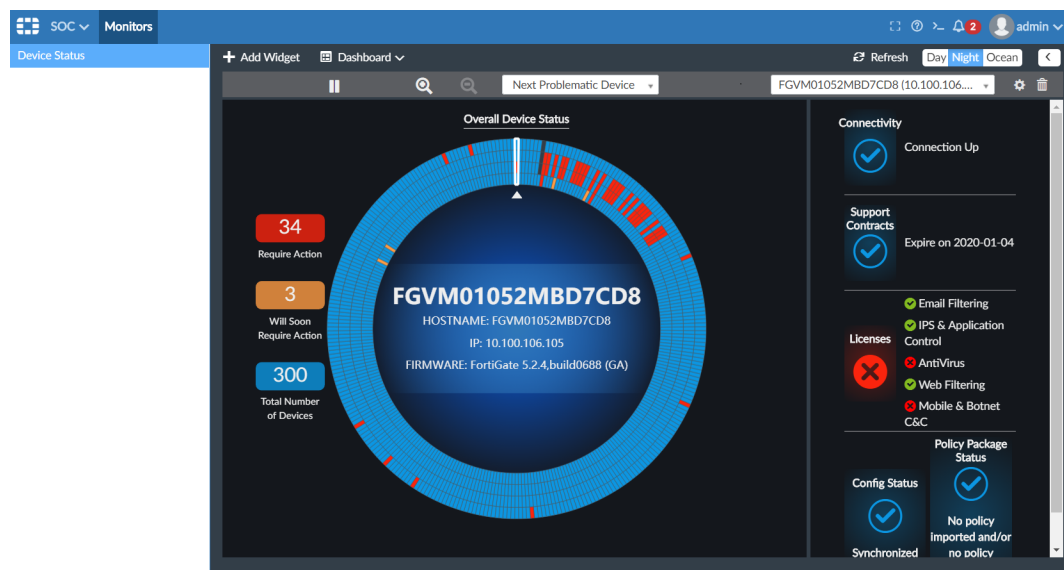
- [Device Status on page 283](#)
- [Using the Monitors dashboard on page 285](#)
- [Customizing the Monitors dashboard on page 286](#)



To prevent timeout, ensure *Idle Timeout* is greater than the widget's *Refresh Interval*. See [Idle timeout on page 532](#) and [Settings icon on page 285](#).

## Device Status

The *Device Status* dashboard communicates the configuration status between FortiManager and managed devices.



The center of the *Device Status* 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 *Device Status* 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> <p>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:</p> <ul style="list-style-type: none"> <li>• Host name</li> <li>• IP address</li> <li>• Firmware version</li> </ul> <p>Information about the following statuses of the selected device is also displayed on the right:</p> <ul style="list-style-type: none"> <li>• Connectivity status</li> <li>• Support Contracts</li> <li>• Licenses</li> <li>• Configuration Status and Policy Package Status</li> </ul> <p>The colored rings in the circle correspond to the status information on the right. The outer ring in the circle corresponds with the <i>Connectivity</i> status. The second most outer ring corresponds to the <i>Supports Contracts</i> status, and so on.</p>
<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 the Monitors dashboard

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

<b>Add Widget</b>	Add widgets to a predefined or custom dashboard. For details, see <a href="#">Customizing the Monitors dashboard on page 286</a> .
<b>Dashboard</b>	Create a new dashboard or reset a predefined dashboard to its default settings. For custom dashboards, you can rename or delete the custom dashboard. For details, see <a href="#">Customizing the Monitors dashboard on page 286</a> .
<b>Create New</b>	Create a new dashboard.
<b>Reset</b>	Reset a predefined dashboard to its default widgets and settings.
<b>Rename</b>	Rename a custom dashboard.
<b>Delete</b>	Delete a custom 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>Refresh</b>	Refresh the data in the widgets.
<b>Background color</b>	Change the background color of the dashboard to make widgets easier to view in different room lighting. <ul style="list-style-type: none"> <li>• <i>Day</i> shows a brighter gray background color.</li> <li>• <i>Night</i> shows a black background.</li> <li>• <i>Ocean</i> shows a blue background color.</li> </ul>
<b>Hide Side-menu or Show Side-menu</b>	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.
<b>Remove widget icon</b>	Delete the widget from a predefined or custom dashboard.
<b>Move widget</b>	Click and drag a widget's title bar to move it to another location.
<b>Resize widget</b>	Click and drag the resize button in the bottom-right of the widget.

## Customizing the Monitors dashboard

You can add any widget to a 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 > Reset*.

### To create a dashboard:

1. In the toolbar, click *Dashboard > Create New*.
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.

### To add a widget:

1. Select the predefined or custom dashboard where you want to add a widget.
2. Click *Add Widget* to expand the menu; then locate the widget you want to add.
3. Click the + button to add widgets.
4. When you have finished adding widgets, click the close button to close the *Add Widget* pane.

# VPN

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.



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 tabs:

<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 290</a>
<b>Monitor</b>	Displays a list of IPsec VPN tunnels, and allows you to bring the tunnels up or down. See <a href="#">Monitoring IPsec VPN tunnels on page 298</a> .
<b>Map View</b>	Displays a world map showing IPsec VPN tunnels. See <a href="#">Map View on page 299</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 308</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 288](#).

### To create IPsec VPN settings:

1. Enable central VPN management. See [Enabling central VPN management on page 288](#).
2. Create a VPN community, sometimes called a VPN topology. See [Creating IPsec VPN communities on page 290](#).
3. Create a managed gateway. See [Creating managed gateways on page 300](#).

**To create SSL-VPN settings:**

1. Create custom profiles. See [Creating SSL VPN portal profiles on page 311](#).  
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 309](#).

**To install VPN objects to devices:**

1. Plan the VPN security policies. See [VPN security policies on page 306](#).
2. In a policy package, create VPN security policies, and select the VPN settings. See [Creating policies on page 176](#).
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 168](#).
4. Install the policy package to the devices. See [Install a policy package on page 165](#).



VPNs can also be configured directly on a FortiGate. To prevent conflicts, the *preserve* field must be selected in the phase 1 and phase 2 interfaces when creating the VPN.

---

## 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*.
2. Select *Enable*.
3. Click *OK* in the confirmation dialog box.

**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-only objects menu to enable DDNS on each FortiGate device. The CLI-only objects menu is available in the Device Manager pane. See [CLI-Only Objects menu on page 62](#).

With the CLI-only objects 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-only objects 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-only objects 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.

## IPsec VPN Communities

You can use the *VPN Management > IPsec VPN* pane to create and monitor full-meshed, star, and dial-up IPsec VPN communities. IPsec VPN communities are also sometimes called VPN topologies.

### Managing IPsec VPN communities

Go to *VPN Manager > IPsec VPN* to manage IPsec VPN communities.

<a href="#">+ Create New</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Column Settings</a> <input type="text"/>								
<input type="checkbox"/>	Seq.#	Name	Topology	Gateways	Authentication	Phase 1 Encryption	Phase 2 Encryption	VPN Zone
<input type="checkbox"/>	1	F	Full Mesh	4 Gateways FGT54_1[root] FGT54_1[root] FGT54_2[root] FGT54_2[root]	Pre-shared Key	3des-sha1, 3des-md5	3des-sha1, 3des-md5	✓
<input type="checkbox"/>	2	dual-l	Star		Pre-shared Key	3des-sha1, 3des-md5	3des-sha1, 3des-md5	✓

The following options are available:

<b>VPN Community</b>	Select to create a new VPN community, edit the selected VPN community, or delete the selected VPN community.
<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 290</a>
<b>Edit</b>	Edit the selected VPN community. See <a href="#">Editing an IPsec VPN community on page 297</a> .
<b>Delete</b>	Delete the selected VPN community or communities. See <a href="#">Deleting VPN communities on page 298</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 300</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 300</a> .

### Creating IPsec VPN communities

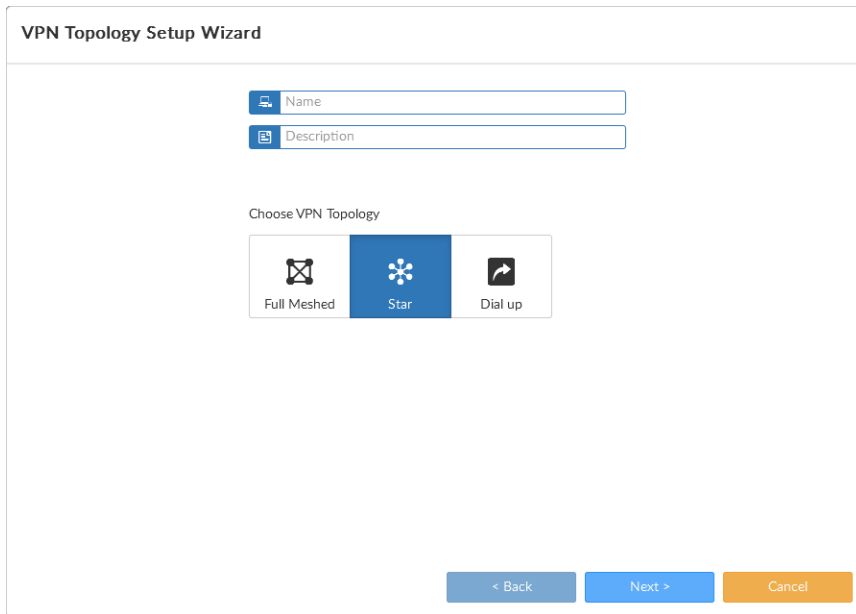
You can create one or more IPsec VPN communities. An IPsec VPN community is also sometimes called a VPN topology. A *VPN Topology Wizard* is available to help you set up topologies.

After you create the IPsec VPN community, you can create the VPN gateway. See [IPsec VPN gateways on page 300](#).

**To create a new IPsec VPN community:**

1. Go to the *VPN Manager > IPsec VPN* tab.
2. Do one of the following:
  - From the *VPN Community* menu select *Create New*.
  - Click *Create New* in the content pane toolbar.
  - Right-click in the tree menu or on an existing community and select *Create New*.

The *VPN Topology Setup Wizard* is displayed.



The image shows the 'VPN Topology Setup Wizard' dialog box. It has a title bar 'VPN Topology Setup Wizard'. Inside, there are two text input fields: 'Name' and 'Description'. Below these fields is a section titled 'Choose VPN Topology'. It contains three buttons with icons: 'Full Meshed' (a square with an 'X'), 'Star' (a star icon, which is highlighted with a blue background), and 'Dial up' (a computer monitor icon). At the bottom right of the dialog are three buttons: '< Back' (disabled), 'Next >' (active), and 'Cancel'.

3. Enter a name for the topology in the *Name* field.
4. Optionally, enter a brief description of the topology in the *Description* field.
5. Choose a topology type: *Full Meshed*, *Star*, or *Dial up*.
  - *Full Meshed*: Each gateway has a tunnel to every other gateway.
  - *Star*: Each gateway has one tunnel to a central hub gateway.
  - *Dial up*: Some gateways, often mobile users, have dynamic IP addresses and contact the gateway to establish a tunnel.

6. Click *Next*.

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

7. Configure the *Authentication* and *Encryption* information for the topology
8. Click *Next*.
9. Configure the *VPN Zone*, *IKE Security Phase 1 Advanced Properties*, *IPsec Security Phase 2 Advanced Properties*, and *Advanced Options*.
10. Click *Next*.
11. Review the topology information on the *Summary* page, then click *OK* to create the topology.
- After you have created the VPN topology, you can create managed and external gateways for the topology.



For descriptions of the options in the wizard, see [VPN community settings on page 292](#).

VPN community settings

The following table describes the options available in the *VPN Topology Setup Wizard* and on the *Edit VPN Community* page.

Name	Type a name for the VPN topology.
Description	Type an optional description.
Choose VPN Topology	Choose a topology type. Select one of: <ul style="list-style-type: none"><li>Full Meshed: Each gateway has a tunnel to every other gateway.</li><li>Star: Each gateway has one tunnel to a central hub gateway.</li></ul>



	<ul style="list-style-type: none"> <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>	<p>Select <i>Certificates</i> or <i>Pre-shared Key</i>.</p> <p>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.</p>
<b>Certificates</b>	<p>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.</p>
<b>Pre-shared Key</b>	<p>If you selected <i>Pre-shared Key</i>, select <i>Generate</i> or <i>Specify</i>.</p> <p>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.</p> <p>Alternatively, you can select to generate a random pre-shared key.</p>
<b>Encryption</b>	<p>Define the IKE Profile. Configure IKE Phase 1 and IKE Phase 2 settings.</p>
<b>IKE Security (Phase 1) Properties</b>	<p>Define the Phase 1 proposal settings.</p>
<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> </ul>

- DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
- SEED: A 16-round Feistel network with 128-bit blocks and a 128-bit key.

Select either of the following authentication message digests to check the authenticity of messages during phase 1 negotiations:

- MD5: Message Digest 5, the hash algorithm developed by RSA Data Security.
- SHA1: Secure Hash Algorithm 1, which produces a 160-bit message digest.
- SHA256: Secure Hash Algorithm 2, which produces a 256-bit message digest.
- SHA384: Secure Hash Algorithm 3, which produces a 384-bit message digest.
- SHA512: Secure Hash Algorithm 3, which produces a 512-bit message digest.

Note: If the encryption is GCM or CHACHA20POLY1305, the authentication options are PRFSHA1, PRFSHA256, PRFSHA384, and PRFSHA512.

To specify more combinations, use the Add button beside any of the table rows.

#### **IPsec Security (Phase 2) Properties**

Define the Phase 2 proposal settings.

When you define phase 2 parameters, you can choose any set of phase 1 parameters to set up a secure connection for the tunnel and authenticate the remote peer. Auto Key configuration applies to both tunnel-mode and interface-mode VPNs.

#### **Encryption Authentication**

Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required.

You need to select at least one combination. The remote peer or client must be configured to use at least one of the proposals that you define.

It is invalid to set both Encryption and Authentication to NULL.

Select one of the following symmetric-key encryption algorithms:

- 3DES: Triple-DES, in which plain text is encrypted three times by three keys.
- AES128: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key.
- AES128GCM: AES128 Galois/Counter Mode (GCM).
- AES192: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key.
- AES256: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key.
- AES256GCM
- ARIA128: A 128-bit block size that uses a 128-bit key.
- ARIA192: A 128-bit block size that uses a 192-bit key.
- ARIA256: A 128-bit block size that uses a 256-bit key.
- CHACHA20POLY1305: Arbitrary length, 96-bit nonce, and 256-bit key.

- DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
- NULL: Do not use an encryption algorithm.
- SEED: A 16-round Feistel network with 128-bit blocks and a 128-bit key.

Select either of the following authentication message digests to check the authenticity of messages during phase 1 negotiations:

- NULL: Do not use a message digest.
- MD5: Message Digest 5, the hash algorithm developed by RSA Data Security.
- SHA1: Secure Hash Algorithm 1, which produces a 160-bit message digest.
- SHA256: Secure Hash Algorithm 2, which produces a 256-bit message digest.
- SHA384: Secure Hash Algorithm 3, which produces a 384-bit message digest.
- SHA512: Secure Hash Algorithm 3, which produces a 512-bit message digest.

Note: If the encryption is GCM or CHACHA20POLY1305, no authentication options can be selected.

To specify more combinations, use the Add button beside any of the table rows.

#### VPN Zone

Select to create VPN zones. When enabled, you can select to create default or custom zones. When disabled, no VPN zones are created.

#### Create Default Zones

Select to have default zones created for you.

#### Use Custom Zone

Select to choose what zones to create.

#### IKE Security Phase 1 Advanced Properties

##### Diffie Hellman Group(s)

Select one or more of the following Diffie-Hellman (DH) groups: *1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 27, 28, 29, 30, 31*.

At least one of the DH group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations.

Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode.

##### Exchange Mode

Select either *Aggressive* or *Main (ID Protection)*.

The FortiGate unit and the remote peer or dialup client exchange phase 1 parameters in either *Main (ID Protection)* or *Aggressive* mode. This choice does not apply if you use IKE version 2, which is available only for route-based configurations.

- In Main mode, the Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information
- In Aggressive mode, the Phase 1 parameters are exchanged in single message with authentication information that is not encrypted.

	Although Main mode is more secure, you must select Aggressive mode if there is more than one dialup Phase 1 configuration for the interface IP address, and the remote VPN peer or client is authenticated using an identifier local ID). Descriptions of the peer options in this guide indicate whether Main or Aggressive mode is required.
<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: <i>1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 27, 28, 29, 30, 31</i>.</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 300](#) for information.

To view IPsec VPN community details:

1. Go to *VPN Manager > IPsec VPN*.
2. Select a community from the tree menu, or double-click on a community in the content pane. The community information pane opens.

Seq.#	Name	Role	Default VPN Interface	Protected Subnet
1	FGT54_2[root]	Spoke	wan2	10.2.1.0
2	FGT54_2[root]	Spoke	wan1	10.2.1.0
3	FGT54_1[root]	Hub	wan1	10.1.1.0
4	FGT54_1[root]	Hub	wan2	10.1.2.0

3. Select *All VPN Communities* in the tree menu 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*.
2. Do one of the following:
  - Double-click on a community or select it in the tree menu, then click *Edit* in the quick status bar or select *VPN Community > Edit*.
  - Right-click on a community and select *Edit* from the menu.
  - Select a community, then 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 292](#).

## 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*.
2. Do one of the following:
  - Select the community in the tree, then select *VPN Community > Delete*.
  - Select the community or communities from the content pane list, then click *Delete* in the toolbar.
  - Select the community or communities from the content pane list or tree menu, then right-click and select *Delete*.
3. Select *OK* in the confirmation box to delete the VPN community or communities.

## Monitoring IPsec VPN tunnels

Go to *VPN Manager > 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>Refresh</span> <span>Bring Tunnel Up</span> <span>Bring Tunnel Down</span> <span>Column Settings</span> <span></span>							
<input type="checkbox"/>	Status	Device	Name	Type	Remote Gateway	Incoming Data	Phase 2 Proposal Uptime
<input type="checkbox"/>	Up	FGT54_1[root]	dual-I_1_3	automatic	100.64.54.2	0.0 KB	1 1d 20h 39m 55s
<input type="checkbox"/>	Down	FGT54_1[root]	dual-I_1_4	automatic	100.64.154.2	0.0 KB	1 2s
<input type="checkbox"/>	Down	FGT54_1[root]	dual-I_2_3	automatic	100.64.54.2	0.0 KB	1 2s
<input type="checkbox"/>	Down	FGT54_1[root]	dual-I_2_4	automatic	100.64.154.2	0.0 KB	1 15s
<input type="checkbox"/>	Up	FGT54_2[root]	dual-I_3_1	automatic	100.64.54.1	0.0 KB	1 1d 20h 39m 51s
<input type="checkbox"/>	Down	FGT54_2[root]	dual-I_3_2	automatic	100.64.154.1	0.0 KB	1 2s
<input type="checkbox"/>	Down	FGT54_2[root]	dual-I_4_1	automatic	100.64.54.1	0.0 KB	1 3s
<input type="checkbox"/>	Down	FGT54_2[root]	dual-I_4_2	automatic	100.64.154.1	0.0 KB	1 11s

### To bring tunnels up or down:

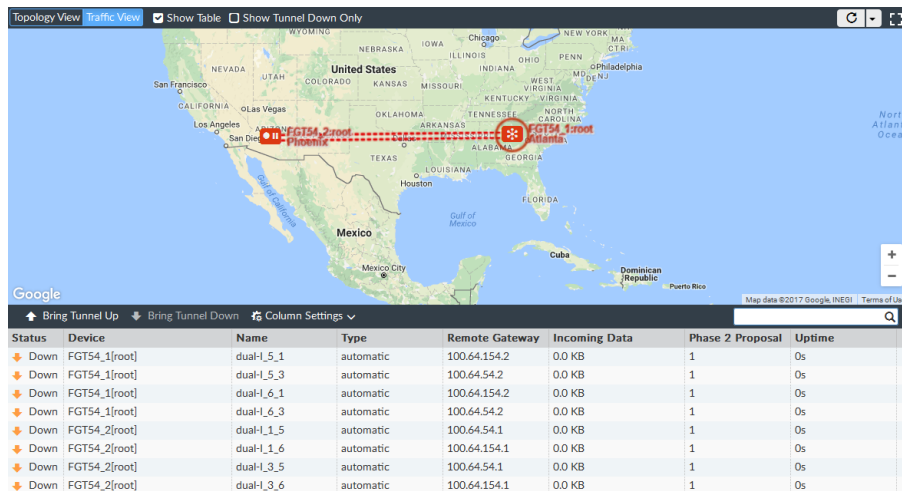
1. Go to *VPN Manager > Monitor*.
2. Find and select the tunnel or tunnels that you need to bring up or down in the list.

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.

## 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 300</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 300</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 298</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>
<b>Refresh</b>	Click to refresh the map view, or click the down arrow and select a refresh rate from the dropdown menu.
<b>Toggle Full Screen</b>	Click to view the map in full screen mode. Press <i>Esc</i> to return to the windowed view.



If necessary, the location of a device can be manually configured when editing the device; see [Editing device information on page 70](#).

## 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 tree menu, or double-click on a community in the list, to manage the VPN gateways in that community.

Star

Name : dual-I  
 Number of VPN : 4  
 Authentication: Pre-shared Key

IKE Security (Phase 1) Properties: 3des-sha1, 3des-md5  
 IPsec Security (Phase 2) Properties: 3des-sha1, 3des-md5

Edit

Seq.#	Name	Role	Default VPN Interface	Protected Subnet
<input type="checkbox"/> 1	FGT54_2[root]	Spoke	wan2	10.2.1.0
<input type="checkbox"/> 2	FGT54_2[root]	Spoke	wan1	10.2.1.0
<input type="checkbox"/> 3	FGT54_1[root]	Hub	wan1	10.1.1.0
<input type="checkbox"/> 4	FGT54_1[root]	Hub	wan2	10.1.2.0

The following options are available:

<b>Create New</b>	Create a new managed or external gateway. See <a href="#">Creating managed gateways on page 300</a> and <a href="#">Creating external gateways on page 305</a> for more information.
<b>Edit</b>	Edit the selected gateway. See <a href="#">Editing an IPsec VPN gateway on page 306</a> .
<b>Delete</b>	Delete the selected gateway or gateways. See <a href="#">Deleting VPN gateways on page 306</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 305](#).

**To create a managed gateway:**

1. Go to *VPN Manager > IPsec VPN*.
2. Select a community from the tree menu, 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 dropdown 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 device from the dropdown list.
<b>Default VPN Interface</b>	Select the interface to use for this gateway from the dropdown 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, or 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 dropdown 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 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>XAUTH Type</b>	<p>Select the XAUTH type: <i>Disable</i>, <i>PAP Server</i>, <i>CHAP Server</i>, or <i>AUTO Server</i>.</p> <p>This option is only available for dial up topologies.</p>
<b>User Group</b>	<p>Select the authentication user group from the dropdown list.</p> <p>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>.</p> <p>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.</p>
<b>Enable IKE Configuration Method ("mode config")</b>	<p>Select to enable or disable IKE configuration method.</p> <p>This option is only available for dial up topologies.</p>
<b>Enable IP Assignment</b>	<p>Select to enable or disable IP assignment.</p> <p>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.</p>
<b>IP Assignment Mode</b>	<p>Select the IP assignment mode: <i>Range</i> or <i>User Group</i>.</p> <p>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.</p>
<b>IP Assignment Type</b>	<p>Select the IP assignment type: <i>IP</i> or <i>Subnet</i>.</p> <p>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.</p>
<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*.
2. Select a community from the tree menu, 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)</i> , or <i>Automatic</i> . This option is only available for full meshed and star topologies.
<b>Peer Type</b>	Select one of the following: <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> A Local ID is an alphanumeric value assigned in the Phase 1 configuration. The local ID of a peer is called a Peer ID. The Local ID or peer ID can be used to uniquely identify one end of a VPN tunnel, enabling a more secure connection. If you have multiple VPN tunnels negotiating, this ensures the proper remote and local ends connect.

When you configure the ID on your end, it is your local ID. When the remote end connects to you, they see it as your peer ID. If you are debugging a VPN connection, the local ID is part of the VPN negotiations. You can use it to help troubleshoot connection problems.

The default configuration is to accept all local IDs (peer IDs). If your local ID is set, the remote end of the tunnel must be configured to accept your ID.

This option is only available for dial up topologies.

<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*.
2. Select a community from the tree menu, or double-click on a community in the list.
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*.
2. Select a community from the tree menu, or double-click on a community in the list.
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.

## 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 173](#) for information on creating policies on your FortiManager.

## 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.

## Manage SSL VPNs

Go to *VPN Manager > SSL VPN* to manage SSL VPNs.

+ Create New Edit Delete Column Settings			
Device	Interface	Port	Certificate
<input type="checkbox"/> FGT54_1	loop1,port1	10443	Fortinet_SSL
<input type="checkbox"/> FGT54_2	loop1,port1	10443	Fortinet_SSL

The following options are available:

<b>Add SSL VPN</b>	Create a new SSL VPN with the <i>Create SSL VPN</i> dialog box. See <a href="#">Creating SSL VPNs on page 309</a> .
<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</i> pane. This option is also available from the right-click menu. See <a href="#">Creating SSL VPNs on page 309</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 310</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 310</a> .
<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*.
2. Click *Add SSL VPN*, or click *Create New* in the content toolbar. The *Create SSL VPN* dialog box or pane is displayed.

**Create New SSL VPN Settings**

Device: Click to select

**Connection Settings**

Listen on Interface(s): Click here to select

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: ON

WINS Server #1: IP

WINS Server #2: IP

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>	<p>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).</p> <p>This setting applies to the SSL VPN session. The interface does not time out when web application sessions or tunnels are up.</p>

<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 94</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> : <a href="https://help.fortinet.com/cli/fos60hlp/60/index.htm">https://help.fortinet.com/cli/fos60hlp/60/index.htm</a> .

## 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*.
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 *Create SSL VPN* 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*.
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

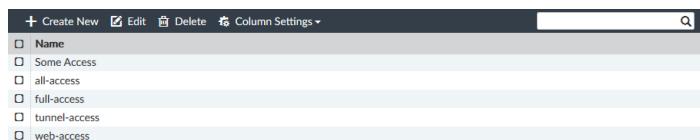
The SSL VPN portal enables remote users to access internal network resources through a secure channel using a web browser. FortiGate administrators can configure login privileges for system users as well as the network resources that are available to the users.

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* and select *Portal Profiles* in the tree menu.



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* and select *Portal Profiles* in the tree menu.
2. Click *Create New* in the toolbar, or right-click and select *Create New*. The *Create New* 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.

Name	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 314</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* and select *Portal Profiles* in the tree menu.
2. Edit an existing profile, or create a new profile. See [Editing portal profiles on page 316](#) or [Creating SSL VPN portal profiles on page 311](#).
3. Click *Create New* in the *Pre-Defined Bookmark* field. *Enable Web Mode* must be selected for this field to be available. The *Create New Bookmark* dialog box opens. The available options will vary depending on the selected type.

4. Configure the following settings, then select **OK** to create the bookmark.

<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>	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> . This option is only available when <i>Type</i> is <i>RDP</i> .
<b>Security</b>	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> . This option is only available when <i>Type</i> is <i>RDP</i> .
<b>Description</b>	Optionally, enter a description of the bookmark.
<b>Single Sign-on</b>	Select the SSO setting for links that require authentication: <i>Disabled</i> , <i>Automatic</i> , or <i>Static</i> . 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. When including a link using SSO use the entire URL, not just the IP address.

This option is only available when *Type* is *Citrix*, *FTP*, *HTTP/HTTPS*, *RDP*, or *SMB*.

The *Static* option is only available when *Type* is *Citrix*, *HTTP/HTTPS*, or *RDP*.

#### To edit a bookmark:

1. Go to *VPN Manager* > *SSL-VPN* and select *Portal Profiles* in the tree menu.
2. Edit an existing profile, or create a new profile. See [Editing portal profiles on page 316](#) or [Creating SSL VPN portal profiles on page 311](#).
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* and select *Portal Profiles* in the tree menu.
2. Edit an existing profile, or create a new profile. See [Editing portal profiles on page 316](#) or [Creating SSL VPN portal profiles on page 311](#).
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* and select *Portal Profiles* in the tree menu.
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* and select *Portal Profiles* in the tree menu.
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.

## Monitor SSL VPNs

SSL VPNs can be monitored by going to *VPN Manager* > *SSL VPN* and selecting *Monitor* from the tree menu.



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.

# Access Points

Use *AP Manager* to manage FortiAP access points.

The AP Manager pane includes the following tabs:

<b>Managed APs</b>	Displays unauthorized and authorized FortiAP devices. You can view, authorize, and edit authorized FortiAP devices.
<b>Monitor</b>	Monitor FortiAP devices and the clients connected to them.
<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</b>	View, create, edit, and import AP profiles, SSIDs, and WIDS profiles.

The AP Manager pane allows you to manage, configure, and assign profiles to FortiAP devices. You can configure multiple profiles that can be assigned to multiple devices. Profiles are installed to devices when you install configurations to the devices.

In central management mode, WiFi templates share a common database. Templates can be applied to any device, regardless of which FortiGate controller it is connected to. In per-device mode, all FortiAP devices and WiFi templates (SSIDs, WIDS profiles, and AP profiles) are managed at the device level – there are no shared objects. The monitor and map view tabs will only show information for FortiAP devices connected to the selected FortiGate controller. The mode can be changed by editing the ADOM that contains the FortiGate controllers ([Creating ADOMs on page 456](#)).

The following steps provide an overview of using AP management to configure and install profiles:

1. Create AP profiles.  
See [WiFi profiles on page 334](#).
2. Assign profiles to FortiAP devices.  
See [Assigning profiles to FortiAP devices on page 326](#).
3. 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 [Configuring a device on page 56](#).

## Managed APs

The *Managed APs* pane allows you to manage FortiAP devices that are controlled by FortiGate devices that 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 platform based groups within a controller.

FortiAP devices can be managed centrally, or per-device (see [Creating ADOMs on page 456](#)). 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 463](#).

Go to **AP Manager > Managed APs** to manage FortiAP devices. Managed APs are organized by their FortiGate controller and group. In per-device mode, there is no **All\_FortiGate** group.

#	Access Point	Connected Via	SSIDs	Channel	Clients	OS Version	AP Profile
1	FP320B3X13000000	192.168.100.116	Radio 1: Radio 1: 0 Radio 2: Radio 2: 0	Radio 1: 0 Radio 2: 0	Radio 1: 0 Radio 2: 0	FP320B-v5.4-build0371	
2	FP320B3X13000000		Radio 1: Radio 1: 0 Radio 2: Radio 2: 0	Radio 1: 0 Radio 2: 0	Radio 1: 1 Radio 2: 0		
3	FP320C3X15000000	192.168.100.112	Radio 1: Radio 1: 6 Radio 2: Radio 2: 132	Radio 1: 1 Radio 2: 0	Radio 1: 1 Radio 2: 0	FP320C-v5.6-build0476	
4	FP320C3X15000000	192.168.100.111	Radio 1: Radio 1: 6 Radio 2: Radio 2: 136	Radio 1: 0 Radio 2: 1	Radio 1: 0 Radio 2: 1	FP320C-v5.6-build0476	
6	PS223E3X17000000	192.168.1.122	Radio 1: Radio 1: 11 Radio 2: Radio 2: 36	Radio 1: 0 Radio 2: 2	Radio 1: 0 Radio 2: 2	PS223E-v5.4-build4137	
7	PS311C3U15000000	192.168.1.120	Radio 1: Radio 1: 36 Radio 2: Radio 2: 0	Radio 1: 0 Radio 2: 0	Radio 1: 0 Radio 2: 0	PS311C-v5.4-build0155	
5	PU421E3X16000000	192.168.100.113	Radio 1: Radio 1: 0 Radio 2: Radio 2: 0	Radio 1: 0 Radio 2: 0	Radio 1: 2 Radio 2: 0	PU421E-v5.4-build0035	

## Quick status bar

You can quickly view the status of devices on the **Managed AP** pane by using the quick status bar, which contains the following options:

- Managed APs
- Online
- Offline
- Unauthorized
- Rogue APs
- Client Connected

You can click each quick status to display in the content pane, or in a pop-up window, only the devices referenced in the quick status.

### To view the quick status bar:

1. Ensure that you are in the correct ADOM.
2. Go to **AP Manager > Managed APs**. The quick status bar is displayed above the content pane.

3. In the tree menu, select a FortiGate, group, or **All\_FortiGate** if central management is enabled. The devices for the group are displayed in the content pane, and the quick status bar updates.

- Click on each quick status to filter the devices displayed on the content pane. For example, click *Offline*, and the content pane will display only devices that are currently offline.
- Click *Rogue APs* to open the rogue AP list in a pop-up window.
- Click *Client Connected* to open a list of WiFi clients in a pop-up window.

## Managing APs

FortiAP devices can be managed from the content pane below the quick status bar on the *AP Manager > Managed APs* pane.

<a href="#">+ Create New</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Assign Profile</a> <a href="#">More</a> <a href="#">Column Settings</a>								
#	Access Point	Connected Via	SSIDs	Channel	Clients	OS Version	AP Profile	
1	FP320B3X00000000	192.168.100.116	Radio 1: Radio 2:	Radio 1: 0 Radio 2: 0	Radio 1:2 Radio 2:2	FP320B-v5.4-build0371		
2	FP320B3X00000000		Radio 1: Radio 2:	Radio 1: 0 Radio 2: 0	Radio 1:0 Radio 2:0			
3	FP320C3X00000000	192.168.100.112	Radio 1: Radio 2:	Radio 1: 6 Radio 2: 132	Radio 1:1 Radio 2:0	FP320C-v5.6-build0476		
4	FP320C3X00000000	192.168.100.111	Radio 1: Radio 2:	Radio 1: 6 Radio 2: 136	Radio 1:0 Radio 2:2	FP320C-v5.6-build0476		
6	PS223E3X00000000	192.168.1.122	Radio 1: Radio 2:	Radio 1: 6 Radio 2: 36	Radio 1:0 Radio 2:0	PS223E-v5.4-build4137		
7	PS311C3U00000000	192.168.1.123	Radio 1: Radio 2:	Radio 1: 165 Radio 2: 0	Radio 1:2 Radio 2:0	PS311C-v5.4-build0155		
5	PU421E3X00000000	192.168.100.113	Radio 1: Radio 2:	Radio 1: 0 Radio 2: 0	Radio 1:0 Radio 2:0	PU421E-v5.4-build0035		

The following options are available from the toolbar and right-click menu:

<b>Create New</b>	Add an AP.
<b>Edit</b>	Edit the selected AP.
<b>Delete</b>	Delete the selected AP.
<b>Assigned 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 326</a> .
<b>Column Settings</b>	Click to select which columns to display or select <i>Reset to Default</i> to display the default columns.
<b>Authorize</b>	<p>Authorize an AP. See <a href="#">Authorizing and deauthorizing FortiAP devices on page 326</a>.</p> <p>This option is also available in the toolbar by selecting <i>More</i>.</p>
<b>Deauthorize</b>	<p>Deauthorize an AP. See <a href="#">Authorizing and deauthorizing FortiAP devices on page 326</a>.</p> <p>This option is also available in the toolbar by selecting <i>More</i>.</p>
<b>Grouping</b>	<p>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 325</a>.</p> <p>This option is only available in the right-click menu.</p>
<b>Upgrade</b>	<p>Upgrade the AP. The AP must already be authorized.</p> <p>You can also select two or more AP devices of the same model and upgrade the devices at the same time.</p>

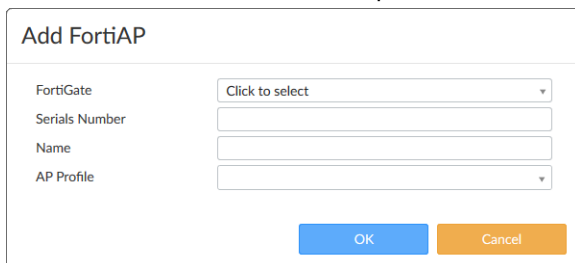
	Before upgrading FortiAP, go to <i>FortiGuard &gt; Firmware Images &gt; Product: FortiAP</i> and click the download icon to manually download the firmware images.
<b>Restart</b>	Restart the AP. This option is only available in the toolbar, by selecting <i>More</i> .
<b>Refresh</b>	Refresh the AP list, or refresh the selected FortiAP devices.
<b>View Clients</b>	View the clients connected to the AP. See <a href="#">Connected clients on page 328</a> .
<b>View Rogue APs</b>	View the Rogue APs. See <a href="#">Rogue APs on page 327</a> . This option is only available in the toolbar, by selecting <i>More</i> .
<b>Show on Google Map</b>	Show the selected AP on Google Map. See <a href="#">Google map on page 331</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 332</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. This option is only available in the toolbar.

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>Connected Via</b>	The IP address 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 328</a> .
<b>OS Version</b>	The OS version on the FortiAP.
<b>AP Profile</b>	The AP Profile assigned to the device, if any.
<b>Comments</b>	User entered comments.
<b>Country</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:**

1. Click *Create New* on the content pane toolbar. The *Add FortiAP* dialog box opens.

The image shows a dialog box titled "Add FortiAP". It contains four input fields: "FortiGate" with a dropdown menu showing "Click to select", "Serials Number" with a text input field, "Name" with a text input field, and "AP Profile" with a dropdown menu. At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (orange).

2. 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="#">AP profiles on page 334</a> .

**To edit FortiAP devices:**

1. In the tree menu, select the group or FortiGate that contains the FortiAP device to be edited.
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.

### Config FortiAP - PS223E3X17000000

Serial Number PS223E3X17000000

Name PS223E3X17000000

Comments  0/35

**Managed AP Status**

Status Online [Restart](#)

Connected Via Ethernet (192.192.1.192)

Base MAC Address 7f:aac:c4d:zed:f3

Join Time 15/15/18 14:56

Clients 68

State Authorized

WTP Mode Normal

Current PS223E-v5.4-build4137 [Upgrade](#)

FortiAP Profile 223e-ps-p

Bonjour Profile bon-test

**Override Radio 1**

Band ☒ 2.4GHz 802.11n/g

2.4 GHz 802.11g/b

Channels ☒ 1 ☐ 2 ☐ 3 ☐ 4  
☐ 5 ☒ 6 ☐ 7 ☐ 8  
☐ 9 ☐ 10 ☒ 11

TX Power Control ☒ 100%  
   
0%  100%

SSIDs ☒ ssid-22

**Override Radio 2**

Band  5GHz 802.11ac/n/a

Channels  (Automatically assigned)

TX Power Control  100%

SSIDs  ssid-22

**Override AP Login Password**

AP Login Password

**Advanced Options** >

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. See <a href="#">Firmware Management on page 88</a>
<b>FortiAP Profile</b>	Select a profile from the dropdown list (see <a href="#">AP profiles on page 334</a> )
<b>Bonjour Profile</b>	Select a profile from the dropdown list (see <a href="#">Bonjour profiles on page 356</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, select the group or FortiGate that contains the FortiAP device to be deleted.
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 *Delete* from the toolbar, or right-click on the FortiAP and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the AP.



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, select the group or FortiGate that contains the FortiAP device to be upgraded.
2. Select two or more FortiAP devices of the same model in the list in the content pane.
3. Right-click on 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 based on FortiAP platforms. A group can only contain one model of FortiAP. A FortiAP can only belong to one group.

Groups are listed in the tree menu under the FortiGate they were created in. They can be created, edited, and deleted as needed.

**To create a FortiAP group:**

1. In the *Managed APs* pane, select *FortiAP Group > Create New* from the toolbar. The *Create New FortiAP Group* dialog box opens.

2. 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>Platform</b>	Select the FortiAP platform that the group will apply to.
<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.

3. Select *OK* to create the group.

**To edit a group:**

1. In the *Managed APs* pane, select a group from the tree menu, then select *FortiAP Group > Edit* from the toolbar.
2. Edit the group name and devices in the group as needed. The FortiGate and the platform cannot be changed.
3. Select *OK* to apply your changes.

**To delete a group:**

1. In the *Managed APs* pane, select a group from the tree menu.
2. Select *FortiAP Group > Delete* from the toolbar.
3. Select *OK* in the confirmation dialog box to delete the group.

## Authorizing and deauthorizing FortiAP devices

**To authorize FortiAP devices:**

1. In the tree menu, select the group or FortiGate that contains the unauthorized FortiAP devices.
2. In the quick status bar, click *Unauthorized*. The unauthorized FortiAP devices are displayed in the content pane.
3. Select the FortiAP devices and either click *More > Authorize* from the toolbar, or right-click and select *Authorize*.
4. Select *OK* in the confirmation dialog box to authorize the selected devices.

**To deauthorize FortiAP devices:**

1. In the tree menu, select the group or 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*.
3. Select *OK* in the confirmation dialog box to deauthorize the selected devices.

## 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 [AP profiles on page 334](#).

**To assign profiles to FortiAP devices:**

1. In the tree menu, select the group or FortiGate that contains the FortiAP device the profile will be applied to.
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 *Assigned Profile* from the toolbar, or right-click on the FortiAP and select *Assigned Profile*. The *Assign AP Profile* window opens.
4. Select a FortiAP profile from the dropdown list, then click *OK* to assign the profile.

**To install FortiAP profiles to devices:**

1. Go to the *Device Manager* pane.
2. Select the FortiGate device that controls the FortiAP device
3. Right click and select *Install Config*, or select *Install > Install Config* from the toolbar.
4. Click *OK* in the confirmation dialog box to install the configuration to the device. See [Configuring a device on page 56](#) for more information.

## Rogue APs

A rogue AP is an unauthorized AP connected to your wired network. This can enable unauthorized access.

Click *Rogue APs* in the quick status bar to open the rogue AP list in a pop-up window.

View Rogue APs

Mark As

Suppress AP

Unsuppress AP

Refresh

Column Settings

Show Offline (198)

Show Accepted (0)

<input type="checkbox"/>	State	Status	SSID	Security Type	Channel	MAC Address	Vendor Info	Signal Strength	Detected By	On-Wire
<input type="checkbox"/>	<div>?</div>	<div>⬆</div>	fortinet	WPA2 Personal	6	70:4ca5:99:da:22	Fortinet, Inc.	<div>-47dBm</div>	PS311C3U15000439(192.168.1.111:5246)	<div>⬇</div>
<input type="checkbox"/>	<div>?</div>	<div>⬆</div>	FTNT-Guest	WPA2 Personal	6	70:4ca5:a3:87:e0	Fortinet, Inc.	<div>-55dBm</div>	PS311C3U15000439(192.168.1.111:5246)	<div>⬇</div>
<input type="checkbox"/>	<div>?</div>	<div>⬆</div>	FTNT-Staff	WPA2 Enterprise	6	70:4ca5:a3:87:e1	Fortinet, Inc.	<div>-56dBm</div>	PS311C3U15000439(192.168.1.111:5246)	<div>⬇</div>
<input type="checkbox"/>	<div>?</div>	<div>⬆</div>	DLI_EPCR580	WPA Personal	11	7ce1ff:01:09:b0	Computer	<div>-55dBm</div>	PS311C3U15000439(192.168.1.111:5246)	<div>⬇</div>
<input type="checkbox"/>	<div>?</div>	<div>⬆</div>	iPADS	WPA2 Personal	100	90:6cac:28:89:a8	Fortinet, Inc.	<div>-13dBm</div>	PS311C3U15000439(192.168.1.111:5246)	<div>⬇</div>
<input type="checkbox"/>	<div>?</div>	<div>⬆</div>	fortinet	WPA2 Personal	11	90:6cac:7c:9b:aa	Fortinet, Inc.	<div>-64dBm</div>	PS311C3U15000439(192.168.1.111:5246)	<div>⬇</div>
<input type="checkbox"/>	<div>?</div>	<div>⬆⚠</div>	fortinet35	WPA/WPA2 Pers	6	90:6cac:a4:37:76	Fortinet, Inc.	<div>-23dBm</div>	PS311C3U15000439(192.168.1.111:5246)	<div>⬇</div>
<input type="checkbox"/>	<div>?</div>	<div>⬆</div>	GuestWireless	WPA2 Personal	100	a2:6cac:28:89:a8		<div>-14dBm</div>	PS311C3U15000439(192.168.1.111:5246)	<div>⬇</div>
<input type="checkbox"/>	<div>?</div>	<div>⬆</div>	LB_CP	OPEN	6	a2:6cac:28:89:e8		<div>-10dBm</div>	PS311C3U15000439(192.168.1.111:5246)	<div>⬇</div>
<input type="checkbox"/>	<div>?</div>	<div>⬆</div>	StaffWireless	WPA2 Personal	6	b2:6cac:1b:72:be		<div>-17dBm</div>	PS311C3U15000439(192.168.1.111:5246)	<div>⬇</div>
<input type="checkbox"/>	<div>?</div>	<div>⬆</div>	StaffWireless	WPA2 Personal	1	b2:6cac:25:d4:64		<div>-22dBm</div>	PS311C3U15000439(192.168.1.111:5246)	<div>⬇</div>
<input type="checkbox"/>	<div>?</div>	<div>⬆</div>	StaffWireless	WPA2 Personal	100	b2:6cac:28:89:a8		<div>-14dBm</div>	PS311C3U15000439(192.168.1.111:5246)	<div>⬇</div>
<input type="checkbox"/>	<div>?</div>	<div>⬆</div>	demo-112	WPA2 Personal	100	c2:6cac:28:89:a8		<div>-13dBm</div>	PS311C3U15000439(192.168.1.111:5246)	<div>⬇</div>
<input type="checkbox"/>	<div>?</div>	<div>⬆</div>	fortinet	WPA2 Personal	6	e8:1cba:39:97:fa		<div>-64dBm</div>	PS311C3U15000439(192.168.1.111:5246)	<div>⬇</div>
<input type="checkbox"/>	<div>?</div>	<div>⬆</div>	fortinetsz2	WPA2 Personal	1	e8:1cba:39:a2:32		<div>-65dBm</div>	PS311C3U15000439(192.168.1.111:5246)	<div>⬇</div>
<input type="checkbox"/>	<div>?</div>	<div>⬆</div>	fortinet	WPA2 Personal	11	e8:1cba:51:cb:1a		<div>-48dBm</div>	PS311C3U15000439(192.168.1.111:5246)	<div>⬇</div>

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. 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>	The state of the AP: <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.

## Connected clients

To view connected wireless clients, click *Client Connected* in the quick status bar to open the WiFi client list in a pop-up window that lists all the clients in the selected FortiGate or group.

To view the clients connected to specific APs, select the APs in the content pane, then right-click on them and select *View Clients*.

View WiFi Clients									
Column Settings -									
#	SSID	FortiAP	IP	Device	Channel	Bandwidth TX/RX	Signal Strength/Noise	Signal Strength	Association Time
1	fortinet26	320c-146	10.1.26.2	8-34-bf911e-d8-34	6	0 kbps	36 dB	-59dBm	05/13/18 03:01

The following columns are available:

<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>IP</b>	The IP address assigned to the wireless client.
<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.

## Monitor

The *Monitor* pane includes a listing of connected clients, and a health monitor that display information about all the APs for the selected FortiGate or group in widgets.

### Clients Monitor

The client monitor lists information about connected clients. Go to *AP Manager > Monitor* and select the *Clients Monitor* tab in the content pane to view the list. Select a specific FortiGate or group in the tree menu to filter the listed clients.

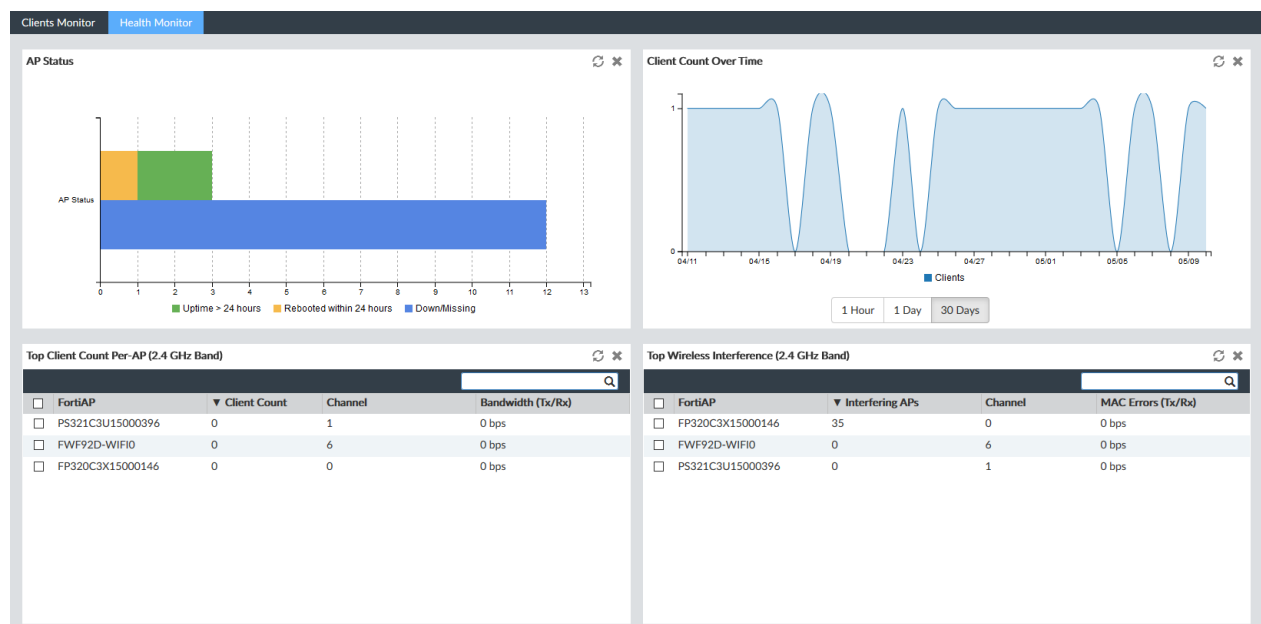
You can search the table by entering a search term in the search field in the toolbar. The visible columns can be adjusted by selecting *Column Settings* in the toolbar. The following columns are available:

<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>IP</b>	The IP address assigned to the wireless client.
<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.

## Health Monitor

Go to *AP Manager > Monitor*, select a FortiGate or group from the tree menu, and select the *Health Monitor* tab in the content pane to open the health monitor.



Widgets can be moved by clicking and dragging their title bar into different locations on the screen. The information in the widgets can be refreshed by clicking the refresh icon in the widget title bar. Widgets with tables can be sorted by any column by clicking the column name.

The following widgets are shown:

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>

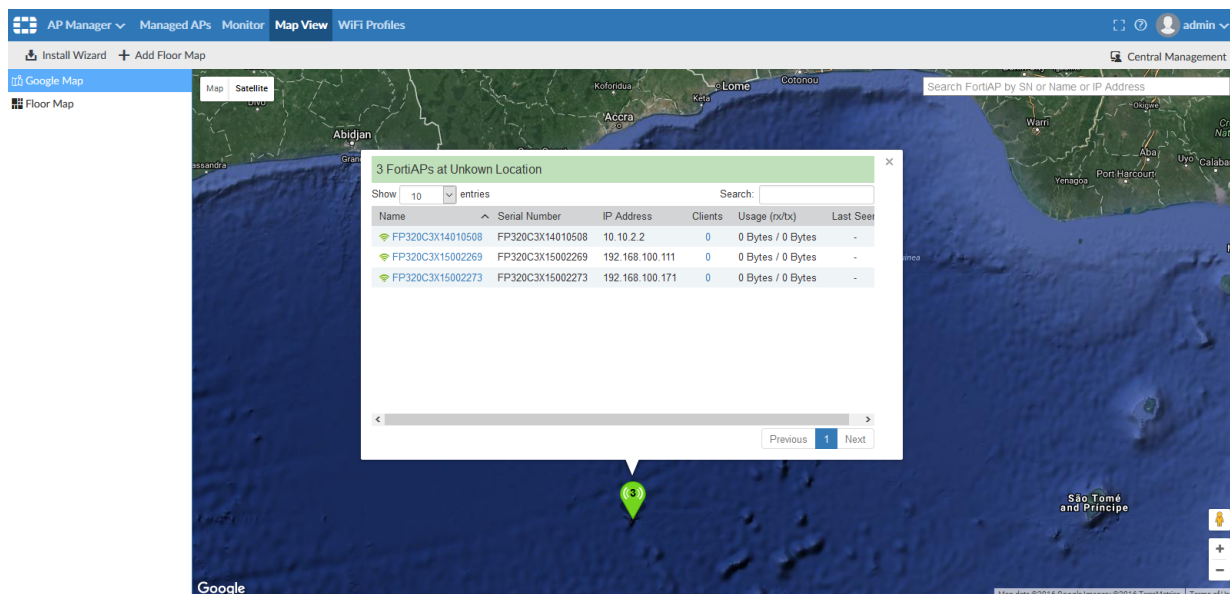
## Map view

The Map View shows the FortiAP devices in two ways:

- Google Map - shows the FortiAP devices placed on Google Maps. See [Google map on page 331](#)
- Floor Map - create a floor map, add an image of a floor map, and place the FortiAP devices on the map. See [Floor map on page 332](#)

## 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.



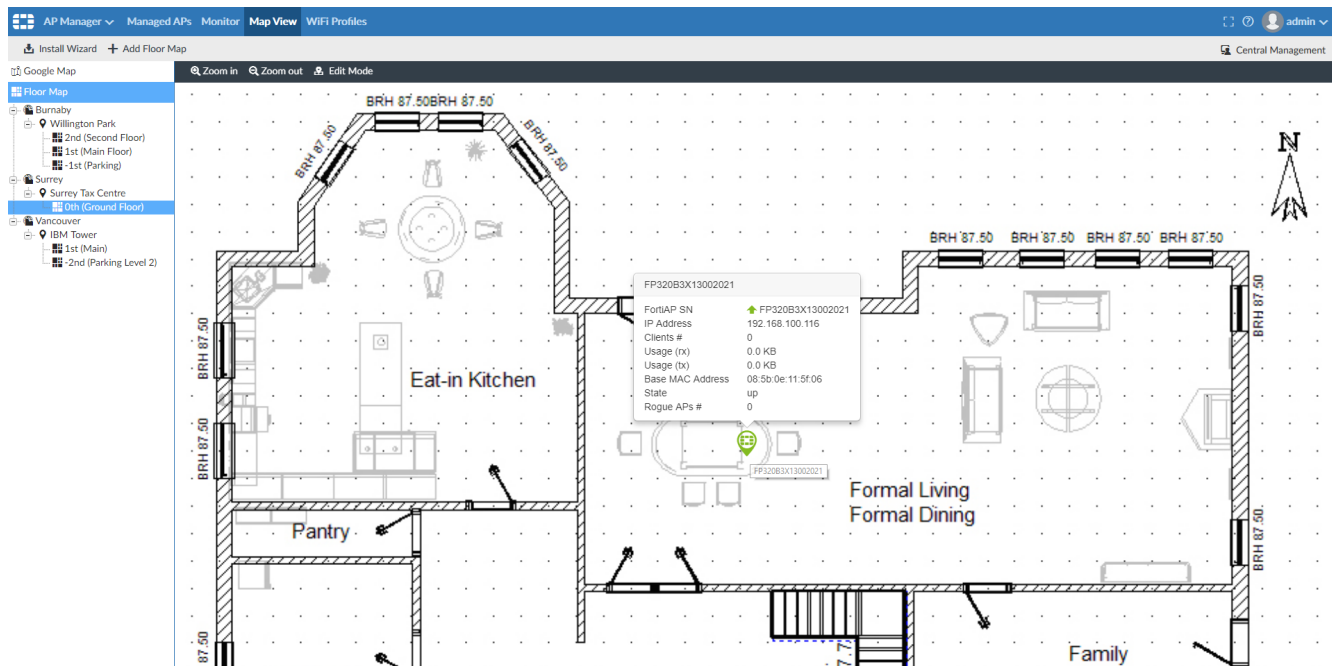
Clicking on a map pin opens a list of the APs connected to that FortiGate. Clicking on the name of an AP from the list will zoom the map into that location and provide further information about the AP, including the serial number, IP address, number of clients, usage, and the last time the AP was seen if it is offline.

Click on the number of client to open the *View WiFi Clients* window (see [Connected clients on page 328](#)). Click on the AP's serial number to open the *Config FortiAP* window, where you can edit the AP settings (see [Managing APs on page 320](#)).

## 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. Click **Add Floor Map**.
2. In the **Add Floor Map** screen, specify the following and click **Next**:
  - Location - select a location or specify a new one.
  - Building - select a building or specify a new one.
3. Specify the **Address** and click **Next**.
4. Specify the following and click **Finish**:
  - Floor Description - specify a description for the floor. This is displayed as the name of the floor map.
  - Floor Index - specify a numeric value. The floors are sorted from highest to lowest based on the Floor Index.
  - Contact - specify a contact name.
  - Phone Number - specify a phone number for this location.
  - Floor Map - upload a file by dragging and dropping here or click **Browse** to select an image of your floor map.

### To position FortiAP devices on the floor map:

1. Click **Floor Map** > [Floor Map name].
2. Click the image of the floor map.
3. Click **Edit Mode** to list the FortiAP devices in the **Positioning APs** pane.
4. Drag and drop the FortiAP devices from the **Positioning APs** pane to the image of the floor map.
5. Click **Save and Return**.  
The FortiAP device is now shown on the floor map.

### To view the properties of a FortiAP device:

1. Click **Floor Map** > [Floor Map name].
2. Click the image of the floor map.

3. Hover over the FortiAP device to view the following details:

- FortiAP Serial Number
- IP Address
- Number of Clients connected
- Usage
- Base MAC Address
- State
- Rogue APs

**To remove FortiAP devices from the floor map:**

1. Click *Floor Map* > *[Floor Map name]*.
2. Click the image of the floor map.
3. Click *Edit Mode*.
4. Right-click the FortiAP device and select *Remove from Floor Map*.
5. Click *Save and Return*.

The FortiAP device is now removed from the Floor Map and added to the *Positioning APs* pane.

## WiFi profiles

The *WiFi Profiles* pane allows you to create and manage SSIDs, and AP, Wireless Intrusion Detection System (WIDS), Bluetooth, Quality of Service (QoS), and Bonjour profiles that can be assigned to managed FortiAP devices.

In per-device mode, templates are not shared between devices.



Settings may vary for different ADOM versions.

---

## AP profiles

AP profiles define radio settings for FortiAP models. The profile specifies details such as the operating mode of the device, SSIDs, and transmit power. Custom AP profiles can be created as needed for new devices.

To view AP profiles, ensure that you are in the correct ADOM, go to *AP Manager > WiFi Profiles*, and select *AP Profile* in the tree menu.

Seq.#	Name	Platform	Radio 1	Radio 2	Comment
1	11ac-only	FortiWiFi local radio	802.11acn only		
2	11n-only	FortiWiFi local radio	802.11gn only		
3	AP-11N-default	Default 11n AP	802.11gn only		
4	FAP112B-default	FAP112B	802.11gn only		
5	FAP112D-default	FAP112D	802.11gn only		
6	FAP11C-default	FAP11C	802.11gn only		
7	FAP14C-default	FAP14C	802.11gn only		
8	FAP210B-default	FAP210B	802.11gn only		
9	FAP21D-default	FAP21D	802.11gn only		
10	FAP220B-default	FAP220B/221B	802.11an_5G	802.11gn only	
11	FAP221C-default	FAP221C	802.11gn only	802.11ac	
12	FAP221E-default	FAP221E	802.11gn only	802.11ac	
13	FAP222B-default	FAP222B	802.11gn only	802.11an_5G	
14	FAP222C-default	FAP222C	802.11gn only	802.11ac	
15	FAP222E-default	FAP222E	802.11gn only	802.11ac	
16	FAP223B-default	FAP223B	802.11an_5G	802.11gn only	
17	FAP223C-default	FAP223C	802.11gn only	802.11ac	
18	FAP223E-default	FAP223E	802.11gn only	802.11ac	

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>Import</b>	Import AP profiles from a connected FortiGate (toolbar only).

### To create custom AP profiles:

1. On the *AP Profile* pane, click *Create New* in the toolbar, or select it from the right-click menu. The *Create New AP Profile* windows opens.

## Create New AP Profile

Name

Comments

Platform

FAP220B/221B

Country/ Region

United States

AP Login Password

Set Leave Unchanged Set Empty

Administrative Access

☐ HTTP ☐ HTTPS ☐ SSH ☐ TELNET

## Radio 1

Mode

Disabled Access Point Dedicated Monitor

WIDS Profile

☐ OFF

Radio Resource Provision

☐ OFF

Client Load Balancing

☐ Frequency Handoff ☐ AP Handoff

Band

5 GHz 802.11n/a

Channel Width

20MHz 40MHz

Short Guard Interval

☐ OFF

Channels

☒ 36 ☒ 40 ☒ 44 ☒ 48  
☒ 149 ☒ 153 ☒ 157 ☒ 161  
☒ 165

TX Power Control

Auto Manual

TX Power

100 %

SSIDs

Auto Manual

Monitor Channel Utilization

☐ OFF

## Radio 2

Mode

Disabled Access Point Dedicated Monitor

WIDS Profile

☐ OFF

Radio Resource Provision

☐ OFF

Client Load Balancing

☐ Frequency Handoff ☐ AP Handoff

Band

2.4 GHz 802.11n/g/b

Channel Width

20MHz

Short Guard Interval

☐ OFF

Channels

☒ 1 ☒ 2 ☒ 3 ☒ 4  
☒ 5 ☒ 6 ☒ 7 ☒ 8  
☒ 9 ☒ 10 ☒ 11

TX Power Control

Auto Manual

TX Power

100 %

SSIDs

Auto Manual

Monitor Channel Utilization

☐ OFF

## Location Based Services

## 2. Enter the following information:

<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>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>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.</li> <li>• <i>Dedicated Monitor</i>: The device is a dedicated monitor. Only the <i>WIDS Profile</i> setting is available.</li> </ul>
<b>WIDS Profile</b>	Select a WIDS profile from the dropdown list. See <a href="#">WIDS profiles on page 348</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>Client Load Balance</b>	Select the client load balancing methods to use: <i>Frequency Handoff</i> and/or <i>AP Handoff</i> .
<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 5GHz 802.11n bands.
<b>Short Guard Interval</b>	Select to enable the short guard interval.
<b>Channels</b>	Select the channel or channels to include. The available channels depend on the selected platform and band.
<b>TX Power Control</b>	Optionally, enable automatic adjustment of transmit power, then specify the minimum and maximum power levels, dBm.
<b>TX Power</b>	If <i>TX Power Control</i> is <i>Manual</i> , enter the TX power in the form of the percentage of the total available power. If <i>TX Power Control</i> is <i>Auto</i> , enter the TX power low and high values, in dBm.
<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>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 IP</b>	FortiPresence server IP address.
<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.

**Advanced Options**

Configure advanced options for the SSID:

- *control-message-offload*: Configure CAPWAP control message data channel offload: *aeroscout-mu*, *aeroscout-tag*, *ap-list*, *ebp-frame*, *sta-list*, *sta-cap-list*, *stats*.
- *dtls-in-kernal*: Enable/disable data channel DTLS in kernel.
- *dtls-policy*: Select the WTP data channel DTLS policy: *clear-text*, *dtls-enabled*, and/or *ipsec-vpn*.
- *energy-efficient-ethernet*: Enable/disable use of energy efficient Ethernet on WTP.
- *ext-info-enable*: Enable/disable station/VAP/radio extension information, providing more detailed statistics for troubleshooting purposes.
- *handoff-roaming*: Enable/disable handoff when a client is roaming.
- *handoff-rssi*: Enter the minimum RSSI handoff value.
- *handoff-sta-thresh*: Enter the threshold value for AP handoff.
- *ip-fragment-preventing*: Prevent IP fragmentation for CAPWAP tunneled control and data packets. Select *tcp-mss-adjust* and/or *icmp-unreachable*.
- *led-schedules*: Recurring firewall schedules for illuminating LEDs on the FortiAP. If *led-state* is enabled, LEDs will be visible when at least one of the schedules is valid.
- *led-state*: Enable/disable use of LEDs on WTP.
- *lldp*: Enable/disable LLDP.
- *max-clients*: Enter the maximum number of STAs supported by the WTP.
- *poe-mode*: Set the WTP, FortiAP, or AP's PoE mode: *auto*, *8023af*, *8023at*, or *power-adapter* (use the power adapter to control the mode).
- *split-tunneling-acl-local-ap-subnet*: Enable/disable split tunneling ACL local AP subnet.
- *tun-mtu-downlink*: Enter the downlink tunnel MTU.
- *tun-mtu-uplink*: Enter the uplink tunnel MTU.
- *wan-port-mode*: Set the WAN port mode: *wan-only* or *wan-lan*.

3. Click *OK* to create the new AP profile.

**To edit a custom AP profile:**

1. Either double-click a profile name, right-click a profile name and select *Edit*, or select a profile then click *Edit* in the toolbar. The *Edit AP Profile* pane opens.
2. Edit the settings as required. The profile name cannot be edited.
3. Click *OK* to apply your changes.

**To delete custom AP profiles:**

1. Select the AP profile or profiles that will be deleted. Default profiles cannot be deleted.
2. Either select *Delete* from the toolbar, or right-click and select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the profile.

**To clone a custom AP profile:**

1. Either select a profile and click *Clone* in the toolbar, or right-click a profile and select *Clone*. The *Clone AP Profile* pane opens.
2. Edit the name of the profile, then edit the remaining settings as required.
3. Click *OK* to clone the profile.

**To import a AP profile:**

1. Click *Import* in the toolbar. The *Import* dialog box opens.
2. Select a FortiGate from the dropdown list. The list will include all of the devices in the current ADOM.
3. Select the profile or profiles to be imported from the dropdown list.
4. Click *OK* to import the profile or profiles.

## SSIDs

To view SSIDs and SSID groups, go to *AP Manager > WiFi Profiles*, and select *SSID* in the tree menu.

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 341</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. On the SSID pane, click *Create New > SSID Group* in the toolbar. The *Create New SSID Group* windows opens.
2. Enter a name for the group in the *Name* field.
3. Optionally, enter a brief description of the group in the *Comment* box.
4. Optionally, add SSIDs to the group in the *Members field*.
5. Click *OK* to create the SSID group.

**To edit an SSID or groups:**

1. Either double-click on an SSID, select as SSID and then click *Edit* in the toolbar, or right-click then select *Edit* from the menu. The *Edit SSID* or *Edit SSID Group* window opens.
2. Edit the settings as required. The SSID name and traffic mode cannot be edited.
3. Click *OK* to apply your changes.



**To delete SSIDs or groups:**

1. Select the SSIDs and groups that you would like to delete.
2. Either click *Delete* in the toolbar, 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. Either select an SSID or group and click *Clone* in the toolbar, or right-click on the SSID or group name, and select *Clone*. The *Clone SSID* or *Clone SSID Group* dialog box opens.
2. Edit the settings as required. An SSID's traffic mode cannot be edited.
3. Click *OK* to clone the SSID.

**To import an SSID:**

1. Click *Import* in the toolbar. The *Import* dialog box opens.
2. Select a FortiGate from the dropdown list. The list will include all of the devices in the current ADOM.
3. Select the SSID or SSIDs to be imported from the *Profile* dropdown 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*.

**To create a new SSID:**

1. On the SSID pane, click *Create New > SSID* in the toolbar, or select it from the right-click menu. The *Create New SSID Profile* windows opens.

**Create New SSID Profile**

Interface Name

Alias

Traffic Mode Tunnel Bridge Mesh

**Address**

IP/Network Mask

IPv6 Address

Administrative Access

☐ AUTO-IPSEC ☐ CAPWAP ☐ FGFM

☐ HTTP ☐ HTTPS ☐ PING

☐ PROBE-RESPONSE ☐ RADIUS-ACCT ☐ SNMP

☐ SSH ☐ TELNET

IPv6 Administrative Access

☐ ANY ☐ CAPWAP ☐ FGFM

☐ HTTP ☐ HTTPS ☐ PING

☐ SNMP ☐ SSH ☐ TELNET

**DHCP Server**

☐ OFF

**WiFi Settings**

SSID

Security Mode WPA2 Only Personal

Pre-shared Key

Client Limit ☐ OFF

Multiple Pre-shared Keys ☐ OFF

Broadcast SSID ON

Schedule always

Block Intra-SSID Traffic ☐ OFF

Broadcast Suppression ON

Filter Clients by MAC Address

RADIUS Server ☐ OFF

VLAN Pooling ☐ OFF

Quarantine Host ON

Encrypt TKIP AES TKIP-AES

QoS Profile

**Advanced Options** >

OK Cancel

2. Enter the following information, then click **OK** to create the new tunnel to wireless controller SSID:

<b>Interface Name</b>	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 from: <i>AUTO-IPSEC</i> , <i>CAPWAP</i> , <i>FGFM</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>ANY</i> , <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.
<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</b>	<p>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>	Select <i>Local</i> or <i>External</i> . If <i>External</i> is selected, enter the URL of the portal. This option is only available when the portal type includes authentication.
<b>User Groups</b>	Select the user group to add from the dropdown list. Select the plus symbol to add multiple groups. This option is only available when the portal type includes authentication.
<b>Exempt Sources</b>	Select exempt sources to add from the dropdown list. This option is only available when the portal type includes authentication.
<b>Devices</b>	Select exempt devices to add from the dropdown list. This option is only available when the portal type includes authentication.
<b>Exempt Destinations</b>	Select exempt destinations to add from the dropdown list. This option is only available when the portal type includes authentication.
<b>Exempt Services</b>	Select exempt services to add from the dropdown list. This option is only available when the portal type includes authentication.
<b>Customize Portal Messages</b>	Select to allow for customized portal messages. Portal messages cannot be customized until after the interface has been created. This option is only available when the portal type includes disclaimer, email collection, or CMCC without MAC authentication.
<b>Redirect after Captive Portal</b>	Select <i>Original Request</i> or <i>Specific URL</i> . If <i>Specific URL</i> is selected, enter the redirect URL. This option is only available when the security mode includes captive portal.
<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 is 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 216</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> </ul>

	<ul style="list-style-type: none"> <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 525</a> for information on adding a RADIUS server.
<b>VLAN Pooling</b>	<p>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.</p> <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> <p>This option is not available when the traffic mode is <i>Mesh</i>.</p>
<b>Quarantine Host</b>	<p>Enable/disable station quarantine (default = enable).</p> <p>This option is only available when the security mode includes WPA or WPA2.</p>
<b>Encrypt</b>	<p>Select the data encryption protocol:</p> <ul style="list-style-type: none"> <li>• <i>TKIP</i>: Temporal Key Integrity Protocol, used by the older WPA standard.</li> <li>• <i>AES</i>: Advanced Encryption Standard, commonly used with the newer WPA2 standard (default).</li> <li>• <i>TKIP-AES</i>: 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).</li> </ul> <p>This option is only available when the security mode includes WPA or WPA2.</p>
<b>QoS Profile</b>	Select the QoS profile from the drop-down list.
<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> .
<b>Per-Device Mapping</b>	Enable per-device mapping to override the SSID profile settings for selected devices. See <a href="#">To add SSID per-device mapping: on page 345</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 [To add SSID per-device mapping: on page 345](#).

### To add SSID per-device mapping:

1. Click *Create New* in the per-device mapping toolbar. The *Per-Device Mapping* dialog-box opens. Configure the following settings and click *OK*.

## Per-Device Mapping

Mapped Device

Mapped IP/NetMask

Mapped DHCP Server ☒ ON ☐

Address Range

+ Create Edit Delete

#	Starting IP	End IP
No records found...		

Netmask

Default Gateway

DNS Server

Advanced... ▾

Mode

NTP Server

Time Zone

Next Bootstrap Server

Additional DHCP Options

Lease Time

+ Create Edit Delete

#	Option Code	Value
No records found...		

MAC Reservation + Access Control

Unknown MAC Address

Action

<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. See <a href="#">To add additional DHCP options: on page 347</a> for details. 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. See <a href="#">To add a MAC address reservation: on page 347</a> for details. 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> .

### 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.



The dialog box is titled "MAC Reservation + Access Control". It contains the following fields and controls:

- MAC Address:** A text input field containing "00:00:00:00:00:00".
- End IP:** A section with three buttons: "Assign IP", "Block", and "Reserve IP". The "Reserve IP" button is highlighted in blue.
- End IP (Field):** A text input field containing "0.0.0.0".
- Description:** A large text area with a character count "0/255" on the right side.
- Buttons:** "OK" (blue) and "Cancel" (orange) buttons at the bottom.

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.

## 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.

To view WIDS profiles, ensure that you are in the correct ADOM, go to *AP Manager > WiFi Profiles*, and select *WIDS Profile* in the tree menu.

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>Import</b>	Import WIDS profiles from a connected FortiGate (toolbar only).

### To create a new WIDS profile:

1. On the WIDS Profile pane, click *Create New* in the toolbar, or select it from the right-click menu. The *Create New WIDS Profile* window opens.



**Create New WIDS Profile**

Name

Comments  0/255

Sensor Mode **Disable** Foreign Channels Only Foreign and Home Channels

Enable Rogue AP Detection **OFF**

**Intrusion Detection Settings**

Intrusion Type	Enable	Threshold	Interval (Seconds)
Asleep Attack	<b>OFF</b>		
Association Frame Flooding	<b>OFF</b>	30	10
Authentication Frame Flooding	<b>OFF</b>	30	10
Broadcasting Deauthentication	<b>OFF</b>		
EAPOL-FAIL Flooding (to AP)	<b>OFF</b>	10	1
EAPOL-LOGOFF Flooding (to AP)	<b>OFF</b>	10	1
EAPOL-START Flooding (to AP)	<b>OFF</b>	10	1
EAPOL-SUCC Flooding (to AP)	<b>OFF</b>	10	1
Invalid MAC OUI	<b>OFF</b>		
Long Duration Attack	<b>OFF</b>	8200	µs
Null SSID Probe Response	<b>OFF</b>		
Premature EAPOL-FAIL Flooding (to Client)	<b>OFF</b>	10	1
Premature EAPOL-SUCC Flooding (to Client)	<b>OFF</b>	10	1
Spoofed Deauthentication	<b>OFF</b>		
Weak WEP IV (Initialization Vector)	<b>OFF</b>		
Wireless Bridge	<b>OFF</b>		

**Advanced Options** ▾

ap-bgscan-duration	20
ap-bgscan-idle	0
ap-bgscan-intv	1
ap-bgscan-report-intv	30
ap-fgscan-report-intv	15
deauth-broadcast	disable
deauth-unknown-src-thresh	10
invalid-mac-oui	disable

**OK** **Cancel**

2. Enter the following information, then click **OK** to create the new 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 Rogue 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>	The intrusion types that can be detected.
<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.
<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>	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.

Intrusion Type	Description
	Several types of EAPOL packets can be detected: <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>	Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the client with these packets can be a denial of service attack. Two types of EAPOL packets can be detected: <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. Either double-click on a profile name, select a profile and then click *Edit* in the toolbar, or right-click on the name then select *Edit* from the menu. The *Edit WIDS* window opens.
2. Edit the settings as required.
3. Click *OK* to apply your changes.

#### To delete WIDS profiles:

1. Select the profile or profiles that will be deleted from the profile list.
2. Either click *Delete* from the toolbar, or right-click then select *Delete*.

3. Click *OK* in the confirmation dialog box to delete the profile or profiles.

#### To clone a WIDS profile:

1. Either select a profile and click *Clone* in the toolbar, or right-click a profile and select *Clone*. The *Clone WIDS* pane opens.
2. Edit the name of the profile, then edit the remaining settings as required.
3. Click *OK* to clone the profile.

#### To import a WIDS profile:

1. Click *Import* in the toolbar. The *Import* dialog box opens.
2. Select a FortiGate from the dropdown list. The list will include all of the devices in the current ADOM.
3. Select the profile or profiles to be imported from the dropdown list.
4. Click *OK* to import the profile or profiles.

## Bluetooth profiles

To view and configure Bluetooth profiles, ensure that you are in the correct ADOM, go to *AP Manager > WiFi Profiles*, and select *Bluetooth Profile* in the tree menu (or from the tabs in version 5.6 ADOMs).



Bluetooth profiles are not available in version 5.4 ADOMs.

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. On the Bluetooth Profile pane, click *Create New* in the toolbar, or select it from the right-click menu. The *Create New Bluetooth Profile* window opens.

**Create New Bluetooth Profile**

Name

Comments  0/63

Advertising ☒ iBeacon ☒ Eddystone-UUID ☒ Eddystone-URL

iBeacon UUID  005ea414-cbd1-11e5-9956-625662870761

Major ID  1000

Minor ID  2000

Eddystone Namespace  0102030405

Eddystone Instance  abcdef

Eddystone URL  http://www.fortinet.com

TX Power  0

Beacon Interval  100 ms

BLE Scanning

**Advanced Options** ▾

eddytone-url-encode-hex  00666f7274696e65-7407

2. Enter the following information:

<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 eddytone URL (127 characters).
<b>TX Power</b>	Transmit power level: <div> <div>0 = -21 dBm</div> <div>5 = -6 dBm</div> <div>10 = 3 dBm</div> </div> <div> <div>1 = -18 dBm</div> <div>6 = -3 dBm</div> <div>11 = 4 dBm</div> </div> <div> <div>2 = -15 dBm</div> <div>7 = 0 dBm</div> <div>12 = 5 dBm</div> </div> <div> <div>3 = -12 dBm</div> <div>8 = 1 dBm</div> </div> <div> <div>4 = -9 dBm</div> <div>9 = 2 dBm</div> </div>
<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 eddytone encoded URL hexadecimal string size (54 characters) in the <i>eddytone-url-encode-hex</i> field.

3. Click *OK* to create the new Bluetooth profile.

**To edit a Bluetooth profile:**

1. Either double-click on a profile name, select a profile and then click *Edit* in the toolbar, or right-click on the name then select *Edit* from the menu. The *Edit Bluetooth Profile* window opens.

2. Edit the settings as required.
3. Click *OK* to apply your changes.

**To delete Bluetooth profiles:**

1. Select the profile or profiles that will be deleted from the profile list.
2. Either click *Delete* from the toolbar, or right-click then select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the profile or profiles.

**To clone a Bluetooth profile:**

1. Either select a profile and click *Clone* in the toolbar, or right-click a profile and select *Clone*. The *Clone Bluetooth Profile* pane opens.
2. Edit the name of the profile, then edit the remaining settings as required.
3. Click *OK* to clone the profile.

**To import a Bluetooth profile:**

1. Click *Import* in the toolbar. The *Import* dialog box opens.
2. Select a FortiGate from the dropdown list. The list will include all of the devices in the current ADOM.
3. Select the profile or profiles to be imported from the dropdown list.
4. Click *OK* to import the profile or profiles.

## QoS profiles

To view and configure Quality of Service (QoS) profiles, ensure that you are in the correct ADOM, go to *AP Manager > WiFi Profiles*, and select *QoS Profile* in the tree menu (or from the tabs in version 5.6 ADOMs).



QoS profiles are not available in version 5.4 ADOMs.

---

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>Import</b>	Import QoS profiles from a connected FortiGate (toolbar only).

**To create a new QoS profile:**

1. On the QoS Profile pane, click *Create New* in the toolbar, or select it from the right-click menu. The *Create New QoS Profile* window opens.

**Create New QoS Profile**

Name

Comments  0/63

Max Uplink Speed (VAPs)  Kbps

Max Downlink Speed (VAPs)  Kbps

Max Uplink Speed (Clients)  Kbps

Max Downlink Speed (Clients)  Kbps

Client Rate Burst ☐ ON

Wi-Fi MultiMedia ☐ ON

U-APSD Power Save Mode ☐ ON

Call Admission Control ☐ ON

Call Capacity

Bandwidth Admission Control ☐ ON

Bandwidth Capacity  Kbps

DSCP Mapping ☐ ON

Voice Access

Video Access

Best Effort Access

Background Access

2. Enter the following information:

<b>Name</b>	Enter a name for the profile.
<b>Comments</b>	Optionally, enter comments.
<b>Max Uplink Speed (VAPs)</b>	The maximum uplink speed (VAPs), in Kbps (0 - 2097152, default = 0).
<b>Max Downlink Speed (VAPs)</b>	The maximum downlink speed (VAPs), in Kbps (0 - 2097152, default = 0).
<b>Max Uplink Speed (Clients)</b>	The maximum uplink speed (Clients), in Kbps (0 - 2097152, default = 0).
<b>Max Downlink Speed (Clients)</b>	The maximum downlink speed (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>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.

3. Click *OK* to create the new QoS profile.

#### To edit a QoS profile:

1. Either double-click on a profile name, select a profile and then click *Edit* in the toolbar, or right-click on the name then select *Edit* from the menu. The *Edit QoS Profile* window opens.
2. Edit the settings as required.
3. Click *OK* to apply your changes.

#### To delete QoS profiles:

1. Select the profile or profiles that will be deleted from the profile list.
2. Either click *Delete* from the toolbar, or right-click then select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the profile or profiles.

#### To clone a QoS profile:

1. Either select a profile and click *Clone* in the toolbar, or right-click a 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 clone the profile.

#### To import a QoS profile:

1. Click *Import* in the toolbar. The *Import* dialog box opens.
2. Select a FortiGate from the dropdown list. The list will include all of the devices in the current ADOM.
3. Select the profile or profiles to be imported from the dropdown list.
4. Click *OK* to import the profile or profiles.

## Bonjour profiles

To view and configure Bonjour profiles, ensure that you are in the correct ADOM, go to *AP Manager > WiFi Profiles*, and select *Bonjour Profile* in the tree menu (or from the tabs in version 5.6 ADOMs).





Bonjour profiles are not available in version 5.4 ADOMs.

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>Import</b>	Import Bonjour profiles from a connected FortiGate (toolbar only).

### To create a new Bonjour profile:

1. On the Bonjour Profile pane, click *Create New* in the toolbar, or select it from the right-click menu. The *Create New Bonjour Profile* window opens.

2. Enter the following information:

<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. 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.

3. Click *OK* to create the new Bonjour profile.

**To edit a Bonjour profile:**

1. Either double-click on a profile name, select a profile and then click *Edit* in the toolbar, or right-click on the name then select *Edit* from the menu. The *Edit Bonjour Profile* window opens.
2. Edit the settings as required.
3. Click *OK* to apply your changes.

**To delete Bonjour profiles:**

1. Select the profile or profiles that will be deleted from the profile list.
2. Either click *Delete* from the toolbar, or right-click then select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the profile or profiles.

**To clone a Bonjour profile:**

1. Either select a profile and click *Clone* in the toolbar, or right-click a profile and select *Clone*. The *Clone Bonjour Profile* pane opens.
2. Edit the name of the profile, then edit the remaining settings as required.
3. Click *OK* to clone the profile.

**To import a Bonjour profile:**

1. Click *Import* in the toolbar. The *Import* dialog box opens.
2. Select a FortiGate from the dropdown list. The list will include all of the devices in the current ADOM.
3. Select the profile or profiles to be imported from the dropdown list.
4. Click *OK* to import the profile or profiles.

# FortiSwitch Manager

The *FortiSwitch Manager* module enables you to centrally manage FortiSwitch templates and VLANs, and monitor FortiSwitch devices that are connected to FortiGate devices. You can configure multiple templates for specific FortiSwitch platforms that can be assigned to multiple devices.

The FortiSwitch Manager module includes the following tabs:

<b>Managed Switches</b>	Displays unauthorized and authorized FortiSwitch devices. You can view, authorize, and edit authorized switches, as well as apply templates to switches.
<b>Monitor</b>	Monitor FortiSwitch devices with a graphical representation of the connected switches.
<b>FortiSwitch Templates</b>	View, create, and edit FortiSwitch templates, VLANs, and security policies. Templates can also be imported.

The following steps provide an overview of using centralized FortiSwitch management to configure and install templates:

1. Create FortiSwitch VLANs.  
See [FortiSwitch VLANs on page 371](#).
2. Create or import FortiSwitch templates.  
See [FortiSwitch Templates on page 368](#).
3. Assign templates to FortiSwitch devices.  
See [Assigning templates to FortiSwitch devices on page 367](#).
4. Install the templates to the 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 [Configuring a device on page 56](#).

## Managed Switches

The *Managed Switches* pane allows you to manage FortiSwitch devices that are controlled by FortiGate devices that are managed by the FortiManager.

FortiSwitch devices, listed in the content pane, are grouped based on the controller that they are connected to.



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 463](#).

Go to *FortiSwitch Manager > Managed Switches* to manage FortiSwitch devices. Managed switches are organized by their FortiGate controller.

FortiGate	FortiSwitch Name	Serial Number	Platform	Connected Via	OS Version	Template	Join Time	Comments
fgt102[root]	test	S124DP3X00000000	FortiSwitch-124D-POE	192.168.4.4	S124DP-v3.5.2-build265,170123 (GA)	124-poe	Fri Mar 30 03:47:20 2118	
fgt102[root]		S424DN3X00000000	FortiSwitch-424D	192.168.4.2	S424DN-v3.5.1-build262,161115 (GA)		Fri Mar 30 21:03:59 2118	
fgt102[root]		S524DN4K00000000	FortiSwitch-524D	192.168.4.3	S524DN-v3.5.1-build262,161115 (GA)		Thu Mar 22 01:09:21 2118	
fgt101[root]	248D-POE	S248DP3W00000000	FortiSwitch-248D-POE	192.168.66.8	S248DP-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:44 2118	
fgt101[root]	424D-FPOE	S424DF3X00000000	FortiSwitch-424D-FPOE	192.168.66.2	S424DF-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:31 2118	
fgt101[root]	424D-POE	S424DP3X00000000	FortiSwitch-424D-POE	192.168.66.6	S424DP-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:50 2118	
fgt101[root]	448D	S448DN3X00000000	FortiSwitch-448D	192.168.66.5	S448DN-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:35 2118	
fgt101[root]	524D-FPOE	S524DF4K00000000	FortiSwitch-524D-FPOE	192.168.66.3	S524DF-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:41 2118	

## 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 options:

- Managed FortiSwitch
- Online
- Offline
- Unauthorized

You can click each quick status to display in the content pane only the devices referenced in the quick status.

### To view the quick status bar:

- If using ADOMs, ensure that you are in the correct ADOM.
- Go to *FortiSwitch Manager > Managed Switches*. The quick status bar is displayed above the content pane.
- In the tree menu, select a FortiGate or *All\_FortiGate*. The devices for the group are displayed in the content pane, and the quick status bar updates.
- Click on each quick status to filter the devices displayed on the content pane. For example, click *Offline*, and the content pane will display only devices that are currently offline.

## Managing FortiSwitches

FortiSwitch devices can be managed from the content pane below the quick status bar on the *FortiSwitch Manager > Managed Switches* pane.

FortiGate	FortiSwitch Name	Serial Number	Platform	Connected Via	OS Version	Template	Join Time	Comments
fgt102[root]	test	S124DP3X00000000	FortiSwitch-124D-POE	192.168.0.1	S124DP-v3.5.2-build265,170123 (GA)	124-poe	Fri Mar 30 03:47:20 2018	
fgt102[root]		S424DN3X00000000	FortiSwitch-424D	192.168.0.2	S424DN-v3.5.1-build262,161115 (GA)		Fri Mar 30 21:03:59 2018	
fgt102[root]		S524DN4K00000000	FortiSwitch-524D	192.168.1.1	S524DN-v3.5.1-build262,161115 (GA)		Thu Mar 22 01:09:21 2018	
fgt101[root]	248D-POE	S248DP3W00000000	FortiSwitch-248D-POE	192.168.2.1	S248DP-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:44 2017	
fgt101[root]	424D-FPOE	S424DF3X00000000	FortiSwitch-424D-FPOE	192.168.1.2	S424DF-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:31 2017	
fgt101[root]	424D-POE	S424DP3X00000000	FortiSwitch-424D-POE	192.168.2.2	S424DP-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:50 2017	
fgt101[root]	448D	S448DN3X00000000	FortiSwitch-448D	192.168.3.2	S448DN-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:35 2017	
fgt101[root]	524D-FPOE	S524DF4K00000000	FortiSwitch-524D-FPOE	192.168.3.1	S524DF-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:41 2017	

The following options are available from the toolbar and right-click menu:

<b>Edit</b>	Edit the selected FortiSwitch.
<b>Delete</b>	Delete the switch or switches.
<b>Assign Template</b>	Assign a template to the switch. Only applicable templates will be listed. See <a href="#">Assigning templates to FortiSwitch devices on page 367</a> .
<b>Authorize</b>	Authorize a switch. See <a href="#">Authorizing and deauthorizing FortiSwitch devices on page 366</a> . This option is also available in the toolbar by selecting <i>More</i> .
<b>Deauthorize</b>	Deauthorize a switch. See <a href="#">Authorizing and deauthorizing FortiSwitch devices on page 366</a> . This option is also available in the toolbar by selecting <i>More</i> .
<b>Restart</b>	Restart the switch. This option is also available in the toolbar by selecting <i>More</i> .
<b>Upgrade</b>	Upgrade the switch. The FortiSwitch must already be authorized. This option is also available in the toolbar by selecting <i>More</i> . Before upgrading FortiSwitch, go to <i>FortiGuard &gt; Firmware Images &gt; Product: FortiSwitch</i> and click the download icon to manually download the firmware images.
<b>Refresh</b>	Refresh the switch list. This option is also available in the toolbar by selecting <i>More</i> .
<b>Connect to CLI</b>	Connect to FortiSwitch device's CLI, if available. This option is also available in the toolbar by selecting <i>More</i> .
<b>Column Settings</b>	Click to select which columns to display or select <i>Reset to Default</i> to display the default columns. This option is only available in the toolbar.
<b>Search</b>	Enter a search string into the search field to search the switch list. This option is only available in the toolbar.

The following information is available in the content pane:

<b>FortiGate</b>	The FortiGate that the FortiSwitch is connected to.
<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>Connected Via</b>	The IP address of the switch.
<b>OS Version</b>	The OS version on the switch.
<b>Template</b>	The FortiSwitch template assigned to the device, if any.
<b>Join Time</b>	The date and time that the switch joined.
<b>Comments</b>	User entered comments.

## Zero Touch Deployment for FortiSwitch

Configure FortiSwitch on FortiManager using its serial number and deploy FortiSwitch devices across the network using zero touch deployment. After configuring FortiSwitch on FortiManager, you can deploy remote FortiSwitch devices by just plugging them into remote FortiGate devices.

Requirements:

- FortiManager version 5.6 ADOM or later.
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with FortiSwitch.
- The FortiSwitch serial number is available.

**To enable zero touch deployment:**

1. Go to *FortiSwitch Manager > Managed Switches*.
2. Click *Create New*. The Add FortiSwitch screen is shown.

Add FortiSwitch

FortiGate	FortiGate1 (root)
Device Interface	port1
Serial Number	S248DF3X17000116
Name	FortiSwitch01

OK Cancel

3. Configure the following settings and click *OK* to create a model FortiSwitch and add it to managed FortiGate:

<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.

4. Click *Close* to close the *Add FortiSwitch* dialog.
5. Go to *Device Manager > Device & Groups* and click *Install Wizard*.
6. Select *Install Device Settings (only)*. Click *Next*.
7. Select the FortiGate device where the FortiSwitch will be connected. Click *Next*.
8. Click *Install*. Wait for the installation to complete.
9. Connect FortiSwitch to FortiGate.
10. The default FortiSwitch template is deployed to FortiSwitch. The progress can be viewed in the notification toolbar in FortiManager.



The Zero Touch Deployment process can also be used to deploy FortiGate devices. For more information, see [Adding a model device on page 40](#).

## Editing switches

FortiSwitch devices can be edited from the *FortiSwitch Manager > Managed Switches* pane.

### To edit FortiSwitch devices:

1. In the tree menu, select the FortiGate that contains the FortiSwitch device to be edited, or select *All\_FortiGate* to list all of the switches.
2. Select the appropriate option from the quick status bar, and locate the switch in the content pane.
3. Double-click on the switch, select the switch and click *Edit* from the toolbar, or right-click on the switch and select *Edit*. The *Edit Managed FortiSwitch* 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 FortiSwitch.
<b>Description</b>	A description of the FortiSwitch, such as its model.
<b>Template</b>	Select the template that will be applied to the FortiSwitch from the dropdown list. Only applicable templates are available.
<b>Status</b>	The status of the FortiSwitch, such as <i>Connected</i> . Click <i>Restart</i> to restart the switch.
<b>Connecting From</b>	The IP address of the switch.
<b>Join Time</b>	The date and time that the switch joined.
<b>State</b>	The state of the AP, such as <i>Authorized</i> . If the switch is authorized, click <i>De-authorize</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 366</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. See <a href="#">Firmware Management on page 88</a>

## Deleting switches

FortiSwitch devices can be deleted from the *FortiSwitch Manager > Managed Switches* pane.

### To delete FortiSwitch devices:

1. In the tree menu, select the FortiGate that contains the switch or switches to be deleted, or select *All\_FortiGate* to list all of the switches.
2. Select the appropriate option from the quick status bar, and locate the switch in the list in the content pane.
3. Select the switch or switches that you need to delete.
4. Click *Delete* from the toolbar, or right-click and select *Delete*.
5. Click *OK* in the confirmation dialog box to delete the switch or switches.

## Configuring Ports on a single FortiSwitch

Configure ports for a single FortiSwitch from FortiManager. To configure the ports for a single FortiSwitch, you must disable Central Management to automatically enable per-device management.

### To configure ports on a managed FortiSwitch:

1. Go to *System Settings > All ADOMs*.
2. Double-click the ADOM that has the FortiGate and FortiSwitch assigned to it.
3. In the *Edit ADOM* screen, clear the *FortiSwitch* check box under *Central Management* and click *OK*.

**Edit ADOM**

Name: root

Type: FortiGate 6.2

Comments: 0/128

Devices: + Select Device

Name	IP Address	Platform
FGVM00TM19002030	192.168.0.185	FortiGate-VM64-ALI
FortiGate_Model_Device		FortiGate-VM64

Mode: ☐ Normal ☐ Backup

Central Management: ☐ VPN ☒ FortiAP ☐ SD-WAN

Default Device Selection for Install: ☒ Select All ☐ Deselect All

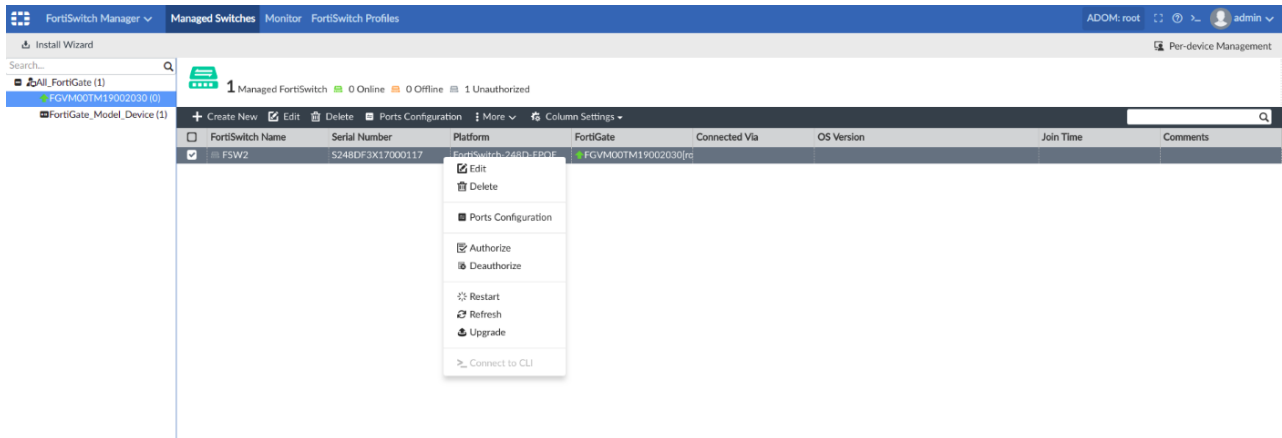
Perform Policy Check Before Every Install: ☐ OFF

Auto-Push Policy Packages When Device Back Online: ☐ Enable ☒ Disable

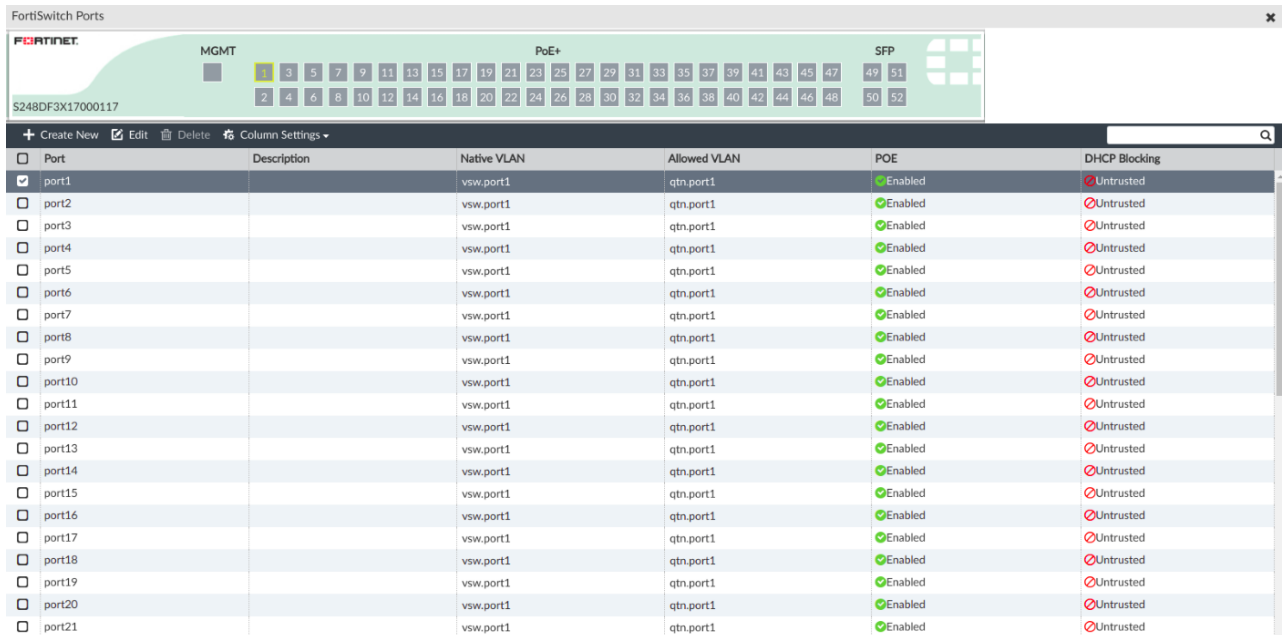
OK Cancel



4. Go to *FortiSwitch Manager > Managed Switches*.
5. Select the FortiGate where the FortiSwitch is connected to.
6. Select the FortiSwitch and click *Ports Configuration* from the toolbar. Alternatively, right-click on the FortiSwitch and select *Ports Configuration*.



7. The *FortiSwitch Ports* screen appears.



8. Double-click a single port in the device diagram to edit the port configuration. Alternatively, select the port in the ports list and click *Edit* in the toolbar.

## Edit Port

Port Name	port1
Description	<div></div> 0/63
Native VLAN	vsw,port1
Allowed VLAN	<div>qtn,port1</div> 1 Entry Selected
Security Policy	
LLDP Profile	default-auto-isl
QoS Policy	default
PoE Status	<input checked="" type="checkbox"/>
DHCP Blocking	<input type="checkbox"/>
IGMP Snooping	<input checked="" type="checkbox"/>
Loop Guard	<input type="checkbox"/>
STP	<input checked="" type="checkbox"/>
Edge Port	<input checked="" type="checkbox"/>
STP BPDU Guard	<input type="checkbox"/>
STP Root Guard	<input type="checkbox"/>

OK
Cancel

9. Modify the port configuration as required and click **OK**.



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.

## Authorizing and deauthorizing FortiSwitch devices

FortiSwitch devices can be authorized and deauthorized from the *Managed Switches* tab, or from the *Edit Managed FortiSwitch* pane (see [Editing switches on page 363](#)).

### To authorize FortiSwitch devices:

1. In the tree menu, select FortiGate that contains the unauthorized FortiSwitch devices, or select *All\_FortiGate* to list all of the switches.
2. In the quick status bar, click *Unauthorized*. The unauthorized FortiSwitch devices are displayed in the content pane.
3. Select the switches and either click *More > Authorize* from 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 FortiGate that contains the FortiSwitch devices to be deauthorized
2. Select the FortiSwitch devices and either click *More > Deauthorize* from the toolbar, or right-click and select *Deauthorize*.
3. Select **OK** in the confirmation dialog box to deauthorize the selected devices.

## Assigning templates to FortiSwitch devices

You use the FortiSwitch Manager pane to assign templates to switches, and you use the Device Manager pane to install the templates to the switches when you install a configuration to the FortiGate that controls the FortiSwitch device.

For more information about creating and managing FortiSwitch templates, see [FortiSwitch Templates on page 368](#).

### To assign a templates:

1. In the tree menu, select the FortiGate that contains the FortiSwitch device that the template will be applied to, or select *All\_FortiGate* to list all of the switches.
2. Select the appropriate option from the quick status bar, and locate the switch in the content pane.
3. Select the switch and click *Assign Template* from the toolbar, or right-click on the switch and select *Assign Template*. The *Assign FortiSwitch Template* dialog box opens.
4. Select a FortiSwitch template from the dropdown list, then click *OK* to assign it.



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 363](#).

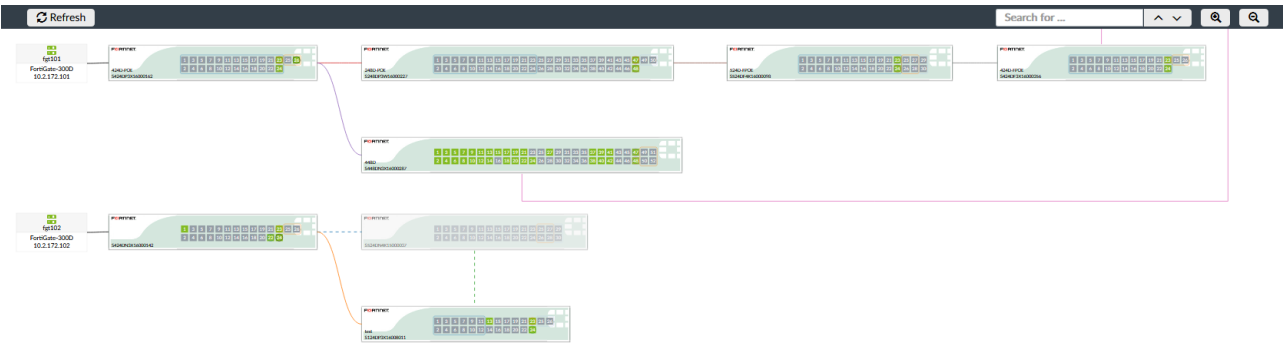
---

### To install templates to devices:

1. Go to the *Device Manager* pane.
2. Select the FortiGate device that controls the FortiSwitch
3. Right click and select *Install Config*, or select *Install > Install Config* from the toolbar.
4. Click *OK* in the confirmation dialog box to install the configuration to the device. See [Configuring a device on page 56](#) for more information.

## Monitor

The *FortiSwitch Manager > Monitor* pane shows a graphical representation of the connected FortiSwitch devices. Use the *Refresh* button to refresh the view, the search box to find a specific device or filter the view, and the zoom buttons to enlarge or shrink the view.



Ports that are transmitting and receiving data are highlighted in green. Port groups, such as PoE or SFP+ ports, are encircled in different colored boxes.

Hovering the cursor over the edge of 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.
Peer Device	<p>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.</p> <p>This item is only displayed when the port is connected to another FortiSwitch device.</p>
Native VLAN	The native VLAN of the port.
PoE	<p>Whether or not the port is currently providing PoE power.</p> <p>This item is only displayed on PoE ports.</p>
Link	The state of the link, either <i>up</i> or <i>down</i> .
Speed	The speed of the port, such as <i>1000Mbps/Full Duplex</i> . The value is <i>0Mbps</i> if the link is down.
Bytes Sent	The total number of bytes sent by the port.
Bytes Received	The total number of bytes received by the port.

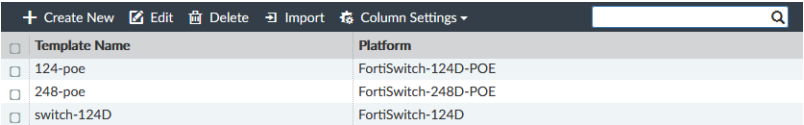
## FortiSwitch Templates

The *FortiSwitch Manager > FortiSwitch Templates* tab allows you to create and manage FortiSwitch templates, VLANs, and security policies that can be assigned to FortiSwitch devices. Templates can also be imported from FortiSwitch devices and then applied to other FortiSwitch devices of the same model.

### FortiSwitch templates

FortiSwitch templates define VLAN, and PoE assignments for a FortiSwitch platform.

To view FortiSwitch templates, ensure that you are in the correct ADOM, go to *FortiSwitch Manager > FortiSwitch Templates*, and select *FortiSwitch Templates* in the tree menu.



Template Name	Platform
124-poe	FortiSwitch-124D-POE
248-poe	FortiSwitch-248D-POE
switch-124D	FortiSwitch-124D

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 369</a> .
<b>Edit</b>	Edit the selected template.
<b>Delete</b>	Delete the selected template or templates.
<b>Import</b>	Import a FortiSwitch template. See <a href="#">Importing FortiSwitch templates on page 371</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. Either double-click a template name, right-click a template and select *Edit*, or select a template then click *Edit* in the toolbar. The *Edit FortiSwitch Template* pane opens.
2. Edit the settings as required, then 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. On the *FortiSwitch Template* pane, click *Create New* in the toolbar. The *Create New FortiSwitch Template* window opens.

**Create New FortiSwitch Template**

Template Name

Comments  0/255

Platforms

Switch VLAN Assignments

+ Add Port + Create Trunk ☒ Edit ☐ Delete

<input type="checkbox"/>	Port	Native VLAN	Allowed VLAN	Security Policy	POE	DHCP Blocking	IGMP Snooping	Loop Guard
<input type="checkbox"/>	<input type="text"/>	+	+	+		✓	✓	✗
<input type="checkbox"/>	<input type="text"/>	+	+	+		✓	✓	✗
<input type="checkbox"/>	<input type="text"/>	+	+	+		✓	✓	✗

< OK Cancel >

2. Enter the following information, then click **OK** to create the new template.

<b>Template Name</b>	Type a name for the template.
<b>Comments</b>	Optionally, enter comments.
<b>Platforms</b>	Select the platform that the template will apply to from the dropdown list.
<b>Switch VLAN Assignments</b>	Configure VLAN assignments. A platform must be selected before VLAN assignments can be configured.
<b>Add Port</b>	Add a port to the table.
<b>Create Trunk</b>	Create a trunk. See <a href="#">To create a trunk group: on page 371</a> .
<b>Edit</b>	Edit the selected trunk.
<b>Delete</b>	Delete the selected ports or trunks.
<b>Port</b>	Select a port profile from the dropdown list.
<b>Native VLAN</b>	Select the native VLAN from the available VLAN objects. See <a href="#">FortiSwitch VLANs on page 371</a> .
<b>Allowed VLAN</b>	Select the allowed VLAN from the available VLAN objects. See <a href="#">FortiSwitch VLANs on page 371</a> .
<b>Security Policy</b>	Select the security policies from the available switch controller security policies. See <a href="#">FortiSwitch security policies on page 378</a> .
<b>POE</b>	If applicable, right-click to enable or disable PoE for the port.
<b>DHCP Blocking</b>	Right-click to 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>IGMP Snooping</b>	Right-click to enable or disable IGMP snooping for the port or trunk. If the port is in a trunk, then IGMP snooping can only be enabled for the trunk, and not the individual ports.
<b>Loop Guard</b>	Right-click to enable or disable Loop Guard for the port. Loop Guard cannot be applied to trunks, or ports that are in trunks.
<b>STP</b>	Right-click to 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>	Right-click to 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>	Right-click to 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>	Right-click to 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.

### To create a trunk group:

1. On the *Create New FortiSwitch Template* pane, click *Create Trunk* in the *Switch VLAN Assignments* toolbar. The *New Trunk Group* dialog box opens.
2. Enter a name for the trunk group in the *Name* field.
3. In the *Members* field, select all the ports that will be in the group from the drop-down list.
4. Select the mode: *lacp-active* (active link aggregation), *lacp-passive* (passive link aggregation), or *static*.
5. Click *OK* to create the trunk group.

## Importing FortiSwitch templates

FortiSwitch templates can be imported from connected devices, and then applied to other FortiSwitch devices of the same model.

### To import a FortiSwitch template:

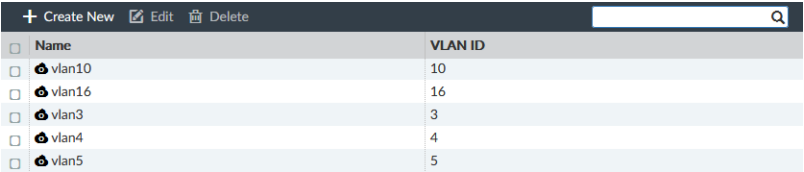
1. On the *FortiSwitch Template* pane, click *Import* in the toolbar. The *Import* window opens.

2. Select a FortiGate from the drop-down list.
3. Select the FortiSwitch whose template will be imported from the drop-down list.
4. Enter a name for the template in the *New Name* field.
5. Click *OK*.  
The template is imported from the device.

## FortiSwitch VLANs

VLANs are used when creating FortiSwitch templates.

To view FortiSwitch VLANs, ensure that you are in the correct ADOM, go to *FortiSwitch Manager > FortiSwitch Templates*, and select *FortiSwitch VLANs* in the tree menu.



Name	VLAN ID
vlan10	10
vlan16	16
vlan3	3
vlan4	4
vlan5	5

The following options are available in the toolbar and right-click menu:

Create New	Create a new FortiSwitch VLAN. See <a href="#">Creating FortiSwitch VLANs on page 372</a> .
Edit	Edit the selected VLAN.
Delete	Delete the selected VLAN or VLANs.
Search	Enter a search string into the search field to search the VLAN list.

**To edit a VLAN:**

1. Either double-click a VLAN, right-click a VLAN and select *Edit*, or select a VLAN then click *Edit* in the toolbar. The *Edit VLAN Definition* pane opens. The interface name and VLAN ID cannot be edited.
2. Edit the settings as required, then click *OK* to apply your changes.

**To delete VLANs:**

1. Select the VLAN or VLANs 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 VLAN or VLANs.

**Creating FortiSwitch VLANs**

**To create a FortiSwitch VLAN:**

1. On the *FortiSwitch VLAN* pane, click *Create New* in the toolbar. The *Create New VLAN Definition* window opens.



**Create New VLAN Definition**

Interface Name

VLAN ID

Role

Estimated Bandwidth

Address

Addressing mode

IP/Network Mask

IPv6 Addressing mode

IPv6 Address/Prefix

Restrict Access

Administrative Access

IPv6 Administrative Access

DHCP Server

Address Range

Netmask

Default Gateway

DNS Server

Advanced...

Mode

NTP Server

Time Zone

Next Bootstrap Server

Additional DHCP Options

Lease Time

MAC Reservation + Access Control

Unknown MAC Address Action

Networked Devices

Device Detection

Admission Control

Security Mode

Authentication Portal

User Access

Exempt Sources

Device

Exempt Destinations

Exempt Services

Miscellaneous

Scan Outgoing Connections to Botnet Sites

Secondary IP Address

Status

Comments

Interface State

Advanced Options

Per-Device Mapping

0

DMZ LAN UNDEFINED WAN

0 Kbps Upstream 0 Kbps Downstream

Manual

0.0.0.0/0.0.0.0

Manual DHCP

::/0

☐ CAPWAP

☐ DNP

☐ FGFM

☐ FTM

☐ HTTP

☐ HTTPS

☐ PING

☐ PROBE-RESPONSE

☐ RADIUS-ACCT

☐ SNMP

☐ SSH

☐ TELNET

☐ CAPWAP

☐ FGFM

☐ HTTP

☐ HTTPS

☐ PING

☐ SNMP

☐ SSH

☐ TELNET

ON

+ Create Edit Delete

Starting IP

End IP

No records found...

0.0.0.0

Same as Interface IP Specify 0.0.0.0

Same as System DNS Same as Interface IP Specify

Server Relay

Local Same as System NTP Specify 0.0.0.0

Disable Same as System Specify

0.0.0.0

604800

+ Create Edit Delete

Option Code

Value

No records found...

assign block

+ Create Edit Delete

MAC Address

Action or IP

Description

No records found...

Regular IPsec

OFF

CAPTIVE-PORTAL NONE

Local External example.com/captive

Restricted to Groups Allow all

+ + + +

BLOCK DISABLE MONITOR

ON

+ Create New Edit Delete

IP/Network Mask

Administrative Access

0/255

Enabled Disabled

+ Create New Edit Delete

Name

VDOM

Details

OK Cancel

2. 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 377</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 377</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 377</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 378](#) 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.*
- 4. Click *OK* to add the address.

**To add per device mapping:**

- 1. Click *Create New* in the *Per-Device Mapping* table toolbar. The *Per-Device Mapping* dialog box opens.

Per-Device Mapping

Mapped Device

Click to select

VLAN ID

0

Mapped IP/Netmask

0.0.0.0/0.0.0.0

DHCP Server

OFF

OK

Cancel

- 2. Select the device to be mapped from the *Mapped Device* drop-down list.
- 3. Enter the VLAN ID.
- 4. Enter the mapped IP address and netmask in the *Mapped IP/Netmask* field.
- 5. If required, enable *DHCP Server* and configure the options (options are the same as when creating a new VLAN definition).
- 6. Click *OK* to add the device mapping.

FortiSwitch security policies

To view FortiSwitch security policies , ensure that you are in the correct ADOM, go to *FortiSwitch Manager > FortiSwitch Templates*, and select *FortiSwitch Security Policies* in the tree menu.



FortiSwitch Security Policies are not available in version 5.4 ADOMs.

+ Create New   Edit   Delete   Import			
<input type="checkbox"/>	#	Name	User Groups
<input type="checkbox"/>	1	802-1X-policy-default	SSO_Guest_Users
<input type="checkbox"/>	2	TLeela	SSO_Guest_Users
<input type="checkbox"/>	3	ismyp	Guest-group
<input type="checkbox"/>	4	pjFry	Guest-group
<input type="checkbox"/>	5	what	SSO_Guest_Users

The following options are available in the toolbar and right-click menu:

Create New	Create a new FortiSwitch security policy. See <a href="#">Creating FortiSwitch security policies on page 379</a> .
Edit	Edit the selected policy.
Delete	Delete the selected policy or policies.
Import	Import security policies from a managed FortiGate device.
Search	Enter a search string into the search field to search the policy list.

**To edit a security policy:**

1. Either double-click a policy, right-click a policy and select *Edit*, or select a policy then click *Edit* in the toolbar. The *Edit Security Policies* pane opens. The name cannot be edited.
2. Edit the settings as required, then click *OK* to apply your changes.

**To delete security policies:**

1. Select the policy or policies that will be deleted.
2. Either click *Delete* from the toolbar, or right-click and select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the selected policy or policies.

**To import security policies:**

1. Click *Import* on the toolbar. The *Import* dialog box opens.
2. Select the FortiGate that the policies will be imported from in the drop-down list.
3. Select the policies that will be imported.
4. If only one policy is being imported, and its name is already used by a policy on the FortiManager, you can optionally enter a new name for the policy. If a new name is not entered, or if you are importing multiple policies, existing policies will be overwritten by imported policies.
5. Click *OK* in the confirmation dialog box to import the policies.

**Creating FortiSwitch security policies****To create a FortiSwitch security policy:**

1. On the *FortiSwitch Security Policies* pane, click *Create New* in the toolbar. The *Create New Security Policies* window opens.

2. 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="#">FortiSwitch VLANs on page 371</a> .

<b>Guest authentication delay</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="#">FortiSwitch VLANs on page 371</a> . This option is not available when <i>Security mode</i> is <i>MAC-based</i> .
<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.



# Endpoint Compliance

The *FortiClient Manager* pane enables you to centrally manage FortiClient profiles for multiple FortiGate devices and monitor FortiClient endpoints that are connected to FortiGate devices.

Endpoint control ensures that workstation computers (endpoints) and other network devices meet security requirements. Otherwise they are not permitted access. Endpoint control enforces the use of FortiClient Endpoint Security and pushes a FortiClient profile to the FortiClient application.

For information about FortiClient, see the *FortiClient Administration Guide*.



Additional configuration options and shortcuts are available using the right-click menu. Right-click on different parts of the navigation panes in the GUI to access these menus.

The *FortiClient Manager* pane includes the following tabs in the blue banner:

<b>FortiTelemetry</b>	View managed FortiGate devices with central FortiClient management enabled. You can enable or disable FortiTelemetry for interfaces, enable or disable FortiClient enforcement on interfaces, and assign FortiClient profile packages to devices.
<b>Monitor</b>	Monitor FortiClient endpoints by compliance status or interface. You can perform the following actions on FortiClient endpoints: block, unblock, quarantine, release quarantine, and unregister. You can also exempt non-compliant FortiClient endpoints from compliance rules.
<b>FortiClient profiles</b>	View and create profile packages and FortiClient profiles. You can also import FortiClient profiles from FortiGate devices.

Centralized FortiClient management is enabled by default. You use the *FortiClient Manager* pane to enable FortiTelemetry and FortiClient enforcement on FortiGate interfaces as well as create and assign FortiClient profile packages to one or more FortiGate devices or VDOMs. Profile packages are installed to devices when you install configurations to the devices.

The following steps provide an overview of using centralized FortiClient management to configure, assign, and install FortiClient profiles:

**To create and assign FortiClient profile packages:**

1. Create a FortiClient profile package. See [Creating FortiClient profile packages on page 388](#).
2. Select the profile package, and create one or more FortiClient profiles. See [Creating FortiClient profiles on page 389](#).
3. Enable FortiTelemetry on FortiGate interfaces. See [Enabling FortiTelemetry on interfaces on page 383](#).
4. Enable FortiClient enforcement on FortiGate interfaces. See [Enabling endpoint control on interfaces on page 384](#).
5. Assign profile packages to FortiGate interfaces. See [Assigning profile packages on page 393](#).

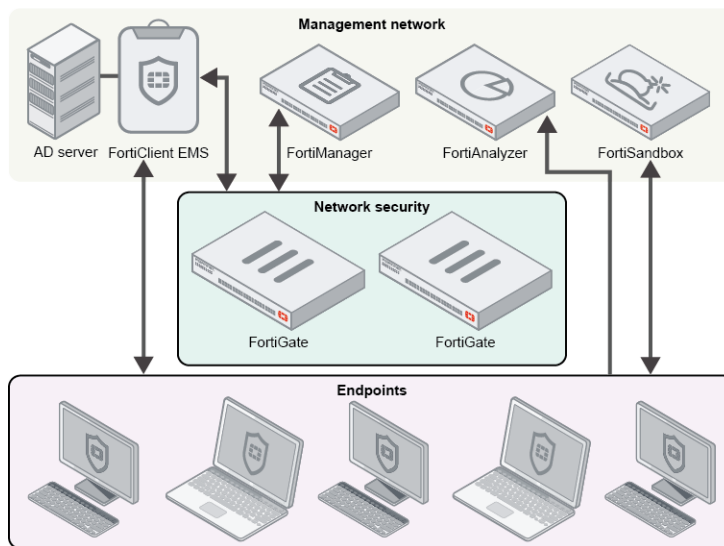
**To install configuration changes to devices:**

1. On the *FortiClient Manager* > *FortiClient Profiles* pane, click *Install Wizard*.
2. Follow the prompts in the wizard. See [Using the Install Wizard to install policy packages and device settings on page 66](#).

## How FortiManager fits into endpoint compliance

The FortiClient settings available in FortiManager are intended to complement FortiClient support that is available with FortiClient EMS and FortiGate. Each product performs specific functions:

- FortiClient EMS is used to deploy FortiClient (Windows) endpoints and FortiClient profiles, and the endpoints can connect FortiClient Telemetry to FortiGate or to FortiClient EMS. You can import FortiClient profiles from FortiGate devices to FortiClient EMS, and use FortiClient EMS to deploy the profiles. Alternately, you can use FortiClient EMS to create and deploy profiles. When FortiClient endpoints connect FortiClient Telemetry to EMS, you can use FortiClient EMS to monitor FortiClient endpoints.
- FortiManager provides central FortiClient management for FortiGate devices that are managed by FortiManager. In FortiManager, you can create one or more FortiClient profiles that you can assign to multiple FortiGate devices. You can also import FortiClient profiles from one FortiGate device and assign the FortiClient profile to other FortiGate devices. When FortiClient endpoints are registered to managed FortiGate devices, you can use FortiManager to monitor FortiClient endpoints from multiple FortiGate devices.
- FortiGate provides compliance rules for network access control. FortiGate devices enforce network compliance for connected FortiClient endpoints. FortiGate devices communicate between FortiClient endpoints and FortiManager.



## FortiTelemetry

On the *FortiClient Manager* > *FortiTelemetry* pane, you can enable and disable FortiTelemetry and FortiClient enforcement on FortiGate interfaces to use for FortiClient communication. You can also assign FortiClient profile

packages to FortiGate devices.

After you make configuration changes, install the changes to the device. See [Installing to devices on page 66](#).

## Viewing devices

The *FortiClient Manager > FortiTelemetry* pane displays FortiGate devices with central FortiClient management enabled.

### To view devices:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *FortiClient Manager > FortiTelemetry*. The list of FortiGate devices is displayed in the tree menu.
3. Select a device.

The following options are available in the toolbar for the selected device:

<b>Add Interface</b>	Click to enable FortiTelemetry on interfaces for the selected device to use for FortiClient communication.
<b>Remove Interface</b>	Click to disable FortiTelemetry on the selected interface.
<b>Assign Profile</b>	Click to assign a FortiClient profile package to the FortiGate.

The following information is displayed in the content pane for the selected device:

<b>Virtual Domain</b>	Displays the name of the virtual domain for the selected FortiGate device if applicable.
<b>Interface</b>	Displays the interfaces with FortiTelemetry enabled for the FortiGate device. The interfaces are used for FortiClient communication, and FortiClient endpoints use the interface to connect or register to FortiGate.
<b>IP</b>	Displays the IP address for the interface.
<b>Enforce FortiClient</b>	Displays whether FortiClient is enforced on the interface. A green checkmark indicates FortiClient is enforced. An x in a circle indicates that FortiClient is not enforced.
<b>Profile Package</b>	Displays the name of the FortiClient profile package that is assigned to the FortiGate interface.

## Enabling FortiTelemetry on interfaces

When you add an interface on the *FortiClient Manager > FortiTelemetry* pane, you are enabling FortiTelemetry for the interface, and the interface is used for connection and communication with FortiClient endpoints.

When you remove an interface on the *FortiClient Manager > FortiTelemetry* pane, you are disabling FortiTelemetry for the interface.

**To enable FortiTelemetry on interfaces:**

1. Go to *FortiClient Manager > FortiTelemetry*. The list of FortiGate devices is displayed in the tree menu.
2. Select a FortiGate device, and click *Add Interface*.
3. Select one or more interfaces to use for FortiClient communication, and click *OK*. The selected interfaces are displayed in the *Interface* column, and FortiTelemetry is enabled for the interfaces.

## Enabling endpoint control on interfaces

When you enable FortiClient enforcement on an interface, you are enabling endpoint control, and all FortiClient endpoints using the interface are required to adhere to the FortiGate compliance rules that are specified in the profile that is applied to the endpoint.

When you disable FortiClient enforcement on an interface, you are disabling endpoint control, and FortiClient endpoints are not required to adhere to FortiGate compliance rules.

**To enable FortiClient enforcement on interfaces:**

1. Go to *FortiClient Manager > FortiTelemetry*. The list of FortiGate devices is displayed in the tree menu.
2. Click a FortiGate device.
3. Right-click an interface, and select *Enable Enforce FortiClient*.  
You can disable FortiClient enforcement for the interface by selecting *Disable Enforce FortiClient*.

## Assigning FortiClient profile packages to devices

You can use the *FortiClient Manager > FortiTelemetry* pane to assign FortiClient profile packages to interfaces for FortiGate devices, and you can use the *Install Wizard* to install profile packages to FortiGate devices when you install a configuration to the FortiGate device.

**To assign FortiClient profile packages:**

1. In the left pane, select a device.
2. In the content pane, click *Assign Profile*. The *Assign Profile* dialog box is displayed.
3. Select a profile package, and click *OK*. The selected profile package is assigned to the added interface(s).
4. Install the configuration changes to the FortiGate device.

## Monitor

On the *FortiClient Manager > Monitor* pane, you can monitor FortiClient endpoints that are registered to FortiGate devices.

## Monitoring FortiClient endpoints

The list of FortiClient endpoints updates automatically when new endpoints are registered to the FortiGate device. You can also click *Refresh* to update the list of FortiClient endpoints.

### To monitor FortiClient endpoints:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *FortiClient Manager > Monitor*.
3. In the tree menu, select a FortiGate device.

The following buttons are available on the toolbar for the selected device:

<b>Refresh</b>	Click to refresh the list of FortiClient endpoints for the selected device.
<b>Action</b>	Click to select one of the following actions for the selected FortiClient endpoint: <ul style="list-style-type: none"> <li>• Block</li> <li>• Unblock</li> <li>• Quarantine</li> <li>• Release Quarantine</li> <li>• Unregister</li> </ul>
<b>Column Settings</b>	Click to select which columns to display or select <i>Reset to Default</i> to display the default columns.
<b>By Interface</b>	Click to organize the display of FortiClient endpoints by the undetected interfaces and interface name. In the <i>Device</i> column, click <i>Undetected</i> or the interface name to hide and display its list of FortiClient endpoints.
<b>By Compliance Status</b>	Click to organize the display of FortiClient endpoints by the following compliance statuses: <i>Noncompliant</i> and <i>Exempt</i> . In the <i>Device</i> column, click <i>Noncompliant</i> or <i>Exempt</i> to hide and display its list of FortiClient endpoints.

The following default columns of information are available for the selected device:

<b>Device</b>	Displays the name of the FortiClient endpoint that is registered to the selected FortiGate device. It also displays an icon that represents the operating system on the FortiClient endpoint. You can hover over each device to view device details.
<b>User</b>	Displays the name of the user logged into the FortiClient endpoint.
<b>IP address</b>	Displays the IP address of the FortiClient endpoint.
<b>Status</b>	Displays one of the following statuses for the FortiClient endpoint: <ul style="list-style-type: none"> <li>• Online</li> <li>• Offline</li> <li>• Registered-Online</li> <li>• Registered-Offline</li> <li>• Un-Registered</li> </ul>
<b>FortiClient Version</b>	Displays the version of FortiClient software installed on the FortiClient endpoint.

<b>FortiClient Profile</b>	Displays the name of the FortiClient profile that is assigned to the FortiClient endpoint.
<b>Compliance</b>	<p>Displays one of the following icons of compliance statuses for the FortiClient endpoint:</p> <ul style="list-style-type: none"> <li>• Compliant</li> <li>• Endpoint is not compliant with FortiClient profile</li> <li>• Quarantined</li> <li>• FortiTelemetry is disabled</li> <li>• Exempt</li> </ul> <p>Hover the mouse over the compliance status icon to view more information. Additional information about why the endpoint is not compliant may also be displayed.</p>

## Monitoring FortiClient endpoints by compliance status

**To monitor FortiClient endpoints by compliance status:**

1. Go to *FortiClient Manager > Monitor*.
2. In the tree menu, select a FortiGate device.
3. Click *By Compliance Status*.  
The list of FortiClient endpoints is displayed by compliance status.
4. In the *Device* column, click the compliance status to hide and display its list of FortiClient endpoints.  
For example, click *Noncompliant* to hide and display the list of FortiClient endpoints with a status of noncompliant.
5. In the *Compliance* column, hover the mouse over the compliance status to view more details.

## Monitoring FortiClient endpoints by interface

**To monitor FortiClient endpoints by interface:**

1. Go to *FortiClient Manager > Monitor*.
2. In the tree menu, select a FortiGate device.
3. Click *By Interface*.  
The list of FortiClient endpoints is displayed by compliance status.
4. In the *Device* column, click *Undetected* or the name of the interface to hide and display its list of FortiClient endpoints.

## Exempting non-compliant FortiClient endpoints

You can exempt FortiClient endpoints that are non-compliant from the compliance rules to allow the endpoints to access the network.

**To exempt non-compliant FortiClient endpoints:**

1. Go to *FortiClient Manager > Monitor*.
2. In the tree menu, select a FortiGate device.

3. Select one or more FortiClient endpoints.
4. Right-click the selected FortiClient endpoint, and select *Exempt this device* or *Exempt all devices of this type*. The FortiClient endpoint is exempt from the compliance rules.
5. Install the configuration changes to the FortiGate device.

## FortiClient profiles

The *FortiClient Manager > Profiles* pane allows you to create and manage FortiClient profile packages and profiles for endpoints. You can create profile packages of profiles for endpoints that are running the following operating systems: Windows, Mac, iOS, and Android.

The following information is displayed on the *FortiClient Manager > FortiClient Profiles* pane:

<b>Profile Package</b>	In the <i>Profile Package</i> menu, you can select to create, rename, or delete a FortiClient profile package.
<b>Assign Profile Package</b>	Assigns the selected FortiClient profile package to a device.
<b>Install Wizard</b>	Click to launch the Install Wizard to install device settings to devices. This process installs the FortiClient profile package that is assigned to the device.

## Viewing profile packages

To view profile packages:

1. Go to *FortiClient Manager > FortiClient Profiles*.
2. Click *All Profile Packages*.

The following options are available in the toolbar:

<b>Create New</b>	Click to create a new FortiClient profile package.
<b>Rename</b>	Click to rename the selected profile package.
<b>Delete</b>	Click to delete the selected profile package and all of its profiles.

The following information is displayed in the content pane:

<b>Package Name</b>	Displays the name of the profile package.
<b>Device Targets</b>	Displays the name of the device to which the profile package has been assigned.

## Viewing FortiClient profiles

To view FortiClient profiles:

1. Go to *FortiClient Manager > FortiClient Profiles*.
2. In the *All Profile Packages* tree menu, click a profile.

The following options are available in the toolbar:

<b>Create New</b>	Click to create a new FortiClient profile for the selected FortiClient profile package.
<b>Edit</b>	Select a profile, and click <i>Edit</i> to edit the profile. Alternatively, double click the profile to open the <i>Edit FortiClient Profile</i> pane.
<b>Delete</b>	Select a profile, and click <i>Delete</i> to delete the profile from the ed FortiClient profile package. Alternately, right-click a profile, and select <i>Delete</i> .
<b>Move</b>	Change the order of the profiles.
<b>Import</b>	Select to import a FortiClient profile from an existing device or VDOM into the selected FortiClient profile package.
<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 displayed in the content pane:

<b>Seq.#</b>	Displays the sequence number of the FortiClient profile.
<b>FortiClient Profile</b>	Displays the name of the FortiClient profile for the selected FortiClient profile package.
<b>Assign To</b>	Displays the device groups, user groups, and users associated with the FortiClient profile.
<b>Comments</b>	Displays any comments about the FortiClient profile.
<b>Non-Compliance Action</b>	Displays the selected non-compliance action settings from the FortiClient profile. The settings include: <i>Warning</i> , <i>Block</i> , or <i>Auto-Update</i> .
<b>Last Modified</b>	Shows the last modified date.

## Creating FortiClient profile packages

FortiClient profile packages contain one or more FortiClient profiles. You assign FortiClient profile packages to devices or VDOMs.

FortiManager includes a default FortiClient profile package, and you can create multiple profiles for the profile package.

You can also create custom FortiClient profile packages and profiles.

### To create profile packages:

1. Go to *FortiClient Manager > FortiClient Profiles*.
2. From the *Profile Package* menu, select *Create New*.
3. Type a name, and click *OK*.



## Creating FortiClient profiles

You can create one or more FortiClient profiles in a FortiClient profile package. The FortiClient profile identifies the FortiGate compliance rules and the non-compliance action to apply to endpoints that fail to meet the compliance rules.



The FortiClient profile does not contain any configuration information for FortiClient. The FortiClient profile only identifies the compliance rules that FortiClient endpoints must meet to maintain access to the network.

---

You can enable compliance rules for the following categories in a FortiClient profile:

- Endpoint Vulnerability Scan on Client
- System Compliance
- Security Posture Check

For each category, you can specify how to handle endpoints that fail to meet the compliance rules. You can choose to block non-compliant endpoints from network access, or you can warn non-compliant endpoints, but allow network access. For example, you could set the non-compliance action to *Block* for *Endpoint Vulnerability Scan on Client*, and you can set the non-compliance action to *Warning* for *Security Posture Check*.

FortiClient profiles can be created, edited, deleted, and imported from devices using the right-click menu and toolbar selections.

---



In FortiOS, this feature is found at *Security Profiles > FortiClient Profiles*.

---

### To create a new FortiClient profile:

1. Go to *FortiClient Manager > FortiClient Profiles*.
2. In the tree menu, select the FortiClient profile package in which to create profiles.
3. In the content pane, click *Create New*.

The *Create New FortiClient Profile* pane opens.

**Create New FortiClient Profile**

Profile Name	<input type="text"/>
Comments	<input type="text"/>
Assign Profile To	
Device Groups	<input type="text"/> Click here to select
User Groups	<input type="text"/> Click here to select
Users	<input type="text"/> Click here to select
Address	<input type="text"/> Click here to select
On-Net Detection By Address	<input type="text"/> Click here to select
Endpoint Vulnerability Scan on Client	<input checked="" type="checkbox"/> ON
Non-compliance action	<input type="text"/> Block <input checked="" type="text"/> Warning
Vulnerability quarantine level ⓘ	High ▾
System compliance	<input checked="" type="checkbox"/> ON
Minimum FortiClient Version	<input type="text"/> OFF
Upload Logs to FortiAnalyzer	<input checked="" type="checkbox"/> ON
	<input checked="" type="checkbox"/> Traffic
	<input checked="" type="checkbox"/> Vulnerability
	<input checked="" type="checkbox"/> Event
Non-compliance action	<input type="text"/> Block <input checked="" type="text"/> Warning
Security Posture Check	<input checked="" type="checkbox"/> ON
Real-time Protection	<input type="text"/> OFF
Third party AntiVirus on Windows ⓘ	<input type="text"/> OFF
Web Filter	<input type="text"/> OFF
Application Firewall	<input type="text"/> OFF
Non-compliance action	<input type="text"/> Block <input checked="" type="text"/> Warning

4. Enter the following information:

<b>Profile Name</b>	Type a name for the new FortiClient profile. When creating a new FortiClient profile, XSS vulnerability characters are not allowed.
<b>Comments</b>	(Optional) Type a profile description.
<b>Assign Profile To</b>	Identify where to assign the profile: <ul style="list-style-type: none"> <li>• <i>Device Groups</i>: Select device groups from the list.</li> <li>• <i>User Groups</i>: Select user groups from the list.</li> <li>• <i>Users</i>: Select users from the list.</li> <li>• <i>Address</i>: Select addresses from the list.</li> </ul> You can assign the profile to user groups and users when using Active Directory authentication or RADIUS authentication for VPN.
<b>On-Net Detection By Address</b>	Identify whether to use an address to detect when endpoints are on-net. Select the address(es) from the list.

5. Set the compliance rules and non-compliance action for *Endpoint Vulnerability Scan on Client*:

<b>Endpoint Vulnerability Scan on Client</b>	Toggle <b>ON</b> to add a rule about <i>Vulnerability Scanning on Client</i> . When toggled <b>ON</b> , the Vulnerability Scanning module must be enabled in FortiClient on endpoints.  Toggle <b>OFF</b> to exclude <i>Vulnerability Scanning on Client</i> from the compliance rules.
--	---

<b>Non-compliance action</b>	Specify how to handle endpoints that fail to meet the compliance rules for <i>Endpoint Vulnerability Scan on Client</i> . Select <i>Block</i> to block not-compliant endpoints from network access. Select <i>Warning</i> to warn not-compliant endpoints, but allow network access.
<b>Vulnerability quarantine level</b>	When <i>Endpoint Vulnerability Scan on Client</i> is toggled to <i>ON</i> , you can select a minimum quarantine level from the <i>Vulnerability quarantine level</i> list. Endpoints with detected vulnerabilities that hit the minimum severity level or higher are quarantined.

6. Set the compliance rules and non-compliance action for *System Compliance*:

<b>System compliance</b>	Toggle <i>ON</i> to enable compliance rules for <i>System compliance</i> and display options for rules. Toggle <i>OFF</i> to exclude system compliance from the compliance rules.
<b>Minimum FortiClient Version</b>	Toggle <i>ON</i> to add a rule about minimum FortiClient version. When toggled <i>ON</i> , endpoints must have the minimum version or higher of FortiClient installed to remain compliant. Specify the minimum version in the <i>Windows endpoints</i> and <i>Mac endpoints</i> boxes. Toggle <i>OFF</i> to remove a rule about minimum FortiClient version from the compliance rules.
<b>Windows endpoints</b>	When <i>Minimum FortiClient Version</i> is toggled <i>ON</i> , you can type the minimum version of FortiClient that is required on endpoints running a Windows operating system.
<b>Mac endpoints</b>	When <i>Minimum FortiClient Version</i> is toggled <i>ON</i> , you can type the minimum version of FortiClient that is required on endpoints running a Macintosh operating system.
<b>Upload logs to FortiAnalyzer</b>	Toggle <i>ON</i> to add a rule about logging. When toggled <i>ON</i> , FortiClient must send logs to FortiAnalyzer for the endpoint to remain compliant. Select which of the following FortiClient logs must be sent to FortiAnalyzer: <ul style="list-style-type: none"> <li>• Traffic</li> <li>• Vulnerability</li> <li>• Event</li> </ul> Toggle <i>OFF</i> to remove a rule about logging from the compliance rules.
<b>Non-compliance action</b>	Specify how to handle endpoints that fail to meet the compliance rules for <i>System Compliance</i> . Select <i>Block</i> to block not-compliant endpoints from network access. Select <i>Warning</i> to warn not-compliant endpoints, but allow network access.

7. Set the compliance rules and non-compliance action for *Security Posture Check*:

<b>Security Posture Check</b>	Toggle <i>ON</i> to enable compliance rules for <i>Security Posture Check</i> and display more options. When toggled <i>ON</i> , select which modules must be enabled in FortiClient for endpoints to remain compliant. Toggle <i>OFF</i> to remove rules about <i>Security Posture Check</i> from the compliance rules.
-------------------------------	---

<b>Real-time Protection</b>	<p>Toggle <i>ON</i> to add a rule about real-time protection to the compliance rules. When toggled <i>ON</i>, FortiClient must have real-time protection enabled for endpoints to remain compliant.</p> <p>Toggle <i>OFF</i> to remove a rule about real-time protection from the compliance rules.</p>
<b>Up-to-date signatures</b>	<p>Toggle <i>ON</i> to add a rule about up-to-date signatures to the compliance rules. When toggled <i>ON</i>, FortiClient real-time protection must have up-to-date signatures for endpoints to remain compliant.</p> <p>Toggle <i>OFF</i> to remove a rule about up-to-date signatures from the compliance rules.</p>
<b>Scan with FortiSandbox</b>	<p>Toggle <i>ON</i> to add a rule about FortiSandbox scanning to the compliance rules. When toggled <i>ON</i>, FortiClient real-time protection must have FortiSandbox scanning enabled for endpoints to remain compliant.</p> <p><b>Note:</b> A FortiSandbox device is required, and the device must be configured to work with FortiClient.</p> <p>Toggle <i>OFF</i> to remove a rule about FortiSandbox scanning from the compliance rules.</p>
<b>Third party AntiVirus on Windows</b>	<p>Toggle <i>ON</i> to add a rule about third-party antivirus software for endpoints running a Windows operating system to the compliance rules. When toggled <i>ON</i>, endpoints running a Windows operating system must have recognized third-party antivirus software installed for endpoints to remain compliant.</p> <p><b>Note:</b> <i>Real-time Protection</i> must be toggled <i>OFF</i> before you can toggle on <i>Third party AntiVirus on Windows</i>.</p> <p>Toggle <i>OFF</i> to remove the rule about third-party antivirus software from the compliance rules.</p>
<b>Web Filter</b>	<p>Toggle <i>ON</i> to add a rule about <i>Web Filter</i> to the compliance rules and display more options.</p> <p>Toggle <i>OFF</i> to exclude a rule about <i>Web Filter</i> from the compliance rules.</p>
<b>Profile</b>	<p>When <i>Web Filter</i> is toggled <i>ON</i>, you can select a web filter profile. A default profile is selected by default.</p>
<b>Application Firewall</b>	<p>Toggle <i>ON</i> to add a rule about <i>Application Firewall</i> to the compliance rules and display more options.</p> <p>Toggle <i>OFF</i> to exclude the setting from the compliance rules.</p>
<b>Application Control Sensor</b>	<p>When <i>Application Firewall</i> is toggled <i>ON</i>, you can select an application control sensor. A default application control sensor is selected by default.</p>
<b>Non-compliance action</b>	<p>Specify how to handle endpoints that fail to meet the compliance rules for <i>Security Posture Check</i>. Select <i>Block</i> to block not-compliant endpoints from network access. Select <i>Warning</i> to warn not-compliant endpoints, but allow network access.</p>

8. Click *OK*.

## Editing FortiClient profiles

### To edit a FortiClient profile:

1. Right-click a profile, and select *Edit*. The *Edit FortiClient Profile <name>* pane is displayed.
2. Edit the settings, and click *OK*.

## Deleting FortiClient profiles

### To delete a FortiClient profile:

1. Right-click a profile, and select *Delete*.
2. Click *OK* in the confirmation dialog box to delete the profile.

## Importing FortiClient profiles

You can import FortiClient profiles from FortiGate.

### To import a FortiClient profile:

1. Go to *FortiClient Manager > FortiClient Profiles*.
2. Select a profile package, and click *Import*. The *Import* dialog box is displayed.
3. Enter the following information:

<b>Import From Device</b>	Select a device from which to import the profile or profiles from the dropdown list. This list will include all the devices available in the ADOM.
<b>Profile</b>	Select the profile to import.
<b>New Name</b>	Select to create a new name for the profile being imported, and then type the name in the field.

4. Click *OK*. The profile is imported into the selected profile package.

## Assigning profile packages

### To assign profile packages:

1. Go to *FortiClient Manager > FortiClient Profiles*.
2. Select a profile package, and click *Assign Profile Package*. The *Assign Profile Package* dialog box is displayed.
3. Select one or more devices, and click *OK*. The profile package is assigned to the device(s).
4. Install the configuration changes to the FortiGate device. See [Configuring a device on page 56](#) for more information.

# Device Firmware and Security Updates

The FortiGuard Distribution Network (FDN) provides FortiGuard services for your FortiManager system and its managed devices and FortiClient agents. The FDN is a world-wide network of FortiGuard Distribution Servers (FDS), which update the FortiGuard services on your FortiManager system on a regular basis so that your FortiManager system is protected against the latest threats.

The FortiGuard services available on the FortiManager system include:

- Antivirus and IPS engines and signatures
- Web filtering and email filtering rating databases and lookups
- Vulnerability scan and management support for FortiAnalyzer

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.

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.

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 [Firewall Devices on page 34](#).
- Enable and configure the FortiManager system's built-in FDS. For more information, see [Configuring network interfaces on page 441](#).
- 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 398](#).
- 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 [Adding devices on page 35](#).

This section contains the following topics:

- [Settings](#)
- [Configuring devices to use the built-in FDS](#)
- [Configuring FortiGuard services](#)
- [Logging events related to FortiGuard services](#)
- [Restoring the URL or antispam database](#)
- [Licensing status](#)
- [Package management](#)
- [Query server management](#)
- [Firmware images](#)



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>.

## 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 399](#).

FortiGuard Server and Service Settings

Enable Communication with FortiGuard Server ☒

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) >

Apply

### 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 399](#).

<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>FortiClient</i> , <i>FortiAnalyzer</i> , and <i>FortiMail</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 396</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 397</a> .
<b>Override FortiGuard Server (Local FortiManager)</b>	Configure web and email filter settings. See <a href="#">Override FortiGuard server (Local FortiManager) on page 398</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 405</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 405</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 403</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 405</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 406](#).

**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-url 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 405](#).

To enable web filter and email filter service updates using a web proxy server, see [Enabling updates through a web proxy on page 405](#).

**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 405](#).

**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 405](#).

**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 407](#).

**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:

<b>Additional number of Private FortiGuard Servers (Excluding This One)</b>	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.
<b>Enable Antivirus and IPS Update Service for Private Server</b>	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.
<b>Enable Web Filter and Email Filter Update Service for Private Server</b>	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.
<b>Allow FortiGates to Access Public FortiGuard Servers When Private Servers Unavailable</b>	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 441](#).

**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 403](#).
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 441](#).  
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 401](#).

---

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
☐ OFF

Enable Antivirus and IPS Service
☒ ON

FortiGate	<input type="checkbox"/> All v4	<input type="checkbox"/> 5.0	<input type="checkbox"/> 5.2	<input type="checkbox"/> 5.4	<input type="checkbox"/> 5.6
FortiClient	<input type="checkbox"/> All v4	<input type="checkbox"/> 5.0	<input type="checkbox"/> 5.2	<input type="checkbox"/> 5.4	
FortiAnalyzer	<input type="checkbox"/> All v4	<input checked="" type="checkbox"/> 5.0	<input checked="" type="checkbox"/> 5.2	<input checked="" type="checkbox"/> 5.4	
FortiMail	<input type="checkbox"/> All v4	<input type="checkbox"/> All v5			

Enable Web Filter Service
☐ OFF

Enable Email Filter Service
☐ OFF

Upload Options for FortiGate/FortiMail

Antivirus/IPS Packages	<input type="button" value="Upload"/>
Web Filter Database	<input type="button" value="Upload"/>
Email Filter Database	<input type="button" value="Upload"/>
Service License	<input type="button" value="Upload"/>

Upload Options for FortiClient

Antivirus/IPS Packages	<input type="button" value="Upload"/>
------------------------	---------------------------------------

### 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

#### AntiVirus/IPS Packages

Select to upload antivirus and 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.

#### Web Filter Database

Select to upload the web filter database. 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 401](#).

#### Email Filter Database

Select to upload the email filter database. Browse for the file you downloaded from the Customer Service & Support portal on your management computer. 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 401](#).

**Service License**

Select to import the FortiGate 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.

**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>
```

## 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 441](#) 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.

## 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 430](#).
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:**

1. Go to *FortiGuard > Settings*.
2. Ensure that *Communication with FortiGuard Server* is set to *Global Servers*.
3. Under *FortiGuard Antivirus and IPS Settings*:
  - a. 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.
  - b. 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.
4. Under *FortiGuard Web Filter and Email Filter Settings*:
  - a. 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.
  - b. 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.
5. 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 update, 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 405](#).

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 396](#).
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 is different 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 398](#).

## 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 396](#).
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 408](#).

---

## Accessing public FortiGuard web and email filter servers

You can configure the FortiManager system 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 devices which 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 396](#).
3. Under the *Advanced* heading, toggle *ON* beside *Log Update Entries from FDS 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 device which uses the 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 Filtering and Email Filter Settings*.
3. Configure the log settings, then click *Apply*:

<b>Log FortiGuard Server Update Events</b>	Enable or disable logging of FortiGuard server update events.
<b>FortiGuard Web Filtering</b>	
<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.
<b>FortiGuard Anti-spam</b>	
<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.
<b>FortiGuard Anti-virus Query</b>	
<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 scheduled next, to synchronize them with the 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 backup or restore this customized database (for FortiGate units).

## Licensing status

FortiManager includes a licensing overview page that allows you to view license information for all managed FortiGate devices. To view the licensing status, go to *FortiGuard > Licensing Status*.

This page displays the following information:

<b>Refresh</b>	Select the refresh icon to refresh the information displayed on this page.
<b>Hide/Show license expired devices only</b>	Toggle to hide and display devices with an expired license only.
<b>Search</b>	Use the search field to find a specific device in the table.
<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>	ADOM information. You can change the order that ADOMs are listed by clicking the column title.
<b>Antivirus</b>	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
<b>IPS</b>	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
<b>Email Filtering</b>	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
<b>Web Filtering</b>	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
<b>Mobile Malware</b>	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
<b>Support</b>	The license status and expiration date. You can change the order that devices are listed by clicking the column title.

### Icon states:

- Green: License OK
- Orange: License will expire soon
- Red: License has expired

## Package management

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>Search</b>	Use the search field to find a specific object in the table.
<b>Seq.#</b>	The sequence number.
<b>Object Name</b>	The name of the object.
<b>Object Type</b>	The type of object for the package.
<b>Package Received</b>	The name of the package.
<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. Select <i>Change</i> to change the version.
<b>Update History</b>	Select 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>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.

## Query server management

The query server manager shows when updates are received 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 the FortiManager device.

### 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>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.

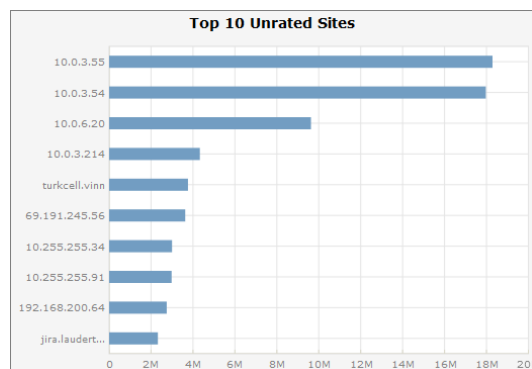
It shows the update times, the events that occurred, the statuses of the updates, and the versions downloaded.



## 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:

<b>Top 10 Unrated Sites</b>	Displays the top 10 unrated sites and the number of events. Hover the cursor over a row to see the exact number of queries.
<b>Top 10 Devices</b>	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.
<b>Number of Queries</b>	Displays the number of queries over a period of time.

## 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, and FortiExtender.

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:

<b>Import Images</b>	Select to open the firmware image import list.
<b>Models</b>	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.
<b>Product</b>	Select a managed product type from the dropdown list.
<b>Search</b>	Use the search field to find a specific entry in the table.

<b>Seq.#</b>	The sequence number.
<b>Model</b>	The device model number that the firmware is applicable to.
<b>Latest Version (Release Date/Time)</b>	The latest version of the firmware that is available.
<b>Preferred Version</b>	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.
<b>Size</b>	The size of the firmware image.
<b>Status</b>	The status of the image, that is, from where it is available.
<b>Action Status</b>	The status of the current action being taken.
<b>Release Notes</b>	A link to a copy of the release for the firmware image that has been downloaded.
<b>Download/Delete</b>	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.

# Locks for Restricting Configuration Changes

Workspace 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. It can only be enabled or disabled from the CLI.

In Normal 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 419](#).

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.

## To enable or disable workspace:

1. Go to *System Settings > Dashboard*.
2. In the *CLI Console* widget 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.

---

## Normal mode

Normal 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 normal 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 452](#)).

---



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 97](#).

---

## Enable normal mode

Normal mode can only be enabled or disabled from the CLI.

---



After changing the workspace mode, your session will end, and you will be required to log back in to the FortiManager.

---

**To enable normal mode:**

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 normal
end
```

---



When `workspace-mode` is normal, *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.

---

## Locking an ADOM

In normal 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 417](#) and [Locking a policy package on page 418](#).

---

**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 normal 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 452](#)).

---

**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 normal 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.

---

## 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 only be enabled or disabled from the CLI.



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:

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 487](#), and each administrator must have a contact email address configured, see [Managing administrator accounts on page 498](#).



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*.

**New Approval Matrix**

ADOM	fgt54-2	
Approval Group # 1	<div style="border: 1px solid #ccc; padding: 2px;"> <span style="border: 1px solid #ccc; padding: 0 5px;">✖ TLeela</span> <span style="border: 1px solid #ccc; padding: 0 5px;">✖ PJFry</span> </div>	-
Approval Group # 2	<div style="border: 1px solid #ccc; padding: 2px;"> <span style="border: 1px solid #ccc; padding: 0 5px;">✖ BBRodriguez</span> <span style="border: 1px solid #ccc; padding: 0 5px;">✖ HConrad</span> </div>	+ -
Send an Email Notification to	<div style="border: 1px solid #ccc; padding: 2px;"> <span style="border: 1px solid #ccc; padding: 0 5px;">✖ admin</span> </div>	
Mail Server	localMail	

OK
Cancel



## 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 487</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 420](#).

## 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 426](#).
5. Click *Create New Session*.

6. Enter a name for session, add a comment describing the session, then click *OK* to start the session. You can now make the required changes to the policy packages and objects. See [Firewall Policy & Objects on page 156](#).

## 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 422](#).
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"	"vpnmgr_tet_spoke2hub"				

**firewall DoS-policy - added (1)**

Seq.#	Policy ID	Interface	Source	Destination	Service	Policy Section	Install On	Others
Added 1	1	"vpnmgr_tet_mesh"	"test_local_subnet_1"	"test_local_subnet_2"	"AH"			

**firewall shaoine-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 420](#)), 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 426](#).
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 426](#).
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 426](#).
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.

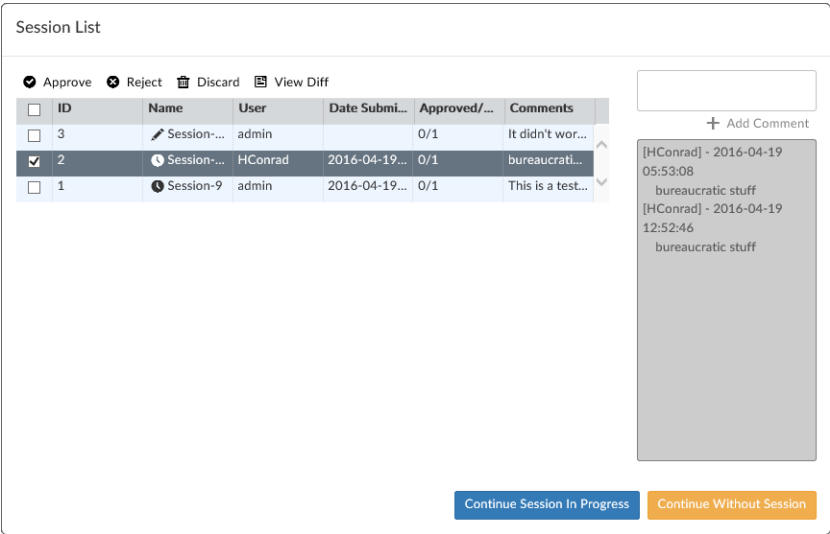
When a session is reverted, a new session is created and automatically submitted for approval.

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 426](#).
- 4. Select the session, then click *Revert*.

The session list

To view the session list, In *Policy & Objects*, go to *Sessions > Session List*. Different options will be available depending on the various states of the sessions (in progress, approved, etc.). When an ADOM is unlocked, only the comments and *View Diff* command are available.



The following options and information are available:

Approve	Approve the selected session. Enter comments in the <i>Approve Session</i> dialog box as required.
Reject	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.
Discard	Discard the selected session. If a session is discarded, all later sessions are also discarded.
Repair	Repair the selected rejected session. A new session will be created and added to the top of the session list with the changes from the rejected session so they can be repaired as needed.
Revert	Revert back to the selected session, undoing all the changes made by later sessions. A new session will be created, added to the top of the session list, and automatically submitted for approval.

<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.

# 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.

---

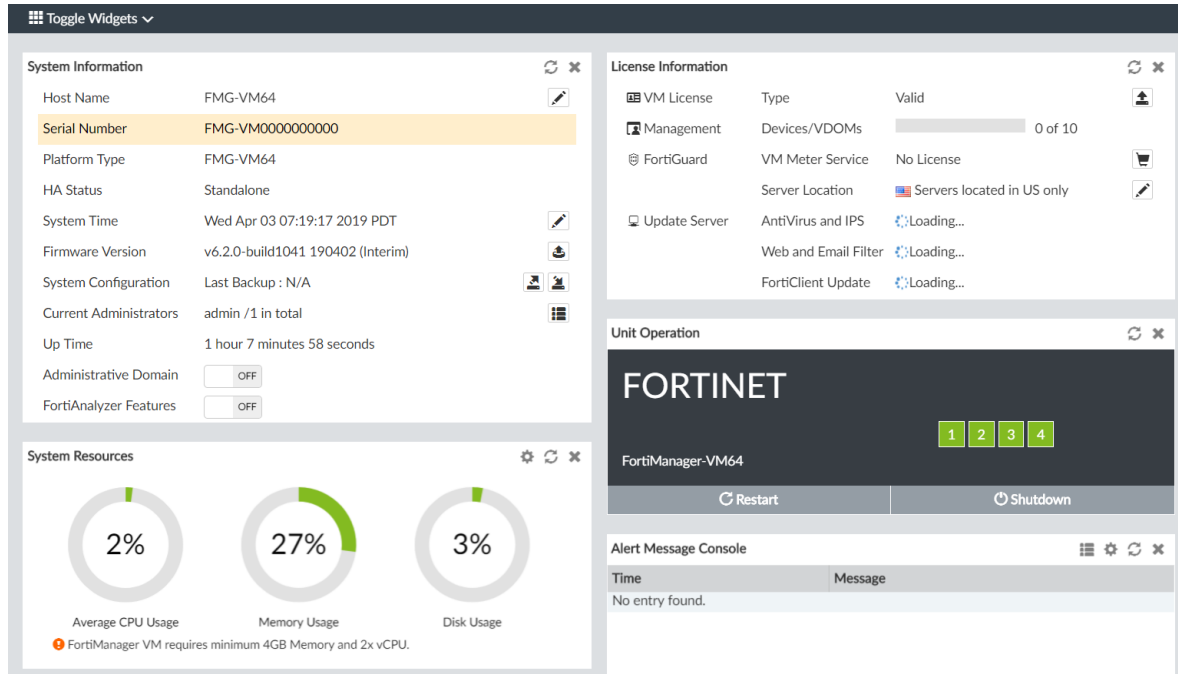
This section contains the following topics:

- [Dashboard on page 429](#)
- [Logging Topology on page 440](#)
- [Network on page 441](#)
- [RAID Management on page 444](#)
- [Administrative Domains on page 450](#)
- [Certificates on page 464](#)
- [Fetcher Management on page 469](#)
- [Event Log on page 474](#)
- [Task Monitor on page 476](#)
- [SNMP on page 478](#)
- [Mail Server on page 487](#)
- [Syslog Server on page 489](#)
- [Meta Fields on page 490](#)
- [Device logs on page 491](#)
- [File Management on page 495](#)
- [Advanced Settings on page 496](#)



## 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 431</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 433</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 436</a>.</p>
<b>License Information</b>	<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 436</a>.</p> <p>From this widget you can manually upload a license for VM systems.</p>

Widget	Description
<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 437</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 438</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 438</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 439</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 439</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 440</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 440</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.
<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.

Action	Steps
<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 432</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 537</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 432</a> .
<b>Firmware Version</b>	The version number and build number of the firmware installed on the FortiManager unit. To update the firmware, you must download the latest version from the Customer Service & 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 433</a> .
<b>System Configuration</b>	The date of the last system configuration backup. The following actions are available: <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 434</a>.</li> <li>Click the restore to restore the configuration from a backup file; see <a href="#">Restoring the configuration on page 435</a>. You can also migrate the configuration to a different FortiManager model by using the CLI. See <a href="#">Migrating the configuration on page 435</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 451</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. See <a href="#">FortiAnalyzer Features on page 18</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>Sync Interval</b>	Enter how often, in minutes, the device should synchronize its time with the NTP server. For example, entering 1440 causes the Fortinet unit to synchronize its time once a day.
<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> .

- Click the checkmark to apply your changes.

## Updating the system firmware

To take advantage of the latest features and fixes, FortiManager provides two ways to upgrade its firmware: manually or through the FDN. For information about upgrading your FortiManager device, see the *FortiManager Upgrade Guide*, or contact Fortinet Customer Service & Support.



Backup the configuration and database before changing the firmware of your FortiManager unit. 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 434](#).



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

### To manually update the FortiManager firmware:

- Download the firmware (the .out file) from the Customer Service & Support website, <https://support.fortinet.com/>.
- Go to *System Settings > Dashboard*.
- In the *System Information* widget, in the *Firmware Version* field, click *Upgrade Firmware*. The *Firmware Upload* dialog box opens.

4. 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*.
5. 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](#).

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



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 [Device Firmware and Security Updates on page 394](#).

The FortiManager firmware can also be updated through the FDN. For more information, see [Firmware images on page 413](#).

## 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 perform a back up after making any changes to the FortiManager configuration or settings that affect the connected devices.

You can perform backups manually or at scheduled intervals. You can also create a backups - called checkpoints - that define a point where the FortiManager and network management is stable and functioning. Should any future configurations cause issues, you have a point where the system is stable.

Fortinet recommends backing up all configuration settings from your FortiManager unit before upgrading the FortiManager firmware.

### 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.

## Restoring the configuration

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

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



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

### To restore the FortiManager configuration:

1. Go to *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.

### To migrate the FortiManager configuration:

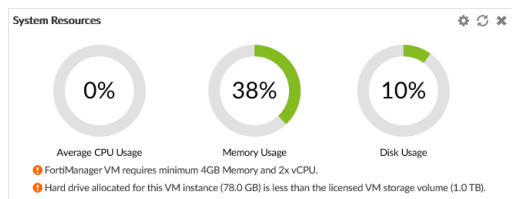
1. In one FortiManager model, go to *System Settings > Dashboard*.
2. Back up the system. See [Backing up the system on page 434](#).
3. In the other FortiManager model, go to *System Settings > Dashboard*.
4. In the *CLI Console* widget, type the following command:  

```
execute migrate all-settings <ftp | scp | sftp> <server> <filepath> <user> <password>
[cryptpasswd]
```

## 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 14](#)). 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	Type	Valid UUG	
Management	Devices/VDOMs	5 of 1,000,000,000	
	FortiGates/Logging Devices	5	
	FortiAPs	26	
FortiGuard	VM Meter Service	No License	
	Server Location	Global Servers	
Update Server	AntiVirus and IPS	288.88.888.88 (Cmymam, BC, Canada)	
	Web and Email Filter	188.888.888.885 (Snnnyrnln, CA, United States)	
	FortiClient Update	88.88.88.885 (Snnnyrnln, CA, United States)	

### VM License

VM license information and status.

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.

### Management

#### Device/VDOMs

The total number of devices and VDOMs connected to the FortiManager and the total number of device and VDOM licenses.

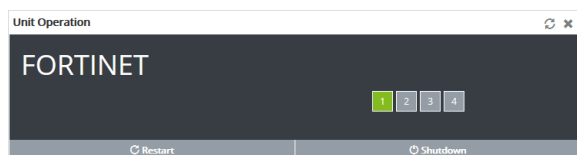


<b>FortiGates/Logging Devices</b>	The number of connected FortiGates and other logging devices.
<b>FortiAPs</b>	The number of connected FortiAPs.
<b>Logging</b>	This section is only shown when <i>FortiAnalyzer Features</i> is enabled. For more information, see <a href="#">FortiAnalyzer Features on page 18</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>VM Storage</b>	The amount of VM storage used and remaining. This field is only visible for FortiManager VM.
<b>FortiGuard</b>	
<b>VM Meter Service</b>	The license status. Click the purchase button to go to the Fortinet Customer Service & Support website, where you can purchase a license.
<b>Secure DNS Server</b>	The SDNS server license status. Click the upload image button to upload a license key.
<b>Server Location</b>	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.
<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.

## 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.

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.

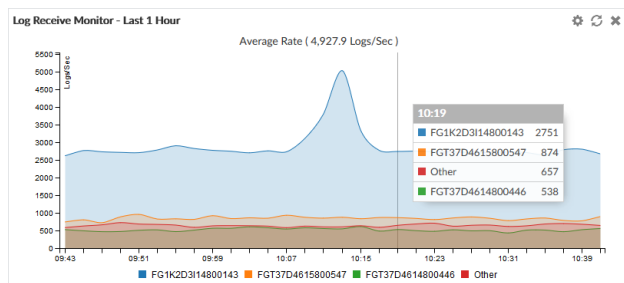
Click *Edit* from the widget toolbar to view the *Alert Message Console Settings*, where you can adjust the number of entries that are visible in the widget, and the refresh interval.

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 18](#).

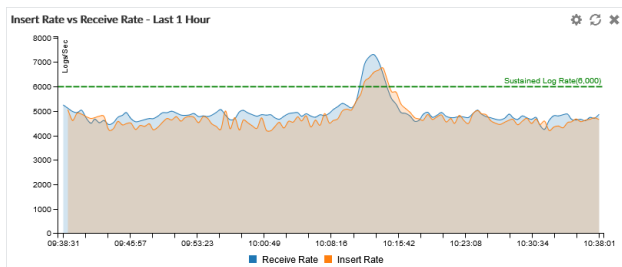
## Insert Rate vs Receive Rate widget

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.

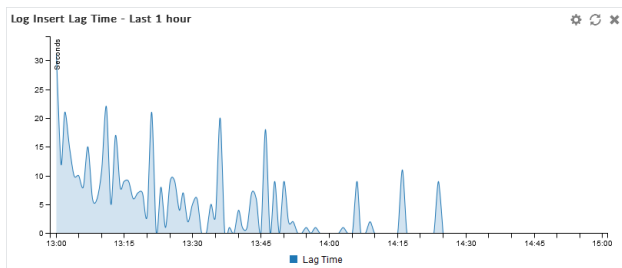


This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 18](#).

## 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.

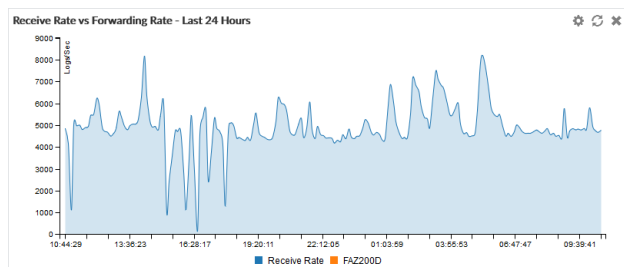


This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 18](#).

## 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.

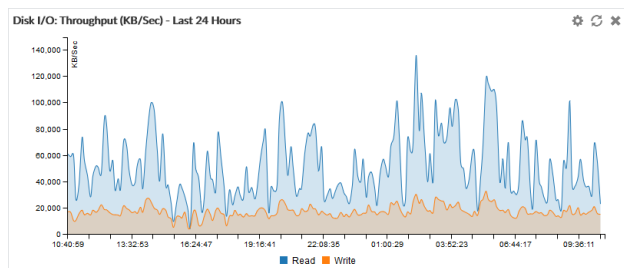


This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 18](#).

## 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.



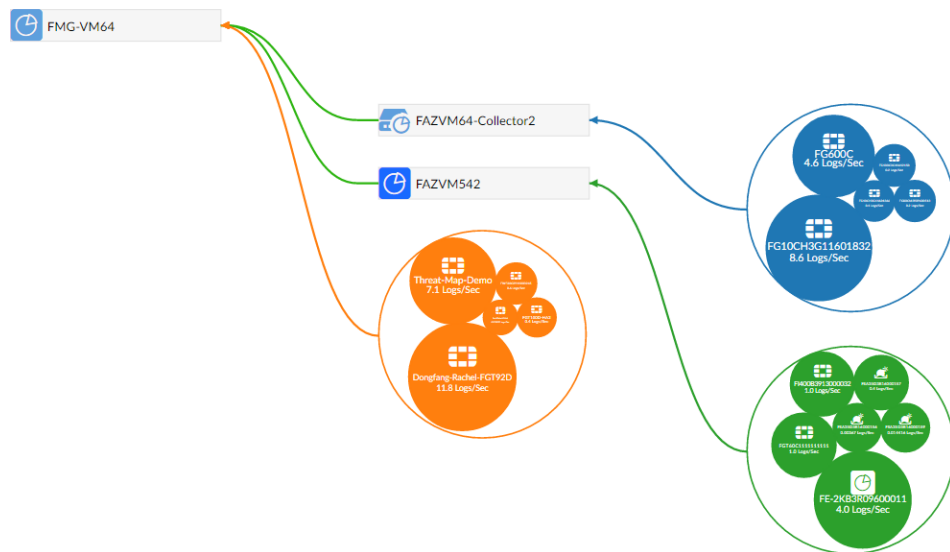
This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 18](#).

## 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 18](#).

## 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.

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 497](#) and [Managing administrator accounts on page 498](#).

## 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 *System Network Management Interface* pane is displayed.

The screenshot shows the 'System Network Management Interface' configuration window for 'port1'. The fields are as follows:

- Name: port1
- IP Address/Netmask: 10.21.1.175/255.255.255.0
- 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
- Default Gateway: 10.21.1.1
- Primary DNS Server: 208.91.112.52
- Secondary DNS Server: 208.91.112.53

At the bottom, there are three tabs: 'All Interfaces' (selected), 'Routing Table', and 'IPv6 Routing Table'.

2. Configure the following settings for *port1*, then click *Apply* 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>	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.
<b>Default Gateway</b>	The default gateway associated with this interface.
<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* 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. 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* 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. 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 IPv4 and IPv6, if applicable.
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* and clicking *Routing Table* and *IPv6 Routing Table*.

### To add a static route:

1. From the IPv4 or IPv6 routing table, click *Create New* in the toolbar. The *Create New Network Route* pane opens.
2. Enter the destination IP address and netmask, or IPv6 prefix, and gateway in the requisite fields.
3. Select the network interface that connects to the gateway from the dropdown list.
4. Click *OK* to create the new static route.

**To edit a static route:**

1. From the IPv4 or IPv6 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 IPv4 or IPv6 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.

## 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 438](#).

#### Summary



RAID Level

Status

Disk Space Usage



Raid-10 [\[Change\]](#)

System is functioning normally.

1890GB Used/ 5442GB Free/ 7332GB Total

#### 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 438](#).



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 437](#) for information.
4. Configure the RAID level. See [Configuring the RAID level on page 447](#).
5. If you backed up the log data, restore it.

## Administrative Domains

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 497](#).



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 [Adding FortiAnalyzer devices on page 49](#).

## Default ADOMs

FortiManager includes default ADOMs for specific types of devices. When you add one or more of these devices to the 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.

## 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*, *FortiClient Manager*, and *VPN Manager* panes are displayed per ADOM. If FortiAnalyzer features are enabled, the *SOC*, *Log View*, *Incidents & Events*, and *Reports* panes are also displayed per ADOM. You select the ADOM you need to work in when you log into the FortiManager unit. [Switching between ADOMs on page 17](#).



ADOMs must be enabled to support FortiMail and FortiWeb logging and reporting. When a FortiMail or FortiWeb device is promoted to the DVM table, the device is added to their respective default ADOM and will be visible in the left-hand tree menu.

---



FortiGate and FortiCarrier devices cannot be grouped into the same ADOM. FortiCarrier devices are added to a specific default FortiCarrier ADOM.

---

### To enable the ADOM feature:

1. Log in to the FortiManager as a super user administrator.
2. Go to *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 460](#).  
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

An ADOM has 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.

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.

## 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*
- *SOC*
- *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 Policy* button on the *Device Manager* pane.

All imported objects are stored in the Device Manager database. They are not stored in the central database, which is used to store objects used in policies.

### To import 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 objects after adding devices:

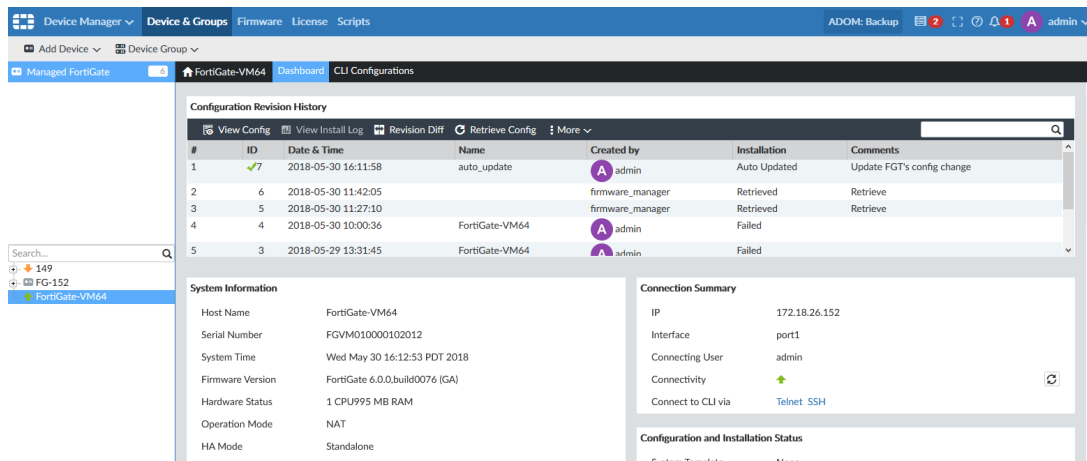
1. Go to *Device Manager > Device & Groups*.
2. Select a device and click *Import Policy*.  
The objects are imported into the Device Manager database.
3. Go to the *Policy & Objects* pane to view the objects.  
You can also create, edit, and delete objects.

## 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 [System dashboard widgets on page 63](#).



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 451](#).

To create and manage ADOMs, go to *System Settings > All ADOMs*.

+ Create New Edit Delete Enter ADOM More					
<input type="checkbox"/>	Name	Firmware Version	Central VPN	Allocated Storage	Devices
▼ Central Management (4)					
<input type="checkbox"/>	ADOM-2	FortiGate 5.4	✗	1000.0 MB	> 1 Device (including 0 VDOM)
<input type="checkbox"/>	FortiCarrier	FortiCarrier 5.4	✗	1000.0 MB	
<input type="checkbox"/>	root	FortiGate 5.4	✓	1000.0 MB	> 1 Device (including 0 VDOM)
<input type="checkbox"/>	Global Database	Global 5.4	✗	-	
▼ Backup Mode (1)					
<input type="checkbox"/>	FG52	FortiGate 5.2	✓	1000.0 MB	
▼ Other Device Types (11)					
<input type="checkbox"/>	FortiAnalyzer	FortiAnalyzer	✗	1000.0 MB	
<input type="checkbox"/>	FortiAuthenticator	FortiAuthenticator	✗	1000.0 MB	
<input type="checkbox"/>	FortiCache	FortiCache	✗	1000.0 MB	
<input type="checkbox"/>	FortiClient	FortiClient	✗	1000.0 MB	
<input type="checkbox"/>	FortiDDoS	FortiDDoS	✗	1000.0 MB	
<input type="checkbox"/>	FortiMail	FortiMail	✗	1000.0 MB	
<input type="checkbox"/>	FortiManager	FortiManager	✗	1000.0 MB	
<input type="checkbox"/>	FortiSandbox	FortiSandbox	✗	1000.0 MB	
<input type="checkbox"/>	FortiWeb	FortiWeb	✗	1000.0 MB	
<input type="checkbox"/>	Syslog	Syslog	✗	1000.0 MB	
<input type="checkbox"/>	Chassis	-	✗	-	

### Create New

Create a new ADOM. See [Creating ADOMs on page 456](#).

### Edit

Edit the selected ADOM. This option is also available from the right-click menu. See [Editing an ADOM on page 460](#).

### Delete

Delete the selected ADOM or ADOMs. You cannot delete default ADOMs. This option is also available from the right-click menu. See [Deleting ADOMs on page 460](#).

<b>Enter ADOM</b>	Switch to the selected ADOM. This option is also available from the right-click menu.
<b>More</b>	Select <i>Expand Devices</i> to expand all of the ADOMs to show the devices in each ADOM. Select <i>Collapse Devices</i> to collapse the device lists. Select <i>Upgrade</i> to upgrade the ADOM; see <a href="#">ADOM versions on page 461</a> . These options are also available from the right-click menu.
<b>Search</b>	Enter a search term to search the ADOM list.
<b>Name</b>	The name of the ADOM. ADOMs are listed in the following groups: <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.
<b>Firmware Version</b>	The firmware version of the ADOM. Devices in the ADOM should have the same firmware version. See <a href="#">ADOM versions on page 461</a> for more information.
<b>Central VPN</b>	Whether or not central VPN management is enabled for the ADOM.
<b>Allocated Storage</b>	The amount of hard drive storage space allocated to the ADOM.
<b>Devices</b>	The number of devices and VDOMs that the ADOM contains. The device list can be expanded or by clicking the triangle.

## Creating ADOMs

To create a new ADOM, you must be logged in as a super user administrator.

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 452](#).
- When FortiAnalyzer features are enabled, you can configure how an ADOM handles log files from its devices. For example, you can configure how much disk space an ADOM can use for logs, and then monitor how much of the allotted disk space is used. You can also specify how long to keep logs indexed in the SQL database and how long to keep logs stored in a compressed format.

### To create an ADOM

1. Ensure that ADOMs are enabled. See [Enabling and disabling the ADOM feature on page 451](#).
2. Go to *System Settings > All ADOMs*.

3. Click *Create New* in the toolbar. The *Create New ADOM* pane is displayed.

**Create New ADOM**

Name:

Type:  6.0 5.6 5.4 5.2

Devices:

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

Central Management: ☐ VPN ☒ FortiAP ☐ SD-WAN

Mode: ☒ Normal ☐ Backup ☐ Unselect All

Default Device Selection for Install: ☒ Select All ☐ Unselect All

Perform Policy Check Before Every Install: ☒ ON ☐ OFF

Action When Conflicts Occur During Policy Check: ☒ Continue Installation ☐ Stop Installation

Auto-Push Policy Packages When Device Back Online: ☐ Enable ☒ Disable

Data Policy: Keep Logs for Analytics:  Days

Keep Logs for Archive:  Days

Disk Utilization: Maximum Allowed:  MB Available: 0.0 KB

Analytics: Archive:  30% ☐ Modify

Alert and Delete When Usage Reaches:

\*If analytic or archive log usages exceed the configured disk quota before the retention period expires, the oldest logs will be deleted.

4. 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 either FortiGate or FortiCarrier 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 458</a> .
<b>Central Management</b>	Select the <i>VPN</i> checkbox to enable central VPN management. Select the <i>SD-WAN</i> checkbox to enable central SD-WAN management. Select the <i>FortiAP</i> checkbox to enable central FortiAP management. This checkbox is selected by default. This option is only available when the <i>Mode</i> is <i>Normal</i> .
<b>Mode</b>	Select <i>Normal</i> mode if you want to manage and configure the connected FortiGate devices from the FortiManager GUI. Select <i>Backup</i> mode if you want to backup the FortiGate configurations to the FortiManager, but configure each FortiGate locally. See <a href="#">ADOM modes on page 452</a> for more information.
<b>Default Device Selection for Install</b>	Select either <i>Select All</i> or <i>Unselect 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 170</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 18</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>SOC &gt; FortiView, Incidents &amp; Events</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>SOC &gt; FortiView, Incidents &amp; Events</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 18</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 452](#)). 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 456](#).

---

**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 513](#)), 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 458](#).

### 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.

---



## ADOM versions

ADOMs can concurrently manage FortiGate units running FortiOS 5.4, 5.6, and 6.0 allowing devices running these versions to share a common database. This allows you to continue to manage an ADOM as normal while upgrading the devices within that ADOM.

When adding a new FortiGate unit to an ADOM, the FortiGate unit should have the same FortiOS version as the ADOM.



This feature can be used to facilitate upgrading to new firmware.  
Importing policies from devices running higher versions than the ADOM is not supported.  
Installation to devices running higher versions is supported.

---



For a complete list of supported devices and firmware versions, see the FortiManager Release Notes.

---

Each ADOM is associated with a specific FortiOS 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 456](#)), and can be updated only after all of the devices within the ADOM have been updated to the same FortiOS firmware version.

The general steps for upgrading an ADOM containing multiple devices running FortiOS 5.4 from 5.4 to 5.6 are as follows:

1. In the ADOM, upgrade one of the FortiGate units to FortiOS 5.6, and then resynchronize the device. See [Firmware on page 87](#) for more information.  
All of the ADOM objects, including Policy Packages, remain as 5.4 objects.
  2. Upgrade the rest of the FortiGate units in the ADOM to FortiOS 5.6.
  3. Upgrade the ADOM to 5.6. See [Upgrading an ADOM on page 464](#) for more information.  
All of the database objects will be converted to 5.6 format, and the GUI content for the ADOM will change to reflect 5.6 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 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 463](#)

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.

**To enable workspace mode, and disable concurrent ADOM access:**

1. Enter the following CLI commands:

```
config system global
    set workspace-mode normal
end
```

**To disable workspace mode, and enable concurrent ADOM access:**

1. Enter the following CLI commands:

```
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
```



After changing the workflow mode, your session will end and you will be required to log back in to the FortiManager.

---

## Locking an ADOM

If workspace is enabled, you must lock an ADOM prior to performing device-level changes to it. 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.



An ADOM can only be upgraded after all the devices within the ADOM have been upgraded. See [ADOM versions on page 461](#) for more information.

### To upgrade an ADOM:

1. Go to *System Settings > All ADOMs*.
2. Right-click on an ADOM and select *Upgrade*, or 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.  
If all of the devices within the ADOM are not already upgraded, the upgrade will be aborted and an error message will be shown. Upgrade the remaining devices within the ADOM, then return to step 1 to try upgrading the ADOM again.

## 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>	<p>Select the ID type from the dropdown list:</p> <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>	Click <i>Browse...</i> and locate the key file on the management computer, or drag and drop the file onto the dialog box. This option is only available when <i>Type</i> is <i>Certificate</i> .
<b>Password</b>	Enter the certificate password. This option is only available when <i>Type</i> is <i>PKCS #12 Certificate</i> or <i>Certificate</i> .
<b>Certificate Name</b>	Enter the certificate name. This option is only available when <i>Type</i> is <i>PKCS #12 Certificate</i> or <i>Certificate</i> .

## Deleting local certificates

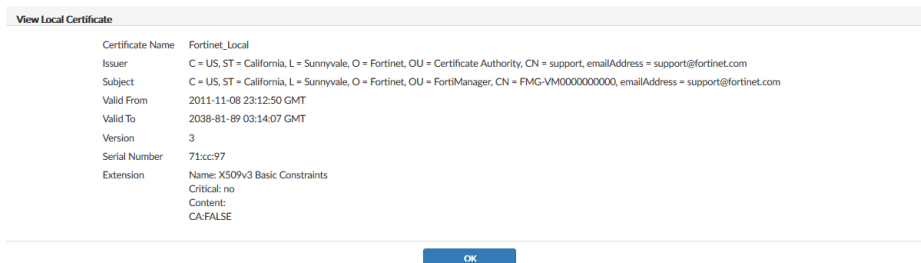
### To delete a local certificate or certificates:

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.



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.

# Fetcher Management

Log fetching is used to retrieve archived logs from one FortiManager device to another. This allows administrators to run queries and reports against historic data, which can be useful for forensic analysis.

The fetching FortiManager can query the server FortiManager and retrieve the log data for a specified device and time period, based on specified filters. The retrieved data are then indexed, and can be used for data analysis and reports.

Log fetching can only be done on two FortiManager devices running the same firmware. A FortiManager device can be either the fetch server or the fetching client, and it can perform both roles at the same time with different FortiManager devices. Only one log fetching session can be established at a time between two FortiManager devices.

The basic steps for fetching logs are:

1. On the client, create a fetching profile. See [Fetching profiles on page 470](#).
2. On the client, send the fetch request to the server. See [Fetch requests on page 471](#).

3. If this is the first time fetching logs with the selected profile, or if any changes have been made to the devices and/or ADOMs since the last fetch, on the client, sync devices and ADOMs with the server. See [Synchronizing devices and ADOMs on page 473](#).
4. On the server, review the request, then either approve or reject it. See [Request processing on page 473](#).
5. Monitor the fetch process on either FortiManager. See [Fetch monitoring on page 474](#).
6. On the client, wait until the database is rebuilt before using the fetched data for analysis.



This pane is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 18](#).

## Fetching profiles

Fetching profiles can be managed from the *Profiles* tab on the *System Settings > Fetcher Management* pane.

Profiles can be created, edited, and deleted as required. The profile list shows the name of the profile, as well as the IP address of the server it fetches from, the server and local ADOMs, and the administrator name on the fetch server.

### To create a new fetching profile:

1. On the client, go to *System Settings > Fetcher Management*.
2. Select the *Profiles* tab, then click *Create New* in the toolbar, or right-click and select *Create New* from the menu. The *Create New Profile* dialog box opens.

3. Configure the following settings, then click *OK* to create the profile.

<b>Name</b>	Enter a name for the profile.
<b>Server IP</b>	Enter the IP address of the fetch server.
<b>User</b>	Enter the username of an administrator on the fetch server, which, together with the password, authenticates the fetch client's access to the fetch server.
<b>Password</b>	Enter the administrator's password, which, together with the username, authenticates the fetch client's access to the fetch server.



The fetch server administrator user name and password must be for an administrator with either a *Standard\_User* or *Super\_User* profile.

**To edit a fetching profile:**

1. Go to *System Settings > Fetching Management*.
2. Double-click on a profile, right-click on a profile then select *Edit*, or select a profile then click *Edit* in the toolbar. The *Edit Profile* pane opens.
3. Edit the settings as required, then click *OK* to apply your changes.

**To delete a fetching profile or profiles:**

1. Go to *System Settings > Fetching Management*.
2. Select the profile or profiles 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 profile or profiles.

## Fetch requests

A fetch request requests archived logs from the fetch server configured in the selected fetch profile. When making the request, the ADOM on the fetch server the logs are fetched from must be specified. An ADOM on the fetching client must be specified or, if needed, a new one can be created. If logs are being fetched to an existing local ADOM, you must ensure the ADOM has enough disk space for the incoming logs.

The data policy for the local ADOM on the client must also support fetching logs from the specified time period. It must keep both archive and analytics logs long enough so they will not be deleted in accordance with the policy. For example: Today is July 1, the ADOM's data policy is configured to keep analytics logs for 30 days (June 1 - 30), and you need to fetch logs from the first week of May. The data policy of the ADOM must be adjusted to keep analytics and archive logs for at least 62 days to cover the entire time span. Otherwise, the fetched logs will be automatically deleted after they are fetched.

**To send a fetch request:**

1. On the fetch client, go to *System Settings > Fetcher Management* and select the *Profiles* tab
2. Select the profile then click *Request Fetch* in the toolbar, or right-click and select *Request Fetch* from the menu. The *Fetch Logs* dialog box opens.

Fetch Logs

Name

FAZVM64

Server IP

222.222.222.222

User

admino

Secure Connection

☒

Server ADOM

root

Local ADOM

root

Devices

FortiGate-VM64

Select Device +

Enable Filters

☐

Time Period

2017/01/30

09

10

2017/02/04

09

10

Index Fetched Logs

☒

Request Fetch

Cancel

- Configure the following settings, then click *Request Fetch*.

The request is sent to the fetch server. The status of the request can be viewed in the *Sessions* tab.

<b>Name</b>	Displays the name of the fetch server you have specified.
<b>Server IP</b>	Displays the IP address of the server you have specified.
<b>User</b>	Displays the username of the server administrator you have provided.
<b>Secure Connection</b>	Select to use SSL connection to transfer fetched logs from the server.
<b>Server ADOM</b>	Select the ADOM on the server the logs will be fetched from. Only one ADOM can be fetched from at a time.
<b>Local ADOM</b>	Select the ADOM on the client where the logs will be received. Either select an existing ADOM from the dropdown list, or create a new ADOM by entering a name for it into the field.
<b>Devices</b>	Add the devices and/or VDOMs that the logs will be fetched from. Up to 256 devices can be added. Click <i>Select Device</i> , select devices from the list, then click <i>OK</i> .
<b>Enable Filters</b>	Select to enable filters on the logs that will be fetched. Select <i>All</i> or <i>Any of the Following Conditions</i> in the <i>Log messages that match</i> field to control how the filters are applied to the logs. Add filters to the table by selecting the <i>Log Field</i> , <i>Match Criteria</i> , and <i>Value</i> for each filter.
<b>Time Period</b>	Specify what date and time range of log messages to fetch.
<b>Index Fetch Logs</b>	If selected, the fetched logs will be indexed in the SQL database of the client once they are received. Select this option unless you want to manually index the fetched logs.

## Synchronizing devices and ADOMs

If this is the first time the fetching client is fetching logs from the device, or if any changes have been made the devices or ADOMs since the last fetch, then the devices and ADOMs must be synchronized with the server.

### To synchronize devices and ADOMs:

1. On the client, go to *System Settings > Fetcher Management* and select the *Profiles* tab
2. Select the profile then click *Sync Devices* in the toolbar, or right-click and select *Sync Devices* from the menu. The *Sync Server ADOM(s) & Device(s)* dialog box opens and shows the progress of the process. Once the synchronization is complete, you can verify the changes on the client. For example, newly added devices in the ADOM specified by the profile.



If a new ADOM is created, the new ADOM will mirror the disk space and data policy of the corresponding server ADOM. If there is not enough space on the client, the client will create an ADOM with the maximum allowed disk space and give a warning message. You can then adjust disk space allocation as required.

## Request processing

After a fetching client has made a fetch request, the request will be listed on the fetch server in the *Received Request* section of the *Sessions* tab on the *Fetcher Management* pane. It will also be available from the notification center in the GUI banner.

Fetch requests can be approved or rejected.

### To process the fetch request:

1. Go to the notification center in the GUI banner and click the log fetcher request, or go to the *Sessions* tab on the *System Settings > Fetcher Management* pane.

Expand All Collapse All				
Request Time	Host/Server IP	User	Status	Action
Received Request(1)				
15:01:55	FAZVM64(FAZ-VM00000000001)	admino	Waiting for approval	<a href="#">Review</a>
Fetch Request(1)				

2. Find the request in the *Received Request* section. You may have to expand the section, or select *Expand All* in the content pane toolbar. The status of the request will be *Waiting for approval*.
3. Click *Review* to review the request. The *Review Request* dialog box will open.

Review Request

Host Name

FAZVM64

Serial No.

FAZ-VM0000000000

Version

v5.6.0

User

Agg

Devices

ADOM	Device	VDOM
root	FGVMEV0000000000	*

Filters

None

Time Period

16:02 2016/01/30 - 16:02 2017/02/02

Secure Connection

☒

Approve

Reject

Close

- Click *Approve* to approve the request, or click *Reject* to reject the request.

If you approve the request, the server will start to retrieve the requested logs in the background and send them to the client. If you reject the request, the request will be canceled and the request status will be listed as *Rejected* on both the client and the server.

## Fetch monitoring

The progress of an approved fetch request can be monitored on both the fetching client and the fetch server.

Go to *System Settings > Fetcher Management* and select the *Sessions* tab to monitor the fetch progress. A fetch session can be paused by clicking *Pause*, and resumed by clicking *Resume*. It can also be canceled by clicking *Cancel*.

Once the log fetching is completed, the status changes to *Done* and the request record can be deleted by clicking *Delete*. The client will start to index the logs into the database.



It can take a long time for the client to finish indexing the fetched logs and make the analyzed data available. A progress bar is shown in the GUI banner; for more information, click on it to open the *Rebuild Log Database* dialog box.

Log and report features will not be fully available until the rebuilding process is complete.

## 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.

Add Filter <input type="text"/>						
Last 1 Day May 28 To May 29						
Download Raw Log Historical Log						
#	Date Time	Level	User	Sub Type	Description	Message
1	2018-05-29 14:20:18	notice	admin-GUI(172.18.26.1)	System manager event	CLI execution info	path=system.log-fetch.client ^ mP34AgCu6bvslx64BD8OF //otJysxG1cKhWjSf7mPJm
2	2018-05-29 14:08:31	information	system	FortiAnalyzer system event	Configuration database object changed	[create] configuration datab
3	2018-05-29 13:36:14	notice	admin-GUI(172.18.26.1)	Device manager event	Device Manager dvm log at notice level	Edited device FG-152 (FGV
4	2018-05-29 13:33:26	notice	admin-GUI(172.18.26.1)	Device manager event	Device Manager dvm log at notice level	Edited device FG-152 (FGV
5	2018-05-29 13:33:15	information	admin	Device manager event	Device manager generic information log	Device FG-152 add succee
6	2018-05-29 13:33:14	notice	admin-GUI(172.18.26.1)	Device manager event	Device Manager dvm log at notice level	Added device FG-152 (FGV

The following options are available:

<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 476</a> .
<b>Last...</b>	Select the amount of time to show from the available options, or select a custom time span or any time.
<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> dropdown list, select the event type (<i>All Event</i>, <i>Push Update</i>, <i>Poll Update</i>, or <i>Manual Update</i>) from the Event dropdown list, and then click <i>Go</i> to browse the logs.</li> </ul> This option is only available when viewing historical logs.
<b>Search</b>	Enter a search term to search the historical logs. This option is only available when viewing historical event logs.
<b>Pagination</b>	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>Device ID</b>	The ID of the related device.		
<b>Sub Type</b>	The log sub-type: <table data-bbox="560 1749 1458 1797"> <tr> <td>System manager event</td><td>HA event</td></tr> </table>	System manager event	HA event
System manager event	HA event		

	FG-FM protocol event	Firmware manager event
	Device configuration event	FortiGuard service event
	Global database event	FortiClient manager event
	Script manager event	FortiMail manager event
	Web portal event	Debug I/O log event
	Firewall objects event	Configuration change event
	Policy console event	Device manager event
	VPN console event	Web service event
	Endpoint manager event	FortiAnalyzer event
	Revision history event	Log daemon event
	Deployment manager event	FIPS-CC event
	Real-time monitor event	Managed devices event
	Log and report manager event	
<b>User</b>	The user that the log message relates to.	
<b>Description</b>	A description of the event.	
<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 FortiView summaries using the toolbar:

- Specify filters in the *Add Filter* box.
  - Regular Search: In the selected summary view, click in the *Add Filter* box, select a filter from the dropdown list, then type a value. Click NOT to negate the filter value. You can add multiple filters at a time, and connect them with an "or".
  - Advanced Search: Click the *Switch to Advanced Search* icon at the right end of the *Add Filter* box to switch to advanced search mode. In this mode, you type in the whole search criteria (log field names and values). Click the *Switch to Regular Search* icon to return to regular search.
- Click *Go* to apply the filter.

## Task Monitor

Using the task monitor, you can 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 496](#).

Delete View: All						
<< first < prev 1 2 3 4 5 next > last >> 25						
<input type="checkbox"/>	ID	Source	Description	User	Status	Start Time ADOM
<input checked="" type="checkbox"/>	3611	Policy Consistency Check	Policy Check	admin	90%	Tue May 29 08:43:50 2018 FG60
< prev 1 next > (1 of 1) Total:1 Pending:0 In Progress:1 Completed ( Success:0 Warning:0 Error:0 ) 1 FG60 90% generating report						
< prev 1 next > (1 of 1)						
<input type="checkbox"/>	3610	Install Package	Copy Package 'Root/FortiGate-VM64_root'	admin	✖	Tue May 29 08:43:47 2018 FG60
<input type="checkbox"/>	3609	Import Wizard	Import Device Objs/Policy	admin	✔	Tue May 29 08:41:01 2018 FG60
<input type="checkbox"/>	3608	Import Wizard	Import Device Objs/Policy	admin	✔	Tue May 29 08:40:48 2018 FG60
<input type="checkbox"/>	3607	Import Wizard	Import Device Objs/Policy	admin	✔	Tue May 29 08:40:34 2018 FG60
<input type="checkbox"/>	3606	Device Manager	Retrieve Device Configuration	firmware_manager	✔	Tue May 29 08:35:18 2018 FG60
<input type="checkbox"/>	3605	Firmware Manager	Device Image Upgrade	admin	✔	Tue May 29 08:32:25 2018 FG60
<input type="checkbox"/>	3604	Device Manager	Add/delete Unregistered Devices	admin	✔	Tue May 29 08:31:10 2018 FG60

The following options are available:

<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</b>	Select which tasks to view from the dropdown list, based on their status. The available options are: <i>Running</i> , <i>Pending</i> , <i>Done</i> , <i>Error</i> , <i>Cancelling</i> , <i>Cancelled</i> , <i>Aborting</i> , <i>Aborted</i> , <i>Warning</i> , and <i>All</i> .
<b>Expand Arrow</b>	In the <i>Source</i> column, select the expand arrow icon to display the specific actions taken under this task. To filter the specific actions taken for a task, select one of the options on top of the action list. Select the history icon to view specific information on task progress. This can be useful when troubleshooting warnings and errors.
<b>Group Error Devices</b>	Select <i>Group Error Devices</i> to create a group of the failed devices, allowing for re-installations to easily be done on only the failed devices.
<b>History</b>	Click the history icon to view task details in a new window.
<b>Pagination</b>	Browse the pages of tasks and adjust the number of tasks shown per page.

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. Click the expand arrow to view details of the specific task and access the history button.
<b>Description</b>	The nature of the task. Click the arrow 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 (hover over the icon to view the description):</p> <ul style="list-style-type: none"> <li>• <i>Done</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>Start Time</b>	The time that the task was started.
<b>ADOM</b>	The ADOM associated with the task.
<b>History</b>	Click the history button to view task details.

## 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

<input type="checkbox"/> Community Name	Queries	Traps	Enable
<input type="checkbox"/> Solara	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Terminus	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Trantor	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

SNMP v3

+ Create New

☒ Edit

☐ Delete

<input type="checkbox"/> User Name	Security Level	Notification Hosts	Queries
<input type="checkbox"/> Bliss	No Authentication, No Privacy		<input checked="" type="checkbox"/>
<input type="checkbox"/> Daneel	Authentication, No Privacy		<input checked="" type="checkbox"/>
<input type="checkbox"/> Fallom	Authentication, Privacy		<input checked="" type="checkbox"/>
<input type="checkbox"/> Golan	No Authentication, No Privacy		<input checked="" type="checkbox"/>

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 480</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 483</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	<input type="text" value="161"/>	<input checked="" type="checkbox"/>
v2c	<input type="text" value="161"/>	<input checked="" type="checkbox"/>

Traps:

Protocol	Port	Enable
v1	<input type="text" value="162"/>	<input checked="" type="checkbox"/>
v2c	<input type="text" value="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>
<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:

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>	The security level of the user. Select one of the following: <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>

Trap message	Description
<b>Memory low</b> (fnTrapMemThreshold)	Memory usage exceeds 90 percent. This threshold can be set in the CLI using the following commands: <pre>config system snmp sysinfo     set trap-low-memory-threshold &lt;percentage value&gt; end</pre>
<b>Log disk too full</b> (fnTrapLogDiskThreshold)	Log disk usage has exceeded the configured threshold. Only available on devices with log disks.
<b>Temperature too high</b> (fnTrapTempHigh)	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</b> (fnTrapVoltageOutOfRange)	Power levels have fluctuated outside of normal levels. Not all devices have voltage monitoring instrumentation.
<b>Power supply failure</b> (fnTrapPowerSupplyFailure)	Power supply failure detected. Available on some devices that support redundant power supplies.
<b>Interface IP change</b> (fnTrapIpChange)	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</b> (fnTrapHASwitch)	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.

**Create New Mail Server Settings**

SMTP Server Name

Mail Server

SMTP Server Port

Enable Authentication ☐

E-Mail Account

Password

OK Cancel

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>	Select to enable 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.



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

IP address (or FQDN)

Syslog Server Port

3. Configure the following settings and then select *OK* to create the mail 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.

### 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.

## Meta Fields

Meta fields allow administrators to add extra information when configuring, adding, or maintaining FortiGate units or adding new administrators. You can make the fields mandatory or optional, and set the length of the field.

With the fields set as mandatory, administrators must supply additional information when they create a new FortiGate object, such as an administrator account or firewall policy. Fields for this new information are added to the FortiGate unit dialog boxes in the locations where you create these objects. You can also provide fields for optional additional information.

The one exception to this is the *System Administrators* object. This object applies only to administrators on the FortiManager unit. All other objects are related to FortiGate units.

Go to *System Settings > Advanced > Meta Fields* to configure meta fields. Meta fields can be added, edited, and deleted.

+ Create New Edit Delete Expand All Collapse All			
<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"/> City	50	Optional	Enabled
<input type="checkbox"/> Company/Organization	50	Optional	Enabled
<input type="checkbox"/> Contact	50	Optional	Enabled
<input type="checkbox"/> Country	50	Optional	Enabled
<input type="checkbox"/> Province/State	50	Optional	Enabled
▼ Device Group			
▼ Administrative Domain			
▶ Firewall Address (1)			
▼ Firewall Address Group			
▶ Central NAT (3)			
▼ Firewall Service			
▶ Firewall Service Group (2)			
▶ Firewall Policy (2)			



Select *Expand All* or *Contract All* from the toolbar or right-click menu to view all of 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

Devices

Name

Length

20

Importance

☐ Optional
 ☒ Required

Status

☐ Disabled
 ☒ Enabled

OK

Cancel

3. Configure the following settings and then select *OK* to create the meta field.

<b>Object</b>	The object this metadata field applies to: <i>System Administrators, Devices, Device Groups, Chassis, Administrative Domain, Firewall Addresses, Firewall Address Groups, Firewall Services, Firewall Service Groups, or Firewall Policy.</i>
<b>Name</b>	Enter the label to use for the field.
<b>Length</b>	Select the maximum number of characters allowed for the field from the dropdown list: <i>20, 50, or 255.</i>
<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.

#### To edit a meta field:

1. Go to *System Settings > Advanced > Meta Fields*.
2. Double-click on a field, right-click on a field and then select *Edit* from the menu, or select a field then click *Edit* in the toolbar. The *Edit Meta Fields* pane opens.
3. Edit the settings as required, and then click *OK* to apply the changes.



The *Object* and *Name* fields cannot be edited.

#### To delete a meta field or fields:

1. Go to *System Settings > Advanced > Meta Fields*.
2. Select the field or fields you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation box to delete the field or fields.



The default meta fields cannot be deleted.

## Device logs

The FortiManager allows you to log system events to disk. You can control device log file size and the use of the FortiManager unit's disk space by configuring log rolling and scheduled uploads to a server.

As the FortiManager unit receives new log items, it performs the following tasks:

- Verifies whether the log file has exceeded its file size limit.
- Checks to see if it is time to roll the log file if the file size is not exceeded.

When a current log file (`tlog.log`) reaches its maximum size, or reaches the scheduled time, the FortiManager unit rolls the active log file by renaming the file. The file name will be in the form of `xlog.N.log` (for example, `tlog.1252929496.log`), where `x` is a letter indicating the log type and `N` is a unique number corresponding to the time the first log entry was received. The file modification time will match the time when the last log was received in the log file.

Once the current log file is rolled into a numbered log file, it will not be changed. New logs will be stored in the new current log called `tlog.log`. If log uploading is enabled, once logs are uploaded to the remote server or downloaded via the GUI, they are in the following format:

```
FG3K6A3406600001-tlog.1252929496.log-2017-09-29-08-03-54.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 18](#).

## Configuring rolling and uploading of logs using the GUI

Go to *System Settings > Advanced > Device Log Setting* to configure device log settings.

Device Log Settings

Registered Device Logs

Roll log file when size exceeds  (10-1000)MB  
☒ Roll log files at scheduled time  
Daily  Hour  Minute  
☒ Upload logs using a standard file transfer protocol  
Upload Server Type   
Upload Server IP   
User Name   
Password   
Remote Directory   
Upload Log Files ☒ When rolled ☐ Daily at  Hour  
☐ Upload log files in gzip file format  
☐ Delete log files after uploading

Local Device Log

☒ Send the local event logs to FortiAnalyzer/FortiManager  
IP Address   
Upload Option ☒ Real-time ☐ Schedule Time  
Severity Level   
☒ Reliable log transmission  
☐ Secure connection

Apply



Configure the following settings, and then select *Apply*:

<b>Registered Device Logs</b>	
<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**

☐ Device log files older than 365 Days Scheduled daily at time 00:00

☐ Reports older than 365 Days Scheduled daily at time 00:00

☐ Content archive files older than 365 Days Scheduled daily at time 00:00

☐ 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 18](#).

## 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>	Select the ADOM mode, either <i>Normal</i> or <i>Advanced</i> . 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.
<b>Download WSDL file</b>	Select the required WSDL functions then click the <i>Download</i> button to download the WSDL file to your management computer. When selecting <i>Legacy Operations</i> , no other options can be selected. Web services is a standards-based, platform independent, access method for other hardware and software APIs. The file itself defines the format of commands the FortiManager will accept as well as the responses to expect. Using the WSDL file, third-party or custom applications can communicate with the FortiManager unit and operate it or retrieve information, just as an administrator can from the GUI or CLI.
<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>Policy Hit Count</b>	Enable or disable policy hit counting.
<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="#">Display options on page 160</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.

# 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 529](#) for more information.

In workflow mode, approval matrices can be create and managed on the *Approval Matrix* pane. See [Workflow approval on page 420](#) for more information.

This section contains the following topics:

- [Trusted hosts on page 497](#)
- [Monitoring administrators on page 498](#)
- [Disconnecting administrators on page 498](#)
- [Managing administrator accounts on page 498](#)
- [Administrator profiles on page 513](#)
- [Authentication on page 520](#)
- [Global administration settings on page 529](#)
- [Two-factor authentication on page 533](#)

## 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 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.

<a href="#">+ Create New</a> <a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Delete</a> <a href="#">Table View</a> <a href="#">Column Settings</a>							
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 roet	fg54:default roet: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 500</a> .
<b>Edit</b>	Edit the selected administrator. See <a href="#">Editing administrators on page 504</a> .
<b>Clone</b>	Clone the selected administrator.
<b>Delete</b>	Delete the selected administrator or administrators. See <a href="#">Deleting administrators on page 504</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 504</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 513</a>
<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 497</a> .

<b>Trusted IPv6 Hosts</b>	The IPv6 trusted host(s) associated with the administrator. See <a href="#">Trusted hosts on page 497</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 to an account with sufficient privileges, or 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 520](#) 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.

**New Administrator**

Avatar + Add Photo Remove Photo

Comments  0/127

Admin Type RADIUS

RADIUS Server

☐ Match all users on remote server

New Password  👁

Confirm Password  👁

Admin Profile Restricted\_User

Administrative Domain All ADOMs All ADOMs except specified ones Specify

Policy Package Access All Packages Specify

Trusted Hosts OFF

Meta Fields ▼

Contact Email  *Optional*

Contact Phone  *Optional*

Advanced Options ▼

change-password disable

ext-auth-accprofile-override disable

ext-auth-adom-override disable

ext-auth-group-match

first-name

last-name

mobile-number

pager-number

restrict-access disable

rpc-permit none

OK Cancel

3. Configure the following settings, and then click *OK* to create the new administrator.

<b>User Name</b>	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>	Optionally, enter a description of the administrator, such as their role, location, or the reason for their account.
<b>Admin Type</b>	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> , or <i>Group</i> . See <a href="#">Authentication on page 520</a> for more information.

<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 set the password as a wildcard.</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>Wildcard</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>Wildcard</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>
<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 531</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 513</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 on page 450</a>.</p>

<b>Policy Package Access</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 505</a>.</p>
<b>Web Filter Profile</b>	<p>Select the web filter profiles that the restricted administrator will be able to edit.</p> <p>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 215</a>.</p>
<b>IPS Sensor</b>	<p>Select the IPS profiles that the restricted administrator will be able to edit.</p> <p>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 215</a>.</p>
<b>Application Sensor</b>	<p>Select the application control profiles that the restricted administrator will be able to edit.</p> <p>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 215</a>.</p>
<b>Trusted Hosts</b>	<p>Optionally, turn on trusted hosts, then enter their IP addresses and netmasks. Up to ten IPv4 and ten IPv6 hosts can be added.</p> <p>See <a href="#">Trusted hosts on page 497</a> for more information.</p>
<b>Meta Fields</b>	<p>Optionally, enter the new administrator's email address and phone number.</p> <p>The email address is also used for workflow session approval notifications, if enabled. See <a href="#">Workflow mode on page 419</a>.</p>
<b>Advanced Options</b>	<p>Configure advanced options, see <a href="#">Advanced options</a> below.</p> <p>For more information on advanced options, see the <i>FortiManager CLI Reference</i>.</p>

### 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.	disable

Option	Description	Default
<b>ext-auth-group-match</b>	Specify the group configured on a Remote Authentication Server.	-
<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
<b>rpc-permit</b>	Select the RPC permit.	none

## 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 14](#) 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
```

## 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.

---



Restricted administrators cannot be used when workflow mode is enabled. See [Workflow mode on page 419](#).

---

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 this 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 and editing quotas. At the bottom is a 'File Filter Rule' section with a table for defining 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 517](#).
2. Create a new administrator and select the restricted administrator profile for the *Admin Profile*, then select the specific ADOM and profiles that the administrator can manage. See [Creating administrators on page 500](#)



Restricted administrators can create new custom signatures for Intrusion Prevention and Application Control.

### To create a custom signature for Intrusion Prevention:

1. Log on as a Restricted Administrator.
2. Go to *Intrusion Prevention > Custom Signatures*.

3. Click *Create New*. The *Create New Custom Signature* screen appears.

Create New Custom Signature

Name

Signature

Status

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.

#### To create a custom signature for Application Control:

1. Log on as a Restricted Administrator.
2. Go to *Application Control > Custom Signatures*.
3. Click *Create New*. The *Create New Custom Application Signature* screen appears.

Create New Custom Application Signature

Name

Signature

Comment

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.

# Web Filter

Select a web filter profile from the tree menu to edit the profile details. Click *Apply* to apply any changes to the profile.

Edit Web Filter Profile

Name

default

Comment

Default web filtering.22/255

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	<div>Configure advanced options, including:<ul style="list-style-type: none"><li><code>https-replacemsg</code>: enable/disable</li><li><code>replacemsg-group</code>: select a group from the list</li><li><code>web-filter-activex-log</code>: enable/disable</li><li><code>web-filter-command-block-log</code>: enable/disable</li><li><code>web-filter-cookie-removal-log</code>: enable/disable</li><li><code>web-filter-js-log</code>: enable/disable</li><li><code>web-filter-jscript-log</code>: enable/disable</li><li><code>web-filter-referer-log</code>: enable/disable</li><li><code>web-filter-unknown-log</code>: enable/disable</li><li><code>web-filter-vbs-log</code>: enable/disable</li><li><code>wisp</code>: enable/disable</li><li><code>wisp-algorithm</code>: <i>auto-learning</i>, <i>primary-secondary</i>, or <i>round-robin</i></li></ul></div>
Inspection Mode	Select <i>Proxy</i> or <i>Flow Based</i> .
Log all URLs	Select to log all URLs.
FortiGuard Categories	<div>Select FortiGuard categories.</div> <div>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>.</div> <div>Use the filter drop-down menu to filter the categories shown in the table based on the action.</div>



<b>Allow Users to override blocked categories</b>	Select to allow users to override blocked categories. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
<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>	Enter the duration of the switch. This option is only available if <i>Switch Duration</i> is <i>constant</i> .
<b>Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex</b>	Select to enforce <i>Safe Search</i> . This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
<b>Restrict YouTube Access</b>	Select to restrict access to YouTube. Select <i>Strict</i> or <i>Moderate</i> . This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
<b>Log all search keywords</b>	Select to log all search keywords. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
<b>Block Invalid URLs</b>	Select to block invalid URLs. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
<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> .

## Intrusion Prevention

Select an IPS profile from the tree menu to edit the profile details. Click *Apply* to apply any changes to the profile.

Edit IPS Profile

Name

all\_default

Comments

All predefined signatures with default setting. 47/255

IPS Signatures

+ Add Signatures

Delete

Edit IP Exemptions

<input type="checkbox"/>	Name	Exempt IPs	Severity	Target	Service	OS	Action	Status	Packet Logging	Applications	ID	Revision
--------------------------	------	------------	----------	--------	---------	----	--------	--------	----------------	--------------	----	----------

IPS Filters

+ Add Filter

Edit Filter

Delete

<input type="checkbox"/>	Filter Details	Action	Packet Logging
<input type="checkbox"/>		Default	

Rate Based Signatures

Enable	Signature	Threshold	Duration(Seconds)	Track By	Action	Block Duration
<input type="checkbox"/>	Digium.Asterisk.File.Descriptor.DoS	20	1	Any	block	None
<input type="checkbox"/>	Digium.Asterisk.IAX2.Call.Number.DoS	275	1	Any	block	None
<input type="checkbox"/>	DotNetNuke.Padding.Oracle.Attack	1000	5	Any	block	None
<input type="checkbox"/>	FTP.Login.Brute.Force	200	10	Any	block	None
<input type="checkbox"/>	FreeBSD.TCP.Reassembly.DoS	10	2	Any	block	None
<input type="checkbox"/>	IMAP.Login.Brute.Force	60	10	Any	block	None
<input type="checkbox"/>	MS.Active.Directory.LDAP.Packet.L.Handling.DoS	100	1	Any	block	None
<input type="checkbox"/>	MS.OWA.Brute.Force	15	1	Any	block	None
<input type="checkbox"/>	MS.RDP.Connection.Brute.Force	200	10	Any	block	None
<input type="checkbox"/>	MS.Windows.Group.Policy.Security.Feature.Bypass	5	2	Any	block	None
<input type="checkbox"/>	MS.Windows.SMB.NTLM.Authentication.Lack.Of.Entropy	35	1	Any	block	None
<input type="checkbox"/>	MS.Windows.SMB.Server.NTLM.Authentication.Bypass	1000	1	Any	block	None
<input type="checkbox"/>	MS.XML.Core.Services.Memory.Corruption	5	10	Any	block	None
<input type="checkbox"/>	MySQL.Login.Brute.Force	60	60	Any	block	None
<input type="checkbox"/>	Novell.Open.Enterprise.Server.HTTPSTK.Service.DoS	18	1	Any	block	None
<input type="checkbox"/>	POP3.Login.Brute.Force	200	10	Any	block	None
<input type="checkbox"/>	SMB.Login.Brute.Force	500	60	Any	block	None
<input type="checkbox"/>	SSH.Connection.Brute.Force	200	10	Any	block	None
<input type="checkbox"/>	Telnet.Login.Brute.Force	60	60	Any	block	None
<input type="checkbox"/>	Wordpress.Login.Brute.Force	1000	10	Any	block	None

Advanced Options

Apply

### Name

The profile name.

### Comment

Optionally, enter a description of the profile.

### IPS Signatures

Click *Add Signatures* to add IPS signatures to the table. The signatures list can be filtered to simplify adding them.

To add or edit a signature's IP exemptions, select a signature then click *Edit IP Exemptions*.

Right-click on a signature to change the action (*Pass*, *Monitor*, *Block*, *Reset*, *Default*, or *Quarantine*), and to enable or disable *Packet Logging*.

**IPS Filters**

Click *Add Filter* to add IPS filters to the table. The filters list can be searched and filtered to simplify adding them.

Right-click on a signature to change the action (*Pass*, *Monitor*, *Block*, *Reset*, *Default*, or *Quarantine*), and to enable or disable *Packet Logging*.

**Rate Based Signatures**

Enable the required rate based signatures, then configure its options: *Threshold*, *Duration*, *Track By*, *Action*, and *Block Duration*.

**Advanced Options**

Enable or disable blocking malicious URLs.

## Application Control

Select an application control profile from the tree menu to edit the profile details. Click *Apply* to apply any changes to the profile.

**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 type="button" value="Allow"/> Unknown Applications

**Application Overrides**

+ Add Signatures ☒ Edit Parameters ☐ Delete

Application Signature	Category	Action
-----------------------	----------	--------

**Filter Overrides**

+ Add Filter ☒ Edit ☐ Delete

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*).

<b>Deep Inspection of Cloud Applications</b>	Select to enable deep inspections of cloud applications.
<b>Allow and Log DNS Traffic</b>	Select to allow and log DNS traffic.
<b>Replacement Messages for HTTP-based Applications</b>	Select to enable replacement messages for HTTP based applications.
<b>Logging of Other Applications</b>	Select to enable the logging of other applications.
<b>Logging of Unknown Applications</b>	Select to enable the logging of unknown applications.
<b>Advanced Options</b>	Configure advanced options: <ul style="list-style-type: none"> <li>• p2p-block-list: Select from <i>bittorent</i>, <i>edonkey</i>, and <i>skype</i>.</li> <li>• replacemsg-group: Select an option from the dropdown list.</li> </ul>

## 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.

+ Create New Edit Clone Delete					
<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 517</a> .
<b>Edit</b>	Edit the selected profile. See <a href="#">Editing administrator profiles on page 519</a> .
<b>Clone</b>	Clone the selected profile. See <a href="#">Cloning administrator profiles on page 519</a> .
<b>Delete</b>	Delete the selected profile or profiles. See <a href="#">Deleting administrator profiles on page 520</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.

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

Setting	Predefined Administrator Profile			
	Super User	Standard User	Restricted User	Package User
<b>FortiGuard Center</b> <b>fgd_center</b>	Read-Write	None	None	Read-Only
<b>License Management</b> <b>fgd-center-licensing</b>	Read-Write	None	None	Read-Only
<b>Firmware Management</b> <b>fgd-center-fmw-mgmt</b>	Read-Write	None	None	Read-Only
<b>Advanced</b> <b>fgd-center-advanced</b>	Read-Write	None	None	Read-Only
<b>Device Manager</b> <b>device-manager</b>	Read-Write	Read-Write	Read-Only	Read-Write
<b>Add/Delete/Edit Devices/Groups</b> <b>device-op</b>	Read-Write	Read-Write	None	Read-Write
<b>Retrieve Configuration from Devices</b> <b>config-retrieve</b>	Read-Write	Read-Write	Read-Only	Read-Only
<b>Revert Configuration from Revision History</b> <b>config-revert</b>	Read-Write	Read-Write	Read-Only	Read-Only
<b>Delete Device Revision</b> <b>device-revision-deletion</b>	Read-Write	Read-Write	Read-Only	Read-Write
<b>Terminal Access</b> <b>term-access</b>	Read-Write	Read-Write	Read-Only	Read-Only
<b>Manage Device Configurations</b> <b>device-config</b>	Read-Write	Read-Write	Read-Only	Read-Write
<b>Provisioning Templates</b> <b>device-profile</b>	Read-Write	Read-Write	Read-Only	Read-Write

Setting		Predefined Administrator Profile			
		Super User	Standard User	Restricted User	Package User
	<b>SD-WAN</b> device-wan-link-load-balance	Read-Write	Read-Write	Read-Only	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> adom-policy-packages	Read-Write	Read-Write	Read-Only	Read-Write
	<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>Lock/Unlock ADOM</b> adom-lock		Read-Write	Read-Write	Read-Only	Read-Write
<b>Lock/Unlock Device/Policy Package</b> device-policy-package-lock		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>		Read-Write	Read-Write	Read-Only	Read-Write



Setting	Predefined Administrator Profile			
	Super User	Standard User	Restricted User	Package User
<b>device-ap</b>				
<b>FortiClient Manager</b> device-forticlient	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>SOC</b> log-viewer	Read-Write	Read-Write	Read-Only	Read-Only
<b>Log View/FortiView/SOC</b> log-viewer	Read-Write	Read-Write	Read-Only	Read-Only
<b>Incidents &amp; Events</b> event-management	Read-Write	Read-Write	Read-Only	Read-Only
<b>Reports</b> report-viewer	Read-Write	Read-Write	Read-Only	Read-Only
<b>CLI only settings</b>				
realtime-monitor	Read-Write	Read-Write	Read-Only	Read
read-passwd	Read-Write	None	None	Read-Only



The SOC setting is only available when FortiAnalyzer features are disabled. The *Log View/FortiView/SOC*, *Incidents & Events*, and *Reports* settings are only available when FortiAnalyzer features are enabled. See [FortiAnalyzer Features on page 18](#).

## 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

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"/>
Advanced	<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"/>
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"/>
Lock/Unlock ADOM	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Lock/Unlock Device/Policy Package	<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"/>
FortiClient 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"/>
Log View/FortiView/NOC - SOC	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Event Manager	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Reports	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Privacy Masking

ON

Masked Data Fields

☐ Domain
 ☐ Destination Name
 ☐ Source IP
 ☐ Destination IP
 ☐ User
 ☐ Source Name
 ☐ Email
 ☐ Message
 ☐ Source MAC

Data Mask Key

OK

Cancel

3. Configure the following settings, and then click *OK* to create the new administrator profile.

<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 Profile</i> , <i>Application Filter</i> , and <i>IPS Sensor</i> . This option is only available when <i>Type</i> is <i>Restricted Admin</i> . See <a href="#">Restricted administrators on page 505</a> for information.
<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.

## 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 delete.

### 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.

## 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 520](#) 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 523](#), [RADIUS servers on page 525](#), [TACACS+ servers on page 526](#), and [Remote authentication server groups on page 527](#) 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)

### To get the CA certificate:

1. Log into your FortiAuthenticator.
2. Go to *Certificate Management > Certificate Authorities > Local CAs*.
3. Select the certificate and select *Export* in the toolbar to save the `ca_fortinet.com` CA certificate to your management computer. The saved CA certificate's filename is `ca_fortinet.com.crt`.

**To get the administrator certificate:**

1. Log into your FortiAuthenticator.
2. Go to *Certificate Management > End Entities > Users*.
3. Select the certificate and select *Export* in the toolbar to save the administrator certificate to your management computer. The saved CA certificate's filename is `admin_fortinet.com.p12`. This PCKS#12 file is password protected. You must enter a password on export.

**To import the administrator certificate into your browser:**

1. In Mozilla Firefox, go to *Options > Advanced > Certificates > View Certificates > Import*.
2. Select the file `admin_fortinet.com.p12` and enter the password used in the previous step.

**To import the CA certificate into the FortiManager:**

1. Log into your FortiManager.
2. Go to *System Settings > Certificates > 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 500](#) 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 both `set clt-cert-req` and `set admin-https-pki-required` are enabled, only PKI administrators can connect to the FortiManager GUI.

---

## 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 523](#), [RADIUS servers on page 525](#), and [TACACS+ servers on page 526](#) 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 523</a> , <a href="#">RADIUS servers on page 525</a> , and <a href="#">TACACS+ servers on page 526</a> .
<b>Edit</b>	Edit the selected remote authentication server. See <a href="#">Editing remote authentication servers on page 522</a> .
<b>Delete</b>	Delete the selected remote authentication server or servers. See <a href="#">Deleting remote authentication servers on page 523</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 523](#), [RADIUS servers on page 525](#), and [TACACS+ servers on page 526](#) 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	<input type="text"/>
Server Name/IP	<input type="text"/>
Port	<input type="text" value="389"/>
Common Name Identifier	<input type="text" value="cn"/>
Distinguished Name	<input type="text"/>
Bind Type	<input type="text" value="Regular"/>
User DN	<input type="text"/>
Password	<input type="password" value="*****"/>
Secure Connection	<input checked="" type="checkbox"/> Enable
Protocol	<input type="text"/>
Certificate	<input type="text" value="No Certificate"/>
Administrative Domain	<input type="button" value="All ADOMs"/> <input type="button" value="Specify"/>
<b>Advanced Options &gt;</b>	

OK Cancel

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 <code>cn</code> . However, some servers use other common name identifiers such as <code>UID</code> .
<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 <code>(objectclass=*)</code>
<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

test-Radius

Server Name/IP

10.2.0.159

Port

1812

Server Secret

\*\*\*\*\*

Connection Status

✓ Successful

Test Connectivity

Test User Credentials

Secondary Server Name/IP

Secondary Server Secret

\*\*\*\*\*

Test Connectivity

Test User Credentials

Authentication Type

ANY

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.

The screenshot shows a configuration window titled "New TACACS+ Server". It contains the following fields and controls:

- Name:** A text input field.
- Server Name/IP:** A text input field.
- Port:** A text input field with the value "49" and a small dropdown arrow on the right.
- Server Key:** A text input field.
- Authentication Type:** A dropdown menu.
- Buttons:** "OK" (blue) and "Cancel" (orange) buttons at the bottom.

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 all Security Fabric 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 (this feature is currently only supported in 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.



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.



When accessing FortiGate from the *Quick Access* menu, if FGT is set up to use the default login page with SSO options, you must select the *via Single Sign-On* button to be automatically authenticated.

---

### To configure FortiManager as the identity provider:

1. Go to *System Settings > SAML SSO*.
2. Select *Identity Provider (IdP)*.
3. In the *IdP Certificate* dropdown, choose a certificate where IdP is used.
4. Select *Download* to get the IdP certificate, used later to configure SPs.
5. Select *Apply*.
6. In the *SP Settings* table, select *Create* to add a service provider.
7. In the *Edit Service Provider* window:
  - Enter a name for the SP.
  - Select *Fortinet* as the *SP Type*.
    - If the SP is not a Fortinet product, select *Custom* as the *SP Type* and copy the *SP Entity ID*, *SP ACS (Login) URL*, and *SP SLS (Logout) URL* from your SPs configuration page.
  - Enter the SP IP address.
  - Copy down the *IdP Prefix*. It is required when configuring SPs.
8. Select *OK*.
9. A custom login page can be created by moving the *Login Page Template* toggle to the *On* position and selecting *Customize*.

### To configure FortiManager as a service provider:

1. Go to *System Settings > SAML SSO*.
2. Select *Service Provider (SP)*.
3. Select *Fortinet* as the *IdP Type*.
4. Enter the IdP IP address and the IdP prefix that you obtained while configuring the IdP device.
5. 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.

6. Confirm that the information is correct and select *Apply*.
7. Repeat the steps for each FAZ/FMG that is to be set as a service provider.

## 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  
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**

**Administration Settings**

HTTP Port: 80

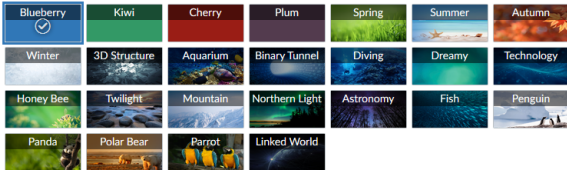
HTTPS Port: 443

HTTPS & Web Service Certificate: server.crt

Idle Timeout: 478  (1-480 Minutes)

**View Settings**

Language: Auto Detect

Theme: 

**Password Policy**

Minimum Length: 8  (8-32 characters)

Must Contain: ☐ Uppercase Letters ☐ Lowercase Letters ☐ Numbers (0-9) ☐ Special Characters

Admin Password Expires after: 0  (days)

**Display Options on GUI**

☒ Show Scripts ☒ Show Add Multiple Button ☒ Show Device List Import/Export Buttons

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 minutes an administrative connection can be idle before the administrator must log in again, from 1 to 480 (8 hours). See <a href="#">Idle timeout on page 532</a> for more information.
View Settings	
<b>Language</b>	Select a language from the dropdown list. See <a href="#">GUI language on page 532</a> for more information.
<b>Theme</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 531</a> and <a href="#">Password lockout and retry attempts on page 531</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.

## Password policy

You can enable and configure password policy for the FortiManager.

### To configure the password policy:

1. Go to *System Settings > Admin > Admin 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
- Spanish
- Traditional Chinese
- Japanese
- Korean

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 five 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. The idle timeout period can be set from 1 to 480 minutes.



**To change the idle timeout:**

1. Go to *System Settings > Admin > Admin Settings*.
2. Change the *Idle Timeout* period as required.
3. Click *Apply*.

## Two-factor authentication

To configure two-factor authentication for administrators 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 *Two-Factor Authenticator Interoperability Guide* and *FortiAuthenticator Administration Guide* in the [Fortinet Document Library](#).

---

**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> .

- Click *OK* to continue to the *Change local user* page.

- 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:

- Go to *Authentication > RADIUS Service > Clients*.
- 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.

### Configure the RADIUS server:

1. Go to *System Settings > Admin > Remote Authentication Server*.
2. Click *Create New > RADIUS* 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>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>Port</b>	Enter the port for FortiAuthenticator traffic.
<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.

**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 500](#).
4. Click *OK* to save the settings.

**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.

# 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.

A FortiManager HA cluster can have a maximum of four units: one primary unit with up to three 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 backup units can be in the same location or different locations. FortiManager HA supports geographic redundancy so the primary unit and backup 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 backup units.

If the primary FortiManager unit fails you must manually configure one of the backup 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 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 HA parameters). As a result, 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

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.

### 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. Interface settings and HA settings are not synchronized. These settings must be configured on each cluster unit.

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.

Configure the following settings:

<b>Cluster Status</b>	Monitor FortiManager HA status. See <a href="#">Monitoring HA status on page 543</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>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>	A password for the HA cluster. All members of the HA cluster must have the same password.  If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different password. The maximum password length is 19 characters.
<b>File Quota</b>	Enter the file quota, from 2048 to 20480 MB (default: 4096 MB).  You cannot configure the file quota for backup units.
<b>Heart Beat Interval</b>	The time the primary unit waits between sending heartbeat packets, in seconds. The heartbeat interval is also the amount of time that backup units waits before expecting to receive a heartbeat packet from the primary unit.  The default heartbeat interval is 5 seconds. The heartbeat interval range is 1 to 255 seconds. You cannot configure the heartbeat interval on the backup units.
<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>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>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>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>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

You can upgrade the firmware of an operating FortiManager cluster in the same way as upgrading the firmware of a standalone FortiManager unit.

To do the upgrade, connect to the primary unit GUI or CLI to upgrade the firmware. Similar to upgrading the firmware of a standalone FortiManager unit, normal FortiManager operations are temporarily interrupted while the cluster firmware upgrades. Because of this interruption, you should upgrade cluster firmware during a maintenance period.

### To upgrade FortiManager HA cluster firmware:

1. Log into the primary unit GUI.

2. Upgrade the primary unit firmware.

The firmware is sent to all backup units, and then all units (primary and backup) are rebooted.

See the *FortiManager Release Notes* and *FortiManager Upgrade Guide* in the [Fortinet Document Library](#) for more information.



You might not be able to connect to the FortiManager GUI until the upgrade synchronization process is complete. During the upgrade, using SSH or telnet to connect to the CLI might be slow. If necessary, use the console to connect to the CLI.

---

# Change Log

Date	Change Description
2019-07-18	Initial release.
2019-07-26	Changed <code>clt-cert-reg</code> to <code>clt-cert-req</code> .
2019-08-30	Modified the <a href="#">High Availability on page 537</a> section.
2019-09-12	Updated the <a href="#">ADOM versions on page 461</a> section.
2019-09-19	Added a note in <a href="#">Tcl scripts on page 113</a> .



**FORTINET®**



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