



FortiManager - Administration Guide

Version 6.4.2

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



May 16, 2022

FortiManager 6.4.2 Administration Guide

02-642-601884-20220516

TABLE OF CONTENTS

Change Log	13
Setting up FortiManager	14
Connecting to the GUI	14
Security considerations	15
Restricting GUI access by trusted host	15
Other security considerations	15
GUI overview	16
Panels	18
Color themes	19
Full-screen mode	19
Switching between ADOMs	19
Using the right-click menu	19
Avatars	19
Showing and hiding passwords	20
FortiAnalyzer Features	20
Enable or disable FortiAnalyzer features	21
Configuring FortiManager appliances	22
Adding devices	22
Installing to managed devices	23
Monitoring managed devices	23
Restarting and shutting down	24
FortiManager Key Concepts	26
FortiManager modules	26
Modules for FortiAnalyzer feature set	27
Object database and FortiManager modules	27
Inside the FortiManager system	28
Communication protocols and devices	28
Object database and devices	29
ADOMs and devices	31
Operations	32
Key features of the FortiManager system	33
Security Fabric	33
Configuration revision control and tracking	34
Centralized management	34
Administrative domains	34
Local FortiGuard service provisioning	34
Firmware management	34
Scripting	34
Logging and reporting	34
Fortinet device life cycle management	35
Firewall Devices	36
ADOMs	37
Adding devices	37
Adding devices using the wizard	38

Authorizing devices	44
Hiding unauthorized devices	45
Adding a FortiGate HA cluster when adding a model device	50
Add a VDOM to a device	52
Adding a Security Fabric group	53
Import policy wizard	54
Configuring the management address	56
Adding FortiAnalyzer devices	57
Adding FortiAnalyzer devices with the wizard	58
Viewing policy rules	61
Importing devices	61
Importing detected devices	61
Importing and exporting device lists	62
Configuring devices	63
Configuring a device	63
Out-of-Sync device	64
Configuring VDOMs	65
Using the device dashboard	67
View system dashboard for managed/logging devices	67
View system interfaces	69
CLI Configurations menu	70
System dashboard widgets	70
Device zones	73
Installing to devices	74
Using the Install Wizard to install policy packages and device settings	74
Using the Install Wizard to install device settings only	76
View a policy package diff	77
Managing devices	78
Using the quick status bar	78
Customizing columns	79
Refreshing a device	79
Editing device information	79
Deleting a device	81
Replacing a managed device	81
Setting unauthorized device options	82
Using the CLI console for managed devices	82
Displaying Security Fabric topology	83
Manage Devices from Map View	83
Managing device configurations	87
View configurations for device groups	88
Checking device configuration status	90
Managing configuration revision history	91
Device groups	95
Default device groups	95
Add device groups	95
Manage device groups	95
Organizing devices using the new folder view	96
Firmware	98

View firmware for device groups	99
Upgrade firmware for device groups	99
Firmware Management	99
Automatic multi-step firmware upgrade on FortiGate	102
Managed devices pull firmware from FortiGuard	104
License	106
License Management	106
Add-on license	108
Provisioning Templates	108
System templates	108
Threat Weight templates	114
Certificate templates	115
Scripts	117
Enabling scripts	118
Configuring scripts	118
CLI script group	123
Script syntax	124
Script history	128
Script samples	128
SD-WAN	149
SD-WAN per-device management	149
SD-WAN central management	158
Monitor SD-WAN	175
FortiExtender	176
FortiMeter	178
Overview	178
Points	179
Authorizing metered VMs	179
Monitoring VMs	180
FortiGate chassis devices	181
Viewing chassis dashboard	182
Firewall Policy & Objects	186
About policies	187
Policy theory	188
Global policy packages	189
Policy workflow	189
Provisioning new devices	189
Day-to-day management of devices	190
Display options	190
Managing policy packages	191
Create new policy packages	191
Create new policy package folders	193
Edit a policy package or folder	193
Clone a policy package	193
Remove a policy package or folder	194
Assign a global policy package	194
Install a policy package	195
Reinstall a policy package	195

Schedule a policy package install	197
Export a policy package	198
Policy package installation targets	198
Perform a policy consistency check	200
View logs related to a policy rule	201
Find and replace objects	202
Managing policies	203
Policy Lookup	205
Creating policies	206
Editing policies	206
Creating Policy Blocks	212
IP policies	214
Create New Firewall Policy	220
Create New Security Policy	223
Virtual wire pair policy	226
NAT policies	228
Proxy policy	229
Central SNAT	232
Central DNAT	233
DoS policies	238
Interface policies	240
Multicast policy	241
Local in policies	242
Traffic shaping policy	243
Managing objects and dynamic objects	245
Create a new object	245
Creating an IPv6 Address Template	250
Promote an Object to Global Database	251
Normalized interfaces	252
Map a dynamic ADOM object	261
Map a dynamic device object	262
Map a dynamic device group	264
Remove an object	265
Edit an object	265
Push to device	266
Clone an object	266
Search objects	266
Find unused objects	267
Find and merge duplicate objects	267
Export signatures to CSV file format	267
CLI Configurations	268
FortiToken configuration example	269
FSSO user groups	269
Interface mapping	272
VIP mapping	273
Modify existing interface-zone mapping	273
Create a new shaping profile	274
Intrusion Prevention filtering options	276
ADOM revisions	277

Fabric View	281
Security Fabric Topology	281
Physical Topology	282
Logical Topology	283
Filter Topology Views	284
Search Topology Views	284
Security Rating	285
Enabling the Security Rating tab	286
Viewing Security Fabric Ratings	286
Security Fabric score	287
Fabric Connectors	288
SDN	288
Threat Feeds	321
Endpoint/Identity	322
FortiView	349
Monitors	349
Device Status	350
Using the Monitors dashboard	351
VPN	353
Overview	353
Enabling central VPN management	354
DDNS support	355
VPN Setup Wizard supports device groups	356
IPsec VPN Communities	369
Managing IPsec VPN communities	369
Creating IPsec VPN communities	370
VPN community settings	372
Monitoring IPsec VPN tunnels	378
Map View	378
IPsec VPN gateways	380
Managing VPN gateways	380
Creating managed gateways	380
Creating external gateways	384
VPN security policies	386
Defining policy addresses	387
Defining security policies	387
SSL VPN	388
Manage SSL VPNs	388
Portal profiles	390
Monitor SSL VPNs	396
Access Points	398
Managed APs	398
Quick status bar	399
Managing APs	400
FortiAP groups	405
Authorizing and deauthorizing FortiAP devices	406
Installing changes to FortiAP devices	406

Rogue APs	406
Authorizing unknown APs	408
Connected clients	409
Spectrum analysis for managed APs	410
Monitor	412
Clients Monitor	412
Health Monitor	413
Map view	415
Google map	415
Floor map	416
WiFi profiles for central management	417
Enabling FortiAP central management	418
AP profiles	418
SSIDs	423
WIDS profiles	431
Bluetooth profiles	435
QoS profiles	437
Bonjour profiles	439
Assigning profiles to FortiAP devices	441
WiFi profiles for per-device management	441
Enabling FortiAP per-device management	442
Creating profiles	442
FortiSwitch Manager	443
Managed Switches	443
Quick status bar	444
Managing FortiSwitches	444
Authorizing and deauthorizing FortiSwitch devices	447
Upgrading firmware for managed switches	447
Using zero-touch deployment for FortiSwitch	448
Installing changes to managed switches	449
Run cable test on FortiSwitch ports from FortiManager	451
Monitor	454
FortiSwitch Templates for central management	455
Enabling FortiSwitch central management	455
FortiSwitch Templates	456
FortiSwitch Profiles for per-device management	467
Enabling per-device management	468
FortiSwitch profiles	468
Configuring a port on a single FortiSwitch	473
Endpoint Compliance	475
How FortiManager fits into endpoint compliance	476
FortiTelemetry	477
Viewing devices	477
Enabling FortiTelemetry on interfaces	478
Enabling endpoint control on interfaces	478
Assigning FortiClient profile packages to devices	479
Monitor	479

Monitoring FortiClient endpoints	479
Monitoring FortiClient endpoints by compliance status	480
Monitoring FortiClient endpoints by interface	481
Exempting non-compliant FortiClient endpoints	481
FortiClient profiles	481
Viewing profile packages	482
Viewing FortiClient profiles	482
Creating FortiClient profile packages	483
Creating FortiClient profiles	483
Editing FortiClient profiles	487
Deleting FortiClient profiles	487
Importing FortiClient profiles	487
Assigning profile packages	487
Device Firmware and Security Updates	489
FDN third-party SSL validation and Anycast support	490
Settings	491
Connecting the built-in FDS to the FDN	494
Operating as an FDS in a closed network	494
Configuring devices to use the built-in FDS	498
Matching port settings	498
Handling connection attempts from unauthorized devices	499
Configure a FortiManager without Internet connectivity to access a local FortiManager as FDS	499
Configuring FortiGuard services	500
Enabling push updates	500
Enabling updates through a web proxy	501
Overriding default IP addresses and ports	502
Scheduling updates	502
Accessing public FortiGuard web and email filter servers	503
Logging events related to FortiGuard services	504
Logging FortiGuard antivirus and IPS updates	504
Logging FortiGuard web or email filter events	504
Restoring the URL or antispam database	505
Licensing status	505
Package management	506
Receive status	506
Service status	507
Query server management	509
Receive status	509
Query status	509
Firmware images	510
Locks for Restricting Configuration Changes	512
Normal mode	512
Enable normal mode	513
Locking an ADOM	513
Locking a device	514
Locking a policy package	515

Lock an individual policy	516
Workflow mode	517
Enable workflow mode	517
Workflow approval	518
Workflow sessions	519
System Settings	526
Dashboard	527
Customizing the dashboard	528
System Information widget	529
System Resources widget	535
License Information widget	536
Registering a device or VM license	537
Unit Operation widget	538
Alert Messages Console widget	538
Log Receive Monitor widget	539
Insert Rate vs Receive Rate widget	539
Log Insert Lag Time widget	540
Receive Rate vs Forwarding Rate widget	540
Disk I/O widget	541
Logging Topology	541
Network	542
Configuring network interfaces	542
Disabling ports	544
Changing administrative access	544
Static routes	544
Packet capture	545
RAID Management	546
Supported RAID levels	546
Configuring the RAID level	549
Monitoring RAID status	549
Checking RAID from command line	550
Swapping hard disks	551
Adding hard disks	552
Administrative Domains	552
Enabling and disabling the ADOM feature	553
ADOM device modes	554
ADOM modes	555
Managing ADOMs	557
Deleting ADOMs	562
ADOM versions	563
Concurrent ADOM access	564
Locking an ADOM	565
Upgrading an ADOM	566
Certificates	566
Local certificates	566
CA certificates	569
Certificate revocation lists	570
Fetcher Management	571

Fetching profiles	572
Fetch requests	573
Synchronizing devices and ADOMs	574
Fetch monitoring	575
Event Log	576
Event log filtering	578
Task Monitor	578
SNMP	580
SNMP agent	580
SNMP v1/v2c communities	581
SNMP v3 users	584
SNMP MIBs	585
SNMP traps	586
Fortinet & FortiManager MIB fields	587
Mail Server	588
Syslog Server	590
Meta Fields	591
Device logs	592
Configuring rolling and uploading of logs using the GUI	593
Configuring rolling and uploading of logs using the CLI	594
File Management	596
Advanced Settings	596
Administrators	598
Trusted hosts	598
Monitoring administrators	599
Disconnecting administrators	599
Managing administrator accounts	599
Creating administrators	601
Editing administrators	605
Deleting administrators	606
Restricted administrators	606
Administrator profiles	616
Permissions	617
Creating administrator profiles	620
Editing administrator profiles	623
Cloning administrator profiles	623
Deleting administrator profiles	623
Authentication	623
Public Key Infrastructure	624
Managing remote authentication servers	625
LDAP servers	626
RADIUS servers	628
TACACS+ servers	630
Remote authentication server groups	630
SAML admin authentication	631
Global administration settings	633
Password policy	635

Password lockout and retry attempts	635
GUI language	636
Idle timeout	636
Two-factor authentication	637
Configuring FortiAuthenticator	637
Configuring FortiManager	639
High Availability	641
Configuring HA options	643
General FortiManager HA configuration steps	645
GUI configuration steps	645
Monitoring HA status	647
Upgrading the FortiManager firmware for an operating cluster	648
FortiManager support for FortiAnalyzer HA	648
Management Extensions	651
SD-WAN Orchestrator	651
FortiWLM	651
Enabling management extension applications	651
CLI for management extensions	652
Appendix A - Supported RFC Notes	654

Change Log

Date	Change Description
2020-08-06	Initial release.
2020-08-07	Updated Creating ACI fabric connectors on page 289 .
2020-08-19	Updated Intrusion Prevention on page 611 .
2020-08-21	Adding Intrusion Prevention filtering options on page 276 .
2020-08-31	Updated Automatic multi-step firmware upgrade on FortiGate on page 102 and Configuring a device on page 63 .
2020-09-11	Adding Configuring the management address on page 56 .
2020-09-14	Updated ADOM versions on page 563 .
2020-09-25	Added Requesting account entitlement files on page 496 .
2020-12-01	Updated Import policy wizard on page 54 .
2020-12-17	Removed <i>Appendix B - Examples</i> and published it as a separate guide.
2021-04-12	Added RFC 2548 to Appendix A - Supported RFC Notes on page 654 .
2022-05-16	Update Central SNAT on page 232 .

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 14](#)
- [Security considerations on page 15](#)
- [GUI overview on page 16](#)
- [FortiAnalyzer Features on page 20](#)
- [Configuring FortiManager appliances on page 22](#)
- [Adding devices on page 22](#)
- [Installing to managed devices on page 23](#)
- [Monitoring managed devices on page 23](#)
- [Restarting and shutting down on page 24](#)

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 16](#).



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 542](#).



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 544](#).



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 599](#) 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 15](#)
- [Other security considerations on page 15](#)

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 598](#) 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.

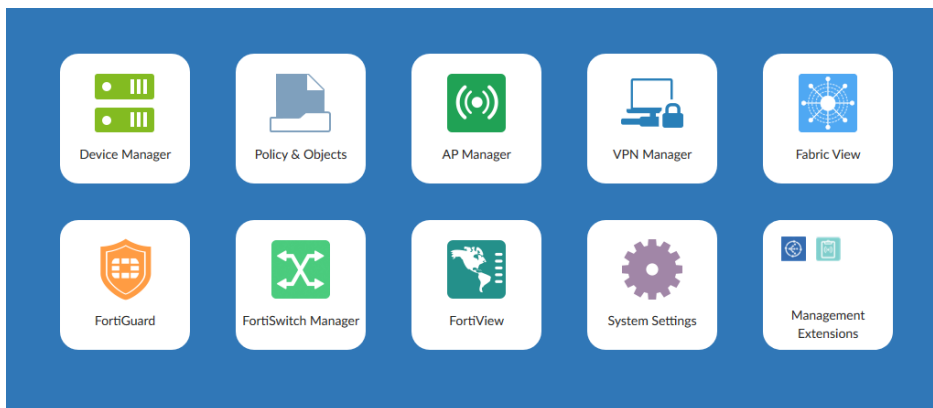


When setting up FortiManager for the first time or after a factory reset, the password cannot be left blank. You are required to set a password when the *admin* user tries to log in to FortiManager from GUI or CLI for the first time. This is applicable to a hardware device as well as a VM. This is to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

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

GUI overview

When you log into the FortiManager GUI, the following home page of tiles is displayed:



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

Device Manager	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 Firewall Devices on page 36 .
Policy & Objects	Configure policy packages and objects. For more information, see Firewall Policy & Objects on page 186 .
AP Manager	Configure and manage FortiAP access points. For more information, see Access Points on page 398 .
FortiClient Manager	Manage FortiClient profiles and monitor FortiClient endpoints that are registered to FortiGate devices. See Endpoint Compliance on page 475 . <i>FortiClient Manager</i> is available only for ADOM versions 6.0 and earlier.
VPN Manager	Configure and manage VPN connections. You can create VPN topologies and managed/external gateways. For more information, see VPN on page 353 .

Fabric View	Configure fabric connectors and view Security Fabric Ratings. See Fabric View on page 281 .
FortiGuard	Manage communication between devices and the FortiManager using the FortiGuard protocol. See Device Firmware and Security Updates on page 489 .
FortiSwitch Manager	Configure and manage FortiSwitch devices. For more information, see FortiSwitch Manager on page 443 .
Management Extensions	Enable and use management extension applications that are released and signed by Fortinet. See Management Extensions on page 651 .
FortiView	View device status information in real-time. When FortiAnalyzer features are enabled, FortiView and additional predefined Monitors are available. See FortiView on page 349 .
Log View	View logs for managed devices. You can display, download, import, and delete logs on this page. You can also define custom views and create log groups. This pane is only available when FortiAnalyzer features are enabled.
Incidents & Events	Configure and view events for logging devices. This pane is only available when FortiAnalyzer features are enabled.
Reports	Generate reports. You can also configure report templates, schedules, and output profiles, and manage charts and datasets. This pane is only available when FortiAnalyzer features are enabled.
System Settings	Configure system settings such as network interfaces, administrators, system time, server settings, and others. You can also perform maintenance and firmware operations. See System Settings on page 526 .

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

HA status	If HA is enabled, the status is shown.
ADOM	If ADOMs are enabled, the required ADOM can be selected from the dropdown list. If enabled, ADOMs can also be locked or unlocked. The ADOMs available from the ADOM menu will vary depending on the privileges of the current user.
Full Screen	Click to view only the content pane in the browser window. See Full-screen mode on page 19 .
Help	Click to open the FortiManager online help, or view the <i>About</i> information for your device (Product, Version, and Build Number).
CLI Console	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.

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

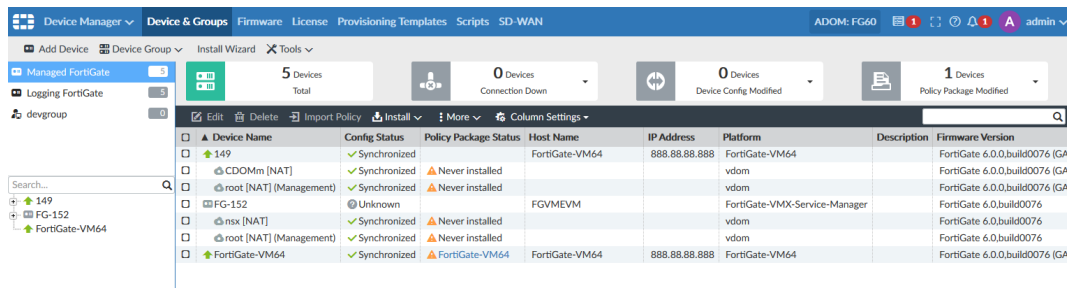
Notification	Click to display a list of notifications. Select a notification from the list to take action on the issue.
admin	Click to change the password or log out of the GUI.

Panes

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

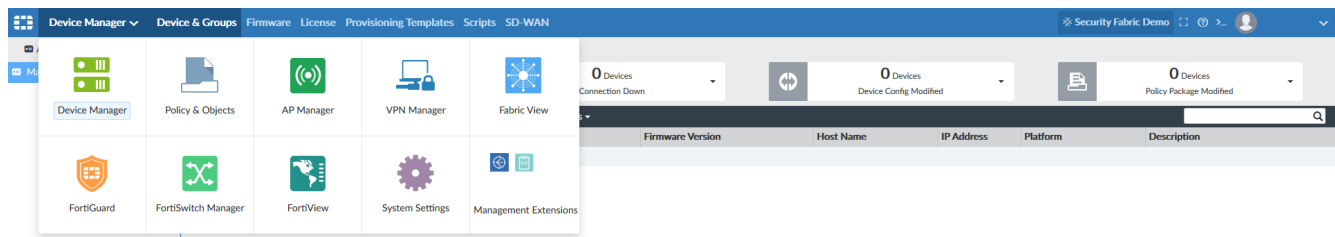
Banner	Along the top of the page; includes the home button (Fortinet logo), tile menu, ADOM menu (when enabled), admin menu, notifications, help button, and CLI console button.
Tree menu	On the left side of the screen; includes the menus for the selected pane.
Content pane	Contains widgets, lists, configuration options, or other information, depending on the pane, menu, or options that are selected. Most management tasks are handled in the content pane.
Toolbar	Directly above the content pane; 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 36](#) 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	Never installed	FGVMEVM		FortiGate-VMX-Service-Manager		FortiGate 6.0.0.build0076
nix [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.



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 633](#).

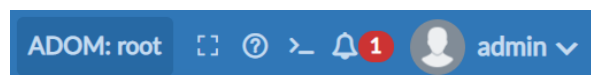
Full-screen mode

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.

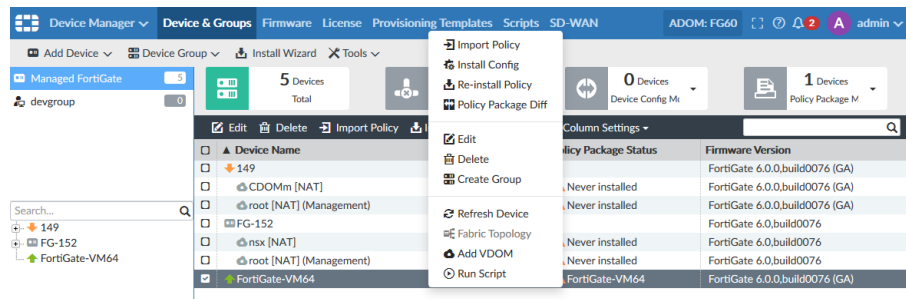


ADOM access is controlled by administrator accounts and the profile assigned to the administrator account. Depending on your account privileges, you might not have access to all ADOMs. See [Managing administrator accounts on page 599](#) for more information.

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 *FortiView > FortiView* and *Log View* panes. FortiManager can display an avatar when FortiClient is managed by FortiGate or FortiClient EMS with logging to FortiManager enabled.

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

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



You can also optionally define an avatar for FortiManager administrators. See [Creating administrators on page 601](#).

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 57](#).

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

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

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

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

Dashboard widgets	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 Dashboard on page 527 .
Logging Topology	View the logging topology. See Logging Topology on page 541 .
Storage Info	View and configure log storage policies. See the FortiAnalyzer Administration Guide . This pane is only available when ADOMs are enabled.
Fetcher Management	Configure log fetching. See Fetcher Management on page 571 .
Device Log Settings	Configure device log file size, log rolling, and scheduled uploads to a server. See Device logs on page 592 .
File Management	Configure the automatic deletion of device log files, quarantined files, reports, and content archive files after a set period of time. See File Management on page 596 .

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 57](#) 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 14](#).
2. Configure IP addresses. See [Configuring network interfaces on page 542](#).
3. Configure the RAID level, if the FortiManager unit supports RAID. See [RAID Management on page 546](#).

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 108](#) 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 552](#).
3. Configure administrator accounts. See [Managing administrator accounts on page 599](#).
4. Add devices to FortiManager. See [Adding devices on page 37](#).
5. If not done when you added the device, import the policy from each online device to FortiManager. See [Import policy wizard on page 54](#).

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 245](#) or [Edit an object on page 265](#).
2. Create or edit policies in a policy package to select the objects. See [Creating policies on page 206](#) or [Editing policies on page 206](#).
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 191](#).
3. Ensure that the installation targets for the policy package include the correct devices. See [Policy package installation targets on page 198](#).
4. Edit device-specific settings by using the device dashboard on the *Device Manager* pane. See [Using the device dashboard on page 67](#).
5. Install the policy package and device settings to devices by using the Installation Wizard. See [Installing to devices on page 74](#).

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 78](#)
- Device dashboard—see [Using the device dashboard on page 67](#)
- Device configurations—see [Managing device configurations on page 87](#)
- Policy packages—see [Managing policy packages on page 191](#)
- *AP Manager* pane—see [Monitor on page 412](#)
- *FortiClient Manager* pane—see [Monitoring FortiClient endpoints on page 479](#)
- *FortiSwitch Manager* pane—see [Monitor on page 454](#)

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 149](#)
- *VPN Manager* pane—see [VPN on page 353](#)

When FortiAnalyzer features are enabled on the FortiManager device, you can also view and analyze log messages from managed devices by using the *FortiView > FortiView, Log View, Event Management, and Reports* panes. See [FortiAnalyzer Features on page 20](#).

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 26](#)
- [Object database and FortiManager modules on page 27](#)
- [Inside the FortiManager system on page 28](#)
- [Key features of the FortiManager system on page 33](#)

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
- FortiView
- 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:

- FortiView (*FortiView* and additional *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 529](#)), or use the following CLI commands:



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

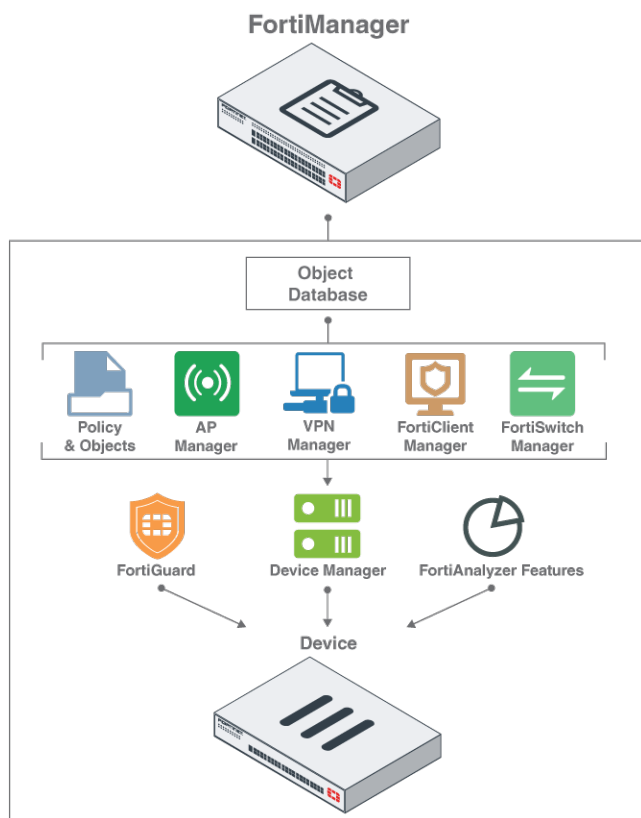
Changing faz status will affect FAZ feature in FMG. If you continue,
system will reboot to add/remove FAZ feature.

```
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.

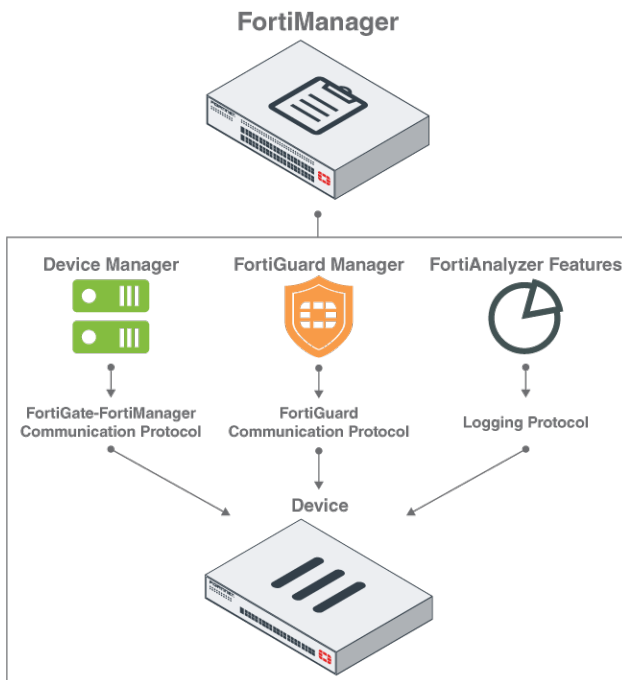


Inside the FortiManager system

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 36](#).

FortiGuard Manager

FortiGuard Manager communicates with devices by using the FortiGuard protocol.

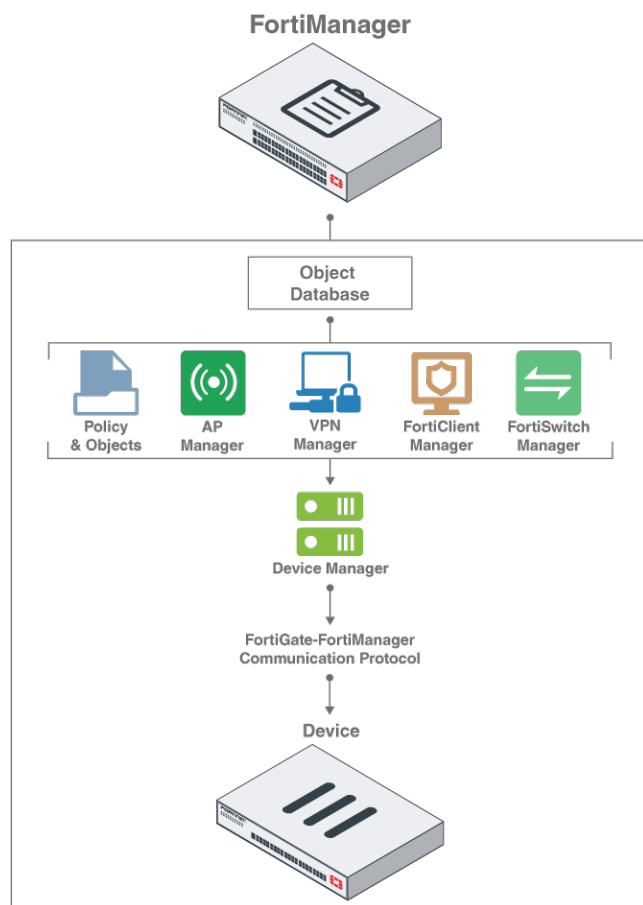
FortiAnalyzer features

When FortiAnalyzer features are enabled for the FortiManager unit, the *FortiView > 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 186](#).

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 398](#).

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 353](#).

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 475](#).

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 443](#).

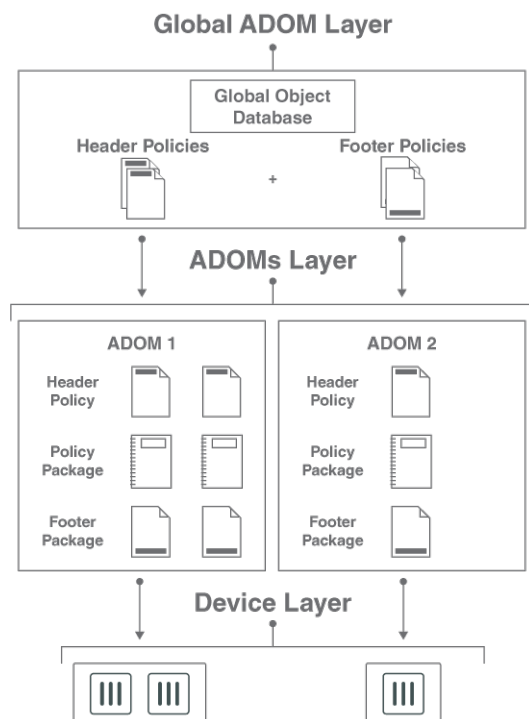
ADOMs and devices

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 74](#).

Re-install

The re-install operation reinstalls a policy package on a FortiGate device. For more information, see [Reinstall a policy package on page 195](#).

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 54](#).

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 555](#).

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 79](#).

Revert

The revert operation loads a saved configuration revision into the device database. For more information, see [Managing configuration revision history on page 91](#).

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 53](#). You can also display the security fabric topology (see [Displaying Security Fabric topology on page 83](#)) and view Security Fabric Ratings (see [Fabric View on page 281](#)).

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 552](#).

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 489](#).

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 117](#).

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.

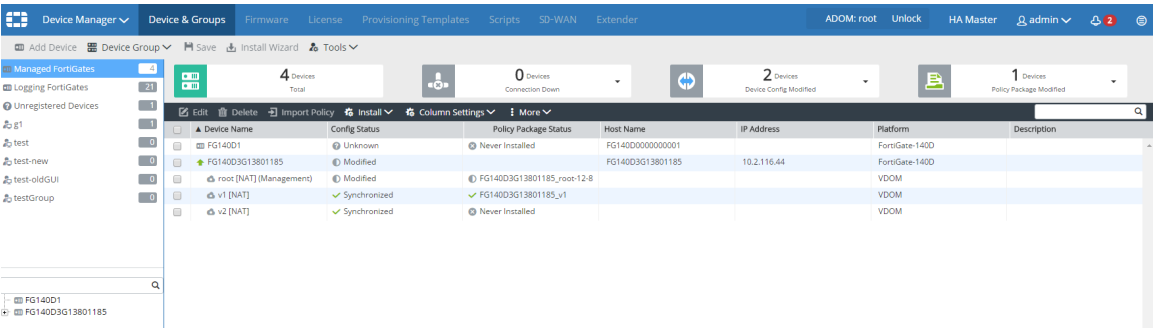
This topic covers navigating the *Device Manager* pane, adding devices, and managing devices. It also covers managing FortiExtender wireless WAN extenders.



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 565](#).



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

Device & Groups	Add, configure, and view managed and logging devices. Use the toolbar to add devices, devices groups, and launch the install wizard. See Adding devices on page 37 . The <i>Device & Groups</i> tab also contains a quick status bar for a selected device group. See Using the quick status bar on page 78 .
Firmware	View information about firmware for devices as well as upgrade firmware. See Firmware on page 98 .
License	View license information for devices as well as push license updates to devices. See License on page 106 .
Provisioning Templates	Configure provisioning templates. For information on system, Threat Weight, FortiClient, and certificate templates, see Provisioning Templates on page 108 .
Scripts	Create new or import scripts. Scripts is disabled by default. You can enable this advanced configuration option in <i>System Systems > Admin > Admin Settings</i> . Select <i>Show Script</i> to enable on this option in the <i>Device Manager</i> pane. See Scripts on page 117 .

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 149](#).

Extender

View and configure FortiExtender. See [FortiExtender on page 176](#).

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, FortiAuthenticator, 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 552](#).



For information on adding devices to an ADOM by using the *Add Device* wizard, see [Adding devices using the wizard on page 38](#).

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 57](#).

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.

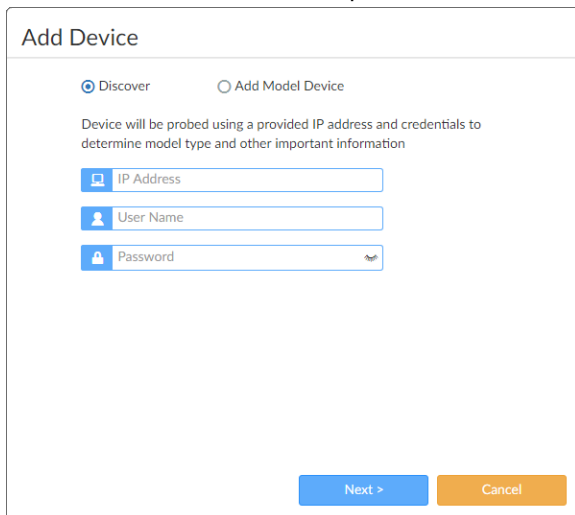


FortiManager will not be able to communicate with the FortiGate if offline mode is enabled. Enabling offline mode will prevent FortiManager from discovering devices.

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.



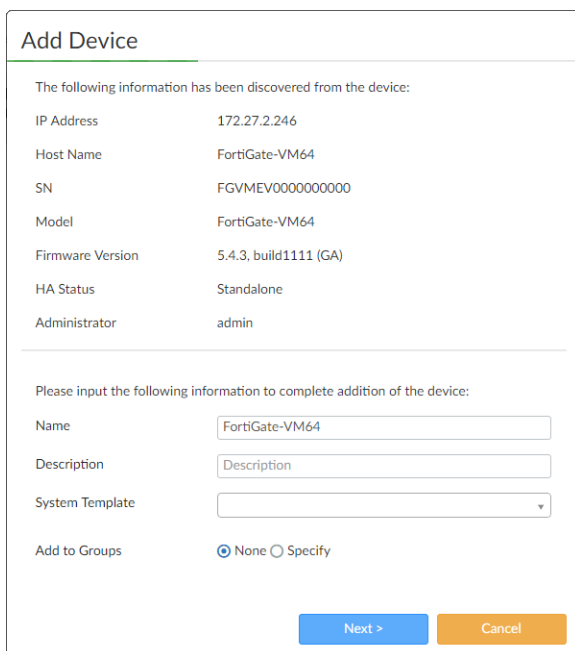
Add Device

☒ Discover ☐ Add Model Device

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

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



Add Device

The following information has been discovered from the device:

IP Address	172.27.2.246
Host Name	FortiGate-VM64
SN	FGVMEV000000000
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

Description

System Template

Add to Groups ☒ None ☐ Specify

5. Configure the following settings:

Name	Type a unique name for the device. The device name cannot contain spaces or special characters.
Description	Type a description of the device (optional).
System Template	System templates can be used to centrally manage certain device-level options from a central location. If required, assign a system template using the dropdown menu. Alternatively, you can select to configure all settings per-device inside <i>Device Manager</i> . For more information, see Provisioning Templates on page 108 .
Add to Groups	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

Item	Count
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

Link Device By

Serial Number

Device Model

Enforce Firmware Version ☐

Firmware Version 6.2

Assign Policy Package ☐

Assign Device Provision Profile ☐

Device Group

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

Add Model Device	Device will be added using the chosen model type and other explicitly entered information.
Name	Type a descriptive name for the device. This name is displayed in the <i>Device Name</i> column. Each device must have a unique name, otherwise the wizard will fail.
Link Device By	<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 <fmg-serial-number> <presared-key></pre>
Serial Number or Pre-Shared Key	<p>Type the device serial number or pre-shared key. This field is mandatory.</p> <p>If using a pre-shared key, each device must have a unique pre-shared key. You can change the pre-shared key after adding the model device. See Editing device information on page 79.</p>
Device Model	Select the device model from the list. If linking by serial number, the serial number must be entered before selecting a device model.
Enforce Firmware Version	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.

Assign Policy Package	Select the check box and select a policy package from the drop-down to assign a particular policy package to the device.
Assign Device Provisioning Profile	Select the check box and select a device provisioning profile from the drop-down to assign a particular provisioning profile to the device.
Device Group	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 91](#).

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.

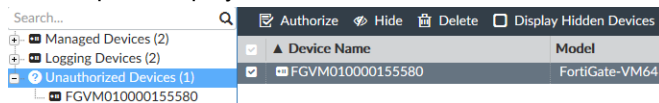
4. If ADOMs are enabled, select the ADOM in the *Add the following device(s) to ADOM* list. If ADOMs are disabled, select *root*.
5. Click *OK* to authorize the device or devices.
The device or devices are authorized and FortiManager can start managing the device or devices.

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.

- a. Go to *Security Fabric > Fabric Connectors*.
- b. Under *Other Fortinet Products*, double-click the FortiManager tile to open it for editing.
- c. In the *IP address* box, type the FortiManager IP address, and click *OK*.

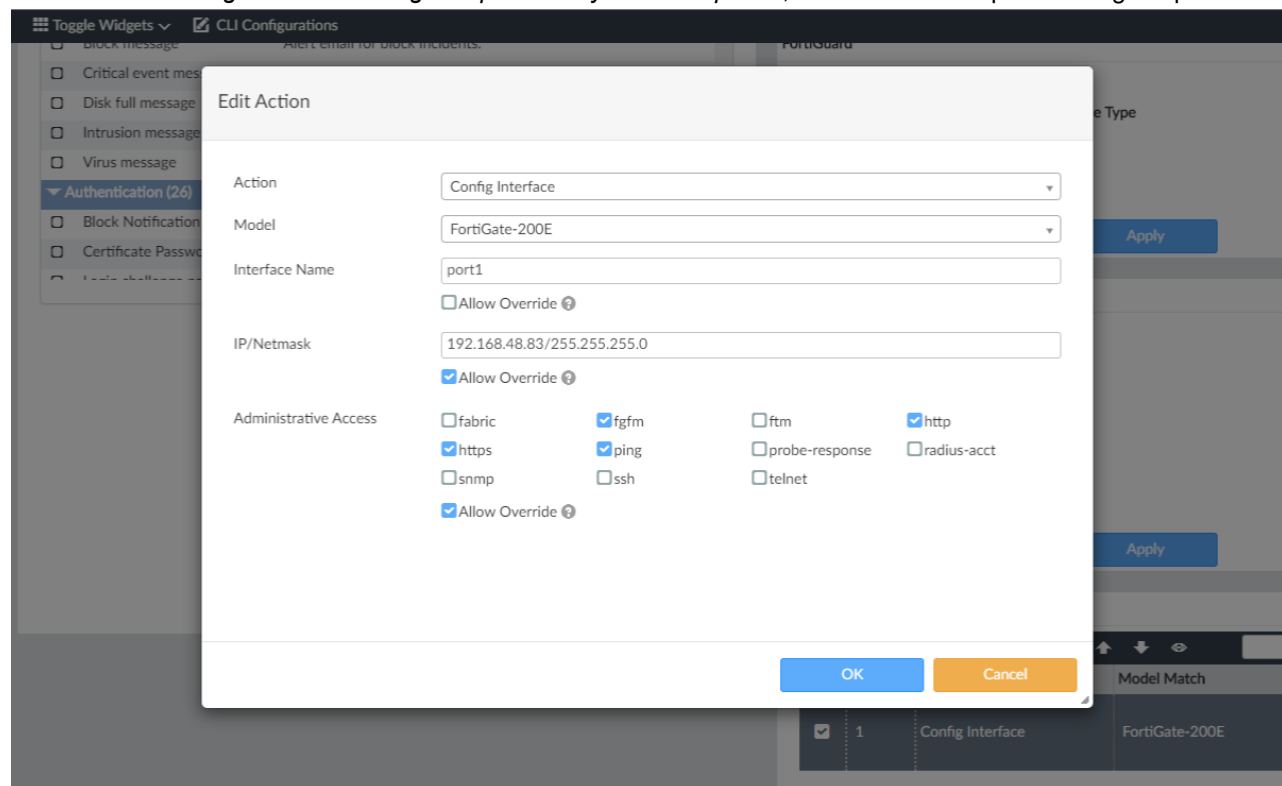
FortiManager automatically links the model device to the real device, and installs configurations to the device.

Example of adding a model device by using device template

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

To add a model device using a provisioning template:

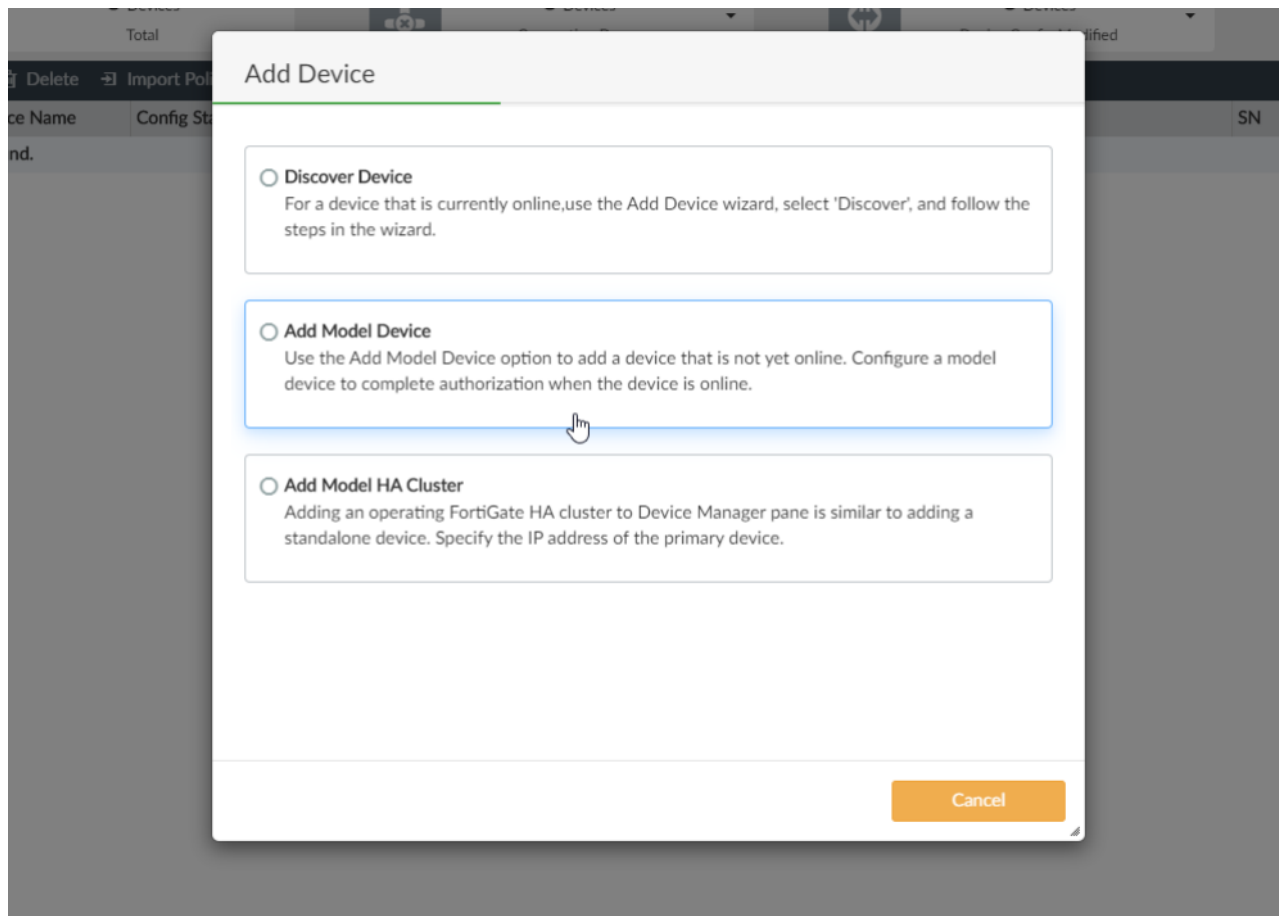
1. Go to *Device Manager > Provisioning Templates > System Templates*, and create a new provisioning template.





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

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



4. Configure the settings as follows:

Name	Enter a name for the model device.
Link Device By	Select <i>Serial Number</i> .
Serial Number	Add the serial number of the FortiGate device to be added.
Device Model	Select the device model from the drop-down list.
Assign Provisioning Template	Select the provisioning template you created in Step 1 from the drop-down list.

Add Device

☒ Add Model Device

Name: FGT200E2

Link Device By: ☒ Serial Number ☐ Pre-shared Key

Serial Number: FG200E4Q17913569

Device Model: FortiGate-200E

☐ Enforce Firmware Version: 6.4 (by default)

Add to Device Group: Click here to select

Add to Folder: /

☐ Assign Policy Package

☒ Assign Provisioning Template: FGT200E_Template

[Override Profile Value](#)

< Previous Next > Cancel

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

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

Dialog Box: Edit Action

Action: Config Interface

Model: FortiGate-200E

Interface Name: port1

IP/Netmask: 192.168.48.183/255.255.255.0

Administrative Access:

<input type="checkbox"/> fabric	<input checked="" type="checkbox"/> fgfm	<input type="checkbox"/> ftm	<input checked="" type="checkbox"/> http
<input checked="" type="checkbox"/> https	<input checked="" type="checkbox"/> ping	<input type="checkbox"/> probe-response	<input type="checkbox"/> radius-acct
<input type="checkbox"/> snmp	<input type="checkbox"/> ssh	<input checked="" type="checkbox"/> telnet	

Buttons: OK, Cancel

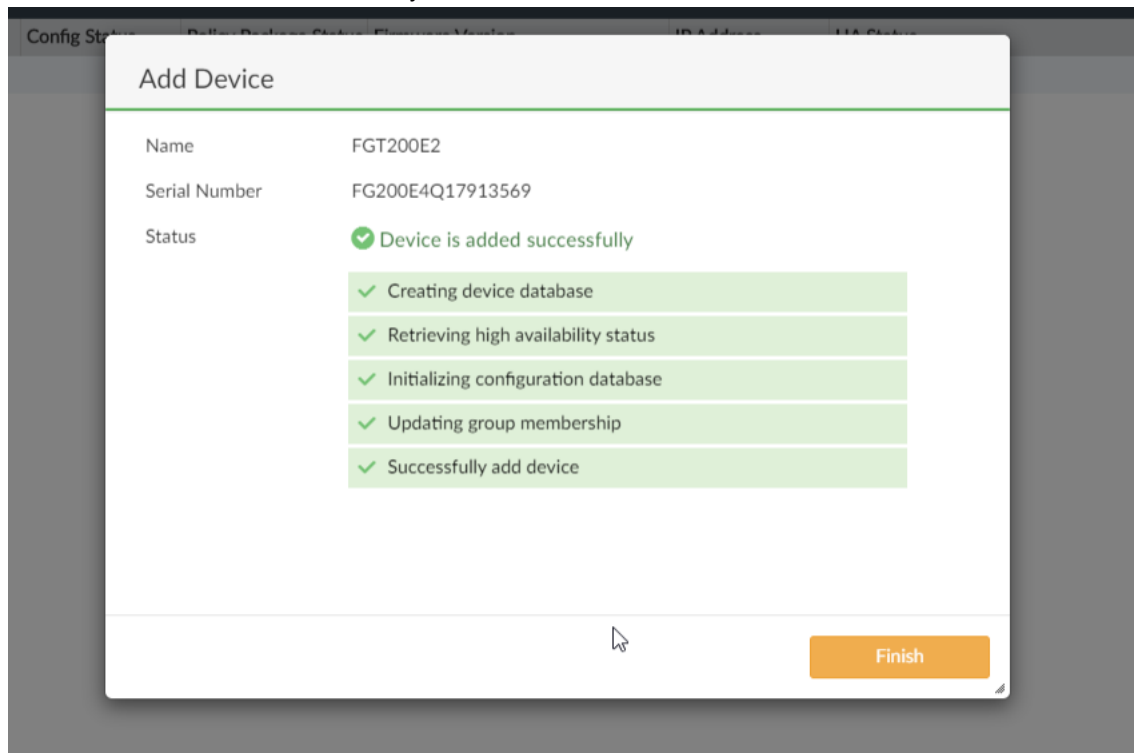
- c. Make the required changes and click *OK*.



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

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

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



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

1 Devices

Total

0 Devices

Connection Down

0 Devices

Device Config Modified

0 Devices

Policy Package Modified

Edit

Delete

Import Policy

Install

More

Column Settings

Device Name

Config Status

Policy Package Status

Firmware Version

IP Address

HA Status

SN

FGT200E2

Synchronized

Never installed

FortiGate 6.4.0,build1718 (Interim)

10.6.106.83

N/A

FG200E4Q17913569

Adding a FortiGate HA cluster when adding a model device

You can add a FortiGate HA cluster using the *Add Model Device* method when adding a new device. The process of adding a FortiGate HA cluster is similar to adding a model device using FortiGate serial numbers. See [Example of adding a model device by serial number on page 45](#).

You can add the two FortiGate devices as model devices to be part of the HA cluster. In the *Add Device* dialog, select *Add Model Device*, and select the *HA Cluster* option. Populate the mandatory fields *HA Mode*, *Serial Number* for both the nodes, *Device Model* type, *Group Name* and *Password* for the HA cluster, *Node 1* and *Node 2* priority, *Monitor*

Interface members, and Heartbeat Interface members.



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



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

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

You can also edit the HA cluster information after adding it. Use the *Edit Device* screen to modify the HA cluster information by modifying the fields *IP Address*, *Admin User* and *Password*, *Cluster Members*, *Enforce Firmware Version*,

System Template, and Policy Package.

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

Split-Task VDOM Multi VDOM

VDOM Name

Description

0/255

Enable

☒

Operation Mode

NAT

NGFW Mode

Profile-based Policy-based

Interface Members

Click here to select

OK

Cancel

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

VDOM Name	Type a name for the new virtual domain.
Description	Optionally, enter a description of the VDOM.
Enable	Select to enable the VDOM.
Operation Mode	Select either <i>NAT</i> or <i>Transparent</i> .
NGFW Mode	Select either <i>Profile-based</i> or <i>Policy-based</i> .
Interface Members	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 83](#).

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 38](#). Alternatively, you can enable Central Management in the root FortiGate unit and specify the IP address of the FortiManager. See [Authorizing devices on page 44](#).
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
FG1000G244811667	✓	✓	FG1000-L2	10.3.121.191	FortGate-101E	
FG101E-L2	✓ Synchronized	⚠ Never Installed	FG101E-L2	10.3.121.191	FortGate-101E	
FG101E-L3	✓ 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	
FGP2004614800316	✓	✓	FG200DPOE-L3	10.3.121.111	FortGate-200D-POE	
FG200DPOE-L3	✓ Auto-update	⚠ Never Installed	FG200DPOE-L3	10.3.121.111	FortGate-200D-POE	
FG81E-HA-L2	✓ Auto-update	⚠ Never Installed	FG81E-HA-L2	10.3.121.181	FortGate-81E-POE	
FGT200DPOE-L1-root*	✓ Auto-update	⚠ Never Installed	FGT200DPOE-L1-root	10.3.121.112	FortGate-200D-POE	
FGVM-076-L2	✓ Auto-update	⚠ Never Installed	FGVM-076-L2	10.3.121.76	FortGate-VM64	

Import policy wizard

The import policy wizard helps you import policy packages and objects from managed FortiGates as well as specify per-device or per-platform mappings for FortiGate interfaces. Default or per-device mapping must exist or the installation will fail.



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

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

To import policy packages and objects:

1. Go to *Device Manager > Device & Groups*.
2. Right-click a device, and select *Import Policy*.

The wizard opens.

Import Device - security-fabric [root]

Create a new policy package for import.

Policy Package Name: security-fabric-

Folder: root

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

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

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

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

Next > Cancel

3. Specify what policies and objects to import:

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

4. Specify mapping types for enabled FortiGate interfaces:

When importing policies and objects from a device, all enabled interfaces require a mapping.

Device Interface	Displays the enabled interfaces for the device for which you are importing policies.
Mapping Type	For each enabled device interface, select one of the of the following options: <i>Per-Device</i> or <i>Per-Platform</i> .

Normalized Interface	Displays the name of the normalized interface to which the device interface is mapped.
Add mapping for all unused device interfaces	Select to automatically create interface maps for unused device interfaces.

5. When finished mapping device interfaces, click *Next*.
The next page displays any object conflicts between the device and FortiManager.
6. If object conflicts are detected, choose whether to use the value from FortiGate or FortiManager, and click *Next*.
The object page searches for dependencies, and reports any conflicts it detects. If conflicts are detected, you must decide whether to use the FortiGate value or the FortiManager value. If there are conflicts, you can select *View Conflict* to view details of each individual conflict. Duplicates will not be imported.
You can click *Download Conflict File* to save a file of the conflicts to your hard drive.
7. When finished managing object conflicts, click *Next*.
A list of objects to be imported is displayed.
8. Click *Next* to start the import process.
When the import process completes, a summary page is displayed.
You can click *Download Import Report*, and save the report file to your hard drive.
Objects are imported into the common database, and the policies are imported into the selected package.



The import process removes all policies that have FortiManager generated policy IDs, such as 1073741825, that were previously learned by the FortiManager device. The FortiGate unit may inherit a policy ID from the global header policy, global footer policy, or VPN console.

9. Click *Finish* to close the wizard.

Configuring the management address

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

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

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

To configure the management address before adding the device:

```
#FMG config
config systems admin setting
set mgmt-addr <FMG_VIP>
```

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 *FortiView > FortiView*, and *Log View*.

For information about FortiAnalyzer features, see [FortiAnalyzer Features on page 20](#). See also [Viewing policy rules on page 61](#) and [View logs related to a policy rule on page 201](#).



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 20](#).

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 108](#).

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: *FortiView > 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.

Add FortiAnalyzer

☒ Discover

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

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:

FAZVM64

Description

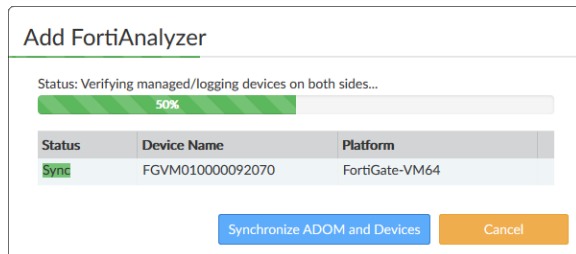
6. Configure the following settings if desired, and click *Next*:

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

The wizard performs the following tasks:

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

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



Status	Device Name	Platform
Sync	FGVM010000092070	FortiGate-VM64

The following table describes the different statuses:

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

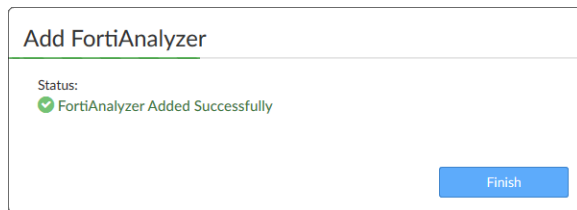
If the FortiManager ADOM does not exist on the FortiAnalyzer device, a warning is displayed. You can add the ADOM and devices to FortiAnalyzer by clicking the *Synchronize ADOM and Devices* button.

7. Click *Synchronize ADOM and Devices* to continue.

- 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.
- 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 108](#).

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 57](#).

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.

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.

Export to CSV

File Name

Options

☒ Export all columns
☐ Export customized columns only

Download

Cancel

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.



You cannot use FortiManager to configure high availability (HA) on FortiGate devices. FortiManager learns about HA settings from managed FortiGate devices, but does not manage that part of the FortiGate configuration. As a result the *System HA* pane is read-only in *Device Manager*.

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

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 578](#).

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.

Delete	Select to remove this virtual domain. This function applies to all virtual domains except the root.
Create New	Select to create a new virtual domain.
Management Virtual Domain	Select the management VDOM and select <i>Apply</i> .
Name	The name of the virtual domain and if it is the management VDOM.
Virtual Domain	Virtual domain type.
IP/Netmask	The IP address and mask. Normally used only for Transparent mode.
Type	Either VDOM Link or Physical.
Access	HTTP, HTTPS, SSH, PING, and/or SNMP.
Resource Limit	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 67](#) 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.

New VDOM Link

Name

Interface 0

Virtual Domain

root

IP/Netmask

0.0.0.0/0.0.0.0

Administrative Access

☐ HTTPS

☐ HTTP

☐ PING

☐ FMG-Access

☐ CAPWAP

☐ SSH

☐ SNMP

Comments

Write a comment

Administrative Status

ON

Interface 1

Virtual Domain

root

IP/Netmask

0.0.0.0/0.0.0.0

Administrative Access

☐ HTTPS

☐ HTTP

☐ PING

☐ FMG-Access

☐ CAPWAP

☐ SSH

☐ SNMP

Comments

Write a comment

Administrative Status

ON

OK

Cancel

4. Enter the following information:

Name	Name of the VDOM link.
Interface #x	The interface number, either 1 or 0.
VDOM	Select the VDOM
IP/Netmask	Type the IP address and netmask for the VDOM.
Administrative Access	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> . Note: HTTP traffic will be automatically redirected to HTTPS.
Description	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 191](#)). 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 69](#)
- [CLI Configurations 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.

4. In the dashboard toolbar, click the tabs to display different options that you can configure for the device. See [Dashboard toolbar on page 68](#).
5. You can control what tabs are displayed by clicking *Display Options*. See [Display Options on page 68](#).

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 > Global 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"/> System	<input checked="" type="checkbox"/> Dashboard <input type="checkbox"/> Port Pair <input checked="" type="checkbox"/> Global Resources <input type="checkbox"/> Modem <input checked="" type="checkbox"/> HA <input type="checkbox"/> DNS <input type="checkbox"/> DNS Service on Interface <input type="checkbox"/> Management <input type="checkbox"/> Administrators <input type="checkbox"/> Local Host ID <input checked="" type="checkbox"/> Replacement Message <input type="checkbox"/> FortiGuard <input type="checkbox"/> Automation Stitch <input type="checkbox"/> Alert Email <input type="checkbox"/> NAT64 Prefix	<input checked="" type="checkbox"/> Interface <input type="checkbox"/> Virtual Domain <input type="checkbox"/> DHCP Server <input type="checkbox"/> Sniffer Interface Policy <input checked="" type="checkbox"/> SNMP <input type="checkbox"/> DNS Database <input type="checkbox"/> Explicit Proxy <input type="checkbox"/> Admin Settings <input type="checkbox"/> Admin Profile <input type="checkbox"/> CA Certificates <input checked="" type="checkbox"/> Replacement Message Group <input type="checkbox"/> Security Fabric <input type="checkbox"/> Log Setting <input type="checkbox"/> Threat Weight <input type="checkbox"/> FortiSandbox
<input checked="" type="checkbox"/> Router	<input checked="" type="checkbox"/> Static Route <input type="checkbox"/> Gateway Detection <input type="checkbox"/> RIP <input type="checkbox"/> Multicast Route	<input type="checkbox"/> Policy Route <input checked="" type="checkbox"/> OSPF <input type="checkbox"/> BGP
<input checked="" type="checkbox"/> WAN Opt. & Cache	<input type="checkbox"/> Settings	<input type="checkbox"/> URL Match List
<input checked="" type="checkbox"/> Security Profiles	<input type="checkbox"/> FortiClient Profile	<input type="checkbox"/> Web Filter Override
<input checked="" type="checkbox"/> VPN	<input type="checkbox"/> IPsec Phase 1 <input type="checkbox"/> Manual Key	<input type="checkbox"/> IPsec Phase 2 <input type="checkbox"/> Concentrator
<input checked="" type="checkbox"/> Wireless	<input type="checkbox"/> Local WiFi Radio	

Check All
Reset to Default
OK
Cancel



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 Configurations menu

FortiManager includes a *CLI Configurations* 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 Configurations 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 Configurations* checkbox, and click *OK*. The *CLI Configurations* menu is displayed in the toolbar.
6. Click *CLI Configurations*.



The options available in the menu will vary from device to device depending on what feature set the device supports. The options will also vary depending on the device firmware version.

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	
View Config	Click a configuration revision, and click <i>View Config</i> to view the configuration details.
View Install Log	Click a configuration revision, and click <i>View Install Log</i> to display the installation log.
Revision Diff	Click a configuration revision, and click <i>Revision Diff</i> to view the difference between the current and previous revisions.
Retrieve Config	Click to retrieve a configuration and create a new revision.
ID	The identification number for the configuration revision.
Date & Time	The date and time for the configuration revision.

Configuration Revision History	
Name	The name of the device.
Created by	The name of the administrator who created the configuration revision.
Installation	The status of the installation for the configuration revision.
Comments	Comments about the device.
System Information	
Host Name	The host name of the device.
Serial Number	The device serial number.
Platform Type	The platform type for the device.
HA Status	FortiGate HA configuration on FortiManager is read-only. Standalone indicates non-HA mode. Active-Passive, Active-Active indicates the device is operating in a cluster.
System Time	The device system time and date information.
Firmware Version	The device firmware version and build number.
System Configuration	Displays the Last Backup. You can backup or restore.
Current Administrators	Displays the number of administrators configured on this device.
Hardware Status	The number of CPUs and the amount of RAM for the device.
Up Time	Displays the duration the device has been up.
Administrative Domain	Toggle the switch <i>ON</i> or <i>OFF</i> to enable or disable ADOMs.
Analyzer Features	Toggle the switch <i>ON</i> or <i>OFF</i> to enable or disable FortiAnalyzer features.
License Information	
VM License	The VM license information.
Support Contract	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.
FortiGuard Services	The contract version, issue date and service status. FortiGuard Services includes the following: Antivirus, Intrusion protection, Web filtering, and Email filtering.
VDOM	The number of virtual domains that the device supports.
Connection Summary	
IP	The IP address of the device.
Interface	The port used to connect to the FortiManager system.
Connecting User	The user name for logging in to the device.

Connection Summary

Connectivity	<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>
Connect to CLI via	Select SSH.

Configuration and Installation Status

Enforce Firmware Version	<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 Adding a model device on page 42.</p>
System Template	<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 Adding a model device on page 42.</p>
Policy Package	<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 Adding a model device on page 42.</p>
Database Configuration	Select <i>View</i> to display the configuration file of the FortiGate unit.
Total Revisions	<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>
Sync Status	<p>The synchronization status with the FortiManager:</p> <ul style="list-style-type: none"> • <i>Synchronized</i>: The latest revision is confirmed as running on the device. • <i>Out_of_sync</i>: The configuration file on the device is not synchronized with the FortiManager system. • <i>Unknown</i>: The FortiManager system is unable to detect which revision (in revision history) is currently running on the device. <p>Select <i>Refresh</i> to update the Installation Status.</p>
Warning	<p>Displays any warnings related to configuration and installation status:</p> <ul style="list-style-type: none"> • <i>None</i>: No warning. • <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. • <i>Unable to detect the FortiGate version</i>: Connectivity error! • <i>Aborted</i>: The FortiManager system cannot access the device.

Configuration and Installation Status

Installation Tracking

Device Settings Status	<ul style="list-style-type: none"> • <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. • <i>UnModified</i>: All configuration displayed on the device is saved as the latest revision in the FortiManager database.
Installation Preview	Select the icon to display a set of commands that will be used in an actual device configuration installation in a new window.
Last Installation	The FortiManager system sent a configuration to the device at the indicated date and time.
Scheduled Installation	A new configuration will be installed on the device at the indicated date and time.
Script Status	Select Configure to view script execution history.
Last Script Run	Displays the date when the last script was run against the managed device.
Scheduled Script	Displays the date when the next script is scheduled to run against the managed device.



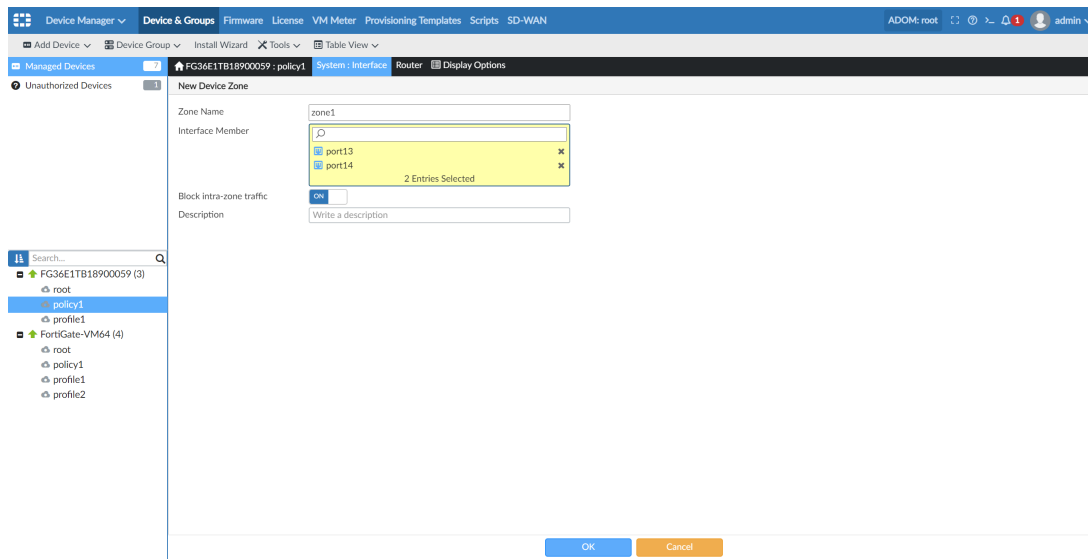
The information presented in the System Information, License Information, Connection Summary, and Configuration and Installation Status widgets will vary depending on the managed device model.

Device zones

When creating a device zone, map the zone to a physical interface. You must also map the zone to a normalized interface to use the zone in a policy. See also [Normalized interfaces on page 252](#).

To create a device zone:

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.
5. Click *Create New > Device Zone*.
The *New Device Zone* pane opens.



6. Complete the options, and click **OK**.
The interface members are physical interfaces.
7. Create a normalized interface for the zone. See [Creating normalized interfaces on page 258](#).

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 74](#).
- To use the *Install Wizard* to install device settings only, see [Using the Install Wizard to install device settings only on page 76](#).
- To reinstall a policy package without using the *Install Wizard*, see [Reinstall a policy package on page 195](#).



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 558](#) 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:

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 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

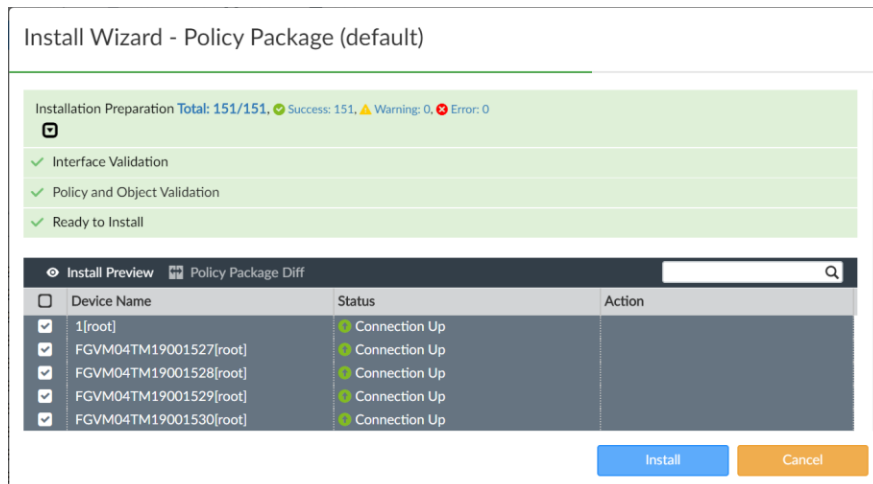
☐ Install Device Settings (only)

Next >

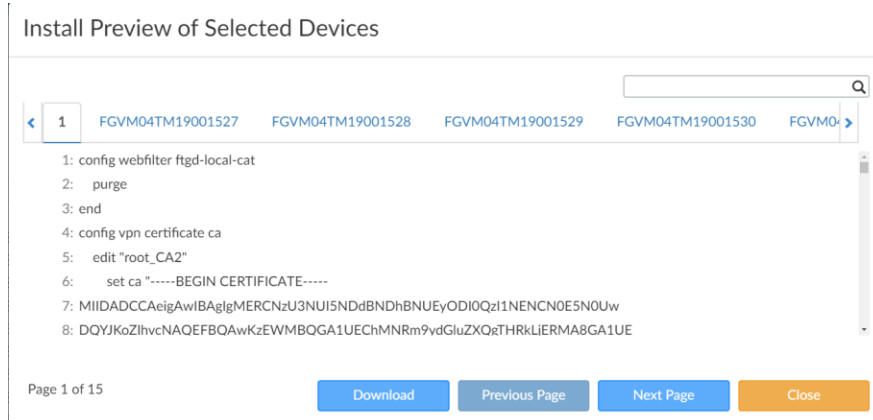
Cancel

Policy Package	Select the policy package from the dropdown list.
Comment	Type an optional comment.
Create ADOM Revision	Select the checkbox to create an ADOM revision.
Revision Name	Type the revision name.
Revision Comments	Type an optional comment.
Schedule Install	Select the checkbox to schedule the installation.
Date	Click the date field and select the date for the installation in the calendar pop-up.
Time	Select the hour and minute from the dropdown lists.

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 200](#)).



5. (Optional) Click the *Install Preview* button to view a preview of the installation. You can view multiple devices at the same time.
 - a. (Optional) Click *Previous Page* or *Next Page* to preview multiple devices.
 - b. (Optional) Click *Download* to 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 77](#).
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.

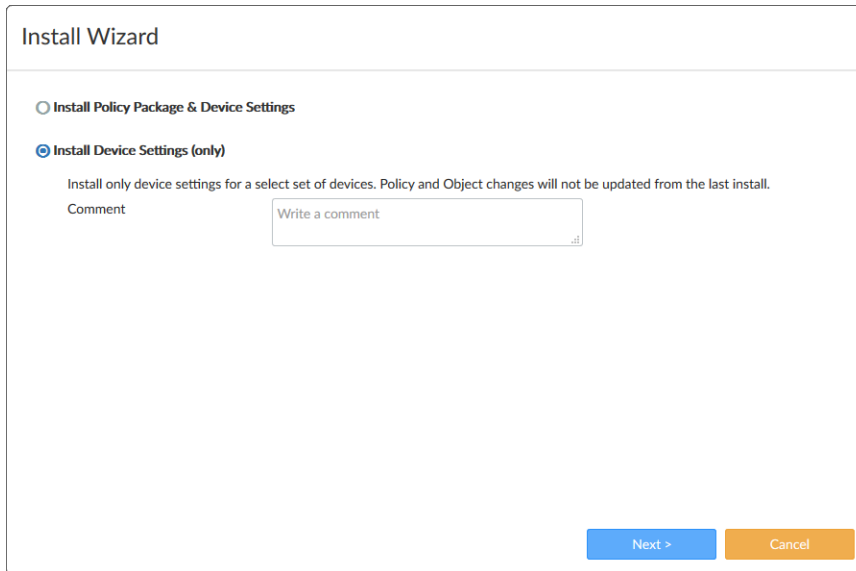
Using the Install Wizard to install device settings only

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	[Details]

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

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

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: FGP200000000000 (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:

Country:

Province/State:

City:

Contact:

OK Cancel

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

Name	The name of the device.
Description	Descriptive information about the device.
IP Address	Enter the IP address of the device.
Pre-Shared Key	Enter the model device's pre-shared key. Select <i>Show Pre-shared Key</i> to see the key. This option is only available when editing a model device that was added with a pre-shared key.
Automatically link to real device	Select to automatically authorize the device to be managed by FortiManager when the device is online. This option is only available when editing a model device.
Serial Number	The serial number of the device. For model devices added with a pre-shared key, this will show the device model.
Firmware Version	The firmware version.
Admin User	Enter the administrator user name.
Password	Enter the administrator user password.
Connected Interface	The connected interface, if the connection is up.
HA Mode	Displays whether the FortiGate unit is operating in standalone or high availability mode.
Geographic Coordinates	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.
Company/Organization	Optionally, enter the company or organization information.
Country	Optionally, enter the country where the device is located.
Province/State	Optionally, enter the province or state.
City	Optionally, enter the city.
Contact	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 95](#)).
- If a template is assigned to the device, the template will remain with no device assignment ([Provisioning Templates on page 108](#)).
- 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 198](#)).
- 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 208](#)).
- If there are VDOMs in other ADOMs, they will be deleted with the device ([ADOM device modes on page 554](#)).

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
```

allow_register [enable disable]	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.
unreg_dev_opt	Set the action to take when an unauthorized device connects to FortiManager.
add_allow_service	Authorize unauthorized devices and allow service requests.
add_no_service	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*.

Connect to:	Shows the device that you are currently connected to. Select the dropdown menu to select another device.
--------------------	--

IP	The IP address of the connected device.
SSH	Connect to the device via SSH.
Connect Disconnect	Connect to the device you select, or terminate the connection.
Close	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

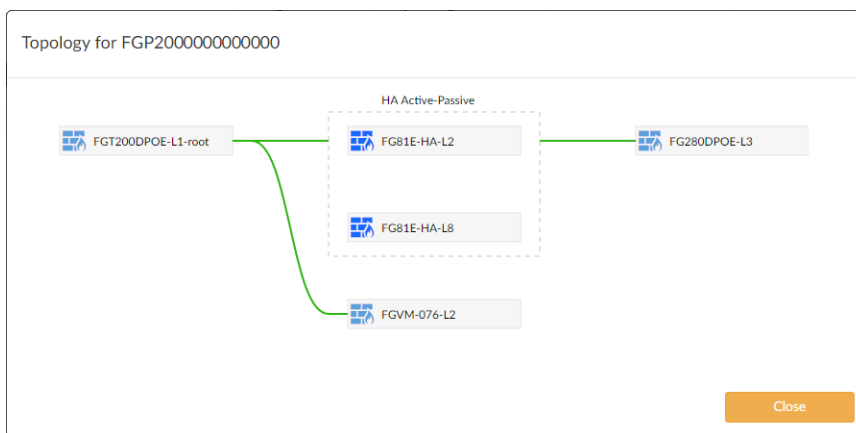
For Security Fabric devices, you can display the Security Fabric topology.

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.

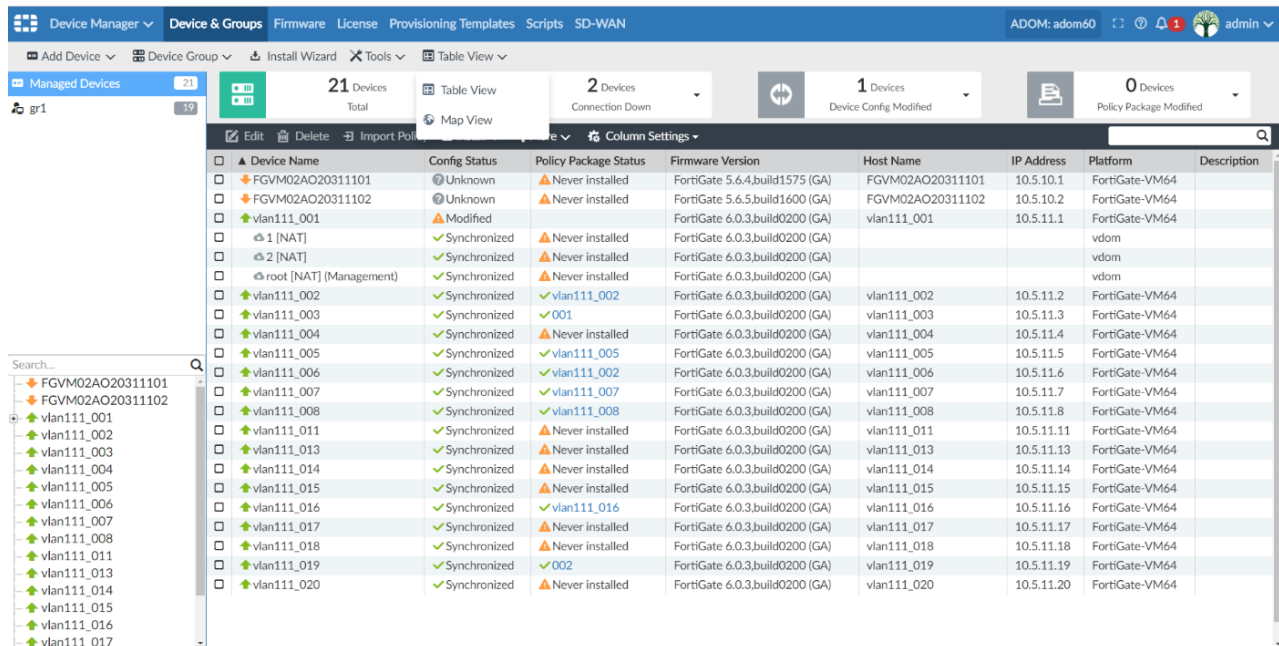


Manage Devices from Map View

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:

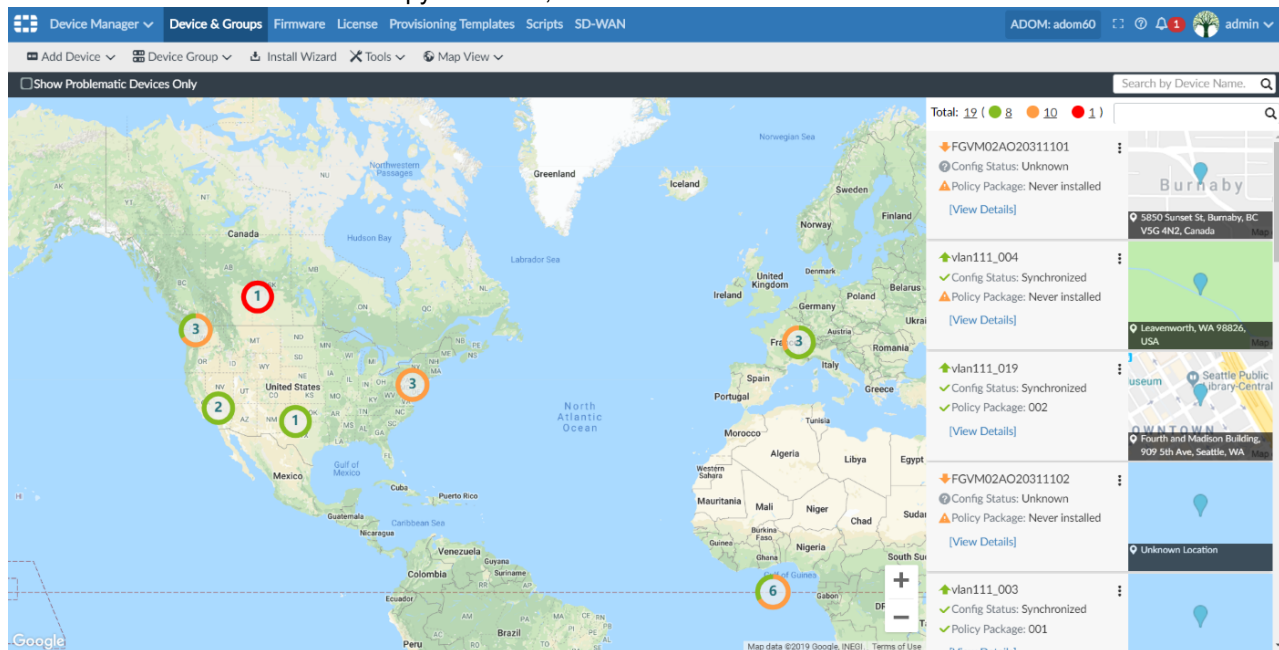
1. Go to Device Manager and select *Map View* from the menu options.



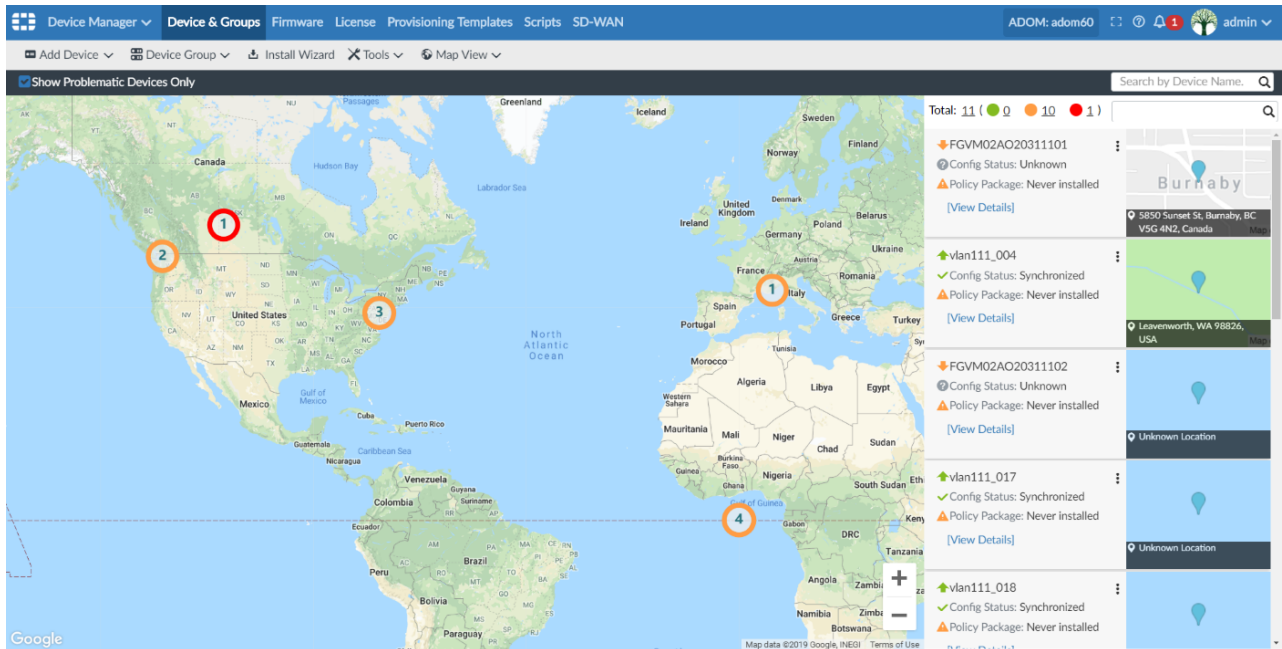
Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	IP Address	Platform	Description
FGVM02AO20311101	Unknown	Never installed	FortiGate 5.6.4.build1575 (GA)	FGVM02AO20311101	10.5.10.1	FortiGate-VM64	
FGVM02AO20311102	Unknown	Never installed	FortiGate 5.6.5.build1600 (GA)	FGVM02AO20311102	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)			vdome	
2 [NAT]	Synchronized	Never installed	FortiGate 6.0.3.build0200 (GA)			vdome	
root [NAT] (Management)	Synchronized	Never installed	FortiGate 6.0.3.build0200 (GA)			vdome	
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.

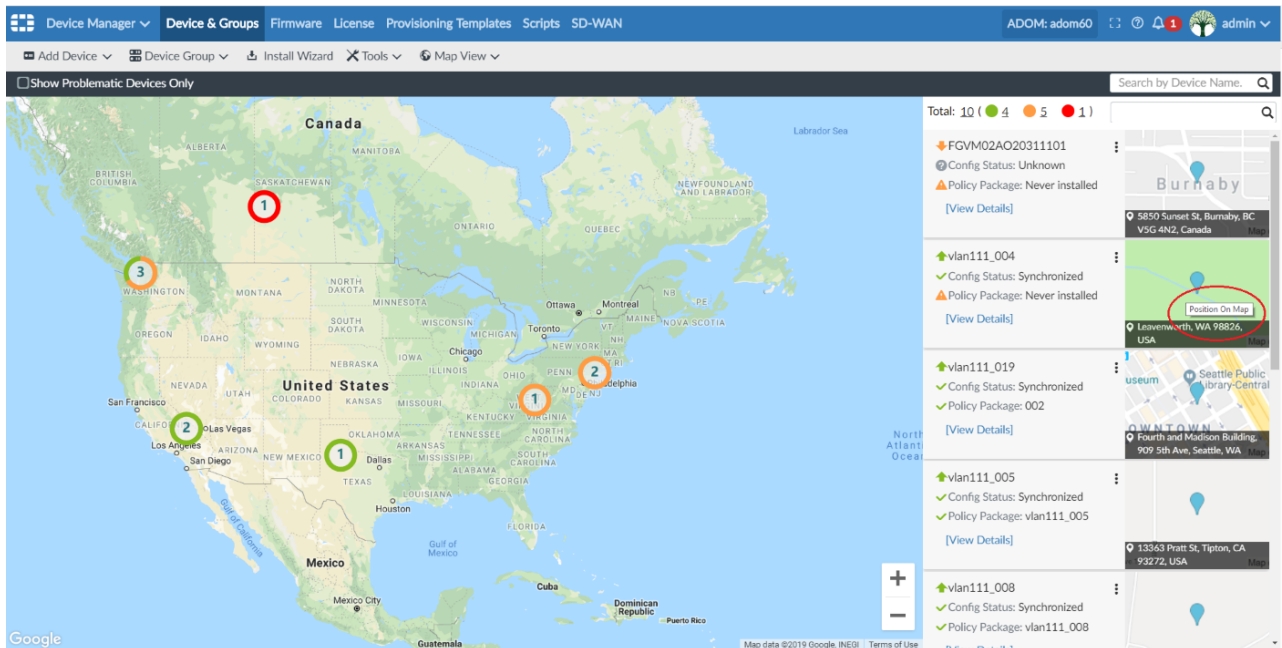
- Green - Shows devices are healthy. The policy package configuration and device configuration are in sync.
- Orange - Shows a warning status. The device configuration status or policy package configuration status is *Out of Sync*. Or, there is no policy imported or no policy package installed.
- Red - 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.



4. 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 Device Manager interface. The 'Device & Groups' tab is selected. The 'Show Unpositioned Devices' filter is active. The table lists devices with their names, geographic coordinates, cities, and countries. A red pin is placed on the map in Sunnyvale, CA, USA, with a label 'Drag to Desired Location'.

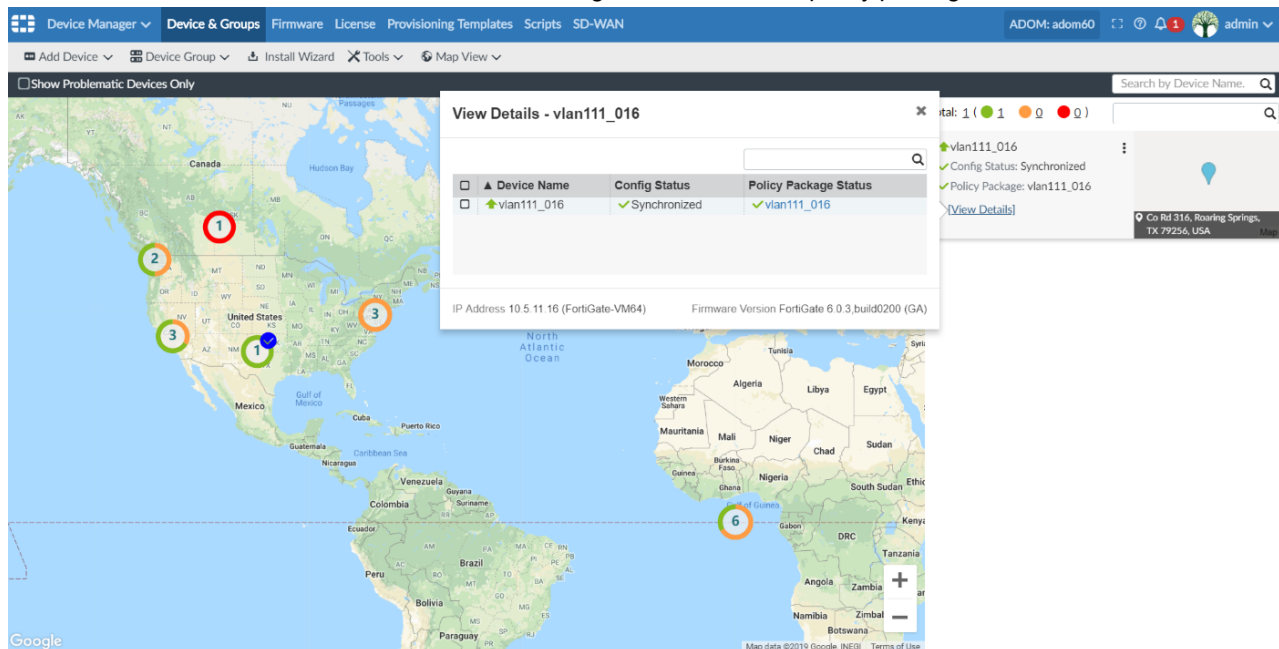
Device Name	Geographic Coordinate	City	Country
FGVM02AO20311101	49.2488091, -122.9805104	Burnaby	Canada
FGVM02AO20311102	0, 0	Unknown Location	Democratic Republic of the Congo
vlan111_001	38.5481654230466, -80.33203125	Webster Springs	United States
vlan111_002	45.089035564831, 0.87890625	Saint-Pierre-de-Chignac	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.

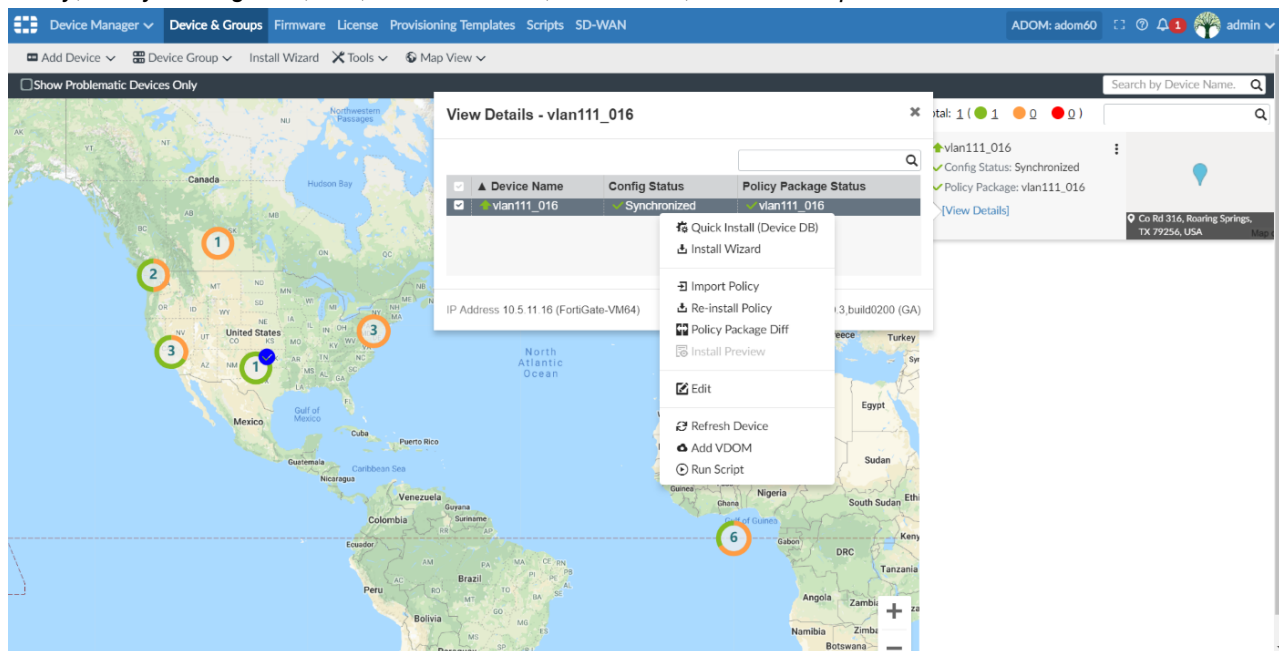
The screenshot shows the FortiManager Device Manager interface. The 'Device & Groups' tab is selected. The 'Show Unpositioned Devices' filter is active. The table lists devices with their names, geographic coordinates, cities, and countries. A red pin is placed on the map in Sunnyvale, CA, USA, with a label 'Drag to Desired Location'.

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.



Device Name	The name of the device and its connectivity status.
Config Status	See the table below for config status details.
Policy Package Status	See the table below for policy package status details. Click on the policy package name to go to view and manage the package (see Managing policy packages on page 191).
Host Name	The host name for the device (available for managed devices).
IP Address	The IP address of the device.
Platform	The platform of the device (available for managed devices).
Description	Description of the device.
HA Status	The HA status of the device.
FortiGuard License	Status of the FortiGuard license for the device.
Firmware Version	The firmware version.
Management Mode	Management mode of the device.
SN	The serial number of the device.
Controller Counter	The number of each device type controlled by this device, such as FortiAPs and FortiSwitches.
Company/Organization	The company or organization information.
Country	The country where the device is located.
Province/State	The province or state.
City	The city.
Contact	The contact information.

The following table identifies the different available config statuses.

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

The following table identifies the different available policy package statuses.

Policy Package Status	Icon	Description
Imported	Green check ✓	Policies and objects are imported into FortiManager.
Synchronized	Green check ✓	Policies and objects are synchronized between FortiManager and the managed device.
Modified	Yellow triangle ⚠	Policies or objects are modified on FortiManager.
Out of Sync	Red X ✖	Policies or objects are modified on the managed device.

Policy Package Status	Icon	Description
Unknown with policy package name	Gray question mark 	Configurations of the managed device are retrieved on FortiManager after being imported/installed.
Never Installed	Yellow triangle 	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:

System Template	Displays the name of the selected system template. Click <i>Change</i> to change the system template.
Database Configuration	Click <i>View</i> to display the database configuration file of the FortiGate unit.
Total Revisions	Displays the total number of configuration revisions and the revision history. Click <i>Revision History</i> to view device history. For details, see Managing configuration revision history on page 91 . Click <i>Revision Diff</i> to compare revisions. For details, see Comparing different configuration files on page 94 .
Sync Status	<p>The synchronization status with the FortiManager.</p> <ul style="list-style-type: none"> • <i>Synchronized</i>: The latest revision is confirmed as running on the device. • <i>Out_of_sync</i>: The configuration file on the device is not synchronized with the FortiManager system. • <i>Unknown</i>: The FortiManager system is unable to detect which revision (in revision history) is currently running on the device. <p>Click <i>Refresh</i> to update the synchronization status.</p>

Warning	<p>Displays any warnings related to configuration and installation status.</p> <ul style="list-style-type: none"> • <i>None</i>: No warning. • <i>Unknown configuration version running on FortiGate: FortiGate configuration has been changed!</i>: The FortiManager system cannot detect which revision (in revision history) is currently running on the device. • <i>Unable to detect the FortiGate version</i>: Connectivity error. • <i>Aborted</i>: The FortiManager system cannot access the device.
Installation Tracking	
Device Settings Status	<ul style="list-style-type: none"> • <i>Modified</i>: Some configuration on the device has changed since the latest revision in the FortiManager database. Click <i>Save Now</i> to install and save the configuration. • <i>UnModified</i>: All configuration displayed on the device is saved as the latest revision in the FortiManager database.
Installation Preview	Click <i>Preview</i> 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 <i>View History</i> 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.
View Install Log	View the installation log for the selected revision.

Revision Diff	Show only the changes or differences between two versions of a configuration file. For details, see Comparing different configuration files on page 94 .
Retrieve Config	View the current configuration running on the device. If there are differences between the configuration file on the device and the configuration file in the repository, a new revision is created and assigned a new ID number.
More	From the More menu, you can select one of the following: <ul style="list-style-type: none"> • Download Factory Default • Revert • Delete • Rename • Import Revision

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

The following columns of information are displayed:

ID	The revision number. Double-click an ID to view the configuration file. You can also click <i>Download</i> to save the configuration file.
Date & Time	The time and date when the configuration file was created.
Name	A name assigned by the user to make it easier to identify specific configuration versions. You can rename configuration versions.
Created by	The name of the administrator account used to create the configuration file.
Installation	Display the status of the installation. <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> .
Comments	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.

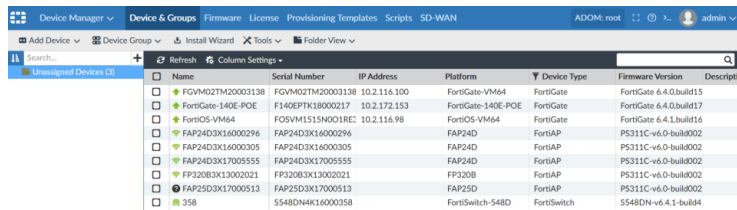
Organizing devices using the new folder view

You can now organize devices within the tree menu in *Device Manager* to display FortiGates. The *Folder View* feature allows you to create, nest, and move folders in the tree menu. You can also move devices between folders.

To access the new folder view:

1. Go to *Device Manager* > *Device & Groups*.
2. In the *Table View* dropdown menu, select *Folder View*.

By default, all the devices are placed under *Unassigned Devices* in the tree menu.

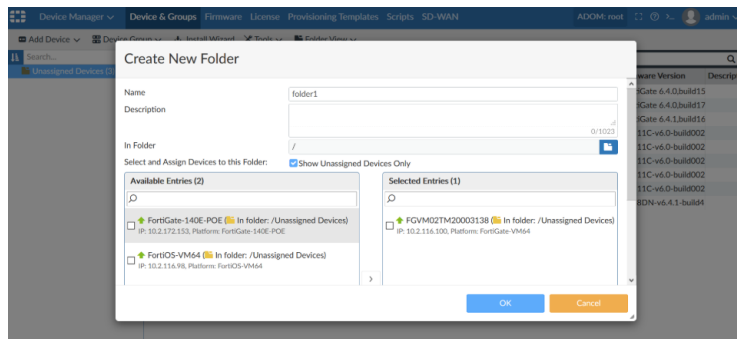


Name	Serial Number	IP Address	Platform	Device Type	Firmware Version	Description
FGVM02TM20003138	FGVM02TM20003138	10.2.116.100	FortiGate-VM64	FortiGate	FortiGate 6.4.0.build15	
FortiGate-140E-POE	F140EPTK38000217	10.2.172.153	FortiGate-140E-POE	FortiGate	FortiGate 6.4.0.build17	
FortiOS-VM64	FOSVM1515N001RE	10.2.116.98	FortiOS-VM64	FortiGate	FortiGate 6.4.1.build16	
FAP24D3X16000296	FAP24D3X16000296		FAP24D	FortiAP	P5311C-v6.0-build002	
FAP24D3X16000305	FAP24D3X16000305		FAP24D	FortiAP	P5311C-v6.0-build002	
FAP24D3X17005555	FAP24D3X17005555		FAP24D	FortiAP	P5311C-v6.0-build002	
FP320B3X13002021	FP320B3X13002021		FP320B	FortiAP	P5311C-v6.0-build002	
FAP25D3X17000513	FAP25D3X17000513		FAP25D	FortiAP	P5311C-v6.0-build002	
358	S548DN4K16000358		FortiSwitch-548D	FortiSwitch	S548DN-v6.4.1-build04	

To create a folder:

1. Go to *Device Manager* > *Device & Groups*.
2. In the *Table View* dropdown menu, select *Folder View*.
3. To create a new folder, either click + beside the *Search* bar in *Folder View*, or right-click *Unassigned Devices*, and select *Create New Folder*.

The *Create New Folder* dialog opens.



Create New Folder

Name: folder1

Description: 0/1023

In Folder: /

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

Available Entries (2):

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

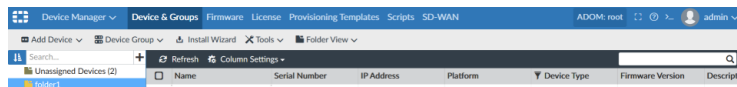
Selected Entries (1):

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

Buttons: OK, Cancel

4. In the *Create New Folder* dialog, enter the name of the folder as *folder1*. Click *OK*.

The new folder is created and visible in the tree menu. Also, the FortiGates in the folder are now displayed in the content pane.



Name	Serial Number	IP Address	Platform	Device Type	Firmware Version	Description
folder1						
FGVM02TM20003138	FGVM02TM20003138	10.2.116.100	FortiGate-VM64	FortiGate	FortiGate 6.4.0.build15	



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

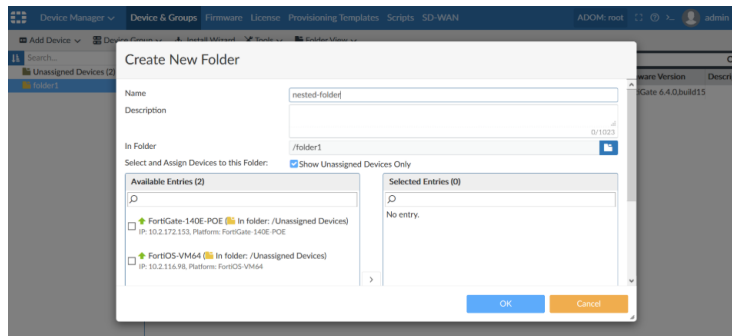
Nested folders

The new *Folder View* supports nested folders.

To create a nested folder:

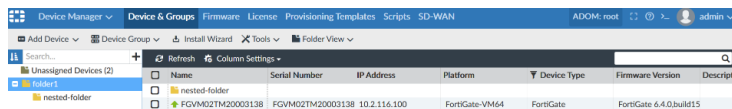
1. In the tree menu, right-click the folder you intend to nest and select *Create New Folder*.
For instance, right-click the previously created folder1 and select *Create New Folder*.
The *Create New Folder* dialog opens.

In Folder shows that the new folder will be created within folder1.



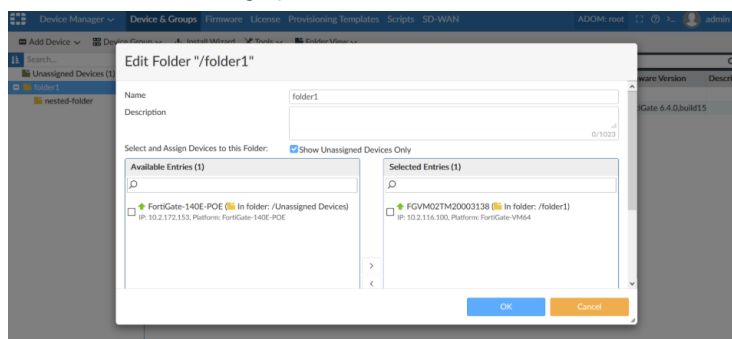
2. In the *Create New Folder* dialog, enter the name of the folder as nested-folder.
Click **OK**.

The nested-folder is created and displayed in the tree menu under the previously created folder1. Also, the folder and the FortiGates in the parent folder are displayed in the content pane.



To move FortiGates between folders:

1. Go to *Device Manager > Device & Groups*.
2. In the *Table View* dropdown menu, select *Folder View*.
3. In the tree menu, right-click the folder where the FortiGate is to be moved, and select *Edit*.
The *Edit Folder* dialog opens.



4. In the *Edit Folder* dialog, select the FortiGate to be moved from the *Available Entries* list.
Click **OK**.



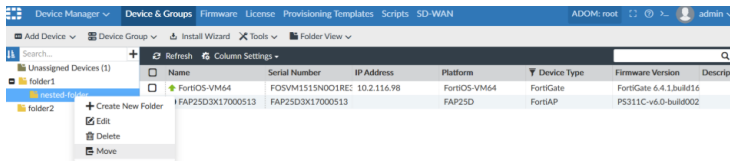
Alternatively, from the *Device & Groups* pane, select a FortiGate, drag and drop it to the folder where you want to move the selected FortiGate.



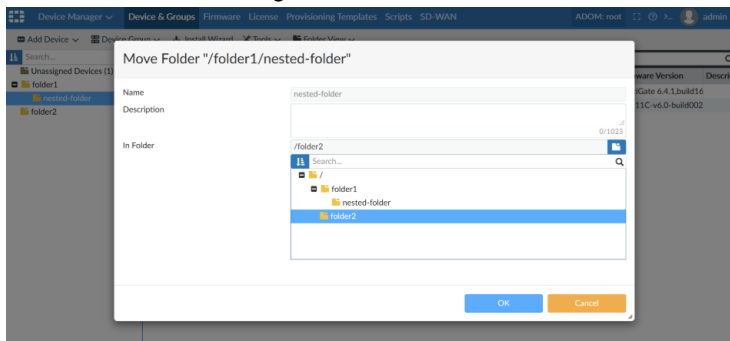
At any given time, a FortiGate can only be added to one folder.

To move a folder:

1. Go to *Device Manager > Device & Groups*.
2. In the *Table View* dropdown menu, select *Folder View*.
3. In the tree menu, right-click the folder you want to move, here nested-folder, and select *Move*. The *Move Folder* dialog opens.

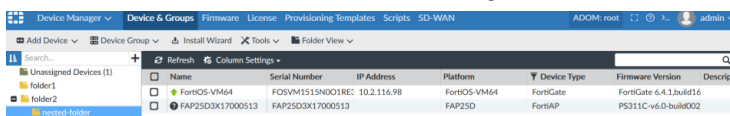


4. In the *Move Folder* dialog, under *In Folder*, select the destination folder, here folder2.



Click **OK**.

The nested-folder moves to folder2 including folders and devices in it.



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 for managed devices as well as the upgrade history for managed devices.

This section contains the following topics:

- [View firmware for device groups on page 99](#)
- [Upgrade firmware for device groups on page 99](#)

- [Firmware Management on page 99](#)
- [Automatic multi-step firmware upgrade on FortiGate on page 102](#)
- [Managed devices pull firmware from FortiGuard on page 104](#)

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 99](#).

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.

When workspace is enabled, you must lock a device (or ADOM) to allow firmware upgrade.

The FortiGate device requires a valid firmware upgrade license. Otherwise a *Firmware Upgrade License Not Found* error is displayed.



When *Boot to Alternate Partition After Upgrade* is selected, the inactive partition will be upgraded.

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

#	Device Name	Platform	Current Build	Upgrade Available	Status
5.4.2 (1)					
1	FortiGate-VM64	FortiGate-VM64	1486	6.0.0 (76) Upgrade	
6.0.0 (2)					
1	lgt142	FortiGate-200D-POE	76	Running Latest Release	
2	lgt148	FortiGate-80E-POE	119	6.0.0 (76) Upgrade	

The following information and options are available:

Upgrade	Select to upgrade the selected device if the device can be upgraded.
View Release Notes	Select to view the release notes for the FortiOS version of the selected device.
Imported Images	Select to display the imported images where you can import or delete images.
Refresh	Refresh the list.
Column Settings	Click to select which columns to display or select <i>Reset to Default</i> to display the default columns.
Device Name	The names of the FortiGate devices in the group, organized by firmware version.
Platform	The device platform.
Current Build	The build installed in the device.
Upgrade Available	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.
Status	The status of the device's license. If the license has expired, the firmware cannot be upgraded.
Upgrade History	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

FGVM00TM19002130: 6.2.1 (932)

Upgrade to

6.0.5 (0268)

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

2019/09/26

15:28

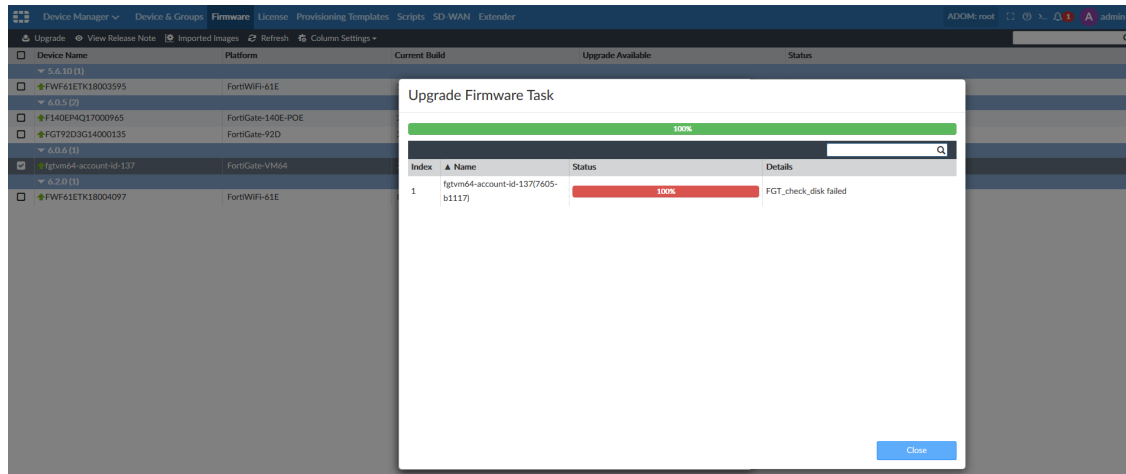
OK

Cancel

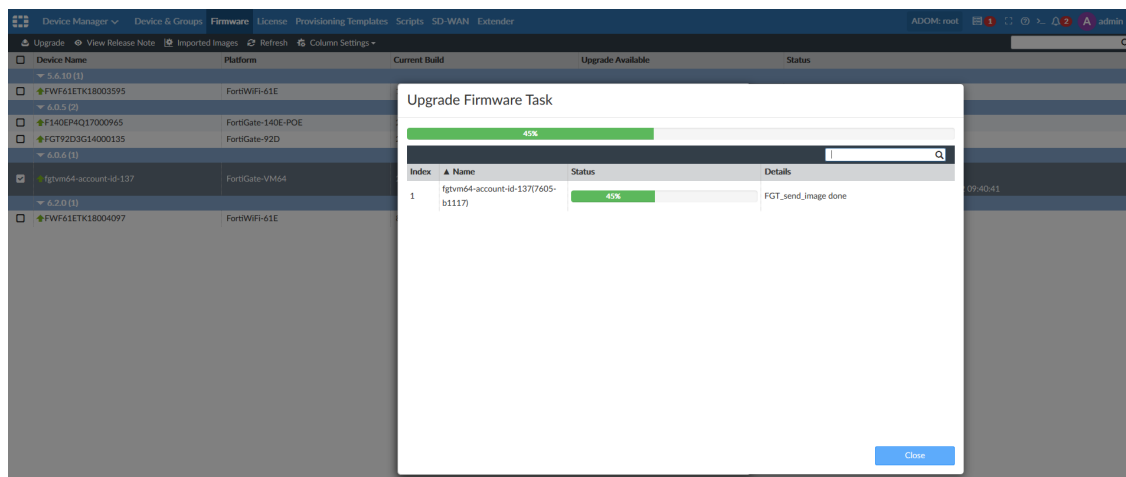
4. Configure the following settings, then click **OK**:

Upgrade to	Select a firmware version from the drop-down list.
Boot From Alternate Partition After Upgrade	Selecting this option causes the device to reboot twice during the upgrade process: first to upgrade the inactive partition, and second to boot back into the active partition.
Let Device Download Firmware from FortiGuard	Select this option to download the firmware directly from FortiGuard. If this option is not selected, FortiManager will download the firmware from FortiGuard. Alternatively, you can import the firmware into FortiManager.
Skip All Intermediate Steps in Upgrade Path if Possible	FortiManager manages the most optimum upgrade path automatically. Select this option to install the selected version directly without going through the upgrade path.
Schedule Upgrade	Select to schedule the upgrade, then enter the date and time for the upgrade.

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



If the check passes, the upgrade proceeds:





FortiOS devices cannot be upgraded to a version that is higher than the FortiManager that is managing them. This rule is applicable only for major and minor versions. For example, FortiManager 6.2.0 cannot upgrade FortiOS devices to 6.3.0 or 7.0.0. When trying to upgrade FortiOS devices to a version higher than FortiManager, the upgrade process cannot be completed and a warning is shown.

When upgrading FortiGate devices to a firmware version that is not part of the upgrade path (shown by the green check mark), the warning *The firmware version is not on firmware upgrade path of selected devices. Upgrading the image may cause the current syntax to break.* is shown. Click *Upgrade to Recommended X.X.X* which shows the recommended version, or *Continue* to upgrade to the selected version. A warning is also shown when upgrading FortiGate devices to a custom firmware.



The disk on the FortiGate is checked automatically before upgrade. To enable skip disk check run the `set skip-disk-check` from the command line.

To disable disk check:

1. Disable disk check by using the CLI:

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

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

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

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

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

```
$ ssh admin@193.168.70.137
WARNING: File System Check Recommended! Unsafe reboot may have caused inconsistency in disk drive.
```

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

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

Automatic multi-step firmware upgrade on FortiGate

When using FortiManager to upgrade firmware on FortiGate, FortiManager can choose the shortest upgrade path based on the FortiGate upgrade matrix. In a multi-step firmware upgrade, each upgrade is a subtask.

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

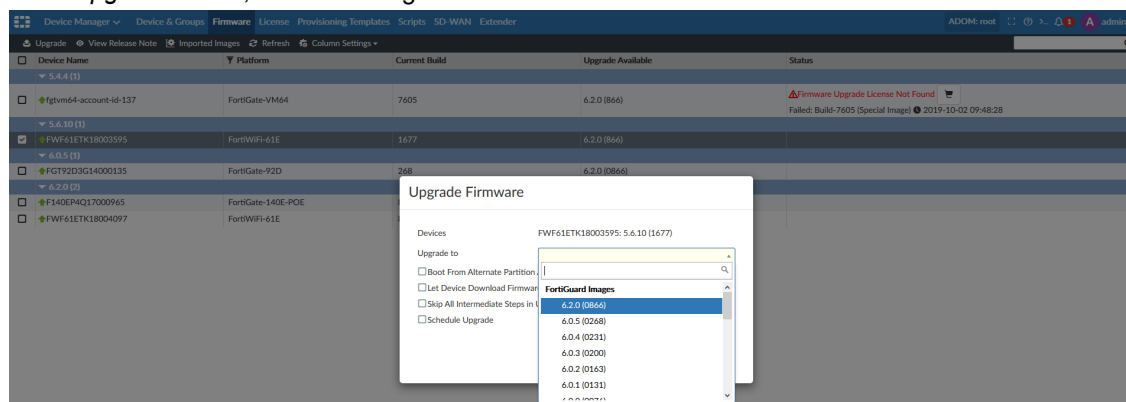
```
# diagnose fwmanager show-dev-upgrade-path 318 6.2.0
device FWF61ETK18003595(318), platform FWF61E, upgrade path from 5.6.10-1677 to 6.2.0-866
is: [6.0.0-76 --> 6.0.2-163 --> 6.0.3-200 --> 6.2.0-866]
```

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

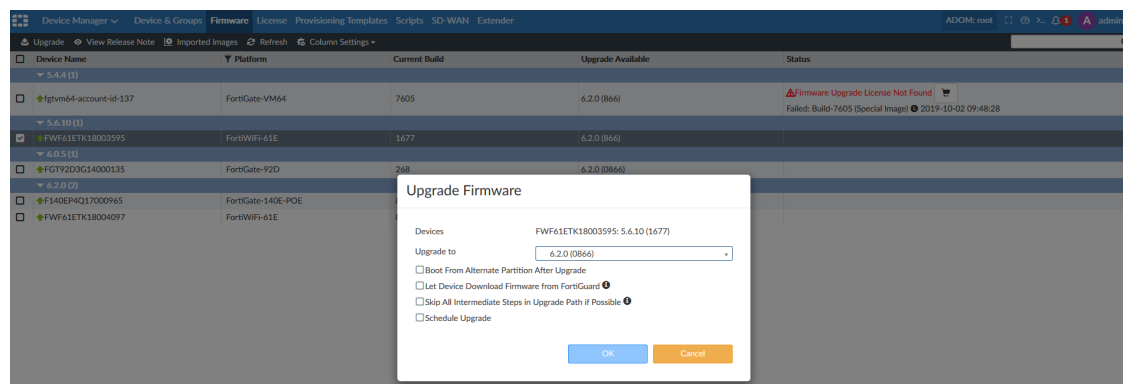
In this example, the device ID is 318, and you want to upgrade the device to FortiOS 6.2.0. The device is currently running FortiOS 5.6.10 build 1677, and the shortest upgrade path to FortiOS 6.2.0 is displayed.

To upgrade using the GUI:

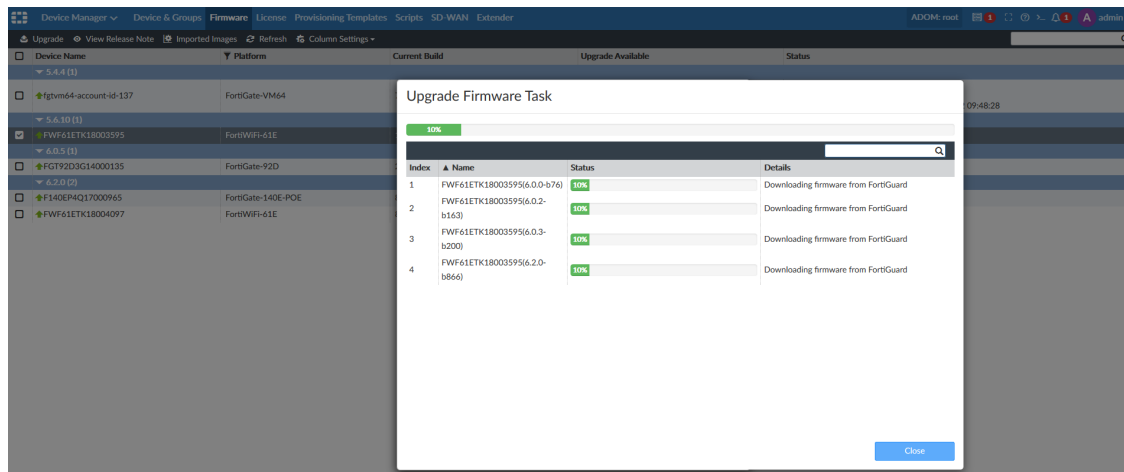
1. Go to *Device Manager > Firmware*.
2. Select a device, and click *Upgrade*.
The *Upgrade Firmware* dialog box is displayed.
3. In the *Upgrade to* box, select an image.



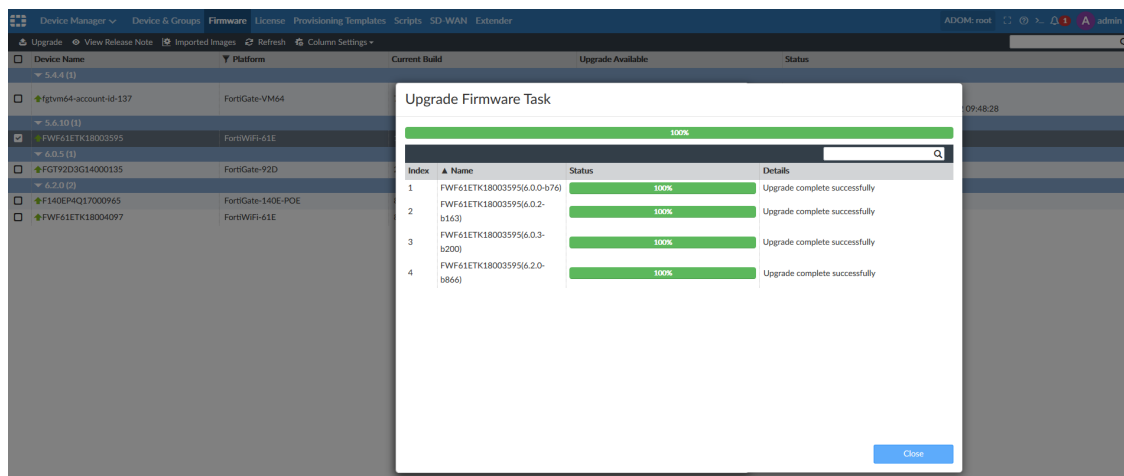
In this example, the FortiGate is running FortiOS 5.6.10, and we are going to upgrade to 6.2.0 (0866).



4. Click *OK*.
The *Upgrade Path Preview* dialog box opens to let you review the upgrade before continuing.
5. Click *OK* to start the upgrade.
FortiManager starts the upgrade. Each upgrade is a subtask.



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



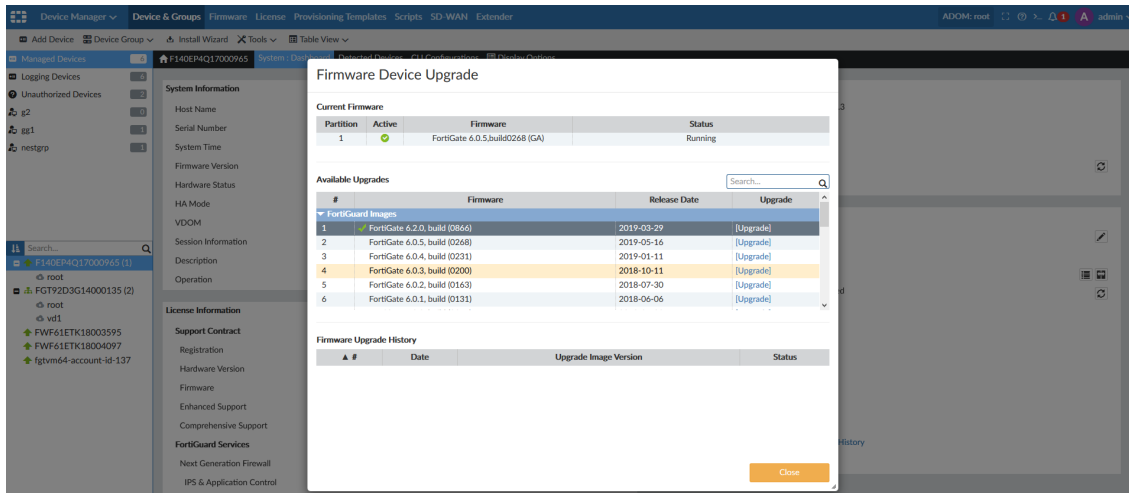
- When the upgrade completes, click *Close*.

Managed devices pull firmware from FortiGuard

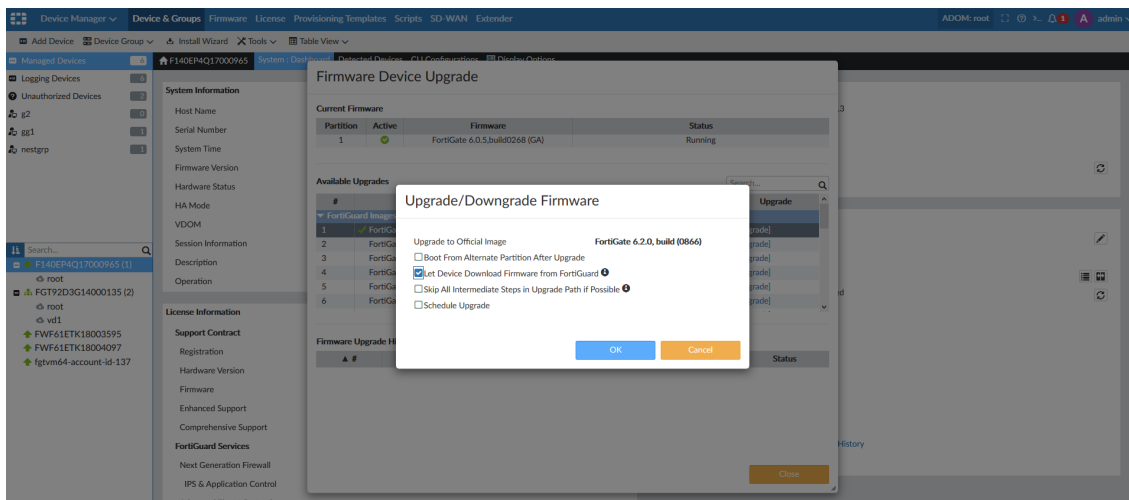
FortiManager retrieves firmware for managed devices from FortiGuard, and you can choose to use the images to upgrade firmware on managed devices.

To upgrade firmware using images retrieved from FortiGuard:

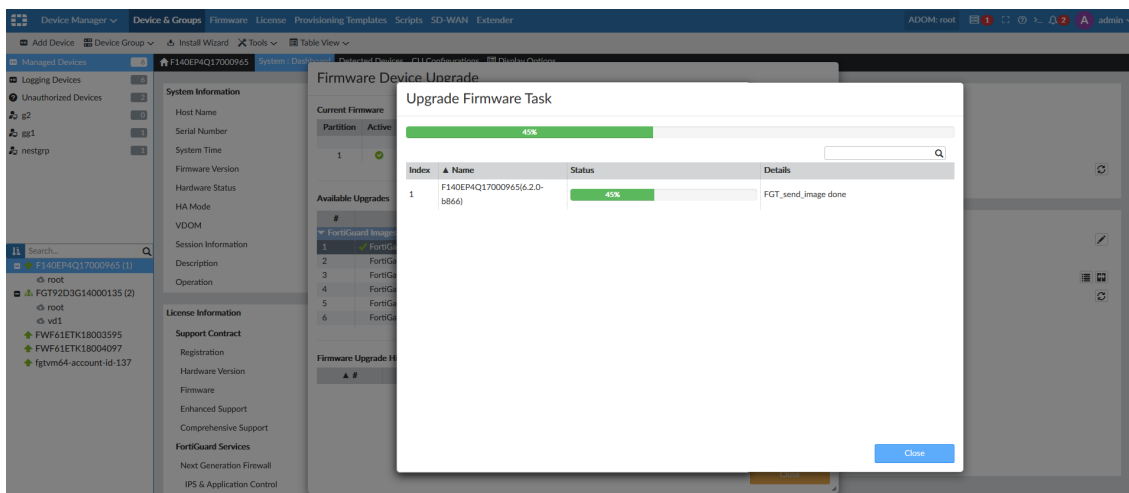
- Go to *Device Manager > Device & Groups*, and select a device.
- In the *System Information* widget, click the *Update* icon beside *Firmware Version*.
The *Firmware Device Upgrade* dialog box displays a list of images retrieved from FortiGuard.



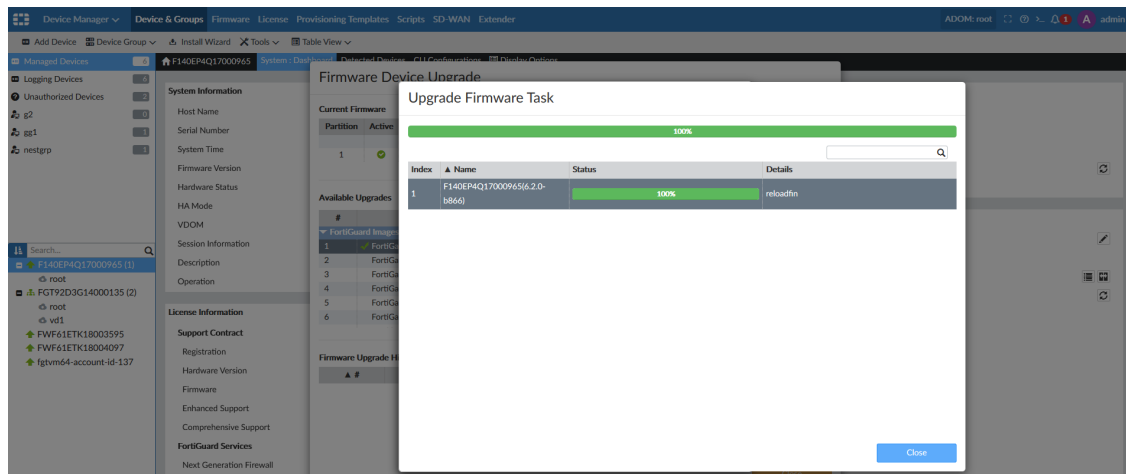
- Click **Upgrade** for the desired FortiGuard image.
The **Upgrade/Downgrade Firmware** dialog box is displayed.



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



The firmware upgrade completes.



5. Click *Close*.

License

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

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

- VDOM disabled: 1 FortiGate = 1 license.
- VDOM enabled: 1 VDOM = 1 license.
- VDOM enabled but no VDOMs: root = 1 license.
- FortiGate in HA mode: No license count for secondary FortiGate.
- Unregistered device in root ADOM: 1 unregistered device = 1 ADOM. License is not counted for hidden devices.
- FortiGate with FMGC contract: No license count for FortiManager VM. License is only counted for FortiManager hardware.



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

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 Manager > Device & Groups > Firmware > License							
<div> <div>Push Update Refresh Export Check License Column Settings</div> <div>ADOM: root admin</div> </div>							
Device Name	Serial Number	Firmware Version	Support Contract	FortiGuard Subscription	Service Status	Virtual Domains	
FGVM00TM19002130	FGVM00TM19002130	6.2.1, build932	8x5	All Valid	Up to Date	(50%)	

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

Device Name	Name of the device
Serial Number	Serial number for the device
Firmware Version	Firmware version for the device
Support Contract	<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"> • N/A: No support contract • 24/7: Support contract level that provides support 24 hours per day and 7 days per week • 8/5: Support contract level
FortiGuard Subscription	<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 & Application Control, Antivirus, Web Filtering, and Email Filtering. License status can include:</p> <ul style="list-style-type: none"> • All valid • Expires in <time> • Expired • Unknown
Service Status	<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"> • Update Available • Up to Date • Expired • Unknown
Virtual Domains	<p>Number of virtual domains. Click the cart icon to go to the Fortinet support site (https://support.fortinet.com)</p>

The following buttons are available on the toolbar:

Push Update	Push a license update to the selected device in the group.
Refresh	Refresh the list of devices in the group.
Export	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.
Check License	<p>Click to launch the <i>Check License</i> screen. Select the FortiGuard license types that you want FortiManager to check expiry dates for and provide warnings when it is expired or approaching expiry date.</p> <p>The <i>FortiGuard Subscription</i> status is updated based on the selection in the Check License screen. If a license is expiring in 30 days, its license status is in orange (warning). If a license is expired already, the status is in red (error).</p>
Column Settings	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 536](#).

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 screenshot displays the FortiManager System Templates configuration interface. It features several widgets for configuring system settings:

- DNS:** Fields for Primary DNS Server, Secondary DNS Server, and Local Domain Name, with an 'Apply' button.
- Alert Email:** Fields for SMTP Server, Authentication (checkbox), SMTP User, and Password, with an 'Apply' button.
- SNMP:** Includes an 'SNMP Agent' checkbox and two sections for 'SNMP v1/v2c' and 'SNMP v3' settings, each with a table for configuration and an 'Apply' button.
- NTP Server:** Includes a 'Synchronize with NTP Server' checkbox, 'Server Type' (Use FortiGuard or Specify), and 'Sync Interval' (1 to 1440 mins), with an 'Apply' button.
- Admin Settings:** Includes fields for HTTP Port, HTTPS Port, SSH Port, Telnet Port, SSH v1 compatibility, Idle Timeout, Allow Concurrent Sessions, Switch Controller, View Settings (Language, Lines per page, Theme), and IPv6 Support on GUI, with an 'Apply' button.
- Replacement Message:** Includes an 'Edit' button, a 'Reset' button, and a table for replacement messages with columns for Name, Description, and Action.

The following widgets and settings are available:

Widget	Description
DNS	Primary DNS Server, Secondary DNS Server, Local Domain Name. You can also allow overrides. See Allowing system template overrides on page 110 .
NTP Server	Synchronize with NTP Server and Sync Interval settings. You can select to use the FortiGuard server or specify one or more other servers.
Alert Email	SMTP Server settings including server, authentication, SMTP user ID, and password.
Admin Settings	Web Administration Ports, Timeout Settings, and Web Administration.
SNMP	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.

Widget	Description
Replacement Messages	You can customize replacement messages. Click <i>Import</i> to select a device and the objects to import.
FortiGuard	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> .
Log Settings	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.
Interface	Zone and interface settings. In the toolbar, you can select to create, edit, or delete the record. To create a new interface, click <i>Create New</i> and specify an action and identify what models will receive the action. You can also allow overrides and preview actions. See Allowing system template overrides on page 110 and Previewing interface actions on page 111 .

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 tree menu, select a template, and expand *This template is assigned to <number> devices* in the content pane.



3. Click *Assigned to Devices*.
The *Assign to Device* dialog box is displayed.
4. In the *Available Entries* list, select one or more devices, and click *>* to move them to the *Selected Entries* list, and then click *OK*.
The devices assigned to the template are shown in the *Assign to Devices* column.

Allowing system template overrides

When you create a system template that includes settings from the *Interface* widget or the *DNS* widget, you can allow value overrides. When overrides are allowed, you can change system template settings for each device after the template is applied. See [Overriding system template settings on page 113](#).

To allow system template overrides:

1. Go to *Device Manager > Provisioning Templates > System Templates*.
2. Double-click a system template to open it for editing.
3. In the *Interface* widget, double-click an interface to open it for editing.
The *Edit Action* dialog box is displayed.

Edit Action

Action: Config Interface

Model: all

Interface Name: port9

☒ Allow Override Value ?

IP/Netmask: 10.2.114.94/255.255.255.0

☒ Allow Override Value ?

Administrative Access:

<input type="checkbox"/> fabric	<input checked="" type="checkbox"/> fgfm	<input type="checkbox"/> ftm
<input type="checkbox"/> http	<input checked="" type="checkbox"/> https	<input type="checkbox"/> ping
<input type="checkbox"/> probe-response	<input type="checkbox"/> radius-acct	<input type="checkbox"/> snmp
<input checked="" type="checkbox"/> ssh	<input type="checkbox"/> telnet	
<input checked="" type="checkbox"/> Allow Override Value ?		

OK Cancel

- By the options for which you want to allow overrides, select the *Allow Override Value* checkbox, and click *OK*.
- In the *DNS* widget, select the *Allow Override Value* checkbox beside the options for which you want to allow overrides.

Toggle Widgets CLI Configurations

This template is assigned to 1 devices. >

DNS

Primary DNS Server: 208.91.112.53

☒ Allow Override Value ?

Secondary DNS Server: 208.91.112.52

☒ Allow Override Value ?

Local Domain Name:

☒ Allow Override Value ?

Loading Advanced Options ...

Apply

Previewing interface actions

After you create an interface action, you can preview the interface action per model or device.

To preview interface actions:

- Go to *Device Manager > Provisioning Templates > System Templates*.
- In the tree menu, select a template with an interface.
The template details are displayed in the content pane.
- In the *Interface* widget, select an interface, and click *Post Action View*.
The *Post Action Preview* dialog box is displayed.
- Beside *Preview on*, click *Platform* or *Device*, and then select the platform or device from the list.
In the following example, the selected platform has the same type of port.

Post Action Preview

Preview on Platform Device

Device Model FortiOS-VM64

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

Cancel

In the following example, the selected platform does not have the same type of port, and an error is displayed.

Device Manager | Device & Groups | Firmware | License | Provisioning Templates | Scripts | SD-WAN | ADOM: fgt64 | admin

system/interface/port9/: runtime error -999: VLAN id must between 1 to 4094 - prop[template action(conf-intf)]: runtime error -2: VLAN id must between 1 to 4094

Post Action Preview

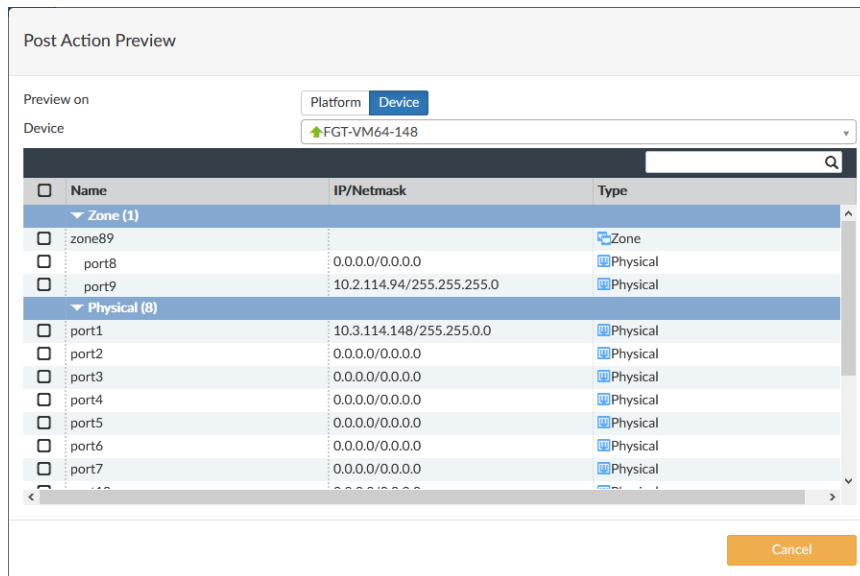
Preview on Platform Device

Device Model FortiGate-40F

<input type="checkbox"/>	Name	IP/Netmask	Type
No record found.			

Cancel

In the following example, the selected device has the same type of port.



- Click *Cancel* to close the dialog box.

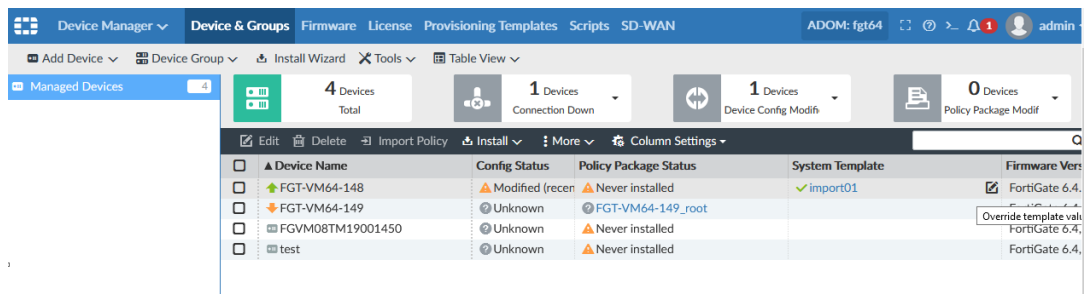
Overriding system template settings

When you create a system template that includes settings from the *Interface* widget or the *DNS* widget, and you have enabled overrides for options, you can override values for each device after the template has been applied.

To override system template settings:

- Go to *Device Manager > Device & Groups > Managed Devices*.
- In the content pane, select a device that uses a system template.
- In the *System Template* column, hover over the template name.

An *Override Template Values* icon is displayed.



- Click the *Override Template Values* icon.
The system template settings are displayed.

import01 widget override


DNS ▾

Primary DNS Server

Secondary DNS Server

Local Domain Name

Interface ▾

 Edit

<input type="checkbox"/>	#	Action	Model Match	Detail
<input type="checkbox"/>	1	Config Interface	all	name: port9; ip: 10.2.114.94/255.255.255.0; allowaccess: 133;
<input type="checkbox"/>	2	Monitor Interface Bandwidth	all	name: port9; monitor-bandwidth: 1;
<input type="checkbox"/>	3	Add Zone	all	name: zone89; interface: 2;
<input type="checkbox"/>	4	Add Aggregate Interface	all	name: agr57; vdom: root;

OK Cancel

- For *DNS* settings, edit the options.
- For *Interface* settings, double-click an action to open it for editing.
The *Edit Action* dialog box is displayed.

Edit Action

Action

Model

Interface Name

IP/Netmask

Administrative Access

<input type="checkbox"/> fabric	<input checked="" type="checkbox"/> fgfm	<input type="checkbox"/> ftm
<input type="checkbox"/> http	<input checked="" type="checkbox"/> https	<input type="checkbox"/> ping
<input type="checkbox"/> probe-response	<input type="checkbox"/> radius-acct	<input type="checkbox"/> snmp
<input checked="" type="checkbox"/> ssh	<input type="checkbox"/> telnet	

OK Cancel

- Edit the settings, and click **OK**.
The setting overrides are saved.
- Click **OK**.

Threat Weight templates

User or client behavior can sometimes increase the risk of being attacked or becoming infected. For example, if one of your network clients receives email viruses on a daily basis while no other clients receive these attachments, extra measures may be required to protect that client, or a discussion with the user about this issue may be warranted.

Before you can decide on a course of action, you need to know the problem is occurring. Threat weight can provide this information by tracking client behavior and reporting on activities that you determine are risky or worth tracking.

Threat weight profiles can be created, edited, and assigned to devices. When Threat Weight Tracking is enabled, the *Log Allowed Traffic* setting is enabled on all policies.

To create a new threat weight profile:

1. Go to the *Device Manager > Provisioning Templates > Threat Weight*.
2. Click *Create New* in the toolbar.
3. In the *Create New Threat Weight* pane, type a name for the profile.
4. Click *OK* to create the new threat weight profile.

To edit a threat weight profile:

1. Select a threat weight profile and click *Edit*. The *Edit Threat Weight* pane opens.
2. Adjust the threat levels as needed, then click *OK* to save your changes:

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

To assign a threat weight profile to a device:

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

Certificate templates

The certificate templates menu allows you to create certificate templates for an external certificate authority (CA) or the local FortiManager CA.

FortiManager includes a certificate authority server for each ADOM. When you create an ADOM, the private and public key pair is created for the ADOM. The key pair is automatically used when you use FortiManager to define IPsec VPNs or SSL-VPNs for a device.

When you add a device to an IPsec VPN or SSL-VPN topology with a certificate template that uses the FortiManager CA, the local FortiManager CA is automatically used. No request for a pre-shared key (PSK) is generated. When the IPsec VPN or SSL-VPN topology is installed to the device, the following process completes automatically:

- The FortiGate device generates a certificate signing request (CSR) file.
- FortiManager signs the CSR file and installs the CSR file on the FortiGate device.
- The CA certificate with public key is installed on the FortiGate device.



Some settings may not be available in all ADOM versions.

The following options are available:

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

To create a new certificate template:

1. Go to *Device Manager > Provisioning Templates > Certificate Templates*.
2. Click *Create New*. The *Create New Certificate Template* pane opens.
3. Enter the following information, then click *OK* to create the certificate template:

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

To edit a certificate template:

1. Select a certificate template, and click *Edit*.
2. Edit the settings as required in the *Edit Certificate Template* pane, and click *OK*.

To delete a certificate template:

1. Select a certificate template, and click *Delete*.
2. Click *OK* in the confirmation dialog box.

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 123](#) 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 633](#).
3. Select *Apply* to apply your changes.

Configuring scripts

To configure, import, export, or run scripts, go to *Device Manager > Scripts*, or *Policy & Objects > Object Configuration > Advanced > Scripts* if you are in the Global Database ADOM. The script list for your current ADOM displays.

The following information is displayed:

Name	The user-defined script name.
Type	The script type.
Target	The script target.
Comments	User defined comment for the script.
Last Modified	The date and time the script was last modified.

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

Run Script / Run	Run the selected script. See Run a script on page 119 .
Schedule Script	Schedule when the selected script will run. See Schedule a script on page 122 .
Create New / New	Create a new script. See Add a script on page 119 .
Edit	Edit the selected script. See Edit a script on page 120 .
Delete	Delete the selected script. See Delete a script on page 121 .
Clone	Clone the selected script. See Clone a script on page 121 .
Import CLI Script / Import	Import a script from your management computer. See Import a script on page 121 .
Export	Export the selected script as a <code>.txt</code> file to your management computer. See Export a script on page 121 .

Select All	Select all the scripts. This option is only available for Global Database scripts.
Search	Enter a search term in the search field to search the scripts.

Run a script

You can select to enable automatic script execution or create a recurring schedule for the script (see [Schedule a script on page 122](#)).

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 128](#) 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 190](#)).
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.

Script Name	Type a unique name for the script.
View Sample Script	This option points to the FortiManager online help.
Comments	Optionally, type a comment for the script.
Type	Specify the type of script. This option is not available for Global Database ADOM scripts.
Run Script on	Select the script target. This settings will affect the options presented when you go to run a script. The options include: <ul style="list-style-type: none">• <i>Device Database</i>• <i>Policy Package or ADOM Database</i>• <i>Remote FortiGate Directly (via CLI)</i> For Global Database ADOM scripts, this option is set to <i>Policy Package or ADOM Database</i> and cannot be changed.
Script Detail	Type the script itself, either manually using a keyboard, or by copying and pasting from another editor.
Advanced Device Filters	Select to adjust the advanced filters for the script. The options include: <ul style="list-style-type: none">• <i>Platform</i> (select from the dropdown list)• <i>Build</i>• <i>Device</i> (select from the dropdown list)• <i>Host name</i>• <i>SN</i> 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:

Devices	Select the devices that the script will be run on. If required, use the search field to find the devices in the list.
Enable Automatic execute after each device install	Select to enable automatic execution of the script or script group after each device install. If this is selected, no schedule can be created. This option is only available is the target is <i>Remote FortiGate Directly (via CLI)</i> .
Enable Schedule	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> .
Recurring	Select how frequently the script or script group will run: <ul style="list-style-type: none"> • <i>One Time</i>- Set the date and time that script or group will run. • <i>Daily</i> - Set the time that the script or group will run everyday. • <i>Weekly</i> - Set the day of the week and the time of day that the script or group will run. • <i>Monthly</i> - Set the day of the month and the time of day that the script or group will run.

CLI script group

CLI scripts can be put into groups so that multiple scripts can be run on a target at the same time.

To manage script groups, go to to *Device Manager > Scripts > CLI Script Group*.

The following information is displayed:

Name	The user-defined script group name.
Members	The scripts that are included in the script group.
Target	The script group target.
Comments	User defined comment for the group.
Last Modified	The date and time the group was last modified.

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

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

Script Group Name	Enter a name for the script group.
Comments	Optionally, type a comment for the script group.
Type	CLI Script. This field is read-only.
Run Script on	Select the script target. This settings will affect the options presented when you go to run a script. The options include: <ul style="list-style-type: none"> • <i>Device Database</i> • <i>Policy Package or ADOM Database</i> • <i>Remote FortiGate Directly (via CLI)</i>
Members	Use the directional arrows to move available scripts to member scripts.

Script syntax

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

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

Syntax applicable for address and address6

```
config firewall address
  edit xxxx

    ...regular FOS command here...

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

Syntax applicable for ippool and ippool6

```
config firewall ippool
  edit xxxx

    ...regular FOS command here...

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

Syntax applicable for vip, vip6, vip46, and vip64

```
config firewall vip
  edit xxxx

    ...regular FOS command here...

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

Syntax applicable for dynamic zone

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

Syntax applicable for dynamic interface

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

Syntax applicable for dynamic multicast interface

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

```
        next
    end
    next
end
```

Syntax applicable for local certificate (dynamic mapping)

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

Syntax applicable for vpn console table

```
config vpnmgr vpntable
    edit xxxx
        set topology star|meshed|dial
        set psk-auto-generate enable|disable
        set psksecret xxxx
        set ikelproposal 3des-sha1 3des-md5 ...
        set ikeldhgroup XXXX
        set ikelkeylifesecc 28800
        set ikelmode aggressive|main
        set ikelqpd enable|disable
        set ikelnattraversal enable|disable
        set ikelnatkeepalive 10
        set ike2proposal 3des-sha1 3des-md5
        set ike2dhgroup 5
        set ike2keylifetype seconds|kbyte|both
        set ike2keylifesecc 1800
        set ike2keylifekbs 5120
        set ike2keepalive enable|disable
        set replay enable|disable
        set pfs enable|disable
        set ike2autonego enable|disable
        set fcc-enforcement enable|disable
        set localid-type auto|fqdn|user-fqdn|keyid|addressasn1dn
        set authmethod psk|signature
        set inter-vdom enable|disable
        set certificate XXXX
    next
end
```

Syntax applicable for vpn console node

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

Syntax applicable for setting installation target on policy package

```
config firewall policy
  edit x

    ...regular policy command here...

    set _scope "<dev_name>"-"<vdom_name>"
  next
end
```

Syntax applicable for global policy

```
config global header policy

  ...regular policy command here...

end

config global footer policy

  ...regular policy command here...

end
```

Script history

The execution history of scripts run on specific devices can be viewed from a device's dashboard. The script log can be viewed in the Task Monitor. The script execution history table also allows for viewing the script history, and re-running the script.

To view the script execution history:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, select the device group, for example, *Managed Devices*. The list of devices display in the content pane and in the bottom tree menu.
3. In the bottom tree menu, select the device whose script history you want to view. The *System: Dashboard* for the device displays in the content pane.
4. In the *Configuration and Installation Status* widget, select *View History* in the *Script Status* field to open the *Script Execution History* pane.
5. To view the script history for a specific script, select the *Browse* icon in the far right column of the table to open the *Script History* dialog box.
6. To re-run a script, select the *Run script now* icon in the far right column of the table. The script is re-run. See [Run a script on page 119](#).
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 578](#).

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 133](#).

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 133](#).

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:

Script `show system interface port1`

Output

```
config system interface
  edit "port1"
    set vdom "root"
    set ip 172.20.120.148 255.255.255.0
    set allowaccess ping https ssh
    set type physical
  next
end
```

Variations Remove the interface name to see a list that includes all the interfaces on the FortiGate device including virtual interfaces such as VLANs.

Note 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:

Script	<code>show route static</code>
Output	<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>
Variations	none

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

Script	<pre> config global diag debug rating end </pre>
Output	<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>
Variations	<p>Output for this script will vary based on the state of the FortiGate device. The preceding output is for a FortiGate device that has never been authorized.</p> <p>For an authorized FortiGate device without a valid license, the output would be similar to:</p> <pre> Locale : english License : Unknown Expiration : N/A Hostname : guard.fortinet.net == Server List (Tue Oct 3 09:34:46 2006) == IP Weight Round-time TZ Packets Curr Lost Total Lost ** None ** </pre>

Setting FortiGate device information with CLI scripts gives you access to more settings and allows you more fine grained control than you may have in the *Device Manager*. Also CLI commands allow access to more advanced options that are not available in the FortiGate GUI. Scripts that set information require more lines.



Any scripts that you will be running on the global database must include the full CLI commands and not use short forms for the commands. Short form commands will not run on the global database.

Create a new account profile called `policy_admin` allowing read-only access to policy related areas:

Script	<pre> config global config system accprofile edit "policy_admin" set fwgrp read set loggrp read set sysgrp read next end end </pre>
Output	<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>
Variations	<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
    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 policies are miss

In analyzing this script:

- line 1 is the required `#!` to indicate this is a Tcl script
- line 2-8 is a loop that reads each policy's information and appends only the policy ID number to an array variable called `fw_policy`
- line 9 opens the CLI to the firewall policy section to prepare for the loop
- line 10 starts the for each loop that increments through all the firewall policy names stored in `fw_policy`
- line 11 checks each policy for an existing `diffservcode_forward 000011` entry - if its not found lines 12-15 are executed, otherwise they are skipped
- line 12 opens the policy determined by the loop counter
- line 13-14 enable `diffserv_forward`, and set it to `000011`
- line 15 saves this entry and prepares for the next one
- line 16 closes the if statement
- line 17 closes the for each loop
- line 18 saves all the updated firewall policy entries

Additional Tcl Scripts

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

Script:

```

#!
#Run on FortiOS v5.00
#This script will display FortiGate's CPU states,
#Memory states, and Up time
puts [exec "# This is an example Tcl script to get the system performance of the
FortiGate\n" "# " 15 ]
    set input [exec "get system status\n" "# " 15]
regexp {Version: *([^\ ]+) ([^\ ]+),build([0-9]+),[0-9]+} $input dummy status(Platform) status
    (Version) status(Build)
if {$status(Version) eq "v5.0"} {
    puts -nonewline [exec "config global\n" "# " 30]
    puts -nonewline [exec "get system performance status\n" "# " 30]
    puts -nonewline [exec "end\n" "# " 30]
} else {

```

```
    puts -nonewline [exec "get system performance\n" "#" 30]
}
```

Output:

```
----- Executing time: 2013-10-21 16:21:43 -----
Starting log (Run on device)
```

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

CPU states: 0% user 0% system 0% nice 90% idle
CPU0 states: 0% user 0% system 0% nice 90% idle
CPU1 states: 0% user 0% system 0% nice 90% idle
Memory states: 73% used
Average network usage: 0 kbps in 1 minute, 0 kbps in 10 minutes, 0 kbps in 30 minutes
Average sessions: 1 sessions in 1 minute, 2 sessions in 10 minutes, 2 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in
    last 10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 6 days, 1 hours, 34 minutes

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

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

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

```
#!/
#Run on FortiOS v5.00
#This script will configure common global, user group and ntp settings
#if you do not want to set a parameter, comment the
#corresponding set command
#if you want to reset a parameter to it's default
#value, set it an empty string
puts [exec "# This is an example Tcl script to configure global, user group and ntp setting
    of FortiGate\n" "#" 15 ]

# global
    set sys_global(admintimeout) ""
# user group
    set sys_user_group(authtimeout) 20
# ntp
    set sys_ntp(source-ip) "0.0.0.0"
    set sys_ntp(ntpsync) "enable"
#procedure to execute FortiGate command
proc fgt_cmd cmd {
puts -nonewline [exec "$cmd\n" "# " 30]
}
#config system global---begin
fgt_cmd "config global"
fgt_cmd "config system global"
```

```
foreach key [array names sys_global] {
if {$sys_global($key) ne ""} {
fgt_cmd "set $key $sys_global($key)"
} else {
fgt_cmd "unset $key"
}
}
fgt_cmd "end"
fgt_cmd "end"
#config system global---end

#config system user group---begin
fgt_cmd "config vdom"
fgt_cmd "edit root"
fgt_cmd "config user group"
fgt_cmd "edit groupname"
foreach key [array names sys_user_group] {
if {$sys_user_group($key) ne ""} {
fgt_cmd "set $key $sys_user_group($key)"
} else {
fgt_cmd "unset $key"
}
}
fgt_cmd "end"
fgt_cmd "end"
#config system user group---end

#config system ntp---begin
fgt_cmd "config global"
fgt_cmd "config system ntp"
foreach key [array names sys_ntp] {
if {$sys_ntp($key) ne ""} {
fgt_cmd "set $key $sys_ntp($key)"
} else {
fgt_cmd "unset $key"
}
}
fgt_cmd "end"
fgt_cmd "end"
#config system ntp---end
```

Output:

```
----- Executing time: 2013-10-22 09:12:57 -----
Starting log (Run on device)
```

```
FortiGate-VM64 # config global
FortiGate-VM64 (global) # config system global
FortiGate-VM64 (global) # unset admintimeout
FortiGate-VM64 (global) # end
FortiGate-VM64 (global) # end
FortiGate-VM64 # config vdom
FortiGate-VM64 (vdom) # edit root
current vf=root:0
FortiGate-VM64 (root) # config user group
FortiGate-VM64 (group) # edit groupname
FortiGate-VM64 (groupname) # set authtimeout 20
FortiGate-VM64 (groupname) # end
```

```

FortiGate-VM64 (root) # end
FortiGate-VM64 # config global
FortiGate-VM64 (global) # config system ntp
FortiGate-VM64 (ntp) # set ntpsync enable
FortiGate-VM64 (ntp) # set source-ip 0.0.0.0
FortiGate-VM64 (ntp) # end
FortiGate-VM64 (global) # end
FortiGate-VM64 #
----- The end of log -----

```

Example: Configure syslogd settings and filters.

Script:

```

#!/
#Run on FortiOS v5.00
#This script will configure log syslogd setting and
#filter
#key-value pairs for 'config log syslogd setting', no
#value means default value.
    set setting_list {{status enable} {csv enable}
{facility alert} {port} {server 1.1.1.2}}
#key-value pairs for 'config log syslogd filter', no
#value means default value.
puts [exec "# This is an example Tcl script to configure log syslogd setting and filter
    setting of FortiGate\n" "# " 15 ]
    set filter_list {{attack enable} {email enable} {severity} {traffic enable} {virus
        disable}
{web enable}}
#set the number of syslogd server, "", "2" or "3"
    set syslogd_no "2"
#procedure to execute FortiGate CLI command
proc fgt_cmd cmd {
puts -nonewline [exec "$cmd\n" "# "]
}
#procedure to set a series of key-value pairs
proc set_kv kv_list {
foreach kv $kv_list {
    set len [llength $kv]
if {$len == 0} {
continue
} elseif {$len == 1} {
fgt_cmd "unset [lindex $kv 0]"
} else {
fgt_cmd "set [lindex $kv 0] [lindex $kv 1]"
} } }
#configure log syslogd setting---begin
fgt_cmd "config global"
fgt_cmd "config log syslogd$syslogd_no setting"
    set_kv $setting_list
fgt_cmd "end"
#configure log syslogd setting---end
#configure log syslogd filter---begin
fgt_cmd "config log syslogd$syslogd_no filter"
    set_kv $filter_list
fgt_cmd "end"
#configure log syslogd filter---end

```

Output:

```
Starting log (Run on device)

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

FortiGate-VM64 (global) # config log syslogd2 filter
FortiGate-VM64 (filter) # set attack enable
FortiGate-VM64 (filter) # set email enable
FortiGate-VM64 (filter) # unset severity
FortiGate-VM64 (filter) # set traffic enable
FortiGate-VM64 (filter) # set virus disable
FortiGate-VM64 (filter) # set web enable
FortiGate-VM64 (filter) # end
FortiGate-VM64 (global) #

----- The end of log -----
```

Example: Configure the FortiGate device to communicate with a FortiAnalyzer unit:**Script:**

```
#!/
#This script will configure the FortiGate device to
#communicate with a FortiAnalyzer unit
#Enter the following key-value pairs for 'config
#system fortianalyzer'
    set status enable
    set enc-algorithm high
#localid will be set as the hostname automatically
#later
puts [exec "# This is an example Tcl script to configure the FortiGate to communicate with a
FortiAnalyzer\n" "# " 15 ]
    set server 1.1.1.1
#for fortianalyzer, fortianalyzer2 or
#fortianalyzer3, enter the corresponding value "",
#"2", "3"
    set faz_no ""
#keys used for 'config system fortianalyzer', if you
#do not want to change the value of a key, do not put
#it in the list
    set key_list {status enc-algorithm localid server }
##procedure to get system status from a FortiGate
proc get_sys_status aname {
upvar $aname a
set input [split [exec "get system status\n" "# " ] \n]
foreach line $input {
if {[regexp {[^:]+):(.*)} $line dummy key value]} continue
    set a([string trim $key]) [string trim $value]
}
}
```

```
#procedure to execute FortiGate command
proc fgt_cmd cmd {
puts -nonewline [exec "$cmd\n" "# "]
}
#set the localid as the FortiGate's hostname
get_sys_status sys_status
set localid $sys_status(Hostname)
#config system fortianalyzer---begin
fgt_cmd "config global"
fgt_cmd "config log fortianalyzer$faz_no setting"
foreach key $key_list {
if [info exists $key] {
    fgt_cmd "set $key [set $key]"
} else {
    fgt_cmd "unset $key"
}
}
fgt_cmd "end"
fgt_cmd "end"
#config system fortianalyzer---end
```

Output:

```
Starting log (Run on device)
FortiGate-VM64 # config global
FortiGate-VM64 (global) # config log fortianalyzer setting
FortiGate-VM64 (setting) # set status enable
FortiGate-VM64 (setting) # set enc-algorithm high
FortiGate-VM64 (setting) # set localid FortiGate-VM64
FortiGate-VM64 (setting) # set server 1.1.1.1
FortiGate-VM64 (setting) # end
FortiGate-VM64 (global) # end
FortiGate-VM64 #
----- The end of log -----
```

Example: Create custom IPS signatures and add them to a custom group.**Script:**

```
#!/
#Run on FortiOS v5.00
#This script will create custom ips signatures and
#change the settings for the custom ips signatures

puts [exec "# This is an example Tcl script to create custom ips signatures and change the
settings for the custom ips signatures on a FortiGate\n" "# " 15 ]
#Enter custom ips signatures, signature names are the
#names of array elements
    set custom_sig(c1) {"F-SBID(--protocol icmp;--icmp_type 10; )"}
    set custom_sig(c2) {"F-SBID(--protocol icmp;--icmp_type 0; )"}
#Enter custom ips settings
    set custom_rule(c1) {{(status enable) {action block} {log enable} {log-packet} {severity
high}}}
    set custom_rule(c2) {{(status enable) {action pass} {log} {log-packet disable} {severity
low}}}
#procedure to execute FortiGate command
proc fgt_cmd cmd {
puts -nonewline [exec "$cmd\n" "# " ]
```

```
}
#procedure to set a series of key-value pairs
proc set_kv kv_list {
foreach kv $kv_list {
set len [llength $kv]
if {$len == 0} {
continue
} elseif {$len == 1} {
fgt_cmd "unset [lindex $kv 0]"
} else {
fgt_cmd "set [lindex $kv 0] [lindex $kv 1]"
}
} }
#config ips custom---begin
fgt_cmd "config vdom"
fgt_cmd "edit root"
fgt_cmd "config ips custom"
foreach sig_name [array names custom_sig] {
fgt_cmd "edit $sig_name"
fgt_cmd "set signature $custom_sig($sig_name)"
fgt_cmd "next"
}
fgt_cmd "end"
#config ips custom settings---begin
foreach rule_name [array names custom_rule] {
fgt_cmd "config ips custom"
fgt_cmd "edit $rule_name"
set_kv $custom_rule($rule_name)
fgt_cmd "end"
}
fgt_cmd "end"
#config ips custom settings---end
```

Output:

```
Starting log (Run on device)
FortiGate-VM64 # config vdom
FortiGate-VM64 (vdom) # edit root
current vf=root:0
FortiGate-VM64 (root) # config ips custom
FortiGate-VM64 (custom) # edit c1
set signature "F-SBID(--protocol icmp;--icmp_type 10; )"
FortiGate-VM64 (c1) # set signature "F-SBID(--protocol icmp;--icmp_type 10; )"
FortiGate-VM64 (c1) # next
FortiGate-VM64 (custom) # edit c2
FortiGate-VM64 (c2) # set signature "F-SBID(--protocol icmp;--icmp_type 0; )"
FortiGate-VM64 (c2) # next
FortiGate-VM64 (custom) # end
FortiGate-VM64 (root) # config ips custom
FortiGate-VM64 (custom) # edit c1
FortiGate-VM64 (c1) # set status enable
FortiGate-VM64 (c1) # set action block
FortiGate-VM64 (c1) # set log enable
FortiGate-VM64 (c1) # unset log-packet
FortiGate-VM64 (c1) # set severity high
FortiGate-VM64 (c1) # end
FortiGate-VM64 (root) # config ips custom
FortiGate-VM64 (custom) # edit c2
```

```

FortiGate-VM64 (c2) # set status enable
FortiGate-VM64 (c2) # set action pass
FortiGate-VM64 (c2) # unset log
FortiGate-VM64 (c2) # set log-packet disable
FortiGate-VM64 (c2) # set severity low
FortiGate-VM64 (c2) # end
FortiGate-VM64 (root) # end
FortiGate-VM64 #
----- The end of log -----

```

Variations:

None.

Tcl file IO

You can write to and read from files using Tcl scripts. For security reasons there is only one directory on the FortiManager where scripts can access files. For this reason, there is no reason to include the directory in the file name you are accessing. For example “/var/temp/myfile” or “~/myfile” will cause an error, but “myfile” or “/myfile” is OK.

The Tcl commands that are supported for file IO are: `file`, `open`, `gets`, `read`, `tell`, `seek`, `eof`, `flush`, `close`, `fcopy`, `fconfigure`, and `fileevent`.

The Tcl file command only supports `delete` subcommand, and does not support the `-force` option.

There is 10MB of disk space allocated for Tcl scripts. An error will be reported if this size is exceeded.

These files will be reset when the following CLI commands are run: `exec format`, `exec reset partition`, or `exec reset all`. The files will not be reset when the firmware is updated unless otherwise specified.

To write to a file:

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

To read from a file:

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

Output	<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:

Syntax	<code>puts [exec_ondb "/adom/<adom_name>/pkg/<pkg_fullpath>" "embedded cli commands" "# "]</code>
Usage	<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:

Syntax	<pre>puts [exec_ondb "/adom/./pkg/<pkg_fullpath>" "embedded cli commands" "# "] or puts [exec_ondb "/pkg/<pkg_fullpath>" "embedded cli commands" "# "]</pre>
Usage	<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:

Syntax	<pre>puts [exec_ondb "/adom/<adom_name>/device/<dev_name>" "embedded cli commands" "# "]</pre>
Usage	<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:

Syntax	<pre>puts [exec_ondb "/adom/<adom_name>/device/." "embedded cli commands" "# "]</pre>
Usage	<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

The *SD-WAN* pane allows you to configure and manage SD-WAN networks on FortiGate devices that are managed by FortiManager. You can use the *SD-WAN* pane for the following modes of management:

- [SD-WAN per-device management on page 149](#)
- [SD-WAN central management on page 158](#)

The tree menu available on the *SD-WAN* pane depends on whether you have central management or per-device management enabled. When per-device management is enabled, the *SD-WAN* pane includes the following tree menu options:

SD-WAN	Create, view, edit, and delete SD-WAN configurations on a device.
Monitor	Monitor the SD-WAN network.

When central management is enabled, the *SD-WAN* pane includes the following tree menu options:

SD-WAN Template	Create, view, edit, and delete templates of SD-WAN configurations that you can assign to one or more devices.
Interface Members	Create, view, edit, and delete interface members. After interface members are created, you can select them in SD-WAN templates.
Health-Check Servers	Create, view, edit, and delete WAN detection servers. After health-check servers are created, you can select them in SD-WAN templates.
BGP Neighbors	Create, view, edit, and delete WAN BGP neighbors. After BGP neighbors are created, you can select them in SD-WAN templates.
Monitor	Monitor the SD-WAN network.

Before FortiManager 6.4.1, you could use SD-WAN interface members directly in a policy. After upgrading to FortiManager 6.4.1, SD-WAN interface members are automatically upgraded to zones. Upgraded SD-WAN members are named *upg-zone-`<interface-name>`*, and they replace interfaces in policies.

SD-WAN per-device management

When per-device management is enabled for SD-WAN, you can use the *SD-WAN* tree menu to configure SD-WAN on each FortiGate device.

The *SD-WAN* tree menu lets you:

- Create interface members and zones
- Create IPsec VPN tunnels by using a wizard
- Create performance SLA
- Create BGP Neighbors
- Create SD-WAN rules

Using SD-WAN per-device management consists of the following steps:

1. Enable SD-WAN per-device management. See [Enabling SD-WAN per-device management on page 150](#).
2. Configure SD-WAN on devices. See [SD-WAN on page 150](#).

3. Install device settings using the *Install Wizard*. See [Using the Install Wizard to install device settings only on page 76](#).
4. Monitor SD-WAN networks. See [Monitor SD-WAN on page 175](#).

Enabling SD-WAN per-device management

You can enable per-device management for SD-WAN per ADOM. When enabled, the *SD-WAN* tab shows the following items in the tree menu:

- *SD-WAN*
- *Monitor*

To enable SD-WAN per-device management:

1. Go to *System Settings > All ADOMs*.
2. Double-click the ADOM to open it for editing.
The *Edit ADOM* window opens.
3. Beside *Central Management*, clear the *SD-WAN* checkbox, and click *OK*.
SD-WAN central management is disabled for the ADOM, and SD-WAN per-device management is enabled for the ADOM.
4. Go to *Device Manager > SD-WAN*, and notice that *Per-device Management* is displayed in the top-right corner.

SD-WAN

In per-device management, you can configure SD-WAN directly on each device.

If you want to add BGP Neighbors to the configuration, you must create the BGP Neighbors first. See [BGP Neighbors \(per-device management\) on page 157](#).

To configure SD-WAN on a device:

1. Ensure that you are in the correct ADOM and that SD-WAN per-device management is enabled for the ADOM.
2. Go to *Device Manager > SD-WAN > SD-WAN*.
3. Click *Create New* in the content pane toolbar.
The *Create New SD-WAN* pane opens.

Per-device Management

Create New SD-WAN

Device:

SD-WAN Status: ☒ ON

Interface Members

ID	Interface Member	Status	Gateway
<input type="checkbox"/> virtual-wan-link			
<input type="checkbox"/> 2	Member 2	Enable	0.0.0.0
<input type="checkbox"/> test			
<input type="checkbox"/> 1	port7	Enable	0.0.0.0
<input type="checkbox"/> 3	Member 3	Enable	0.0.0.0

Create VPN

Performance SLA

Name	Health-Check Server	Detect Protocol	Failure Threshold	Recovery Threshold

OK Cancel

4. Enter the following information, and click *OK* to :

Device	Select the device to configure.
SD-WAN Status	Select <i>On</i> or <i>Off</i> .
Interface Members	Zones and interface members can be added, edited, and removed. See Zones and interface members (per-device management) on page 152.
Create VPN	See IPsec VPN Wizard (per-device management) on page 153.
Performance SLA	See Performance SLA (per-device management) on page 155.
Neighbor	See BGP Neighbors (per-device management) on page 157.
SD-WAN Rules	See SD-WAN rules (per-device management) on page 156.
Advanced Options	Configure the following advanced options:
fail-detect	Enable/disable fail detection features for this interface.
neighbor-hold-boot-time	Specify the interval.
neighbor-hold-down	Enable/disable neighbor hold down for this interface.
neighbor-hold-down-time	Specify the interval.

To edit an SD-WAN configuration:

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

3. Select the 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 configuration as required, and click *OK* to apply your changes.

To delete an SD-WAN configuration:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN > SD-WAN*.
3. Select the device 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 SD-WAN configuration.

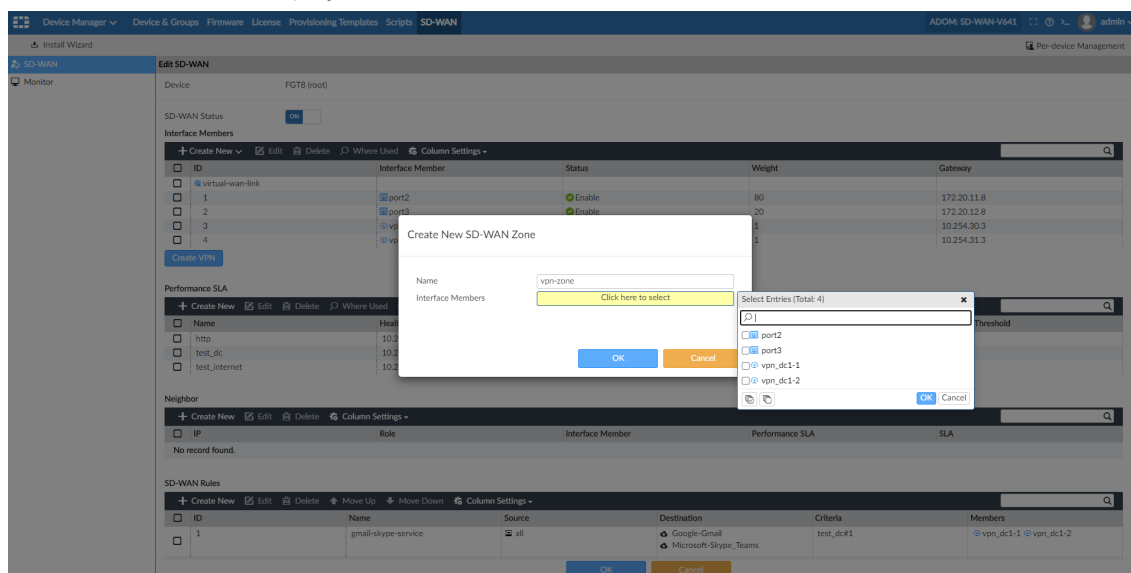
Zones and interface members (per-device management)

When SD-WAN per-device management is enabled, you can create SD-WAN zones and interface members. You can select SD-WAN zones as source and destination interfaces in firewall policies. You cannot select interface members of SD-WAN zones in firewall policies.

The default SD-WAN zone is named `virtual-wan-link`.

To create an SD-WAN zone:

1. Ensure that you are in the correct ADOM and that SD-WAN per-device management is enabled for the ADOM.
2. Go to *Device Manager > SD-WAN > SD-WAN*.
The list of devices with SD-WAN configurations is displayed.
3. Double-click a device to open its configuration for editing, or click *Create New* to create a new SD-WAN configuration.
The SD-WAN settings are displayed.
4. In the *Interface Members* section, click *Create New > SD-WAN Zone*.
The *Create New SD-WAN Zone* dialog box is displayed.
5. In the *Name* box, type a name for the zone.
6. Click the *Interface Members* box.
The list of interfaces is displayed.



7. Select the interfaces to be members of the zone, and click **OK**.
8. Click **OK** to finish creating the zone.

To create an SD-WAN interface member:

1. Ensure that you are in the correct ADOM and that SD-WAN per-device management is enabled for the ADOM.
2. Go to *Device Manager > SD-WAN > SD-WAN*.
The list of devices with SD-WAN configurations is displayed.
3. Double-click a device to open its configuration for editing, or click *Create New*.
The SD-WAN settings are displayed.
4. In the *Interface Members* section, click *Create New > SD-WAN Member*.
The *Create New SD-WAN Interface Member* dialog box is displayed.

5. Click the *Interface Members* box, and select an interface.
6. In the *SD-WAN Zone* box, select a zone.
7. Click **OK**.
The interface is added to the zone.

IPsec VPN Wizard (per-device management)

When per-device management is enabled, the SD-WAN settings pane includes access to an IPsec VPN Wizard. You can use the wizard to create IPsec VPN tunnels and automatically generate interface members for the tunnel.

To configure the IPsec VPN in SD-WAN:

1. Ensure that you are in the correct ADOM and that SD-WAN per-device management is enabled for the ADOM.
2. Go to *Device Manager > SD-WAN > SD-WAN*.
3. Select any device or VDOM and click *Edit*. If no device is available, click *Create New*.
The *Edit SD-WAN* pane or *Create New SD-WAN* is displayed.

4. Under *Interface Members*, click *Create VPN*.

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

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

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

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

Device: FGVM020000155864 (root)

SD-WAN Status: ☒ ON

Interface Members

+ Create New Edit Delete Move Up Move Down

#	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	0.0.0.0		

Create VPN

Performance SLA

+ Create New Edit Delete

#	Name	Detect Server	Detect Protocol	Failure Threshold	Recovery Threshold

SD-WAN Rules

+ Create New Edit Delete Move Up Move Down

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

Advanced Options >

OK Cancel

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

Performance SLA (per-device management)

To create a new performance SLA:

1. Ensure that you are in the correct ADOM and that SD-WAN per-device management is enabled for the ADOM.
2. Go to *Device Manager* > *SD-WAN* > *SD-WAN*.
The list of devices with SD-WAN configurations is displayed.
3. Double-click a device to open its configuration for editing, or click *Create New* to create a new SD-WAN configuration.
The SD-WAN settings are displayed.
4. In the Performance SLA section, click *Create New*.
The *Create Performance SLA* dialog-box opens

Create New Performance SLA

Name

IP Version

Detect Protocol

Health-Check Server + 🗑️

Participants Specify

Enable Probe Packets ☒

SLA

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

OK Cancel

- Configure the options, and click **OK** to create the performance SLA.
For more information about the options, see [Performance SLA \(central management\)](#) on page 166.

SD-WAN rules (per-device management)

Configure SD-WAN rules for WAN links by specifying the required network parameters.

To create a new SD-WAN rule:

- Ensure that you are in the correct ADOM and that SD-WAN per-device management is enabled for the ADOM.
- Go to *Device Manager* > *SD-WAN* > *SD-WAN*.
The list of devices with SD-WAN configurations is displayed.
- Double-click a device to open its configuration for editing, or click *Create New* to create a new SD-WAN configuration.
The SD-WAN settings are displayed.
- In the *SD-WAN Rules* section, click *Create New*.
The *Create New SD-WAN Rule* dialog-box opens.

Create New SD-WAN Rule

Name

IP Version

Source

Source Address

Users

User Groups

Destination

Address Internet Service

Address

Protocol

Type of Service Bit Mask

Outgoing Interfaces

Strategy

Interface Preference

5. Configure the options, and click **OK** to create the new SD-WAN rule.
For more information about the options, see [SD-WAN rules \(central management\)](#) on page 168.

BGP Neighbors (per-device management)

When per-device management is enabled for SD-WAN, you can create SD-WAN rules that include Border Gateway Protocol (BGP) neighbors. You must create BGP neighbors for FortiGate devices before you can add them to the SD-WAN network.

To create BGP Neighbors for FortiGate devices:

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.

To configure BGP Neighbor for SD-WAN (per-device management):

1. Ensure that you are in the correct ADOM and that SD-WAN per-device management is enabled for the ADOM.
2. Go to *Device Manager* > SD-WAN > SD-WAN.
3. Click *Create New*.
The *Create New SD-WAN* pane opens.
4. In the *Device* list, select the FortiGate device to which you added BGP Neighbors.
The BGP Neighbors added to the FortiGate (Device Manager) automatically appear under *Neighbor*.

The screenshot shows the 'Create New SD-WAN' configuration window in FortiManager. The interface includes a top navigation bar with tabs like 'Device Manager', 'Device & Groups', 'Firmware', 'License', 'Provisioning Templates', 'Scripts', and 'SD-WAN'. The main content area is divided into several sections:

- Device:** A dropdown menu showing 'FGVM00TM19002130 (root)'.
- Detect Servers:** A table with columns: #, Name, Detect Server, Detect Protocol, Failure Threshold, and Recovery Threshold. It lists five default servers: Default_AWS, Default_FortiGuard, Default_Gmail, Default_Google Search, and Default_Office_365.
- Neighbor:** A table with columns: #, IP, Role, Member, Health Check, and SLA. It lists two neighbors: 10.21.2.201 (primary) and 10.21.2.202 (standalone).
- SD-WAN Rules:** A table with columns: #, Name, Source, Destination, Criteria, and Members. It lists one rule: 'sd-wan' with Source 'ALL' and Destination 'ALL'.
- Advanced Options:** A section with various configuration options:
 - fail-alert-interfaces:** A dropdown menu showing 'port1'.
 - fail-detect:** A dropdown menu showing 'disable'.
 - neighbor-hold-boot-time:** A text input field showing '500'.
 - neighbor-hold-down:** A dropdown menu showing 'disable'.
 - neighbor-hold-down-time:** A text input field showing '0'.

At the bottom of the window, there are 'OK' and 'Cancel' buttons.

5. Toggle the SD-WAN Status to *ON*.
6. Configure the following *Advanced Options*:

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

7. Click *OK*.

SD-WAN central management

When central management is enabled for SD-WAN, you can configure SD-WAN templates and assign the templates to FortiGate devices. 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 159](#).
2. Specify the health-check servers that will monitor the network parameters. See [Health-Check Servers on page 171](#).

3. (Optional) Specify BGP Neighbors.
4. Create an SD-WAN template that includes the following:
 - a. Add zones and 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. BGP Neighbors - create BGP neighbors.
 - d. SD-WAN Rules - create rules and configure advanced options on network traffic management.
 See [SD-WAN templates on page 162](#).
5. Assign the SD-WAN templates to FortiGate devices. See [Assign SD-WAN templates to devices on page 174](#).
6. Install device settings using the *Install Wizard*. See [Using the Install Wizard to install device settings only on page 76](#).
7. Go to *SD-WAN > Monitor* to monitor the FortiGate devices. See [Monitor SD-WAN on page 175](#).



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 SD-WAN central management

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

- SD-WAN Templates
- Interface Members
- Health-Check Servers
- BGP Neighbors
- Monitor

To enable central SD-WAN management:

1. Go to *System Settings > All ADOMs*.
2. Double-click the ADOM to open it for editing.
The *Edit ADOM* window opens. (See [Editing an ADOM on page 562](#).)
3. Beside *Central Management*, select the *SD-WAN* checkbox, and click *OK*.
SD-WAN per-device management is disabled for the ADOM, and SD-WAN central management is enabled for the ADOM.
4. Go to *Device Manager > SD-WAN*, and notice that *Central Management* is displayed in the top-right corner.

Interface members

When SD-WAN central management is enabled, you can create new WAN interface members, and then select them in SD-WAN templates.

To create a new interface member:

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

Create New WAN Interface

Name	<input style="width: 95%;" type="text"/>
Description	<div style="border: 1px solid #ccc; height: 40px; width: 95%;"></div> <div style="text-align: right; font-size: 0.8em;">0/256</div>
Normalized Interface	<div style="border: 1px solid #ccc; padding: 2px;">None ▼</div>
Gateway	<div style="border: 1px solid #ccc; padding: 2px;">0.0.0.0</div>
Weight	<div style="border: 1px solid #ccc; padding: 2px;">1</div>
Cost	<div style="border: 1px solid #ccc; padding: 2px;">0</div>
Volume Ratio	<div style="border: 1px solid #ccc; padding: 2px;">1</div>
Per-Device Mapping	<div style="border: 1px solid #ccc; padding: 2px;"><input type="checkbox"/> OFF</div>
Advanced Options >	

OK

Cancel

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

Name	Enter the name of the WAN detect server.
Description	Enter a description of the server.
Normalized Interface	Specify the normalized interface for the WAN link.
Gateway	The default gateway for this interface. Usually the default gateway of the Internet service provider that this interface is connected to.
Weight	Weight of this interface for weighted load balancing (0 - 255). More traffic is directed to interfaces with higher weights.
Volume Ratio	Measured volume ratio (this value / sum of all values = percentage of link volume, 0 - 255).
Per-Device Mapping	Enable per-device mapping. See Interface members per-device mapping on page 161 .
Advanced Options	
gateway6	IPv6 gateway address.

ingress-spillover-threshold	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.
priority	Priority of the interface (0 - 4294967295). Used for SD-WAN rules or priority rules.
source	Source IPv4 address.
source6	Source IPv6 address.
spillover-threshold	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.
status	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.

Interface members per-device mapping

To add WAN interface per-device mapping:

1. Ensure that you are in the correct ADOM and that SD-WAN central management is enabled for the 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*.

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

Per-Device Mapping

Mapped Device: Click to select

Gateway: 0.0.0.0

Weight: 1

Cost: 0

Volume Ratio: 1

Advanced Options >

OK Cancel

- Select a *Mapped Device* from the drop-down list.
- Enter the *Gateway* IP address, *Weight*, *Cost*, *Volume Ratio*, and *Advanced Options*.
- Click *OK*.

To edit WAN interface per-device mapping:

- Ensure that you are in the correct ADOM and that SD-WAN central management is enabled for the ADOM.
- Go to *Device Manager > SD-WAN > Interface Members*.
- Click *Create New* in the content pane toolbar, or right-click and select *Create New*. The *Create New WAN Interface* page opens.
- Select a per device mapping then click *Edit* in the per-device mapping toolbar. The *Edit Interface Member* dialog-box opens.
- Edit the settings as required, then click *OK*.

To delete WAN interface per-device mappings:

- Ensure that you are in the correct ADOM and that SD-WAN central management is enabled for the ADOM.
- Go to *Device Manager > SD-WAN > Interface Members*.
- Click *Create New* in the content pane toolbar, or right-click and select *Create New*. The *Create New WAN Interface* page opens.
- Select one or more per device mapping, then click *Delete* in the per-device mapping toolbar.
- Click *OK* in the confirmation dialog box to delete the mapping or mappings.

SD-WAN templates

When SD-WAN central management is enabled, you can create SD-WAN templates with the required network parameters, and then apply the templates to multiple devices.

Before creating SD-WAN templates:

- Create the interface members. See [Interface members on page 159](#).
- Create health-check servers. See [Health-Check Servers on page 171](#).
- Create BGP Neighbors. See [BGP Neighbors on page 173](#).

To create a new SD-WAN template:

1. Ensure that you are in the correct ADOM and that SD-WAN central management is enabled for the ADOM.
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

SD-WAN Status ☒ ON ☐ OFF

Interface Members

+ Create New ☐ Edit ☐ Delete ☐ Move Up ☐ Move Down

#	ID	Port
---	----	------

Performance SLA

+ Create New ☐ Edit ☐ Delete ☐

#	Name	Detect Server	Detect Protocol	Failure Threshold	Recovery Threshold
---	------	---------------	-----------------	-------------------	--------------------

Neighbor

+ Create New ☐ Edit ☐ Delete ☐

#	Neighbor	Member	Health Check	SLA
---	----------	--------	--------------	-----

SD-WAN Rules

+ Create New ☐ Edit ☐ Delete ☐ Move Up ☐ Move Down

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

Advanced Options >

OK Cancel

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

Name	Enter the name of the template.
Description	Enter a description of the template.
SD-WAN Status	Select <i>On</i> or <i>Off</i> .
Interface Members	Interface members can be added, edited, and removed. An interface member must be created before it can be added to a template, see Interface members on page 159 .
Performance SLA	See Performance SLA (central management) on page 166 .
Neighbor	See BGP Neighbors on page 173 .
SD-WAN Rules	See SD-WAN rules (central management) on page 168 .
Advanced Options	Configure the following advanced options:
fail-detect	Enable/disable fail detection features for this interface.

neighbor-hold-boot-time	Specify the interval.
neighbor-hold-down	Enable/disable neighbor hold down for this interface.
neighbor-hold-down-time	Specify the interval.

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

Name

Device

Click to select ▼

Description

0/255

OK

Cancel

4. Configure the following settings and click *OK*:
 - Name - specify a name for the SD-WAN template.
 - Device - select the FortiGate device from where to select the SD-WAN template.
 - Description - optionally provide a description.

The SD-WAN template is imported 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.

Zones and interface members (central management)

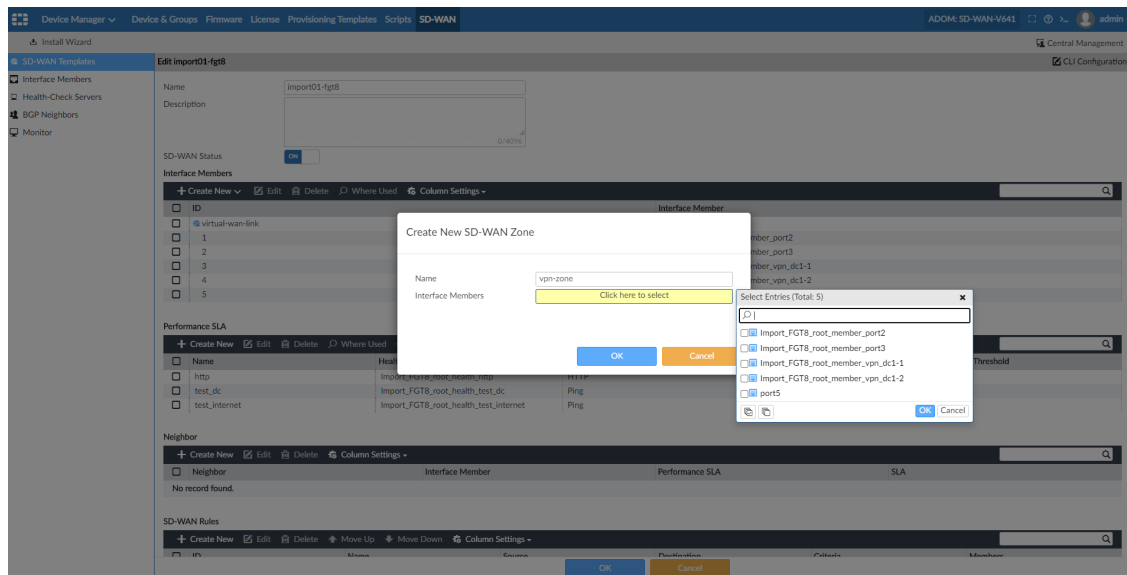
When central management is enabled, you can create SD-WAN zones and interface members in SD-WAN templates. You can select SD-WAN zones as source and destination interfaces in firewall policies. You cannot select interface members of SD-WAN zones in firewall policies.

A normalized interface is automatically created when you create an SD-WAN zone.

The default SD-WAN zone is named `virtual-wan-link`.

To create an SD-WAN zone:

1. Ensure that you are in the correct ADOM and that SD-WAN central management is enabled for the ADOM.
2. Go to *Device Manager* > *SD-WAN* > *SD-WAN Templates*.
The templates are displayed in the content screen.
3. Double-click a template to open it for editing, or click *Create New*.
The SD-WAN template settings are displayed.
4. In the *Interface Members* section, click *Create New* > *SD-WAN Zone*.
The *Create New SD-WAN Zone* dialog box is displayed.
5. In the *Name* box, type a name for the zone.
6. Click the *Interface Members* box.
The list of interfaces is displayed.

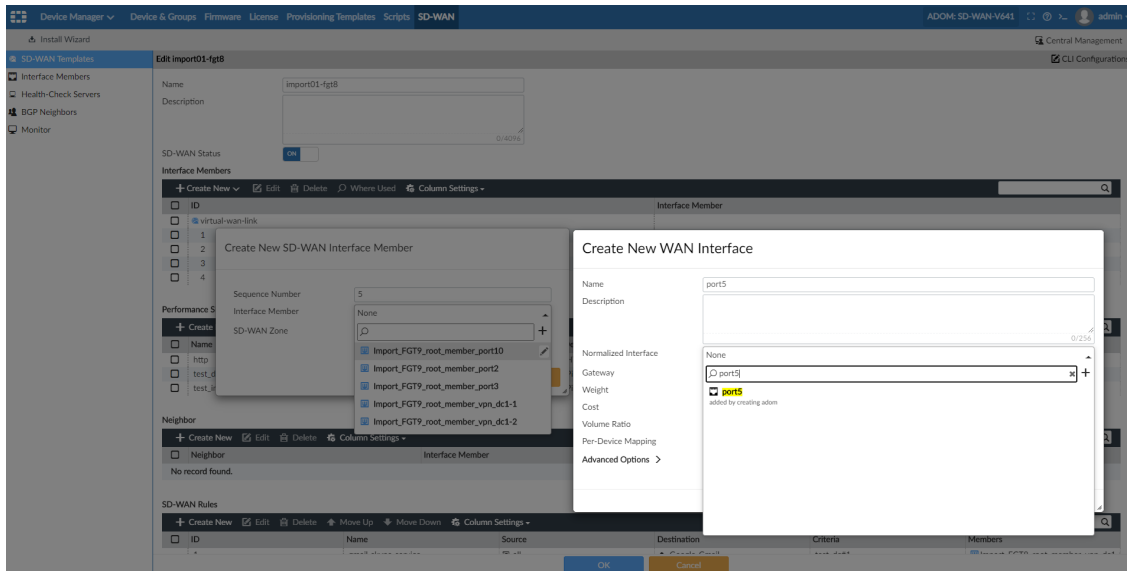


7. Select the interfaces to be members of the zone, and click *OK*.
8. Click *OK* to finish creating the zone.

To create an SD-WAN interface member:

1. Ensure that you are in the correct ADOM and that SD-WAN central management is enabled for the ADOM.
2. Go to *Device Manager* > *SD-WAN* > *SD-WAN Templates*.
3. Double-click a template to open it for editing, or click *Create New*.
The SD-WAN template settings are displayed.

4. Create a new SD-WAN interface:
 - a. In the *Interface Member* list, click the + icon.
The *Create New WAN Interface* dialog box is displayed.



- b. In the *Name* box, type a name for the interface.
 - c. In the *Normalized Interface*, select an interface.
 - d. Complete the remaining options, and click **OK**.
The SD-WAN interface is created.
5. In the *SD-WAN Zone* box, select the zone.
6. Click **OK**.
The interface is added to the zone.

Performance SLA (central management)

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. If using ADOMs, ensure that you are in the correct ADOM.
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:

Name	Enter the name of the performance SLA.
Detect Protocol	Select the detection method for the profile check: <ul style="list-style-type: none"> • Ping • TCP ECHO • UDP ECHO • HTTP • TWAMP
Detect Server	Enter the IP address of the WAN interface that you want to monitor.
Member	Select available interface members. The interfaces must already be added to the template.
SLA	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.
Link Status	
Interval	Status check interval, or the time between attempting to connect to the server, in seconds (1 - 3600, default = 1).
Failure Before Inactive	Specify the number of failures before the link becomes inactive (1 - 10, default = 5).
Restore Link After	Specify the number of successful responses received before server is considered recovered (1 - 10, default = 5).
Action When Inactive	Specify what happens with the WAN link becomes inactive.

Update Static Route	Select to update the static route when the WAN link becomes inactive.
Cascade Interfaces	Select to cascade interfaces when the WAN link becomes inactive.
Advanced Options	
addr-mode	Address mode (IPv4 or IPv6).
http-get	URL used to communicate with the server if the protocol is HTTP.
http-match	Response string expected from the server if the protocol is HTTP.
interval	Status check interval, or the time between attempting to connect to the server, in seconds (1 - 3600, default = 5).
packet-size	Packet size of a TWAMP test session (64 - 1024).
threshold-alert-jitter	Alert threshold for jitter (ms, default = 0), range [0-4294967295].
threshold-alert-latency	Alert threshold for latency, in milliseconds (0 - 4294967295, default = 0).
threshold-alert-packetloss	Alert threshold for packet loss, in percent (0 - 100, default = 0).
threshold-warning-jitter	Warning threshold for jitter, in milliseconds (0 - 4294967295, default = 0).
threshold-warning-latency	Warning threshold for latency, in milliseconds (0 - 4294967295, default = 0).
threshold-warning-packetloss	Warning threshold for packet loss, in percent (0 - 100, default = 0).

SD-WAN rules (central management)

Configure SD-WAN rules for WAN links by specifying the required network parameters. The SD-WAN rules are applied to the FortiGate device when the SD-WAN template is applied.

To create a new SD-WAN rule:

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

Name	Enter the name of the rule.
Source	
Address	Add one or more address from the drop-down.
Users	Add one or more users from the drop-down.
User Groups	Add one or more groups from the drop-down.
Destination	
Address	Select an address or addresses from the drop-down list. This option is only available when <i>Destination</i> is <i>Address</i> .
Internet Service	Select a service or services from the drop-down list. This option is only available when <i>Destination</i> is <i>Internet Service</i> .
Internet Service Group	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> .
Custom Internet Service	Select a service or services from the drop-down list. This option is only available when <i>Destination</i> is <i>Internet Service</i> .
Custom Internet Service Group	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> .
Application	Select an application or applications from the drop-down list. This option is only available when <i>Destination</i> is <i>Internet Service</i> .

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

packet-loss-weight	Coefficient of packet-loss in the formula of custom-profile-1, range[0-10000000].
route-tag	IPv4 route map route-tag, range [0-4294967295].
src-negate	Enable/disable negation of source address match.
src6	Source IPv6 address name.
status	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 SD-WAN central management is enabled for the ADOM.
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:

Name	Enter the name of the WAN detect server.
Description	Enter a description of the server.
Detect Server	Enter the IP address of the WAN interface that you want to monitor. Click the plus icon to add more interfaces.
Per-Device Mapping	Enable per-device mapping. See Health-check servers per-device mapping on page 172 .

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:

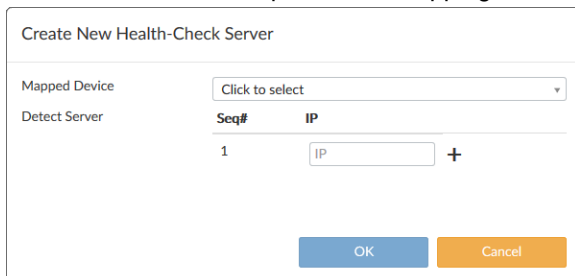
1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN > Health-Check Servers*.
3. Select the server or servers from the list and click *Delete* in the toolbar, or right-click the server then select *Delete*.
4. Click *OK* in the confirmation dialog box to delete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

Health-check 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.



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.

BGP Neighbors

When central management is enabled for SD-WAN, you can create SD-WAN rules that include Border Gateway Protocol (BGP) neighbors. You must create BGP neighbors for FortiGate devices before you can add them to the SD-WAN templates.

To configure BGP Neighbors for SD-WAN (central management):

1. Go to *Device Manager > SD-WAN > BGP Neighbors*.
2. Click *Create New*.
3. The *Create New WAN BGP Neighbor* pane opens:

4. Configure the following:

Name	Enter the name of the WAN BGP neighbor.
Description	Enter a description of the template.
Neighbor IP	Enter an IP for the neighbor.
Role	Select <i>standalone</i> , <i>primary</i> , or <i>secondary</i> .
Per-Device Mapping	Switch per-device mapping to ON and click <i>Create New</i> . Configure the following:
Mapped Device	Enable/disable fail detection features for this interface.
Description	Specify a description.
IP	Specify the IP.
Role	Select <i>standalone</i> , <i>primary</i> , or <i>secondary</i> .

5. Click *OK*.

Assign SD-WAN templates to devices

When SD-WAN central management is enabled, you can assign SD-WAN templates to FortiGate devices. The network parameters specified in the SD-WAN template are used to measure the performance of the WAN link on the FortiGate device.

To assign an SD-WAN template to a FortiGate device:

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 Templates*.
The SD-WAN templates are displayed in the content pane.
3. Select a template, and click *Assign to Device*.
The *Assign to Device* page opens.

4. In the *Available Entries* list, select a *FortiGate*, and click > to move the FortiGate to the *Selected Entries* list.
5. Click *OK*.

To edit an assigned device:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN > SD-WAN Templates*.
3. Select the template with the assigned device, and click *Assign to Device* in the toolbar, or right-click the device and select *Assign to Device*.
The *Assign to Device* page opens.
4. Edit the assigned devices, and click *OK* to apply your changes.

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>)

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

Device	Name of the device.
SD-WAN	Interface members.
Internet Services	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 > Destination type > Internet Service</i> in FortiGate.

Applications	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 > Destination type > Internet Service</i> in FortiGate.
Upload	Volume of data transmitted up stream
Download	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 <i>Every 5 Minutes</i> to <i>Every 30 Minutes</i> . Alternatively, you can select <i>Manual Refresh</i> 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.

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:

Device Name	The name of the FortiGate device that is managing the FortiExtender.
--------------------	--

Serial Number	The serial number of the FortiExtender.
Priority	The FortiExtender priority, either <i>Primary</i> or <i>Secondary</i> .
Model	The FortiExtender model.
Management Status	The FortiExtender management status, either <i>Authorized</i> or <i>Deauthorized</i> .
Status	The FortiExtender status, either <i>Up</i> or <i>Down</i> .
Network	The FortiExtender network status and carrier name.
Current Usage	The current data usage.
Last Month Usage	The data usage for the last month.
Version	The FortiExtender firmware version.
IP	The FortiExtender IP address.

The right-click menu and toolbar options include:

Refresh	Select a FortiExtender in the list, right-click, and select <i>Refresh</i> in the menu to refresh the information displayed.
Edit	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.
Upgrade	Select a FortiExtender in the list, right-click, and select <i>Upgrade</i> in the menu to upgrade the FortiExtender firmware.
Authorize	Select a FortiExtender in the list, right-click, and select <i>Authorize</i> in the menu to authorize the unit for management.
Deauthorize	Select a FortiExtender in the list, right-click, and select <i>Deauthorize</i> in the menu to deauthorize the unit for management.
Restart	Select a FortiExtender in the list, right-click, and select <i>Restart</i> in the menu to restart the unit.
Set Primary	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.
Status	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. The <i>Status</i> pane also shows LTE connection status and GSM signal details.

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:

Modem Settings	Configure the dial mode, redial limit, and quota limit.
-----------------------	---

PPP Authentication	Configure the user name, password, and authentication protocol.
General	Configure the usage cycle reset day, AT dial script, modem password, and enable/disable allowing network initiated updates to modem setting.
GSM / LTE	Configure the access point name (APN), SIM PIN, and LTE multiple mode.
CDMA	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 179](#).
 6. Ensure that the VM is authorized for central management by FortiManager. See [Adding devices on page 37](#).
 7. Authorize the metered VMs in FortiManager. See [Authorizing metered VMs on page 179](#).



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 37](#).

To authorize metered FortiOS VMs:

1. Ensure that the VM is authorized for central management by FortiManager. See [Adding devices on page 37](#).
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*:

Trial	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.
Regular	Regular license. Points used based on the service level and volume of traffic going to FortiGuard.

6. Select the *Services*:

Firewall	Firewall only. This option cannot be deselected.
IPS	IPS services.
Web Filter	Web filtering services.
AntiVirus	Antivirus services.
App Control	Application control services.
Full UTM	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 44](#).

To authorize metered FortiWeb VMs:

1. Ensure that the FortiWeb VM is authorized for central management by FortiManager. See [Adding devices on page 37](#).
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 596](#) for more information.
2. Under *Advanced Settings*, select *Chassis Management*.
3. Set the *Chassis Update Interval*, from 4 to 1440 minutes.
4. Click *Apply*.

To add a chassis:

1. Go to *Device Manager > Device & Groups*,
2. Right-click in the tree menu and select *Chassis > Add*. The *Create Chassis* window opens.
3. Complete the following fields, then click *OK*:

Name	Type a unique name for the chassis.
Description	Optionally, type any comments or notes about this chassis.
Chassis Type	Select the chassis type: Chassis 5050, 5060, 5140 or 5140B.
IP Address	Type the IP address of the Shelf Manager running on the chassis.
Authentication Type	Select Anonymous, MD5, or Password from the dropdown list.
Admin User	Type the administrator user name.
Password	Type the administrator password.
Chassis Slot Assignment	You cannot assign FortiGate-5000 series blades to the slot until after the chassis has been added.

To edit a chassis and assign FortiGate 5000 series blade to the slots:

1. Go to *Device Manager > Device & Groups*.
2. Right-click the chassis, and select *Edit*.
3. Modify the fields, except *Chassis Type*.

4. For *Chassis Slot Assignment*, from the dropdown list of a slot, select a FortiGate 5000 series blade to assign it to the slot. You can select a FortiGate, FortiCarrier, or FortiSwitch unit.



You can only assign FortiSwitch units to slot 1 and 2.

5. Click *OK*.

Viewing chassis dashboard

You can select a chassis from the chassis list in the content pane, and view the status of the FortiGate blades in the slots, power entry module (PEM), fan tray (FortiGate-5140 only), Shelf Manager, and shelf alarm panel (SAP).

Viewing the status of the FortiGate blades

In the *Device Manager* tab, select the Blades under the chassis whose blade information you would like to view.

The following is displayed:

Refresh	Select to update the current page. If there are no entries, Refresh is not displayed.
Slot #	The slot number in the chassis. <ul style="list-style-type: none"> • The FortiGate 5050 chassis contains five slots numbered 1 to 5. • The FortiGate 5060 chassis contains six slots numbered 1 to 6. • The FortiGate 5140 and 5140B chassis contains fourteen slots numbered 1 to 14.
Extension Card	If there is an extension card installed in the blade, this column displays an arrow you can select to expand the display. The expanded display shows details about the extension card as well as the blade.
Slot Info	Indicates whether the slot contains a node card (for example, a FortiGate 5001SX blade) or a switch card (for example, a FortiSwitch 5003 blade) or is empty.
State	Indicates whether the card in the slot is installed or running, or if the slot is empty.
Temperature Sensors	Indicates if the temperature sensors for the blade in each slot are detecting a temperature within an acceptable range. <ul style="list-style-type: none"> • <i>OK</i>: All monitored temperatures are within acceptable ranges. • <i>Critical</i>: A monitored temperature is too high (usually about 75°C or higher) or too low (below 10°C).
Current Sensors	Indicates if the current sensors for the blade in each slot are detecting a current within an acceptable range. <ul style="list-style-type: none"> • <i>OK</i>: All monitored currents are within acceptable ranges. • <i>Critical</i>: A monitored current is too high or too low.
Voltage Sensors	Indicates if the voltage sensors for the blade in each slot are detecting a voltage within an acceptable range.

	<ul style="list-style-type: none"> • <i>OK</i>: All monitored voltages are within acceptable ranges. • <i>Critical</i>: A monitored voltage is too high or too low.
Power Allocated	Indicates the amount of power allocated to each blade in the slot.
Action	Select <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> .
Edit	Select to view the detailed information on the voltage and temperature of a slot, including sensors, status, and state. You can also edit some voltage and temperature values.
Update	Select to update the slot.

To edit voltage and temperature values:

1. Go to *[chassis name] > Blades* and, in the content pane, select the *Edit* icon of a slot.
The detailed information on the voltage and temperature of the slot including sensors, status, and state is displayed.
2. Select the *Edit* icon of a voltage or temperature sensor.
3. For a voltage sensor, you can modify the *Upper Non-critical*, *Upper Critical*, *Lower Non-critical*, and *Lower Critical* values.
4. For a temperature sensor, you can modify the *Upper Non-critical* and *Upper Critical* values.
5. Select *OK*.

Viewing the status of the power entry modules

You can view the status of the PEMs by going to *[chassis name] > PEM*. The FortiGate 5140 chassis displays more PEM information than the FortiGate 5050.

The following is displayed:

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

Power Available	Available power for each pair of fuses.
Power Allocated	Power allocated to each pair of fuses.
Used By	The slot that uses the power.

Viewing fan tray status (FG-5140 and FG-5140B chassis only)

Go to *[chassis name] > Fan Tray* to view the chassis fan tray status.

The following is displayed:

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

Viewing shelf manager status

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

The following is displayed:

Refresh	Select to update the current page.
Shelf Manager	The order numbers of the shelf managers in the chassis.
Model	The shelf manager model.
State	The operation status of the shelf manager.
Temperature	The temperature of the shelf manager.
-48V Bus A	Status of the -48V Bus A: present or absent.
-48V Bus B	Status of the -48V Bus B: present or absent.
Power Allocated	Power allocated to each shelf manager.

Voltage Sensors	Lists the voltage sensors for the shelf manager.
State	Indicates if the voltage sensors for the shelf manager are detecting a voltage within an acceptable range. <ul style="list-style-type: none"> • <i>OK</i>: All monitored voltages are within acceptable ranges. • <i>Below lower critical</i>: A monitored voltage is too low.
Voltage	Voltage value for a voltage sensor.
Edit	Select to modify the thresholds of a voltage sensor.

Viewing shelf alarm panel (SAP) status

You can view the shelf alarm panel (SAP) status for a chassis. The shelf alarm panel helps you monitor the temperature and state of various sensors in the chassis.

Go to *[chassis name] > SAP* to view the chassis SAP status.

The following is displayed:

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

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 616](#).

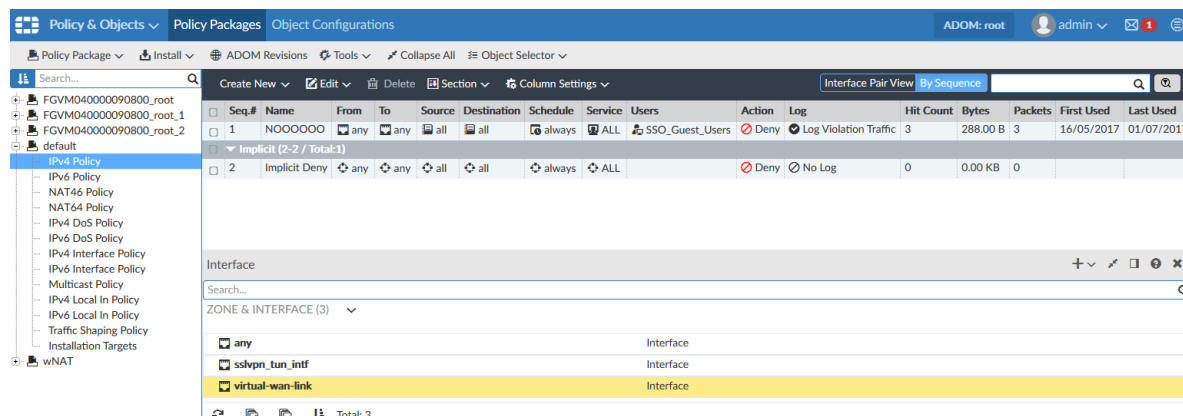


If *Display Policy & Objects in Dual Pane* is enabled, the *Policy Packages* and *Object Configurations* tabs will be shown on the same pane, with *Object Configurations* on the lower half of the screen. See [Display options on page 190](#).



If workspace is enabled, the ADOM must be locked before changes can be made. See [Locking an ADOM on page 565](#).

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 517](#).



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:

Policy Package	Click to access the policy package menu. The menu options are the same as the right-click menu options.
Install Wizard	Click to access the Install menu. You can start the Install Wizard where you can install policy packages and device settings. You can also re-install a policy.
ADOM Revisions	Click to create, edit, delete, restore, lock, and unlock ADOM Revisions.
Tools	Click to select one of the following tools from the menu: <i>Display Options</i> , <i>Find Unused Objects</i> , or <i>Find Duplicate Objects</i> .
Collapse/Expand All	Collapse or expand all the categories in the policy list.
Object Selector	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.
Search	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:

ADOM Revisions	Click to create, edit, delete, restore, lock, and unlock ADOM Revisions.
Tools	Click to select one of the following tools from the menu: <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:

Lock Unlock	Select to lock or unlock the ADOM.
Sessions	Click to display the sessions list where you can save, submit, or discard changes made during the session.

About policies

FortiManager provides administrators the ability to customize policies within their organization as they see fit. Typically, administrators may want to customize access and policies based on factors such as geography, specific security requirements, or legal requirements.

Within a single ADOM, administrators can create multiple policy packages. FortiManager provides you the ability to customize policy packages per device or VDOM within a specific ADOM, or to apply a single policy package for all devices within an ADOM. These policy packages can be targeted at a single device, multiple devices, all devices, a single VDOM, multiple VDOMs, or all devices within a single ADOM. By defining the scope of a policy package, an administrator can modify or edit the policies within that package and keep other policy packages unchanged.

FortiManager can help simplify provisioning of new devices, ADOMs, or VDOMs by allowing you to copy or clone existing policy packages.

Policy theory

Security policies control all traffic attempting to pass through a unit between interfaces, zones, and VLAN subinterfaces.

Security policies are instructions that units use to decide connection acceptance and packet processing for traffic attempting to pass through. When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a security policy matching the packet.

Security policies can contain many instructions for the unit to follow when it receives matching packets. Some instructions are required, such as whether to drop or accept and process the packets, while other instructions, such as logging and authentication, are optional.

Policy instructions may include Network Address Translation (NAT), or Port Address Translation (PAT), or they can use virtual IPs or IP pools to translate source and destination IP addresses and port numbers.

Policy instructions may also include Security Profiles, which can specify application-layer inspection and other protocol-specific protection and logging, as well as IPS inspection at the transport layer.

You configure security policies to define which sessions will match the policy and what actions the device will perform with packets from matching sessions.

Sessions are matched to a security policy by considering these features of both the packet and policy:

- Policy Type and Subtype
- Incoming Interface
- Source Address
- Outgoing Interface
- Destination Address
- Schedule and time of the session's initiation
- Service and the packet's port numbers.

If the initial packet matches the security policy, the device performs the configured action and any other configured options on all packets in the session.

Packet handling actions can be *ACCEPT*, *DENY*, *IPSEC*, or *SSL-VPN*.

- **ACCEPT** policy actions permit communication sessions, and may optionally include other packet processing instructions, such as requiring authentication to use the policy, or specifying one or more Security Profiles to apply features such as virus scanning to packets in the session. An **ACCEPT** policy can also apply interface-mode IPsec VPN traffic if either the selected source or destination interface is an IPsec virtual interface.
- **DENY** policy actions block communication sessions, and you can optionally log the denied traffic. If no security policy matches the traffic, the packets are dropped, therefore it is not required to configure a **DENY** security policy in the last position to block the unauthorized traffic. A **DENY** security policy is needed when it is required to log the denied traffic, also called "violation traffic".
- **IPSEC** and **SSL VPN** policy actions apply a tunnel mode IPsec VPN or SSL VPN tunnel, respectively, and may optionally apply NAT and allow traffic for one or both directions. If permitted by the firewall encryption policy, a tunnel may be initiated automatically whenever a packet matching the policy arrives on the specified network interface, destined for the local private network.

Create security policies based on traffic flow. For example, in a policy for POP3, where the email server is outside of the internal network, traffic should be from an internal interface to an external interface rather than the other way around. It is typically the user on the network requesting email content from the email server and thus the originator of the open connection is on the internal port, not the external one of the email server. This is also important to remember when viewing log messages, as the source and destination of the packets can seem backwards.

Global policy packages

Global policies and objects function in a similar fashion to local policies and objects, but are applied universally to all ADOMs and VDOMs inside your FortiManager installation. This allows users in a carrier, service provider, or large enterprise to support complex installations that may require their customers to pass traffic through their own network.

For example, a carrier or host may allow customers to transit traffic through their network, but do not want their customer to have the ability to access the carrier's internal network or resources. Creating global policy header and footer packages to effectively surround a customer's policy packages can help maintain security.

Global policy packages must be 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.

The screenshot displays the FortiManager 'Policy & Objects' configuration interface. The top pane shows a list of policy packages, including 'FGVM040000090800_root', 'Test Laura', 'default', and 'wNAT'. The bottom pane shows a list of interfaces and zones, including 'Interface (5)' and 'Zone (6)'. The interface list includes 'any', 'sslvpn_tun_intf', 'virtual-wan-link', 'Linkob1', and 'Meshow1'. The zone list includes 'vpnmgr_test_hub2spoke', 'vpnmgr_test_mesh', 'vpnmgr_test_spoke2hub', 'vpnmgr_tet_mesh', and 'vpnmgr_tet_spoke2hub'.

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

Name
 In Folder 
 Central NAT ☐
 NGFW Mode Profile-based Policy-based
 Consolidated Firewall Mode ☐ OFF

OK Cancel

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

Name	Enter a name for the new policy package.
In Folder	Optionally, click the <i>In Folder</i> button to select a folder for the package.
Central NAT	Select the <i>Central NAT</i> check box to enable <i>Central SNAT</i> and <i>Central DNAT</i> policy types.
NGFW Mode	Select the NGFW mode, <i>Profile-based</i> (default) or <i>Policy-based</i> .
SSL/SSH Inspection	Select an SSL/SSH inspection type from the dropdown list. This option is only available for version 5.6 and later ADOMs when <i>NGFW Mode</i> is <i>Policy-based</i> .
Consolidated Firewall Mode	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 208](#).

To install a policy package to a target device:

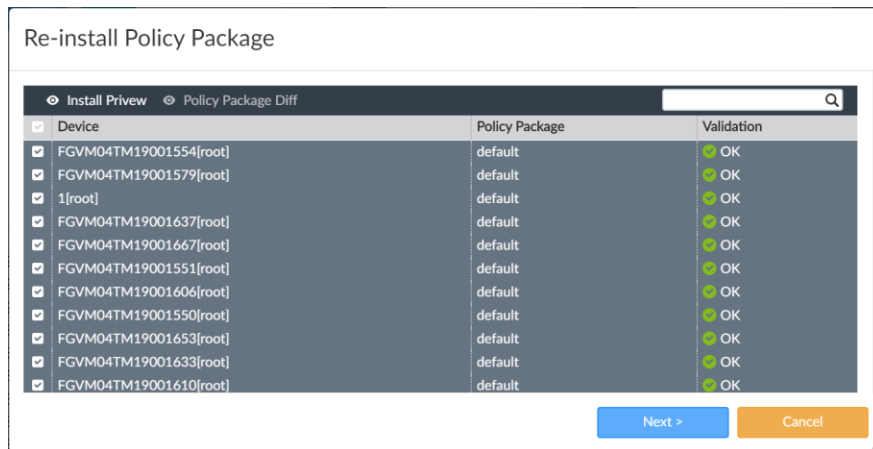
1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects > Policy Packages*.
3. Select a policy package and from the *Install* menu or right-click menu select *Install Wizard*. The *Install Wizard* opens.
4. Follow the steps in the install wizard to install the policy 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 74](#). For more information on editing the installation targets, see [Policy package installation targets on page 198](#).

Reinstall a policy package

You can reinstall a policy package in *Policy & Objects* or *Device Manager*.

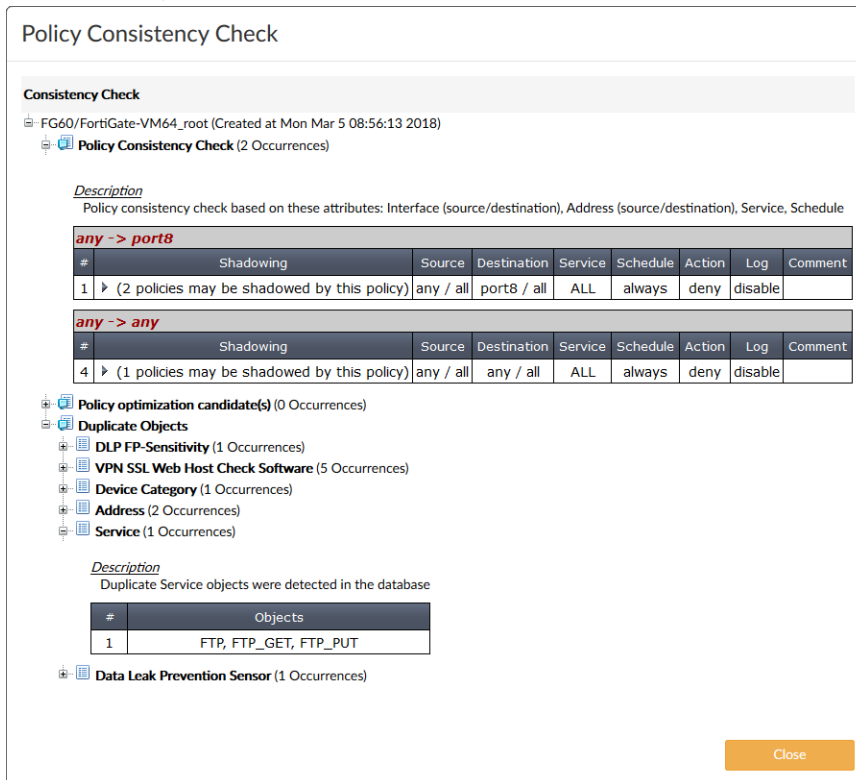
To reinstall a policy package:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Perform one of the following actions:
 - Go to *Policy & Objects > Policy Packages*, and select a policy package.
 - Go to *Device Manager*, and select devices or VDOMs. You can select more than one device at a time.
3. In the toolbar, select *Install > Re-install Policy*.
After data is gathered, the *Re-install Policy Package* window is displayed.



4. (Optional) View policy consistency check results (see [Perform a policy consistency check on page 200](#)).

a. Click the *Policy Check Result* button.

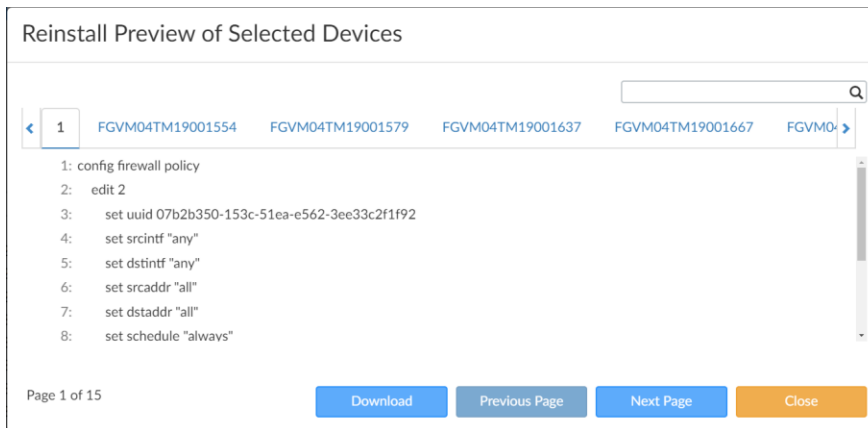


b. Click the *Close* button to close the page and return to the wizard.

5. (Optional) View a preview of the installation. You can preview multiple devices at the same.

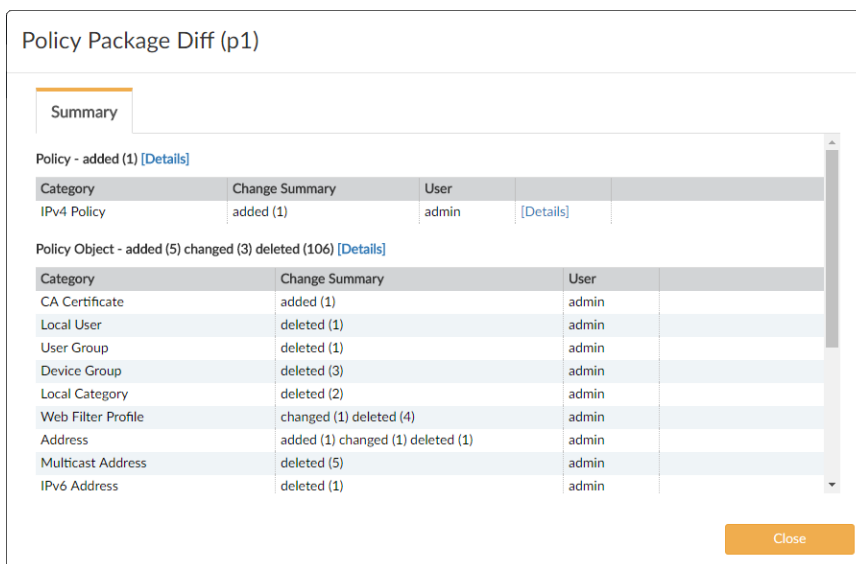
a. Click the *Install Preview* button.

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



- b. Click *Next Page* or *Previous page* to view multiple devices
 - c. Click the *Download* button to download a text file of the preview information.
 - d. Click the *Close* button to close the page and return to the wizard.
6. (Optional) View the difference between the current policy package and the policy in the device.
- a. Click the *Policy Package Diff* button.

After data is gathered, the *Policy Package Diff* page is displayed.



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

Schedule a policy package install

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

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

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

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

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

To edit or cancel an install schedule:

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

Export a policy package

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

To export a policy package:

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

Policy package installation targets

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

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

The following information is displayed:

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

The following table identifies the different available config statuses.

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

The following table identifies the different available policy package statuses.

Policy Package Status	Icon	Description
Imported	Green check ✓	Policies and objects are imported into FortiManager.
Synchronized	Green check ✓	Policies and objects are synchronized between FortiManager and the managed device.
Modified	Yellow triangle ⚠	Policies or objects are modified on FortiManager.
Out of Sync	Red X ✖	Policies or objects are modified on the managed device.

Policy Package Status	Icon	Description
Unknown with policy package name	Gray question mark 	Configurations of the managed device are retrieved on FortiManager after being imported/installed.
Never Installed	Yellow triangle 	No policy package is imported or installed.



When importing a device with agentless FSSO configured (that is, the device polls the AD servers), the status of all policy packages that reference *user fssso-polling* is *Modified*. This is because FortiManager sends all fssso-polling objects to all devices that are using agentless FSSO.

The following options are available:

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

Perform a policy consistency check

The policy check tool allows you to check all policy packages within an ADOM to ensure consistency and eliminate conflicts that may prevent your devices from passing traffic. This allows you to optimize your policy sets and potentially reduce the size of your databases.

The check will verify:

- Object duplication: two objects that have identical definitions
- Object shadowing: a higher priority object completely encompasses another object of the same type
- Object overlap: one object partially overlaps another object of the same type
- Object orphaning: an object has been defined but has not been used anywhere.

The policy check uses an algorithm to evaluate policy objects, based on the following attributes:

- The source and destination interface policy objects
- The source and destination address policy objects
- The service and schedule policy objects.



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

This function can be enabled when editing the ADOM (see [Editing an ADOM on page 562](#)).

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

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

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

Policy optimization candidate(s) (0 Occurrences)

Duplicate Objects

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

Description
 Duplicate Service objects were detected in the database

#	Objects
1	FTP, FTP_GET, FTP_PUT

Data Leak Prevention Sensor (1 Occurrences)

Close

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 57](#).

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 190](#) 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		Ni

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 204](#).



If workspace or workflow is enabled, the ADOM must be locked before changes can be made. See [Locking an ADOM on page 565](#).



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	<input checked="" type="checkbox"/> any	<input checked="" type="checkbox"/> any	<input checked="" type="checkbox"/> swscan.appl	<input checked="" type="checkbox"/> all

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

Device/VDOM	Select the FortiGate device or the VDOM from the drop-down.
Source Interface	Select the source interface from the drop-down.
Protocol	Select the protocol from the drop-down.
Protocol Number	Specify a number between 1 to 255.
Source	Specify the source IP address.
Destination	Specify the destination IP address or a Fully Qualified Domain Name (FQDN).



The Policy Lookup feature is available only for IPv4 and IPv6 policies.



FortiManager must be in sync with the FortiGate devices or VDOMs either by installing or importing the policy. If FortiManager is not in sync with the FortiGate devices, a message will be shown that the device is out of sync. You can still perform the policy lookup, but the results may not be accurate.

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 207](#) and [Drag and drop objects on page 208](#).

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.

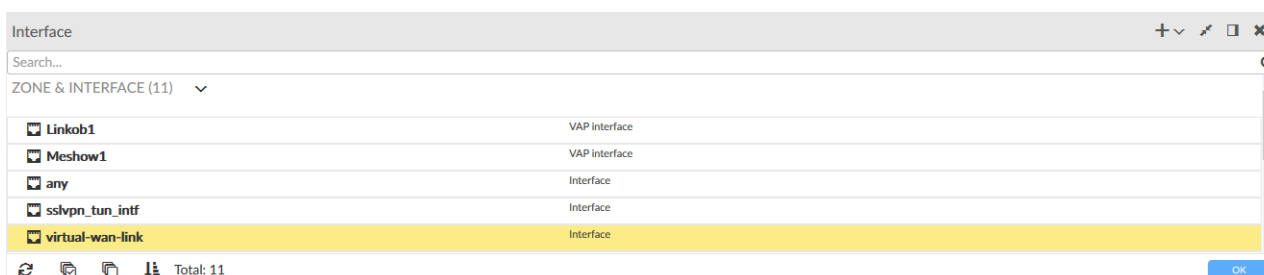
Select a policy, and from the *Section* menu, click *Add*. Type a section name, and click *OK* to add a section to the currently selected policy.

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 190](#).

**Create New**

Click the create new dropdown list, then select the object type to make a new object. See [Create a new object on page 245](#).

Collapse / Expand All

Expand or collapse all of the object groups shown in the pane.

Dock to bottom / right

Move the *Object Selector* frame to the bottom or right side of the content pane.

Close

Close the *Object Selector* frame.

Search	Enter a search term to search the object list.
Refresh	Refresh the list.
Select All	Select all objects in the list.
Deselect All	Deselect all objects in the list.
Sort	Sort the object list alphabetically.

Objects can be added or removed from the selected cell by clicking on them, and then selecting OK to apply the change and close the *Object Selection* pane.

Objects can also be dragged and dropped from the pane to applicable, highlighted cells in the policy list.

Right-click on an object in the pane to *Edit* or *Clone* the object, and to see where it is used. See [Edit an object on page 265](#) and [Clone an object on page 266](#).

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 198](#)), then click *OK*.

The policy will now be installed only on the selected installation targets, and not the other devices to which the policy package is assigned.

Configuring policy details

Various policy details can be configured directly from the policy tables, such as the policy schedule, service, action, security profiles, and logging.

To edit a policy schedule with dual pane disabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
4. In the *Schedule* column, click the cell in the policy that you want to edit. The *Object Selector* frame is displayed.
5. In the *Object Selector* frame, locate the schedule object, then drag and drop the object onto the cell in the *Schedule* column for the policy that you want to change.
6. Click *OK* to close the *Object Selector* frame.

To edit a policy schedule with dual pane enabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
4. In the object pane, go to *Firewall Objects > Schedules*.
5. Locate the schedule object, then drag and drop the object onto the cell in the *Schedule* column for the policy that you want to change.

To edit a policy service with dual pane disabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
4. In the *Service* column, click the cell in the policy that you want to edit. The *Object Selector* frame opens.
5. In the *Object Selector* frame, locate the service object, and then drag and drop the object onto the cell in the *Service* column for the policy that you want to change.
6. Click *OK* to close the *Object Selector* frame.

To edit a policy service with dual pane enabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
4. In the object pane, go to *Firewall Objects > Services*. The services objects are displayed in the content pane.
5. Locate the service object, then drag and drop the object onto the cell in the *Service* column for the policy that you want to change.

To edit a services object:

1. Go to *Policy & Objects > Object Configuration*.
2. In the tree menu, go to *Firewall Objects > Services*. The services objects are displayed in the content pane.
3. Select a services object, and click *Edit*. The *Edit Service* dialog box is displayed.

4. Configure the following settings, then click **OK** to save the service. The custom service will be added to the available services.

Name	Edit the service name as required.
Comments	Type an optional comment.
Service Type	Select <i>Firewall</i> or <i>Explicit Proxy</i> .
Show in service list	Select to display the object in the services list.
Category	Select a category for the service.
Protocol Type	Select the protocol from the dropdown list. Select one of the following: <i>TCP/UDP/SCTP</i> , <i>ICMP</i> , <i>ICMP6</i> , or <i>IP</i> .
IP/FQDN	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.
Type	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> .
Code	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> .
Protocol Number	Type the protocol number in the text field. This menu item is available when <i>Protocol Type</i> is set to <i>IP</i> .
Advanced Options	For more information on advanced option, see the <i>FortiOS CLI Reference</i> .
check-reset-range	<p>Configure ICMP error message verification.</p> <ul style="list-style-type: none"> disable: The FortiGate unit does not validate ICMP error messages. strict: If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) TCP(C,D) header, then if FortiManager can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. If it is enabled, the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the <code>anti-replay</code> option checks packets. default: Use the global setting defined in <code>system global</code>. <p>This field is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i>. This field is not available if <i>explicit-proxy</i> is enabled.</p>
Color	Click the icon to select a custom, colored icon to display next to the service name.
session-ttl	<p>Type the default session timeout in seconds.</p> <p>The valid range is from 300 - 604 800 seconds. Type 0 to use either the <code>per-policy session-ttl</code> or <code>per-VDOM session-ttl</code>, as applicable.</p> <p>This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i>.</p>

tcp-halfclose-timer	<p>Type how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded. The valid range is from 1 to 86400 seconds. Type 0 to use the global setting defined in <code>system global</code>.</p> <p>This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i>.</p>
tcp-halfopen-timer	<p>Type how many seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded. The valid range is from 1 to 86400 seconds. Type 0 to use the global setting defined in <code>system global</code>.</p> <p>This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i>.</p>
tcp-timewait-timer	<p>Set the length of the TCP TIME-WAIT state in seconds. As described in RFC 793, the "...TIME-WAIT state represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request."</p> <p>Reducing the length of the TIME-WAIT state means the FortiGate unit can close terminated sessions faster, which means that more new sessions can be opened before the session limit is reached.</p> <p>The valid range is 0 to 300 seconds. A value of 0 sets the TCP TIME-WAIT to 0 seconds. Type 0 to use the global setting defined in <code>system global</code>.</p> <p>This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i>.</p>
udp-idle-timer	<p>Type the number of seconds before an idle UDP connection times out. The valid range is from 1 to 86400 seconds.</p> <p>Type 0 to use the global setting defined in <code>system global</code>.</p> <p>This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i>.</p>

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

Create New Policy Block

Name

Central NAT

OFF

NGFW Mode

Profile-based

Policy-based

OK

Cancel

- 4. Configure the following details, then click *OK* to create the Policy Block.

Name	Enter a name for the new Policy Block.
Central NAT	Toggle <i>Central NAT</i> to <i>ON</i> to enable <i>Central SNAT</i> and <i>Central DNAT</i> policy types.
NGFW Mode	Select the NGFW mode, <i>Profile-based</i> (default) or <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:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. Go to *Policy Blocks* > *[Policy_Block_Name]* > *IPv4* or *IPv6*.
4. Click *Create New*. See [IP policies on page 214](#) on how to create an IPv4 or IPv6 policy.

To copy a policy into a Policy Block:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. Click *[Policy_Package_Name]*. For example, click *Default*.
4. Click *IPv4* or *IPv6*.
5. Select one or more policies.
6. Right-click and select *Copy*.
7. Go to *Policy Blocks* > *[Policy_Block_Name]* > *IPv4* or *IPv6*.
8. 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.

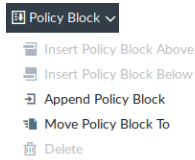


After a Policy Block is appended to a Policy Package, you can add or remove policies from the Policy Block. You need to append the Policy Block to the Policy Package only once. It is not required to append the Policy Block to the Policy Package again after adding or removing policies from the Policy Block.

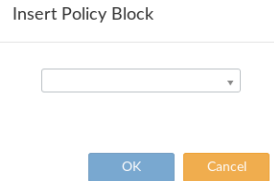
To append an existing policy to a Policy Block:

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*.



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

Incoming Interface

any

Outgoing Interface

any

Source Internet Service

OFF

Source Address

all

Source User

+

Source User Group

+

Source Device

+

Destination Internet Service

OFF

Destination Address

all

Service

ALL

Schedule

always

Action

Deny Accept IPSEC

Log Traffic

☒ Log Violation Traffic
☐ Generate Logs when Session Starts

Comments

Meta Fields >

Advanced Options >

OK

Cancel

5. Enter the following information:

Name	Enter a unique name for the policy. Each policy must have a unique name.
Incoming Interface	<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 Create a new object on page 245 for more information.</p>
Outgoing Interface	Select outgoing interfaces.
Source Internet Service	<p>Turn source internet service on or off, then select services.</p> <p>This option is only available for IPv4 policies.</p>
Source Address	<p>Select source addresses.</p> <p>This option is only available when <i>Source Internet Service</i> is off.</p>
Source User	<p>Select source users.</p> <p>This option is only available when <i>Source Internet Service</i> is off.</p>
Source User Group	<p>Select source user groups.</p> <p>This option is only available when <i>Source Internet Service</i> is off.</p>
Source Device	<p>Select source devices, device groups, and device categories.</p> <p>This option is only available when <i>Source Internet Service</i> is off.</p>
Destination Internet Service	<p>Turn destination internet service on or off, then select services.</p> <p>This option is only available for IPv4 policies.</p>
Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups.

	This option is only available when <i>Destination Internet Service</i> is off.
Service	Select services and service groups. This option is only available when <i>Destination Internet Service</i> is off.
Schedule	Select schedules, one time or recurring, and schedule groups.
Application	Select applications. This option is only available when <i>NGFW Mode</i> is <i>Policy-based</i> for the policy package; see Create new policy packages on page 191 .
URL Category	Select URL categories. This option is only available when <i>NGFW Mode</i> is <i>Policy-based</i> for the policy package; see Create new policy packages on page 191 .
Action	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.
Log Traffic	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"> • <i>No Log</i> • <i>Log Security Events</i> • <i>Log All Sessions</i>
Generate Logs when Session Starts	Select to generate logs when the session starts.
Capture Packets	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
NAT	Select to enable NAT. 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 Create new policy packages on page 191 .
VPN Tunnel	Select a VPN tunnel dynamic object from the dropdown list. Select to allow traffic to be initiated from the remote site. This option is available when the <i>Action</i> is <i>IPSEC</i> .
Security Profiles	Select to add security profiles or profile groups. This option is available when the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> . The following profile types can be added: <ul style="list-style-type: none"> • AntiVirus Profile • Web Filter Profile • Application Control • IPS Profile • Email Filter Profile • DLP Sensor • VoIP Profile

	<ul style="list-style-type: none"> • ICAP Profile • SSL/SSH Inspection • Web Application Firewall • DNS Filter • Proxy Options • Profile Group (available when <i>Use Security Profile Group</i> is selected)
Shared Shaper	Select traffic shapers. This option is available if the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> .
Reverse Shaper	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.
Per-IP Shaper	Select per IP traffic shapers. This option is available if the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> .
Comments	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the <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
auth-cert	HTTPS server certificate for policy authentication (IPv4 only).	none
auth-path	Enable or disable authentication-based routing (IPv4 only).	disable
auth-redirect-addr	HTTP-to-HTTPS redirect address for firewall authentication (IPv4 only).	none
auto-asic-offload	Enable or disable policy traffic ASIC offloading.	enable
block-notification	Enable or disable block notification (IPv4 only).	disable
captive-portal-exempt	Enable or disable exemption of captive portal (IPv4 only).	disable
custom-log-fields	Select the custom log fields from the dropdown list.	none
delay-tcp-npu-session	Enable or disable TCP NPU session delay in order to guarantee packet order of 3-way handshake (IPv4 only).	disable
diffserv-forward	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic.	disable
diffserv-reverse	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
diffservcode-forward	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
diffservcode-rev	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
disclaimer	Enable or disable user authentication disclaimer (IPv4 only).	disable
dscp-match	Enable or disable DSCP check.	disable
dscp-negate	Enable or disable negate DSCP match.	disable
dscp-value	Enter the DSCP value.	000000
dsri	Enable or disable DSRI (Disable Server Response Inspection) to ignore HTTP server responses.	disable
dstaddr-negate	Enable or disable negated destination address match.	disable
firewall-session-dirty	Packet session management, either <i>check-all</i> or <i>check-new</i> .	check-all
fsso-agent-for-ntlm	Select the FSSO agent for NTLM from the dropdown list (IPv4 only).	none
identity-based-route	Name of identity-based routing rule (IPv4 only).	none
internet-service-negate	When enabled, Internet services match against any Internet service EXCEPT the selected Internet service (IPv4 only).	disable
internet-service-src-negate	Enables or disables the use of Internet Services in source for this policy. If enabled, <i>internet-service-src</i> specifies what the service must NOT be (IPv4 only).	disable
learning-mode	Enable or disable learning mode for policy (IPv4 only).	disable
match-vip	Enable or disable match DNATed packet (IPv4 only).	disable
natinbound	Enable or disable policy NAT inbound.	disable
natip	Type the NAT IP address in the text field (IPv4 only).	0.0.0.0
natoutbound	Enable or disable policy NAT outbound.	disable
np-acceleration	Enable or disable UTM Network Processor acceleration.	enable
ntlm	Enable or disable NTLM authentication (IPv4 only).	disable
ntlm-enabled-browsers	Type a value in the text field (IPv4 only).	none
ntlm-guest	Enable or disable NTLM guest (IPv4 only).	disable
outbound	Enable or disable policy outbound.	disable
permit-any-host	Enable to accept UDP packets from any host (IPv4 only).	disable
permit-stun-host	Enable to accept UDP packets from any STUN host (IPv4 only).	disable

Option	Description	Default
radius-mac-auth-bypass	Enable MAC authentication bypass. The bypassed MAC address must be received from RADIUS server.	disable
redirect-url	URL redirection after disclaimer/authentication (IPv4 only).	none
replacemsg-override-group	Specify authentication replacement message override group.	none
rtp-addr	Select the RTP address from the dropdown list (IPv4 only).	none
rtp-nat	Enable to apply source NAT to RTP packets received by the firewall policy (IPv4 only).	disable
scan-botnet-connections	Enable or disable scanning of connections to Botnet servers (IPv4 only).	disable
schedule-timeout	Enable to force session to end when policy schedule end time is reached (IPv4 only).	disable
send-deny-packet	Enable to send a packet in reply to denied TCP, UDP or ICMP traffic.	disable
service-negate	Enable or disable negated service match.	disable
session-ttl	Type a value for the session time-to-live (TTL) from 300 to 604800, or type 0 for no limitation.	0
srcaddr-negate	Enable or disable negated source address match.	disable
ssh-filter-profile	Select an SSH filter profile from the dropdown list.	None
ssl-mirror	Enable or disable SSL mirror.	disable
ssl-mirror-intf	Mirror interface name.	none
tcp-mss-receiver	Type a value for the receiver's TCP MSS.	0
tcp-mss-sender	Type a value for the sender's TCP MSS.	0
tcp-session-without-syn	Enable or disable creation of TCP session without SYN flag. <ul style="list-style-type: none"> • <code>all</code> - Enable TCP session without SYN. • <code>data-only</code> - Enable TCP session data only. • <code>disable</code> - Disable TCP session without SYN. 	disable
timeout-send-rst	Enable sending a TCP reset when an application session times out.	disable
vlan-cos-fwd	Type the VLAN forward direction user priority.	255
vlan-cos-rev	Type the VLAN reverse direction user priority.	255
vlan-filter	Set VLAN filters.	
wanopt	Enable or disable WAN optimization (IPv4 only).	disable
wanopt-detection	WAN optimization auto-detection mode (IPv4 only).	active
wanopt-passive-opt	WAN optimization passive mode options. This option decides what IP address will be used to connect server (IPv4 only).	default

Option	Description	Default
wanopt-peer	WAN optimization peer (IPv4 only).	none
wanopt-profile	WAN optimization profile (IPv4 only).	none
wccp	Enable or disable Web Cache Communication Protocol (WCCP) (IPv4 only).	disable
webcache	Enable or disable web cache (IPv4 only).	disable
webcache-https	Enable or disable web cache for HTTPS (IPv4 only).	disable
wssso	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

Incoming Interface

any

Outgoing Interface

any

Source Internet Service

OFF

IPv4 Source Address

all

IPv6 Source Address

all

Source User

+

Source User Group

+

Destination Internet Service

OFF

IPv4 Destination Address

all

IPv6 Destination Address

all

Service

ALL

Firewall / Network Options

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:

Name	Enter a unique name for the policy. Each policy must have a unique name.
Incoming Interface	<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 Create a new object on page 245 for more information.</p>
Outgoing Interface	Select outgoing interfaces.
Source Internet Service	<p>Turn source internet service on or off, then select services.</p> <p>This option is only available for IPv4 policies.</p>
FSSO Groups	Select the FSSO groups added via Fortinet Single Sign-On. For more information about FSSO groups, see FSSO user groups on page 269 .
IPv4 Source Address	<p>Select the IPv4 source addresses.</p> <p>This option is only available when <i>Source Internet Service</i> is off.</p>
IPv6 Source Address	<p>Select the IPv6 source addresses.</p> <p>This option is only available when <i>Source Internet Service</i> is off.</p>
Source User	<p>Select source users.</p> <p>This option is only available when <i>Source Internet Service</i> is off.</p>
Source User Group	Select source user groups.

	This option is only available when <i>Source Internet Service</i> is off.
Source Device	Select source devices, device groups, and device categories. This option is only available when <i>Source Internet Service</i> is off.
Destination Internet Service	Turn destination internet service on or off, then select services. This option is only available for IPv4 policies.
IPv4 Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups. This option is only available when <i>Destination Internet Service</i> is off.
IPv6 Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups. This option is only available when <i>Destination Internet Service</i> is off.
Service	Select services and service groups. This option is only available when <i>Destination Internet Service</i> is off.
Firewall / Network Options	Central NAT is enabled by default so NAT settings from matching Central SNAT policies will be applied.
Security Profiles	Select one of the following options for SSL/SSH Inspection: <ul style="list-style-type: none"> • certificate-inspection • custom-deep-inspection • deep-inspection • no-inspection New objects can be created by clicking the <i>Create New</i> icon in the <i>Object Selector</i> frame. See Create a new object on page 245 for more information.
Comments	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the <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
auto-asic-offload	Enable or disable policy traffic ASIC offloading.	enable
cifs-profile	Enable or disable authentication-based routing (IPv4 only).	disable
diffserv-forward	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic.	disable
diffserv-reverse	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
diffservcode-forward	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
diffservcode-rev	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
http-policy-redirect	Select the custom log fields from the dropdown list.	none
inspection-mode	Enable or disable TCP NPU session delay in order to guarantee packet order of 3-way handshake (IPv4 only).	disable
outbound	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic.	disable
session-ttl	Type a value for the session time-to-live (TTL) from 300 to 604800, or type 0 for no limitation.	0
ssh-filter-profile	Select an SSH filter profile from the drop-down list.	None
ssh-policy-redirect	Enable or disable SSH policy redirect.	disable
tcp-mss-receiver	Type a value for the receiver's TCP MSS.	0
tcp-mss-sender	Type a value for the sender's TCP MSS.	0
wanopt	Enable or disable WAN optimization (IPv4 only).	disable
wanopt-detection	Select the WAN optimization as active, passive, or off.	active
wanopt-passive-opt	WAN optimization passive mode options. This option decides what IP address will be used to connect server (IPv4 only).	default
wanopt-peer	WAN optimization peer (IPv4 only).	none
wanopt-profile	WAN optimization profile (IPv4 only).	none
webcache	Enable or disable web cache (IPv4 only).	disable
webcache-https	Select the FSSO agent for NTLM from the drop-down list (IPv4 only).	none
webproxy-forward-server	Name of identity-based routing rule (IPv4 only).	none
webproxy-profile	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="button" value="any"/> <input type="button" value="X"/>
Outgoing Interface	<input type="button" value="any"/> <input type="button" value="X"/>
Source	<input type="button" value="all"/> <input type="button" value="X"/>
Destination	<input type="button" value="all"/> <input type="button" value="X"/>
Service	<input type="button" value="App Default"/> <input type="button" value="Specify"/>
Schedule	<input type="button" value="always"/> <input type="button" value="X"/>
Application	<input type="button" value="+"/>
URL Category	<input type="button" 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:

Name	Enter a unique name for the policy. Each policy must have a unique name.
Incoming Interface	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 Create a new object on page 245 for more information.
Outgoing Interface	Select outgoing interfaces.
Source	Select source addresses.

Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
Service	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.
Schedule	Select schedules, one time or recurring, and schedule groups.
Application	Select applications.
URL Category	Select URL categories.
Action	Select an action for the policy to take: <i>ACCEPT</i> or <i>DENY</i> .
Log Traffic	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"> • <i>No Log</i> • <i>Log Security Events</i> • <i>Log All Sessions</i>
Generate Logs when Session Starts	Select to generate logs when the session starts.
Security Profiles	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"> • Proxy Options • AntiVirus Profile • IPS Profile • Email Filter Profile • DLP Sensor
Comments	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the <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
application-list	Select from the drop-down list.	None
cifs-profile	Enable or disable authentication-based routing (IPv4 only).	None
dnsfilter-profile	Select from the drop-down list.	None
icap-profile	Select from the drop-down list.	None
custom-log-fields	Select the custom log fields from the drop-down list.	none

Option	Description	Default
internet-service-negate	When enabled, Internet services match against any Internet service except the selected Internet service (IPv4 only).	disable
internet-service-src-negate	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
service-negate	Enable or disable negated service match.	disable
ssh-filter-profile	Select an SSH filter profile from the drop-down list.	None
ssl-ssh-profile	Select an SSL SSH profile from the drop-down list.	no-inspection
utm-status	Enable or disable the Unified Threat Management status.	disable
voip-profile	Select the VOIP profile.	None
webfilter-profile	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 307](#).



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:

Name	Enter a unique name for the policy. Each policy must have a unique name.
Virtual Wire Pair Interface	Select an interface. You can type the name of the interface to search for it in the list.
Virtual Wire Pair	Select an arrow to indicate the flow of traffic between ports.
Source Internet Service	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.
Source Address	Select source addresses.

	This option is only available when <i>Source Internet Service</i> is off.
Source User	Select source users. This option is only available when <i>Source Internet Service</i> is off.
Source User Group	Select source user groups. This option is only available when <i>Source Internet Service</i> is off.
Source Device	Select source devices, device groups, and device categories. This option is only available when <i>Source Internet Service</i> is off.
Internet Service	Toggle <i>ON</i> to enable Internet service. Toggle <i>OFF</i> to disable Internet service.
Destination Internet Service	Turn destination internet service on or off, then select services.
Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups. This option is available when <i>Destination Internet Service</i> is <i>OFF</i> .
Service	Select services and service groups. This option is available when <i>Destination Internet Service</i> is <i>OFF</i> .
Schedule	Select schedules, one time or recurring, and schedule groups.
Action	Select an action for the policy to take: <i>Deny</i> or <i>Accept</i> .
Log Traffic	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"> • <i>No Log</i> • <i>Log Security Events</i> • <i>Log All Sessions</i>
Generate Logs when Session Starts	Select to generate logs when the session starts.
Capture Packets	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
Security Profiles	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"> • Antivirus Profile • Web Filter Profile • Application Control • IPS Profile • Email Filter Profile • DLP Sensor • VoIP Profile • ICAP Profile • SSL/SSH Inspection • Web Application Firewall • DNS Filter

	<ul style="list-style-type: none"> • Proxy Options • Profile Group (available when <i>Use Security Profile Group</i> is selected)
Shared Shaper	Select traffic shapers. This option is available if the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> .
Reverse Shaper	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.
Per-IP Shaper	Select per IP traffic shapers. This option is available if the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> .
Description	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	Configure advanced options, see Advanced options on page 217 . 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:

Incoming Interface	Click the field then select interfaces from the <i>Object Selector</i> frame, or drag and drop the address from the object pane.
Outgoing Interface	Select outgoing interfaces.
Source Address	Select source addresses.

Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
Service	Select services and service groups.
Schedule	Select schedules, one time or recurring, and schedule groups.
Action	Select an action for the policy to take: <i>ACCEPT</i> , or <i>DENY</i> .
Log Allowed Traffic	Select to log allowed traffic.
NAT	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.
Dynamic IP Pool	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.
Traffic Shaping	Select traffic shapers. This option is available if the <i>Action</i> is <i>ACCEPT</i> .
Reverse Traffic Shaping	Select traffic shapers. This option is available if at least one forward traffic shaper is selected.
Per-IP Traffic Shaping	Select per IP traffic shapers. This option is available if the <i>Action</i> is <i>ACCEPT</i> .
Description	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	
ippool	Enable IP pools. This option is only available for NAT46 policies.
permit-any-host	Enable to accept UDP packets from any host.
poolname	Select a firewall IP pool from the dropdown list (default = None). This option is only available for NAT46 policies.
tcp-mss-receiver	Enter a value for the receiver's TCP MSS.
tcp-mss-sender	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.

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

Explicit Proxy Type	Select the explicit proxy type: <i>Explicit Web</i> , <i>Transparent Web</i> , <i>FTP</i> , or <i>WAN Optimize</i> .
Incoming Interface	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> .
Outgoing Interface	Select outgoing interfaces.
Source	Select source addresses.
Destination	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
Service	Select services and service groups from the object selector pane.
Schedule	Select schedules, one time or recurring, and schedule groups.
Action	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> .
Log Traffic	Select one of the following options: <ul style="list-style-type: none"> • <i>No Log</i>

	<ul style="list-style-type: none"> • <i>Log Security Events</i> • <i>Log All Sessions</i> <p>When <i>Log All Sessions</i> is selected, you can select to generate logs when the session starts.</p> <p>This option is available when the <i>Action</i> is <i>Accept</i>.</p>
Log Violation Traffic	<p>Select to log violation traffic.</p> <p>This option is available when the <i>Action</i> is <i>Deny</i>.</p>
Disclaimer Options	<p>Set the Display Disclaimer: <i>Disable</i>, <i>By Domain</i>, <i>By Policy</i>, or <i>By User</i>.</p> <p>Optionally, select a custom message in the <i>Customize Messages</i> field if not disabled.</p> <p>These options are available when the <i>Action</i> is <i>Accept</i>.</p>
Security Profiles	<p>Select to add security profiles or profile groups.</p> <p>The following profile types can be added:</p> <ul style="list-style-type: none"> • Antivirus Profile • Web Filter Profile - not available when the proxy type is set to <i>FTP</i> • Application Control - not available when the proxy type is set to <i>FTP</i> • IPS Profile - not available when the proxy type is set to <i>FTP</i> • DLP Sensor • ICAP - not available when the proxy type is set to <i>FTP</i> • Web Application Firewall - not available when the proxy type is set to <i>FTP</i> • Proxy Options • SSL/SSH Inspection • Profile Group (available when <i>Use Security Profile Group</i> is selected) <p>This option is available when the <i>Action</i> is <i>Accept</i>.</p>
Redirect URL	<p>Enter the redirect URL.</p> <p>This option is only available when the <i>Action</i> is <i>Redirect</i>.</p>
Web Proxy Forwarding Server	<p>Select a web proxy forwarding server from the dropdown list.</p> <p>This option is not available when the proxy type is set to <i>FTP</i>.</p>
Comments	<p>Add a description of the policy, such as its purpose, or the changes that have been made to it.</p>
Advanced Options	<p>Configure advanced options, see Advanced options below.</p> <p>For more information on advanced option, see the <i>FortiOS CLI Reference</i>.</p>

Advanced options

Option	Description	Default
dstaddr-negate	Enable or disable negated destination address match.	disable
global-label	Enter a global label.	-
http-tunnel-auth	Enable or disable HTTP tunnel authentication	disable
internet-service-negate	Enable or disable negated internet service.	disable

Option	Description	Default
label	Enter a label	-
poolname	Select a firewall IP pool from the dropdown list.	None
scan-botnet-connections	Enable or disable scanning of connections to Botnet servers.	disable
service-negate	Enable or disable negated service match.	disable
session-ttl	Session TTL for sessions accepted by this policy (300 - 6040800 seconds, 0 = use system default).	0
srcaddr-negate	Enable or disable negated source address match.	disable
ssh-filter-profile	Name of an existing SSH filter profile.	None
transparent	Use IP address of client to connect to server.	disable
webcache	Enable or disable web cache.	disable
webcache-https	Enable or disable web cache for HTTPS.	disable
webproxy-profile	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 when creating or editing the policy package for this option to be available in the tree menu. See [Create new policy packages on page 191](#).

Central SNAT must be enabled in *Tools > Display Options* as well for the option to be visible in the tree menu. See [Display options on page 190](#)

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:

Incoming Interface	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.
Outgoing Interface	Select outgoing interfaces.
Source Address	Select source addresses.
Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
NAT	Select to enable NAT.
IP Pool Configuration	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.
Protocol	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.
Comments	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Meta Fields	If configured, enter values for the required meta fields, and optionally for the optional fields. See Meta Fields on page 591 .
Advanced Options	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 191](#).

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:

Name	Enter a unique name for the DNAT.
Comments	Optionally, enter comments about the DNAT, such as its purpose, or the changes that have been made to it.
Color	Select a color.
Interface	Select an interface.
Network Type	Select the network type: <i>Static NAT</i> , <i>DNS Translation</i> , or <i>FQDN</i> .
External IP Address/Range	Enter the start and end external IP addresses in the fields. If there is only one address, enter it in both fields. This option is not available when the network type is <i>FQDN</i> .
Mapped IP Address/Range	Enter the mapped IP address. This option is not available when the network type is <i>FQDN</i> .
External IP Address	Enter the external IP address. This option is only available when the network type is <i>FQDN</i> .
Mapped Address	Select the mapped address. This option is only available when the network type is <i>FQDN</i> .
Source Interface Filter	Select a source interface filter.
Optional Filters	Enable or disable optional filters.
Source Address	Add source IP, range, or subnet filters. Multiple filters can be added using the <i>Add</i> icon.

Services	Enable and add services.
Port Forwarding	Enable or disable port forwarding.
Protocol	Select the protocol: <i>TCP</i> , <i>UDP</i> , <i>SCTP</i> , or <i>ICMP</i> .
External Service Port	Enter the external service port. This option is not available when <i>Protocol</i> is <i>ICMP</i> .
Map to Port	Enter the map to port. This option is not available when <i>Protocol</i> is <i>ICMP</i> .
Enable ARP Reply	Select to enable ARP reply.
Add To Groups	Optionally, select groups to add the virtual IP to from the list.
Advanced Options	Configure advanced options, see Advanced options . For more information on advanced option, see the <i>FortiOS CLI Reference</i> .
Per-Device Mapping	Enable or disable per-device mapping. If multiple imported VIP objects have the same name but different details, the object type will become <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
dns-mapping-ttl	Enter time-to-live for DNS response, from 0 to 604 800. 0 means use the DNS server's response time.	0
extaddr	Select an address.	None
gratuitous-arp-interval	Set the time interval between sending of gratuitous ARP packets by a virtual IP. 0 disables this feature.	0
http-cookie-age	Set how long the browser caches cooking, from 0 to 525600 seconds.	60
http-cookie-domain	Enter the domain name to restrict the cookie to.	none
http-cookie-domain-from-host	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

Option	Description	Default
http-cookie-generation	The exact value of the generation is not important, only that it is different from any generation that has already been used.	0
http-cookie-path	Limit the cookies to a particular path.	none
http-cookie-share	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
http-ip-header-name	Enter a name for the custom HTTP header that the original client IP address is added to.	none
https-cookie-secure	Enable or disable using secure cookies for HTTPS sessions.	disable
id	Custom defined ID.	0
max-embryonic-connections	The maximum number of partially established SSL or HTTP connections, from 0 to 100000.	1000
nat-source-vip	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
outlook-web-access	If enabled, the <code>Front-End-Https: on</code> header is inserted into the HTTP headers, and added to all HTTP requests.	disable
ssl-algorithm	Set the permitted encryption algorithms for SSL sessions according to encryption strength: <ul style="list-style-type: none"> <code>high</code>: permit only high encryption algorithms: AES or 3DES. <code>medium</code>: permit high or medium (RC4) algorithms. <code>low</code>: permit high, medium, or low (DES) algorithms. <code>custom</code>: only allow some preselected cipher suites to be used. 	high
ssl-client-fallback	Enable to prevent Downgrade Attacks on client connections.	enable
ssl-client-renegotiation	Select the SSL secure renegotiation policy. <ul style="list-style-type: none"> <code>allow</code>: allow, but do not require secure renegotiation. <code>deny</code>: do not allow renegotiation. <code>secure</code>: require secure renegotiation. 	allow
ssl-client-session-state-max	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
ssl-client-session-state-timeout	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
ssl-client-session-state-type	The method to use to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate.	both

Option	Description	Default
	<ul style="list-style-type: none"> • 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. • count: expire SSL session states when <code>ssl-client-session-state-max</code> is exceeded. • disable: expire all SSL session states. • time: expire SSL session states when <code>ssl-client-session-state-timeout</code> is exceeded. 	
ssl-dh-bits	The number of bits used in the Diffie-Hellman exchange for RSA encryption of the SSL connection: 768, 1024, 1536, 2048, 3072, or 4096.	2048
ssl-hpkp	Enable or disable including HPKP header in response.	disable
ssl-hpkp-age	The number of seconds that the client should honor the HPKP setting (60 - 157680000).	5184000
ssl-hpkp-backup	Certificate to generate the backup HPKP pin from (size = 35, datasource (s) = vpn.certificate.local.name, vpn.certificate.ca.name).	None
ssl-hpkp-include-subdomains	Enable or disable indicating that the HPKP header applies to all subdomains.	disable
ssl-hpkp-primary	Certificate to generate the primary HPKP pin from (size = 35, datasource (s) = vpn.certificate.local.name, vpn.certificate.ca.name).	None
ssl-hpkp-report-uri	URL to report HPKP violations to (size = 255).	
ssl-hsts	Enable or disable including HSTS header in response.	disable
ssl-hsts-age	The number of seconds that the client should honour the HSTS setting (60 - 157680000).	5184000
ssl-hsts-include-subdomains	Enable or disable indicating that the HSTS header applies to all subdomains.	disable
ssl-http-location-conversion	Enable to replace http with https in the reply's Location HTTP header field.	disable
ssl-http-match-host	Enable 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
ssl-max-version	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> .	tls-1.2
ssl-min-version	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> .	tls-1.0
ssl-pfs	<p>Select the handling of Perfect Forward Secrecy (PFS) by controlling the cipher suites that can be selected.</p> <ul style="list-style-type: none"> • allow: allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected. 	allow

Option	Description	Default
	<ul style="list-style-type: none"> <code>deny</code>: allow only non-Diffie-Hellman cipher-suites, so PFS is not applied. <code>require</code>: allow only Diffie-Hellman cipher-suites, so PFS is applied. 	
ssl-send-empty-frags	<p>Enable to precede the record with empty fragments to thwart attacks on CBC IV.</p> <p>Disable this option if SSL acceleration will be used with an old or buggy SSL implementation which cannot properly handle empty fragments.</p>	enable
ssl-server-algorithm	<p>Set the permitted encryption algorithms for SSL server sessions according to encryption strength:</p> <ul style="list-style-type: none"> <code>high</code>: permit only high encryption algorithms: AES or 3DES. <code>medium</code>: permit high or medium (RC4) algorithms. <code>low</code>: permit high, medium, or low (DES) algorithms. <code>custom</code>: only allow some preselected cipher suites to be used. 	client
ssl-server-max-version	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> .	client
ssl-server-min-version	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> .	client
ssl-server-session-state-max	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.	100
ssl-server-session-state-timeout	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.	60
ssl-server-session-state-type	<p>The method to use to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate.</p> <ul style="list-style-type: none"> <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. <code>count</code>: expire SSL session states when <code>ssl-client-session-state-max</code> is exceeded. <code>disable</code>: expire all SSL session states. <code>time</code>: expire SSL session states when <code>ssl-client-session-state-timeout</code> is exceeded. 	both
weblogic-server	Enable or disable adding an HTTP header to indicate SSL offloading for a WebLogic server.	disable
websphere-server	Enable or disable adding an HTTP header to indicate SSL offloading for a WebSphere server.	disable

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 options.

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:

Incoming Interface	Select the incoming interface from the <i>Object Selector</i> frame, or drag and drop the address from the object pane.
Source Address	Select the source address.
Destination Address	Select the destination address.
Service	Select the service.
L3 Anomalies	
ip_src_session	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.
ip_dst_session	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.
L4 Anomalies	
tcp_syn_flood	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.
tcp_port_scan	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.
tcp_src_session	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.
tcp_dst_session	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.
udp_flood	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.
udp_scan	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.
udp_src_session	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.
udp_dst_session	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.
icmp_flood	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.
icmp_sweep	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.
icmp_src_session	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.
icmp_dst_session	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.
sctp_flood	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.
sctp_scan	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.
sctp_src_session	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.
sctp_dst_session	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.
Advanced Options	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:

Source	
Interface	Select the source zone from the <i>Object Selector</i> frame, or drag and drop the address from the object pane.
Address	Select the source address.
Destination	
Address	Select the destination address.
Service	Select the service.
Log Traffic	Select the traffic to log: <i>No Log</i> , <i>Log Security Events</i> , or <i>Log All Sessions</i> .
AntiVirus Profile	Select to enable antivirus and select the profile from the dropdown list.
Web Filter Profile	Select to enable Web Filter and select the profile from the dropdown list.
Application Control	Select to enable Application Control and select the profile from the dropdown list.
IPS Profile	Select to enable IPS and select the profile from the dropdown list.
Email Filter Profile	Select to enable Email Filter and select the profile from the dropdown list.
DLP Sensor	Select to enable DLP Sensor and select the profile from the dropdown list.
Advanced Options	
comments	Add comments about the policy.
dsri	Enable or disable DSRI (default = disable).
scan-botnet-connections	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:

Incoming Interface	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.
Outgoing Interface	Click in the field and select outgoing interfaces from the multicast interface list. If no multicast interfaces are configured, one must be created.
Source Address	Click the field and select the source firewall addresses.
Source NAT	Enable source NAT.
Source NAT Address	Enter the source NAT IP address.
Destination Interface	Click the field and select the destination firewall addresses.
Destination NAT	Enter the destination NAT IP address.
Protocol Option	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> .
Port Range	Set the port range. This option is only available when <i>Protocol Option</i> is <i>TCP</i> or <i>UDP</i> .
Protocol Number	Enter the protocol number, from 1 to 256. This option is only available when <i>Protocol Option</i> is <i>Others</i> .
Log Traffic	Select to log traffic.
Advanced Options	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:

Interface	Click the field then select an interface from the object selector frame, or drag and drop the interface from the object pane.
Source Address	Select source addresses.
Destination Address	Select destination addresses, address groups, . virtual IPs, and virtual IP groups.
Service	Select services and service groups.
Schedule	Select schedules, one time or recurring, and schedule groups.
Action	Select an action for the policy to take: <i>ACCEPT</i> or <i>DENY</i> .
HA Management Interface Only	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:

IP Version	Select the IP address version: <i>IPv4</i> or <i>IPv6</i> .
Matching Criteria	
Source Internet Service	Turn source internet service on or off, then select services.
Source Address	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.
Destination Internet Service	Turn destination internet service on or off, then select services.
Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups. This option is only available when <i>Destination Internet Service</i> is off.
Service	Select services and service groups. This option is only available when <i>Destination Internet Service</i> is off.
Application Category	Select application categories.
Application	Select applications.
URL Category	Select URL categories.
Users	Select users.
User Groups	Select user groups.
Apply Shaper	
Outgoing Interface	Select outgoing interfaces.
Traffic Shaping	Select traffic shapers.
Reverse Traffic Shaping	Select traffic shapers.
Per-IP Traffic Shaping	Select per IP traffic shapers.
Advanced Options	
class-id	Set the class ID (2 - 31, default = 0).
schedule	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 190](#).

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 208](#).



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.



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 Configurations > ips* or *Device Manager > [FortiGate_Name] > CLI Configurations > application* to view the modified ID for the particular VDOM.



If you create an object in the Global Database, and assign the object to a regular ADOM, you cannot delete the object from the Global Database. You must unassign the object from the regular ADOM before deleting it from the Global Database.



If a 6.0 ADOM contains a Wildcard FQDN addresses, upgrading to a 6.2 ADOM will assign a unique FQDN address to each wildcard object. This is only applicable if the FortiGate devices that are upgraded from FortiOS 6.0 to FortiOS 6.2.

Color code an object

Objects can be color coded for easy identification.

To color code an object:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
3. Select the object type that you will be creating. For example, view the interface by going to *Normalized Interface > Normalized Interface*.

The interface list is displayed in the content pane. The available interfaces are selectable on the content pane toolbar.

4. In the content pane, click *Create New*.
The *Create New Normalized Interface* pane opens.

5. Select or specify the values for the following fields:
 - Name - specify a name for the object.
 - Description - enter a brief description.
 - Color - click the black port to display the color options, and select a color for this object.
 - Default Mapping - select the check box to configure the default mapping for this object. See [Map a dynamic ADOM object on page 261](#)
 - Per-Platform mapping - switch the slider to *ON* for mapping this interface to a platform.
 - Per-Device Mapping - switch the slider to *ON* for mapping this interface to a FortiGate device. See [Interface mapping on page 272](#)
6. Click *OK*.



If a color code is not selected while creating an object, black is assigned as the default color.

Support FQDN address objects in firewall policies

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

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

The screenshot displays two sections of the FortiManager interface, labeled '6.0 ADOM' and '6.2 ADOM', showing the 'Object Configurations' for Firewall Addresses.

6.0 ADOM: The table lists several Firewall Address objects. Two objects are highlighted with red boxes: 'wildcard-address-qian' (type Wildcard FQDN, details Wildcard FQDN:qian.com) and 'wildcard-address-1' (type Wildcard FQDN, details Wildcard FQDN:*qa.local). A red arrow points from the 'wildcard-address-qian' row to the '6.2 ADOM' section.

6.2 ADOM: The table shows the same objects after the upgrade. The types have changed to 'FQDN'. The corresponding objects are 'wildcard-address-qian' (type FQDN, details FQDN:qian.com) and 'wildcard-address-1' (type FQDN, details FQDN:*qa.local). A red box highlights these two objects.

A red text annotation on the right side of the 6.2 ADOM section states: "After ADOM upgraded from v6.0 to v6.2, 'wildcard-fqdn' address changed to 'fqdn' type".

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

The screenshot displays the 'Object Configurations' for Firewall Addresses in a 6.2 ADOM, showing objects created during the upgrade process.

The table lists various Firewall Address objects. Two objects are highlighted with red boxes: 'fqdn-qian' (type FQDN, details FQDN:test.com) and '_upg_wild_fqdn-qian' (type FQDN, details FQDN:*qian.com). A red arrow points from the 'fqdn-qian' row to the '_upg_wild_fqdn-qian' row.

A red text annotation on the right side of the table states: "ADOM-v6.0 proxy policy used fqdn address, it created a new _upg_wild_fqdn address after ADOM upgraded to v6.2".

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

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

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

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

Create New Address

Address Name: newfqdn-wild-address

Color: [icon]

Type: FQDN

FQDN: *.fortinet.com

Interface: any

Static Route Configuration: OFF

Comments: [text area]

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

Advanced Options: >

Per-Device Mapping: OFF

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

Create New IPv4 Policy

Name: policy

Incoming Interface: any

Outgoing Interface: any

Source Internet Service: OFF

FSSO Groups: +

Source Address: all

Source User: +

Source User Group: +

Destination Internet Service: OFF

Destination Address: newfqdn-wild-address

Service: ALL

Schedule: always

Action: Deny | Accept | IPSEC

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

NAT: [checkbox]

Security Profiles: [checkbox]

Address List (selected: newfqdn-wild-address):

- login.microsoft.com
- login.microsoftonline.com
- login.windows.net
- newfqdn-wild-address
- none
- update.microsoft.com
- wildcard-address-1
- wildcard-address-qian
- wildcard-google.com

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 ⓘ

<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	

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

Name	Specify the name for the IPv6 address template.
IPv6 Address Prefix	Specify a prefix for the IPv6 address.
Subnet Segments	<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"> • country • state • city • site • lan • vlan
Create New	To create a new segment, you must delete one of the existing predefined segments if you already have six subnet segments. Click <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> .
Edit Segment	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> .

Edit Values for Segment

Click *Edit values for Segment*. Click + to add a row. Specify the *Name*, select the *Format*, and specify the *Value*. Click *OK*.

Delete

Select one or more subnet segments and click *Delete*.



The administrator can only define 6 segments and each segment can have a maximum of 16 bits. The administrator can toggle *Exclusive* to *Enable* to only choose from the predefined segments.



The length of the IPv6 address prefix must be greater than 1 bit.

Promote an Object to Global Database

Objects from an ADOM can be promoted to the Global Database for reuse.



Existing objects or newly created objects can be promoted to the Global Database.

To promote an object:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
3. Select the object type that you want to promote. For example, view the interface by going to *Normalized Interface > Normalized Interface*.

The interface list is displayed in the content pane. The available interfaces are selectable on the content pane toolbar.

4. Right-click the object and select *Promote to Global*.
5. If you want to rename the object, specify a new name in the *New Name* field. Leave the *New Name* field blank to keep the original name for the object.
6. Click *Promote*.
The object is now promoted to the Global Database.

Normalized interfaces

A normalized interface defines mapping rules. In mapping rules, interfaces are mapped per-device and/or per platform. You can have both per-device and per-platform mappings in a normalized interface. When the normalized interface is used in a policy, the per-device mappings have higher priority than per-platform mappings. The first match is used.

Default normalized interfaces are created when ADOMs are created. Default normalized interfaces contain a number of per-platform mapping rules for all FortiGate models. For example, port1 is mapped to port1, and WAN is mapped to WAN in default per-platform mapping rules. Default per-platform mapping rules allow you to install policies to FortiGates without first creating custom mapping rules.

You can map normalized interface names to different physical interface names on different FortiGate models. For example, you can map a normalized interface named *LAN* to port1 on one FortiGate and to port2 on another FortiGate.

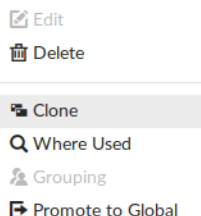
You can delete default normalized interfaces and create new normalized interfaces. You can also delete per-platform mappings in a default normalized interface.

Zones are created using *Device Manager*, and you can map zones to normalized interfaces. See also [Device zones on page 73](#).

You can also select normalized interfaces when you create virtual wire pairs.

This section contains the following topics:

- [Viewing normalized interfaces on page 252](#)
- [Viewing normalized interfaces mapped to devices on page 253](#)
- [Viewing where normalized interfaces are used on page 254](#)
- [Editing per-platform mapping rules on page 255](#)
- [Deleting per-platform mapping rules on page 256](#)
- [Deleting default normalized interfaces on page 257](#)
- [Creating normalized interfaces on page 258](#)
- [Creating virtual wire pairs on page 260](#)

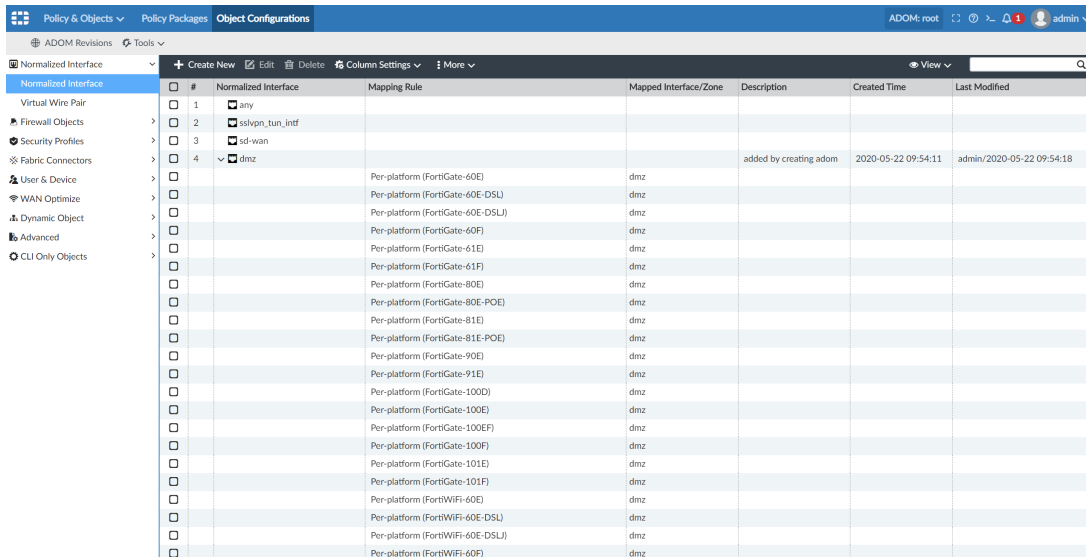


Viewing normalized interfaces

You can view all normalized interfaces and their mapping rules. You can also collapse or expand all mapping rules and mapped interface/zones for normalized interfaces.

To view normalized interfaces:

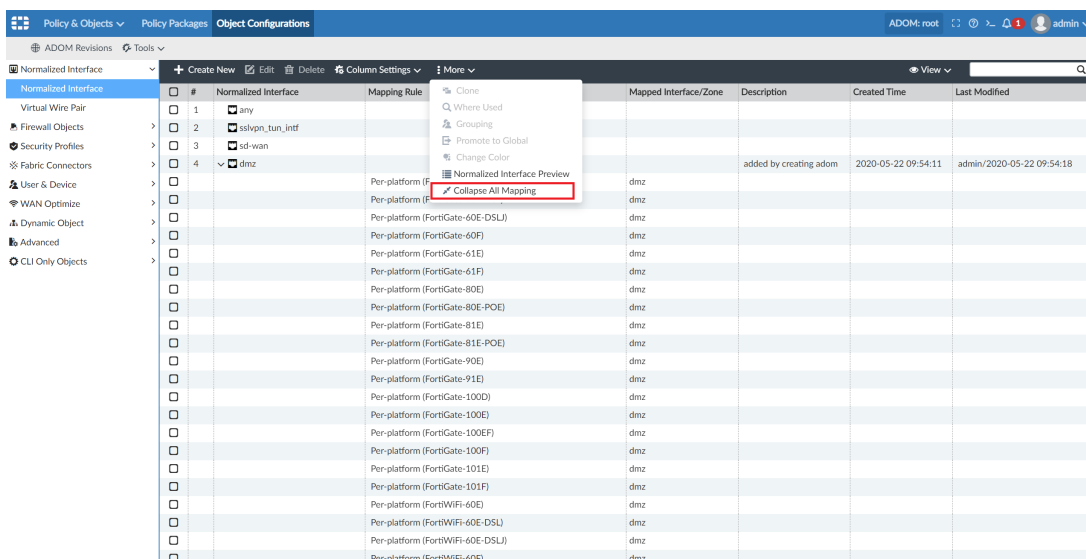
1. Go to *Policy & Objects > Object Configurations > Normalized Interface > Normalized Interface* pane.
The list of normalized interfaces are displayed in the content pane.
In the following example, the normalized interface named *dmz* is displayed, and it contains per-platform mappings for a number of FortiGate devices. The *dmz* normalized interface was added when an ADOM was created.



#	Normalized Interface	Mapping Rule	Mapped Interface/Zone	Description	Created Time	Last Modified
1	any					
2	sslvpn_tun_intf					
3	id-wan					
4	dmz			added by creating adom	2020-05-22 09:54:11	admin/2020-05-22 09:54:18
		Per-platform (FortiGate-60E)	dmz			
		Per-platform (FortiGate-60E-DSL)	dmz			
		Per-platform (FortiGate-60E-DSLJ)	dmz			
		Per-platform (FortiGate-60F)	dmz			
		Per-platform (FortiGate-61E)	dmz			
		Per-platform (FortiGate-61F)	dmz			
		Per-platform (FortiGate-80E)	dmz			
		Per-platform (FortiGate-80E-POE)	dmz			
		Per-platform (FortiGate-81E)	dmz			
		Per-platform (FortiGate-81E-POE)	dmz			
		Per-platform (FortiGate-90E)	dmz			
		Per-platform (FortiGate-91E)	dmz			
		Per-platform (FortiGate-100D)	dmz			
		Per-platform (FortiGate-100E)	dmz			
		Per-platform (FortiGate-100EF)	dmz			
		Per-platform (FortiGate-100F)	dmz			
		Per-platform (FortiGate-101E)	dmz			
		Per-platform (FortiGate-101F)	dmz			
		Per-platform (FortiWiFi-60E)	dmz			
		Per-platform (FortiWiFi-60E-DSL)	dmz			
		Per-platform (FortiWiFi-60E-DSLJ)	dmz			
		Per-platform (FortiWiFi-60F)	dmz			

2. From the *More* menu, select *Collapse All Mapping*.

The list of normalized interfaces is displayed, but the mapping rules and mapped interface/zone information is hidden.



#	Normalized Interface	Mapping Rule	Mapped Interface/Zone	Description	Created Time	Last Modified
1	any					
2	sslvpn_tun_intf					
3	id-wan					
4	dmz			added by creating adom	2020-05-22 09:54:11	admin/2020-05-22 09:54:18
		Per-platform (FortiGate-60E)	dmz			
		Per-platform (FortiGate-60E-DSL)	dmz			
		Per-platform (FortiGate-60E-DSLJ)	dmz			
		Per-platform (FortiGate-60F)	dmz			
		Per-platform (FortiGate-61E)	dmz			
		Per-platform (FortiGate-61F)	dmz			
		Per-platform (FortiGate-80E)	dmz			
		Per-platform (FortiGate-80E-POE)	dmz			
		Per-platform (FortiGate-81E)	dmz			
		Per-platform (FortiGate-81E-POE)	dmz			
		Per-platform (FortiGate-90E)	dmz			
		Per-platform (FortiGate-91E)	dmz			
		Per-platform (FortiGate-100D)	dmz			
		Per-platform (FortiGate-100E)	dmz			
		Per-platform (FortiGate-100EF)	dmz			
		Per-platform (FortiGate-100F)	dmz			
		Per-platform (FortiGate-101E)	dmz			
		Per-platform (FortiGate-101F)	dmz			
		Per-platform (FortiWiFi-60E)	dmz			
		Per-platform (FortiWiFi-60E-DSL)	dmz			
		Per-platform (FortiWiFi-60E-DSLJ)	dmz			
		Per-platform (FortiWiFi-60F)	dmz			

3. From the *More* menu, select *Expand All Mapping*.

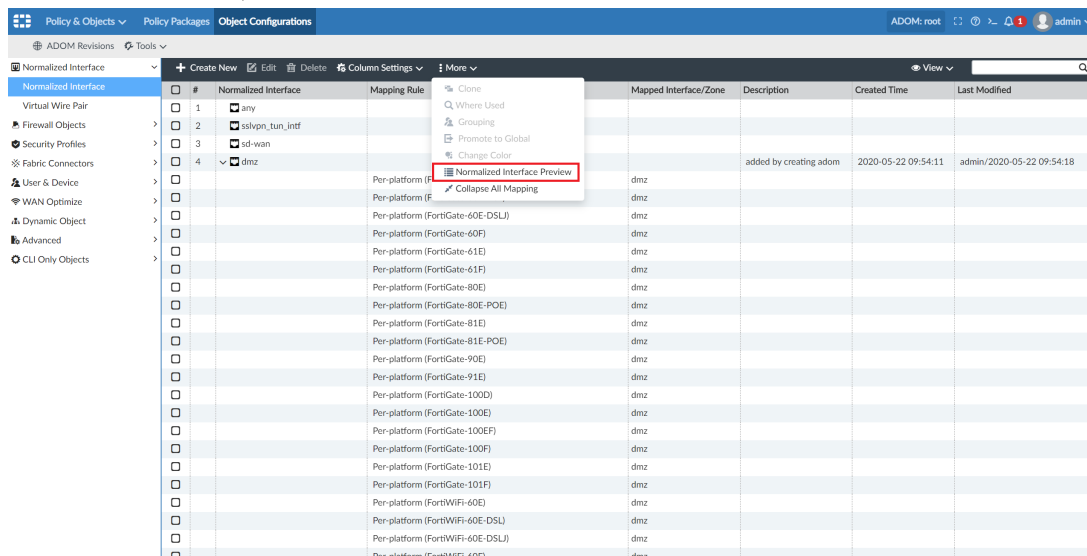
The list of normalized interfaces and the mapping rules as well as mapped interface/zone information are displayed.

Viewing normalized interfaces mapped to devices

For each managed FortiGate device, you can view the number of normalized interfaces mapped to it.

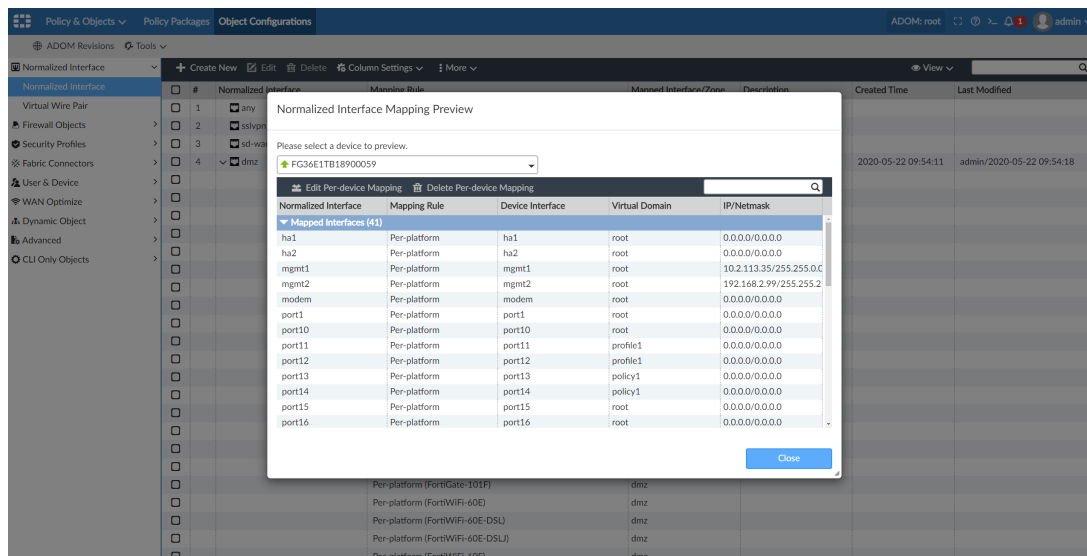
To view normalized interfaces mapped to devices:

1. Go to **Policy & Objects > Object Configurations > Normalized Interface > Normalized Interface**.
2. From the **More** menu, select **Normalized Interface Preview**.



The **Normalized Interface Mapping Preview** window is displayed.

3. From the drop-down list, select a device.
The mapping preview for the selected device is displayed.



Scroll to the bottom to view unmapped interfaces.

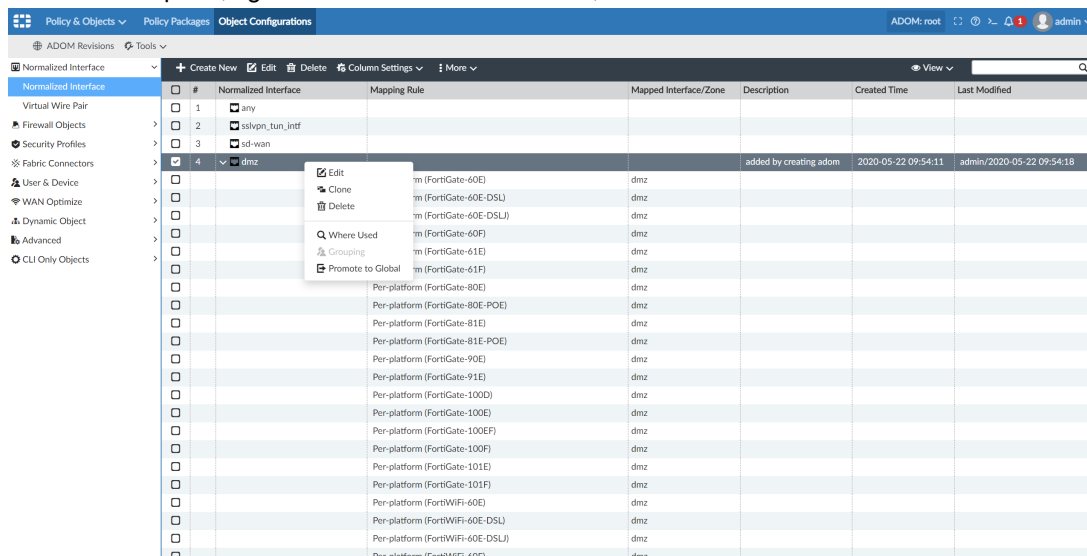
4. (Optional) Select a mapping, and click **Edit Per-device Mapping** or **Delete Per-device Mapping**.
5. Click **Close**.

Viewing where normalized interfaces are used

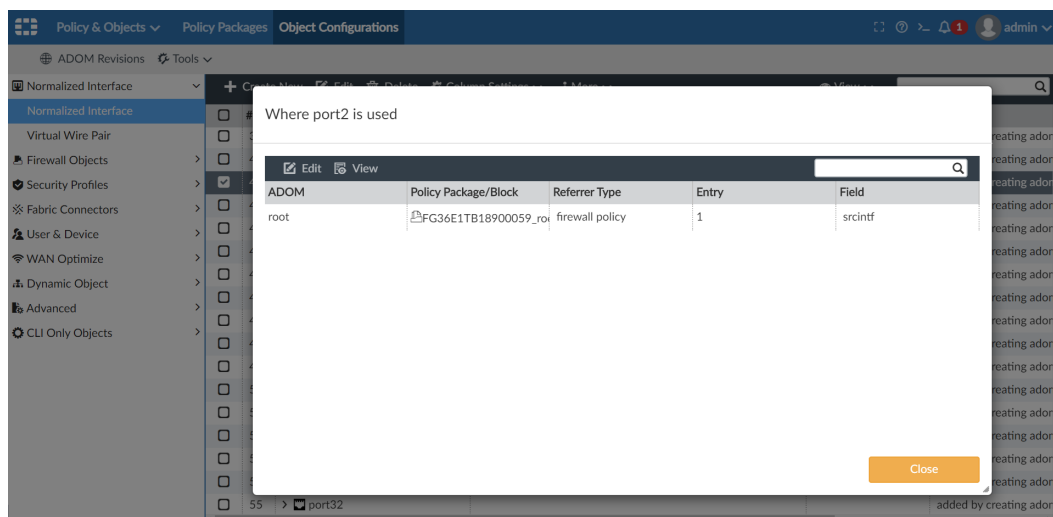
You can view what policy packages use a normalized interface.

To view where normalized interfaces are used:

1. Go to *Policy & Objects > Object Configurations > Normalized Interface > Normalized Interface*.
2. In the content pane, right-click a normalized interface, and select *Where Used*.



The *Where <normalized interface name> is used* dialog box is displayed. The name of the policy package that uses the selected normalized interface is identified.



3. Click *Close*.

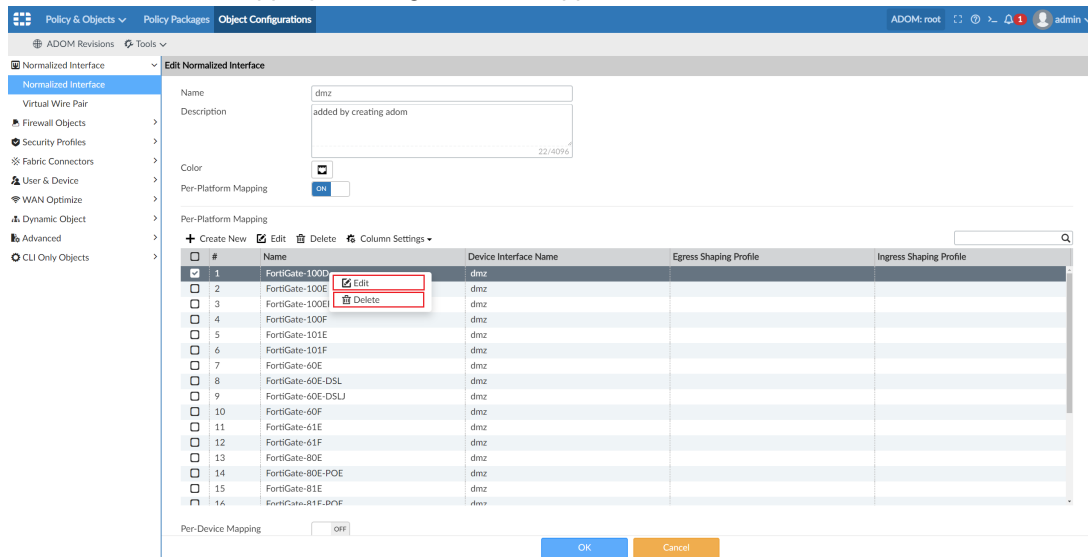
Editing per-platform mapping rules

You can edit per-platform mapping rules in normalized interfaces.

When you change mapping rules, the object is modified, and the status for any policy package that uses the modified object changes to *Modified* on the *Device Manager* pane. You must reinstall the affected policy packages again to provide the changes to the device.

To edit per-platform mapping rules:

1. Go to *Policy & Objects > Object Configurations > Normalized Interface > Normalized Interface*.
2. In the content pane, right-click a normalized interface, and select *Edit*.
The *Edit Normalized Interface* pane appears.
3. In the *Per-Platform Mapping* table, right-click a mapped device, and select *Edit*.



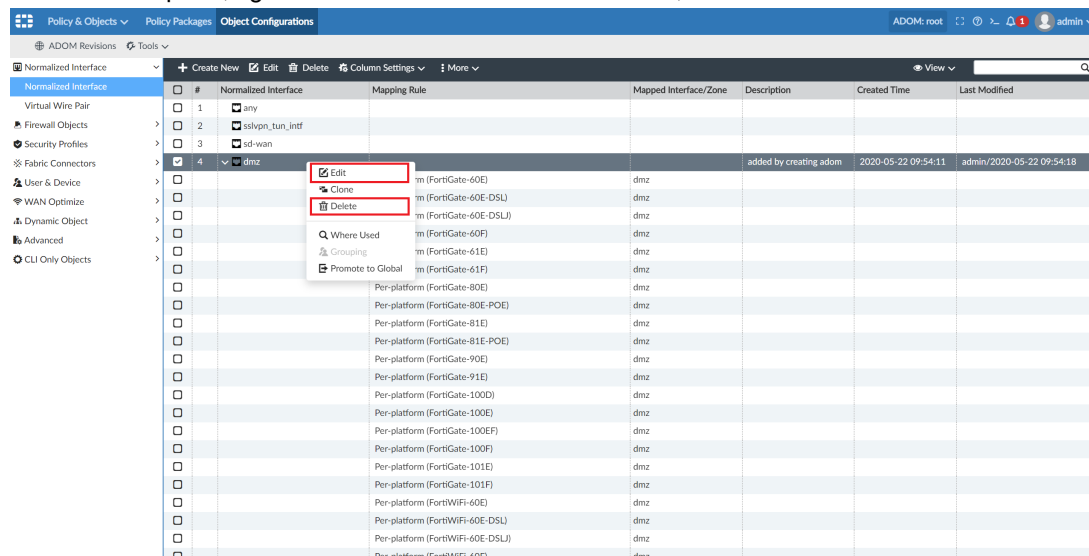
4. Edit the options, and click *OK*.
The mapping rule is saved.
5. Click *OK*.
The normalized interface is saved.

Deleting per-platform mapping rules

A number of normalized interfaces are created by default when an ADOM is created. You can edit default normalized interfaces to delete per-platform mapping rules.

To delete per-platform mapping rules:

1. Go to *Policy & Objects > Object Configurations > Normalized Interface > Normalized Interface*.
2. In the content pane, right-click a default normalized interface, and select *Edit*.



The *Edit Normalized Interface* pane appears.

3. In the *Per-Platform Mapping* table, select a mapped device, and click *Delete*.
4. Click *OK*.

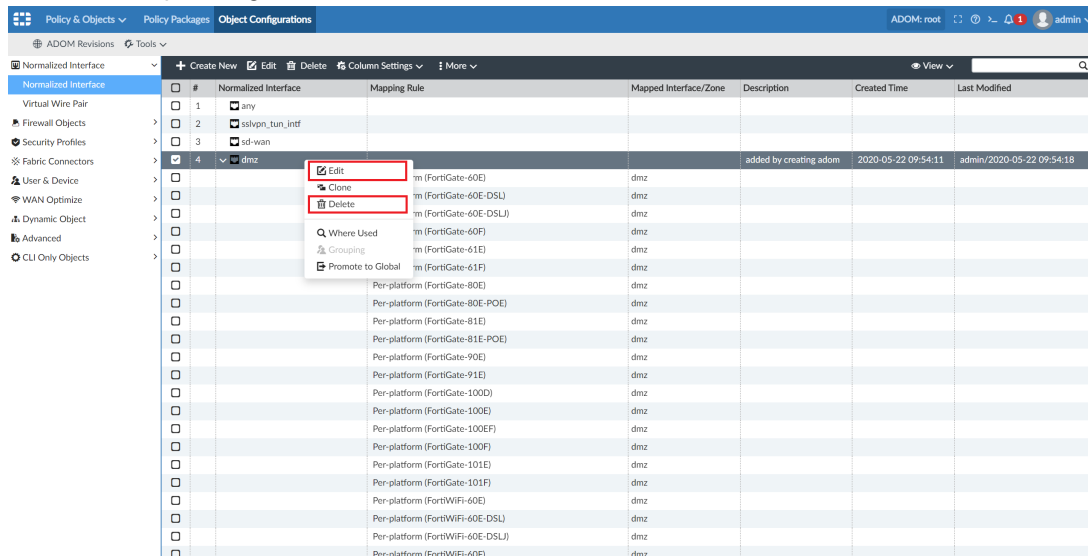
The normalized interface is saved.

Deleting default normalized interfaces

You can delete the default normalized interfaces that are automatically created when ADOMs are created.

To delete default normalized interfaces:

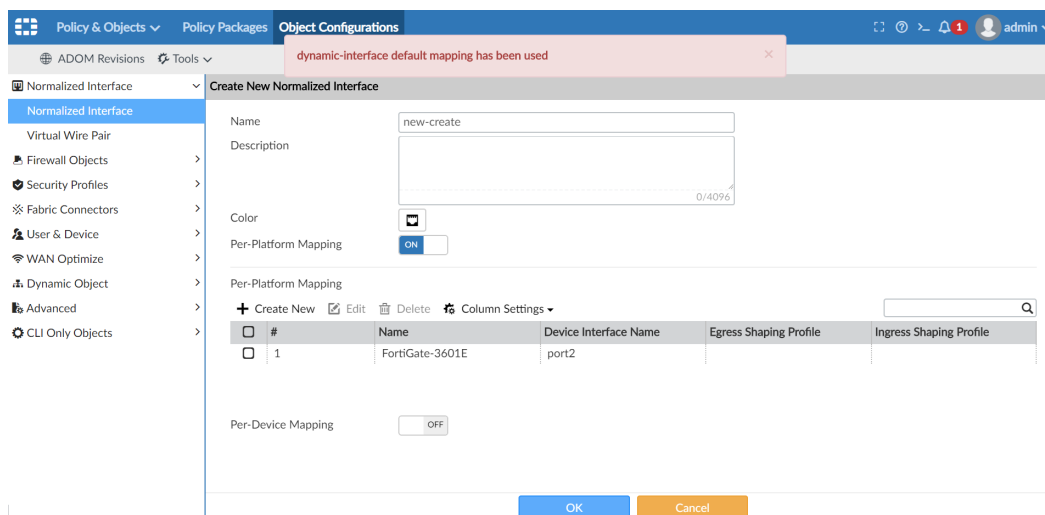
1. Go to **Policy & Objects > Object Configurations > Normalized Interface > Normalized Interface**.
2. In the content pane, right-click a normalized interface, and select **Delete**.



3. Click **OK**.
The normalized interface is deleted.

Creating normalized interfaces

If you want to use a physical interface name in a per-platform mapping rule in a normalized interface, you must first delete the default per-platform mapping rule from the default per-platform interface. Otherwise the *dynamic-interface default mapping has been used* error is displayed, and you cannot create the normalized interface.

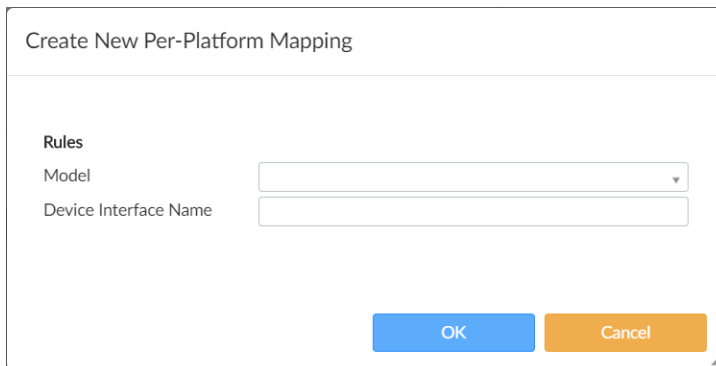


To delete the default per-platform mapping rule:

1. Go to *Policy & Objects > Object Configurations > Normalized Interface > Normalized Interface*.
2. In the content pane, right-click the default per-platform normalized interface, and select *Edit*.
The *Edit Normalized Interface* page appears.
3. In the *Per-Platform Mapping* table, right-click the default per-platform mapping rule, and select *Delete*.
4. Click *OK*.

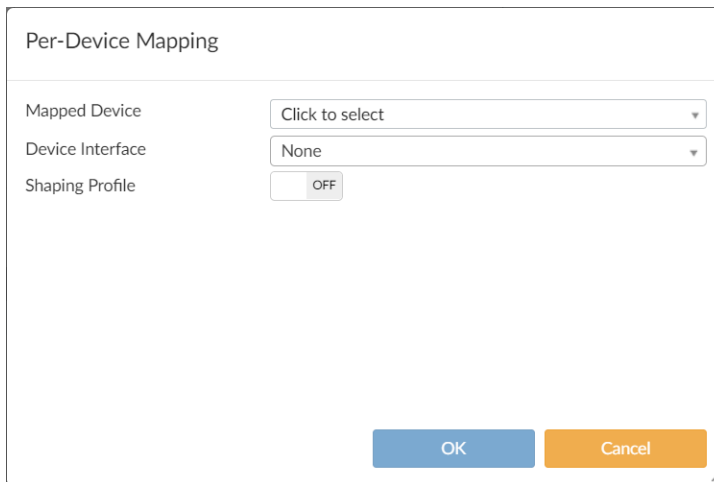
To create normalized interfaces for zones:

1. Go to *Policy & Objects > Object Configurations > Normalized Interface > Normalized Interface*.
2. Click *Create New*.
The *Create New Normalized Interface* pane is displayed.
3. Complete the *Name*, *Description*, and *Color* options.
4. Add a per-platform mapping.
 - a. Toggle *Per-Platform Mapping* to *ON*.
The *Per-Platform Mapping* table is displayed.
 - b. Click *Create New*.
The *Create new Per-Platform Mapping* dialog box is displayed.



The dialog box titled "Create New Per-Platform Mapping" contains a "Rules" section with two input fields: "Model" (a dropdown menu) and "Device Interface Name" (a text box). At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (orange).

- c. In the *Model* list, select the model for which you created the zone.
 - d. In the *Device Interface Name* box, type the name of the interface.
 - e. Click *OK*.
5. Add a per-device mapping.
 - a. Toggle *Per-Device Mapping* to *ON*.
The *Per-Device Mapping* table is displayed.
 - b. Click *Create New*.
The *Create new Per-Device Mapping* dialog box is displayed.



Per-Device Mapping

Mapped Device: Click to select

Device Interface: None

Shaping Profile: OFF

OK Cancel

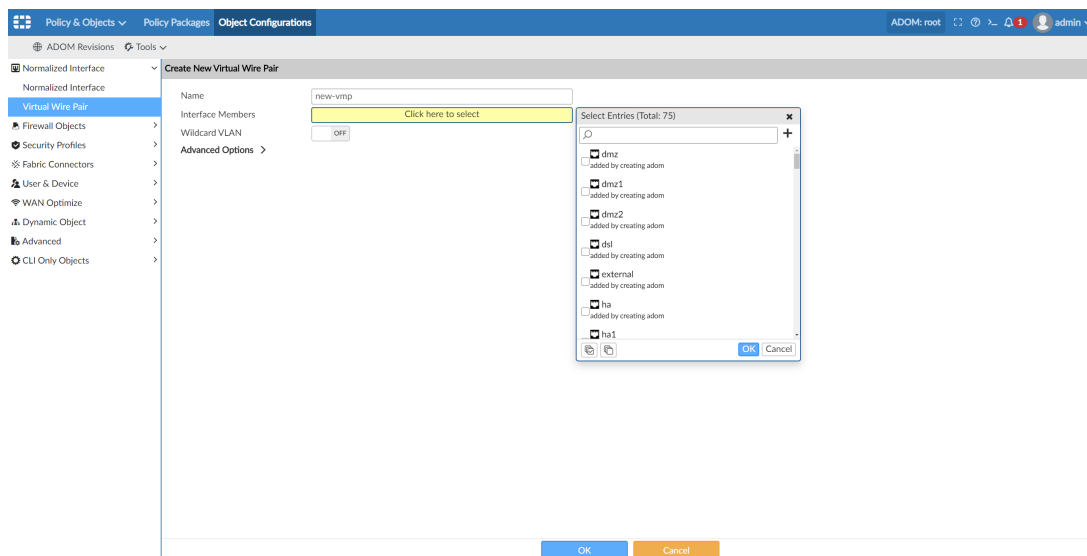
- c. In the *Mapped Device* list, select the model for which you created the zone.
- d. In the *Device Interface* list, select the zone.
- e. Click **OK**.
6. Click **OK**.

Creating virtual wire pairs

You select normalized interfaces when you create virtual wire pairs.

To create virtual wire pairs:

1. Go to *Policy & Objects > Object Configurations > Normalized Interface > Virtual Wire Pair*.
2. Click **Create New**.
The *Create New Virtual Wire Pair* pane is displayed.
3. In the *Name* box, type a name for the virtual wire pair.
4. Click the *Interface Members* box.
The list of normalized interfaces is displayed.



The screenshot shows the FortiManager interface with the **Policy & Objects** tab selected. The left sidebar shows the navigation tree with **Virtual Wire Pair** selected under **Normalized Interface**. The main pane displays the **Create New Virtual Wire Pair** configuration. The **Name** field is set to 'new-vwmp'. The **Interface Members** field has a yellow button that says 'Click here to select'. The **Wildcard VLAN** field is set to 'OFF'. The **Advanced Options** section is expanded. A **Select Entries** dialog box is open, showing a list of normalized interfaces: dmz, dmz1, dmz2, dsl, external, and ha1. Each entry is preceded by a checkbox and the text 'added by creating adom'. The **OK** button is highlighted in blue.

5. Select one or more normalized interfaces, and click *OK*.
6. Complete the remaining options, and click *OK*.

Map a dynamic ADOM object

The devices and VDOMs to which a global object is mapped can also be viewed from the object list. You can add an object to groups and enable dynamic mapping. These options are not available for all objects.

When the *Dynamic Mapping* option is available, select *Create New* to configure the dynamic mapping.

To configure a dynamic mapping via a CLI script, the configuration for the mapping must be defined in the dynamic object under the *config dynamic_mapping* sub-tree. The CLI script must be run on a policy package instead of the device database. For information on running CLI scripts, see [Scripts on page 117](#)



Default mapping is only used when there is no per-device mapping for a particular device. You must have either a per-device mapping or a default mapping in a policy package. Otherwise, the policy package installation will fail.

When you import a policy package, a per-device mapping is usually added when the object is already used by a FortiGate.

Examples:

Example 1: Dynamic VIP

```
config firewall vip
  edit "vip1"
  ...
  config dynamic_mapping
    edit "FW60CA3911000089"- "root"
      set extintf "any"
      set extip 172.18.26.100
      set mappedip 192.168.3.100
      set arp-reply disable
    next
  end
end
```

Example 2: Dynamic Address

```
config firewall address
  edit "address1"
  ...
  config dynamic_mapping
    edit "FW60CA3911000089"- "root"
      set subnet 192.168.4.0 255.255.255.0
    next
  end
end
```

Example 3: Dynamic Interface

```
config dynamic interface
```

```
...
config dynamic_mapping
  edit "FW60CA3911000089"-"root"
    set local-intf internal
    set intrazone-deny disable
  next
end
end
```

Map a dynamic device object

Dynamic device objects can be mapped to FortiGate devices using per-device mapping.

To view the dynamic device objects:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
3. Go to *Tools > Display Options*.
4. Select *Dynamic Object* and click *OK*.

The following device objects are available:

- [Create a Local Certificate on page 262](#)
- [Create a VPN Tunnel on page 263](#)
- [Create Multicast Interface on page 264](#)



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

Q

▢

▲

Name

VDOM

Details

OK

Cancel

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

Name	Specify the name for the Dynamic Local Certificate.
Description	Specify a description.
Per-Device Mapping	Toggle Per-Device Mapping to <i>ON</i> . Click <i>Create New</i> . Select the <i>Mapped Device</i> and <i>VPN Local Certificate</i> . Click <i>OK</i> .

Create a VPN Tunnel

Create a VPN tunnel to sync with devices using per-device mapping.

To create a VPN tunnel:

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

Create New Dynamic VPN Tunnel

Name

Description

Per-Device Mapping

+ Create New

Edit

Delete

Column Settings

ON

Q

▢

▲

Name

VDOM

Details

OK

Cancel

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

Name	Specify the name for the Dynamic VPN Tunnel.
Description	Specify a description.
Per-Device Mapping	Toggle Per-Device Mapping to <i>ON</i> . Click <i>Create New</i> . Select the <i>Mapped Device</i> and <i>VPN Tunnel</i> . Click <i>OK</i> .

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

Per-Device Mapping

+ 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*:

Name	Specify the name for the Dynamic Multicast Interface.
Description	Specify a description.
Default Mapping	Toggle Per-Device Mapping to <i>ON</i> and specify the interface for default mapping.
Per-Device Mapping	Toggle Per-Device Mapping to <i>ON</i> . Click <i>Create New</i> . Select the <i>Mapped Device</i> and <i>Interface</i> . Click <i>OK</i> .

Map a dynamic device group

When you create and edit a device group, you can choose whether to use the FortiManager ADOM or the FortiGate device to manage members for the device group.

To create a dynamic device group:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations > User & Device > Customer Devices & Groups*.
3. From the *Create New* menu, select *Device Group*.
4. Complete the following options, then click *OK*.

Group Name	Type a name for the device group.
-------------------	-----------------------------------

Managed on ADOM	Specify whether to use the FortiManager ADOM or the FortiGate device to manage members for the device group. When you select the <i>Managed on ADOM</i> checkbox, the FortiManager ADOM manages members for the object, and you must specify members for the object. When you clear the <i>Manage on ADOM</i> checkbox, the FortiGate device manages members for the object, and you must specify members by using FortiGate, not FortiManager.
Members	Select members for the device group.
Comments	(Optional) Type a comment.
Per-Device Mapping	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 266](#).

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.

Name	Category	Technology	Popularity	Risk
126.Mail	Email	Browser-Based	★★★★★	Medium
1koun	Video/Audio	Client-Server	★★★★★	Medium
1und1.Mail	Email	Browser-Based	★★★★★	Medium
2ch	Social.Media	Browser-Based	★★★★★	Elevated
2ch_Post	Social.Media	Browser-Based	★★★★★	Elevated
360.Safeguard.Update	Update	Client-Server	★★★★★	Low
360.Yunpan	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium
360.Yunpan_File.Download	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium
360.Yunpan_File.Upload	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium
360.Yunpan_Login	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium
3PC	Network.Service		★★★★★	Elevated
4shared	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium
4shared_File.Download	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium
4shared_File.Upload	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium
5ch	Social.Media	Browser-Based	★★★★★	Elevated
5ch_Post	Social.Media	Browser-Based	★★★★★	Elevated

[Total: 3266]

Export to CSV Use Selected Signatures Cancel

6. Click *Export to CSV*.

The *Export to CSV* dialog box is displayed.

File Name: App_Signatures_root_2018-01-31-155641.csv

Options:

☒ Export all columns

☐ Export customized columns only

Download Cancel

7. (Optional) Change the file name.
8. Select whether to export all columns or only customized columns.
9. Click *Download*.

CLI Configurations

FortiManager adds the ability to configure objects that are available only via the FortiOS command line interface, as well as settings that are not available in the FortiManager GUI.

FortiToken configuration example

To configure FortiToken objects for FortiToken management:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
3. Go to *User & 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 195](#).
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*.



When you upgrade an ADOM from 5.4 or 5.6 to 6.0.0 and later, objects are automatically moved from *Policy & Objects > Object Configurations > User & Device > Single Sign-On* to *Policy & Objects > Object Configurations > Fabric Connectors > SSO/Identity*.

To get groups from FSSO:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
3. Expand *Fabric Connectors*, and select *SSO/Identity*.
4. Click *Create New > Fortinet Single Sign-On Agent* from the drop-down list.
5. Enter a unique name for the agent in the *Name* field.
6. Enter the IP address or name, password, and port number of the FSSO servers in the FSSO Agent field. Add and remove servers as needed by clicking the *Add* and *Remove* icons at the end of the rows.
7. Select *Collector Agent* in the *User Group Source* field.

- Click *Apply & Refresh*. The *Retrieve FSSO User Groups* dialog box will open.

Retrieve FSSO User Groups

System will connect to the specified FSSO agent directly to retrieve FSSO user groups. Click "Next" to continue.

Next
Cancel

- Click *Next*. The groups are retrieved from the FSSO.
- 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:

- Ensure you are in the correct ADOM.
- Go to *Policy & Objects > Object Configurations*.
- Expand *Fabric Connectors*, and select *SSO/Identity*.
- Click *Create New > Fortinet Single Sign-On Agent* from the drop-down list.

Create New Fortinet Single Sign-On Agent

Name	<input style="width: 90%;" type="text"/>		
Type	<div style="border: 1px solid #ccc; padding: 2px;">Active Directory / FortiAuthenticator</div>		
FSSO Agent	IP/Name	Password	Port
	<input style="width: 80%;" type="text"/>	<input style="width: 80%;" type="password"/>	<div style="border: 1px solid #ccc; padding: 2px;">8000</div> + -
	<input style="width: 80%;" type="text"/>	<input style="width: 80%;" type="password"/>	<div style="border: 1px solid #ccc; padding: 2px;">8000</div> + -
User Group Source	<div style="display: flex; gap: 5px;"> <div style="border: 1px solid #ccc; padding: 2px;">Collector Agent</div> <div style="border: 1px solid #ccc; padding: 2px;">Via FortiGate</div> <div style="background-color: #007bff; color: white; padding: 2px 5px; border-radius: 3px;">Local</div> </div>		
LDAP Server	<div style="border: 1px solid #ccc; padding: 2px;">None</div>		
Proactively Retrieve from LDAP Server	<div style="display: flex; align-items: center;"> <div style="width: 15px; height: 15px; background-color: #007bff; margin-right: 5px;"></div> <div style="border: 1px solid #ccc; padding: 2px;">ON</div> </div>		
Search Filter	<div style="border: 1px solid #ccc; padding: 2px;">(objectCategory=group)</div>		
Interval (minutes)	<div style="border: 1px solid #ccc; padding: 2px;">180</div>		
SSL	<div style="display: flex; align-items: center;"> <div style="width: 15px; height: 15px; background-color: #6c757d; margin-right: 5px;"></div> <div style="border: 1px solid #ccc; padding: 2px;">OFF</div> </div>		
Per-Device Mapping	<div style="display: flex; align-items: center;"> <div style="width: 15px; height: 15px; background-color: #6c757d; margin-right: 5px;"></div> <div style="border: 1px solid #ccc; padding: 2px;">OFF</div> </div>		
Advanced Options >			

- Enter a unique name for the agent in the *Name* field.
- Select *Local* in the *User Group Source*.
- Select an LDAP server from the drop-down list. LDAP Servers can be added and configured from *User & Device > LDAP Servers*.
- Toggle *Proactively Retrieve from LDAP Server* to ON.
- Specify the value for the *Search Filter* and the *Interval* in minutes.
- For the Select LDAP Groups option, select *Remote Server*. Alternatively, select *Manually Specify* and specify the group names.
- 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 90](#).

1. Go to *Policy & Objects > Object Configurations*.
2. Expand *Fabric Connectors*, and select *SSO/Identity*.
3. Click *Create New > Fortinet Single Sign-On Agent* from the drop-down list. The *Create New Fortinet Single Sign-On Agent* window opens.

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

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

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

Create New Fortinet Single Sign-On Agent

Name

FSSO Agent

IP/Name	Password	Port	
10.222.788.878	••••••••	8000	+
<input type="text"/>	••••••••	8000	+

Select FSSO Groups ☐ From FSSO Agents ☒ Via FortiGate

User Groups

CN=a'test,DC=FSSOtest,DC=com
 CN=qa01.fmg,CN=Users,DC=FSSOtest,DC=com
 CN=qa03,CN=Users,DC=FSSOtest,DC=com
 CN=qa04,CN=Users,DC=FSSOtest,DC=com
 OU=EQUIPE,DC=FSSOtest,DC=com

LDAP Server

Per-Device Mapping

Advanced Options >

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



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

To get groups from AD:

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

Interface mapping

After creating an interface on the FortiManager, an interface mapping must be created so that the new interface can be used when creating policies. To do this, create a new dynamic interface with per-device mapping.

To create a new dynamic interface with per-device mapping:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
3. Go to *Normalized Interface > Normalized Interface* and click *Create New*.
4. Enter a name and description for the interface.
5. Turn on *Per-Device Mapping*.
6. Click *Create New*. The *Per-Device Mapping* dialog box opens.

7. Select the device or VDOM in the *Mapped Device* field, select the interface in the *Device Interface* field, then click *OK*.
8. Click *OK* to create the new dynamic interface object.
The mapped interface can now be used when creating policies.

VIP mapping

Normally, Virtual IP (VIP) objects map to a single interface, or *ANY*, just as with FortiOS. In the special case where the interface that the VIP is bound to belongs to a zone, FortiManager handles importing and installing the object in a unique way.

When importing a policy package, the VIP is bound to the zone instead of the interface. If per-device mapping is enabled for the VIP, FortiManager automatically adds dynamic mapping for that device that maps the VIP to the specific interface. To use the VIP on another FortiGate, you can add an interface mapping entry for the other FortiGate. The zone acts as filter, limiting the interfaces that can be selected. That is, you can only select an external interface that is a member of the selected zone.

FortiManager binds the VIP to a zone because it needs to know which policies the VIP could be applied to. FortiGate devices use different logic because they already know the zone membership.

In FortiOS, VIPs can only be bound to an interface, and not a zone. Consequently, if there is no matching per-device mapping, FortiManager will convert the binding to *ANY* when installing configuration changes to FortiGate. Depending on the circumstance, this can be avoided by:

- Leaving per-device mapping enabled on the VIP at the ADOM, and letting FortiManager add the required per-device mappings.
- If you are configuring FortiManager to start using the VIP on other FortiGates, adding the per-device mappings manually.

Modify existing interface-zone mapping

Interfaces mapped to a zone locally on FortiGate devices are not visible in Device Manager on FortiManager. It is recommended to create objects in FortiManager instead of creating it on FortiGate devices locally. If an interface is already mapped to a zone in FortiGate, it must be unmapped first. A zone must be created in FortiManager, added to a policy and installed to FortiGate. For convenience and ease of use, it is better to manage Object Configuration and Interface Mapping from FortiManager.

If an Interface is mapped to a Zone in FortiGate:

1. Log on to the FortiGate device.
2. Delete the Interface/Zone mapping from *Interfaces > [Interface_Name] > Delete*.
3. Log on to FortiManager.
4. 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. After the profile is created, you can assign it to an interface.

To create a new shaping profile:

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

Create New Shaping Profile

Name:

Default Shaping Group (2-31):

Comments: 0/1023

Additional Shaping Groups

<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

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

Name	Specify the name for the shaping profile.
Default Shaping Group	Specify a default shaping group between 2-31.
Comments	Optionally enter comments about the shaping profile.
Additional Shaping Groups	Click <i>Create New</i> . Specify the <i>Shaping Group</i> , <i>Guaranteed Bandwidth(%)</i> , <i>Maximum Bandwidth(%)</i> and <i>Priority</i> . Click OK .

6. Assign the shaping profile to an interface. See [Assigning a shaping profile on page 275](#).



After shaping profiles are defined, they can be assigned to each ADOM interface you want to do traffic shaping for egress. The shaping profile can be set as default as well as in dynamic mapping. Any changes to the shaping profile is applied to the FortiGate devices dynamically.

Assigning a shaping profile

You can assign an interface-based shaping profile for each device.



To display this option, go to *Device Manager > Device & Groups*. From the dashboard toolbar, select *Display Options*, and then select the *Interface* checkbox.

To assign a shaping profile:

- Go to *Device Manager > Device & Groups*.
 - In the tree menu, select the device group.
 - Below the tree menu, select a device.
- In the dashboard toolbar, go to *System > Interface*.
- Select an interface from the list. The *Edit Interface* page opens.
- Toggle *Shaping Profile* to **ON**. The *Egress* and *Ingress* dropdowns are displayed.
- Select a shaping profile from the dropdown, and then click **OK**.

Viewing the traffic shaping monitor

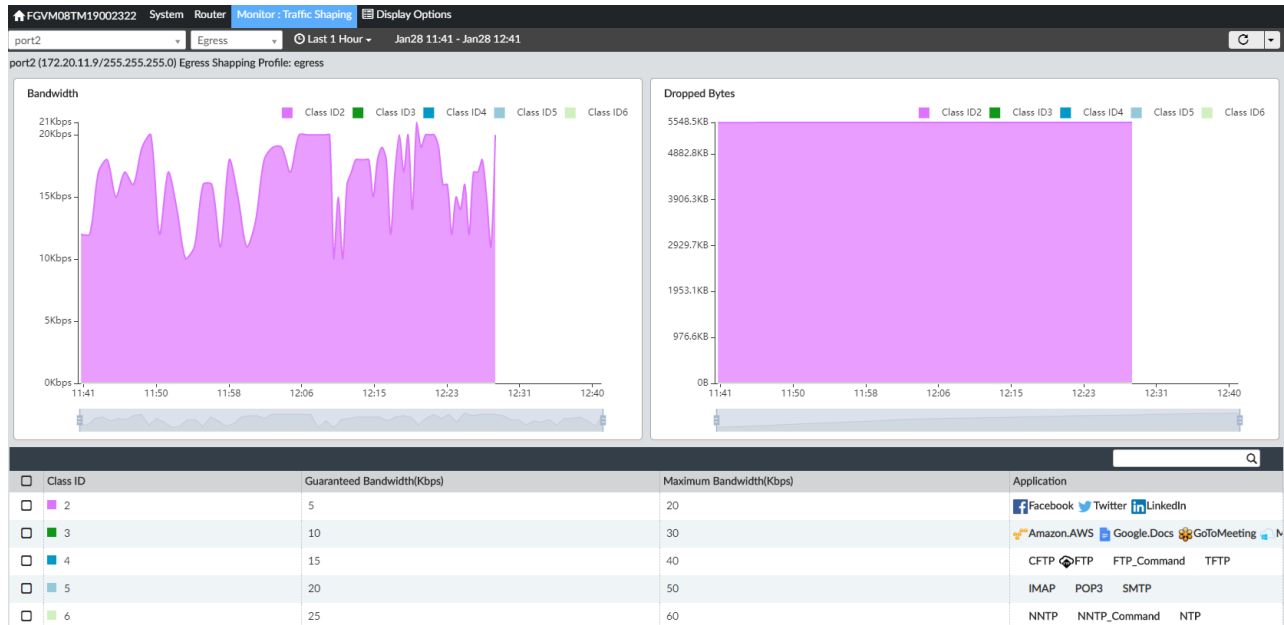
You can view the *Traffic Shaping* monitor in the *Device & Groups* pane of the *Device Manager*.



To display this option, go to *Device Manager > Device & Groups*. From the dashboard toolbar, select *Display Options*, and then select the *Traffic Shaping* checkbox.

To view the Traffic Shaping monitor:

1. Go to *Device Manager > Device & Groups*.
 - a. In the tree menu, select the device group.
 - b. Below the tree menu, select a device.
2. In the dashboard toolbar, go to *Monitor > Traffic Shaping*.
3. From the dropdown, select an interface.
 - The *Bandwidth* chart shows the bandwidth for each class.
 - The *Dropped Bytes* chart shows the statistics for bytes dropped after shaping is applied.
 - The table below the charts contains a legend for all class IDs and shows which applications are affected.



Intrusion Prevention filtering options

Intrusion Prevention (IPS), detects and blocks network-based attacks. You can configure IPS sensors based on IPS signatures, IPS filters, outgoing connections to botnet sites, and rate-based signatures. FortiManager includes eight preloaded IPS sensors:

- *all_default*
- *all_default_pass*
- *default*
- *high_security*
- *protect_client*
- *protect_email_server*
- *protect_http_server*
- *wifi-default*

You can customize these sensors, or you can create your own and apply it to a firewall policy.



This functionality requires a subscription to FortiGuard IPS Service.

Hold-time

The hold-time option allows you to set the amount of time that signatures are held after a FortiGuard IPS signature update per VDOM. During the holding period, the signature's mode is *monitor*. The new signatures are enabled after the hold-time, to avoid false positives.

The hold-time can be from 0 days and 0 hours (default) up to 7 days, in the format ##d##h.

To delay an IPS signature activation:

1. Go to *Device Manager > Device & Groups*.
2. Select a managed device.
3. In the toolbar, click *CLI Configuration*. To display the menu, see [CLI Configurations menu on page 70](#).
4. In configurations menu, go to *System > IPS*. The *system ips* dialog box is displayed.
5. Ensure *override-signature-hold-by-id* is enabled.
6. In the *signature-hold-time* field, enter the number of days or hours hold and monitor the IPS signatures.

CVE pattern

The CVE pattern option allows you to filter IPS signatures based on CVE IDs or with a CVE wildcard, ensuring that any signatures tagged with that CVE are automatically included.

To add an IPS CVE filter:

1. Go to *Policy & Objects > Object Configurations > Security Profiles > Intrusion Prevention*.
2. Create a new profile or select the profile you want to update.
3. In the *IPS Signatures and Filters* section, create a new filter or select a filter to update. The *Create New IPS Signatures and Filters* dialog box is displayed.
4. Add the CVE filter.
 - a. Click the *Filter* icon.
 - b. Click *Add Filter > CVE ID*.
 - c. Enter the CVE ID, then click *Use Filters*, and click *OK*.
5. Click *OK*.

ADOM revisions

ADOM revision history allows you to maintain a revision of the policy packages, objects, and VPN console settings in an ADOM. Revisions can be automatically deleted based on given variables, and individual revisions can be locked to prevent them being automatically deleted.

To configure ADOM revisions, go to *Policy & Objects*, and click *ADOM Revisions*.

This page displays the following:

ID	The ADOM revision identifier.
Name	The name of the ADOM revision. This field is user-defined when creating the ADOM revision. A green lock icon will be displayed beside the ADOM revision name when you have selected <i>Lock this revision from auto deletion</i> .
Created by	The administrator that created the ADOM revision.
Created Time	The ADOM revision creation date and time.
Comment	Optional comments typed in the <i>Description</i> field when the ADOM revision was created.

The following options are available:

Create New	Select to create a new ADOM revision.
Edit	Right-click on a revision in the table and select <i>Edit</i> in the menu to edit the ADOM revision.
Delete	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.
Restore	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.
More > Lock Revision	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.
More > Unlock Revision	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.
View Revision Diff	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.
Settings	Select to configure the automatic deletion settings for ADOM revisions.
Close	Select to close the <i>ADOM Revision</i> dialog box and return to the <i>Policy & 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:

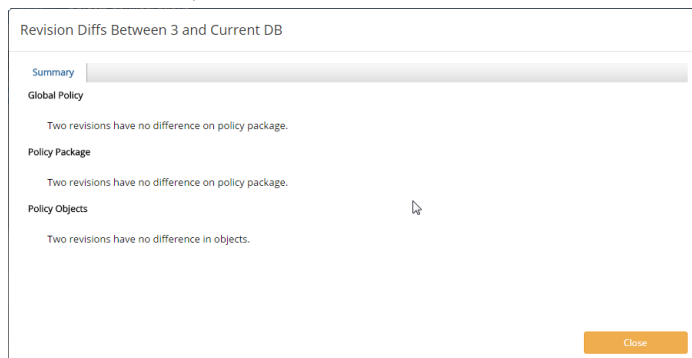
1. Open the *ADOM Revisions* window.
2. Select a revision, and click *Restore*. A confirmation dialog box will appear.
3. Click *OK* to continue.
The *Restore Revision* dialog box opens. Restoring a revision will revert policy packages, objects and VPN console to the selected version.
4. Click *OK* to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

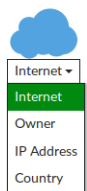
- [Security Fabric Topology on page 281](#)
- [Physical Topology on page 282](#)
- [Logical Topology on page 283](#)
- [Filter Topology Views on page 284](#)
- [Search Topology Views on page 284](#)
- [Security Rating on page 285](#)
- [Fabric Connectors on page 288](#)

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.

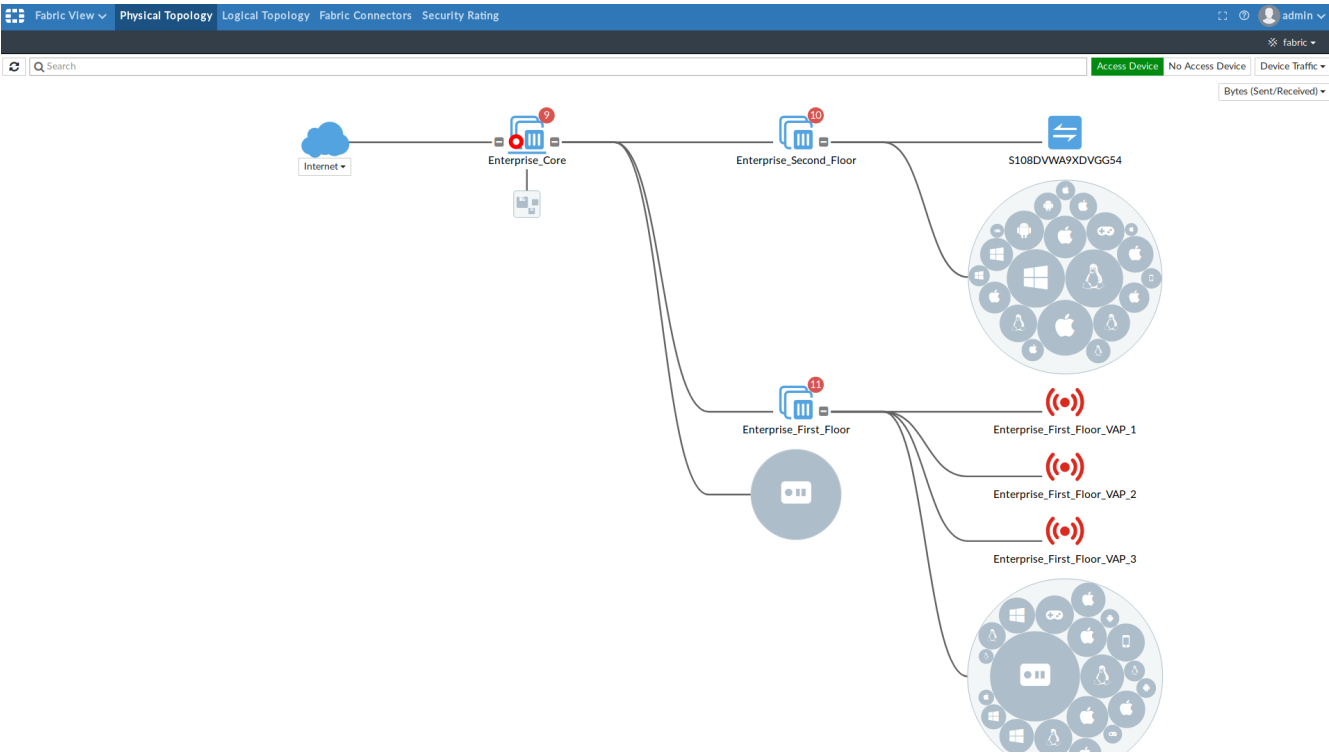
Switch stacking

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.

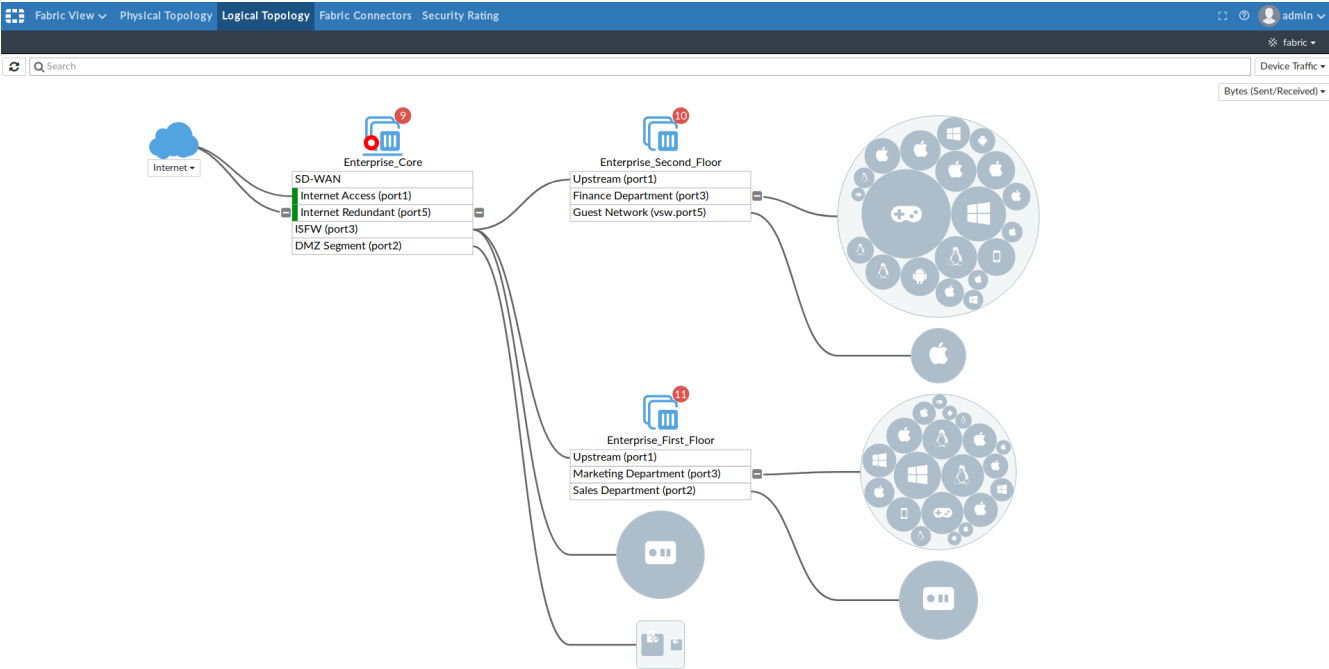
FortiGate	Enterprise_First_Floor
Hostname	Enterprise_First_Floor
Serial	FGVM010000154924
Model	FortiGate VM64-KVM
Version	v6.2.0 build0776
Operation Mode	NAT
Inspection Mode	Proxy-based
Topology	<div>Enterprise_Core Enterprise_First_Floor 3 Downstream Fabric Devices</div>
Management IP	10.100.88.101
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 <ul style="list-style-type: none">Enterprise_First_Floor<ul style="list-style-type: none">3 Downstream Fabric Devices
Management IP	10.100.88.101
CPU Usage	1%
Memory Usage	48%

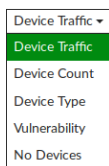
Security Fabric Rating recommendations are also shown in the topology, beside the icon of the device the recommendations apply to.

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:

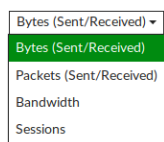
In the drop-down menu to the right of the *Search* field, select one of the following:



- Device Traffic
- Device 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)
- Packets (Sent/Received)
- Bandwidth
- Session

Search Topology Views

The search bar, located above the Physical and Logical Topology views, can help you easily find what you're looking for in the network topology and quickly resolve security issues. The search highlights devices that match your search criteria, and grays out devices that don't match.

To see a list of items that you can search for, mouse over the search bar and a tool tip appears that shows Searchable Information list, organized by host and by Fortinet device type. The following image shows the search bar and the Searchable Information list:

Searchable Information

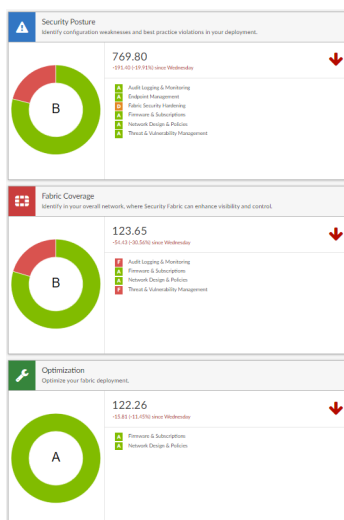
Host	Status, Host Name, Server, MAC Address, Other MAC Addresses, IP Address, Interface, Online Interfaces, Operating System, User, Comment, Authorized User, Unauthorized User
FortiGate	Serial Number, Host Name, Management IP, Model Label, Operating Mode, Parent, Version, IP Address
FortiSwitch	Serial Number, Name, Version
FortiAP	Serial Number, Name, Version

- For hosts, you can search for host information, such as status, host name, and server.
- For FortiGate, you can search for device information, such as serial number, host name, and management IP address.
- For FortiSwitch and FortiAP, you can search for device information, such as serial number, name and OS version.

Security Rating

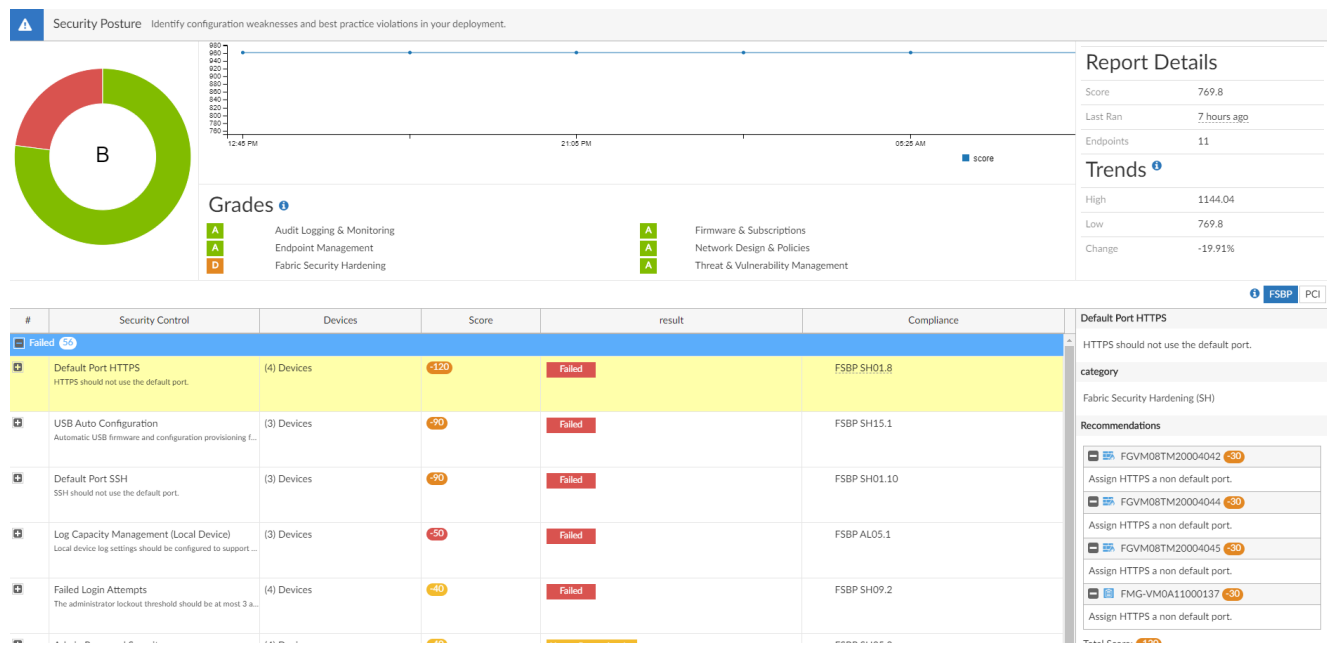
The *Fabric View > Security Rating* pane displays Security Fabric Ratings of configurations for FortiGate Security Fabric groups. You can view the results for multiple FortiGate Security Fabric groups. You must generate the Security Fabric Ratings by using FortiOS before you can view the information in FortiManager.

The *Security Rating* pane is separated into three major scorecards: *Security Posture*, *Fabric Coverage*, and *Optimization*, which provide an executive summary of the three largest areas of security focus in the Security Fabric.



The scorecards show an overall letter grade and breakdown of the performance in sub-categories. Clicking a scorecard drills down to a detailed report of itemized results and compliance recommendations. The point score represents the net score for all passed and failed items in that area.

The report includes the security controls that were tested against, linking to specific FSBP or PCI compliance policies. Click the *FSBP* and *PCI* buttons to reference the corresponding standard. Users can search or filter the report results.



To exit the current view, click the icon beside the scorecard title to return to the summary view.

For more information about security ratings, and details about each of the checks that are performed, go to [Security Best Practices & Security Rating Feature](#).



Security rating licenses are required to run security rating checks across all the devices in the Security Fabric. It also allows ratings scores to be submitted to and received from FortiGuard for ranking networks by percentile.

See <https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/security-rating.html> for information.

Enabling the Security Rating tab

The *Security Rating* tab is displayed when FortiManager is managing FortiGate units that have Security Fabric enabled and are part of a Security Fabric group.

If ADOMs are enabled in FortiManager, the *Security Rating* tab is only available in FortiGate ADOMs that contain a Security Fabric group.

Viewing Security Fabric Ratings

You can view Security Fabric Ratings of configurations for all FortiGate units in a Security Fabric Group or for individual FortiGate units in a Security Fabric group.



You cannot use FortiManager to generate Security Fabric Ratings; you must use FortiOS to generate Security Fabric Ratings for a FortiGate Security Fabric group, and then you can see the Security Fabric Ratings in FortiManager.

For more information about each of the checks that are performed, see the [Fortinet Recommended Security Best Practices](#) document.

To view Security Fabric Ratings:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Fabric View > Security Rating*.
3. In the tree menu, select the *Security Fabric* group.
The Security Fabric Rating results are displayed in the content pane for the selected Security Fabric group.
You can filter the results. For example, you can view only failed results by clicking the *Failed <number>* button, and you can click the *All Results <number>* button to view all results again.
4. In the content pane, select *All FortiGates* to view results for all FortiGates in the group, or select individual FortiGate units to display results for only the selected unit.

Security Fabric score

The Security Fabric score is calculated when a security rating check is run, based on the severity level of the checks that are passed or failed. A higher scores represents a more secure network. Points are added for passed checks and removed for failed checks.

Severity level	Weight (points)
Critical	50
High	25
Medium	10
Low	5

To calculate the number of points awarded to a device for a passed check, the following equation is used:

$$\text{score} = \frac{\text{<severity level weight>}}{\text{<\# of FortiGates>}} \times \text{<secure FortiGate multiplier>}$$

The secure FortiGate multiplier is determined using logarithms and the number of FortiGate devices in the Security Fabric.

For example, if there are four FortiGate devices in the Security Fabric that all pass the compatible firmware check, the score for each FortiGate device is calculated with the following equation:

$$\frac{50}{4} \times 1.292 = 16.15 \text{ points}$$

All of the FortiGate devices in the Security Fabric must pass the check in order to receive the points. If any one of the FortiGate devices fails a check, the devices that passed are not awarded any points. For the device that failed the check, the following equation is used to calculate the number of points that are lost:

$$\text{score} = \text{<severity level weight>} \times \text{<secure FortiGate multiplier>}$$

For example, if the check finds two critical FortiClient vulnerabilities, the score is calculated with the following equation:

$$-50 \times 2 = -100 \text{ points}$$

Scores are not affected by checks that do not apply to your network. For example, if there are no FortiAP devices in the Security Fabric, no points will be added or subtracted for the FortiAP firmware version check.

Fabric Connectors

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

- [SDN](#)
- [Threat Feeds](#)
- [Endpoint/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
- VMware NSX-T
- Nuage Virtualized Services Platform
- Horizon (OpenStack)
- Oracle Cloud Infrastructure
- VMWare ESXi
- VMware vCentre

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 289](#)
- [Creating AWS fabric connectors on page 291](#)
- [Creating Microsoft Azure fabric connectors on page 293](#)
- [Creating VMware NSX fabric connectors on page 294](#)
- [Creating VMware NSX-T connector on page 296](#)
- [Creating Nuage fabric connectors on page 304](#)
- [Creating Horizon connector on page 308](#)
- [Creating Oracle Cloud Infrastructure \(OCI\) connector on page 309](#)
- [Creating VMWare ESXi connector on page 311](#)
- [Creating VMware vCenter connectors on page 316](#)
- [Importing address names to fabric connectors on page 305](#)
- [Configuring dynamic firewall addresses for fabric connectors on page 307](#)
- [Configuring virtual wire pairs on page 307](#)

Creating ACI fabric connectors

With FortiManager, you can create a fabric connector for Application Centric Infrastructure (ACI), and then import address names from ACI to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate 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, either directly or via the Fortinet SDN Connector.

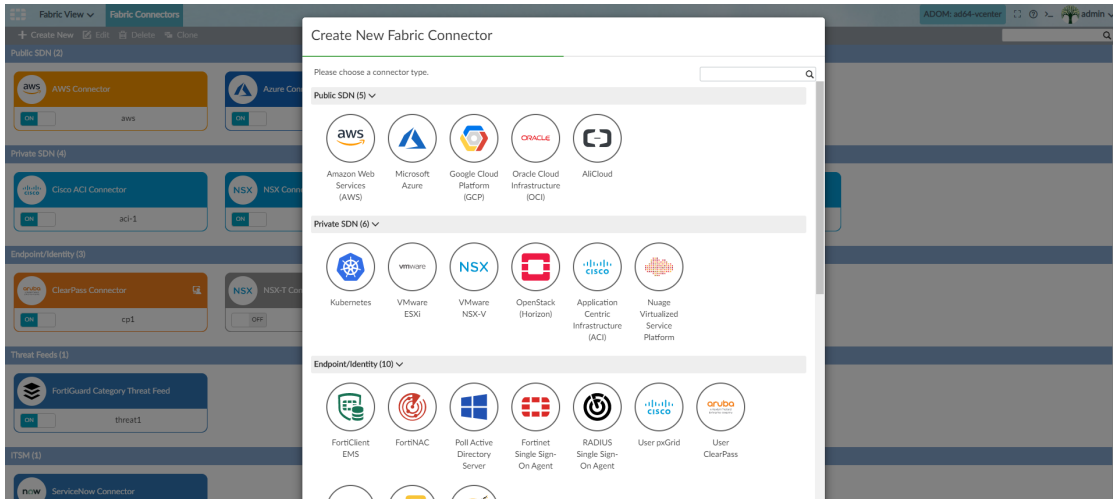
If ADOMs are enabled, you can create multiple fabric connectors per ADOM; however, each fabric connector requires a unique IP address.

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 *Private SDN*, select *Application Centric Infrastructure*. The *Application Centric Infrastructure* screen is displayed.

Create New Fabric Connector

Private SDN
Application Centric Infrastructure (ACI)

Connector Settings

Name

Status ☒ ON ☐ OFF

Cisco ACI Connector

ACI Type ☒ FortiSDN Connector ☐ Direct Connection

IP

Port ☒ Use Default ☐ Specify

Username

Password

Advanced Options >

< Back OK Cancel

4. Configure the following options, and then click *OK*:

Name	Type a name for the fabric connector object.
Status	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>Off</i> to disable the fabric connector object.
ACI Type	Select <i>FortiSDN Connector</i> or <i>Direct Connection</i> as the <i>ACI Type</i> .
IP	Type the IP address for Fortinet SDN Connector.
Port	Identify the port used for Fortinet SDN Connector.

	Perform one of the following options: <ul style="list-style-type: none"> Click <i>Use Default</i> to use the default port. Click <i>Specify</i> and type the port number.
User Name	Type the user name for Fortinet SDN Connector.
Password	Type the password for Fortinet SDN Connector.

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 305](#).
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 214](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 195](#).
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 *Public SDN*, select *Amazon Web Services*. The *Amazon Web Services* screen is displayed.

4. Configure the following options, and then click **OK**:

Name	Type a name for the fabric connector object.
Type	Displays <i>Amazon Web Services (AWS)</i> .
AWS access key ID	Type the access key ID from AWS.
AWS secret access key	Type the secret access key from AWS.
AWS region name	Type the region name from AWS.
AWS VPC ID	Type the AWS VPC ID.
Update Interval (s)	Specify how often in seconds that the dynamic firewall objects should be updated.
Status	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 305](#).
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 214](#).
 3. Install the policy package to FortiGate. See [Install a policy package on page 195](#).
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 *Public SDN*, select *Microsoft Azure*. The *Microsoft Azure* screen is displayed.

Create New Fabric Connector



Connector Settings

Name

Status

☒ ON

Update Interval (s) ⓘ

Use Default

Specify

Azure Connector

Use Managed Identity

☐ OFF

Server Region

Global

Directory ID ⓘ

Application ID ⓘ

Client secret ⓘ

Resource path

☐ OFF

Advanced Options >

< Back

OK

Cancel

4. Configure the following options, and then click *OK*:

Name	Type a name for the fabric connector object.
Type	Displays Microsoft Azure.
Azure tenant ID	Type the tenant ID from Azure.
Azure client ID	Type the client ID from Azure.

Azure client secret	Type the client secret from Azure.
Azure subscription ID	Type the subscription ID for Azure.
Azure resource group	Type the resource group for Azure.
Update Interval (s)	Specify how often in seconds that the dynamic firewall objects should be updated.
Status	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
Advanced Options	Expand to specify advanced options for Azure.
azure-region	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 307](#).
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 214](#).
3. Install the policy package to FortiGate. See [Install a policy package on page 195](#).
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 *Private SDN*, select *VMware NSX-V*. The *VMware NSX-V* screen is displayed.

Create New Fabric Connector



Connector Settings

Name

Status

ON ☐

Update Interval (s) ⓘ

Use Default Specify

NSX Connector

Server

Username

Password

VMX

Service Name

Image Location

REST API

Port

Interface

Mgmt Sync

Password

Advanced Options >

< Back

OK

Cancel

4. Configure the following options, and then click **OK**:

Name	Type a name for the fabric connector object.
Type	Displays <i>VMware NSX</i> .
IP	Type the IP address for VMware NSX.
User Name	Type the user name for VMware NSX.
Password	Type the password for VMware NSX.
Update Interval (s)	Specify how often in seconds that the dynamic firewall objects should be updated.
Status	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
VMX	The VMX options identify settings used by the FortiGate VMX Service Manager to communicate with the REST API for NSX Manager.
Service Name	Type the name of the FortiGate VMX service defined on NSX Manager.
Image Location	Type the location of the FortiGate VMX deployment template used by NSX Manager to deploy the FortiGate VMX service.

REST API	The REST API options specify how the FortiGate VMX Service Manager communicates with the REST API for NSX Manager.
Port	Type the port used by the FortiGate VMX Service Manager to communicate with NSX Manager.
Interface	Select the interface used by the FortiGate VMX Service Manager to communicate with NSX Manager. Choose between Mgmt and Sync.
Password	Type the password that FortiGate VMX Service Manager uses with the REST API to communicate with NSX Manager. Note: This is not the admin password for FortiGate VMX Service Manager.

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 305](#).
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 307](#).
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 226](#).
4. Install the policy package to FortiGate or FortiGate VMX Service Manager. See [Install a policy package on page 195](#).
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 VMware NSX-T connector

FortiManager supports VMware NSX-T connectors.

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

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

1. [Enabling read-write JSON API access on page 296](#)
2. [Creating a fabric connector for VMware NSX-T on page 297](#)
3. [Downloading the FortiGate VM deployment image on page 300](#)
4. [Registering a service from FortiManager to VMware NSX-T on page 300](#)
5. [Deploying a FortiGate VM from VMware NSX-T on page 302](#)
6. [Creating and installing policy packages on page 303](#)

Enabling read-write JSON API access

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

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

To enable read-write JSON API access:

1. On FortiManager, go to *System Settings > Administrators*.
2. Double-click an administrator account to open it for editing.
3. Beside *JSON API Access*, select *Read-Write*, and click *OK*.

System Settings ▾

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

Edit Administrator

User Name: admin

Avatar: + Change Photo - Remove Photo

Comments:

Admin Type: LOCAL

Admin Profile: Super_User

JSON API Access: Read-Write

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

Policy Package Access: All Packages | Specify

Trusted Hosts: OFF

Meta Fields >

Advanced Options >

Creating a fabric connector for VMware NSX-T

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

To create a fabric connector for VMware NSX-T:

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

Policy & Objects ▾

- Policy Packages
- Object Configurations**

ADOM: adom-scanner

+ Create New ▾ | Edit | Delete | Import | Column Settings ▾ | More ▾

Normalized Interface ▾

Firewall Objects ▾

Security Profiles ▾

Fabric Connectors ▾

SDN

Threat Feeds

Endpoint/Identity

User & Authentication ▾

Type	Details	Created Time	Last Modified
AUTO		2020-07-17 09:17:47	admin/2020-07-17 09:17:47
ClearPass Connector	10.210.34.247	2020-04-21 16:25:11	admin/2020-04-21 16:25:16
NSX-T Connector	3.2.3.3	2020-07-09 13:07:24	admin/2020-07-09 13:07:24
NSX-T Connector	172.18.37.198	2020-03-16 16:47:19	admin/2020-06-30 11:27:49

3. Complete the options, and click OK.

Policy & Objects Policy Packages **Object Configurations**

ADOM Revisions Tools

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

Create New NSX-T Connector

Name: nsxt-2.4.2
Status: OFF

NSX-T Manager Configurations
Server: 172.18.41.132
User Name: admin
Password: masked

FortiManager Configurations
IP Address: 172.18.37.142
User Name: qa
Password: masked

Apply & Refresh OK Cancel

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

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

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

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

The screenshot shows the 'Edit NSX-T Connector' configuration page in FortiManager. The left sidebar contains a tree view with 'Zone/Interface', 'Firewall Objects', 'Security Profiles', 'Fabric Connectors', 'SDN', 'Threat Feeds', 'SSO/Identity', and 'User & Device'. The 'Object Configurations' tab is selected. The 'Edit NSX-T Connector' form has the following fields:

- Name: nsxt-2.4.2
- Status: ON (toggle)
- NSX-T Manager Configurations:
 - Server: 172.18.41.132
 - User Name: admin
 - Password: masked
- Registered Services (0): + Add Service
- FortiManager Configurations:
 - IP Address: 172.18.37.142
 - User Name: qa
 - Password: masked
 - Connector Users: Search... (No item)

Buttons at the bottom: Apply & Refresh, OK, Cancel.

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

The screenshot shows the 'Edit NSX-T Connector' configuration page in FortiManager. The left sidebar contains a tree view with 'Zone/Interface', 'Firewall Objects', 'Security Profiles', 'Fabric Connectors', 'SDN', 'Threat Feeds', 'SSO/Identity', and 'User & Device'. The 'Object Configurations' tab is selected. The 'Edit NSX-T Connector' form has the following fields:

- Name: nsxt-2.4.2
- Status: ON (toggle)
- NSX-T Manager Configurations:
 - Server: 172.18.41.132
 - User Name: admin
 - Password: masked
- Registered Services (0): + Add Service
- FortiManager Configurations:
 - IP Address: 172.18.37.142
 - User Name: qa
 - Password: masked
 - Connector Users: Search... (List of dynamic firewall address objects)

The 'Connector Users' list contains the following objects:

- nsx_nsxt-2.4.2_default/groups/group1 (6/6)
- nsx_nsxt-2.4.2_default/groups/group2 (8/8)
 - nsx (1.1.1.0)
 - nsx (1.1.1.0-4.4.4.0)
 - nsx (2.2.2.0)
 - nsx (3.3.3.0)
 - nsx (5.5.5.0)
 - nsx (6.6.6.0)
 - nsx (7.7.7.0)
 - nsx (8.8.8.0)
- nsx_nsxt-2.4.2_default/groups/group3 (8/8)

Buttons at the bottom: Apply & Refresh, Disable Server, Cancel.

Downloading the FortiGate VM deployment image

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

To download the FortiGate VM deployment image:

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

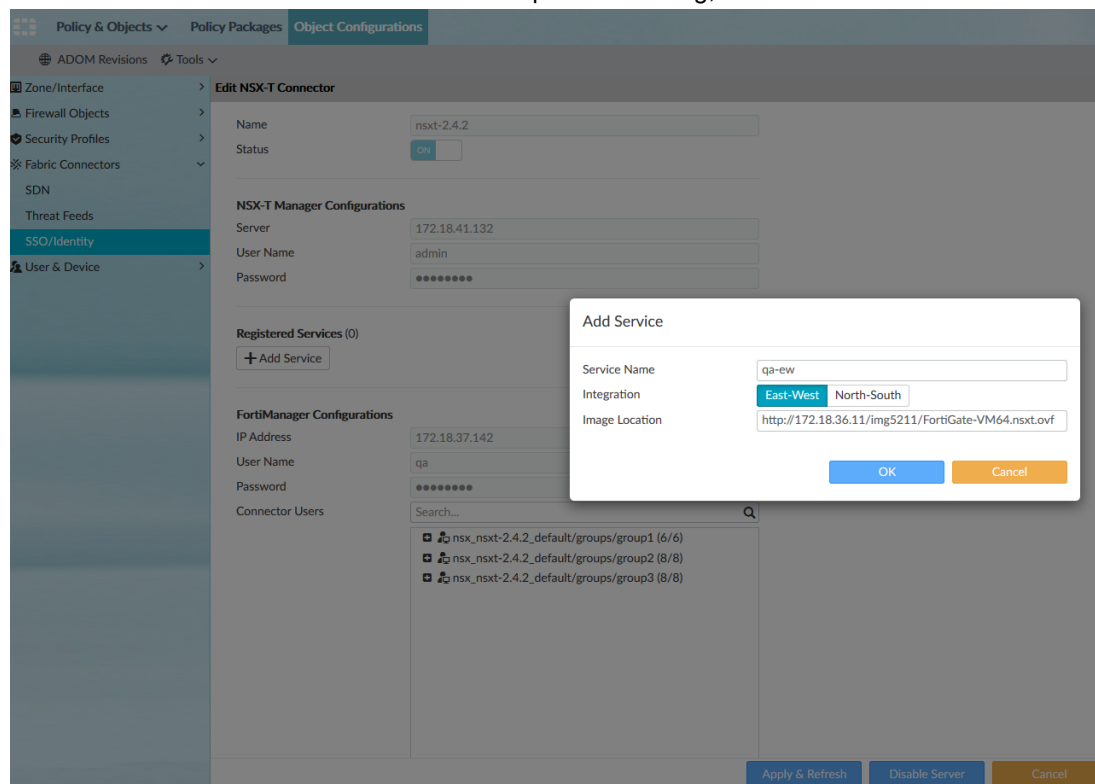
Registering a service from FortiManager to VMware NSX-T

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

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

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

1. Ensure that you know the URL for the location of the preconfigured deployment image for FortiGate VM and VMware NSX-T.
2. On FortiManager, go to *Policy & Objects > Object Configurations > Fabric Connectors > Endpoint/Identity*.
3. Double-click the VMware NSX-T connector to open it for editing, and click *Add Service*.



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

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

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

The screenshot displays the 'Edit NSX-T Connector' configuration page in the FortiManager interface. The left sidebar shows the navigation menu with 'Policy & Objects' selected. The main content area is titled 'Edit NSX-T Connector' and contains several configuration sections:

- Name:** nsxt-2.4.2
- Status:** ON
- NSX-T Manager Configurations:**
 - Server:** 172.18.41.132
 - User Name:** admin
 - Password:** masked
- Registered Services (1):**
 - Service Name:** qa-ew
 - Service ID:** 47f318d9-2f6d-4ccc-918f-c6fc905b30b5
 - Implementations:** EAST_WEST
- FortiManager Configurations:**
 - IP Address:** 172.18.37.142
 - User Name:** qa
 - Password:** masked
 - Connector Users:** nsx_nsxt-2.4.2_default/groups/group1 (6/6), nsx_nsxt-2.4.2_default/groups/group2 (8/8), nsx_nsxt-2.4.2_default/groups/group3 (8/8)

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

You can add multiple services.

Deploying a FortiGate VM from VMware NSX-T

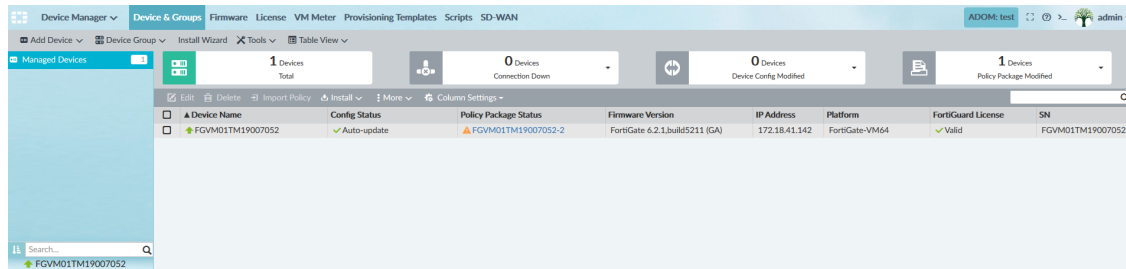
You must deploy the preconfigured FortiGate VM image from the VMware NSX-T manager, and then authorize FortiManager to centrally manage the FortiGate VM.

To deploy a FortiGate VM from VMware NSX-T:

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

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

- On FortiManager, go to *Device Manager*, and authorize the FortiGate VM for management by FortiManager.



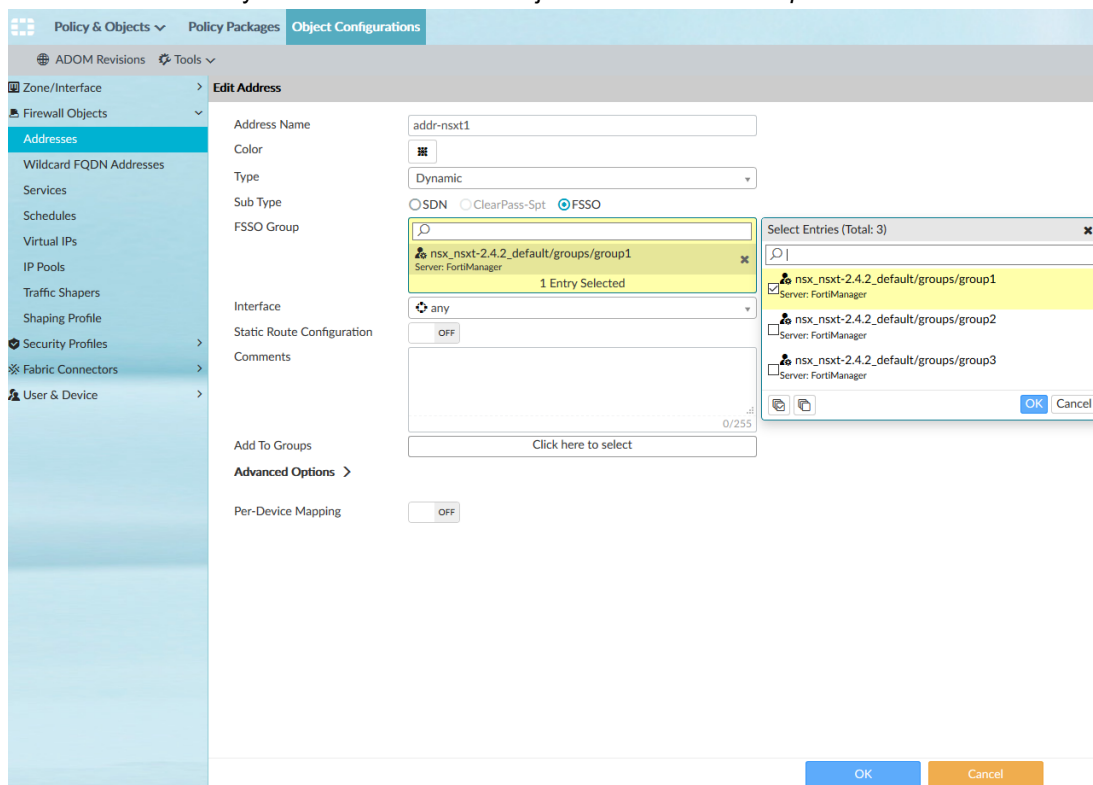
FortiManager can now manage FortiGate.

Creating and installing policy packages

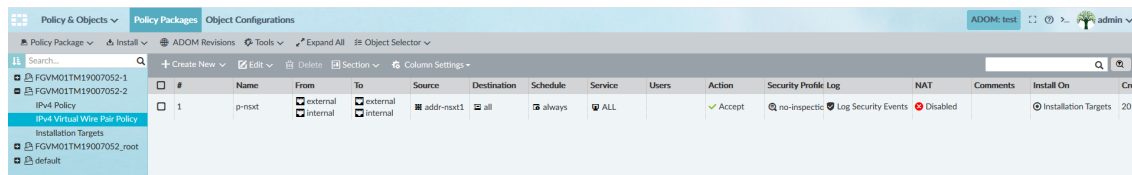
You must create an IPv4 virtual wire pair policy that contains the dynamic firewall address objects, and install the policy to FortiGate. Then FortiGate can use the dynamic address objects.

To create and install policy packages:

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



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



3. Install the policy package to FortiGate.

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

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 *Private SDN*, select *Nuage Virtualized Service Platform*. The *Nuage Virtualized Service Platform* screen is displayed.

Create New Fabric Connector  Private SDN
Nuage Virtualized Service Platform

Connector Settings

Name

Status ☒ ON ☐

Nuage Connector

IP

Port

Username

Password

Advanced Options >

4. Configure the following options, and then click **OK**:

Name	Type a name for the fabric connector object.
Type	Displays Nuage Virtualized Services Platform.
IP	Type the IP address for Fortinet SDN Connector.
Port	Identify the port used for Fortinet SDN Connector. Perform one of the following options: <ul style="list-style-type: none"> Click <i>Use Default</i> to use the default port. Click <i>Specify</i> and type the port number.
User Name	Type the user name for Fortinet SDN Connector.
Password	Type the password for Fortinet SDN Connector.
Status	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:

- Create dynamic firewall address objects. See [Configuring dynamic firewall addresses for fabric connectors on page 307](#).
You cannot import address names from Nuage Virtualized Services Platform to FortiManager.
- 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 214](#).
- Install the policy package to FortiGate. See [Install a policy package on page 195](#).
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 307](#).

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:

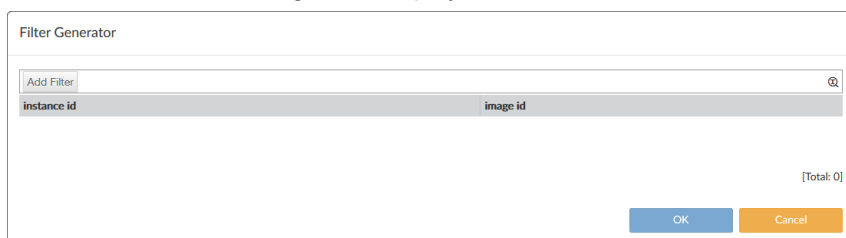
1. Go to *Policy & Objects > Object Configurations*.
2. In the tree menu, go to *Security Fabric > Fabric Connectors*.
3. In the content pane, right-click the fabric connector, and select *Import*.
The *Import SDN Connector* dialog box is displayed.



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:

Address Name	Type a name for the firewall address object.
Type	Select <i>Fabric Connector Address</i> .
SDN	Select the Microsoft Azure fabric connector.
Filter	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:

Address Name	Type a name for the firewall address object.
Type	Select <i>Fabric Connector Address</i> .
SDN	Select the Nuage Virtualized Services Platform fabric connector.
Organization	Type the name of the organization for the Nuage Virtualized Services Platform.
Subnet Name	Type the name of the subnet for the Nuage Virtualized Services Platform.
Policy Group	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 *Normalized Interface > Virtual Wire Pair*.
3. In the content pane, click *Create New*.
4. Complete the following options, and click *OK*.

Name	Type a name for the virtual wire pair.
Interface Members	Select two interface members.
Wildcard VLAN	<p>Toggle <i>ON</i> to enable wildcard VLANs for the virtual wire pair. When enabled, all VLAN-tagged traffic can pass through the virtual wire pair, if allowed by the virtual wire pair firewall policies.</p> <p>Toggle <i>OFF</i> to disable wildcard VLANs for the virtual wire pair.</p>

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):

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

3. Under *Private SDN*, select *OpenStack*. The *OpenStack (Horizon)* screen is displayed.

4. Configure the following options, and then click *OK*:

Name	Type a name for the fabric connector object.
Type	Displays OpenStack (Horizon).
Domain	Type the Domain for Fortinet SDN Connector.
Server	Type the IP address for the SDN Connector.
User Name	Type the user name for Fortinet SDN Connector.
Password	Type the password for Fortinet SDN Connector.
Update Interval (s)	Specify the update interval for the Fortinet SDN Connector. Select one of the following options: <ul style="list-style-type: none"> Click <i>Use Default</i> to use the default interval. Click <i>Specify</i> and specify the interval.
Status	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 *Public SDN*, select *Oracle Cloud Infrastructure*. The *Oracle Cloud Infrastructure (OCI)* screen is displayed.

Create New Fabric Connector

Public SDN
Oracle Cloud Infrastructure (OCI)

Connector Settings

Name

Status ☒ ON

Update Interval (s)

OCI Connector

Use Metadata IAM ☐ OFF

Server Region Type

Server Region

User ID

Tenant ID

Compartment ID

Certificate

System Certificate for Connection

Advanced Options >

< Back OK Cancel

4. Configure the following options, and then click *OK*:

Name	Type a name for the fabric connector object.
Type	Displays Oracle Cloud Infrastructure (OCI).
User ID	Type the User ID for the Fortinet SDN Connector.
OCI Tenant ID	Type the OCI Tenant ID.
OCI Compartment ID	Type the OCI Compartment ID.
OCI Server Region	Select the OCI Server Region from the drop-down.

OCI Certificate	Select the OCI Certificate from the drop-down.
Update Interval (s)	Specify the update interval for the Fortinet SDN Connector. Select one of the following options: <ul style="list-style-type: none"> Click <i>Use Default</i> to use the default interval. Click <i>Specify</i> and specify the interval.
Status	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 *Private SDN*, select *VMWare ESXi*. The *VMWare ESXi* screen is displayed.

Create New Fabric Connector

Private SDN
VMware ESXi

Connector Settings

Name

Status ☒ ON ☐ OFF

Update Interval (s)

ESXi Connector

Server

Username

Password

Advanced Options >

< Back OK Cancel

4. Configure the following options, and then click *OK*:

Name	Type a name for the fabric connector object.
Type	Displays VMWare ESXi.
Server	Type the IP address for the SDN Connector.
User Name	Type the user name for Fortinet SDN Connector.
Password	Type the password for Fortinet SDN Connector.
Update Interval (s)	Specify the update interval for the Fortinet SDN Connector. Select one of the following options: <ul style="list-style-type: none"> Click <i>Use Default</i> to use the default interval. Click <i>Specify</i> and specify the interval.
Status	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 *Private SDN*, select *Kubernetes*. The *Kubernetes* screen is displayed.

Create New Fabric Connector

Private SDN
Kubernetes

Connector Settings

Name:

Status: ☒ ON ☐ OFF

Update Interval (s):

Kubernetes Connector

IP:

Port:

Secret Token:

Advanced Options >

< Back OK Cancel

4. Configure the following options, and then click *OK*:

Name	Type a name for the fabric connector object.
Type	Displays Kubernetes.
IP	Type the IP address for the SDN Connector.
Port	Specify the port for the Fortinet SDN Connector. Select one of the following options: <ul style="list-style-type: none"> • Click <i>Use Default</i> to use the default port. • Click <i>Specify</i> and specify the port.
Secret Token	Specify a secret token for the Fortinet SDN Connector.
Update Interval (s)	Specify the update interval for the Fortinet SDN Connector. Select one of the following options: <ul style="list-style-type: none"> • Click <i>Use Default</i> to use the default interval. • Click <i>Specify</i> and specify the interval.
Status	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 Kubernetes connector is imported. Click *Close* to close the import dialog.
7. 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 *Public SDN*, select *AliCloud*. The *Alibaba Cloud* screen is displayed.

Create New Fabric Connector

Public SDN
AliCloud

Connector Settings

Name

Status

ON

Update Interval (s)

Use Default Specify

AliCloud Connector

AccessKey ID

AccessKey Secret

Region ID

Advanced Options

>

< Back

OK

Cancel

4. Configure the following options, and then click *OK*:

Name	Type a name for the fabric connector object.
Type	Displays Alibaba Cloud Service (ACS).
AccessKey ID	Specify the AccessKey ID for the SDN Connector.
AccessKey Secret	Specify the AccessKey Secret for the SDN Connector.
Region ID	Specify the Region ID for the Fortinet SDN Connector.
Update Interval (s)	Specify the update interval for the Fortinet SDN Connector. Select one of the following options: <ul style="list-style-type: none"> Click <i>Use Default</i> to use the default interval. Click <i>Specify</i> and specify the interval.
Status	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:

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

3. Under *Public SDN*, select *Google Cloud Platform*. The *Google Cloud Platform* screen is displayed.

4. Configure the following options, and then click *OK*:

Name	Type a name for the fabric connector object.
Type	Displays Google Cloud Platform (GCP).
Project Name	Specify the Project Name for the SDN Connector.
Service Account Email	Specify the Service Account Email for the SDN Connector.
Private Key	Specify the Private Key for the Fortinet SDN Connector.
Update Interval (s)	Specify the update interval for the Fortinet SDN Connector. Select one of the following options: <ul style="list-style-type: none"> Click <i>Use Default</i> to use the default interval. Click <i>Specify</i> and specify the interval.
Status	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 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.

Creating VMware vCenter connectors

You can create SDN connectors for VMware vCentre to allow FortiGate to retrieve dynamic addresses from VMware vCenter via FortiManager.

Following is an overview of how to configure an SDN connector for VMware vCenter:

1. Create an SDN connector for VMware vCenter. See [Creating SDN connectors for VMware vCenter on page 317](#).
2. Create a dynamic address object that references the SDN connector for VMware vCenter. See [Creating dynamic addresses on page 318](#).
3. Create a firewall policy. See [Creating firewall policies on page 319](#).

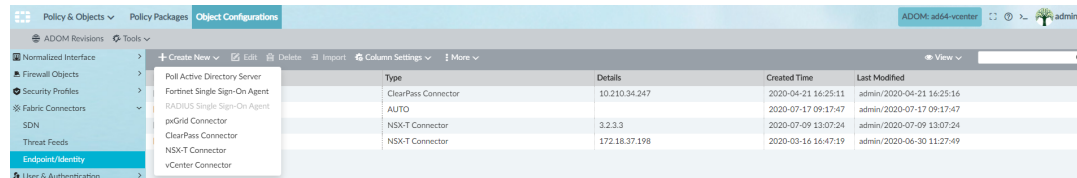
- Install the changes to FortiGate. See [Installing changes to FortiGate on page 320](#).
FortiGate can retrieve dynamic addresses from VMware vCenter via FortiManager.
This example assumes that VMware vCenter is already set up.

Creating SDN connectors for VMware vCenter

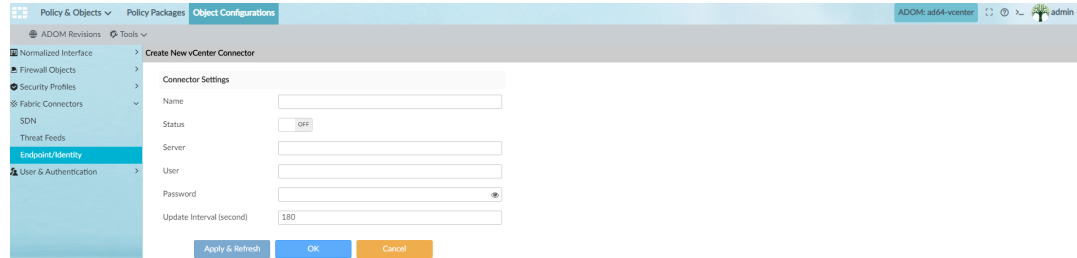
To create SDN connectors for VMware vCenter:

- Go to *Policy & Objects > Object Configurations > Fabric Connectors > Endpoint/Identity*.
- Click *Create New > vCenter Connector*.

The pane opens.

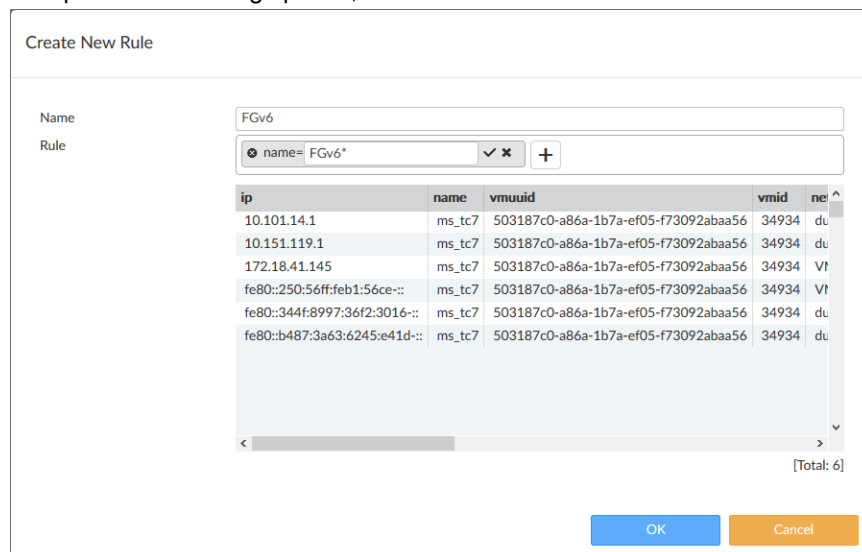


- Complete the following options, and click *Apply & Refresh*:



The *Rule* section is displayed.

- Under *Rule*, click *Create New*.
- Complete the following options, and click *OK*.



FortiManager retrieves IP addresses from the VMware vCenter server.

Policy & Objects ▾ Policy Packages Object Configurations

ADOM Revisions Tools ▾

Zone/Interface > Edit vCenter Connector

Firewall Objects >

Security Profiles >

Fabric Connectors ▾

SDN

Threat Feeds

SSO/Identity

User & Device >

Name: fmg-stress

Status: ☒ ON

Server: 172.18.41.70

User: ellen@vsphere.local

Password: ••••••••

Update Interval: 30

Default Group: stress1

Rule

Name	Rule
<input type="checkbox"/> FGv6	name=FGv6*
<input type="checkbox"/> ej-2k	name=ej_vlan*
<input type="checkbox"/> ej-vlan124	name=ej_vlan124*
<input type="checkbox"/> ej-vlan124-top3-001	name=ej_vlan124-top3-0001
<input type="checkbox"/> ej-vlan128	name=ej_vlan128*

Connector Users

Search...

- ☒ vc_fmg-stress_FGv6 (250/250)
- ☒ vc_fmg-stress_ej-2k (1747/1747)
- ☒ vc_fmg-stress_ej-vlan124 (250/250)
- ☒ vc_fmg-stress_ej-vlan124-top3-001 (1/1)
- ☒ vc_fmg-stress_ej-vlan128 (250/250)
- ☒ vc_fmg-stress_stress1 (83/83)

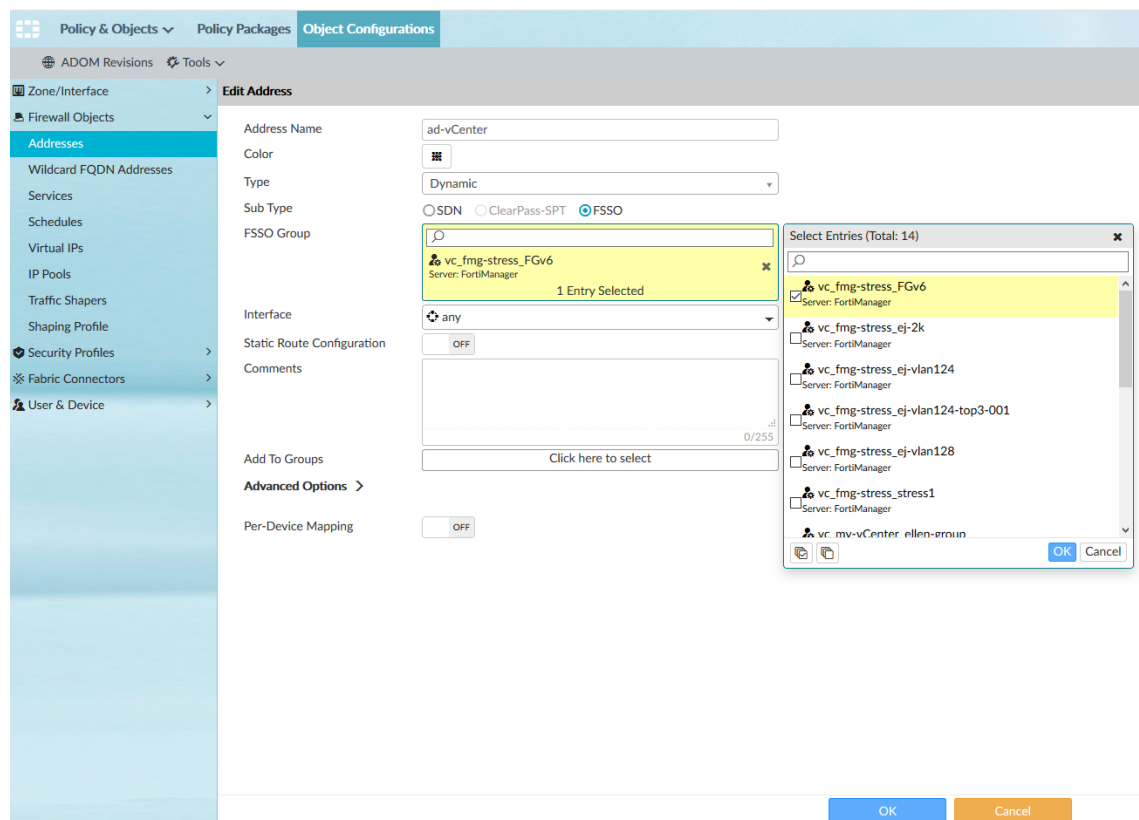
https://172.18.37.131/p/app/#

Apply & Refresh OK Cancel

Creating dynamic addresses

To create dynamic addresses:

1. Go to *Policy & Objects > Object Configurations > Firewall Objects > Addresses*.
2. Click *Create New > Address*, or double-click an existing address object to open it for editing.
3. Complete the following options, and click *OK*.
 - a. In the *Address Name* box, type a name.
 - b. In the *Type* box, select *Dynamic*.
 - c. Beside *Sub Type*, select *FSSO*.
 - d. In the *FSSO Group* box, select the SDN connector that you created.
 - e. Set the remaining objects as desired.



The dynamic address is created.

Creating firewall policies

To create firewall policies:

1. Go to *Policy & Objects > Policy Packages*.
2. In the tree menu, click IPv4 Policy under the target FortiGate.

3. Click *Create New* , or double-click an existing policy to open it for editing.

Policy & Objects | **Policy Packages** | Object Configurations

Policy Package | Install | ADOM Revisions | Tools | Collapse All | Object Selector

Search...

Edit IPv4 Policy

Name: p1

Incoming Interface: any

Outgoing Interface: any

Source Internet Service: OFF

Source Address: all

Source User: +

Source User Group: +

FSSO Groups: +

Destination Internet Service: OFF

Destination Address: ad-vCenter

Service: ALL

Schedule: always

Action: Deny | Accept | IPSEC

Log Violation Traffic: ☒

☐ Generate Logs when Session Starts

Comments:
 0/1023

Advanced Options >

OK Cancel

4. Complete the options, and click *OK*.
The policy package is created.

Installing changes to FortiGate

To install changes to FortiGate:

1. Go to *Policy & Objects* > *Policy Packages*.
2. In the tree menu, right-click *Installation Targets* under the target FortiGate, and select *Install Wizard*.
The *Install Wizard* dialog box opens.
3. Select *Install Policy Package & Device Settings*.

4. In the *Policy Package* list, select the policy package, and click *Next*.

Install Wizard - Policy Package and Device Setting (FortiGate-VM_root)

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

<input checked="" type="checkbox"/>	▲ Device Name	IP Address	Platform
<input checked="" type="checkbox"/>	FortiGate-VM	10.59.8.162	FortiGate-VM64

< Back Next > Cancel

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

The policy package is installed.

FortiGate can retrieve dynamic addresses from VMware vCenter via FortiManager.

FortiGate VM64 FortiGate-VM

ad-vCenter resolves to:

Type	Details	Interface	Visibility	Ref.
Subnet	0.0.0.0/0		Visible	0
Subnet	0.0.0.0/0		Hidden	0
IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel Interface (ssLroot)	Visible	0
Dynamic (FSSO)	vc_fmng-stress_FGv6		Visible	1
Subnet	0.0.0.0/0		Visible	1

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 322](#)

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*:

Type	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> .
Name	Type a name for the fabric connector object.
URI of external resource	Type the link to an external text file. The path must start with <code>http://</code> , <code>https://</code> , or <code>fmg://</code> , for example, <code>http://example.com/url</code> .
Category ID	Type the category ID. The ID is between 192 and 221. Available only when <i>Type</i> displays <i>Domain List</i> .
Refresh Rate	The time in minutes to refresh the external resource.
Comments	(Optional) Type comments about the connector.
Status	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.

Endpoint/Identity

You can use the *Fabric Connectors* tab to create the following types of Endpoint/Identity connectors:

- AD Polling
- FSSO
- RADIUS
- Cisco pxGrid
- Aruba ClearPass
- VMware NSX-T

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 323](#)
- [Creating FSSO connectors on page 323](#)
- [Creating RADIUS connectors on page 324](#)
- [Creating Cisco pxGrid connector on page 324](#)
- [Creating ClearPass connector on page 331](#)
- [Creating VMware NSX-T connector on page 346](#)

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 *Endpoint/Identity*, select *Poll Active Directory Server*.
4. Configure the following options, and then click *OK*:

Server Name/IP	Type the name or IP address for the Active Directory server.
Local User	Type the user name required to log into the Active Directory server.
Password	Type the password required to log into the Active Directory server.
Enable Polling	Toggle <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 *Endpoint/Identity*, select *Fortinet Single Sign-on Agent*.
4. Configure the following options, and then click *OK*:

Name	Type a name for the connector object.
-------------	---------------------------------------

FSSO Agent	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.
Select FSSO Groups	Specify whether to get FSSO groups from FSSO agents or via FortiGate.
User Groups LDAP Server	Select the name of the LDAP server to be used to get group information from the Directory Service.
Per-Device Mapping	(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.
Advanced Options	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.
3. Under *Endpoint/Identity*, select *RADIUS Single Sign-On Agent*.
4. Configure the following options, and then click *OK*:

Name	Type the name of the RADIUS SSO agent.
Use RADIUS Shared Secret	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.
Send RADIUS Responses	Toggle <i>On</i> to send RADIUS response packets after receiving start and stop records. Toggle <i>OFF</i> to disable this feature.
Advanced Options	Expand to view and configure advanced options for RADIUS single sign-on agents. For details, see the <i>FortiOS CLI Reference</i> .

Creating Cisco pxGrid connector

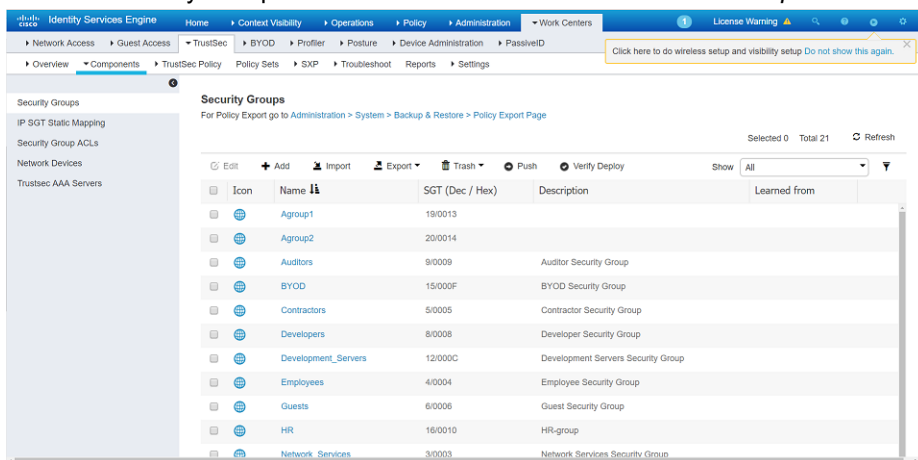
Cisco pxGrid for FortiManager centralizes the updates from pxGrid for all FortiGate devices, and leverages the efficient FSSO protocol to apply dynamic policy updates to FortiGate.

Requirements:

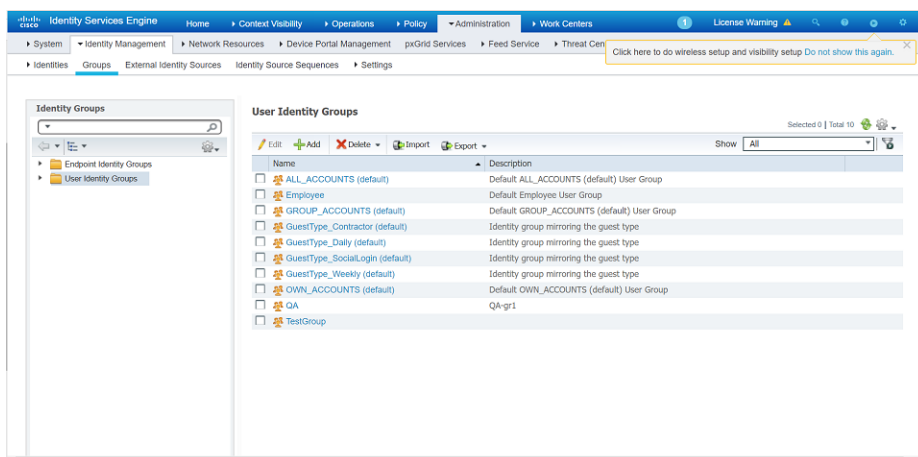
- FortiManager version 5.6 ADOM or later.
The method described in this topic for creating fabric connectors requires version 6.0 ADOM or later.
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with Cisco pxGrid.
- Configure the Cisco ISE server and download the certificate.

To configure Cisco ISE server:

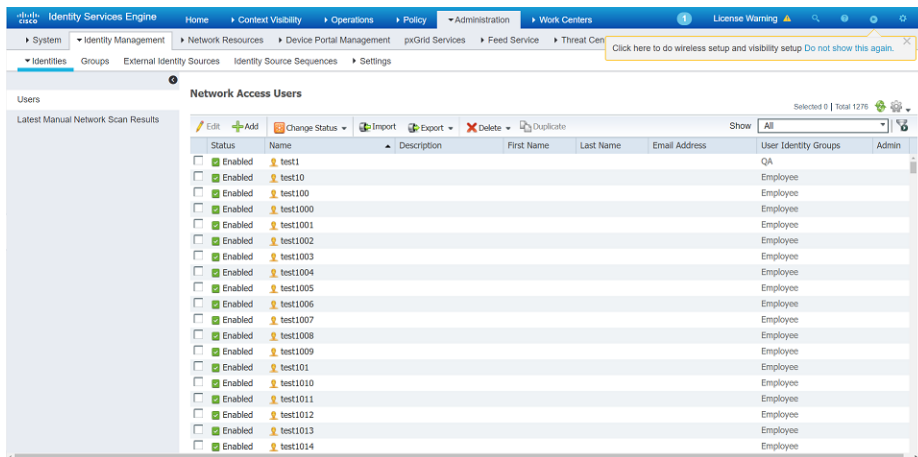
1. Create a Security Group: Go to *ISE > Work Centers > TrustSec > Components > Security Groups*. Click *Add*.



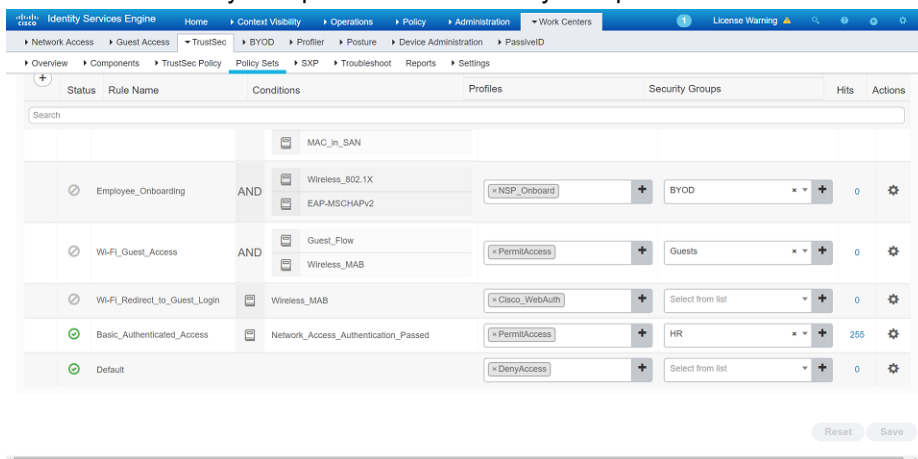
2. Create a User Identity Group: Go to *ISE > Administration > Identity Management > Groups > User Identity Groups*. Click *Add*.



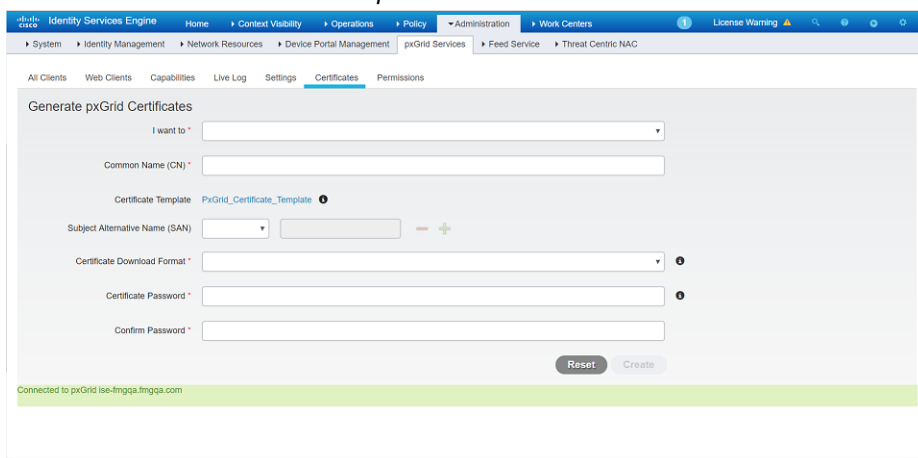
3. Create a user and add it to User Identity Group: Go to *ISE > Administration > Identity Management > Identities*. Click *Add*.



4. Match the Security Group with User Identity Group in the policy: Go to *ISE > Work Centers > TrustSec > Components > Policy Sets*. Right-click and go to *Authorization policy > Basic_Authenticated_Access* and click *Edit* to match the Security Group with the User Identity Group.



5. Generate the pxGrid certificate and download it to the local computer: Go to *ISE > Administration > pxGrid Services > Certificate* and select *Generate pxGrid Certificates*.



6. See log for current users: Go to *ISE > Operations > RADIUS > Live Logs*.

The screenshot shows the ISE Live Logs page. At the top, there are several status indicators: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), Client Stopped Responding (0), and Repeat Counter (0). Below these, there are filters for Refresh (Never), Show (Latest 20 records), and Within (Last 3 hours). The main table displays log entries for user 'test2'.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP A
Mar 01, 2019 02:52:32.196 PM	Success		0	test2	00:11:22:33:44:55	Unknown	Default >> D...	Default >> B...	PermitAcces...	192...
Mar 01, 2019 02:52:03.737 PM	Success			test2	00:11:22:33:44:55	Unknown	Default >> D...	Default >> B...	PermitAcces...	192...
Mar 01, 2019 02:44:06.881 PM	Failure			test2	00:11:22:33:44:55		Default >> D...	Default		192...

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*.

The screenshot shows the ISE Live Sessions page. It includes filters for Refresh (Every 1 minute), Show (Latest 20 records), and Within (Last 24 hours). The main table displays live session information for user 'test2'.

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.

The screenshot shows the FortiManager System Settings - Local Certificates page. The left sidebar shows the navigation menu with 'Local Certificates' selected. The main area displays a table of certificates.

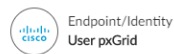
Certificate Name	Subject	Status
fmgga	CN = fmgga.com	OK
Fortinet_Local	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiManager, CN = FMG1KD3A15000085, emailAddress = support@fortinet.com	OK
Fortinet_Local2	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiManager, CN = FMG1KD3A15000085, emailAddress = support@fortinet.com	OK

2. Go to *Fabric View > Fabric Connectors*.

3. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.

4. Under *Endpoint/Identity*, select *User pxGrid*.
5. Configure the following options and click **OK** to create the User pxGrid connector:

Create New Fabric Connector



Connector Settings

Name

Status ☐ OFF

Server

CA Certificate

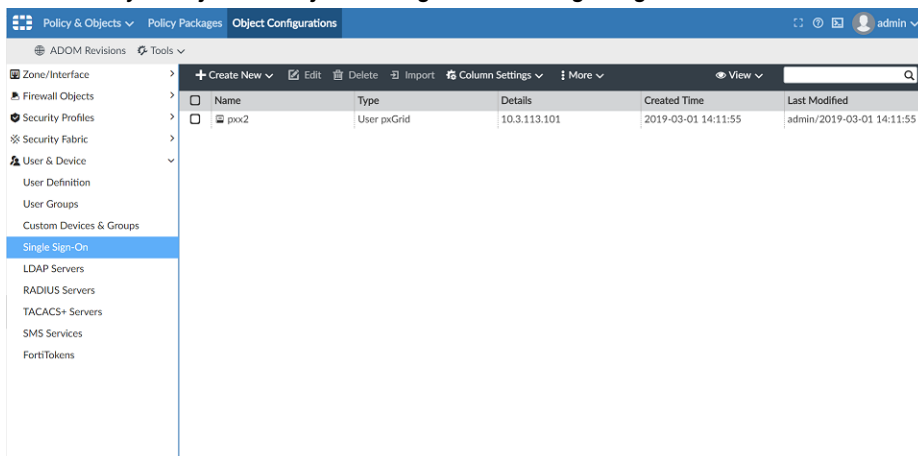
Client Certificate

< Back Apply & Refresh OK Cancel

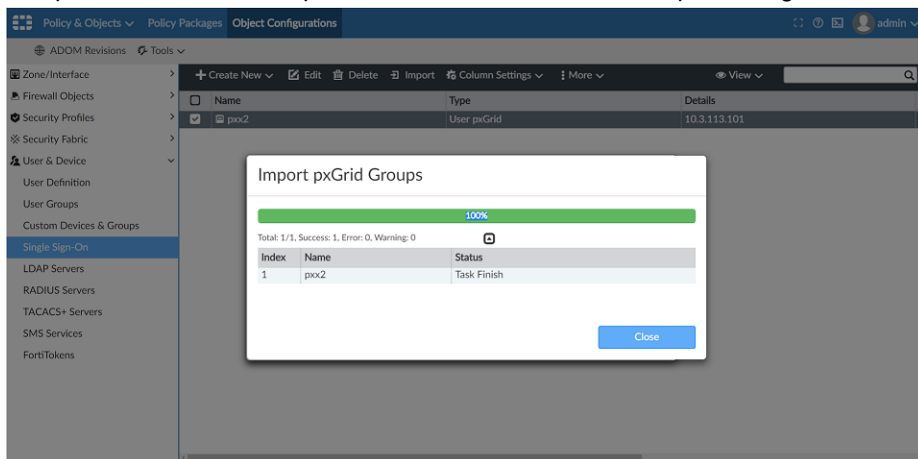
6.

Name	Type a name for the fabric connector object.
Status	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
Server	Type the IP address for Cisco ISE server.
CA Certificate	Select the imported CA Certificate.
Client Certificate	Select the imported Client Certificate.

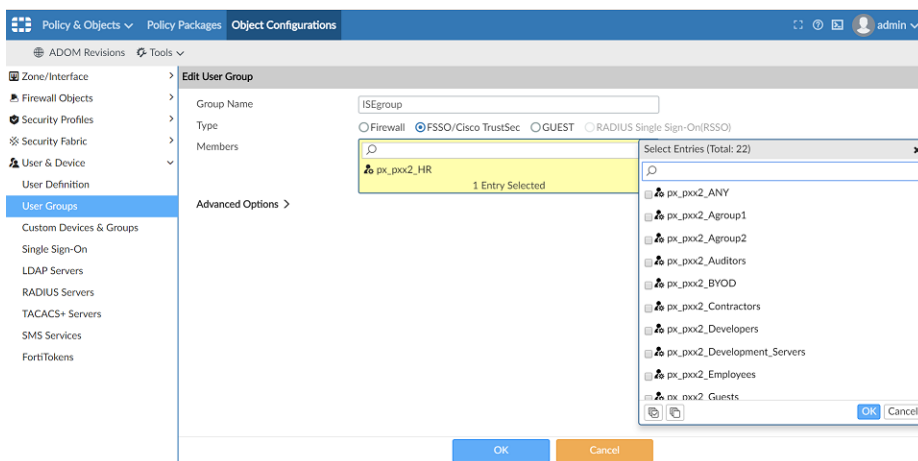
7. Go to *Policy & Objects > Object Configuration > Single Sign-On*. Select the connector and click *Import*.



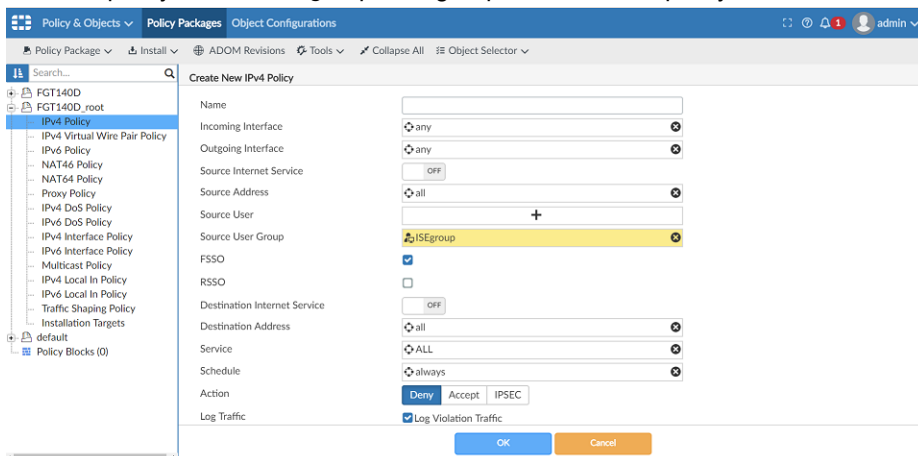
8. The pxGrid connector is imported. Click *Close* to close the import dialog.



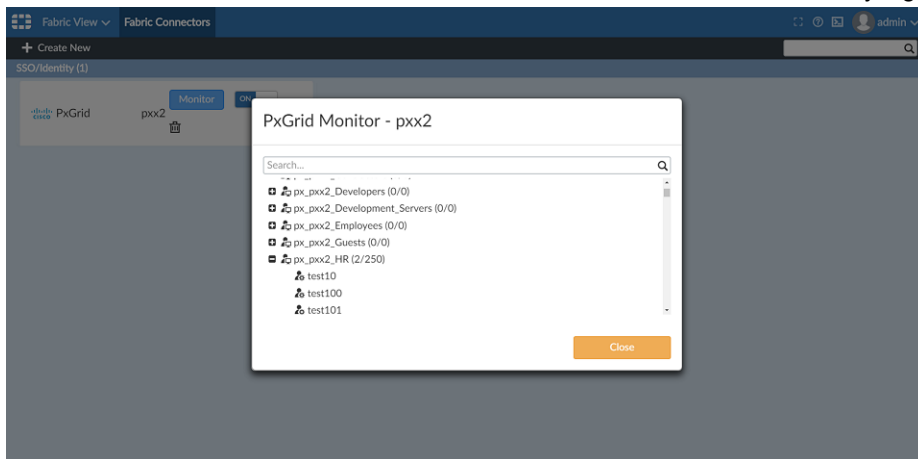
9. Click *User Groups* and create a new group. Set the type as *FSSO/Cisco TrustSec*, and select *pxGrid* user as a member.



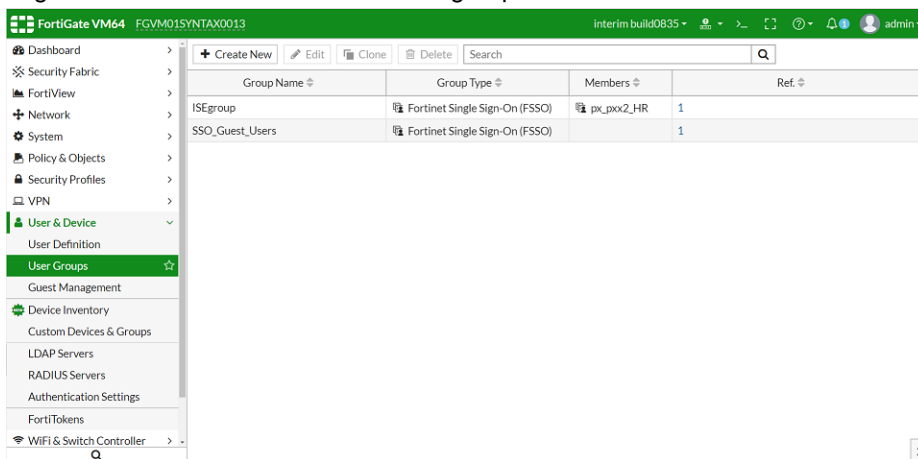
10. Create a policy with the *ISEgroup* user group and install the policy to FortiGate.



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
fssso-refresh-interval FSSO refresh interval (60 - 1800 seconds).
fssso-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_grp1 Workstation: MemberOf: fscs1
IP: 192.168.1.20 User: test2 Groups: px_fcl_security_grp1 Workstation: MemberOf: fscs1
Total number of logons listed: 2, filtered: 0
----end of FSSO logons----
diag debug authd fsso refresh-logon
diag debug authd fsso refresh-group
```

Creating ClearPass connector

ClearPass Policy Manager (CCPM) is a network access system that can send information about authenticated users to third party systems, such as a FortiGate or FortiManager. ClearPass connector for FortiManager centralizes updates from ClearPass for all FortiGate devices and leverages the efficient FSSO protocol to apply dynamic policy updates to FortiGate.

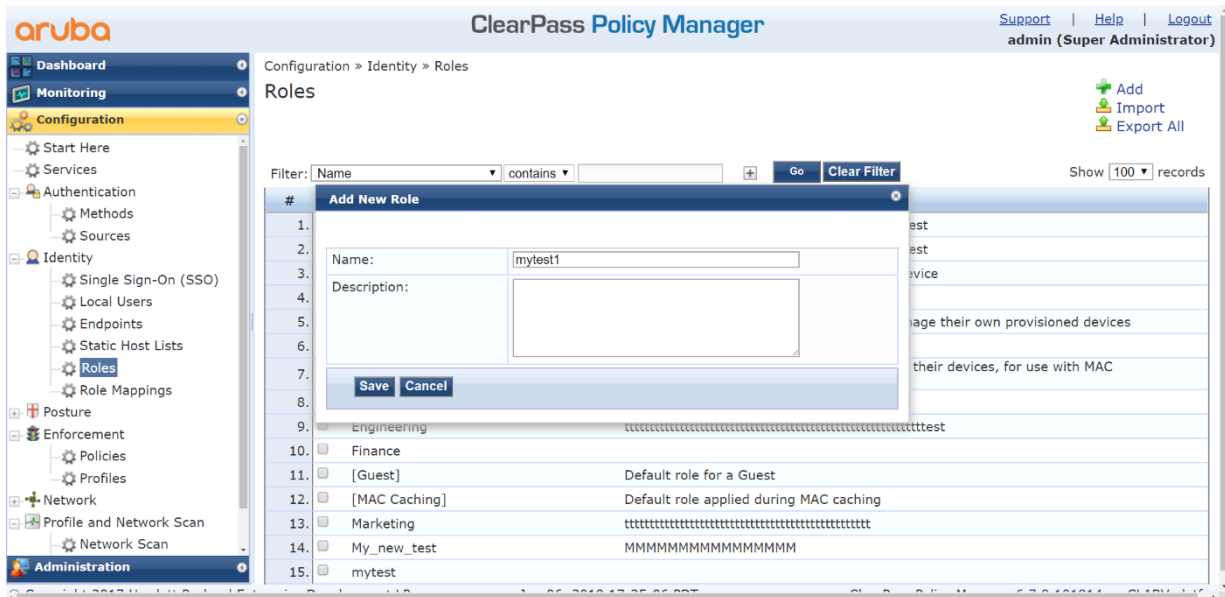
You can create multiple ClearPass connectors per ADOM.

Requirements:

- FortiManager version 5.6 or later ADOM
This example applies to version 6.0 or later ADOMs.
- FortiGate is managed by FortiManager and configured to work with ClearPass
- JSON API is exposed, allowing ClearPass to call it

To configure ClearPass:

1. Log in to *ClearPass Policy Manager*..
2. Create roles:
 - a. Go to *Configuration > Identity > Roles*.
 - b. Click *Add*.
 - c. For the name, enter *mytest1*.
FortiManager will get this group as an Active Directory group.
The *Description* field is optional.



d. Click **Save**.

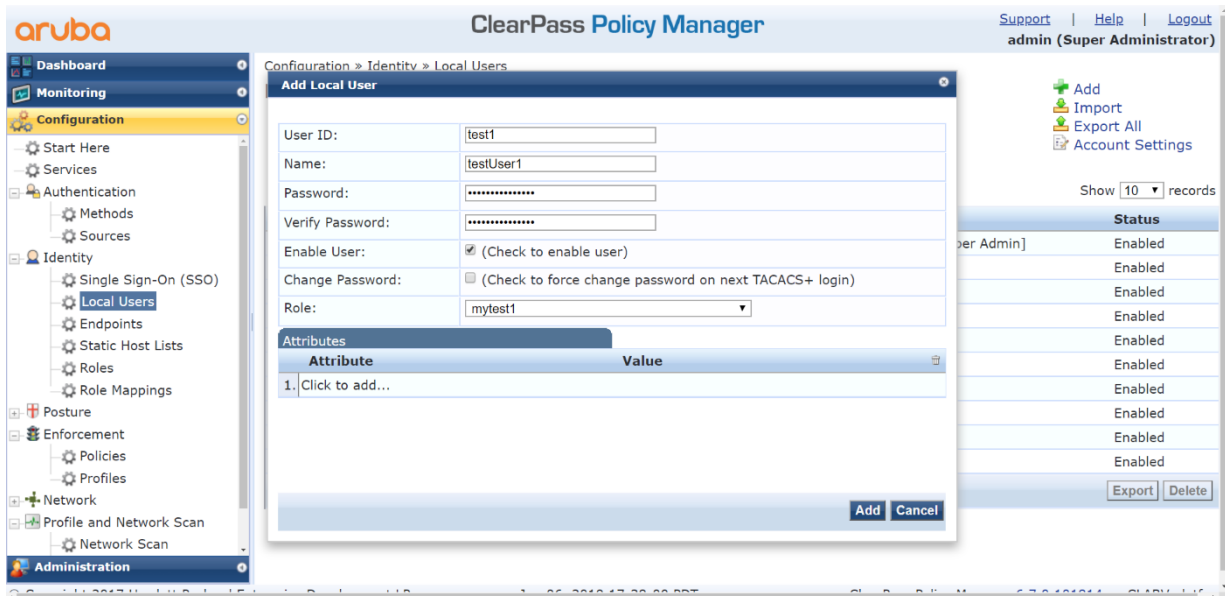
3. Create local users:

a. Go to *Configuration > Identity > Local Users*.

b. Click **Add**.

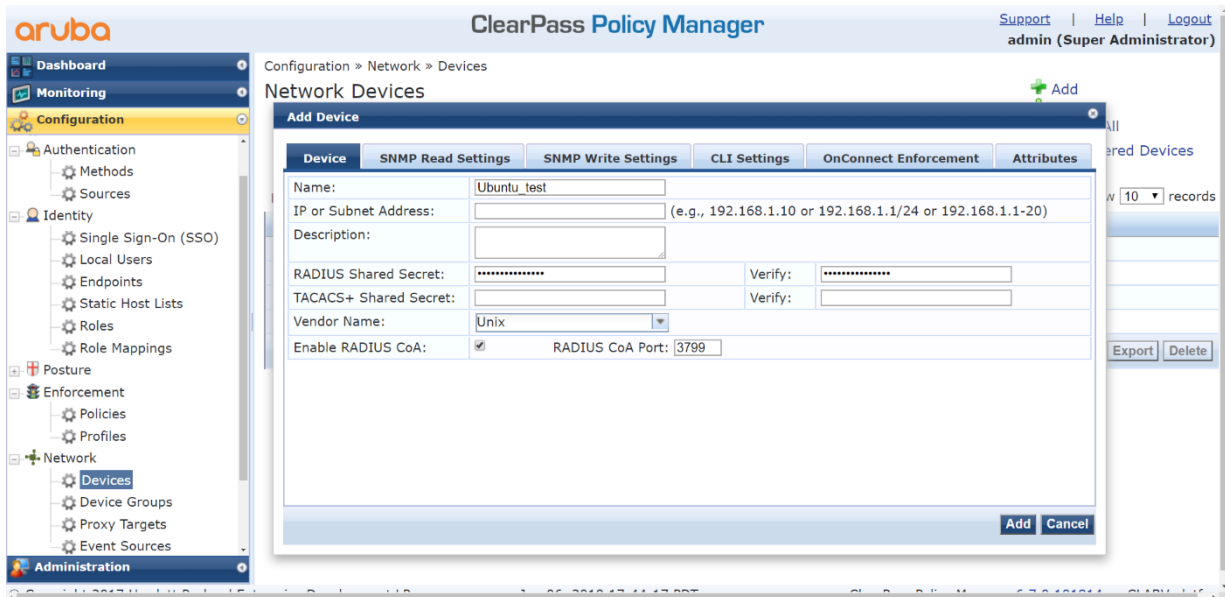
c. Configure the following:

- Set *User ID* to *test1*.
- Set *Name* to *testUser1*.
- Set *Password* to *qa1234*.
- Select *Enable*.
- Set *Role* to *mytest1*.

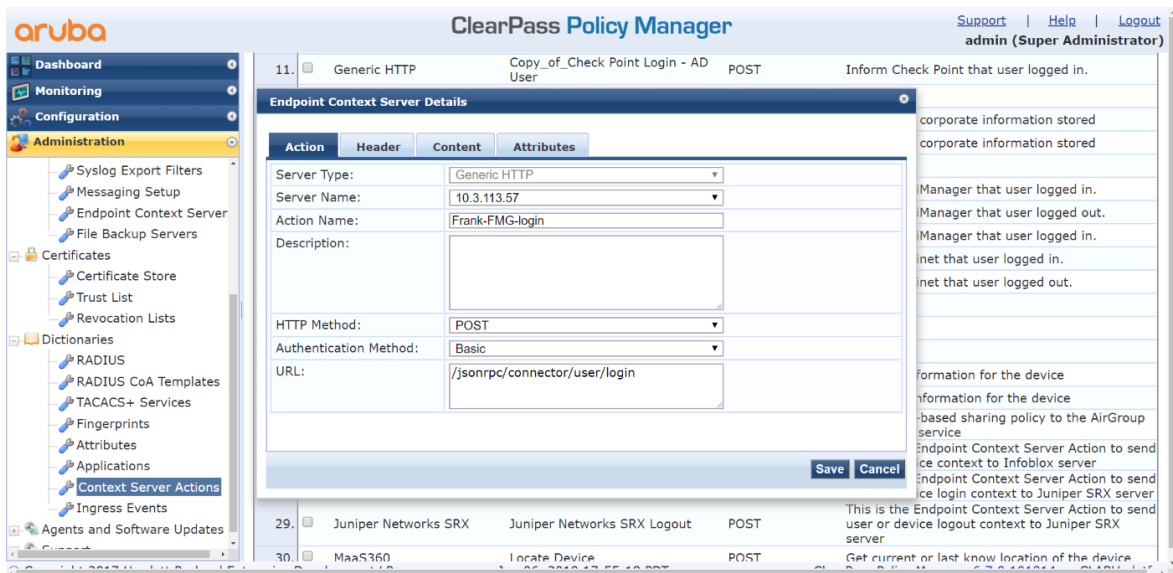


d. Click **Add**.

4. Add an Ubuntu simulator:
 - a. Go to *Configuration > Network > Devices*.
 - b. Click *Add*.
 - c. Configure the following settings:
 - Set *Name* to *Ubuntu_test*.
 - Set *IP or Subnet Address* to *10.3.113.61*.
 - Set *RADIUS Shared Secret* to *qa1234*.
 - Set *Vendor Name* to *Unix*.

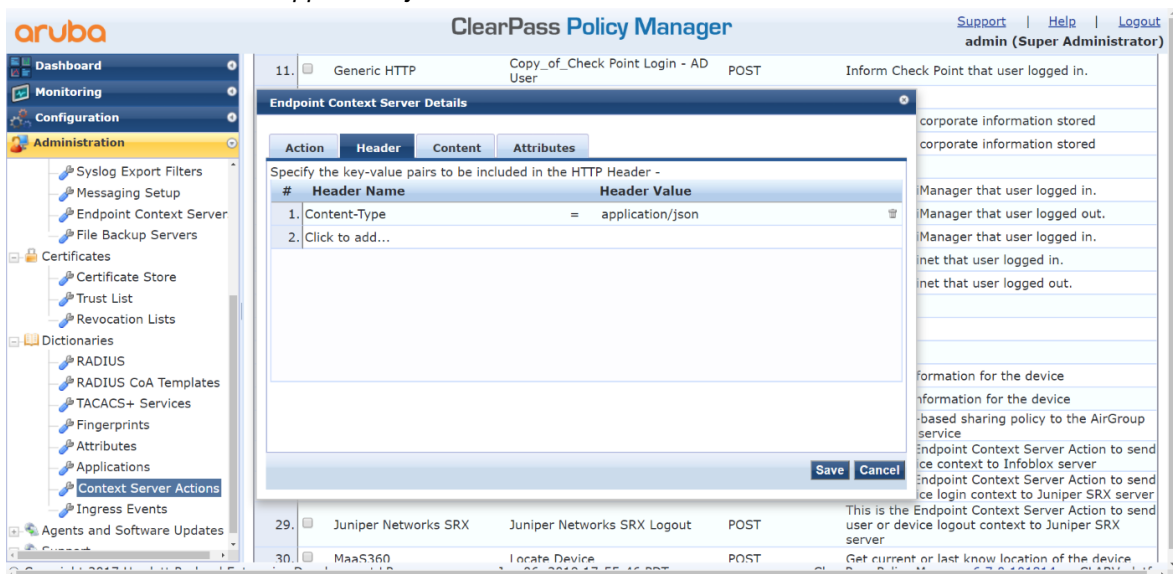


- d. Click *Add*.
5. Configure FortiManager to get packets from ClearPass:
 - a. Add FortiManager as the Endpoint Context Server:
 - i. Go to *Administration > External Servers > Endpoint Context Servers*.
 - ii. Click *Add*.
 - iii. Configure the following:
 - Set *Server Type* to *Generic HTTP*.
 - Set *Server Name* to *10.3.113.57* (the FortiManager IP address).
 - Set *Authentication Method* to *Basic*.
 - Set *Username* to *admin* (the administrator on FortiManager).
 - b. Create Endpoint Context Server Login action for FortiManager:
 - i. Go to *Administration > Dictionaries > Context Server Actions*
 - ii. Click *Add*.
 - iii. On the *Action* tab, configure the following:
 - Set *Server Type* to *Generic HTTP*.
 - Set *Server Name* to *10.3.113.57* (the FortiManager IP address).
 - Set *Action Name* to *Frank-FMG-login*.
 - Set *Description* to *Inform FortiManager that the user logged on*.
 - Set *HTTP Method* to *POST*.
 - Set *Authentication Method* to *Basic*.
 - Set *URL* to */jsonrpc/connector/user/login*



iv. On the *Header* tab, configure the following:

- Set *Header Name* to *Content-Type*.
- Set *Header Value* to *application/json*.



v. On the *Content* tab, configure the following:

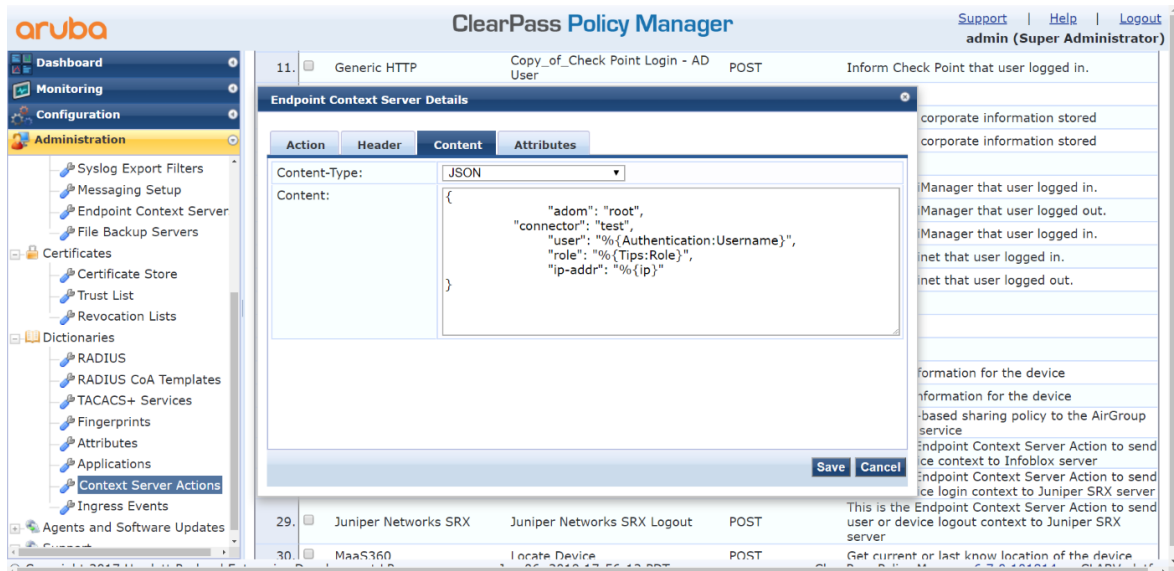
- Set *Content-Type* to *JSON*.
- Set *Content* to:

```
{
```

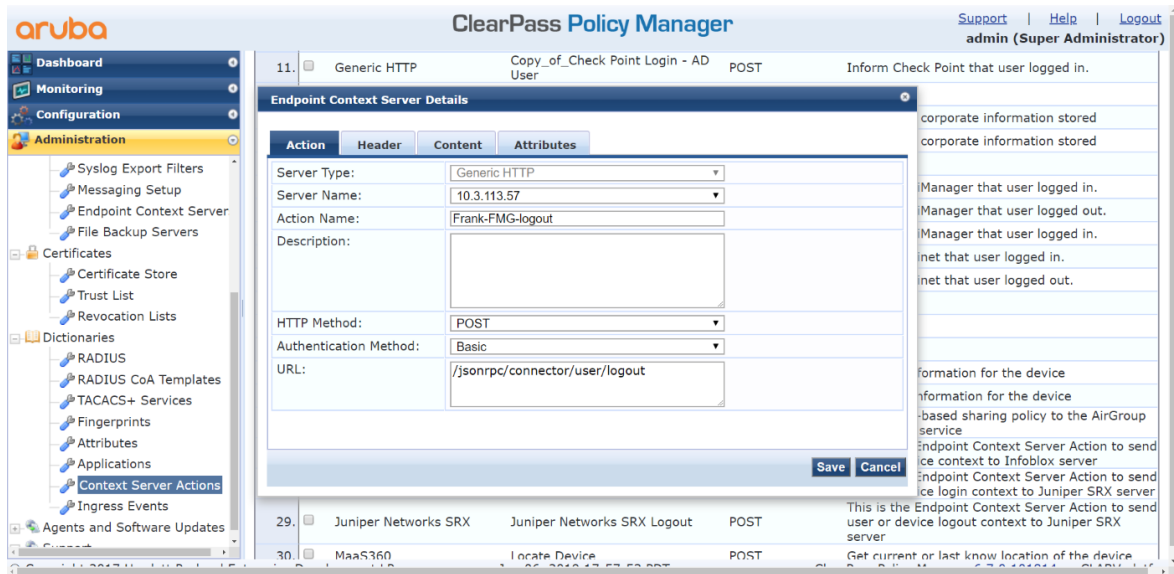
```

"adom": "root",
"connector": "test", <-----the connector name created on FortiManager
"user": "%{Authentication:Username}",
"role": "%{Tips:Role}",
"ip-addr": "%{ip}"
}

```



- vi. Click **Save**.
- c. Create Endpoint Context Server Logout action for FortiManager:
 - i. Go to **Administration > Dictionaries > Context Server Actions**
 - ii. Click **Add**.
 - iii. On the **Action** tab, configure the following:
 - Set **Server Type** to *Generic HTTP*.
 - Set **Server Name** to *10.3.113.57* (the FortiManager IP address).
 - Set **Action Name** to *Frank-FMG-logout*.
 - Set **Description** to *Inform FortiManager that the user logged out*.
 - Set **HTTP Method** to *POST*.
 - Set **Authentication Method** to *Basic*.
 - Set **URL** to */jsonrpc/connector/user/logout*



iv. On the *Header* tab, configure the following:

- Set *Header Name* to *Content-Type*.
- Set *Header Value* to *application/json*.

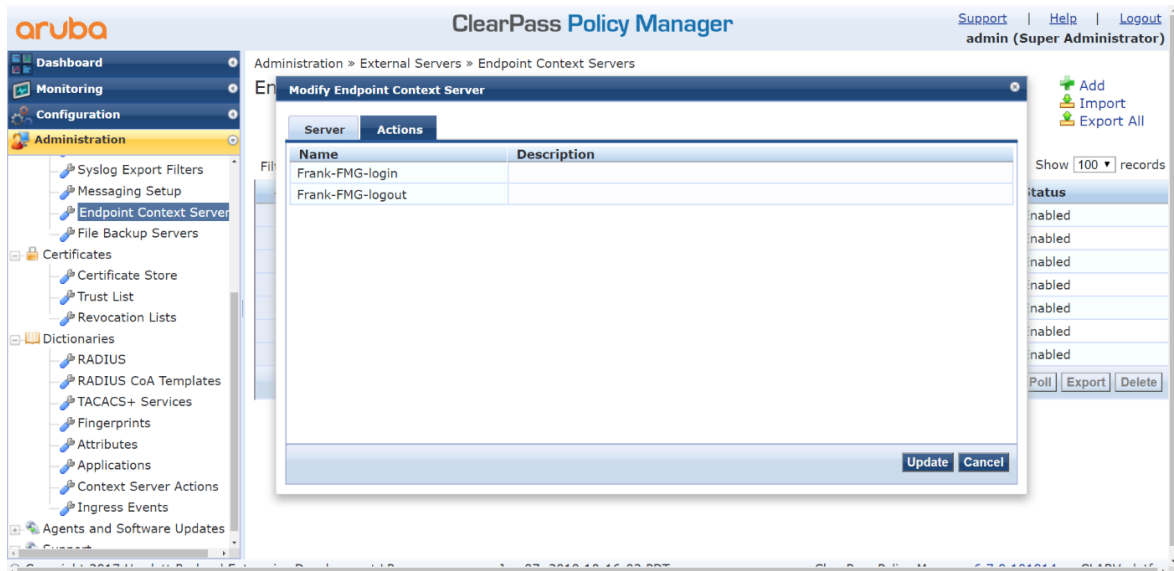
v. On the *Content* tab, configure the following:

- Set *Content-Type* to *JSON*.
- Set *Content* to:

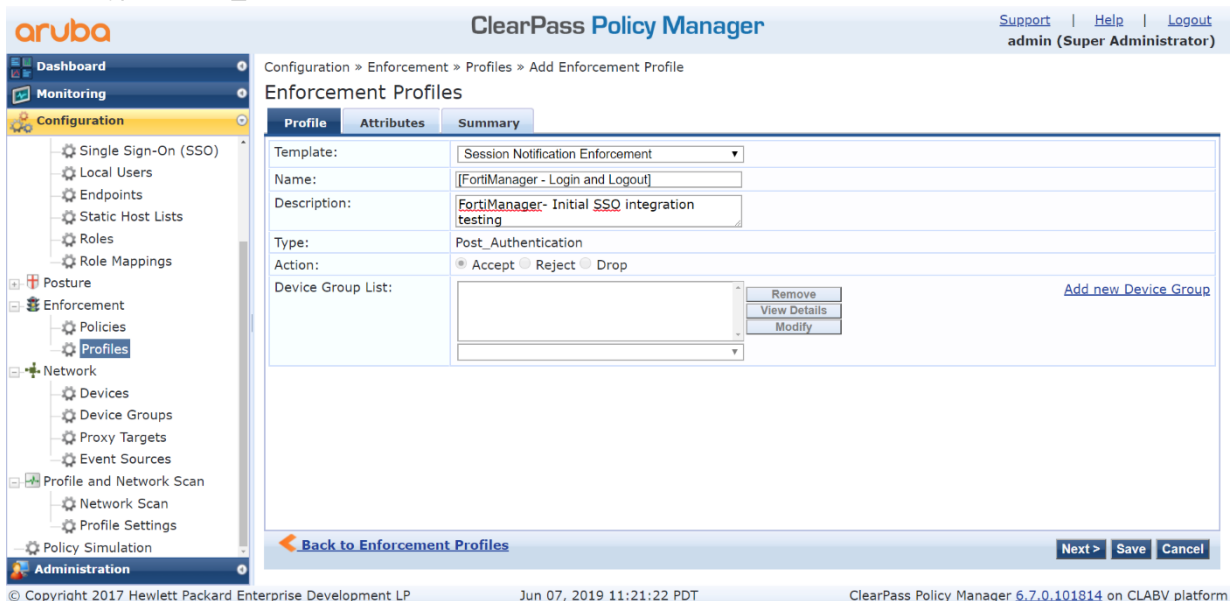
```
{
  "adom": "root",
  "connector": "test",
  "user": "%{Authentication:Username}",
  "role": "%{Tips:Role}",
  "ip-addr": "%{ip}"
}
```

vi. Click **Save**.

- d. Check that the actions are added to the server:
 - i. Go to *Administration > External Servers > Endpoint Context Servers > 10.3.113.57 > Actions*.
 - ii. Locate the two just created actions.



6. Create a profile:
 - a. Go to *Configuration > Enforcement > Profiles*.
 - b. Click **Add**.
 - c. On the *Profile* tab, configure the following:
 - Set *Template* to *Session Notification Management*.
 - Set *Name* to *FortiManager Login and Logout*.
 - Set *Description* to *FortiManager - Initial SSO integration testing*.
 - Set *Type* to *Post_Authentication*.



- d. On the *Attributes* tab, configure the following attributes:

Type	Name	Value
Session-Notify	Server Type	Generic HTTP
Session-Notify	Login Action	Frank-FMG-login
Session-Notify	Logout Action	Frank-FMG-logout
Session-Notify	Server IP	10.3.113.57

aruba ClearPass Policy Manager

Configuration > Enforcement > Profiles > Add Enforcement Profile

Enforcement Profiles

Type	Name	Value
1. Session-Notify	Server Type	= Generic HTTP
2. Session-Notify	Login Action	= Frank-FMG-login
3. Session-Notify	Logout Action	= Frank-FMG-logout
4. Session-Notify	Server IP	= 10.3.113.57
5. Click to add...		

Back to Enforcement Profiles

Next > Save Cancel

© Copyright 2017 Hewlett Packard Enterprise Development LP Jun 07, 2019 10:28:12 PDT ClearPass Policy Manager 6.7.0.101814 on CLABV platform

- e. Click Save.

7. Create a policy:

- Go to *Configuration > Enforcement > Policies*.
- Click Add.
- On the *Enforcement* tab, configure the following:
 - Set *Name* to *FortiManager testing*.
 - Set *Enforcement Type* to *RADIUS*.
 - Set *Default Profile* to *Allow Access Profile*.

aruba ClearPass Policy Manager

Support | Help | Logout
admin (Super Administrator)

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement Rules Summary

Name: fortimanager testing

Description:

Enforcement Type: ☒ RADIUS ☐ TACACS+ ☐ WEBAUTH (SNMP/Agent/CLI/CoA) ☐ Application ☐ Event

Default Profile: [Allow Access Profile] [View Details](#) [Modify](#) [Add new Enforcement Profile](#)

[Back to Enforcement Policies](#) [Next >](#) [Save](#) [Cancel](#)

© Copyright 2017 Hewlett Packard Enterprise Development LP Jun 07, 2019 10:31:04 PDT ClearPass Policy Manager 6.7.0.101814 on CLABV platform

d. On the *Rules* tab, configure the following:

- Set *Type* to *Date*.
- Set *Name* to *Date-Time*.
- Set *Operation* to *EXISTS*.
- Set *Profile Names* to *[Post Authentication][FortiManager - Login and Logout]*.

aruba ClearPass Policy Manager

Support | Help | Logout
admin (Super Administrator)

Configuration » Enforcement » Policies » Add

Rules Editor

Conditions

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Date	Date-Time	EXISTS	
2. Click to add...			

Enforcement Profiles

Profile Names: [Post Authentication][FortiManager - Login and Logout] [Move Up](#) [Move Down](#) [Remove](#)

[Back to Enforcement Policies](#) [Next >](#) [Save](#) [Cancel](#)

© Copyright 2017 Hewlett Packard Enterprise Development LP Jun 07, 2019 10:32:58 PDT ClearPass Policy Manager 6.7.0.101814 on CLABV platform

e. Click *Save*.

8. Create services:

- Go to *Configuration > Services*.
- Click *Add*.
- On the *Service* tab, configure the following:
 - Set *Name* to *API Test Access OAuth2 API User Access*.
 - Set *Description* to *Authentication service for API access using OAuth2*.

- Set *Type* to *Aruba Application Authentication*.
- Set *Status* to *Enabled*.

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration (selected), and Administration. Under Configuration, there are links for Start Here, Services (selected), Authentication, Identity, Posture, Enforcement, Policies, Profiles, Network, Profile and Network Scan, and Policy Simulation. The main content area displays the configuration for 'API Test Access OAuth2 API User Access'. The 'Summary' tab is active, showing fields for Name, Description, Type, Status, Monitor Mode, and More Options. The 'Service Rule' section shows a table with columns Type, Name, and Operator. The table contains one row: '1. Application' with Name 'Name' and Operator 'EQUALS'. At the bottom, there are buttons for 'Back to Services', 'Disable', 'Copy', 'Save', and 'Cancel'.

Configuration > Services > Edit - API Test Access OAuth2 API User Access

Services - API Test Access OAuth2 API User Access

Summary Service Authentication Roles Enforcement

Name: API Test Access OAuth2 API User Access

Description: Authentication service for API access using OAuth2

Type: Aruba Application Authentication

Status: Enabled

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization

Service Rule

Matches ☒ ANY or ☐ ALL of the following conditions:

Type	Name	Operator
1. Application	Name	EQUALS
2. Click to add...		

Back to Services

Disable Copy Save Cancel

© Copyright 2017 Hewlett Packard Enterprise Development LP Aug 23, 2019 10:56:11 PDT ClearPass Policy Manager 6.7.0.101814 on CLABV platform

- d. On the *Authentication* tab, set *Authentication Sources* to:

[Local User Repository] [Local SQL DB]
[Admin User Repository] [Local SQL DB]

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration (selected), and Administration. Under Configuration, there are links for Start Here, Services (selected), Authentication, Identity, Posture, Enforcement, Policies, Profiles, Network, Profile and Network Scan, and Policy Simulation. The main content area displays the configuration for 'API Test Access OAuth2 API User Access'. The 'Summary' tab is active, showing fields for Name, Description, Type, Status, Monitor Mode, and More Options. The 'Service Rule' section shows a table with columns Type, Name, and Operator. The table contains one row: '1. Application' with Name 'Name' and Operator 'EQUALS'. At the bottom, there are buttons for 'Back to Services', 'Disable', 'Copy', 'Save', and 'Cancel'.

Configuration > Services > Edit - API Test Access OAuth2 API User Access

Services - API Test Access OAuth2 API User Access

Summary Service Authentication Roles Enforcement

Name: API Test Access OAuth2 API User Access

Description: Authentication service for API access using OAuth2

Type: Aruba Application Authentication

Status: Enabled

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization

Service Rule

Matches ☒ ANY or ☐ ALL of the following conditions:

Type	Name	Operator
1. Application	Name	EQUALS
2. Click to add...		

Back to Services

Disable Copy Save Cancel

© Copyright 2017 Hewlett Packard Enterprise Development LP Aug 23, 2019 10:56:11 PDT ClearPass Policy Manager 6.7.0.101814 on CLABV platform

- e. On the *Enforcement* tab, configure the following:

- Set *Enforcement Policy* to *[Guest Operator Logins]*.
- Set *Description* to *Enforcement policy controlling access to Guest application.*
- Set *Default Profile* to *[Deny Application Access Profile]*.

- Set *Rules Evaluation Algorithm* to *first-applicable*.
- Create the following two conditions:

Conditions		Enforcement Profiles
1.	(Tips:Role EQUALS [User Authenticated]) AND (Authentication:Source EQUALS [Local User Repository])	[Operator Login - Local Users]
2.	(Tips:Role EQUALS [User Authenticated]) AND (Authentication:Source EQUALS [Admin User Repository])	[Operator Login - Admin Users]

- Click **Save**.
- Click **Add** again to add another service.
- On the **Service** tab, configure the following:
 - Set *Name* to *AuthN user for Fortimanager Testing*.
 - Set *Description* to *Authorization service for AirGroup device access*.
 - Set *Type* to *RADIUS Enforcement (Generic)*.
 - Set *Status* to *Enabled*.
 - Create the following service rule:

Type	Name	Operator	Value
Radius:IEFT	NAS-IP-Address	EQUALS	10.0.0.1

- On the **Authentication** tab, configure the following:
 - Set *Authentication Methods* to *[PAP]*.
 - Set *Authentication Sources* to *[Local User Repository] [Local SQL DB]*.
- On the **Enforcement** tab, configure the following:
 - Set *Enforcement Policy* to *fortimanager testing*.
 - Set *Default Profile* to *[AllowAccess Profile]*.

- Set *Rules Evaluation Algorithm* to *evaluate-all*.
- Create the following condition:

Conditions	Enforcement Profiles
1. (GuestUser:Company Name NOT_EQUALS ABCDE)	[FortiManager-login and Logout]

The screenshot shows the ClearPass Policy Manager web interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Start Here, Services, Authentication, Identity, Posture, Enforcement, Policies, Profiles, Network, Profile and Network Scan, and Policy Simulation. The main content area is titled 'ClearPass Policy Manager' and shows the configuration for 'AuthN user for FortiManager Testing'. The 'Configuration' tab is selected, and the 'Service' sub-tab is active. The 'Service' section shows the following details:

- Name: AuthN user for FortiManager Testing
- Description: Authorization service for AirGroup device access
- Type: RADIUS Enforcement (Generic)
- Status: Enabled
- Monitor Mode: Disabled
- More Options: -

The 'Service Rule' section shows a table with the following data:

Type	Name	Operator	Value
1. Radius:IETF	NAS-IP-Address	EQUALS	10.0.0.1

The 'Authentication' section shows the following details:

- Authentication Methods: [PAP]
- Authentication Sources: [Local User Repository]
- Strip Username Rules: -
- Service Certificate: -

The 'Roles' section shows the following details:

- Role Mapping Policy: -

The 'Enforcement' section shows the following details:

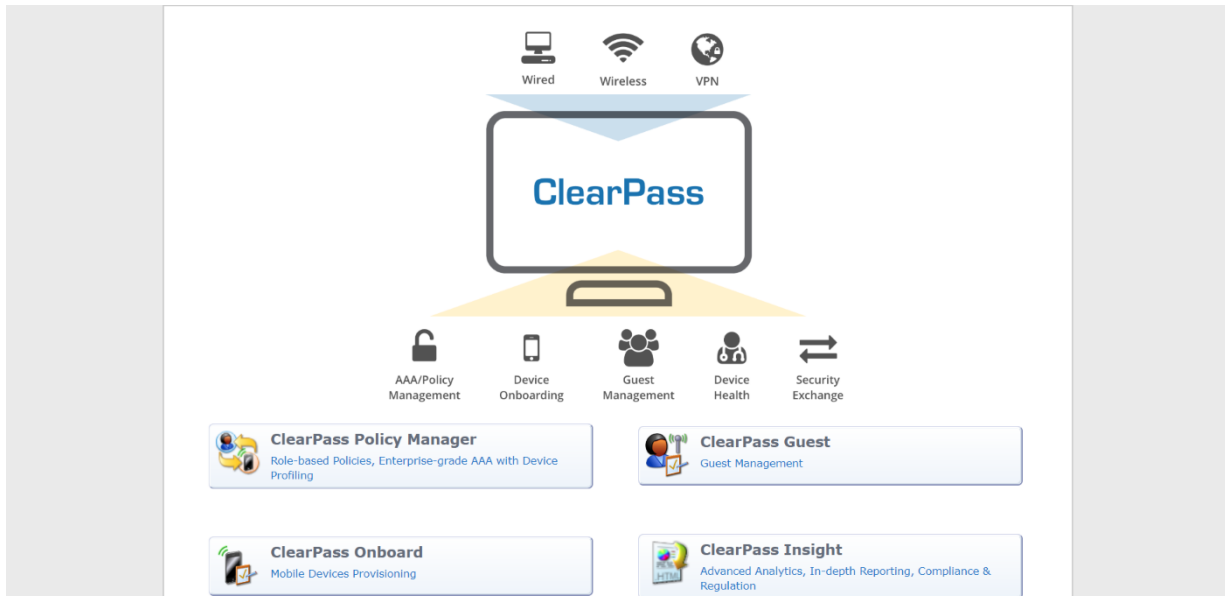
- Use Cached Results: Disabled
- Enforcement Policy: fortimanager testing

At the bottom of the configuration page, there are buttons for 'Back to Services', 'Disable', 'Copy', 'Save', and 'Cancel'. The footer of the page contains the following information:

© Copyright 2017 Hewlett Packard Enterprise Development LP Aug 23, 2019 10:59:28 PDT ClearPass Policy Manager 6.7.0.101814 on CLABV platform

- k. Click **Save**.
9. Configure the administrator the FortiManager fabric connector uses to access CPPM APIs:
 - a. Go to *Administration > Admin Users*.
 - b. Click **Add**.
 - c. Configure the following:
 - Set *User ID* to *admin*.
 - Set *Name* to *admin*.
 - Set *Password* to *qa987654*.
 - In *Verify Password* enter the password again.
 - Select *Enable User*.
 - Set *Privilege Level* to *API Administrator*.
 - d. Click **Save**.

10. Create an API Client:

a. Log in to *ClearPass Guest*.b. Go to *Administration > API Services > API Clients*.c. Click *Create API Client*.

d. Configure the following:

- Set *Client ID* to *test*.
- Set *Description* to *FMG login from it*.
- Select *Enable API client*.
- Set *Operator Profile* to *Super Administrator*.
- Set *Grant Type* to *Username and password credentials (grant_type=password)*.
- In *Public Client* select *This client is public (trusted) client*.
- In *Refresh Token* select *Allow the use of refresh tokens for this client*.

The screenshot shows the 'Create API Client' form in the ClearPass Guest interface. The form is titled 'Create API Client' and includes the following fields and options:

- * Client ID:** test
- Description:** FMG login from it
- Enabled:** ☒ Enable API client
- * Operator Profile:** Super Administrator
- * Grant Type:** Username and password credentials (grant_type=password)
- Public Client:** ☒ This client is a public (trusted) client
- Refresh Token:** ☒ Allow the use of refresh tokens for this client
- Access Token Lifetime:** 8 hours
- Refresh Token Lifetime:** 14 days

The form also includes a sidebar with navigation options: Guest, Onboard, Configuration, Administration, Start Here, AirGroup Services, API Services, API Explorer, SOAP Web Services, Data Retention, Extensions, Import Configuration, Operator Logins, Plugin Manager, and Support.

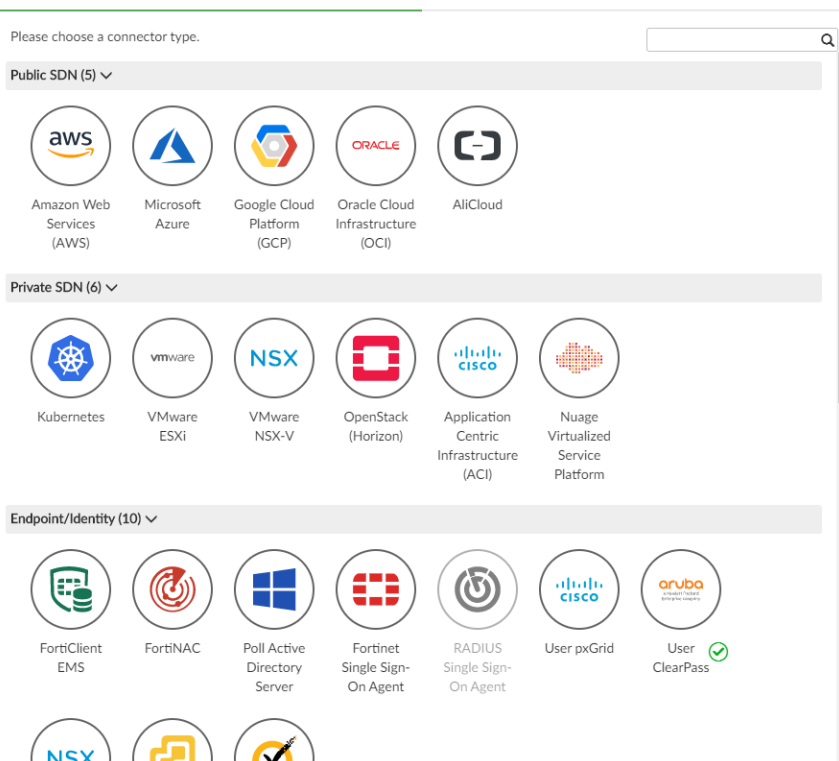
e. Click *Save*.

To configure FortiManager:

1. Log in to FortiManager.
2. Run the following CLI command:

```
config system admin user
  edit admin
    set rpc-permit read-write
  next
end
```
3. Go to *Fabric View > Fabric Connectors*.
4. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.

Create New Fabric Connector



5. Under *Endpoint/Identity*, select *User ClearPass*.
6. Configure the following:
 - Set *Name* to *test*. This name must be same as the one used in the ClearPass actions.
 - Set *Status* to *On*.
 - Set *Server* to *10.3.113.102* (the ClearPass IP address).
 - Set *Client* to *test* (the previously created ClearPass API client).
 - Set *User* to *admin* (the ClearPass login name).
 - Set *Password* to *qa1234* (the ClearPass login password).

Create New Fabric Connector

Endpoint/Identity
User ClearPass

Connector Settings

Name	<input type="text"/>
Status	<input type="checkbox"/> OFF
Server	<input type="text"/>
Client	<input type="text"/>
User	<input type="text"/>
Password	<input type="password"/>

< Back

Apply & Refresh

OK

Cancel

7. Click **OK**.

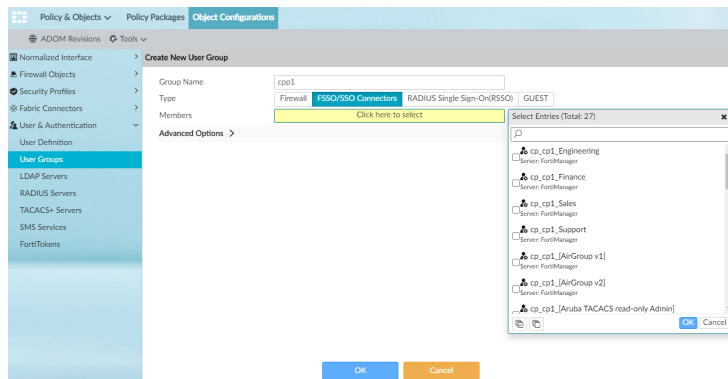
8. Get the role and user from ClearPass:

- Go to *Policy & Objects > Object Configurations > Fabric Connectors > Endpoint/Identity*.
- Edit the ClearPass connector and click *Apply & Refresh*.

FortiManager retrieves the roles and users from ClearPass. Users with green icons are currently logged in.

9. Install the address group from ClearPass to FortiGate:

- On the FortiManager, go to *Policy & Objects > Object Configurations > User & Authentication > User Groups*.
- Click *Create New*.
- Configure the following:
 - Set *Group Name* to *cpp1*.
 - Set *Type* to *FSSO/SSO Connectors*.
 - Select *Members* as *ClearPass adgrp*.



10. Use the new user group in a policy to install it to FortiGate.

11. To check that the group was installed on the FortiGate:

- a. On the FortiGate, go to *User & Device > User Groups*. The group will be in the user group list.
- b. Edit the group to view its members.
- c. In the CLI console, enter the following:

```
# diagnose debug authd fsso list
----FSSO logons----
IP: 10.210.15.185  User: user1  Groups: cp_test_Finance  Workstation:  MemberOf: cppl
Total number of logons listed: 1, filtered: 0
----end of FSSO logons----
```

Creating VMware NSX-T connector

With FortiManager, you can create a fabric connector for VMware NSX-T. You can create multiple VMware NSX-T connectors per ADOM.

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.

To enable read-write JSON API access:

1. Go to *System Settings > Administrators*.
2. Double-click the *admin* account to open it for editing.
3. Beside *JSON API Access*, select *Read-Write*, and click *OK*.

To create a fabric connector for VMware NSX-T:

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

3. Under *Endpoint/Identity*, select *VMware NSX-T*. The *VMware NSX-T* screen is displayed.

Create New Fabric Connector NSX Endpoint/Identity
VMware NSX-T

Connector Settings

Name

Status ☐ OFF

NSX-T Manager Configurations

Server

User Name

Password

FortiManager Configurations

IP Address

User Name

Password

4. Configure the following options, and then click *OK*:

Name	Type a name for the fabric connector object.
Status	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.
NSX-T Manager Configuration	
Server	Type the IP address of the NSX-T server.
User Name	Type the user name for the NSX-T server.
Password	Type the password for the NSX-T server.
FortiManager Configurations	
IP Address	Type the IP address for FortiManager.
User Name	Type the user name for FortiManager.
Password	Type the password for FortiManager.

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

5. Edit the connector to set *Status* to *On*.
FortiManager retrieves the groups from VMware NSX-T and stores them as dynamic firewall objects.

To download the FortiGate VM deployment image:

- Download the preconfigured deployment image from the Fortinet Support Site for (<https://support.fortinet.com>) FortiGate VM for VMware NSX-T:
`fortigate-vm64-nsxt.ovf`
- Place the deployment image on a server that VMware NSX-T and FortiManager can access.
- Note the URL for the deployment image. You will need to add the URL to FortiManager.

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

1. Ensure that you know the URL for the location of the preconfigured deployment image for FortiGate VM and VMware NSX-T.
2. On the *Fabric View* pane, edit the connector for VMware NSX-T, and click *Add Service*.
3. In the *Service Name* box, type a name for the service.
4. In the *Integration* box, select *East-West* or *North-South* to specify the direction of network traffic.
5. In the *Image Location* box, type the URL for the location of the preconfigured deployment file for FortiGate VM.
6. Click *OK*.

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

To deploy a FortiGate VM from VMware NSX-T and enable central management:

1. Go to VMware NSX-T manager, and deploy the FortiGate VM.
The deployment file is configured to automatically enable central management.
2. When prompted by the deployment of FortiGate VM, enter the IP address of the FortiManager used for central management.
The FortiGate is displayed in FortiManager on the *Device Manager* pane as an unauthorized device.
3. On FortiManager, go to *Device Manager* and authorize the FortiGate.

To complete the fabric connector setup:

1. In the policy package in which you will be creating the new policy, create an IPv4 virtual wire pair policy and include the firewall address objects for VMware NSX-T. See [IP policies on page 214](#).
2. Install the policy package to FortiGate. See [Install a policy package on page 195](#).
FortiGate communicates with NSX-T via FortiManager to dynamically populate the firewall address objects with IP addresses.

FortiView

Use FortiView to view the configuration status of managed devices.

- [Monitors on page 349](#)

If FortiAnalyzer features are enabled, the FortiView pane and additional monitors are available. For more information, see the *FortiAnalyzer Administration Guide*.

Monitors

FortiView *Monitors* include a predefined dashboard for *Device Status*.

- [Device Status on page 350](#)
- [Using the Monitors dashboard on page 351](#)



To prevent timeout, ensure *Idle Timeout* is greater than the widget's *Refresh Interval*. See [Idle timeout on page 636](#) and [Settings icon on page 352](#).

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:

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

The *Device Status* dashboard includes the following information:

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

- IP address
- Firmware version

Information about the following statuses of the selected device is also displayed on the right:

- Connectivity status
- Support Contracts
- Licenses
- Configuration Status and Policy Package Status

The colored rings in the circle correspond to the status information on the right. The outer ring in the circle corresponds with the *Connectivity* status. The second most outer ring corresponds to the *Supports Contracts* status, and so on.

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

Using the Monitors dashboard

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

Edit Dashboard	Add, remove, resize, or move widgets on a predefined dashboard.
Devices	Select the devices to include in the widget data.
Time Period	Select a time period from the dropdown menu, or set a custom time period.
Refresh	Refresh the data in the widgets.
Background theme	Change the background color of the dashboard to make widgets easier to view in different room lighting. <ul style="list-style-type: none"> • <i>Day</i> shows a brighter gray background color. • <i>Night</i> shows a black background. • <i>Ocean</i> shows a blue background color.

Hide Side-menu or Show Side-menu	Hide or show the tree menu on the left. In a typical SOC environment, the side menu is hidden and dashboards are displayed in full screen mode.
---	---

Use the controls in the widget title bar to work with widgets.

Settings icon	Change the settings of the widget.
----------------------	------------------------------------

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:

IPsec VPN	Displays all of defined IPsec VPN communities and associated devices for the selected ADOM. You can create, monitor, and manage VPN settings. See IPsec VPN Communities on page 369
Monitor	Displays a list of IPsec VPN tunnels, and allows you to bring the tunnels up or down. See Monitoring IPsec VPN tunnels on page 378 .
Map View	Displays a world map showing IPsec VPN tunnels. See Map View on page 378
SSL-VPN	Create, monitor, and manage SSL-VPN settings. You can also create, edit, and delete portal profiles for SSL-VPN settings. See SSL VPN on page 388 .

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 354](#).

You can also configure VPN settings directly on a FortiGate by using *Device Manager*, and the configuration is stored in the device database. When you create a VPN configuration by using *VPN Manager*, FortiManager copies the VPN configuration from the objects database to the device database before installing the configuration to FortiGates. In addition, FortiManager checks for differences between the configuration in the device database and the configuration on FortiGate. If any differences are found, FortiManager only installs the configuration differences to FortiGate. This process helps avoid conflicts.



If you are using both *Device Manager* and *VPN Manager* to configure VPN settings, you should avoid using *Device Manager* to modify the settings created by *VPN Manager*, because when installing a policy package again, the settings from *VPN Manager* will override the previous changes to those settings from *Device Manager*. *Device Manager* should only be used to create or modify VPN configurations that are not created by *VPN Manager*.

To create IPsec VPN settings:

1. Enable central VPN management. See [Enabling central VPN management on page 354](#).
2. Create a VPN community, sometimes called a VPN topology. See [Creating IPsec VPN communities on page 370](#).
3. Create a managed gateway. See [Creating managed gateways on page 380](#).

To create SSL-VPN settings:

1. Create custom profiles. See [Creating SSL VPN portal profiles on page 391](#).
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 388](#).

To install VPN objects to devices:

1. Plan the VPN security policies. See [VPN security policies on page 386](#).
2. In a policy package, create VPN security policies, and select the VPN settings. See [Creating policies on page 206](#).
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 198](#).
4. Install the policy package to the devices. See [Install a policy package on page 195](#).

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 Configurations menu to enable DDNS on each FortiGate device. The CLI Configurations menu is available in the Device Manager pane. See [CLI Configurations menu on page 70](#).

With the CLI Configurations menu, you can use the `config system ddns` command to enable DDNS on a per-device basis. The selected monitoring interface must be the interface that supports your tunnel, for example:

```
config system ddns
  edit 1
    set ddns-server FortiGuardDDNS
    set ddns-domain "<HOST1>.fortiddns.com"
    set monitor-interface "port14"
  next
end
```

You can also use the CLI Configurations menu to configure DDNS on multiple FortiGate interfaces. Once configured, you can use FortiManager to view all the DDNS entries, but you cannot edit the entries.

Following is an example of how to configure DDNS on multiple FortiGates by using the CLI Configurations menu:

```
config system ddns
  edit 1
    set ddns-server FortiGuardDDNS
    set ddns-domain "<HOST1>.fortiddns.com"
    set use-public-ip enable
    set monitor-interface "wan"
  next
  edit 2
    set ddns-server FortiGuardDDNS
    set ddns-domain "<HOST2>.fortiddns.com"
    set use-public-ip disable
    set monitor-interface "wwan"
  next
end
```

Multiple DDNS entries are useful when using SDWAN and multiple broadband links.

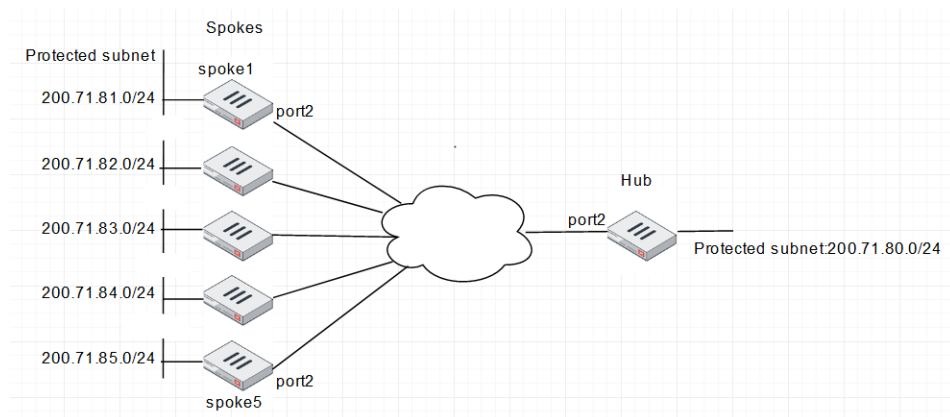
VPN Setup Wizard supports device groups

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

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

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

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



Following is a summary of how to use device groups:

1. Create device groups. See [Creating device groups on page 357](#).
2. Create protected subnet firewall addresses for hub and spoke devices. See [Creating protected subnet firewall addresses on page 357](#).
3. Create a VPN community. See [Creating VPN communities on page 359](#).
4. Add spoke FortiGate units to the VPN community. See [Adding spoke FortiGate units to the VPN community on page 360](#).
5. Add the hub FortiGate units to the VPN community. See [Adding the hub FortiGate unit to the VPN community on page 362](#).
The hub and spokes are created.
6. Install VPN configuration and firewall policies to hub and spoke devices. See [Installing firewall policies to hub and spoke devices on page 365](#)

This topic also covers how to:

- Remove a spoke member from a VPN community. See [Removing a spoke member from a VPN community on page 366](#)
- Add a spoke member to a VPN community. See [Adding a spoke member to a VPN community on page 368](#)

Creating device groups

To create device groups:

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

Create New Device Group

Group Name

spoke_group

Description

+ Add Member

Remove Member

Search...

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

OK

Cancel

5. Click *OK* to save the group.

Creating protected subnet firewall addresses

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

To create protected subnet firewall addresses:

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

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

Create New Address

Address Name	<input type="text" value="Protected_hub_subnet"/>
Color	<div style="border: 1px solid #ccc; width: 20px; height: 20px; background-color: #ccc; display: flex; align-items: center; justify-content: center;">■</div>
Type	<div style="border: 1px solid #ccc; padding: 2px;">Subnet ▼</div>
IP/Netmask	<input type="text" value="200.71.80.0/255.255.255.0"/>
Interface	<div style="border: 1px solid #ccc; padding: 2px;">any ▼</div>
Static Route Configuration	<div style="border: 1px solid #ccc; padding: 2px; text-align: center;">OFF</div>
Comments	<div style="border: 1px solid #ccc; height: 50px; margin-top: 5px;"></div>
Add To Groups	<div style="border: 1px solid #ccc; padding: 2px; text-align: center;">Click here to select</div>

Advanced Options >

Per-Device Mapping	<div style="border: 1px solid #ccc; padding: 2px; text-align: center;">OFF</div>
--------------------	--

4. From the *Create New* menu, select *Address*.

The *Create New Address* pane opens.

5. Create a protected subnet firewall address with per-device mapping for spoke FortiGate units, and click **OK**.

Create New Address

Address Name	<input type="text" value="protected_subnet_spoke"/>
Color	<div style="border: 1px solid #ccc; width: 20px; height: 20px; background-color: #ccc; display: flex; align-items: center; justify-content: center;">■</div>
Type	<div style="border: 1px solid #ccc; padding: 2px;">Subnet ▼</div>
IP/Netmask	<input type="text" value="210.71.0.0/255.255.0.0"/>
Interface	<div style="border: 1px solid #ccc; padding: 2px;">any ▼</div>
Static Route Configuration	<div style="border: 1px solid #ccc; padding: 2px; text-align: center;">OFF</div>
Comments	<div style="border: 1px solid #ccc; height: 50px; margin-top: 5px;"></div>
Add To Groups	<div style="border: 1px solid #ccc; padding: 2px; text-align: center;">Click here to select</div>

Advanced Options >

Per-Device Mapping	<div style="border: 1px solid #ccc; padding: 2px; text-align: center;">ON</div>
--------------------	---

+ Create New
 ✎ Edit
🗑 Delete
⚙ Column Settings ▼

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


Creating VPN communities

To create a VPN community:




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

VPN Topology Setup Wizard

 star

 Description

Choose VPN Topology

 Full Meshed
  Star
  Dial up

< Back

Next >

Cancel

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

VPN Topology Setup Wizard

Authentication & Encryption Settings:

Authentication

Pre-shared Key Certificates



- ☒ Generate (random)
☐ Specify

Encryption

IKE Security (Phase 1) Properties

IKE Version

1 2

#	Encryption	Authentication	
1	AES128	SHA1	+ 
2	AES256	SHA256	+ 

IPsec Security (Phase 2) Properties

< Back

Next >

Cancel

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

VPN Topology Setup Wizard

VPN Zone ☒ ON

☒ Create Default Zones

☐ Use Custom Zone

IKE Security Phase 1 Advanced Properties

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

Exchange Mode ☐ Aggressive ☒ Main (ID Protection)

Key Life (120-172800 seconds)

Dead Peer Detection ☐ Disable ☐ On Idle ☒ On Demand

IPsec Security Phase 2 Advanced Properties

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

< Back Next > Cancel

Adding spoke FortiGate units to the VPN community

To add spoke FortiGate units to the VPN community:

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

VPN Gateway Setup Wizard - star

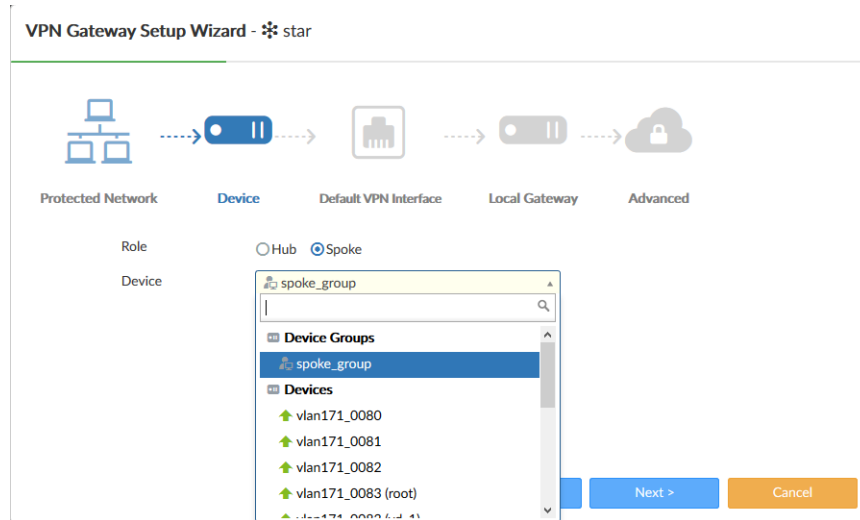
Protected Network Device Default VPN Interface Local Gateway Advanced

Protected Subnet

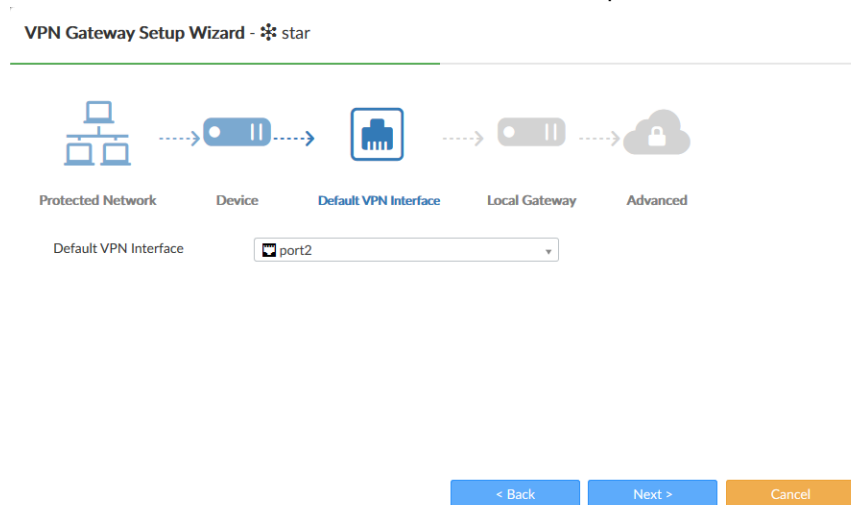
protected_subnet_spoke
IP/Netmask:210.71.0.0/255.255.0.0
1 Entry Selected

< Back Next > Cancel

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

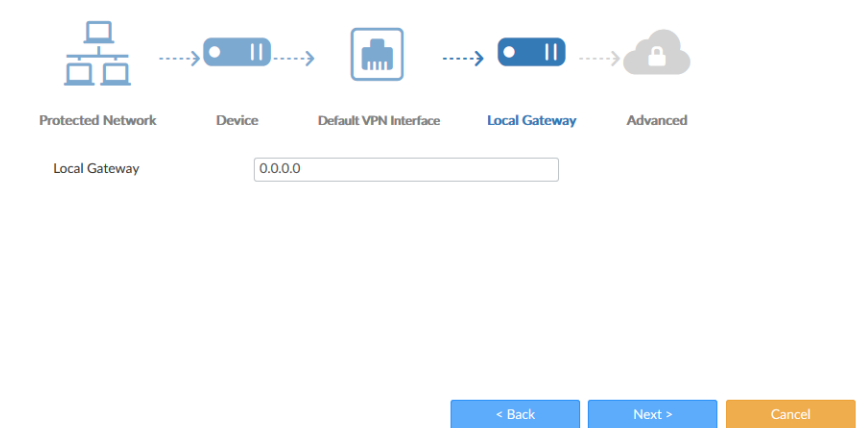


5. Set the *Default VPN Interface* options, and click *Next*.
 - a. Beside *Default VPN Interface*, select the interface for spokes, which is often the internet-facing interface.



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

VPN Gateway Setup Wizard - ⚙️ star



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

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

VPN Gateway Setup Wizard - ⚙️ star

Local ID

Routing ☐ Manual (via Device Manager) ☒ Automatic

Advanced Options >

< Back OK Cancel






Adding the hub FortiGate unit to the VPN community

To add a hub FortiGate unit to the VPN community:

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

3. Set the *Protected Network* options, and then click *Next*:
 - a. Beside *Protected Subnet*, click *Click here to select*, and select the protected subnet.

VPN Gateway Setup Wizard - ⚙️ star



Protected Subnet

Protected_subnet_hub
IP/Netmask:200.71.80.0/255.255.255.0
1 Entry Selected






< Back

Next >

Cancel

4. Set the *Device* options, and then click *Next*:
 - a. Beside *Role*, select *Hub*.
 - b. Beside *Device*, select the device for the hub.

VPN Gateway Setup Wizard - ⚙️ star



Role ☒ Hub ☐ Spoke

Device






< Back

Next >

Cancel

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

VPN Gateway Setup Wizard - ⚙️ star








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

Default VPN Interface

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

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

VPN Gateway Setup Wizard - ⚙️ star



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

Local Gateway

7. Set the *Advanced* options, and click *OK*.

- a. Beside *Routing*, select *Manual (via Device Manager)* or *Automatic*.

VPN Gateway Setup Wizard - star

Local ID:

Routing: ☐ Manual (via Device Manager) ☒ Automatic

Summary Network(s)

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

Advanced Options >

< Back OK Cancel

The hub and spoke are created.

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

VPN Community Install Wizard

star

Name: star

Number of VPN: 2

Authentication: Pre-shared Key

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

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

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

Installing firewall policies to hub and spoke devices

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

To install configurations to hub and spoke devices:

- Go to *Policy & Object > Policy Packages*.
- Create firewall policies for hub and spoke FortiGates.

Policy & Objects Policy Packages Object Configurations ADOM: vpn_mgmt

Policy Package Install ADOM Revisions Tools Collapse All Object Selector

Search...

default IPsec Policy Installation Targets

star IPsec Policy Installation Targets

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

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

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

Install Wizard

☒ **Install Policy Package & Device Settings**

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

Policy Package

star

Comment

0/127

☐ Create ADOM Revision

☐ Schedule Install

☐ **Install Device Settings (only)**

Next >

Cancel

5. Complete the wizard to install the configurations.

Removing a spoke member from a VPN community

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

To remove a spoke member from a VPN community:

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

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

Edit Device Group

Group Name: spoke_group

Description:
 0/128

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

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

OK Cancel

- d. Click OK to save the changes.

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

Install Wizard - Policy Package (star)

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

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

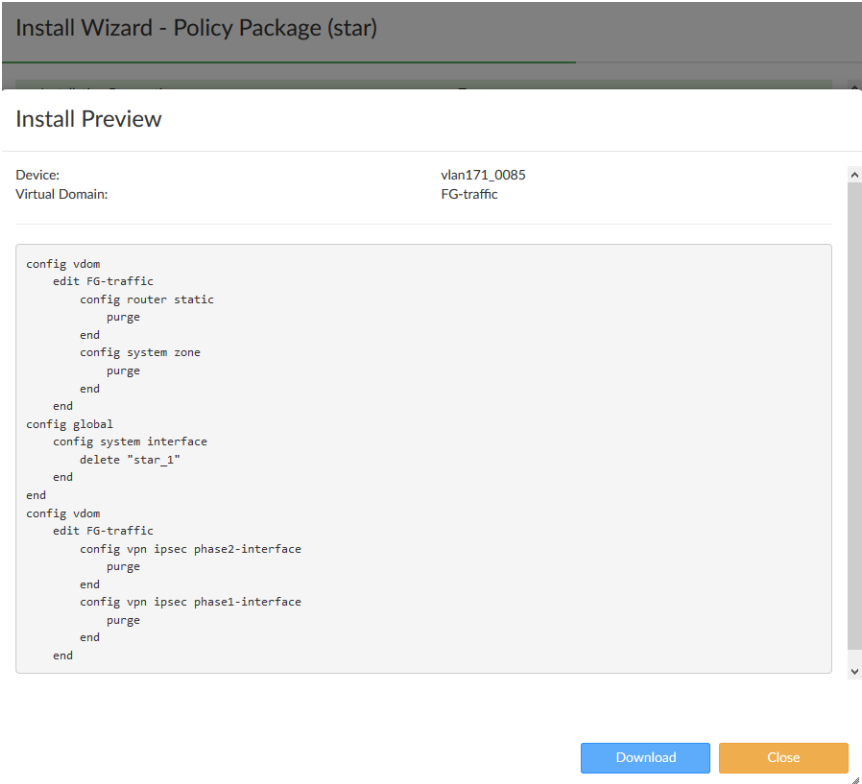
Install Preview

Device: vlan171_0080
Virtual Domain: root

```

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

The *Install Preview* page shows that FortiManager will delete related configurations on the spoke FortiGate named *vlan171_0085*.

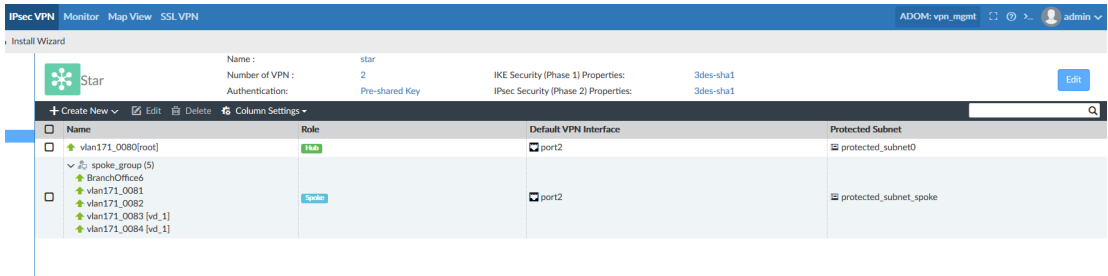


Adding a spoke member to a VPN community

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

To add a new spoke member to a VPN community:

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



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

Install Preview

Device: BranchOffice6

Virtual Domain: root

```
config vpn ipsec phase1-interface
  edit "star_1"
    set interface "port2"
    set comments "[created by FMG VPN Manager]"
    set dhgrp 1 5
    set proposal 3des-sha1
    set keylife 28800
    set peertype any
    set remote-gw 100.71.80.1
    set net-device disable
    set add-gw-route enable
    set psksecret ENC Z8Zpc/bwU2j1HxCfWzO/Xkklz1iO6IOFpF2mmab0XvcAk+pnJrLz5+MLa6KZwR821VYN0GU4AL8P2BL5g5w1irFHSTRfIOE
  next
end
config system interface
  edit "star_1"
    set vdom "root"
    set type tunnel
    set snmp-index 114
    set interface "port2"
  next
end
config system zone
  edit "vpnmgr_star_spoke2hub"
    set interface "star_1"
  next
end
config vpn ipsec phase2-interface
  edit "star_1_0"
    set phase1name "star_1"
    set proposal 3des-sha1
    set auto-negotiate enable
    set comments "[created by FMG VPN Manager]"
    set dhgrp 1 5
    set keylifeseconds 1800
```

IPsec VPN 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.

+ Create New Edit Delete Column Settings

<input type="checkbox"/>	Seq.#	Name	Topology	Gateways	Authentication	Phase 1 Encryption	Phase 2 Encryption	VPN Zone	Description
<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:

VPN Community

Select to create a new VPN community, edit the selected VPN community, or delete the selected VPN community.

Install Wizard

Launch the Install Wizard to install IPsec VPN settings to devices.

Create New	Create a new VPN community. See Creating IPsec VPN communities on page 370
Edit	Edit the selected VPN community. See Editing an IPsec VPN community on page 377 .
Delete	Delete the selected VPN community or communities. See Deleting VPN communities on page 378 .
Column Settings	Configure which columns are displayed, or click <i>Reset to Default</i> to reset the display to the default columns.
Search	Enter a search term to search the communities list.
Configure Gateways	Go to the gateway list for the community. This option is only available from the right-click menu. See IPsec VPN gateways on page 380 .
Add Managed Gateway	Start the <i>VPN Gateway Setup Wizard</i> . This option is only available from the right-click menu. See Creating managed gateways on page 380 .

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 380](#).

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.

VPN Topology Setup Wizard


Name

Description


Choose VPN Topology



Full Meshed



Star



Dial up

< Back Next > Cancel

- Enter a name for the topology in the *Name* field.
- Optionally, enter a brief description of the topology in the *Description* field.
- Choose a topology type: *Full Meshed*, *Star*, or *Dial up*.
 - Full Meshed*: Each gateway has a tunnel to every other gateway.
 - Star*: Each gateway has one tunnel to a central hub gateway.
 - Dial up*: Some gateways, often mobile users, have dynamic IP addresses and contact the gateway to establish a tunnel.
- Click *Next*.

VPN Topology Setup Wizard

Authentication & Encryption Settings:

Authentication Pre-shared Key Certificates

☒ Generate(random)
☐ Specify

Encryption

IKE Security (Phase 1) Properties

IKE Version 1 2

#	Encryption	Authentication	
1	3DES	MD5	+ 🗑
2	AES256	MD5	+ 🗑

IPsec Security (Phase 2) Properties

#	Encryption	Authentication	
1	CHACHA20POLY1305		+ 🗑
2	ARIA256	MD5	+ 🗑

< Back Next > Cancel

- Configure the *Authentication* and *Encryption* information for the topology

8. Click *Next*.
9. Configure the *VPN Zone*, *IKE Security Phase 1 Advanced Properties*, *IPsec Security Phase 2 Advanced Properties*, and *Advanced Options*.
10. Click *Next*.
11. Review the topology information on the *Summary* page, then click *OK* to create the topology.
After you have created the VPN topology, you can create managed and external gateways for the topology.



For descriptions of the options in the wizard, see [VPN community settings on page 372](#).

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"> • <i>Full Meshed</i>: Each gateway has a tunnel to every other gateway. • <i>Star</i>: Each gateway has one tunnel to a central hub gateway. • <i>Dial up</i>: Some gateways, often mobile users, have dynamic IP addresses and contact the gateway to establish a tunnel.
Authentication	Select <i>Certificates</i> or <i>Pre-shared Key</i> . When you select <i>Pre-shared Key</i> , FortiGate implements the Encapsulated Security Payload (ESP) protocol. Internet Key Exchange (IKE) is performed automatically based on pre-shared keys or X.509 digital certificates.
Certificates	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 > Provisioning Templates > Certificate Templates</i> pane.
Pre-shared Key	If you selected <i>Pre-shared Key</i> , select <i>Generate</i> or <i>Specify</i> . When you select <i>Specify</i> , type the pre-shared key that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. You must define the same key at the remote peer or client. The key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters. Alternatively, you can select to generate a random pre-shared key.
Encryption	Define the IKE Profile. Configure IKE Phase 1 and IKE Phase 2 settings.

IKE Security (Phase 1) Properties	Define the Phase 1 proposal settings.
IKE Version	<p>Select IKE version 1 or 2 (default = 2). For more information about IKE v2, refer to RFC 4306.</p>
Encryption Authentication	<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"> • 3DES: Triple-DES, in which plain text is encrypted three times by three keys. • AES128: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key. • AES128GCM: AES128 Galois/Counter Mode (GCM). • AES192: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key. • AES256: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key. • AES256GCM • ARIA128: A 128-bit block size that uses a 128-bit key. • ARIA192: A 128-bit block size that uses a 192-bit key. • ARIA256: A 128-bit block size that uses a 256-bit key. • CHACHA20POLY1305: Arbitrary length, 96-bit nonce, and 256-bit key. • DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • SEED: A 16-round Feistel network with 128-bit blocks and a 128-bit key. <p>Select either of the following authentication message digests to check the authenticity of messages during phase 1 negotiations:</p> <ul style="list-style-type: none"> • 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. <p>Note: If the encryption is GCM or CHACHA20POLY1305, the authentication options are PRFSHA1, PRFSHA256, PRFSHA384, and PRFSHA512.</p> <p>To specify more combinations, use the Add button beside any of the table rows.</p>

IPsec Security (Phase 2) Properties	<p>Define the Phase 2 proposal settings.</p> <p>When you define phase 2 parameters, you can choose any set of phase 1 parameters to set up a secure connection for the tunnel and authenticate the remote peer. Auto Key configuration applies to both tunnel-mode and interface-mode VPNs.</p>
Encryption Authentication	<p>Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required.</p> <p>You need to select at least one combination. The remote peer or client must be configured to use at least one of the proposals that you define. It is invalid to set both Encryption and Authentication to NULL.</p> <p>Select one of the following symmetric-key encryption algorithms:</p> <ul style="list-style-type: none"> • 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. <p>Select either of the following authentication message digests to check the authenticity of messages during phase 1 negotiations:</p> <ul style="list-style-type: none"> • 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)	<p>Select one or more of the following Diffie-Hellman (DH) groups: 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 27, 28, 29, 30, 31.</p> <p>At least one of the DH group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations.</p> <p>Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode.</p>
Exchange Mode	<p>Select either <i>Aggressive</i> or <i>Main (ID Protection)</i>.</p> <p>The FortiGate unit and the remote peer or dialup client exchange phase 1 parameters in either <i>Main (ID Protection)</i> or <i>Aggressive</i> mode. This choice does not apply if you use IKE version 2, which is available only for route-based configurations.</p> <ul style="list-style-type: none"> 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. <p>Although Main mode is more secure, you must select Aggressive mode if there is more than one dialup Phase 1 configuration for the interface IP address, and the remote VPN peer or client is authenticated using an identifier local ID). Descriptions of the peer options in this guide indicate whether Main or Aggressive mode is required.</p>
Key Life	Type the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The keylife can be from 120 to 172800 seconds.
Dead Peer Detection	Select this checkbox to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required. You can use this option to receive notification whenever a tunnel goes up or down, or to keep the tunnel connection open when no traffic is being generated inside the tunnel. For example, in scenarios where a dialup client or dynamic DNS peer connects from an IP address that changes periodically, traffic may be suspended while the IP address changes.
IPsec Security Phase 2 Advanced Properties	

Diffie Hellman Group(s)	<p>Select one or more of the following Diffie-Hellman (DH) groups: 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 27, 28, 29, 30, 31.</p> <p>At least one of the DH group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations.</p> <p>Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode.</p>
Replay detection	Select to enable or disable replay detection. Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel.
Perfect forward secrecy (PFS)	<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>
Key Life	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.
Autokey Keep Alive	<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>
Auto-Negotiate	Select to enable or disable auto-negotiation.
NAT Traversal	Select the checkbox if a NAT device exists between the local FortiGate unit and the VPN peer or client. The local FortiGate unit and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared) to connect reliably.
Keep-alive Frequency	If NAT traversal is enabled or forced, type a keep-alive frequency setting (10-900 seconds).
Advanced-Options	For more information on advanced options, see the <i>FortiOS CLI Reference</i> .
fcc-enforcement	Enable or disable FCC enforcement.
inter-vdom	Enable or disable the inter-vdom setting.
localid-type	<p>Select the local ID type from the dropdown list. Select one of:</p> <ul style="list-style-type: none"> • <i>address</i>: IP Address • <i>asn1dn</i>: ASN.1 Distinguished Name • <i>auto</i>: Select type automatically • <i>fqdn</i>: Fully Qualified Domain name • <i>keyid</i>: Key Identifier ID • <i>user-fqdn</i>: User Fully Qualified Domain Name

negotiate-timeout

Enter the negotiation timeout value. The default is 30 seconds.

npu-offload

Enable (default) or disable offloading of VPN session to a network processing unit (NPU).

View IPsec VPN community details

The VPN community information pane includes a quick status bar showing the community settings and the list of gateways in the community. Gateways can also be managed from this pane. See [IPsec VPN gateways on page 380](#) 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 372](#).

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.

<div><div><div><div><div></div></div><div>Refresh</div></div><div><div><div></div></div><div>Bring Tunnel Up</div></div><div><div><div></div></div><div>Bring Tunnel Down</div></div><div><div><div></div></div><div>Column Settings</div></div></div><div></div></div>								
<input type="checkbox"/>	Status	Device	Name	Type	Remote Gateway	Incoming Data	Phase 2 Proposal	Uptime
<input type="checkbox"/>	<div><div></div><div>Up</div></div>	FGT54_1[root]	dual-I_1_3	automatic	100.64.54.2	0.0 KB	1	1d 20h 39m 55s
<input type="checkbox"/>	<div><div></div><div>Down</div></div>	FGT54_1[root]	dual-I_1_4	automatic	100.64.154.2	0.0 KB	1	2s
<input type="checkbox"/>	<div><div></div><div>Down</div></div>	FGT54_1[root]	dual-I_2_3	automatic	100.64.54.2	0.0 KB	1	2s
<input type="checkbox"/>	<div><div></div><div>Down</div></div>	FGT54_1[root]	dual-I_2_4	automatic	100.64.154.2	0.0 KB	1	15s
<input type="checkbox"/>	<div><div></div><div>Up</div></div>	FGT54_2[root]	dual-I_3_1	automatic	100.64.54.1	0.0 KB	1	1d 20h 39m 51s
<input type="checkbox"/>	<div><div></div><div>Down</div></div>	FGT54_2[root]	dual-I_3_2	automatic	100.64.154.1	0.0 KB	1	2s
<input type="checkbox"/>	<div><div></div><div>Down</div></div>	FGT54_2[root]	dual-I_4_1	automatic	100.64.54.1	0.0 KB	1	3s
<input type="checkbox"/>	<div><div></div><div>Down</div></div>	FGT54_2[root]	dual-I_4_2	automatic	100.64.154.1	0.0 KB	1	11s

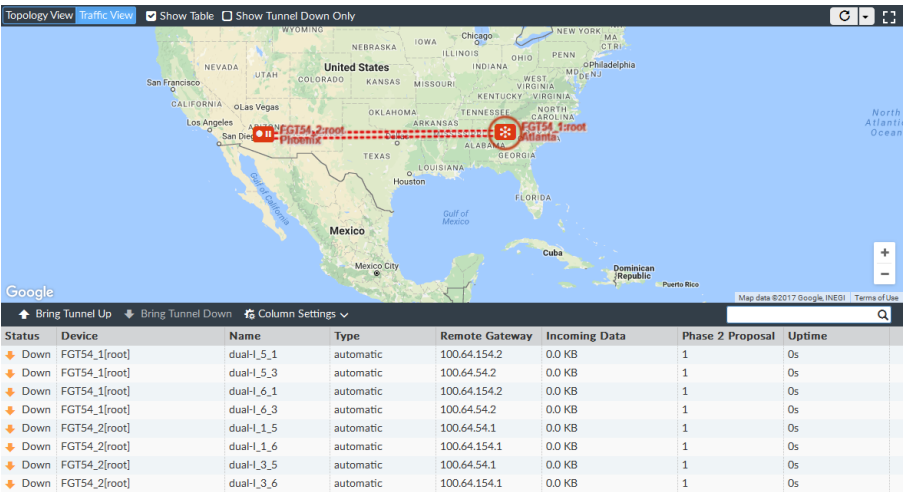
To bring tunnels up or down:

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:

Topology View	The topology view shows the configured VPN gateways. See IPsec VPN gateways on page 380 .
Traffic View	The traffic view shows network traffic through the tunnels between protected subnets.
Show Table	Select to show the connection table on the bottom of the pane. In the topology view, this option is only available when a specific community is selected. <ul style="list-style-type: none">The topology table shows the VPN gateway list and toolbar, with a column added for location. See Managing VPN gateways on page 380 for information.The traffic table shows the same information and options as the <i>Monitor</i> tab. See Monitoring IPsec VPN tunnels on page 378 for information.
Show Tunnel Down Only	Select to show only tunnels that are currently down. This option is only available on the traffic view.
Refresh	Click to refresh the map view, or click the down arrow and select a refresh rate from the dropdown menu.
Toggle Full Screen	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 79](#).

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.

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

The following options are available:

Create New	Create a new managed or external gateway. See Creating managed gateways on page 380 and Creating external gateways on page 384 for more information.
Edit	Edit the selected gateway. See Editing an IPsec VPN gateway on page 386 .
Delete	Delete the selected gateway or gateways. See Deleting VPN gateways on page 386 .
Column Settings	Configure which columns are displayed, or click <i>Reset to Default</i> to reset the display to the default columns.
Search	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 384](#).

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.

VPN Gateway Setup Wizard - Dup

Protected Network Device Default VPN Interface Local Gateway Advanced

Protected Subnet

< Back Next > Cancel

4. Proceed through the five pages of the wizard, filling in the following values as required, then click *OK* to create the managed gateway.

Protected Subnet	Select a protected subnet from the drop-down list.
Role	Select the role of this gateway: <i>Hub</i> or <i>Spoke</i> . This option is only available for star and dial up VPN topologies.
Device	Select a <i>Device</i> or <i>Device Group</i> from the drop-down list.
Default VPN Interface	Select the interface to use for this gateway from the drop-down list.
Hub-to-Hub Interface	Select the interface to use for hub to hub communication. This is required if there are multiple hubs. This option is only available for star and dial up topologies with the role set to <i>Hub</i> .
Local Gateway	Enter the local gateway IP address.
Local ID	Enter a local ID.
Routing	Select the routing method: <i>Manual (via Device Manager)</i> , or <i>Automatic</i> .
Summary Network(s)	Select the network from the dropdown list and select the priority. Click the add icon to add more entries. This option is only available for star and dial up topologies with the role set to <i>Hub</i> .
Peer Type	Select one of the following: <ul style="list-style-type: none"> • <i>Accept any peer ID</i> • <i>Accept this peer ID</i>: Enter the peer ID in the text field

- *Accept a dialup group*: Select a group from the drop-down list
- *Accept peer*: Select a peer from the dropdown list
- *Accept peer group*: Select a peer group from the drop-down list

A Local ID is an alphanumeric value assigned in the Phase 1 configuration.

The local ID of a peer is called a Peer ID. The Local ID or peer ID can be used to uniquely identify one end of a VPN tunnel, enabling a more secure connection. If you have multiple VPN tunnels negotiating, this ensures the proper remote and local ends connect.

When you configure the ID on your end, it is your local ID. When the remote end connects to you, they see it as your peer ID. If you are debugging a VPN connection, the local ID is part of the VPN negotiations. You can use it to help troubleshoot connection problems.

The default configuration is to accept all local IDs (peer IDs). If your local ID is set, the remote end of the tunnel must be configured to accept your ID.

This option is only available for dial up topologies.

XAUTH Type	Select the XAUTH type: <i>Disable</i> , <i>PAP Server</i> , <i>CHAP Server</i> , or <i>AUTO Server</i> . This option is only available for dial up topologies.
User Group	Select the authentication user group from the dropdown list. This field is available when <i>XAUTH Type</i> is set to <i>PAP Server</i> , <i>CHAP Server</i> , or <i>AUTO Server</i> . When the FortiGate unit is configured as an XAuth server, enter the user group to authenticate remote VPN peers. The user group can contain local users, LDAP servers, and RADIUS servers. The user group must be added to the FortiGate configuration before the group name can be cross referenced.
Enable IKE Configuration Method ("mode config")	Select to enable or disable IKE configuration method. This option is only available for dial up topologies.
Enable IP Assignment	Select to enable or disable IP assignment. This option is only available for dial up topologies. When the role is set to <i>Hub</i> , this option is only available when <i>Enable IKE Configuration Method</i> is on.
IP Assignment Mode	Select the IP assignment mode: <i>Range</i> or <i>User Group</i> . This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IP Assignment</i> turned on.
IP Assignment Type	Select the IP assignment type: <i>IP</i> or <i>Subnet</i> . This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IP Assignment</i> turned on.
IPv4 Start IP	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.
IPv4 End IP	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.
IPv4 Netmask	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.
Add Route	Select to enable or disable adding a route for this gateway. This option is only available for dial up topologies.
DNS Server #1 to #3	Enter the DNS server IP addresses to provide IKE Configuration Method to clients. This option is only available for dial up topologies with the role set to <i>Hub</i> and either <i>Enable IKE Configuration Method</i> turned on, or <i>DNS Service</i> is set to <i>Specify</i> .
WINS Server #1 and #2	Enter the WINS server IP addresses to provide IKE Configuration Method to clients. This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned on.
IPv4 Split include	Select the address or address group from the dropdown list. This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned on.
Exclusive IP Range	Enter the start and end IP addresses of the exclusive IP address range. Click the add icon to add more entries. This option is only available for dial up topologies with the role set to <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.
DHCP Server	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.
Default Gateway	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.
DNS Service	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.
Netmask	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.
IPsec Lease Hold	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.
Auto-Configuration	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.

DHCP Server IP Range	<p>Enter the start and end IP addresses of the DHCP server range. Click the add icon to add more entries.</p> <p>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.</p>
Advanced Options	
authpasswd	Enter the XAuth client password for the FortiGate.
authusr	Enter the XAuth client user name for the FortiGate.
banner	<p>Enter the banner value.</p> <p>Specify the message to send to IKE Configuration Method clients. Some clients display this message to users.</p>
dns-mode	<p>Select the DNS mode from the dropdown list:</p> <ul style="list-style-type: none"> <i>auto</i>: Assign DNS servers in the following order: <ul style="list-style-type: none"> a. Servers assigned to interfaces by DHCP b. Per-VDOM assigned DNS servers c. Global DNS servers <i>manual</i>: Use the DNS servers specified in <i>DNS Server #1 to #3</i>.
domain	Enter the domain value.
public-ip	<p>Enter the public IP address.</p> <p>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.</p>
route-overlap	Select the route overlap method from the dropdown list: <i>allow</i> , <i>use-new</i> , or <i>use-old</i> .
spoke-zone	Select a spoke zone from the dropdown list.
unity-support	Enable or disable unity support.
vpn-interface-priority	Set the VPN gateway interface priority. The default value is 1.
vpn-zone	Select a VPN zone from the dropdown list.

Creating external gateways

External gateways are not managed by the FortiManager device.

To create an external gateway:

1. Go to *VPN Manager > IPsec VPN*.
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.

New VPN External Gateway

Node Type ☒ Hub ☐ Spoke

Gateway Name

Gateway IP

Hub IP

Create Phase2 per Protected Subnet Pair ☐ OFF

Peer Type ☒ Accept any peer ID

☐ Accept this peer ID

☐ Accept a dialup group

Protected Subnet Click here to select

Local Gateway IP Address

4. Configure the following settings, then click **OK** to create the external gateway:

Node Type	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.
Gateway Name	Enter the gateway name.
Gateway IP	Select the gateway IP address from the dropdown list.
Hub IP	Select the hub IP address from the dropdown list. This option is only available for star and dial up topologies with the role set to <i>Hub</i> .
Create Phase2 per Protected Subnet Pair	Toggle the switch to <i>On</i> to create a phase2 per protected subnet pair.
Routing	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.
Peer Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> • <i>Accept any peer ID</i> • <i>Accept this peer ID</i>: Enter the peer ID in the text field • <i>Accept a dialup group</i>: Select a group from the dropdown list <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>
Protected Subnet	Select a protected subnet from the list. You can add multiple subnets.
Local Gateway	Enter the local gateway IP address.

Editing an IPsec VPN gateway

To edit a VPN gateway, you must be logged in as an administrator with sufficient privileges. The gateway role and device (if applicable) cannot be edited.

To edit IPsec VPN communities:

1. Go to *VPN Manager > IPsec VPN*.
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 203](#) 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:

Add SSL VPN	Create a new SSL VPN with the <i>Create SSL VPN</i> dialog box. See Creating SSL VPNs on page 388 .
Install Wizard	Launch the <i>Install Wizard</i> to install SSL VPN settings to devices.
Create New	Create a new SSL VPN with the <i>Create SSL VPN</i> pane. This option is also available from the right-click menu. See Creating SSL VPNs on page 388 .
Edit	Edit the selected VPN. This option is also available from the right-click menu. See Editing SSL VPNs on page 390 .
Delete	Delete the selected VPN or VPNs. This option is also available from the right-click menu. See Deleting SSL VPNs on page 390 .
Search	Enter a search term to search the VPN list.

Creating SSL VPNs

To create SSL VPNs, you must be logged in as an administrator with sufficient privileges. Multiple VPNs can be created.

To add SSL-VPN:

1. Go to *VPN Manager > SSL-VPN*.
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:

Connection Settings

Listen on Interface(s):

Listen on Port:

Restrict Access: ☐ Allow access from any host ☐ Limit access to specific hosts

Idle Logout: ☐ OFF

Server Certificate:

Require Client Certificate: ☐ OFF

Tunnel Mode Client Settings

Address Range: ☐ Automatically assign addresses ☐ Specify custom IP ranges

DNS Server: ☐ Same as client system DNS ☐ Specify

Specify WINS Servers: ☒ ON

WINS Server #1:

WINS Server #2:

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.

Device	Select a FortiGate device or VDOM.
Connection Settings	Specify the connection settings.
Listen on Interface(s)	Define the interface the FortiGate will use to listen for SSL VPN tunnel requests. This is generally your external interface.
Listen on Port	Enter the port number for HTTPS access.
Restrict Access	Allow access from any hosts, or limit access to specific hosts. If limiting access, select the hosts that have access in the <i>Hosts</i> field.
Idle Logout	<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>
Server Certificate	Select the signed server certificate to use for authentication. Alternately, select a certificate template that is configured to use the FortiManager CA. See Certificate templates on page 115 .
Require Client Certificate	Select to use group certificates for authenticating remote clients. When the remote client initiates a connection, the FortiGate unit prompts the client for its client-side certificate as part of the authentication process. For information on using PKI to provide client certificate authentication, see the Authentication Guide.
Tunnel Mode Client Settings	Specify tunnel mode client settings. These settings determine how tunnel mode clients are assigned IP addresses.
Address Range	Either automatically assign address, or specify custom IP ranges.
DNS Server	Select to use the same DNS as the client system, or to specify DNS servers. Enter up to two DNS servers to be provided for the use of clients.

Specify WINS Servers	Select to specify WINS servers. Enter up to two WINS servers to be provided for the use of clients.
Allow Endpoint Registration	Select to allow endpoint registration.
Authentication/Portal Mapping	Select the users and groups that can access the tunnel. Note: the default portal cannot be empty.
Create New	Create a new authentication/portal mapping entry. Select the <i>Users</i> , <i>Groups</i> , <i>Realm</i> , and <i>Portal</i> , then click <i>OK</i> .
Edit	Edit the selected mapping.
Delete	Delete the selected mapping or mappings.
Advanced Options	Configure advanced SSL VPN options. For information, see the <i>FortiOS CLI Reference</i> .

Editing SSL VPNs

To edit an SSL VPN, you must be logged in as an administrator with sufficient privileges. The device cannot be edited.

To edit an SSL VPN:

1. Go to *VPN Manager > SSL VPN*.
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

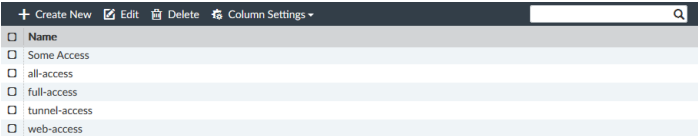
The SSL VPN portal enables remote users to access internal network resources through a secure channel using a web browser. FortiGate administrators can configure login privileges for system users as well as the network resources that are available to the users.

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:

Create New	Create a new portal profile.
Edit	Edit the selected profile.
Delete	Delete the selected profile or profiles.
Column Settings	Adjust the visible columns.
Search	Enter a search term to search the portal profile list.

Creating SSL VPN portal profiles

To create SSL VPN portal profiles, you must be logged in as an administrator with sufficient privileges. Multiple profiles can be created.

To create portal profiles:

1. Go to *VPN Manager > SSL-VPN* 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.
Limit Users to One SSL VPN Connection at a Time	Set the SSL VPN tunnel so that each user can only be logged in to the tunnel one time per user log in. Once they are logged in to the portal, they cannot go to another system and log in with the same credentials until they log out of the first connection.
Tunnel Mode	Select to configure and enable tunnel mode access. These settings determine how tunnel mode clients are assigned IPv4 addresses.
Enable Split Tunneling	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.
Routing Address	If you enable split tunneling, you are required to set the address that your corporate network is using. Traffic intended for the routing address will not be split from the tunnel.

Source IP Pools	Select an IPv4 pool for users to acquire an IP address when connecting to the portal. There is always a default pool available if you do not create your own.
IPv6 Tunnel Mode	Select to configure and enable tunnel mode access. These settings determine how tunnel mode clients are assigned IPv6 addresses.
Enable IPv6 Split Tunneling	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.
IPv6 Routing Address	If you enable split tunneling, you are required to set the address that your corporate network is using. Traffic intended for the routing address will not be split from the tunnel.
Source IP Pools	Select an IPv6 pool for users to acquire an IP address when connecting to the portal. There is always a default pool available if you do not create your own.
Tunnel Mode Client Options	These options affect how the FortiClient application behaves when connected to the FortiGate VPN tunnel. When enabled, a checkbox for the corresponding option appears on the VPN log in screen in FortiClient, and is disabled by default.
Allow client to save password	The user's password is stored on the user's computer and will automatically populate each time they connect to the VPN.
Allow client to connect automatically	When the FortiClient application is launched, for example after a reboot or system start up, FortiClient will automatically attempt to connect to the VPN tunnel.
Allow client to keep connections alive	The FortiClient connection will not shut down. When not selected, during periods of inactivity, FortiClient will attempt to stay connected every three minutes for a maximum of 10 minutes.
Enable Web Mode	Select to enable web mode access.
Portal Message	The text header that appears on the top of the web portal.
Theme	A color styling specifically for the web portal: <i>blue</i> , <i>green</i> , <i>mariner</i> , <i>melongene</i> , or <i>red</i> .
Show Session Information	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.
Show Connection Launcher	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.
Show Login History	Include user log in history on the web portal, then specify the number of history entries.
User Bookmarks	Include bookmarks on the web portal. Bookmarks are used as links to internal network resources. When a bookmark is selected from a bookmark list, a pop-up window opens with the web page. VNC and RDP require a browser plugin. FTP and Samba replace the bookmarks page with an HTML file-browser.

Pre-Defined Bookmarks	The list of predefined bookmarks. Click <i>Create New</i> to add a bookmark. See Predefined bookmarks on page 394 for information.
Enable FortiClient Download	Select to enable FortiClient downloads.
Download Method	Select the method to use for downloading FortiClient from the SSL VPN portal. Choose between <i>Direct</i> and <i>SSL-VPN Proxy</i> . This option is only available when <i>Enable FortiClient Download</i> is <i>On</i> .
Customize Download Location	Select to specify a custom location to use for downloading FortiClient. You can specify a location for FortiClient (Windows) and FortiClient (Mac). Type the URL in the <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> .
Advanced Options	Configure advanced options. For information, see the <i>FortiOS CLI Reference</i> .

Predefined bookmarks

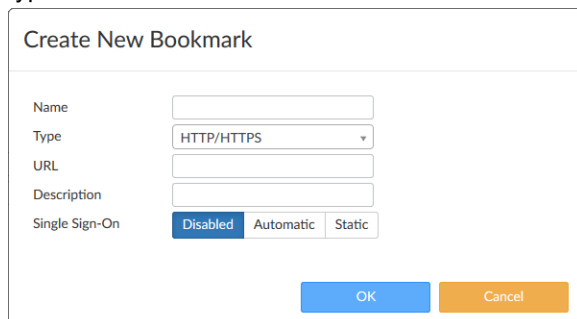
Bookmarks are used as links to specific resources on the network. When a bookmark is selected from a bookmark list, a window opens with the requested web page. RDP and VNC open a window that requires a browser plug-in. FTP replaces the bookmark page with an HTML file-browser.

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 396](#) or [Creating SSL VPN portal profiles on page 391](#).
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.



The dialog box titled "Create New Bookmark" contains the following fields and controls:

- Name:** A text input field.
- Type:** A dropdown menu with "HTTP/HTTPS" selected.
- URL:** A text input field.
- Description:** A text input field.
- Single Sign-On:** Three radio buttons labeled "Disabled", "Automatic", and "Static". The "Disabled" button is currently selected.
- Buttons:** "OK" (blue) and "Cancel" (orange) buttons at the bottom right.

4. Configure the following settings, then select **OK** to create the bookmark.

Name	Enter a name for the bookmark.
Type	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> .
URL	Enter the bookmark URL. This option is only available when <i>Type</i> is <i>Citrix</i> , or <i>HTTP/HTTPS</i> .
Folder	Enter the bookmark folder. This option is only available when <i>Type</i> is <i>FTP</i> or <i>SMB</i> .
Host	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> .
Remote Port	Enter the remote port. This option is only available when <i>Type</i> is <i>Port Forward</i> .
Listening Port	Enter the listening port. This option is only available when <i>Type</i> is <i>Port Forward</i> .
Show Status Window	Enable to show the status window. This option is only available when <i>Type</i> is <i>Port Forward</i> .
Port	Enter the port number. This option is only available when <i>Type</i> is <i>RDP</i> or <i>VNC</i> .
Username	Enter the user name. This option is only available when <i>Type</i> is <i>RDP</i> .
Password	Enter the password. This option is only available when <i>Type</i> is <i>RDP</i> or <i>VNC</i> .
Keyboard Layout	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> .
Security	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> .
Description	Optionally, enter a description of the bookmark.
Single Sign-on	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 <i>Type</i> is <i>Citrix</i> , <i>FTP</i> , <i>HTTP/HTTPS</i> , <i>RDP</i> , or <i>SMB</i> . The <i>Static</i> option is only available when <i>Type</i> is <i>Citrix</i> , <i>HTTP/HTTPS</i> , or <i>RDP</i> .

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 396](#) or [Creating SSL VPN portal profiles on page 391](#).
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 396](#) or [Creating SSL VPN portal profiles on page 391](#).
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:

Device	The device or VDOM name.
User	The user name.

Remote Host	The remote host.
Last Login	The time of the last log in.
Active Connections	The number of active connections on the VPN.

Access Points

The *AP Manager* pane allows you to manage FortiAP access points that are controlled by FortiGate devices that are managed by FortiManager. You can use *AP Manager* for the following modes of management:

- Central management of managed access points
- Per-device management of managed access points

The *AP Manager* pane includes the following tabs:

Managed APs	Displays unauthorized and authorized FortiAP devices. You can view, authorize, and edit authorized FortiAP devices.
Monitor	Monitor FortiAP devices and the clients connected to them.
Map view	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.
WiFi profiles for central management on page 417	When central management is enabled, you can view, create, edit, and import profiles. WiFi profiles share a common database. You can apply profiles to any device, regardless of which FortiGate controller it is connected to.
WiFi profiles for per-device management on page 441	When per-device management is enabled, you can change settings for each managed access point. All FortiAP devices and WiFi profiles are managed at the device level with no shared objects.

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 558](#)). 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 565](#).

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: 1 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: 1 Radio 2: 0	Radio 1: 1 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:

- Ensure that you are in the correct ADOM.
- Go to *AP Manager > Managed APs*. The quick status bar is displayed above the content pane.



- 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.

+ Create New Edit Delete Assign Profile More Column Settings							
#	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:

Create New	Add an AP.
Edit	Edit the selected AP.
Delete	Delete the selected AP.
Assigned Profile	Assign a profile from the list to the AP. Only applicable profiles will be listed. See Assigning profiles to FortiAP devices on page 441 .
Column Settings	Click to select which columns to display or select <i>Reset to Default</i> to display the default columns.
Authorize	<p>Authorize an AP. See Authorizing and deauthorizing FortiAP devices on page 406.</p> <p>This option is also available in the toolbar by selecting <i>More</i>.</p>
Deauthorize	<p>Deauthorize an AP. See Authorizing and deauthorizing FortiAP devices on page 406.</p> <p>This option is also available in the toolbar by selecting <i>More</i>.</p>
Grouping	<p>Move the selected FortiAP devices into a new group. The APs must be the same model to be grouped. See FortiAP groups on page 405.</p> <p>This option is only available in the right-click menu.</p>
Upgrade	<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> <p>Before upgrading FortiAP, go to <i>FortiGuard > Firmware Images > Product: FortiAP</i> and click the download icon to manually download the firmware images.</p>
Restart	<p>Restart the AP.</p> <p>This option is only available in the toolbar, by selecting <i>More</i>.</p>
Refresh	Refresh the AP list, or refresh the selected FortiAP devices.

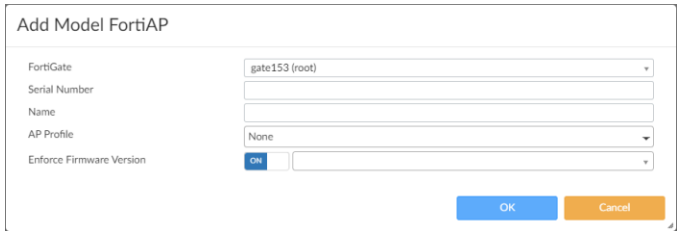
View Clients	View the clients connected to the AP. See Connected clients on page 409 .
View Rogue APs	View the Rogue APs. See Rogue APs on page 406 . This option is only available in the toolbar, by selecting <i>More</i> .
View Spectrum Analysis	View the spectrum analysis for managed APs. See Spectrum analysis for managed APs on page 410 . This option is available in the right-click menu, and in the toolbar by selecting <i>More</i> .
Show on Google Map	Show the selected AP on Google Map. See Google map on page 415 . This option is only available in the right-click menu.
Show on Floor Map	Show the selected AP on the floor map. See Floor map on page 416 . This option is only available in the right-click menu.
Search	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:

FortiGate	The FortiGate unit that is managing the AP.
Access Point	The serial number of the AP.
Connected Via	The IP address of the AP.
SSIDs	The SSIDs associated with the AP.
Channel	The wireless radio channels that the access point uses.
Clients	The number of clients connected to the AP. Select a value to open the View WiFi Clients window to view more details about the clients connected to that radio. See Connected clients on page 409 .
OS Version	The OS version on the FortiAP.
AP Profile	The AP Profile assigned to the device, if any.
Comments	User entered comments.
Country	The Country code that the FortiAP is using.
Join Time	The date and time that the FortiAP joined.
LLDP	The Link Layer Discovery Protocol
Operating TX Power	The transmit power of the wireless radios.
Serials #	The serial number of the device
WTP Mode	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.



2. Enter the following information, then click *OK* to add the device:

FortiGate	Select the FortiGate that the AP will be added to from the dropdown list. If you have already selected a FortiGate in the tree menu, this field will contain that FortiGate.
Serials Number	Enter the device's serial number.
Name	Enter a name for the device.
AP Profile	Select an AP profile to apply to the device from the dropdown list. See AP profiles on page 418 .
Enforce Firmware Version	Toggle <i>ON</i> to enforce a firmware version and select the firmware version from the drop-down menu. Toggle <i>OFF</i> to disable this feature.

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.

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:dc:c4:4d:ee: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

ON

2.4GHz 802.11n/g

Channels

2.4 GHz

802.11g/b

ON

(Automatically assigned)

☒ 1

☐ 2

☐ 3

☐ 4

☐ 5

☒ 6

☐ 7

☐ 8

☐ 9

☐ 10

☒ 11

TX Power Control

ON

100%

Auto

Manual

0%

100%

SSIDs

ON

ssid-22

Auto

Manual

Override Radio 2

Band

OFF

5GHz 802.11ac/n/a

Channels

OFF

(Automatically assigned)

TX Power Control

OFF

100%

SSIDs

OFF

ssid-22

Override AP Login Password

ON

Set

Leave Unchanged

Set Empty

AP Login Password

Advanced Options >

OK

Cancel

4. Edit the following options, then click *Apply* to apply your changes:

Serial Number	The device's serial number. This field cannot be edited.
Name	The name of the AP.
Comments	Comments about the AP, such as its location or function.
Managed AP Status	Various information about the AP.
Status	The status of the AP, such as <i>Connected</i> , or <i>Idle</i> . Click <i>Restart</i> to restart the AP.
Connected Via	The method by which the device is connected to the controller.

Base MAC Address	The MAC address of the device.
Join Time	The time that the AP joined.
Clients	The number of clients currently connected to the AP.
State	The state of the AP, such as <i>Authorized</i> , or <i>Discovered</i> .
Current	The AP's current firmware version. Select <i>Upgrade</i> to upgrade the firmware to a newer version if you have one available. See Firmware Management on page 99
FortiAP Profile	Select a profile from the dropdown list (see AP profiles on page 418)
Bonjour Profile	Select a profile from the dropdown list (see Bonjour profiles on page 439)
Override Radio	Override the selected profiles settings.
Band	If applicable, select the wireless band, and select the wireless protocol from the dropdown list. The available options depend on the selected platform. In two radio devices, both radios cannot use the same band.
Channels	Select the channel or channels to include, or let them be automatically assigned. The available channels depend on the selected platform and band.
TX Power Control	Enable/disable automatic adjustment of transmit power. <ul style="list-style-type: none"> • <i>Auto</i>: Enter the TX power low and high values, in dBm. • <i>Manual</i>: Enter the TX power in the form of the percentage of the total available power.
SSIDs	Manually choose the SSIDs that APs using this profile will carry, or let them be selected automatically.
Override AP Login Password	Enable/disable overriding the login password: <ul style="list-style-type: none"> • <i>Set</i>: Set the AP login password. • <i>Leave Unchanged</i>: Leave the password unchanged. • <i>Set Empty</i>: Remove the password.
Advanced Options	Configure advanced options. For information, see the <i>FortiOS CLI Reference</i> . https://help.fortinet.com/cli/fos60hlp/60/index.htm .

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:

Name	Enter a name for the group.
FortiGate	Select the FortiGate under which the group will be created.
Platform	Select the FortiAP platform that the group will apply to.
FortiAPs	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.

Installing changes to FortiAP devices

To install changes to FortiAP 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 63](#) 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.

Access Points

View Rogue APs

<input type="checkbox"/> Mark As <input checked="" type="checkbox"/> Suppress AP <input checked="" type="checkbox"/> Unsuppress AP <input checked="" type="checkbox"/> Refresh <input checked="" type="checkbox"/> Column Settings										<input type="checkbox"/> Show Offline (198) <input type="checkbox"/> Show Accepted (0)	<input type="text"/>
<input type="checkbox"/>	State	Status	SSID	Security Type	Channel	MAC Address	Vendor Info	Signal Strength	Detected By	On-Wire	
<input type="checkbox"/>	?	↑	fortinet	WPA2 Personal	6	70:4ca5:99:da:22	Fortinet, Inc.	-47dBm	PS311C3U15000439(192.168.1.111:5246)	↓	
<input type="checkbox"/>	?	↑	FTNT-Guest	WPA2 Personal	6	70:4ca5:a3:87:e0	Fortinet, Inc.	-55dBm	PS311C3U15000439(192.168.1.111:5246)	↓	
<input type="checkbox"/>	?	↑	FTNT-Staff	WPA2 Enterprise	6	70:4ca5:a3:87:e1	Fortinet, Inc.	-56dBm	PS311C3U15000439(192.168.1.111:5246)	↓	
<input type="checkbox"/>	?	↑	DU_EPCR580	WPA Personal	11	7ce1ff:01:09:b0	Computer	-55dBm	PS311C3U15000439(192.168.1.111:5246)	↓	
<input type="checkbox"/>	?	↑	iPADS	WPA2 Personal	100	90:6cac:28:89:a8	Fortinet, Inc.	-13dBm	PS311C3U15000439(192.168.1.111:5246)	↓	
<input type="checkbox"/>	?	↑	fortinet	WPA2 Personal	11	90:6cac:7c:9b:aa	Fortinet, Inc.	-64dBm	PS311C3U15000439(192.168.1.111:5246)	↓	
<input type="checkbox"/>	?	↑ ⚠	fortinet35	WPA/WPA2 Pers	6	90:6cac:a4:37:76	Fortinet, Inc.	-23dBm	PS311C3U15000439(192.168.1.111:5246)	↓	
<input type="checkbox"/>	?	↑	GuestWireless	WPA2 Personal	100	a2:6cac:28:89:a8		-14dBm	PS311C3U15000439(192.168.1.111:5246)	↓	
<input type="checkbox"/>	?	↑	LB_CP	OPEN	6	a2:6cac:28:89:e8		-10dBm	PS311C3U15000439(192.168.1.111:5246)	↓	
<input type="checkbox"/>	?	↑	StaffWireless	WPA2 Personal	6	b2:6cac:1b:72:be		-17dBm	PS311C3U15000439(192.168.1.111:5246)	↓	
<input type="checkbox"/>	?	↑	StaffWireless	WPA2 Personal	1	b2:6cac:25:d4:64		-22dBm	PS311C3U15000439(192.168.1.111:5246)	↓	
<input type="checkbox"/>	?	↑	StaffWireless	WPA2 Personal	100	b2:6cac:28:89:a8		-14dBm	PS311C3U15000439(192.168.1.111:5246)	↓	
<input type="checkbox"/>	?	↑	demo-112	WPA2 Personal	100	c2:6cac:28:89:a8		-13dBm	PS311C3U15000439(192.168.1.111:5246)	↓	
<input type="checkbox"/>	?	↑	fortinet	WPA2 Personal	6	e8:1cba:39:97:fa		-64dBm	PS311C3U15000439(192.168.1.111:5246)	↓	
<input type="checkbox"/>	?	↑	fortinetsz2	WPA2 Personal	1	e8:1cba:39:a2:32		-65dBm	PS311C3U15000439(192.168.1.111:5246)	↓	
<input type="checkbox"/>	?	↑	fortinet	WPA2 Personal	11	e8:1cba:51:cb:1a		-48dBm	PS311C3U15000439(192.168.1.111:5246)	↓	

The following options are available:

Mark As	Mark a rogue AP as: <ul style="list-style-type: none"> • Accepted: for APs that are an authorized part of your network or are neighboring APs that are not a security threat. • Rogue: for unauthorized APs that On-wire status indicates are attached to your wired networks. • Unclassified: the initial status of a discovered AP. You can change an AP back to unclassified if you have mistakenly marked it as <i>Rogue</i> or <i>Accepted</i>.
Suppress AP	Suppress the selected APs. This will prevent users from connecting to the AP. When suppression is activated against an AP, the controller sends deauthentication messages to the rogue AP's clients posing as the rogue AP, and also sends deauthentication messages to the rogue AP posing as its clients. Before enabling this feature, verify that operation of Rogue Suppression is compliant with the applicable laws and regulations of your region.
Unsuppress AP	Turn of suppression for the selected rogue APs.
Refresh	Refresh the rogue AP list.
Column Settings	Click to select which columns to display or select <i>Reset to Default</i> to display the default columns.

The following columns are available:

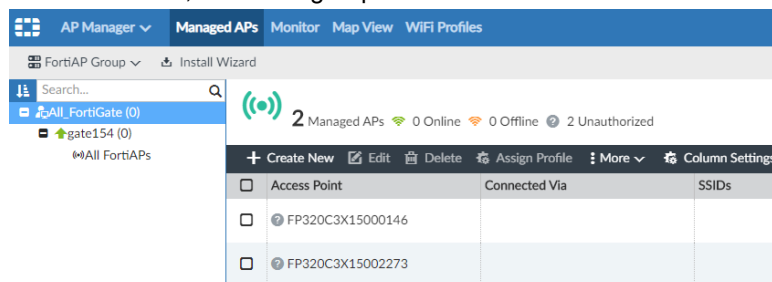
State	The state of the AP: <ul style="list-style-type: none"> • Suppressed: red suppressed icon • Rogue: orange rogue icon • Accepted: green wireless signal mark • Unclassified: gray question mark
Status	Whether the AP is active (green) or inactive (orange).
SSID	The wireless service set identifier (SSID) or network name for the wireless interface.
Security Type	The type of security currently being used.
Channel	The wireless radio channel that the access point uses.
MAC Address	The MAC address of the wireless interface.
Vendor Info	The name of the vendor.
Signal Strength	The relative signal strength of the AP.
Detected By	The name or serial number of the AP unit that detected the signal.
On-Wire	A green up-arrow indicates a suspected rogue, based on the on-wire detection technique. An orange down-arrow indicates AP is not a suspected rogue.
First Seen	How long ago this AP was first detected. This column is not visible by default.
Last Seen	How long ago this AP was last detected. This column is not visible by default.
Rate	The data rate in, bps. This column is not visible by default.

Authorizing unknown APs

FortiManager can now authorize unknown APs that are connected to a managed FortiGate.

To authorize unknown APs:

1. Enable *JSON API access to Read-Write*. See [To enable read-write JSON API access](#).
2. In the tree menu, select the group or FortiGate that contains the unknown FortiAP devices to be authorized.



3. Select the unknown FortiAP devices and either click *More > Authorize* from the toolbar, or right-click and select *Authorize*.
4. Wait awhile and then select the APs and click *More > Refresh*.
APs are now online and displayed.

Access Point	Connected Via	SSIDs	Channel
FP320C3X15000146	192.168.100.111		Radio 1: 1 Radio 2: 132
FP320C3X15002273	192.168.100.112		Radio 1: 6 Radio 2: 140



You must enable *JSON API access to Read-Write* to be able to authorize unknown FortiAP devices.

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*.

#	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:b7:f3:11:d8:34	6	0 kbps	36 dB	-59dBm	05/13/18 03:01

The following columns are available:

SSID	The SSID that the client connected to.
FortiAP	The serial number of the FortiAP unit that the client connected to.
IP	The IP address assigned to the wireless client.
Device	The type of device that the client is using.
Channel	The wireless radio channel that is used.
Bandwidth Tx/Rx	Client received and transmitted bandwidth, in Kbps.
Signal Strength/Noise	The signal-to-noise ratio in dBs calculated from signal strength and noise level.
Signal Strength	The relative signal strength of the AP.
Association Time	How long the client has been connected to this access point.
Authentication	The type of authentication used.
Bandwidth RX	Client received bandwidth, in Kbps.

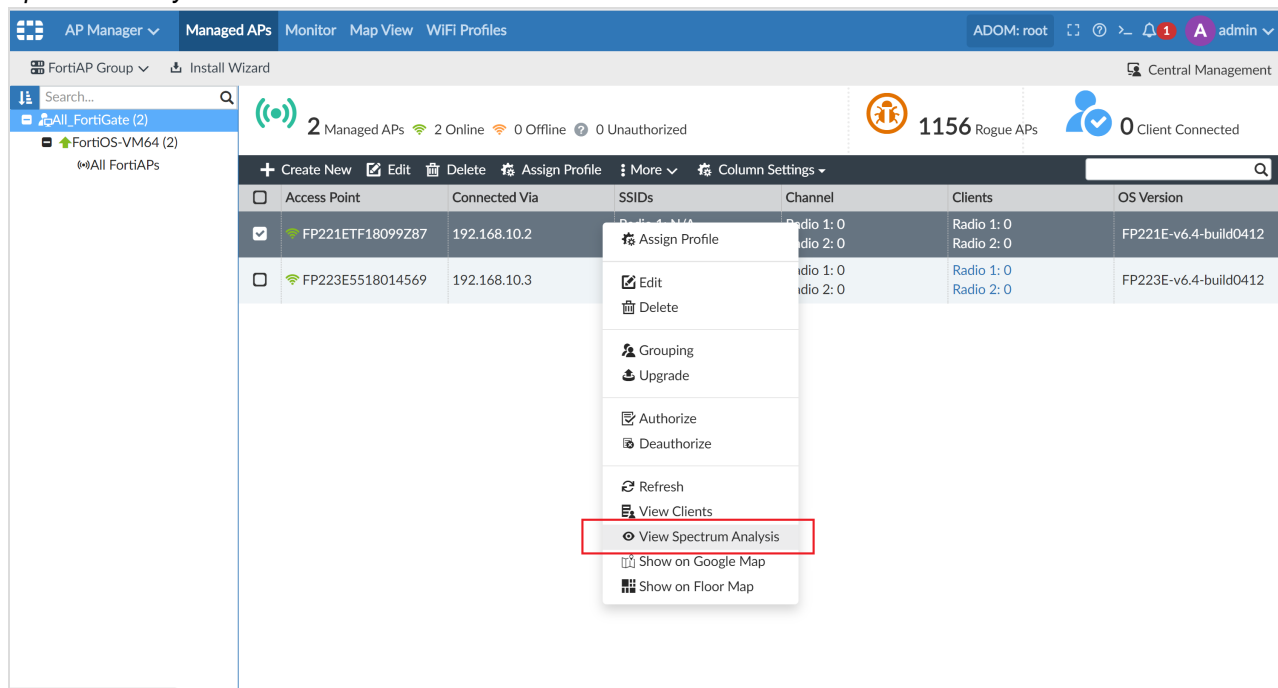
Bandwidth TX	Client transmitted bandwidth, in Kbps.
Device OS	The OS version on the FortiAP.
Host Information	The host name of the WiFi client, if available.
Idle Time	The amount of time that the client has been idle.
Manufacturer	The manufacturer of the client device.
Rate	The connection rate between the WiFi client and the AP.
Name	The name of the FortiGate device that the FortiAP is attached to.

Spectrum analysis for managed APs

You can view the spectrum analysis for managed APs in FortiManager 6.4.2. Spectrum analysis is available through *AP Manager > Managed APs*.

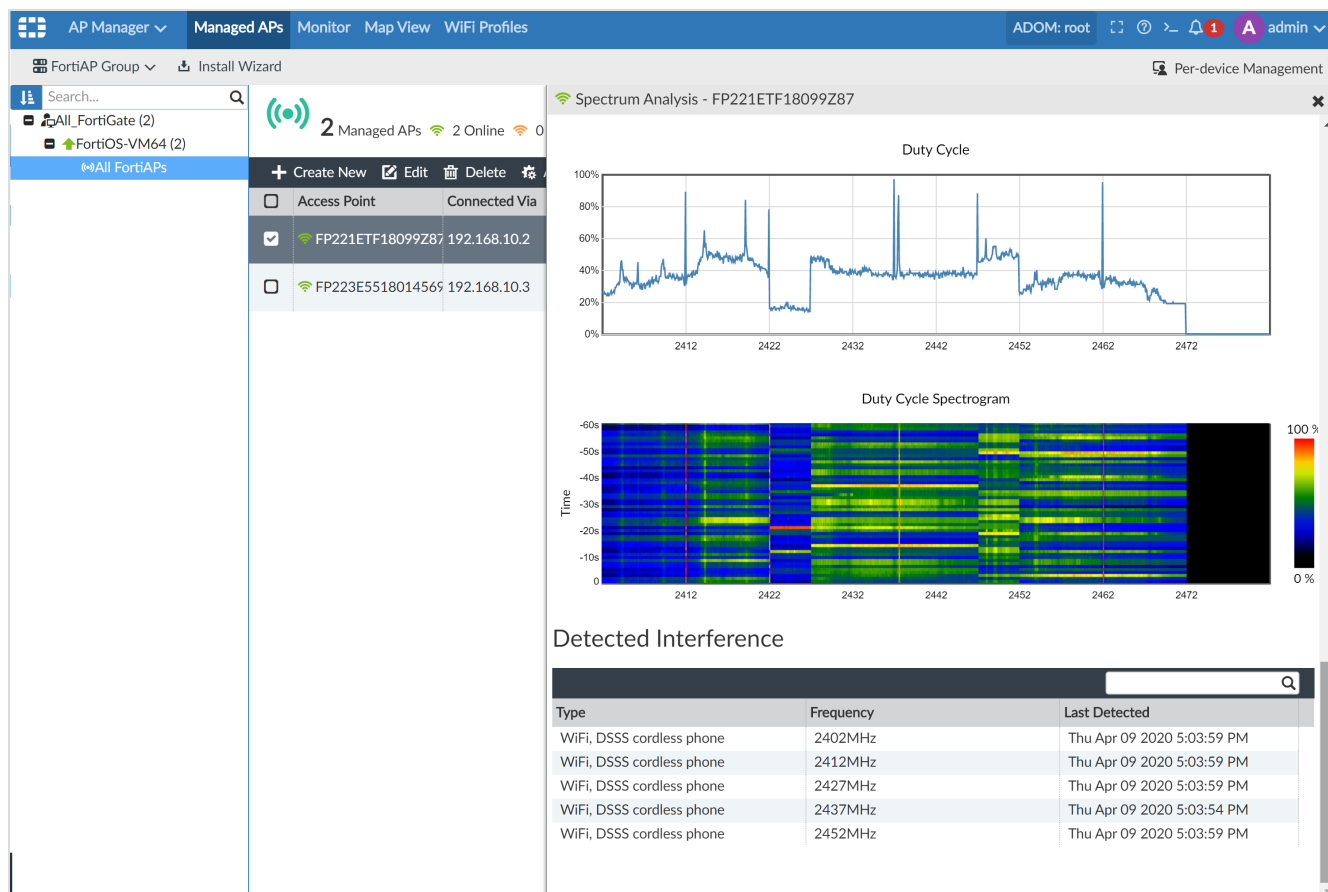
To view the spectrum analysis for a managed AP in the FortiManager GUI:

1. Ensure the *JSON API Access* field is set to *Read-Write*, by editing the administrator. See [Editing administrators on page 605](#).
2. Create a new WiFi profile or modify an existing WiFi profile, by setting the radio mode setting to *Dedicated Monitor*. See [AP profiles on page 418](#).
3. Assign the profile to the managed AP. See [Assigning profiles to FortiAP devices on page 441](#).
4. Use the *Install Wizard* to install the changes to FortiGate. See [Using the Install Wizard to install device settings only on page 76](#).
5. On the *Managed APs* screen, select a managed AP, click *More* from the toolbar or right-click, and click *View Spectrum Analysis*:



The *Spectrum Analysis* in the form of *Signal Interference*, *Signal Interference Spectrogram*, *Duty Cycle*, and *Duty Cycle Spectrogram* charts, along with the tabulated *Detected Interference* information is displayed.





AP capabilities will be limited during spectrum analysis.

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:

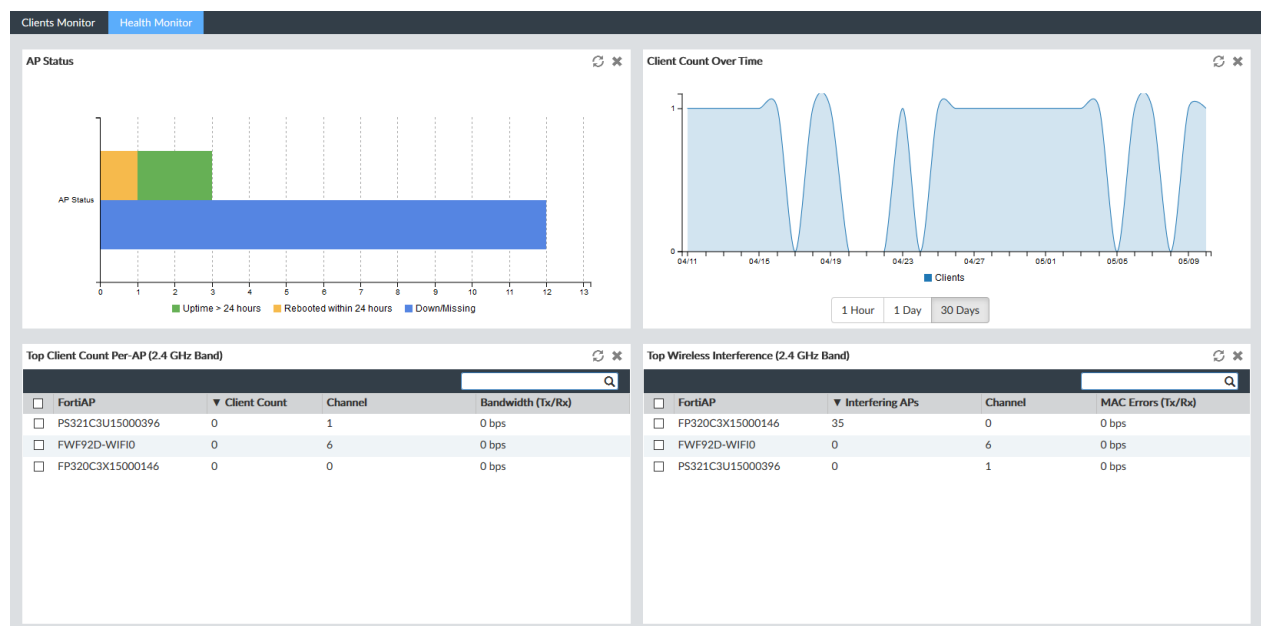
SSID

The SSID that the client connected to.

FortiAP	The serial number of the FortiAP unit that the client connected to.
IP	The IP address assigned to the wireless client.
Device	The type of device that the client is using.
Channel	The wireless radio channel that is used.
Bandwidth TX/RX	Client received and transmitted bandwidth, in Kbps.
Signal Strength/Noise	The signal-to-noise ratio in dBs calculated from signal strength and noise level.
Signal Strength	The relative signal strength of the AP.
Association Time	How long the client has been connected to this access point.
Authentication	The type of authentication used.
Bandwidth RX	Client received bandwidth, in Kbps.
Bandwidth TX	Client transmitted bandwidth, in Kbps.
Device OS	The OS version on the FortiAP.
Host Information	The host name of the WiFi client, if available.
Idle Time	The amount of time that the client has been idle.
Manufacturer	The manufacturer of the client device.
Rate	The connection rate between the WiFi client and the AP.
Name	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
AP Status	<p>Displays a bar graph of:</p> <ul style="list-style-type: none"> <i>Uptime > 24 hours</i>: The number of APs that have been up for over 24 hours. <i>Rebooted within 24 hours</i>: the number of APs that have been rebooted within the past 24 hours. <i>Down/Missing</i>: Down or missing APs. <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>
Client Count Over Time	<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>
Top Client Count Per-AP (2.4 GHz or 5 GHz Band)	<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>

Widget	Description
Top Wireless Interference (2.4 GHz or 5 GHz Band)	Lists the number of interfering APs in the 2.4GHz and 5GHz band for each FortiAP. Also includes columns for the channel and the number of MAC Errors for each AP.
Login Failures Information	Lists the time of a log in failure, the SSID involved, the Host Name/MAC, and the User Name.

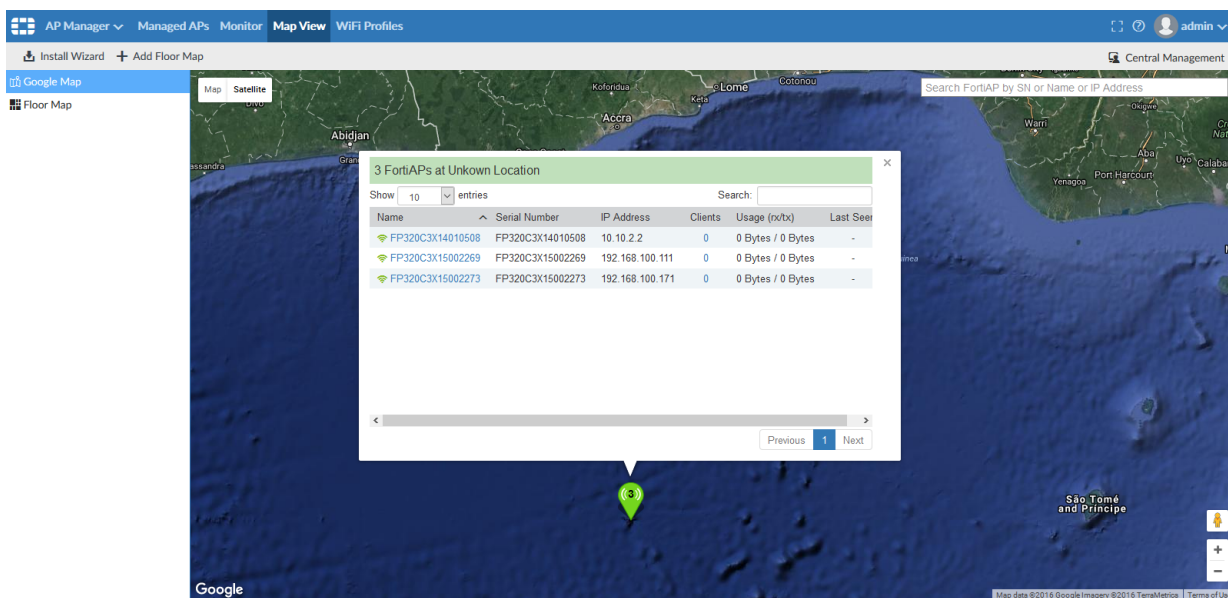
Map view

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 415](#)
- 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 416](#)

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.

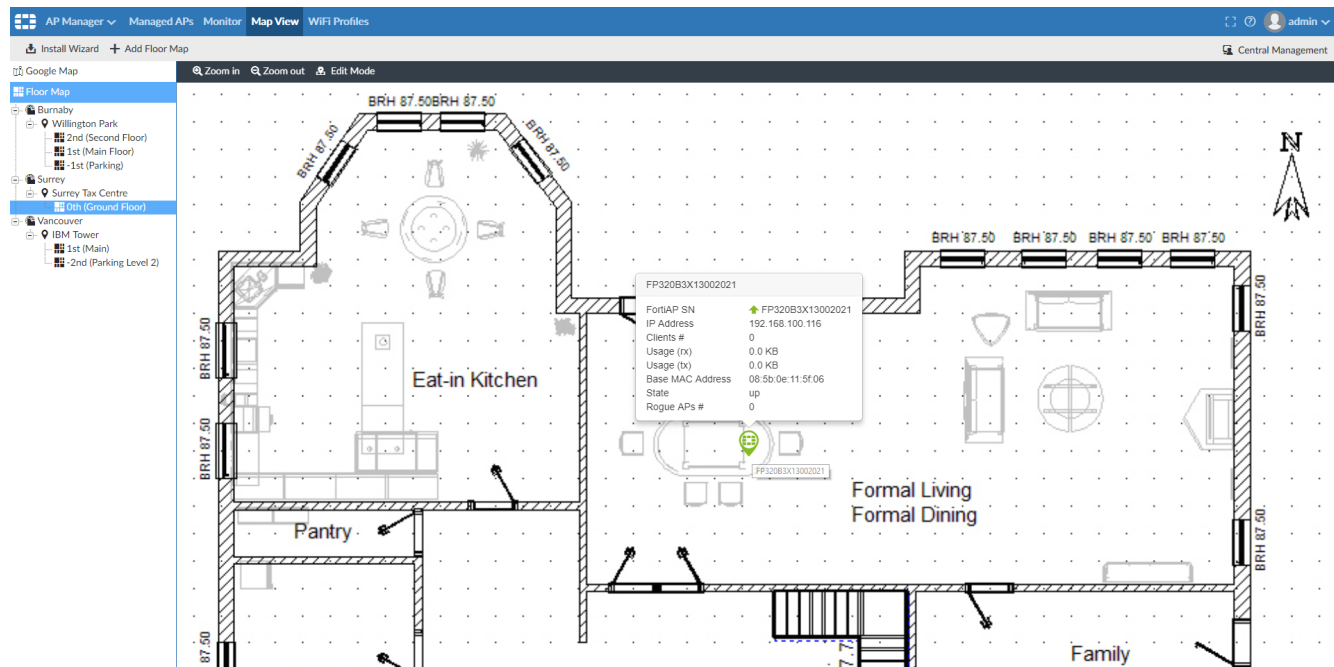


Clicking on a map pin opens a list of the APs connected to that FortiGate. Clicking on the name of an AP from the list will zoom the map into that location and provide further information about the AP, including the serial number, IP address, number of clients, usage, and the last time the AP was seen if it is offline.

Click on the number of client to open the *View WiFi Clients* window (see [Connected clients on page 409](#)). 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 400](#)).

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 for central management

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.



Settings may vary for different ADOM versions.

1. Enable central management of access points.
See [Enabling FortiAP central management on page 418](#).
2. Create AP profiles.
See [WiFi profiles for central management on page 417](#).
3. Assign profiles to FortiAP devices.
See [Assigning profiles to FortiAP devices on page 441](#).
4. Install FortiAP profiles to devices.
On the *Device Manager* pane, select the FortiGate device that controls the FortiAP device, then select *Install* > *Install Config* from the toolbar, and follow the prompts in the wizard. See [Installing changes to FortiAP devices on page 406](#).

Enabling FortiAP central management

When central management is enabled, you can create templates for a variety of FortiAP configurations, and assign templates to multiple managed access points.

To enable central management:

1. Go to *System Settings > All ADOMs*.
2. Double-click the ADOM to open it for editing.
3. Beside *Central Management*, select the *FortiAP* checkbox, and click *OK*.
Central management is enabled for FortiAP.

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	FAP111C-default	FAP111C	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	
19	FAP224D-default	FAP224D	802.11an_5G	802.11gn only	

The following options are available in the toolbar and right-click menu:

Create New	Create a new AP profile.
Edit	Edit the selected AP profile.
Delete	Delete the selected AP profile.
Clone	Clone the selected AP profile.
Import	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	<input type="text"/>			
Comments	<input type="text" value="0/255"/>			
Platform	FAP220B/221B			
Country/ Region	United States			
AP Login Password	<input type="button" value="Set"/> <input type="button" value="Leave Unchanged"/> <input type="button" value="Set Empty"/>			
Administrative Access	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS <input type="checkbox"/> SSH <input type="checkbox"/> TELNET			
Radio 1				
Mode	<input type="button" value="Disabled"/> <input type="button" value="Access Point"/> <input type="button" value="Dedicated Monitor"/>			
WIDS Profile	<input type="button" value="OFF"/>			
Radio Resource Provision	<input type="button" value="OFF"/>			
Client Load Balancing	<input type="checkbox"/> Frequency Handoff <input type="checkbox"/> AP Handoff			
Band	5 GHz <input type="button" value="802.11n/a"/>			
Channel Width	<input type="button" value="20MHz"/> <input type="button" value="40MHz"/>			
Short Guard Interval	<input type="button" value="OFF"/>			
Channels	<input checked="" type="checkbox"/> 36 <input checked="" type="checkbox"/> 40 <input checked="" type="checkbox"/> 44 <input checked="" type="checkbox"/> 48 <input checked="" type="checkbox"/> 149 <input checked="" type="checkbox"/> 153 <input checked="" type="checkbox"/> 157 <input checked="" type="checkbox"/> 161 <input checked="" type="checkbox"/> 165			
TX Power Control	<input type="button" value="Auto"/> <input type="button" value="Manual"/>			
TX Power	<input type="text" value="100"/> <input type="button" value="↑"/> <input type="button" value="↓"/> %			
SSIDs	<input type="button" value="Auto"/> <input type="button" value="Manual"/>			
Monitor Channel Utilization	<input type="button" value="OFF"/>			
Radio 2				
Mode	<input type="button" value="Disabled"/> <input type="button" value="Access Point"/> <input type="button" value="Dedicated Monitor"/>			
WIDS Profile	<input type="button" value="OFF"/>			
Radio Resource Provision	<input type="button" value="OFF"/>			
Client Load Balancing	<input type="checkbox"/> Frequency Handoff <input type="checkbox"/> AP Handoff			
Band	2.4 GHz <input type="button" value="802.11n/g/b"/>			
Channel Width	<input type="button" value="20MHz"/>			
Short Guard Interval	<input type="button" value="OFF"/>			
Channels	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 7 <input checked="" type="checkbox"/> 8 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 11			
TX Power Control	<input type="button" value="Auto"/> <input type="button" value="Manual"/>			
TX Power	<input type="text" value="100"/> <input type="button" value="↑"/> <input type="button" value="↓"/> %			
SSIDs	<input type="button" value="Auto"/> <input type="button" value="Manual"/>			
Monitor Channel Utilization	<input type="button" value="OFF"/>			
Location Based Services				

2. Enter the following information:

Name	Type a name for the profile.
Comment	Optionally, enter comments.
Platform	Select the platform that the profile will apply to from the dropdown list.
Country/ Region	Select the country or region from the drop-down list.
AP Login Password	Set, leave unchanged (default), or empty the AP login password.
Administrative Access	Allow management access to the managed AP via <i>telnet</i> , <i>http</i> , <i>https</i> , and/or <i>ssh</i> .
Radio 1 & 2	Configure the radio settings. The Radio 2 settings will only appear if the selected platform has two radios.
Mode	Select the radio operation mode: <ul style="list-style-type: none"> • <i>Disabled</i>: The radio is disabled. No further radio settings are available. • <i>Access Point</i>: The device is an access point. • <i>Dedicated Monitor</i>: The device is a dedicated monitor. Only the <i>WIDS Profile</i> setting is available.
WIDS Profile	Select a WIDS profile from the dropdown list. See WIDS profiles on page 431 .
Radio Resource Provision	Select to enable radio resource provisioning. This feature measures utilization and interference on the available channels and selects the clearest channel at each access point.
Client Load Balance	Select the client load balancing methods to use: <i>Frequency Handoff</i> and/or <i>AP Handoff</i> .
Band	Select the wireless protocol from the dropdown list. The available bands depend on the selected platform. In two radio devices, both radios cannot use the same band.
Channel Width	Select 20MHz or 40MHz channel width. This option is only available for 5GHz 802.11n bands.
Short Guard Interval	Select to enable the short guard interval.
Channels	Select the channel or channels to include. The available channels depend on the selected platform and band.
TX Power Control	Optionally, enable automatic adjustment of transmit power, then specify the minimum and maximum power levels, dBm.
TX Power	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.
SSIDs	Manually choose the SSIDs that APs using this profile will carry, or let them be selected automatically.

Monitor Channel Utilization	Enable/disable monitoring channel utilization.
FortiPresence	
Mode	Select the FortiPresence mode: <ul style="list-style-type: none"> • <i>Disable</i> • <i>Foreign channels only</i> • <i>Foreign and home channels</i>
Project name	The FortiPresence project name.
Password	FortiPresence secret password.
FortiPresence server IP	FortiPresence server IP address.
FortiPresence server port	FortiPresence server UDP listening port (default = 3000).
Report rogue APs	Enable/disable FortiPresence reporting of Rogue APs.
Report unassociated clients	Enable/disable FortiPresence reporting of unassociated devices.
Report transmit frequency (in seconds)	FortiPresence report transmit frequency, in seconds (5 - 65535, default = 30).
Ekahau blink	Enable/disable Ekahau blink location based services.
RTLS controller server IP	Enter the realtime location services (RTLS) controller server IP address.
RTLS controller server port	The RTLS controller server port (default = 8569).
Ekahau tag MAC address	Enter the Ekahau tag MAC address.
AeroScout	Enable/disable AeroScout location based services.
AeroScout server IP	Enter the AeroScout server IP address.
AeroScout server port	Enter the AeroScout server port.
MU mode dilution factor	Enter the MU mode dilution factor (default = 20).
MU mode dilution timeout	Enter the MU mode dilution timeout (default = 5).
Locate WiFi clients when not connected	Enable/disable locating WiFi client when they are not connected.

Advanced Options

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:

Create New	Create a new SSID (see Creating SSIDs on page 424) or SSID group.
Edit	Edit the selected SSID or group.
Clone	Clone the selected SSID or group.
Delete	Delete the selected SSID or group.
Import	Import SSIDs from a connected FortiGate (toolbar only).
Where Used	View where the SSID is used.
Column Settings	Adjust the visible columns.

To create a new SSID group:

1. 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* window 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

WiFi Settings

SSID

Security Mode WPA2 Only Personal

Pre-shared Key

Client Limit

Multiple Pre-shared Keys

Broadcast SSID ON

Schedule always

Block Intra-SSID Traffic

Broadcast Suppression ON

ARPs for known clients
 DHCP uplink
 2 Entries Selected

Filter Clients by MAC Address

RADIUS Server

VLAN Pooling

Quarantine Host ON

Encrypt TKIP AES TKIP-AES

QoS Profile

Advanced Options >

2. Enter the following information, then click *OK* to create the new tunnel to wireless controller SSID:

Interface Name	Type a name for the SSID.
Alias	Set the alias for SSID.
Traffic Mode	Select the traffic mode: <i>Tunnel</i> , <i>Bridge</i> , or <i>Mesh</i> .
Address	These options are only available when <i>Traffic Mode</i> is <i>Tunnel</i> .
IP/Network Mask	Enter the IP address and netmask.
IPv6 Address	Enter the IPv6 address.
Administrative Access	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> .
IPv6 Administrative Access	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> .
DHCP Server	Turn the DHCP server on or off.
WiFi Settings	

SSID	Type the wireless service set identifier (SSID), or network name, for this wireless interface. Users who want to use the wireless network must configure their computers with this network name.																		
Security Mode	<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>																		
Pre-shared Key	<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>																		
Local Standalone	<p>Enable/disable AP local standalone (default = disable).</p> <p>This option is only available when the traffic mode is <i>Bridge</i>.</p>																		
Local Authentication	<p>Enable/disable AP local authentication.</p> <p>This option is only available when the traffic mode is <i>Bridge</i>.</p>																		
Client Limit	The maximum number of clients that can simultaneously connect to the AP (0 - 4294967295, default = 0, meaning no limitation).																		
Client Limit per Radio	<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>																		
Multiple Pre-Shared Keys	<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>																		
Default Client Limit Per Key	<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>																		
Portal Type	<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>																		

Authentication Portal	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.
User Groups	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.
Exempt Sources	Select exempt sources to add from the dropdown list. This option is only available when the portal type includes authentication.
Devices	Select exempt devices to add from the dropdown list. This option is only available when the portal type includes authentication.
Exempt Destinations	Select exempt destinations to add from the dropdown list. This option is only available when the portal type includes authentication.
Exempt Services	Select exempt services to add from the dropdown list. This option is only available when the portal type includes authentication.
Customize Portal Messages	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.
Redirect after Captive Portal	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.
Authentication	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.
Broadcast SSID	Enable/disable broadcasting the SSID (default = enable). Broadcasting enables clients to connect to the wireless network without first knowing the SSID. For better security, do not broadcast the SSID.
Schedule	Select a schedule to control the availability of the SSID. For information on creating a schedule object, see Create a new object on page 245 .
Block Intra-SSID Traffic	Enable/disable blocking communication between clients of the same AP (default = disable).
Broadcast Suppression	Optional suppression of broadcast message types: <ul style="list-style-type: none"> • <i>All other broadcast</i>: All other broadcast messages • <i>All other multicast</i>: All other multicast messages • <i>ARP poison</i>: ARP poison messages from wireless clients • <i>ARP proxy</i>: ARP requests for wireless clients as a proxy • <i>ARP replies</i>: ARP replies from wireless clients • <i>ARPs for known clients</i>: ARP for known messages • <i>ARPs for unknown clients</i>: ARP for unknown messages • <i>DHCP downlink</i>: Downlink DHCP messages

	<ul style="list-style-type: none"> • <i>DHCP starvation</i>: DHCP starvation req messages • <i>DHCP uplink</i>: Uplink DHCP messages • <i>IPv6</i>: IPv6 packets • <i>NetBIOS datagram service</i>: NetBIOS datagram services packets • <i>NetBIOS name service</i>: NetBIOS name services packets
Filter Clients by MAC Address	Enable/disable using a RADIUS server to filter clients by MAC address, then select the server from the drop-down list. See RADIUS servers on page 628 for information on adding a RADIUS server.
VLAN Pooling	<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"> • <i>Managed AP Group</i>: Select devices to include in the group. • <i>Round Robin</i> • <i>Hash</i> <p>This option is not available when the traffic mode is <i>Mesh</i>.</p>
Quarantine Host	<p>Enable/disable station quarantine (default = enable).</p> <p>This option is only available when the security mode includes WPA or WPA2.</p>
Encrypt	<p>Select the data encryption protocol:</p> <ul style="list-style-type: none"> • <i>TKIP</i>: Temporal Key Integrity Protocol, used by the older WPA standard. • <i>AES</i>: Advanced Encryption Standard, commonly used with the newer WPA2 standard (default). • <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). <p>This option is only available when the security mode includes WPA or WPA2.</p>
QoS Profile	Select the QoS profile from the drop-down list.
Advanced Options	Configure advanced options. For information, see the <i>FortiOS CLI Reference</i> .
Per-Device Mapping	Enable per-device mapping to override the SSID profile settings for selected devices. See Adding SSID per-device mapping on page 428 .



If you select WPA Enterprise, WPA Only Enterprise, or WPA2 Only Enterprise, you can add a different RADIUS server using per-device mapping. See [Adding SSID per-device mapping on page 428](#).

Adding SSID per-device mapping

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

<input type="checkbox"/>	#	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

<input type="checkbox"/>	#	Option Code	Value
No records found...			

MAC Reservation + Access Control

Unknown MAC Address

Action

Mapped Device	Select the device to be mapped from the drop-down.
Mapped IP/NetMask	Specify the Mapped IP/NetMask.
Mapped DHCP Server	Set the <i>DHCP Server</i> to <i>ON</i> if you want to map a DHCP Server to this device.
Address Range	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> .
Netmask	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> .
Default Gateway	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> .
DNS Server	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> .
Mode	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> .
NTP Server	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> .

Time Zone	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> .
Next Bootstrap Server	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> .
Additional DHCP Options	In the <i>Lease Time</i> field, enter the lease time, in seconds (default = 604800 (7 days)). Add DHCP options to the table. For details, see Adding additional DHCP options on page 430 . 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> .
MAC Reservation + Access Control	Select the action to take with unknown MAC addresses: <i>assign</i> or <i>block</i> . Add MAC address actions to the table. For details, see Adding a MAC address reservation on page 430 . 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> .
DHCP Server IP	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> .
Type	Select the type: <i>Regular</i> , or <i>IPsec</i> . This option is only available when <i>DHCP Server</i> is <i>ON</i> .

Adding additional DHCP options

To add additional DHCP options:

1. Click *Create* in the *Additional DHCP Options* table toolbar. The *Additional DHCP Options* dialog box opens.

Additional DHCP Options

Option Code: 0

Type: **hex** ip string

Hexadecimal Value:

OK Cancel

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.

Adding a MAC address reservation

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.

MAC Reservation + Access Control

MAC Address

00:00:00:00:00:00

End IP

Assign IP

Block

Reserve IP

0.0.0.0

Description

0/255

OK

Cancel

- 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:

Create New	Create a new WIDS profile.
Edit	Edit the selected WIDS profile.
Delete	Delete the selected WIDS profile.
Clone	Clone the selected WIDS profile.
Import	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	OFF		
Association Frame Flooding	OFF	30	10
Authentication Frame Flooding	OFF	30	10
Broadcasting Deauthentication	OFF		
EAPOL-FAIL Flooding (to AP)	OFF	10	1
EAPOL-LOGOFF Flooding (to AP)	OFF	10	1
EAPOL-START Flooding (to AP)	OFF	10	1
EAPOL-SUCC Flooding (to AP)	OFF	10	1
Invalid MAC OUI	OFF		
Long Duration Attack	OFF	8200	μs
Null SSID Probe Response	OFF		
Premature EAPOL-FAIL Flooding (to Client)	OFF	10	1
Premature EAPOL-SUCC Flooding (to Client)	OFF	10	1
Spoofed Deauthentication	OFF		
Weak WEP IV (Initialization Vector)	OFF		
Wireless Bridge	OFF		

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:

Name	Enter a name for the profile.
Comments	Optionally, enter comments.
Sensor Mode	
Enable Rogue AP Detection	Select to enable rogue AP detection.
Background Scan Every	Enter the number of seconds between background scans.
Enable Passive Scan Mode	Enable/disable passive scan mode.
Auto Suppress Rogue APs in Foreground Scan	Enable/disable automatically suppressing rogue APs in foreground scans. This options is only available when the sensor mode is not disabled.

Disable Background Scan During Specified Time	Enable/disable background scanning during the specified time. Specify the days of week, and the start and end times.
Intrusion Type	The intrusion types that can be detected.
Enable	Select to enable the intrusion type.
Threshold	If applicable, enter a threshold for reporting the intrusion, in seconds except where specified.
Interval (Seconds)	If applicable, enter the interval for reporting the intrusion, in seconds.
Advanced Options	
ap-bgscan-duration	Listening time on a scanning channel, in milliseconds (10 - 1000, default = 20).
ap-bgscan-idle	Waiting time for channel inactivity before scanning this channel, in milliseconds (0 - 1000, default = 0).
ap-bgscan-intv	Period of time between scanning two channels, in seconds (1 - 600, default = 1).
ap-bgscan-report-intv	Period of time between background scan reports, in seconds (15 - 600, default = 30).
ap-fgscan-report-intv	Period of time between foreground scan reports, in seconds (15 - 600, default = 15).
deauth-broadcast	Enable/disable broadcasting deauthentication detection (default = disable).
deauth-unknown-src-thresh	Threshold value per second to deauthenticate unknown sources for DoS attacks, in seconds (0 - 65535, 0 = no limit, default = 10).
invalid-mac-oui	Enable/disable invalid MAC OUI detection (default = disable).

Intrusion types

Intrusion Type	Description
Asleep Attack	ASLEAP is a tool used to perform attacks against LEAP authentication.
Association Frame Flooding	A Denial of Service attack using association requests. The default detection threshold is 30 requests in 10 seconds.
Authentication Frame Flooding	A Denial of Service attack using association requests. The default detection threshold is 30 requests in 10 seconds.
Broadcasting Deauthentication	This is a type of Denial of Service attack. A flood of spoofed de-authentication frames forces wireless clients to de-authenticate, then re-authenticate with their AP.
EAPOL Packet Flooding (to AP)	Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the AP with these packets can be a denial of service attack.

Intrusion Type	Description
	<p>Several types of EAPOL packets can be detected:</p> <ul style="list-style-type: none"> • EAPOL-FAIL • EAPOL-LOGOFF • EAPOL-START • EAPOL-SUCC
Invalid MAC OUI	Some attackers use randomly-generated MAC addresses. The first three bytes of the MAC address are the Organizationally Unique Identifier (OUI), administered by IEEE. Invalid OUIs are logged.
Long Duration Attack	To share radio bandwidth, WiFi devices reserve channels for brief periods of time. Excessively long reservation periods can be used as a denial of service attack. You can set a threshold between 1000 and 32 767 microseconds. The default is 8200μ.
Null SSID Probe Response	When a wireless client sends out a probe request, the attacker sends a response with a null SSID. This causes many wireless cards and devices to stop responding.
Premature EAPOL Packet Flooding (to client)	<p>Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the client with these packets can be a denial of service attack.</p> <p>Two types of EAPOL packets can be detected:</p> <ul style="list-style-type: none"> • EAPOL-FAIL • EAPOL-SUCC
Spoofed Deauthentication	Spoofed de-authentication frames form the basis for most denial of service attacks.
Weak WEP IV Detection	A primary means of cracking WEP keys is by capturing 802.11 frames over an extended period of time and searching for patterns of WEP initialization vectors (IVs) that are known to be weak. WIDS detects known weak WEP IVs in on-air traffic.
Wireless Bridge	WiFi frames with both the FromDS and ToDS fields set indicate a wireless bridge. This will also detect a wireless bridge that you intentionally configured in your network.

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:

Create New	Create a new Bluetooth profile.
Edit	Edit the selected Bluetooth profile.
Delete	Delete the selected Bluetooth profile.
Clone	Clone the selected Bluetooth profile.
Import	Import Bluetooth profiles from a connected FortiGate (toolbar only).

To create a new Bluetooth profile:

1. 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

Major ID

Minor ID

Eddystone Namespace

Eddystone Instance

Eddystone URL

TX Power

Beacon Interval ms

BLE Scanning

Advanced Options ▾

eddytone-url-encode-hex

2. Enter the following information:

Name	Enter a name for the profile.
Comments	Optionally, enter comments.
Advertising	Select the advertising types: <i>iBeacon</i> , <i>Eddystone-UUID</i> , and <i>Eddystone-URL</i> .
iBeacon UUID	The iBeacon Universally Unique Identifier (UUID) is automatically assigned, but can be manually reset (63 characters).
Major ID	The major ID (1 - 65535, default = 1000).
Minor ID	The minor ID (1 - 65535, default = 2000).
Eddystone Namespace	The eddytone namespace ID (10 characters).
Eddystone Instance	The eddytone instance ID (6 characters).
Eddystone URL	The eddytone URL (127 characters).
TX Power	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>
Beacon Interval	The beacon interval, in milliseconds (40 - 3500, default = 100).
BLE Scanning	Enable/disable Bluetooth Low Energy (BLE) scanning.
Advanced Options	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:

Create New	Create a new QoS profile.
Edit	Edit the selected QoS profile.
Delete	Delete the selected QoS profile.
Clone	Clone the selected QoS profile.
Import	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:

Name	Enter a name for the profile.
Comments	Optionally, enter comments.
Max Uplink Speed (VAPs)	The maximum uplink speed (VAPs), in Kbps (0 - 2097152, default = 0).
Max Downlink Speed (VAPs)	The maximum downlink speed (VAPs), in Kbps (0 - 2097152, default = 0).
Max Uplink Speed (Clients)	The maximum uplink speed (Clients), in Kbps (0 - 2097152, default = 0).
Max Downlink Speed (Clients)	The maximum downlink speed (Clients), in Kbps (0 - 2097152, default = 0).
Client Rate Burst	Enable/disable client rate burst (default = disable).
Wi-Fi MultiMedia	Enable/disable WiFi Multimedia (WMM) control (default = enable).
U-APSD Power Save Mode	Enable/disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode (default = enable). This option is only available if <i>Wi-Fi MultiMedia</i> is enabled.
Call Admission Control	Enable/disable WMM call admission control (default = disable). This option is only available if <i>Wi-Fi MultiMedia</i> is enabled.
Call Capacity	The maximum number of VoWLAN phones allowed (0 - 60, default = 10). This option is only available if <i>Call Admission Control</i> is enabled.
Bandwidth Admission Control	Enable/disable WMM bandwidth admission control (default = disable). This option is only available if <i>Call Admission Control</i> is enabled.
Bandwidth Capacity	The maximum bandwidth capacity allowed, in Kbps (1 - 600000, default = 2000). This option is only available if <i>Bandwidth Admission Control</i> is enabled.
DSCP Mapping	Enable/disable differentiated Services Code Point (DSCP) mapping (default = disable).

Voice Access	DSCP mapping for voice access category (default = 48, 56). This option is only available if <i>DSCP Mapping</i> is enabled.
Video Access	DSCP mapping for video access category (default = 32, 40). This option is only available if <i>DSCP Mapping</i> is enabled.
Best Effort Access	DSCP mapping for best effort access category (default = 0, 24). This option is only available if <i>DSCP Mapping</i> is enabled.
Background Access	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:

Create New	Create a new Bonjour profile.
Edit	Edit the selected Bonjour profile.
Delete	Delete the selected Bonjour profile.
Clone	Clone the selected Bonjour profile.
Import	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:

Name	Enter a name for the profile.
Comments	Optionally, enter comments.
Policy List	Configure the policy list.
Create New	Create a new policy list entry. Select the following, then click <i>OK</i> : <ul style="list-style-type: none"> • <i>Description</i>: Description of the Bonjour profile policy. • <i>From VLAN</i>: The VLAN ID that the Bonjour service will be advertised from (0 - 4094, default = 0). • <i>To VLAN</i>: The VLAN ID that the Bonjour service will be made available to (0 - 4094, default = all). • <i>Services</i>: Services for the VLAN.
Edit	Edit the selected entry.
Delete	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.

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 418](#).

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.

WiFi profiles for per-device management

When per-device management is enabled, you can configure changes on each managed access point. The following steps provide an overview of using per-device access point management:

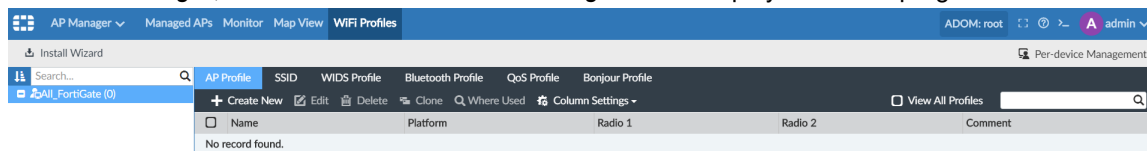
1. Enable per-device management.
See [Enabling FortiAP per-device management on page 442](#).
2. Configure profiles for each managed access point.
See [Creating profiles on page 442](#).
3. Install changes to managed access points.
See [Installing changes to FortiAP devices on page 406](#).

Enabling FortiAP per-device management

When per-device management is enabled, you can configure changes on each managed FortiAP.

To enable access point per-device management:

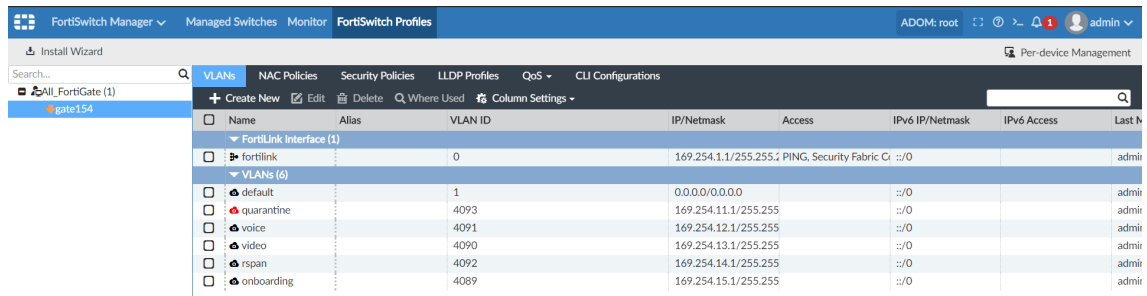
1. Go to *System Settings > All ADOMs*.
2. Double-click the ADOM to open it for editing.
3. Beside *Central Management*, clear the *FortiAP* checkbox, and click *OK*.
Central management is disabled, and per-device management is enabled for *AP Manager*.
4. Go to *AP Manager*, and notice that *Per-device Management* is displayed in the top-right corner.



Creating profiles

To create profiles:

1. Go to *FortiAP Manager > WiFi Profiles*.
2. In the tree menu, select a FortiGate.
The *AP Profile* tab is displayed.



3. In the content pane, click the tab for the profile you want to create, and click *Create New*.
The pane for the selected tab opens.
4. Edit the options, and click *OK*.
The changes are saved to the FortiGate database.

FortiSwitch Manager

The *FortiSwitch Manager* pane allows you to manage FortiSwitch devices that are controlled by FortiGate devices that are managed by FortiManager. You can use *FortiSwitch Manager* for the following modes of management:

- Central management of managed switches
- Per-device management of managed switches

The tabs available on the *FortiSwitch Manager* pane depend on whether you have central management or per-device management enabled. When **central management** is enabled, the *FortiSwitch Manager* module includes the following tabs:

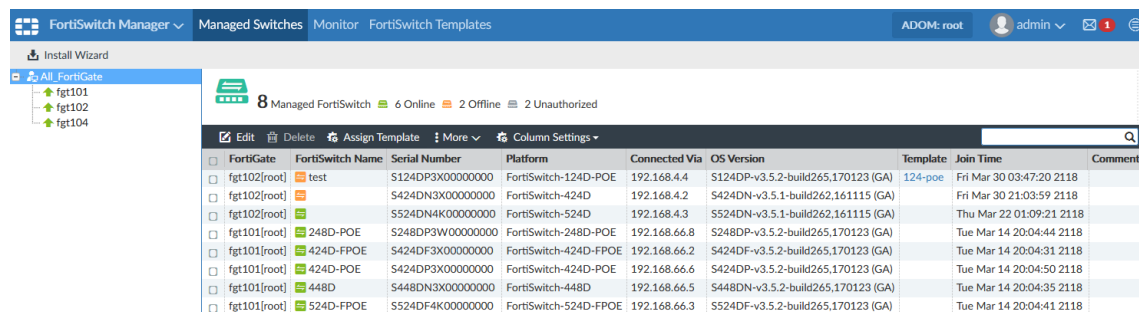
Managed Switches	Displays unauthorized and authorized FortiSwitch devices. You can view, authorize, and edit authorized switches, as well as apply templates to switches.
Monitor	Monitor FortiSwitch devices with a graphical representation of the connected switches.
FortiSwitch Templates	View, create, and edit FortiSwitch templates, VLANs, and security policies. Templates can also be imported.

When **per-device management** is enabled, the *FortiSwitch Manager* module includes the following tabs:

Managed Switches	Displays unauthorized and authorized FortiSwitch devices. You can view, authorize, and edit authorized switches as well as configure ports for each managed switch.
Monitor	Monitor FortiSwitch devices with a graphical representation of the connected switches.
FortiSwitch Profiles	View, create, and edit VLANs, NAC policies, security policies, LLDP profiles, and QoS policies settings for each managed switch. You can also use the CLI to configure switches.

Managed Switches

Go to *FortiSwitch Manager > Managed Switches* to access managed 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	



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 565](#).

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
- Unknown

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:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *FortiSwitch Manager > Managed Switches*. The quick status bar is displayed above the content pane.



1 Managed FortiSwitch 0 Online 0 Offline 0 Unauthorized 1 Unknown

3. 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.
4. 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.

Edit Delete Assign Template More Column Settings									
FortiGate	FortiSwitch Name	Serial Number	Platform	Connected Via	OS Version	Template	Join Time	Comments	
<input type="checkbox"/> 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		
<input type="checkbox"/> fgt102[root]		S424DN3X00000000	FortiSwitch-424D	192.168.0.2	S424DN-v3.5.1-build262,161115 (GA)		Fri Mar 30 21:03:59 2018		
<input type="checkbox"/> fgt102[root]		S524DN4K00000000	FortiSwitch-524D	192.168.1.1	S524DN-v3.5.1-build262,161115 (GA)		Thu Mar 22 01:09:21 2018		
<input type="checkbox"/> fgt101[root]		S248DP3W00000000	FortiSwitch-248D-POE	192.168.2.1	S248DP-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:44 2017		
<input type="checkbox"/> 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		
<input type="checkbox"/> 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		
<input type="checkbox"/> fgt101[root]	448D	S448DN3X00000000	FortiSwitch-448D	192.168.3.2	S448DN-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:35 2017		
<input type="checkbox"/> 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:

Edit	Edit the selected FortiSwitch.
Delete	Delete the switch or switches.
Ports Configuration	Available when per-device management is enabled for <i>FortiSwitch Manager</i> . Configure ports for the selected FortiSwitch. See Configuring a port on a single FortiSwitch on page 473 .
Assign Template	Available when central management is enabled for <i>FortiSwitch Manager</i> . Assign a template to the switch. Only applicable templates will be listed. See Assigning templates to FortiSwitch devices on page 467 .
Upgrade	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, you can optionally go to <i>FortiGuard > Firmware Images > Product: FortiSwitch</i> , and click the download icon to manually download the firmware images.
Authorize	Authorize a switch. See Authorizing and deauthorizing FortiSwitch devices on page 447 . This option is also available in the toolbar by selecting <i>More</i> .
Deauthorize	Deauthorize a switch. See Authorizing and deauthorizing FortiSwitch devices on page 447 . This option is also available in the toolbar by selecting <i>More</i> .
Restart	Restart the switch. This option is also available in the toolbar by selecting <i>More</i> .
Connect to CLI	Connect to FortiSwitch device's CLI, if available. This option is also available in the toolbar by selecting <i>More</i> .
Cable Test	Trigger a FortiSwitch cable test. See Run cable test on FortiSwitch ports from FortiManager on page 451 . This option is only available on ADOM 6.4 and later. FortiSwitch cable test can also be accessed by selecting <i>More</i> in the toolbar.
Refresh	Refresh the switch list. This option is also available in the toolbar by selecting <i>More</i> .
Column Settings	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.
Search	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:

FortiSwitch Name	The name assigned to the switch.
Serial Number	The serial number of the switch.
Platform	The FortiSwitch model.

FortiGate	The FortiGate that the FortiSwitch is connected to.
Connected Via	The IP address of the switch.
OS Version	The OS version on the switch.
Template	The FortiSwitch template assigned to the device, if any.
Join Time	The date and time that the switch joined.
Comments	User entered comments.

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. In the content pane, select the switch and click *Edit* from the toolbar, or right-click on the switch and select *Edit*. The *Edit Managed FortiSwitch* window opens.

The following example is of *FortiSwitch Manager* with central management enabled.

Edit Managed FortiSwitch

Serial Number

S448DN3X16000000

Name

Description

Template

Managed Switch Status

Status

Connected

Restart

Connecting From

169.258.1.018

Join Time

Mon May 14 15:15:49 2018

State

Authorized

Deauthorize

Firmware

FortiSwitch OS Version

S448DN-v3.6.5-build403,180226 (GA) [\[Upgrade\]](#)

Apply

Return

3. Edit the following options, then click *Apply* to apply your changes.

Serial Number	The device's serial number. This field cannot be edited.
Name	The name of the FortiSwitch.
Description	A description of the FortiSwitch, such as its model.
Template	Available when central management is enabled for <i>FortiSwitch Manager</i> . Select the template that will be applied to the FortiSwitch from the dropdown list. Only applicable templates are available.
Status	The status of the FortiSwitch, such as <i>Connected</i> . Click <i>Restart</i> to restart the switch.
Connecting From	The IP address of the switch.

Join Time	The date and time that the switch joined.
State	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 Authorizing and deauthorizing FortiSwitch devices on page 447 .
FortiSwitch OS Version	The OS version on the switch. Click <i>Upgrade</i> to upgrade the firmware to a newer version if you have one available. See Firmware Management on page 99

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. In the content pane, select the switch or switches, and click *Delete* from the toolbar, or right-click and select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the switch or switches.

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 446](#)).

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.

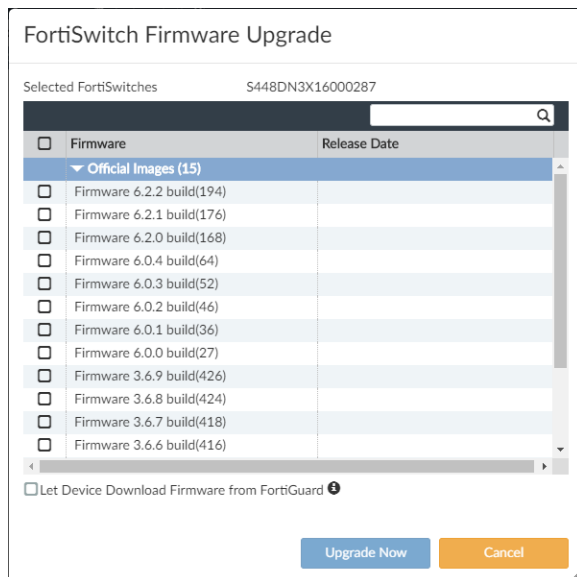
Upgrading firmware for managed switches

You can use FortiManager to upgrade firmware for FortiSwitch units. By default, FortiManager retrieves the firmware from FortiGuard.

You can also optionally import special firmware images for FortiSwitch to the FortiGuard module, and then use them to upgrade FortiSwitch units.

To upgrade firmware for managed switches:

1. Go to *FortiSwitch Manager > Managed Switches*.
2. In the tree menu, select a FortiGate.
The managed FortiSwitches are displayed in the content pane.
3. Right-click a FortiSwitch, and select *Upgrade*.
The *FortiSwitch Firmware Upgrade* dialog box is displayed.



4. Select the firmware, and click *Upgrade Now*.

Using zero-touch deployment for FortiSwitch

Configure FortiSwitch on FortiManager using its serial number and deploy FortiSwitch devices across the network using zero touch deployment. After configuring FortiSwitch on FortiManager, you can deploy remote FortiSwitch devices by just plugging them into remote FortiGate devices.

Requirements:

- FortiManager version 5.6 ADOM or later.
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with FortiSwitch.
- The FortiSwitch serial number is available.

To enable zero touch deployment:

1. Go to *FortiSwitch Manager > Managed Switches*.
2. Click *Create New*. The *Add Model FortiSwitch* pane is displayed.

3. Configure the following settings, and click *OK*:

FortiGate	Select the FortiGate device or VDOM from the drop-down.
Device Interface	Select the port where the FortiSwitch will be connected.
Serial Number	Specify the FortiSwitch serial number.
Name	Specify a name.
Enforce Firmware Version	Toggle <i>ON</i> to enforce a firmware version and select the firmware version from the drop-down menu. Toggle <i>OFF</i> to disable this feature.

A model FortiSwitch is created and added to the managed FortiGate.

4. Click *Close* to close the *Add Model FortiSwitch* pane.
5. Configure the switch.
 - For *FortiSwitch Manager* with central management enabled, see [Assigning templates to FortiSwitch devices on page 467](#).
 - For *FortiSwitch Manager* with per-device management enabled, see [Configuring a port on a single FortiSwitch on page 473](#).

Because this is a model device, FortiManager saves the changes to the FortiGate database.

6. Connect FortiSwitch to FortiGate.
The FortiSwitch settings are deployed to FortiSwitch. You can view the progress on the notification toolbar in FortiManager.



You can also use the Zero Touch Deployment process to deploy FortiGate devices. For more information, see [Adding a model device on page 42](#).

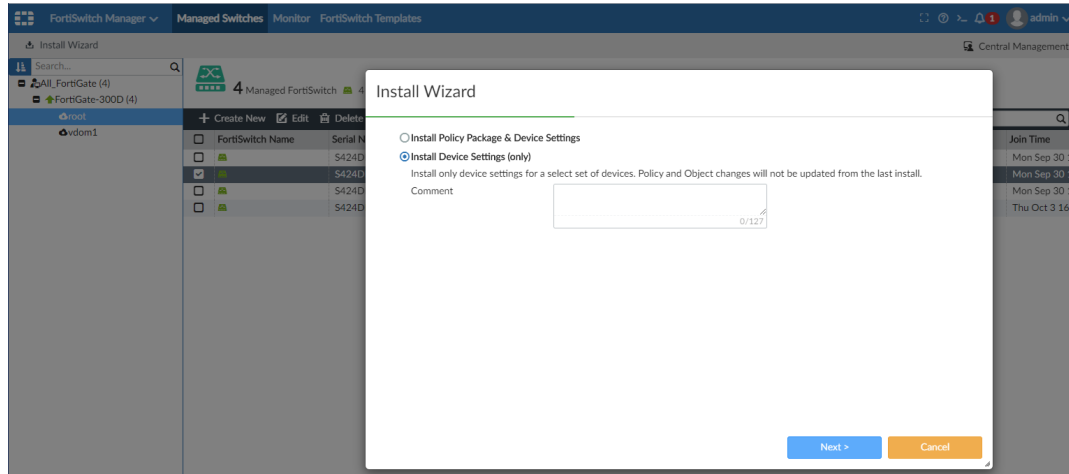
Installing changes to managed switches

On the *FortiSwitch Manager* pane, you can use the *Install Wizard* to install changes to managed FortiSwitch devices. Alternately you can install changes when you install a configuration to the FortiGate that manages the switch.

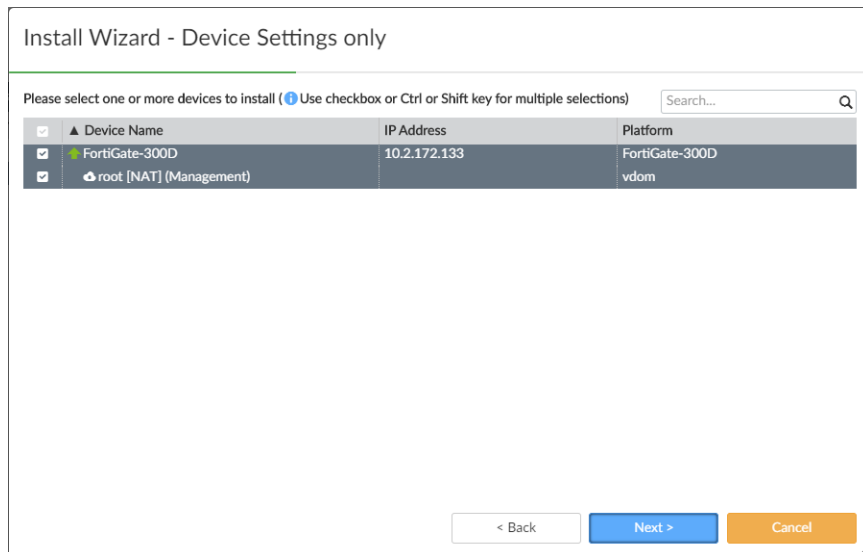
To install changes to managed switches:

1. Go to *FortiSwitch Manager > Managed Switches*.
2. In the tree menu, select the FortiGate device that controls the FortiSwitch, and click *Install Wizard*.
The managed switches are displayed in the content pane.

3. In the content pane, select the switch, and click *Install Wizard*.
The *Install Wizard* is displayed.



4. Select *Install Device Settings (only)*, and click *Next*.
The *Device Settings only* pane is displayed.



5. Select the device, and click *Next*.
The *Device Settings* pane is displayed.

Install Wizard - Device Settings

Only successfully validated device may be installed. Please confirm and click "Install" button to continue.

☐

▲ Device Name

☐

FortiGate-300D

Status

Connection Up

Action

Install Preview

Install

Cancel

6. (Optional) Click *Install Preview* to review the changes.
7. Click *Install*.

Run cable test on FortiSwitch ports from FortiManager

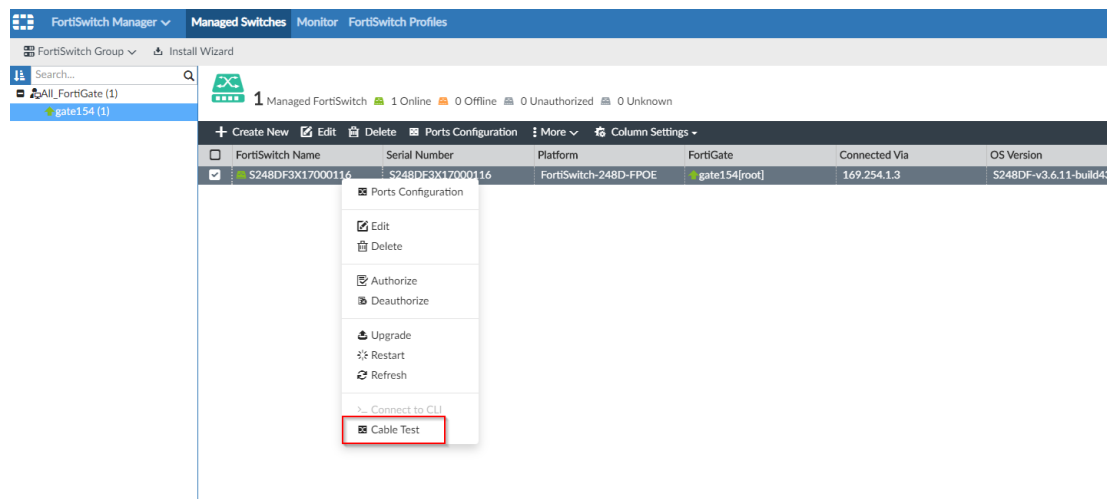
You can trigger a FortiSwitch cable test from FortiManager.



The FortiSwitch cable test is only available on ADOM 6.4 and later.

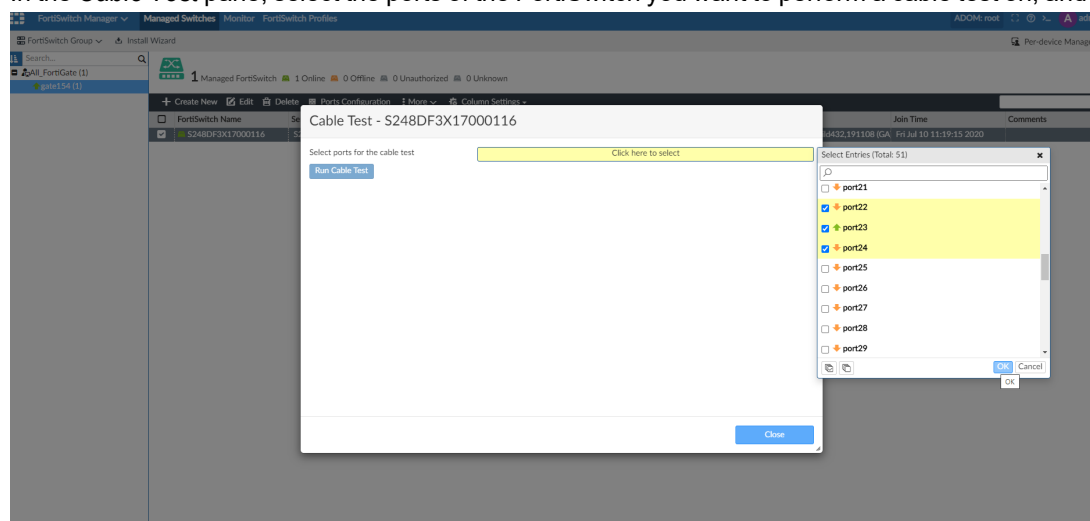
To perform a FortiSwitch cable test:

1. Go to *FortiSwitch Manager > Managed Switches*.
2. In the tree menu, select a FortiGate that contains the FortiSwitch on which the cable test is to be performed.
3. Select the FortiSwitch and either click *More > Cable Test* from the toolbar, or right-click the FortiSwitch and select *Cable Test*.



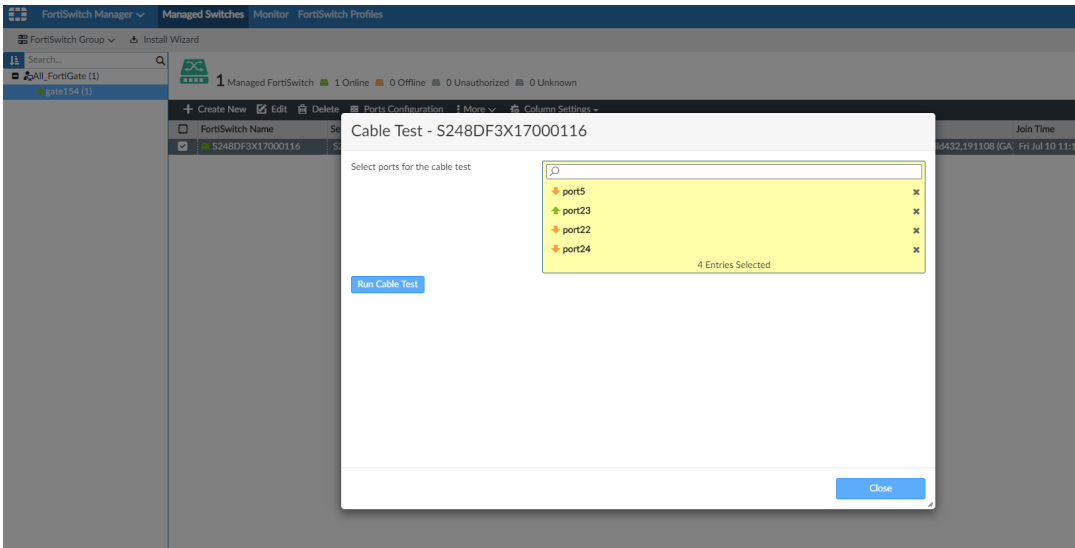
The *Cable Test* pane opens.

4. In the *Cable Test* pane, select the ports of the FortiSwitch you want to perform a cable test on, and click *OK*.

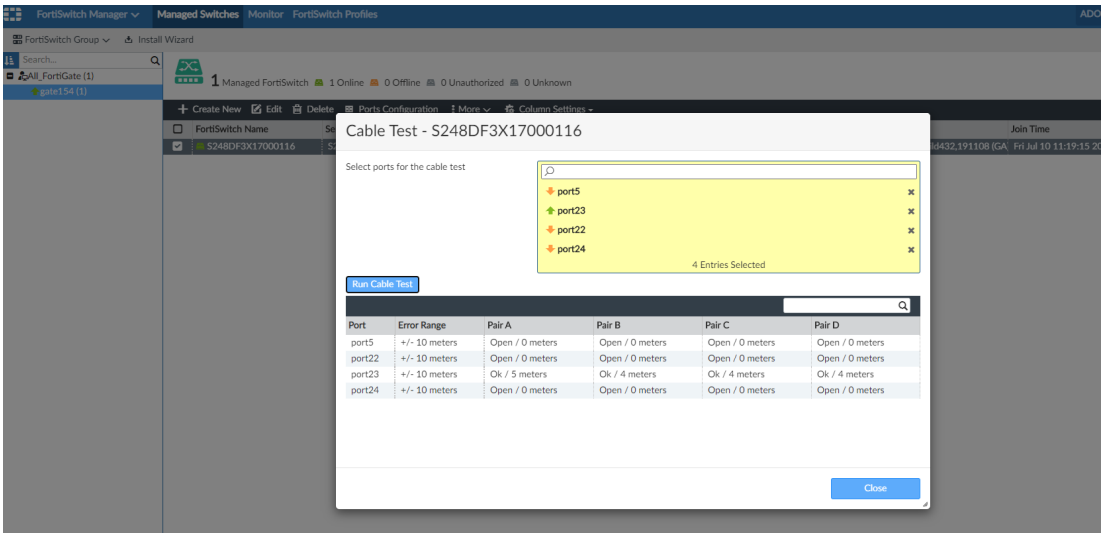


The *Select Entries* list does not contain FortiLink ports because cable test is not allowed for the FortiLink interface.

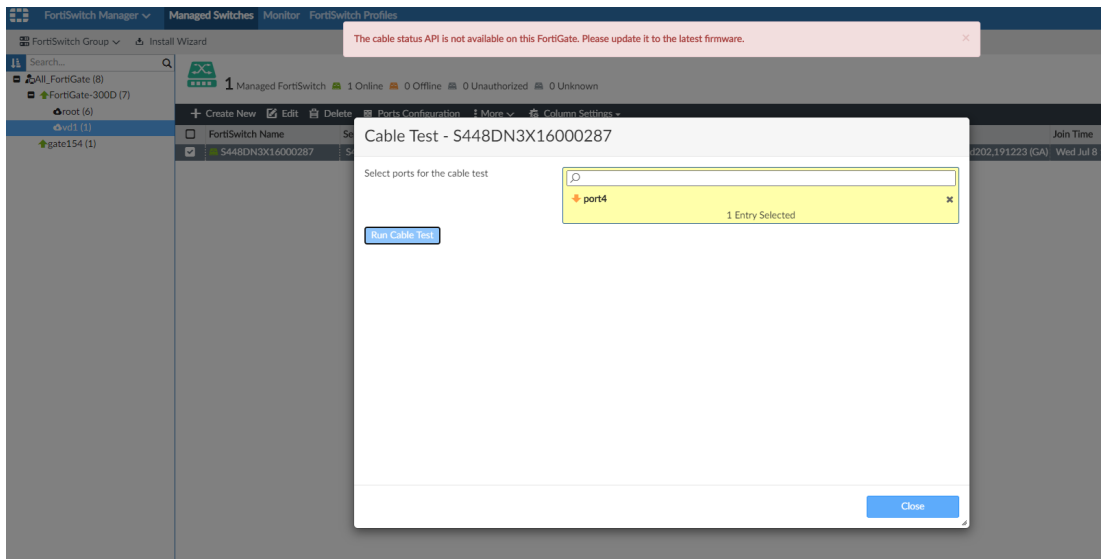
5. Click *Run Cable Test* to run the FortiSwitch cable test on the selected ports.



Once the cable test is finished, the results are displayed.



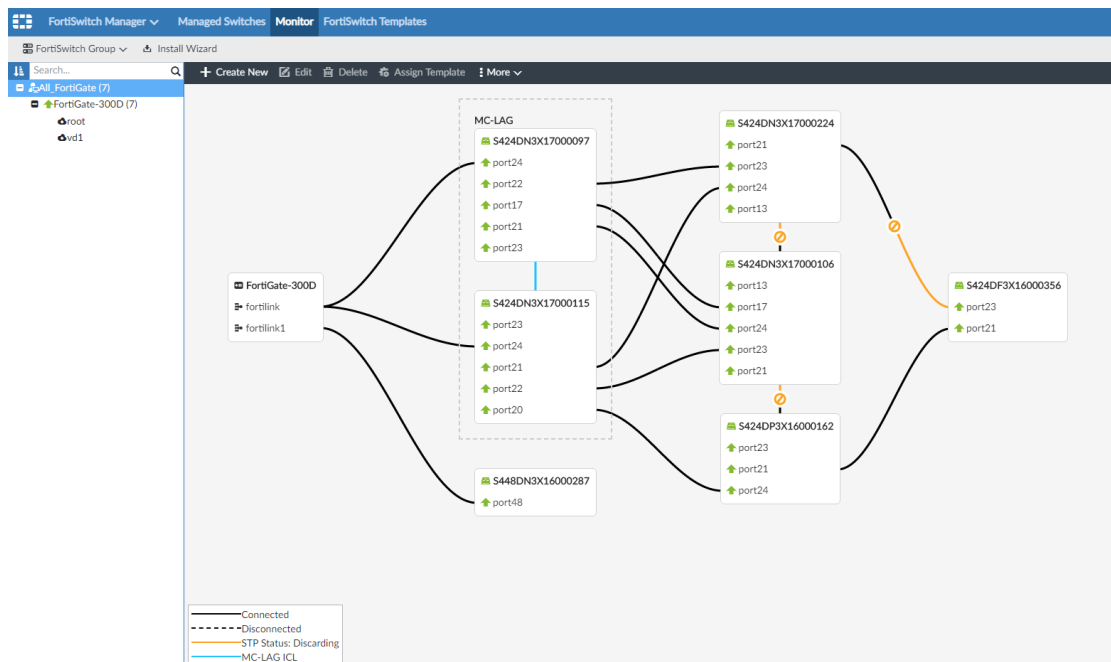
If the cable test API is not available for your version of FortiOS (6.4 branch, but build 1704 or earlier), an error prompt is displayed asking you to update to the latest firmware.



Monitor

The *FortiSwitch Manager > Monitor* pane shows a graphical representation of the connected FortiSwitch devices. You can now see topology view similar to FortiOS for selected devices. This gives you the visibility of the managed FortiSwitch status, connection topology, and MC-LAG status among others.

Use the *Refresh* button to refresh the view, the search box to find a specific device or filter the view, and hover over connections or ports to get more information.



Ports that are transmitting and receiving data are highlighted in green.

Hovering the cursor over a port group will open a pop-up showing the type of port in the group. Hovering the cursor over a port will open a pop-up showing information about the port, including:

Port	The port number.
FortiSwitch	The name of the FortiSwitch.
Peer Device	The device that this switch is connected to. The current port, as well as the port that it is connected to on the connected, and the connection between the two devices, will be highlighted. This item is only displayed when the port is connected to another FortiSwitch device.
Native VLAN	The native VLAN of the port.
PoE	Whether or not the port is currently providing PoE power. This item is only displayed on PoE ports.
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.
STP Status	<i>Forwarding</i> or <i>Discarding</i> STP status.
Bytes Sent	The total number of bytes sent by the port.
Bytes Received	The total number of bytes received by the port.

FortiSwitch Templates for central management

When central management is enabled, you can create templates for a variety of switch configurations, and assign templates to multiple managed switches. The following steps provide an overview of using centralized FortiSwitch management to configure and install templates:

1. Enable central management of switches. See [Enabling FortiSwitch central management on page 455](#).
2. Create FortiSwitch VLANs. See [Creating VLANs on page 468](#).
3. Create or import FortiSwitch templates. See [FortiSwitch Templates on page 456](#).
4. Assign templates to FortiSwitch devices. See [Assigning templates to FortiSwitch devices on page 467](#).
5. Install the templates to the devices. See [Installing changes to managed switches on page 449](#).

Enabling FortiSwitch central management

When central management is enabled, you can create templates for a variety of switch configurations, and assign templates to multiple managed switches.

To enable central management:

1. Go to *System Settings > All ADOMs*.
2. Double-click the ADOM to open it for editing.

3. Beside *Central Management*, select the *FortiSwitch* checkbox, and click *OK*.

Edit ADOM

Name

root

Type

FortiGate

6.2

Comments

0/128

Devices

Name	IP Address	Platform
FortiGate-140E-POE	10.2.172.153	FortiGate-140E-POE
FortiGate-300D	10.2.172.133	FortiGate-300D

Mode

Normal

Backup

Central Management

VPN

FortiSwitch

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

Central management is enabled for FortiSwitch.

FortiSwitch Templates

The *FortiSwitch Manager > FortiSwitch Templates* tab is available when central management is enabled. You can use the *FortiSwitch Templates* tab to create and manage FortiSwitch templates, VLANs, security policies, LLDP profiles, and QoS policies that can be assembled into templates, and then the template assigned to FortiSwitch devices. You can also import templates from FortiSwitch devices, and then apply the template to other FortiSwitch devices of the same model.

Accessing FortiSwitch templates

FortiSwitch templates define VLAN and PoE assignments for a FortiSwitch platform.

To view FortiSwitch templates:

- 1. Ensure that you are in the correct ADOM.
- 2. Go to *FortiSwitch Manager > FortiSwitch Templates*, and select *FortiSwitch Templates* in the tree menu.

+ Create New Edit Delete Import Column Settings	
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:

Create New	Create a new FortiSwitch template. See Creating FortiSwitch templates on page 457 .
Edit	Edit the selected template.
Delete	Delete the selected template or templates.

Import	Import a FortiSwitch template. See Importing FortiSwitch templates on page 459 .
Column Settings	Adjust the visible columns.
Search	Enter a search string into the search field to search the template list.

To edit a template:

1. Double-click a template name.
Alternately you can right-click a template, and click *Edit* in the toolbar.
The *Edit FortiSwitch Template* pane opens.
2. Edit the settings as required.
3. Click *OK* to apply your changes.

To delete templates:

1. Select the template or templates that will be deleted.
2. Either click *Delete* from the toolbar, or right-click and select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the selected template or templates.

Creating FortiSwitch templates

When creating a new FortiSwitch template, the platform must be selected before configuring VLAN assignments.

To create a FortiSwitch template:

1. Go to *FortiSwitch Manager > FortiSwitch Templates*.
2. In the tree menu, select *FortiSwitch Templates*.
3. In the content pane, click *Create New* in the toolbar. The *Create New FortiSwitch Template* window opens.

4. Enter the following information, then click *OK* to create the new template.

Template Name	Type a name for the template.
Comments	Optionally, enter comments.
Platforms	Select the platform that the template will apply to from the dropdown list.

Switch VLAN Assignments	Configure VLAN assignments. A platform must be selected before VLAN assignments can be configured.
Add Port	Add a port to the table.
Create Trunk	Create a trunk. See To create a trunk group: on page 458 .
Edit	Edit the selected trunk.
Delete	Delete the selected ports or trunks.
Port	Select a port profile from the dropdown list.
Native VLAN	Select the native VLAN from the available VLAN objects. See Creating FortiSwitch VLANs on page 459 .
Allowed VLAN	Select the allowed VLAN from the available VLAN objects. See Creating FortiSwitch VLANs on page 459 .
Security Policy	Select the security policies from the available switch controller security policies. See FortiSwitch security policies on page 465 .
POE	If applicable, right-click to enable or disable PoE for the port.
DHCP Blocking	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.
IGMP Snooping	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.
Loop Guard	Right-click to enable or disable Loop Guard for the port. Loop Guard cannot be applied to trunks, or ports that are in trunks.
STP	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.
Edge Port	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.
STP BPDU Guard	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.
STP Root Guard	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.

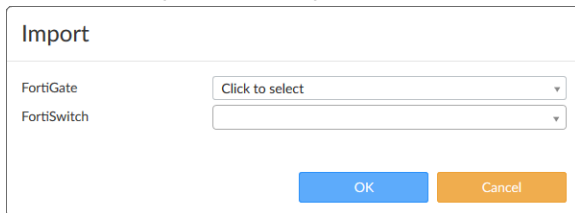
3. In the *Members* field, select all the ports that will be in the group from the drop-down list.
4. Select the mode: *lacp-active* (active link aggregation), *lacp-passive* (passive link aggregation), or *static*.
5. Click *OK* to create the trunk group.

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. Go to *FortiSwitch Manager > FortiSwitch Templates*.
2. In the tree menu, select *FortiSwitch Templates*.
3. In the content pane, click *Import* in the toolbar. The *Import* window opens.



4. Select a FortiGate from the drop-down list.
5. Select the FortiSwitch whose template will be imported from the drop-down list.
6. (Optional) Enter a name for the template in the *New Name* field.
7. Click *OK*.
The template is imported from the device.

Creating FortiSwitch VLANs

To create a FortiSwitch VLAN:

1. Go to *FortiSwitch Manager > FortiSwitch Templates*.
2. In the tree menu, select *VLANs*.

3. In the content pane, click *Create New* in the toolbar. The *Create New VLAN Definition* window opens.

Create New VLAN Definition

Interface Name

VLAN ID

0

Role

DMZ LAN UNDEFINED WAN

Estimated Bandwidth

0 Kbps Upstream 0 Kbps Downstream

Address

Manual

0.0.0.0/0.0.0.0

IPv6 Addressing mode

Manual DHCP

IPv6 Address/Prefix

::/0

Restrict Access

Administrative Access

☐ CAPWAP
☐ DNP
☐ FGFM

☐ FTM
☐ HTTP
☐ HTTPS

☐ PING
☐ PROBE-RESPONSE
☐ RADIUS-ACCT

☐ SNMP
☐ SSH
☐ TELNET

IPv6 Administrative Access

☐ CAPWAP
☐ FGFM
☐ HTTP

☐ HTTPS
☐ PING
☐ SNMP

☐ SSH
☐ TELNET

DHCP Server

ON

Address Range

+ Create Edit Delete

Starting IP

End IP

No records found...

Netmask

0.0.0.0

Default Gateway

Same as Interface IP Specify 0.0.0.0

DNS Server

Same as System DNS Same as Interface IP Specify

Advanced...

Mode

Server Relay

NTP Server

Local Same as System NTP Specify 0.0.0.0

Time Zone

Disable Same as System Specify

Next Bootstrap Server

0.0.0.0

Additional DHCP Options

Lease Time

604800

+ Create Edit Delete

Option Code

Value

No records found...

MAC Reservation + Access Control

Unknown MAC Address Action

assign block

+ Create Edit Delete

MAC Address

Action or IP

Description

No records found...

Type

Regular IPsec

Networked Devices

Device Detection

OFF

Admission Control

Security Mode

CAPTIVE-PORTAL NONE

Authentication Portal

Local External example.com/captive

User Access

Restricted to Groups Allow all

Exempt Sources

Device

Exempt Destinations

Exempt Services

Miscellaneous

Scan Outgoing Connections to Botnet Sites

BLOCK DISABLE MONITOR

Secondary IP Address

ON

+ Create New Edit Delete

IP/Network Mask

Administrative Access

Status

Comments

0/255

Interface State

Enabled Disabled

Advanced Options

Per-Device Mapping

ON

+ Create New Edit Delete

Name

VDOM

Details

OK

Cancel

FortiManager 6.4.2 Administration Guide
Fortinet Inc.

460

4. Enter the following information, then click **OK** to add the new VLAN.

Interface Name	Enter a name for the interface.
VLAN ID	Enter the VLAN ID
Role	Select the role for the interface: <i>DMZ</i> , <i>LAN</i> , <i>UNDEFINED</i> , or <i>WAN</i> .
Estimated Bandwidth	Enter the estimated upstream and downstream bandwidths. This option is only available when <i>Role</i> is <i>WAN</i> .
Address	
Addressing mode	The addressing mode.
IP/Network Mask	Enter the IP address and netmask.
IPv6 Addressing mode	Select the IPv6 addressing mode: <i>Manual</i> or <i>DHCP</i> .
IPv6 Address/Prefix	Enter the IPv6 address. This option is only available when <i>IPv6 Addressing mode</i> is <i>Manual</i> .
Restrict Access	
Administrative Access	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> .
IPv6 Administrative Access	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> .
DHCP Server	Turn the DHCP server on or off. This option is only available when <i>Role</i> is <i>LAN</i> or <i>UNDEFINED</i> .
DHCP Server IP	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> .
Address Range	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> .
Netmask	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> .
Default Gateway	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> .

DNS Server	<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>
DNS Server 1 - 3	<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>
Mode	<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>
NTP Server	<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>
Time Zone	<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>
Next Bootstrap Server	<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>
Additional DHCP Options	<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 To add additional DHCP options: on page 464 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>
MAC Reservation + Access Control	<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 To add a MAC address reservation: on page 464 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>
Type	<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>
Networked Devices	<p>These options are only available when <i>Role</i> is <i>DMZ</i>, <i>LAN</i>, or <i>UNDEFINED</i>.</p>
Device Detection	<p>Turn device detection on or off.</p>
Active Scanning	<p>Turn active scanning on or off.</p>

	This option is only available when <i>Device Detection</i> is on.
Admission Control	These options are only available when <i>Role</i> is <i>LAN</i> or <i>UNDEFINED</i> .
Security Mode	Select the security mode: <i>CAPTIVE-PORTAL</i> , or <i>NONE</i> .
Authentication Portal	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> .
User Access	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> .
User Groups	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> .
Exempt Sources	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> .
Device	Select user devices, device categories, and/or device groups. This option is only available when <i>Security Mode</i> is <i>CAPTIVE-PORTAL</i> .
Exempt Destinations	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> .
Exempt Services	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> .
Miscellaneous	
Scan Outgoing Connections to Botnet Sites	Select <i>Block</i> , <i>Disable</i> , or <i>Monitor</i> .
Secondary IP Address	Turn secondary IP addresses on or off. Add IP addresses to the table. See To add a secondary IP address: on page 464 for details. Addresses can also be edited and deleted as required.
Status	
Comments	Optionally, enter comments.
Interface State	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 465](#) 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:

1. Ensure that you are in the correct ADOM.
2. Go to *FortiSwitch Manager > FortiSwitch Templates*.
3. In the tree menu, select *Security Policies*.



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 Creating FortiSwitch security policies on page 466 .
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. Go to *FortiSwitch Manager > FortiSwitch Templates*.
2. In the tree menu, select *Security Policies*.
3. In the content pane, click *Create New* in the toolbar. The *Create New Security Policies* window opens.

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

Name	Type a name for the template.
Security mode	Select the security mode, <i>Port-based</i> or <i>MAC-based</i> .

User groups	Select the user groups that the security policy will apply to.
Guest VLAN	Enable a guest VLAN, and select the VLAN from the available VLAN objects. See Creating FortiSwitch VLANs on page 459 .
Guest authentication delay	Set the guest authentication delay, in seconds (1 - 900, default = 30).
Authentication fail VLAN	Enable an authentication failure VLAN, and select the VLAN from the available VLAN objects. See Creating FortiSwitch VLANs on page 459 . This option is not available when <i>Security mode</i> is <i>MAC-based</i> .
MAC authentication bypass	Enable MAC Authentication Bypass (MAB).
EAP pass-through	Enable EAP pass-through.
Override RADIUS timeout	Enable overriding the RADIUS timeout.

Assigning templates to FortiSwitch devices

When central management is enabled for *FortiSwitch Manager*, you can assign templates to switches. For more information about creating and managing FortiSwitch templates, see [FortiSwitch Templates on page 456](#).

To assign a templates:

1. Go to *FortiSwitch Manager > Managed Switches*.
2. In the tree menu, select a FortiGate to list its managed switches, or select *All_FortiGate* to list all switches. The list of managed FortiSwitch units is displayed in the content pane.
3. Use the quick status bar to filter the list of switches in the content pane and help locate the switch.
4. Select the switch, and click *Assign Template* from the toolbar.
5. Select a FortiSwitch template from the dropdown list, then click *OK* to assign it.
6. Install the changes. See [Installing changes to managed switches on page 449](#).



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 446](#).

FortiSwitch Profiles for per-device management

When per-device management is enabled, you can configure changes on each managed switch. The following steps provide an overview of using per-device FortiSwitch management:

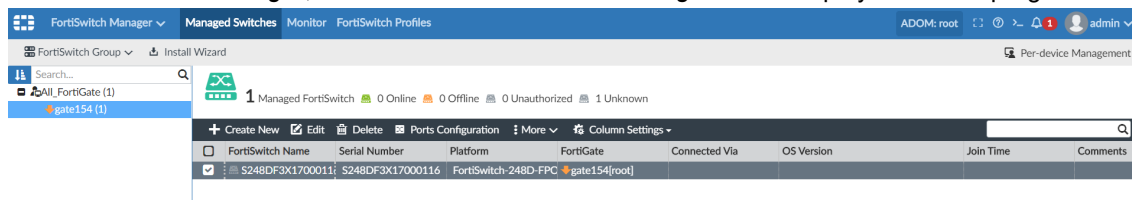
1. Enable per-device management. See [Enabling per-device management on page 468](#).
2. Configure policies and profiles for managed switches.
You can configure VLANs, NAC policies, security policies, LLDP profiles, and QoS policies, and the changes are saved to the FortiGate database. See [FortiSwitch profiles on page 468](#).
3. Configure ports for each managed switch.
When you configure ports, you can assign the profiles and policies that you created. See [Configuring a port on a single FortiSwitch on page 473](#).
4. Install changes to managed switches. See [Installing changes to managed switches on page 449](#).

Enabling per-device management

When per-device management is enabled, you can configure changes on each managed switch.

To enable FortiSwitch per-device management:

1. Go to *System Settings > All ADOMs*.
2. Double-click the ADOM to open it for editing.
3. Beside *Central Management*, clear the *FortiSwitch* checkbox, and click *OK*.
Central management is disabled, and per-device management is enabled for FortiSwitch.
4. Go to *FortiSwitch Manager*, and notice that *Per-device Management* is displayed in the top-right corner.



FortiSwitch profiles

The *FortiSwitch Manager > FortiSwitch Profiles* tab is available when per-device management is enabled for FortiSwitch Manager. You can use the *FortiSwitch Profiles* tab to create and manage VLANs, NAC policies, security policies, LLDP profiles, and QoS profiles that you can assign to individual switches.

Creating VLANs

To create VLANs:

1. Go to *FortiSwitch Manager > FortiSwitch Profiles*.
2. In the tree menu, select a FortiGate.
The *VLANs* tab is displayed.

VLANs	NAC Policies	Security Policies	LLDP Profiles	QoS	CLI Configurations			
<div>+ Create New Edit Delete Where Used Column Settings</div>								
<input type="checkbox"/>	Name	Alias	VLAN ID	IP/Netmask	Access	IPv6 IP/Netmask	IPv6 Access	Last N
▼ FortiLink Interface (1)								
<input type="checkbox"/>	fortilink		0	169.254.1.1/255.255.255.255	PING, Security Fabric Co	::/0		admin
▼ VLANs (6)								
<input type="checkbox"/>	default		1	0.0.0.0/0.0.0.0		::/0		admin
<input type="checkbox"/>	quarantine		4093	169.254.11.1/255.255.255.255		::/0		admin
<input type="checkbox"/>	voice		4091	169.254.12.1/255.255.255.255		::/0		admin
<input type="checkbox"/>	video		4090	169.254.13.1/255.255.255.255		::/0		admin
<input type="checkbox"/>	rspan		4092	169.254.14.1/255.255.255.255		::/0		admin
<input type="checkbox"/>	onboarding		4089	169.254.15.1/255.255.255.255		::/0		admin

- Click *Create New*.
- The *Create New VLAN Definition* pane opens.
- Edit the options, and click *OK*.
The changes are saved to the FortiGate database.

Creating NAC policies

To create NAC policies:

- Go to *FortiSwitch Manager > FortiSwitch Profiles*.
- In the tree menu, select a FortiGate.
The *VLANs* tab is displayed.
- Click the *NAC Policies* tab.
The NAC policies are displayed.

VLANs	NAC Policies	Security Policies	LLDP Profiles	QoS	CLI Configurations
<div> + Create New + Edit + Delete Where Used Column Settings </div>					
Name	Patterns	Action	Description	Matched Devices	
No record found.					

- Click *Create New*.
The *Create New NAC Policies* pane opens.
- Set the options, and click *OK*.
The changes are saved to the FortiGate database.

Creating security policies

To create security policies:

- Go to *FortiSwitch Manager > FortiSwitch Profiles*.
- In the tree menu, select a FortiGate.
The *VLAN* tab is displayed.
- Click the *Security Policies* tab.
The security policies are displayed.

VLANs	NAC Policies	Security Policies	LLDP Profiles	QoS	CLI Configurations
<div> + Create New + Edit + Delete Where Used Column Settings </div>					
Name	User Groups	Last Modified	Created Time		
802-1X-policy-default	SSO_Guest_Users	admin/2020-06-12 11:36:35	2020-06-12 11:36:35		

- Click *Create New*.
The *Create New Security Policies* pane opens.
- Edit the options, and click *OK*.
The changes are saved to the FortiGate database.

Creating LLDP profiles

To create LLDP profiles:

1. Go to *FortiSwitch Manager > FortiSwitch Profiles*.
2. In the tree menu, select a FortiGate.
The *VLAN* tab is displayed.
3. Click the *LLDP Profiles* tab.
The *LLDP profiles* are displayed.

VLANs NAC Policies Security Policies LLDP Profiles QoS CLI Configurations			
+ Create New Edit Delete Where Used Column Settings			
<input type="checkbox"/> Name	Last Modified		Created Time
<input type="checkbox"/> default	admin/2020-06-12 11:36:35		2020-06-12 11:36:35
<input type="checkbox"/> default-auto-isl	admin/2020-06-12 11:36:35		2020-06-12 11:36:35
<input type="checkbox"/> default-auto-mclag-icl	admin/2020-06-12 11:36:35		2020-06-12 11:36:35
<input type="checkbox"/> fortivoice.fortilink	admin/2020-06-12 11:36:35		2020-06-12 11:36:35

4. Click *Create New*.
The *Create New FortiSwitch LLDP Profiles* pane opens.

Create New FortiSwitch LLDP Profiles

Name

Transmitted LLDP-MED TLVs

☐ inventory-management ☐ location-identification
☐ network-policy ☐ power-management

Transmitted IEEE 802.1 TLVs

☐ port-vlan-id

Transmitted IEEE 802.3 TLVs

☐ max-frame-size

Auto inter-switch LAG

☒ ON

Auto isl hello timer duration

3

Auto isl port group ID

0

Auto isl receive timeout

60

Custom TLV Entry

[+ Create New](#) [Edit](#) [Delete](#) [Column Settings](#)

<input type="checkbox"/> #	Name	OUI (3 hex bytes)	OUI Subtype	Information String
No record found.				

Create & Refresh

OK

Cancel

5. Edit the options, and click *OK*.
The changes are saved to the FortiGate database.

Creating QoS policies

You can set the following types of QoS policies for each managed switch:

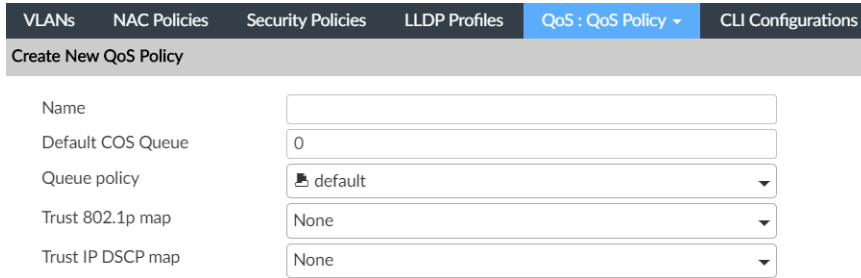
- QoS policies
- QoS egress queue policies
- QoS IP precedence/DSCP policies
- QoS 802.1 policies

To create QoS policies:

1. Go to *FortiSwitch Manager > FortiSwitch Profiles*.
2. In the tree menu, select a FortiGate.
3. From the *QoS* menu, select *QoS policy*.
The QoS policies are displayed in the content pane.

4. Click *Create New*.

The *Create New QoS Policy* pane opens.



5. Set the options, and click *OK*.

The changes are saved to the FortiGate database.

To create QoS egress queue policies:

1. Go to *FortiSwitch Manager > FortiSwitch Profiles*.

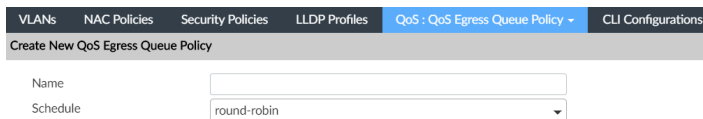
2. In the tree menu, select a FortiGate.

3. From the QoS menu, select *QoS Egress Queue Policy*.

The QoS egress queued policies are displayed in the content pane.

4. Click *Create New*.

The *Create New Egress Queue Policy* pane opens.



5. Set the options, and click *OK*.

The changes are saved to the FortiGate database.

To create QoS IP precedence/DSCP policies:

1. Go to *FortiSwitch Manager > FortiSwitch Profiles*.

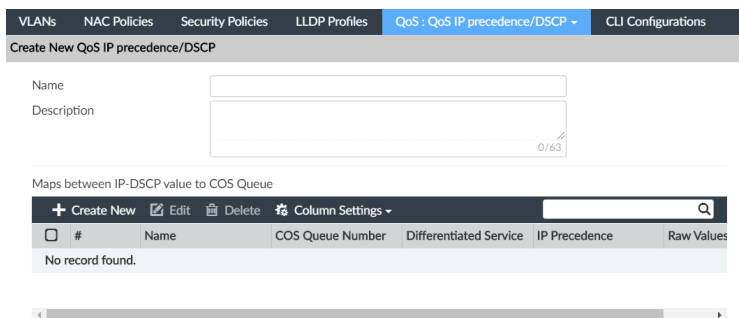
2. In the tree menu, select a FortiGate.

3. From the QoS menu, select *QoS IP precedence/DSCP*.

The QoS IP precedence/DSCP policies are displayed in the content pane.

4. Click *Create New*.

The *Create New QoS IP precedence/DSCP* pane opens.



- Set the options, and click *OK*.
The changes are saved to the FortiGate database.

To create QoS 802.1p policies:

- Go to *FortiSwitch Manager > FortiSwitch Profiles*.
- In the tree menu, select a FortiGate.
- From the QoS menu, select *QoS 802.1p*.
The *QoS 802.1p* policies are displayed in the content pane.
- Click *Create New*.
The *Create New 802.1* pane opens.

QoS : QoS 802.1p

Create New QoS 802.1p

Name

Description

COS queue mapped to dot1p priority number

Priority-0	queue-0
Priority-1	queue-0
Priority-2	queue-0
Priority-3	queue-0
Priority-4	queue-0
Priority-5	queue-0
Priority-6	queue-0
Priority-7	queue-0

- Set the options, and click *OK*.
The changes are saved to the FortiGate database.

Using the CLI

You can use the CLI for per-device configuration to access settings that might not yet be available in the GUI.

To use the CLI:

- Go to *FortiSwitch Manager > FortiSwitch Profiles*.
- In the tree menu, select a FortiGate.
The *VLAN* tab is displayed.
- Click the *CLI Configurations* tab.
The commands are displayed in the content pane.
- Use the tree menu to navigate between the commands.
The options display in the content pane.

The screenshot shows the FortiSwitch Manager interface with the 'CLI Configurations' tab selected. The left sidebar shows a tree view with 'switch-controller' expanded, and '802-1X-settings' selected. The main panel displays the configuration for 'switch-controller 802-1X-settings' with the following fields:

- link-down-auth: set-unauth (dropdown)
- max-reauth-attempt: 3 (text input, range: 0 - 15, default: 3)
- reauth-period: 60 (text input, range: 0 - 1440, default: 60)
- tx-period: 30 (text input, range: 4 - 60, default: 30)

- Set the options, and click *Apply*.
The changes are saved to the FortiGate database.

Configuring a port on a single FortiSwitch

When per-device management is enabled, you can use the *FortiSwitch Manager* pane to configure ports for each managed switch.

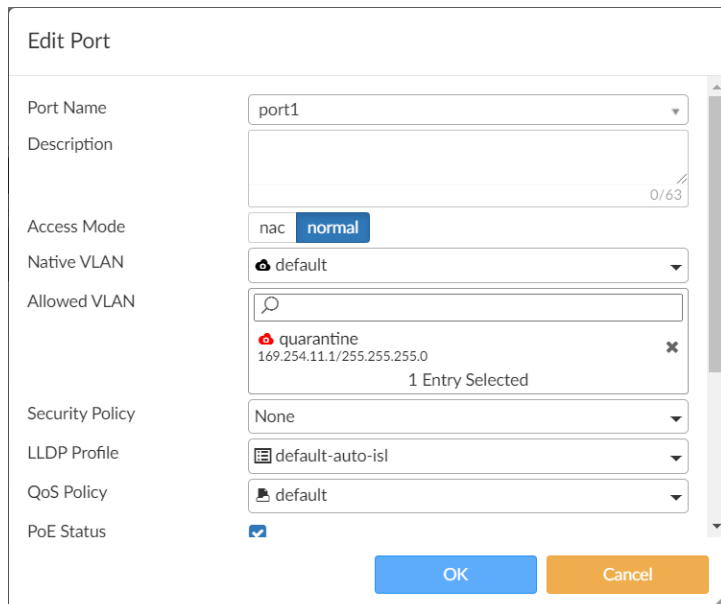
To configure ports on a managed FortiSwitch:

- Go to *FortiSwitch Manager > Managed Switches*.
- In the tree menu, select a FortiGate.
The list of managed switches is displayed in the content pane.
- Double-click a switch.
The *FortiSwitch Ports* pane opens.

The screenshot shows the 'FortiSwitch Ports' configuration pane. At the top, there is a header bar with 'MGMT' and 'PoE+' tabs. Below the header, there is a grid of port numbers (1-52) and a search bar. The main table lists the ports and their configurations:

Port	Description	Access Mode	Enabled Features	Native VLAN	Allowed VLAN	POE	Device Information	DHCP
port1		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		
port2		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		
port3		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		
port4		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		
port5		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		
port6		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		
port7		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		
port8		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		
port9		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Enabled		

4. Double-click a port to open it for editing.
The *Edit Port* dialog box is displayed.



5. Edit the options, and click *OK*.
The changes are saved to the FortiGate database.



Right-click each port to modify POE, DHCP Blocking, IGMP Snooping, IGMP Snooping, STP, Loop Guard, Edge Port, STP BPDU Guard, and STP Root Guard directly from the context-menu.

Endpoint Compliance



The *FortiClient Manager* pane is available for ADOM versions 6.0 and earlier, and you must enable the module by using the CLI. The *FortiClient Manager* pane is not available for ADOM versions 6.2 and later because FortiClient endpoints no longer send FortiTelemetry to FortiGate devices.

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.

The FortiClient Manager pane is available for ADOM version 6.0 and earlier, and you must enable the module by using the CLI.

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:

FortiTelemetry	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.
Monitor	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.
FortiClient profiles	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 enable FortiClient Manager:

1. Ensure that you are using ADOM version 6.0 or earlier.
2. Enable *FortiClient Manager* by using the CLI:

```
config system admin setting
(setting)# set show-fct-manager enable
(setting)# end
```

To create and assign FortiClient profile packages:

1. Create a FortiClient profile package. See [Creating FortiClient profile packages on page 483](#).
2. Select the profile package, and create one or more FortiClient profiles. See [Creating FortiClient profiles on page 483](#).
3. Enable FortiTelemetry on FortiGate interfaces. See [Enabling FortiTelemetry on interfaces on page 478](#).
4. Enable FortiClient enforcement on FortiGate interfaces. See [Enabling endpoint control on interfaces on page 478](#).
5. Assign profile packages to FortiGate interfaces. See [Assigning profile packages on page 487](#).

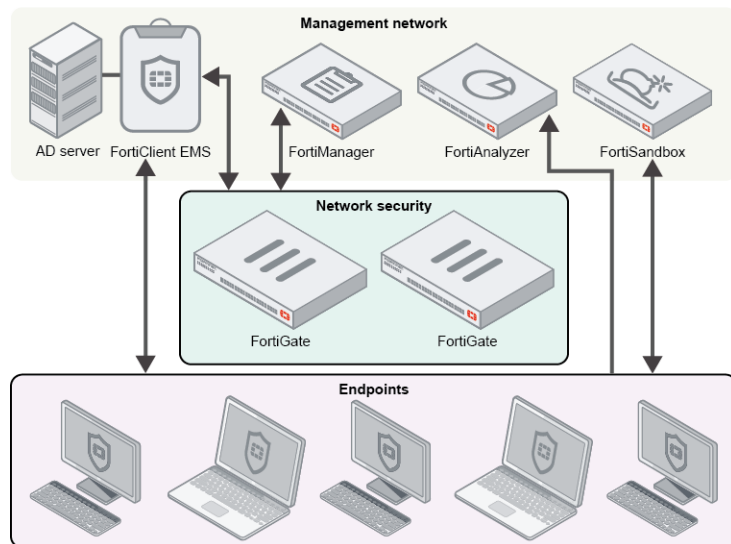
To install configuration changes to devices:

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 74](#).

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 74](#).

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:

Add Interface	Click to enable FortiTelemetry on interfaces for the selected device to use for FortiClient communication.
Remove Interface	Click to disable FortiTelemetry on the selected interface.
Assign Profile	Click to assign a FortiClient profile package to the FortiGate.

The following information is displayed in the content pane for the selected device:

Virtual Domain	Displays the name of the virtual domain for the selected FortiGate device if applicable.
Interface	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.
IP	Displays the IP address for the interface.
Enforce FortiClient	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.
Profile Package	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:

Refresh	Click to refresh the list of FortiClient endpoints for the selected device.
Action	Click to select one of the following actions for the selected FortiClient endpoint: <ul style="list-style-type: none"> • Block • Unblock • Quarantine • Release Quarantine • Unregister
Column Settings	Click to select which columns to display or select <i>Reset to Default</i> to display the default columns.
By Interface	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.

By Compliance Status	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:

Device	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.
User	Displays the name of the user logged into the FortiClient endpoint.
IP address	Displays the IP address of the FortiClient endpoint.
Status	Displays one of the following statuses for the FortiClient endpoint: <ul style="list-style-type: none"> • Online • Offline • Registered-Online • Registered-Offline • Un-Registered
FortiClient Version	Displays the version of FortiClient software installed on the FortiClient endpoint.
FortiClient Profile	Displays the name of the FortiClient profile that is assigned to the FortiClient endpoint.
Compliance	Displays one of the following icons of compliance statuses for the FortiClient endpoint: <ul style="list-style-type: none"> • Compliant • Endpoint is not compliant with FortiClient profile • Quarantined • FortiTelemetry is disabled • Exempt <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:

Profile Package	In the <i>Profile Package</i> menu, you can select to create, rename, or delete a FortiClient profile package.
Assign Profile Package	Assigns the selected FortiClient profile package to a device.
Install Wizard	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:

Create New	Click to create a new FortiClient profile package.
Rename	Click to rename the selected profile package.
Delete	Click to delete the selected profile package and all of its profiles.

The following information is displayed in the content pane:

Package Name	Displays the name of the profile package.
Device Targets	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:

Create New	Click to create a new FortiClient profile for the selected FortiClient profile package.
Edit	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.
Delete	Select a profile, and click <i>Delete</i> to delete the profile from the selected FortiClient profile package. Alternately, right-click a profile, and select <i>Delete</i> .
Move	Change the order of the profiles.
Import	Select to import a FortiClient profile from an existing device or VDOM into the selected FortiClient profile package.
Column Settings	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:

Seq.#	Displays the sequence number of the FortiClient profile.
FortiClient Profile	Displays the name of the FortiClient profile for the selected FortiClient profile package.

Assign To	Displays the device groups, user groups, and users associated with the FortiClient profile.
Comments	Displays any comments about the FortiClient profile.
Non-Compliance Action	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> .
Last Modified	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.

4. Enter the following information:

Profile Name	Type a name for the new FortiClient profile. When creating a new FortiClient profile, XSS vulnerability characters are not allowed.
Comments	(Optional) Type a profile description.
Assign Profile To	Identify where to assign the profile: <ul style="list-style-type: none"> • <i>Device Groups</i>: Select device groups from the list. • <i>User Groups</i>: Select user groups from the list. • <i>Users</i>: Select users from the list. • <i>Address</i>: Select addresses from the list. You can assign the profile to user groups and users when using Active Directory authentication or RADIUS authentication for VPN.
On-Net Detection By Address	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*:

Endpoint Vulnerability Scan on Client	Toggle <i>ON</i> to add a rule about <i>Vulnerability Scanning on Client</i> . When toggled <i>ON</i> , the Vulnerability Scanning module must be enabled in FortiClient on endpoints. Toggle <i>OFF</i> to exclude <i>Vulnerability Scanning on Client</i> from the compliance rules.
Non-compliance action	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.
Vulnerability quarantine level	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*:

System compliance	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.
Minimum FortiClient Version	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.
Windows endpoints	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.
Mac endpoints	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.
Upload logs to FortiAnalyzer	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"> • Traffic • Vulnerability • Event Toggle <i>OFF</i> to remove a rule about logging from the compliance rules.
Non-compliance action	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*:

Security Posture Check	<p>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.</p> <p>Toggle <i>OFF</i> to remove rules about <i>Security Posture Check</i> from the compliance rules.</p>
Real-time Protection	<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>
Up-to-date signatures	<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>
Scan with FortiSandbox	<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>Note: A FortiSandbox devices 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>
Third party AntiVirus on Windows	<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>Note: <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>
Web Filter	<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>
Profile	<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>
Application Firewall	<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>
Application Control Sensor	<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>

Non-compliance action

Specify how to handle endpoints that fail to meet the compliance rules for *Security Posture Check*. Select *Block* to block not-compliant endpoints from network access. Select *Warning* to warn not-compliant endpoints, but allow network access.

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:

Import From Device	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.
Profile	Select the profile to import.
New Name	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 63](#) 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 36](#).

- Enable and configure the FortiManager system's built-in FDS. For more information, see [Configuring network interfaces on page 542](#).
- 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 494](#).
- 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 37](#).

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>.

FDN third-party SSL validation and Anycast support

You can enable Anycast to optimize the routing performance to FortiGuard servers. Relying on Fortinet DNS servers, FortiManager obtains a single IP address for the domain name of each FortiGuard service. BGP routing optimization is transparent to FortiManager. The domain name of each FortiGuard service is the common name in that service's certificate. The certificate is signed by a third-party intermediate CA. The FortiGuard server uses the Online Certificate Status Protocol (OCSP) stapling technique, enabling FortiManager to always validate the FortiGuard server certificate efficiently.

When Anycast is enabled, FortiManager only completes the TLS handshake with a FortiGuard server that provides a *good* OCSP status for its certificate. Any other status will result in a failed SSL connection. OCSP stapling is reflected on the signature interval (currently, 24 hours), and good means that the certificate is not revoked at that timestamp. The FortiGuard servers query the CA's OCSP responder every four hours and update its OCSP status. If the FortiGuard server is unable to reach the OCSP responder, it keeps the last known OCSP status for seven days. This cached OCSP status is immediately sent out when a client connection request is made, which optimizes the response time.

To enable Anycast support:

1. Enable Anycast support

```
config fmupdate fds-setting
(fds-setting)# set fortiguard-anycast enable
(fds-setting)# end
```

2. (Optional) Specify an authorized mirror server hosted by AWS for better performance.

```
config fmupdate fds-setting
(fds-setting)# set fortiguard-anycast-source {aws | fortinet}
(fds-setting)# end
```


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 494](#).

FortiGuard Server and Service Settings

Enable Communication with FortiGuard Server

ON

Communication with FortiGuard Server

☒ Global Servers
 ☐ Servers Located in US Only

Enable Antivirus and IPS Service

OFF

Enable Web Filter Service

OFF

Enable Email Filter Service

OFF

Server Override Mode

☐ Strict (Access Override Server Only)
 ☒ Loose (Allow Access Other Servers)

FortiGuard Antivirus and IPS Settings >

FortiGuard Web Filter and Email Filter Settings >

Override FortiGuard Server (Local FortiManager) >

Apply

Enable Communication with FortiGuard Server	When toggled <i>OFF</i> , you must manually upload packages, databases, and licenses to your FortiManager. See Operating as an FDS in a closed network on page 494 .
Communication with FortiGuard Server	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.
Enable Antivirus and IPS Service	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.
Enable Web Filter and Service	Toggle <i>ON</i> to enable web filter services. When uploaded to FortiManager, the Web Filter database version is displayed.
Enable Email Filter Service	Toggle <i>ON</i> to enable email filter services. When uploaded to FortiManager, the Email Filter databases versions are displayed.
Server Override Mode	Select <i>Strict (Access Override Server Only)</i> or <i>Loose (Allow Access Other Servers)</i> override mode.
FortiGuard Antivirus and IPS Settings	Configure antivirus and IPS settings. See FortiGuard antivirus and IPS settings on page 492 .
FortiGuard Web Filter and Email Filter Settings	Configure web and email filter settings. See FortiGuard web and email filter settings on page 492 .
Override FortiGuard Server (Local FortiManager)	Configure web and email filter settings. See Override FortiGuard server (Local FortiManager) on page 493 .

FortiGuard antivirus and IPS settings

In this section you can enable settings for FortiGuard Antivirus and IPS settings. The following settings are available:

Use Override Server Address for FortiClient	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the add icon to add additional override servers, up to a maximum of ten. Select the delete icon to remove entries. To override the default server for updating FortiClient device's FortiGuard services, see Overriding default IP addresses and ports on page 502 .
Use Override Server Address for FortiGate/FortiMail	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the add icon to add additional override servers, up to a maximum of ten. Select the delete icon to remove entries. To override the default server for updating FortiGate/FortiMail device's FortiGuard services, see Overriding default IP addresses and ports on page 502 .
Allow Push Update	Configure to allow urgent or critical updates to be pushed directly to the FortiManager system when they become available on the FDN. The FortiManager system immediately downloads these updates. To enable push updates, see Enabling push updates on page 500 .
Use Web Proxy	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 Enabling updates through a web proxy on page 501 .
Scheduled Regular Updates	Configure when packages are updated without manually initiating an update request. To schedule regular service updates, see Scheduling updates on page 502 .
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 <i>View FDS and FortiGuard Download History</i> .

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 Hour 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)	<p>Configure connections for overriding the default built-in FDS or web proxy server for web filter and email filter settings.</p> <p>To override an FDS server for web filter and email filter services, see Overriding default IP addresses and ports on page 502.</p> <p>To enable web filter and email filter service updates using a web proxy server, see Enabling updates through a web proxy on page 501.</p>
Use Override Server Address for FortiClient	<p>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.</p>
Use Override Server Address for FortiGate/FortiMail	<p>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.</p> <p>To override the default server for updating FortiGate device's FortiGuard services, see Overriding default IP addresses and ports on page 502.</p>
Use Web Proxy	<p>Configure the FortiManager system's built-in FDS to connect to the FDN through a web proxy. IPv4 and IPv6 are supported.</p> <p>To enable updates using a web proxy, see Enabling updates through a web proxy on page 501.</p>
Polling Frequency	<p>Configure how often polling is done.</p>
Log Settings	<p>Configure logging of FortiGuard server update, web filtering, email filter, and antivirus query events.</p> <ul style="list-style-type: none"> • <i>Log FortiGuard Server Update Events</i>: enable or disable • <i>FortiGuard Web Filtering</i>: Choose from <i>Log URL disabled</i>, <i>Log non-URL events</i>, and <i>Log all URL lookups</i>. • <i>FortiGuard Anti-spam</i>: Choose from <i>Log Spam disabled</i>, <i>Log non-spam events</i>, and <i>Log all Spam lookups</i>. • <i>FortiGuard Anti-virus Query</i>: Choose from <i>Log Virus disabled</i>, <i>Log non-virus events</i>, and <i>Log all Virus lookups</i>. <p>To configure logging of FortiGuard web filtering and email filtering events, see Logging FortiGuard web or email filter events on page 504.</p>

Override FortiGuard server (Local FortiManager)

Configure and enable alternate FortiManager FDS devices, rather than using the local FortiManager system. You can set up as many alternate FDS locations, and select what services are used. The following settings are available:

Additional number of Private FortiGuard Servers (Excluding This One)	<p>Select the add icon to add a private FortiGuard server. Select the delete icon to remove entries.</p> <p>When adding a private server, you must type its IP address and time zone.</p>
Enable Antivirus and IPS Update Service for Private Server	<p>When one or more private FortiGuard servers are configured, update antivirus and IPS through this private server instead of using the default FDN.</p> <p>This option is available only when a private server has been configured.</p>

Enable Web Filter and Email Filter Update Service for Private Server

When one or more private FortiGuard servers are configured, update the web filter and email filter through this private server instead of using the default FDN.
This option is available only when a private server has been configured.

Allow FortiGates to Access Public FortiGuard Servers When Private Servers Unavailable

When one or more private FortiGuard servers are configured, managed FortiGate units will go to those private servers for FortiGuard updates. Enable this feature to allow those FortiGate units to then try to access the public FDN servers if the private servers are unreachable.
This option is available only when a private server has been configured.



The FortiManager system's network interface settings can restrict which network interfaces provide FDN services. For more information, see [Configuring network interfaces on page 542](#).

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 500](#).
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 542](#).

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 496](#).

Go to *FortiGuard > Settings* to configure FortiManager as a local FDS server and to upload update packages and license.

FortiGuard Server and Service Settings

Enable Communication with FortiGuard Server

Enable Antivirus and IPS Service

FortiGate	<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

Enable Email Filter Service

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.

	<p>Click OK to upload the package to FortiManager.</p> <p>As the database can be large, uploading with the CLI is recommended. See Uploading packages with the CLI on page 496.</p>
Email Filter Database	<p>Select to upload the email filter database. Browse for the file you downloaded from the Customer Service & Support portal on your management computer.</p> <p>Click OK to upload the package to FortiManager.</p> <p>As the database can be large, uploading with the CLI is recommended. See Uploading packages with the CLI on page 496.</p>
Service License	<p>Select to import the FortiGate license. Browse for the file on your management computer, or drag and drop the file onto the dialog box.</p> <p>Click OK to upload the package to FortiManager.</p> <p>A license file can be obtained from support by requesting your account entitlement for the device. See Requesting account entitlement files on page 496.</p>
Upload Options for FortiClient	
AntiVirus/IPS Packages	<p>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.</p> <p>Click OK to upload the package to FortiManager.</p>

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 | dcomp> <remote_
    file> <ip> <port> <remote_path> <user> <password>
```

Requesting account entitlement files

When FortiManager is operating in a closed network, you can request account entitlement files from Fortinet Customer Service & Support for devices, and then upload the files to the *FortiGuard* module. This allows devices in the closed network to check licenses. See [Operating as an FDS in a closed network on page 494](#).

You can request an entitlement file from Fortinet Customer Service & Support by creating a support ticket.

To request account entitlement files:

1. Log in to the Fortinet Customer Service & Support site (<https://support.fortinet.com/>).
2. Go to *Assistance* > *Create a Ticket*.

The *Ticket Wizard* is displayed, starting at the *1 Request Type* page.

The screenshot shows the 'Ticket Wizard' interface. At the top, there's a navigation bar with 'Customer Service & Support', 'Home', 'Asset', 'Assistance' (highlighted), 'Download', 'Feedback', and '753 Fortinet'. Below this is a header for 'Ticket Wizard' with a 'Create Ticket' button. A progress bar shows four steps: 1 (selected), 2, 3, and 4. The main content area is titled 'Specify Request Ticket Type' and lists two options: 'Technical Support Ticket' and 'Customer Service'. The 'Customer Service' option is selected, and its description is visible: 'You can create customer service tickets for questions related to contracts and account management.'

3. In the *Specify Request Ticket Type* list, expand *Customer Service*, and click *Submit a Ticket*.

This screenshot shows the same 'Ticket Wizard' interface as the previous one, but with the 'Customer Service' option expanded. Under 'Customer Service', there are two sub-options: 'Submit Ticket' (with a plus icon) and 'Start Web Chat' (with a chat bubble icon). The 'Submit Ticket' option is highlighted.

The wizard moves to the *2 Basic Info* page, where you can specify ticket information.

4. On the *Specify Ticket Information* page, complete the following options, and click *Next*.
 - a. In the *Serial Number* box, add the serial number for the device for which you want an entitlement file.
 - b. In the *Subject* box, type *Entitlement file*.
 - c. In the *Category* list, select *CS Contract/License*.

Customer Service & Support Home Asset Assistance Download Feedback 753 Fortinet

Ticket Wizard CS Ticket Serial Number: N/A

1 Request Type > 2 Basic Info > 3 Comment > 4 Completion

Specify Ticket Information

Serial Number: ?

Contact Information

Name*:

Email*: ?

Telephone:

Mobile Phone:

Ticket Information

Subject*:

Category*:

The wizard moves to the 3 *Comment* page, where you can add a comment.

5. In the *Add Comment* box, request the entitlement file, and click *Next*.
The request is complete.
6. Monitor your email to receive the entitlement file, and download it to your computer.

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 542](#) 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 528](#).
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 501](#).

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 492](#).
3. Toggle **ON** beside *Allow Push Update*.
4. If there is a NAT device or firewall between the FortiManager system and the FDN which denies push packets to the FortiManager system's IP address on UDP port 9443, type the IP Address and/or Port number on the NAT device which will forward push packets to the FortiManager system. The FortiManager system will notify the FDN to send push updates to this IP address and port number.
 - *IP Address* is the external or virtual IP address on the NAT device for which you will configure a static NAT or port forwarding.
 - *Port* is the external port on the NAT device for which you will configure port forwarding.
5. Click *Apply*.
6. If you performed step 4, also configure the device to direct that IP address and/or port to the FortiManager system.
 - If you entered a virtual IP address, configure the virtual IP address and port forwarding, and use static NAT mapping.
 - If you entered a port number, configure port forwarding; the destination port must be UDP port 9443, the FortiManager system's listening port for updates.

To enable push through NAT in the CLI:

Enter the following commands:

```
config fmupdate fds-setting
  config push-override-to-client
    set status enable
  config announce-ip
    edit 1
      set ip <override IP that FortiGate uses to download updates from FortiManager>
      set port <port that FortiManager uses to send the update announcement>
    end
  end
end
```

Enabling updates through a web proxy

If the FortiManager system's built-in FDS must connect to the FDN through a web (HTTP or HTTPS) proxy, you can specify the IP address and port of the proxy server.

If the proxy requires authentication, you can also specify a user name and password.

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 494](#).

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 492](#).
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 antispy database on page 505](#).

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 492](#).
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*:

Log FortiGuard Server Update Events	Enable or disable logging of FortiGuard server update events.
FortiGuard Web Filtering	
Log URL disabled	Disable URL logging.
Log non-URL events	Logs only non-URL events.
Log all URL lookups	Logs all URL lookups (queries) sent to the FortiManager system's built-in FDS by FortiGate devices.
FortiGuard Anti-spam	
Log Spam disabled	Disable spam logging.
Log non-spam events	Logs email rated as non-spam.
Log all Spam lookups	Logs all spam lookups (queries) sent to the FortiManager system's built-in FDS by FortiGate devices.
FortiGuard Anti-virus Query	
Log Virus disabled	Disable virus logging.
Log non-virus events	Logs only non-virus events.
Log all Virus lookups	Logs all virus queries sent to the FortiManager system's built-in FDS by FortiGate devices.

Restoring the URL or antispam database

Formatting the hard disk or partition on FortiManager 3000 units and higher deletes the URL and antispam databases required to provide FortiGuard email filter and web filtering services through the built-in FDS. The databases will re-initialize when the built-in FDS is 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:

Refresh	Select the refresh icon to refresh the information displayed on this page.
----------------	--

Hide/Show license expired devices only	Toggle to hide and display devices with an expired license only.
Search	Use the search field to find a specific device in the table.
Device Name	The device name or host name. You can change the order that devices are listed by clicking the column title.
Serial Number	The device serial number
Platform	The device type, or platform.
ADOM	ADOM information. You can change the order that ADOMs are listed by clicking the column title.
Antivirus	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
IPS	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
Email Filtering	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
Web Filtering	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
Mobile Malware	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
Support	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:

Refresh	Select to refresh the table.
Show Used Object Only	Clear to show all package information. Select to show only relevant package information.
Search	Use the search field to find a specific object in the table.
Package Name	The name of the package downloaded from FortiGuard.
Product	What product the package is for.
Version	The version of the package if applicable.
Latest Version (Release Date/Time)	The package version.
Size	The size of the package.
To Be Deployed Version	The package version that is to be deployed. Select <i>Change</i> to change the version.
Update History	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:

Push Pending	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.
Push All Pending	Select <i>Push All Pending</i> in the toolbar to push pending updates to all of the devices in the list.
Refresh	Select to refresh the list.
By Package	Displays the service status information by installed package name.
By Device	Displays the service status information by device name.
Search	Use the search field to find a specific device or package in the table.

Service status by Device

When you click the *By Device* button in the toolbar, the *Service Status* page displays a list of all the managed FortiGate devices, their last update time, and their status.

You can pushing pending updates to the devices, either individually or all at the same time. You can refresh the list by clicking *Refresh* in the toolbar.

Device	The device serial number or host name is displayed.
Status	<p>The service update status. A device's status can be one of the following:</p> <ul style="list-style-type: none"> • <i>Up to Date</i>: The latest package has been received by the FortiGate unit. • <i>Never Updated</i>: The FortiGate unit has never requested or received the package. • <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. • <i>Problem</i>: The FortiGate unit missed the scheduled query, or did not correctly receive the latest package. • <i>Unknown</i>: The FortiGate unit's status is not currently known.
Last Update Time	The date and time of the last update.

Service status by Package

When you click the *By Package* button, the *Service Status* page shows a list of all the installed packages, the applicable firmware version, the package version, and the progress on package installation to devices. You can drill-down to view the installed device list.

The content pane displays the following information:

Installed Packages Name	The name of the installed package.
Applicable Firmware Version	The firmware version of the device for which the installed package is created.
Package Version	The version of the installed package.
Installed Devices	The package installation progress for the devices. Click the <i><number> of <number></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.

Device Name	The name of the device.
Current Version	The version of the package.

Status	The device update status.
Last Update Time	The time of the last package update.

4. Click the *Back* arrow to return to the previous page.

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:

Refresh	Select to refresh the table.
Search	Use the search field to find a specific entry in the table.
History	The record of received packages.
Package Received	The name of the received package.
Latest Version (Release Date/Time)	The latest version of the received package.
Size	The size of the package.
Update History	Click to view the package update history.

Update history

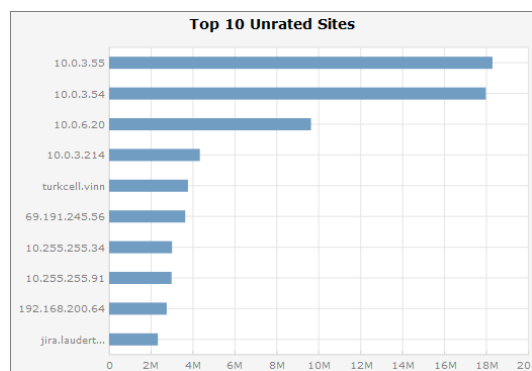
When you click the *Update History* button for a package, the *Update History* pane is displayed for the package.

It shows the update times, the events that occurred, the statuses of the updates, and the versions downloaded.

Query status

Go to *FortiGuard > Query Server Management > Query Status* to view graphs that show:

- The number of queries made from all managed devices to the FortiManager unit over a user selected time period
- The top ten unrated sites
- The top ten devices for a user selected time period



The following information is displayed:

Top 10 Unrated Sites	Displays the top 10 unrated sites and the number of events. Hover the cursor over a row to see the exact number of queries.
Top 10 Devices	Displays the top 10 devices and number of sessions. Hover the cursor over a row to see the exact number of queries. Click a row to see a graph of the queries for that device.
Number of Queries	Displays the number of queries over a period of time.

Firmware images

Go to *FortiGuard > Firmware Images* to manage the firmware images stored on the FortiManager device. You can import firmware images for FortiGate, FortiCarrier, FortiAnalyzer, FortiManager, FortiAP, FortiExtender, FortiSwitch, and FortiClient.

You can download only those images that are needed from the FDS systems, and customize which firmware images are available for deployment.

The following information and settings are available:

Import Images	Select to open the firmware image import list.
Models	From the dropdown list, select <i>All</i> to show all the available models on the FortiGuard server, or select <i>Managed</i> to show only the models that are currently being managed by the FortiManager device.
Product	Select a managed product type from the dropdown list.
Search	Use the search field to find a specific entry in the table.
Seq.#	The sequence number.
Model	The device model number that the firmware is applicable to.
Latest Version (Release Date/Time)	The latest version of the firmware that is available.

Preferred Version	The firmware version that you would like to use on the device. Click <i>Change</i> to open the <i>Change Version</i> dialog box, then select the desired version from the dropdown list and select <i>OK</i> to change the preferred version.
Size	The size of the firmware image.
Status	The status of the image, that is, from where it is available.
Action Status	The status of the current action being taken.
Release Notes	A link to a copy of the release for the firmware image that has been downloaded.
Download/Delete	Download the firmware image from the FDS if it is available. If the firmware images has already been downloaded, then delete the firmware image from the FortiManager device.

For information about upgrading your FortiManager device, see the [FortiManager Release Notes](#) or contact Fortinet Customer Service & Support.

To import a firmware image:

1. Go to *FortiGuard > Firmware Images*, and click *Import Images* in the toolbar.
2. Select a device in the list, and click *Import* in the toolbar. The *Firmware Upload* dialog box, opens.
3. Click *Browse* to browse to the desired firmware image file, or drag and drop the file onto the dialog box.
4. Click *OK* to import the firmware image.



Firmware images can be downloaded from the Fortinet Customer Service & Support site at <https://support.fortinet.com/> (support account required).

To delete firmware images:

1. Go to *FortiGuard > Firmware Images*, and click *Import Images* in the toolbar.
2. Select the firmware images you would like to delete.
3. Click *Delete* in the toolbar. A confirmation dialog box appears.
4. Click *OK* to delete the firmware images.

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 517](#).

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 554](#)).



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 119](#).

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 514](#) and [Locking a policy package on page 515](#).

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 554](#)).

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.

Lock an individual policy

In normal workspace mode, administrators can lock individual policies.

If you want to modify a policy, you don't need to lock the entire policy package. Once you lock a policy, a padlock icon appears beside the policy. Others are now unable to modify your policy or lock the policy package where the locked policy is in, and unable to lock the ADOM.



If you move your cursor to the padlock icon, you can see who locked the policy and the time at which it was locked.

To enable per policy lock:

Per policy lock can only be enabled via the CLI.

1. In the *CLI Console* widget enter the following CLI commands:

```
config system global
    set per-policy-lock enable
end
```

To lock a policy:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the policy package list, select the policy package, and right-click on the policy and select *Edit*. The *Edit IPv4 Policy* pane opens.
4. In the *Edit IPv4 Policy* pane, modify the name and then click *OK*.
A padlock icon in the locked state is shown next to the policy name to indicate that it is locked.
You can still lock the policy package or the whole ADOM with confirmation.
Other administrators are now unable to make changes to this policy or the policy package, and cannot lock the ADOM without first forcing you to disconnect.
5. Click *Save* in the toolbar to save your changes.



A green padlock icon next to the sequence number of the policy indicates that the current administrator locked the policy. A red padlock icon indicates that another administrator locked the policy.

Sequence lock:

If you add two or more policies, a sequence lock appears at the top. The sequence lock ensures that the order of the policies is managed by one administrator at any given time, other administrators see a red padlock icon at the top.

Once you save your changes, the sequence lock disappears allowing other administrators to change the order of the policies.



If an administrator sets up a sequence lock, other administrators can neither create a new policy nor insert a policy. They can however, edit an existing policy.

Workflow mode

Workflow mode is used to control the creation, configuration, and installation of policies and objects. It helps to ensure all changes are reviewed and approved before they are applied.

When workflow mode is enabled, the ADOM must be locked and a session must be started before policy or object changes can be made in an ADOM. Workflow approvals must be configured for an ADOM before any sessions can be started in it.

Once the required changes have been made, the session can either be discarded and the changes deleted, or it can be submitted for approval. The session can also be saved and continued later, but no new sessions can be created until the saved session has been submitted or discarded.

When a session is submitted for approval, email messages are sent to the approvers, who can then approve or reject the changes directly from the email message. Sessions can also be approved or rejected by the approvers from within the ADOM itself.



Sessions must be approved in the order they were created.

If one approver from each approval group approves the changes, then another email message is sent, and the changes are implemented. If any of the approvers reject the changes, then the session can be repaired and resubmitted as a new session, or discarded. When a session is discarded, all later sessions are also discarded. After multiple sessions have been approved, a previous session can be reverted to, undoing all the later sessions.

The changes made in a session can be viewed at any time from the session list in the ADOM by selecting *View Diff*. The ADOM does not have to be locked to view the differences.

Enable workflow mode

Workflow mode can 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 588](#), and each administrator must have a contact email address configured, see [Managing administrator accounts on page 599](#).



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

✖ TLeele

✖ PJFry

-

Approval Group # 2

✖ BBRodriguez

✖ HConrad

+ -

Send an Email Notification to

✖ admin

Mail Server

localMail

OK

Cancel

3. Configure the following settings:

ADOM	Select the ADOM from the dropdown list.
Approval Group	Select to add approvers to the approval group. Select the add icon to create a new approval group. Select the delete icon to remove an approval group. At least one approver from each group must approve the change for it to be adopted.
Send an Email Notification to	Select to add administrators to send email notifications to.
Mail Server	Select the mail server from the dropdown list. A mail server must already be configured. See Mail Server on page 588 .

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 518](#).

Starting a workflow session

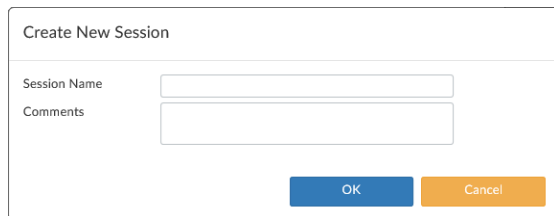
A workflow session must be started before changes can be made to the policies and objects. A session can be saved and continued at a later time, discarded, or submitted for approval.



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 524](#).
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 186](#).

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 520](#).
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	[Details]
FortiGate-VM64_CDOMm_1		admin	2018-02-21 08:41:08	changed	[Details]
FortiGate-VM64_root		admin	2018-02-21 08:40:12	changed	[Details]
Model1		admin	2018-02-21 08:39:39	changed	[Details]

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

Category	User	Update Time	Change Summary
system virtual-wire-pair	admin	2018-02-21 08:40:35	added (1)

[Download](#) [Close](#)

3. Select *Details* to view specific changes within a policy package or the policy objects.

Revision Diffs Between 1 and 2

Summary Policy Objects **FortiGate-VM64_CDOMm_1** **FortiGate-VM64_root**

firewall policy - added (1)

Seq.#	Policy ID	Name	From	To	Source	Destination	Schedule	Service	Action	Log	Status	Security Profiles	Policy Section	Install On	Others
Added 1	1	VpairO	"port1"	"port10"	"all"	"all"	"always"	"ALL"							

firewall multicast-policy - added (1)

Seq.#	Policy ID	Source Interface	Source	Destination Interface	Destination	Protocol	Source NAT	Destination NAT	Action	Log	Policy Section	Install On	Others
Added 1	1	"any"	"all"	"any"	"all"	0	1	0.0.0.0					

firewall local-in-policy - added (1)

Seq.#	Policy ID	Source	Destination	Service	Schedule	Interface	Action	Policy Section	Install On	Others
Added 1	1	"all"	"all"	"ALL"	"always"	"vpnmgmt_tet_spoke2hub"				

firewall DoS-policy - added (1)

Seq.#	Policy ID	Interface	Source	Destination	Service	Policy Section	Install On	Others
Added 1	1	"vpnmgmt_tet_mesh"	"test_local_subnet_1"	"test_local_subnet_2"	"AH"			

firewall shapine-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 518](#)), and the ADOM is automatically unlocked.

To submit a session for approval:

1. Select *Sessions > Submit*.
2. Enter the following in the *Submit for Approval* dialog box:

Comments	Enter a comment describing the changes that have been made in this session.
Attach configuration change details	Select to attach configuration change details to the email message.

3. Click *OK* to submit the session.

Approving or rejecting a session

Sessions can be approved or rejected by the members of the approval groups either directly from the email message that is generated when the session is submitted, or from the session list. 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 524](#).
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 524](#).
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 524](#).
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 524](#).
4. Select the session, then click *Revert*.

The session list

To view the session list, In *Policy & Objects*, go to *Sessions > Session List*. Different options will be available depending on the various states of the sessions (in progress, approved, etc.). When an ADOM is unlocked, only the comments and *View Diff* command are available.

Session List

☒ Approve
 ☒ Reject
 ☒ Discard
 ☒ View Diff

ID	Name	User	Date Submi...	Approved/...	Comments
<input type="checkbox"/> 3	Session-...	admin	2016-04-19...	0/1	It didn't wor...
<input checked="" type="checkbox"/> 2	Session-...	HConrad	2016-04-19...	0/1	bureaucrati...
<input type="checkbox"/> 1	Session-9	admin	2016-04-19...	0/1	This is a test...

+ Add Comment

[HConrad] - 2016-04-19 05:53:08
 bureaucratic stuff
 [HConrad] - 2016-04-19 12:52:46
 bureaucratic stuff

Continue Session In Progress
 Continue Without Session

The following options and information are available:

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.
View Diff	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.
ID	A unique number to identify the session.

Name	The user-defined name to identify the session. The icon shows the status of the session: waiting for approval, approved, rejected, repaired, or in progress. Hover the cursor over the icon to see a description.
User	The administrator who created the session.
Date Submitted	The date and time the session was submitted for approval.
Approved/...	The number of approval groups that have approved the session out of the number of groups that have to approve the session. Hover the cursor over the table cell to view the group members.
Comments	The comments for the session. All the comments are shown on the right of the dialog box for the selected session. Session approvers can also add comments to the selected session without having to approve or reject the session.
Create New Session	Select to create a new workflow session. This option is not available when a session has been saved or is already in progress.
Continue Session in Progress	Select to continue a session that was previously saved or is already in progress. This option is only available when a session is in progress or saved.
Continue Without Session	Select to continue without starting a new session. When a new session is not started, all policy and objects are read-only.

System Settings

System Settings allows you to manage system options for your FortiManager device.



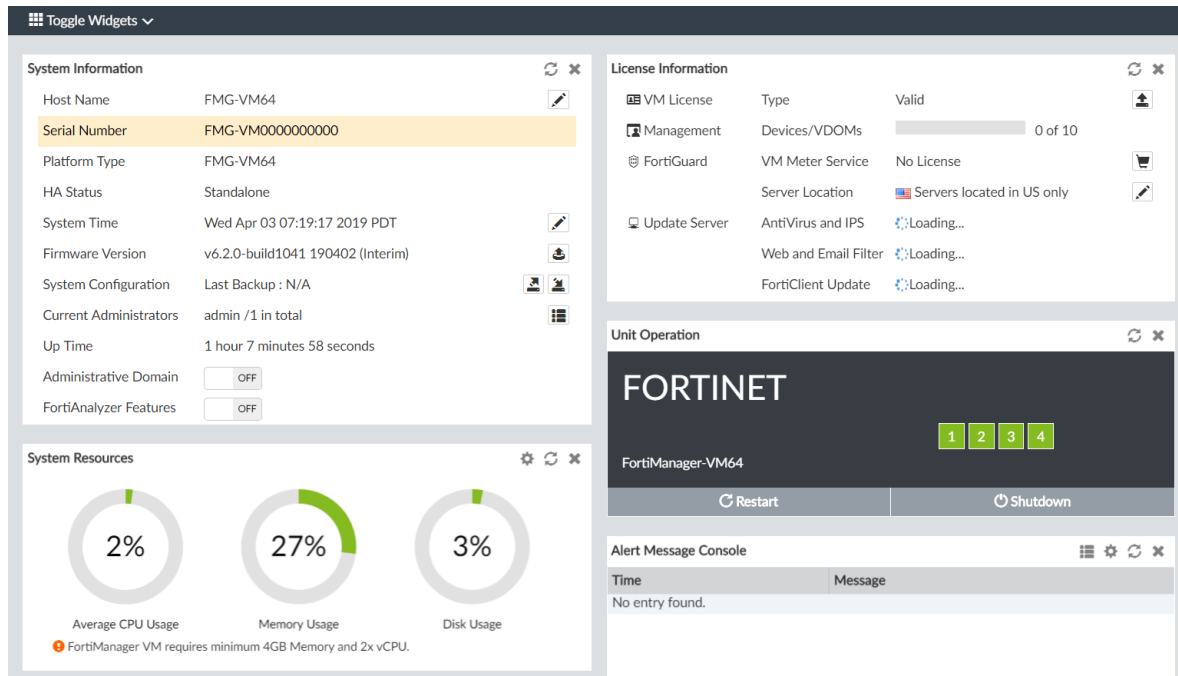
Additional configuration options and short-cuts are available using the right-click menu. Right-click the mouse on different navigation panes on the GUI page to access these options.

This section contains the following topics:

- [Dashboard on page 527](#)
- [Logging Topology on page 541](#)
- [Network on page 542](#)
- [RAID Management on page 546](#)
- [Administrative Domains on page 552](#)
- [Certificates on page 566](#)
- [Fetcher Management on page 571](#)
- [Event Log on page 576](#)
- [Task Monitor on page 578](#)
- [SNMP on page 580](#)
- [Mail Server on page 588](#)
- [Syslog Server on page 590](#)
- [Meta Fields on page 591](#)
- [Device logs on page 592](#)
- [File Management on page 596](#)
- [Advanced Settings on page 596](#)

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
System Information	<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 System Information widget on page 529.</p> <p>From this widget you can manually update the FortiManager firmware to a different release. For more information, see Updating the system firmware on page 531.</p> <p>The widget fields will vary based on how the FortiManager is configured, for example, if ADOMs are enabled.</p>
System Resources	<p>Displays the real-time and historical usage status of the CPU, memory and hard disk. For more information, see System Resources widget on page 535.</p>
License Information	<p>Displays the devices being managed by the FortiManager unit and the maximum numbers of devices allowed. For more information, see License Information widget on page 536.</p> <p>From this widget you can manually upload a license for VM systems.</p>

Widget	Description
Unit Operation	Displays status and connection information for the ports of the FortiManager unit. It also enables you to shutdown and restart the FortiManager unit or reformat a hard disk. For more information, see Unit Operation widget on page 538 .
Alert Message Console	Displays log-based alert messages for both the FortiManager unit and connected devices. For more information, see Alert Messages Console widget on page 538 .
Log Receive Monitor	Displays a real-time monitor of logs received. You can view data per device or per log type. For more information, see Log Receive Monitor widget on page 539 . The <i>Log Receive Monitor</i> widget is available when <i>FortiAnalyzer Features</i> is enabled.
Insert Rate vs Receive Rate	Displays the log insert and receive rates. For more information, see Insert Rate vs Receive Rate widget on page 539 . The <i>Insert Rate vs Receive Rate</i> widget is available when <i>FortiAnalyzer Features</i> is enabled.
Log Insert Lag Time	Displays how many seconds the database is behind in processing the logs. For more information, see Log Insert Lag Time widget on page 540 . The <i>Log Insert Lag Time</i> widget is available when <i>FortiAnalyzer Features</i> is enabled.
Receive Rate vs Forwarding Rate	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 Receive Rate vs Forwarding Rate widget on page 540 . The <i>Receive Rate vs Forwarding Rate</i> widget is available when <i>FortiAnalyzer Features</i> is enabled.
Disk I/O	Displays the disk utilization, transaction rate, or throughput as a percentage over time. For more information, see Disk I/O widget on page 541 . 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
Move a widget	Move the widget by clicking and dragging its title bar, then dropping it in its new location
Add a widget	Select <i>Toggle Widgets</i> from the toolbar, then select the name widget you need to add.
Delete a widget	Click the <i>Close</i> icon in the widget's title bar.
Customize a widget	For widgets with an edit icon, you can customize the widget by clicking the Edit icon and configuring the settings.

Action	Steps
Reset the dashboard	Select <i>Toggle Widgets > 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:

Host Name	The identifying name assigned to this FortiManager unit. Click the edit host name button to change the host name. For more information, see Changing the host name on page 530 .
Serial Number	The serial number of the FortiManager unit. The serial number is unique to the FortiManager unit and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
Platform Type	Displays the FortiManager platform type, for example <i>FMGVM64</i> (virtual machine).
HA Status	Displays if FortiManager unit is in High Availability mode and whether it is the Primary or Secondary unit in the HA cluster. For more information see High Availability on page 641 .
System Time	The current time on the FortiManager internal clock. Click the edit system time button to change system time settings. For more information, see Configuring the system time on page 530 .
Firmware Version	<p>The version number and build number of the firmware installed on the FortiManager unit.</p> <p>You can access the latest firmware version available on FortiGuard from FortiManager.</p> <p>Alternately you can manually download the latest firmware from the Customer Service & Support website at https://support.fortinet.com. Click the update button, then select the firmware image to load from the local hard disk or network volume. For more information, see Updating the system firmware on page 531.</p>
System Configuration	<p>The date of the last system configuration backup. The following actions are available:</p> <ul style="list-style-type: none"> Click the backup button to backup the system configuration to a file; see Backing up the system on page 534. Click the restore to restore the configuration from a backup file; see Restoring the configuration on page 534. You can also migrate the configuration to a different FortiManager model by using the CLI. See Migrating the configuration on page 535.
Current Administrators	The number of administrators currently logged in. Click the current session list button to view the session details for all currently logged in administrators.

Up Time	The duration of time the FortiManager unit has been running since it was last started or restarted.
Administrative Domain	Displays whether ADOMs are enabled. Toggle the switch to change the Administrative Domain state. See Enabling and disabling the ADOM feature on page 553 .
FortiAnalyzer Features	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 FortiAnalyzer Features on page 20 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.

- Configure the following settings to either manually configure the system time, or to automatically synchronize the FortiManager unit's clock with an NTP server:

System Time	The date and time according to the FortiManager unit's clock at the time that this pane was loaded or when you last clicked the <i>Refresh</i> button.
Time Zone	Select the time zone in which the FortiManager unit is located and whether or not the system automatically adjusts for daylight savings time.
Update Time By	Select <i>Set time</i> to manually set the time, or <i>Synchronize with NTP Server</i> to automatically synchronize the time.
Set Time	Manually set the data and time.
Select Date	Set the date from the calendar or by manually entering it in the format: YYYY/MM/DD.
Select Time	Select the time.
Synchronize with NTP Server	Automatically synchronize the date and time.
Sync Interval	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.
Server	Enter the IP address or domain name of an NTP server. Click the plus icon to add more servers. To find an NTP server that you can use, go to http://www.ntp.org .

- Click the checkmark to apply your changes.

Updating the system firmware

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

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



Back up the configuration and database before changing the firmware of FortiManager. Changing the firmware to an older or incompatible version may reset the configuration and database to the default values for that firmware version, resulting in data loss. For information on backing up the configuration, see [Backing up the system on page 534](#).



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



Installing firmware replaces the current network vulnerability management engine with the version included with the firmware release that you are installing. After you install the new firmware, make sure that your vulnerability definitions are up-to-date. For more information, see [Device Firmware and Security Updates on page 489](#).

To update FortiManager firmware using FortiGuard:

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

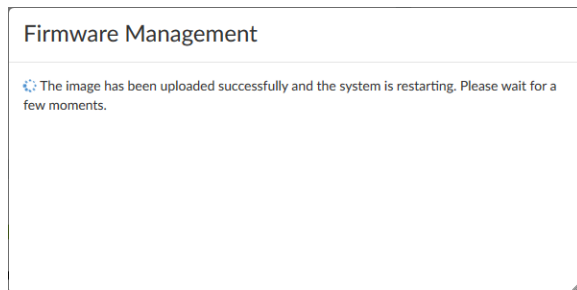
3. From the *FortiGuard Firmware* box, select the version of FortiManager for the upgrade, and click *OK*.
The *FortiGuard Firmware* box displays all FortiManager firmware images available for upgrade. A green checkmark displays beside the recommended image for FortiManager upgrade.

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

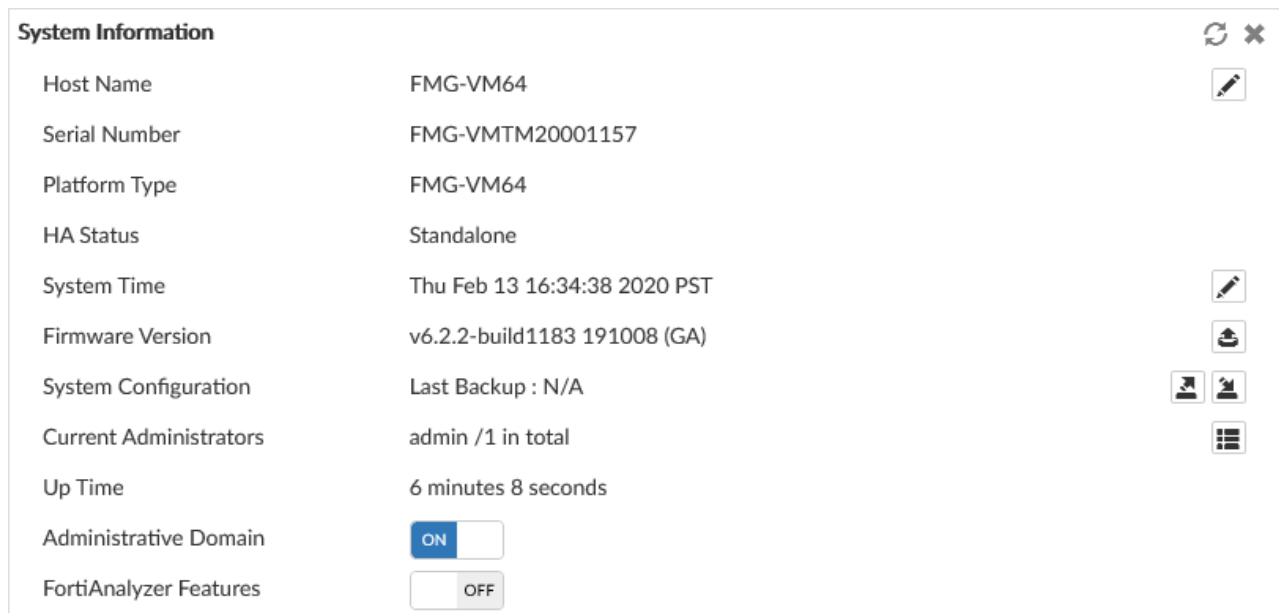
FortiManager downloads the firmware image from FortiGuard.

Index	Name	Status	Time Used	History

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



After FortiManager restarts, the upgrade is complete.



To manually update FortiManager firmware:

1. Download the firmware (the `.out` file) from the Customer Service & Support website, <https://support.fortinet.com/>.
2. Go to *System Settings > Dashboard*.
3. In the *System Information* widget, in the *Firmware Version* field, click *Upgrade Firmware*. The *Firmware Upload* dialog box opens.
4. 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.

You can also update FortiManager firmware images by using the *FortiGuard* module. For more information, see [Firmware images on page 510](#).

Backing up the system

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

If any management extensions, such as SD-WAN Orchestrator, are enabled, the backup file includes the configuration for each enabled management extension.

You can perform backups manually or at scheduled intervals. You can also create 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.

If your FortiManager has management extensions enabled, the configuration for the enabled management extension, such as SD-WAN Orchestrator, is restored too.



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

To restore the FortiManager configuration:

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

Choose Backup File	Select <i>Browse</i> to find the configuration backup file you want to restore, or drag and drop the file onto the dialog box.
Password	Type the encryption password, if applicable.
Overwrite current IP, routing and HA settings	Select the checkbox to overwrite the current IP, routing, and HA settings.
Restore in Offline Mode	Informational checkbox. Hover over the help icon for more information.

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:

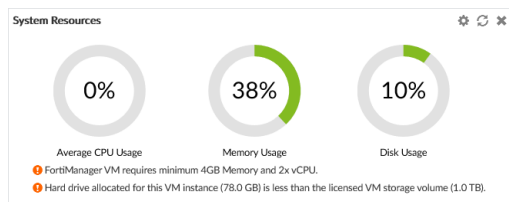
1. In one FortiManager model, go to *System Settings > Dashboard*.
2. Back up the system. See [Backing up the system on page 534](#).
3. In the other FortiManager model, go to *System Settings > Dashboard*.
4. In the *CLI Console* widget, type the following command:

```
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 16](#)). Clicking on a warning opens the [FortiManager VM Install Guide](#).

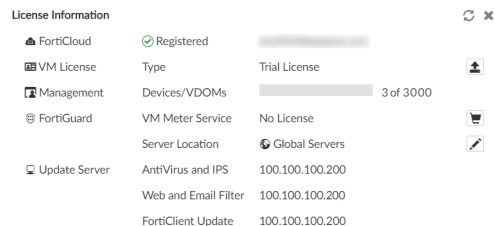


To toggle between real-time and historical data, click *Edit* in the widget toolbar, select *Historical* or *Real-time*, edit the other settings as required, then click *OK*.

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.



FortiCloud	The license registration status and the FortiCloud account.
VM License	<p>VM license information and status.</p> <p>Click the upload license button to upload a new VM license file.</p> <p>This field is only visible for FortiManager VM.</p> <p>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: <i>Duplicate License has been found! Your VM license will expire in XX hours (Grace time: 24 hours)</i></p> <p>Users will have 24 hours to upload a valid license before the duplicate license is blocked.</p>
Management	
Device/VDOMs	The total number of devices and VDOMs connected to the FortiManager and the total number of device and VDOM licenses.
FortiGates/Logging Devices	The number of connected FortiGates and other logging devices.
FortiAPs	The number of connected FortiAPs.
Logging	This section is only shown when <i>FortiAnalyzer Features</i> is enabled. For more information, see FortiAnalyzer Features on page 20 .
Device/VDOMs	The total number of devices and VDOMs connected to the FortiManager and the total number of device and VDOM licenses.
GB/Day	<p>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.</p> <p>The GB/Day log volume can be viewed per ADOM through the CLI using:</p> <pre>diagnose fortilogd logvol-adom <name>.</pre>
VM Storage	The amount of VM storage used and remaining.

This field is only visible for FortiManager VM.

FortiGuard

VM Meter Service

The license status.
Click the purchase button to go to the Fortinet Customer Service & Support website, where you can purchase a license.

Secure DNS Server

The SDNS server license status.
Click the upload image button to upload a license key.

Server Location

The locations of the FortiGuard servers, either global or US only.
Click the edit icon to adjust the location. Changing the server location will cause the FortiManager to reboot.

Update Server

AntiVirus and IPS

The IP address and physical location of the Antivirus and IPS update server.

Web and Email Filter

The IP address and physical location of the web and email filter update server.

FortiClient Update

The IP address and physical location of the FortiClient update server.

Registering a device or VM license

Register your device with FortiCloud to receive customer services, such as firmware updates and customer support. Users are required to register a VM license the first time they log in to FortiManager VM.



To view a list of registered devices, log in to FortiCloud, and go to *Asset > Manage/View Products*.


To register a FortiManager device:

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

To register a FortiManager VM license:

1. Go to the FortiManager login page.
2. Take one of the following actions:

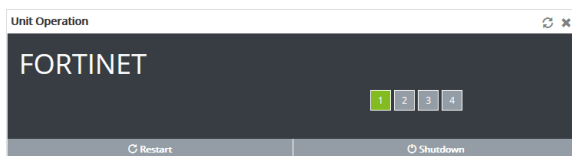
Action	Description
Upload License	<ol style="list-style-type: none"> 1. Click <i>Browse</i> to upload the license file, or drag it onto the field. 2. Click <i>Upload</i>. After the license file is uploaded, the system will restart to verify it. This

Action	Description
	may take a few moments.
	 <p>To download the license file, log in to FortiCloud, and go to <i>Asset > Manage/View Products</i>, then click the product serial number.</p>
Login with FortiCloud	<p>If a valid license is not associated with the account, you can start a free trial license for up to three devices.</p> <ol style="list-style-type: none"> 1. Click <i>Login with FortiCloud</i>. 2. Log in with our account credentials or create a new account. <p>FortiManager connects to FortiCloud to get the trial license. The system will restart to apply the trial license.</p>

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.

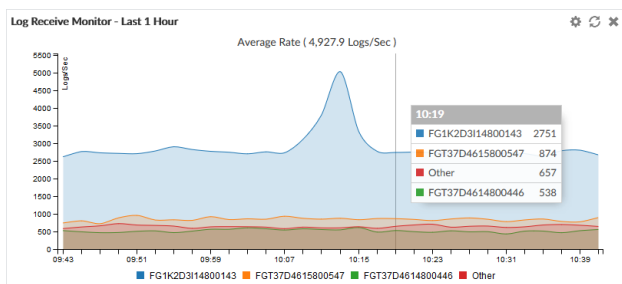
Click *Edit* from the widget toolbar to view the *Alert Message Console Settings*, where you can adjust the number of entries that are visible in the widget, and the refresh interval.

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 20](#).

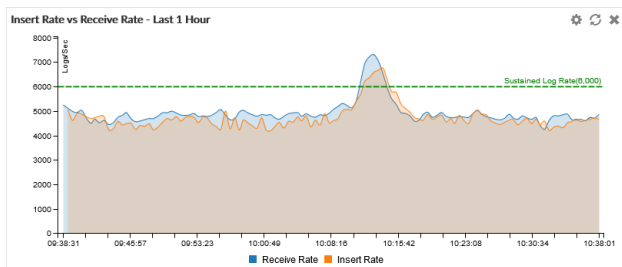
Insert Rate vs Receive Rate widget

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.



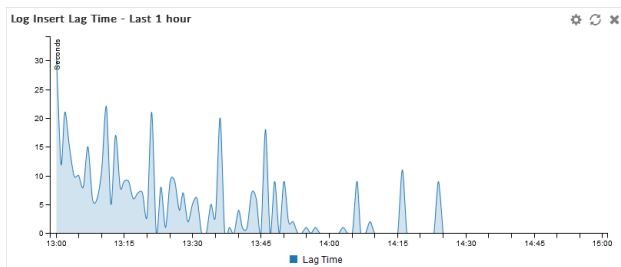


This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 20](#).

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.

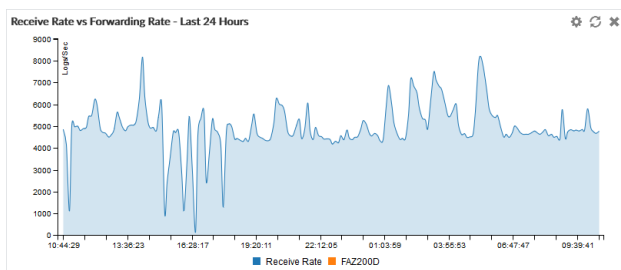


This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 20](#).

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.

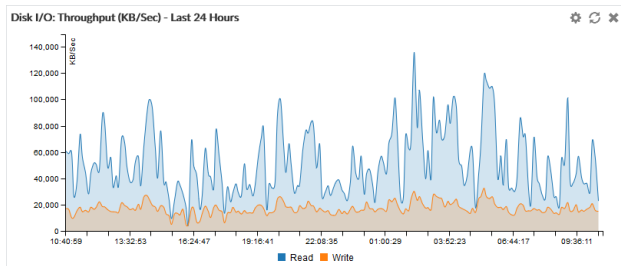


This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 20](#).

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.



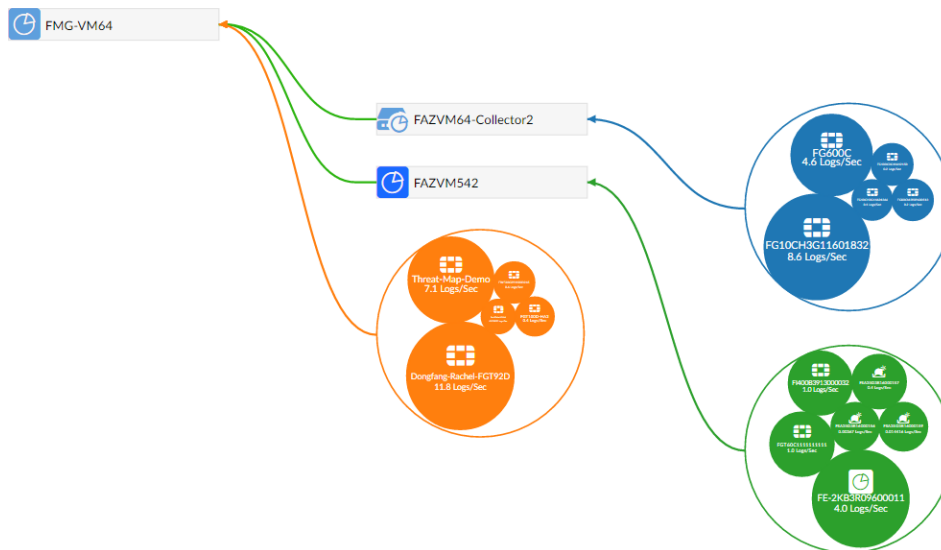
This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features](#) on page 20.

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 20](#).

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 598](#) and [Managing administrator accounts on page 599](#).

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.

System Network Management Interface

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

All Interfaces Routing Table IPv6 Routing Table

2. Configure the following settings for *port1*, then click *Apply* to apply your changes.

Name	Displays the name of the interface.
IP Address/Netmask	The IP address and netmask associated with this interface.
IPv6 Address	The IPv6 address associated with this interface.
Administrative Access	Select the allowed administrative service protocols from: HTTPS, HTTP, PING, SSH, SNMP, and Web Service.
IPv6 Administrative Access	Select the allowed IPv6 administrative service protocols from: HTTPS, HTTP, PING, SSH, SNMP, and Web Service.
Service Access	<p>Select the Fortinet services that are allowed access on this interface. These include <i>FortiGate Updates</i> and <i>Web Filtering</i>. By default all service access is enabled on port1, and disabled on port2.</p> <p>Select <i>Bind to IP Address</i> and specify the IP address. The IP address specified in Bind to IP address must be on the same subnet as the IP address of the interface. This IP address is only for FortiGate 443 requests.</p>
Default Gateway	The default gateway associated with this interface.
Primary DNS Server	The primary DNS server IP address.
Secondary DNS Server	The secondary DNS server IP address.

To configure additional ports:

1. Go to *System Settings > Network* 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.

Packet capture

Packets can be captured on configured interfaces by going to *System > Network > Packet Capture*.

The following information is available:

Interface	The name of the configured interface for which packets can be captured. For information on configuring an interface, see Configuring network interfaces on page 542 .
Filter Criteria	The values used to filter the packet.
# Packets	The number of packets.
Maximum Packet Count	The maximum number of packets that can be captured on a sniffer.
Progress	The status of the packet capture process.
Actions	Allows you to start and stop the capturing process, and download the most recently captured packets.

To start capturing packets on an interface, select the *Start capturing* button in the *Actions* column for that interface. The *Progress* column changes to *Running*, and the *Stop capturing* and *Download* buttons become available in the *Actions* column.

To add a packet sniffer:

1. From the *Packet Capture* table, click *Create New* in the toolbar. The *Create New Sniffer* pane opens.
2. Configure the following options:

Interface	The interface name (non-changeable).
Max. Packets to Save	Enter the maximum number of packets to capture, between 1-10000. The default is 4000 packets.
Include IPv6 Packets	Select to include IPv6 packets when capturing packets.
Include Non-IP Packets	Select to include non-IP packets when capturing packets.
Enable Filters	You can filter the packet by <i>Host(s)</i> , <i>Port(s)</i> , <i>VLAN(s)</i> , and <i>Protocol</i> .

3. Click *OK*.

To download captured packets:

1. In the *Actions* column, click the *Download* button for the interface whose captured packets you want to download. If no packets have been captured for that interface, click the *Start capturing* button.
2. When prompted, save the packet file (*sniffer_[interface].pcap*) to your management computer. The file can then be opened using packet analyzer software.

To edit a packet sniffer:

1. From the *Packet Capture* table, click *Edit* in the toolbar. The *Edit Sniffer* pane opens.
2. Configure the packet sniffer options
3. Click *OK*.

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 538](#).

Summary



RAID Level

Status

Disk Space Usage

Raid-10 [\[Change\]](#)

System is functioning normally.

1890GB Used / 5442GB Free / 7332GB Total

25% Used

Disk Management

Disk Number	Disk Status	Size(GB)	Disk Model
0	✓	1862	ST2000NM0033-9ZM175
1	✓	1862	ST2000NM0033-9ZM175
2	✓	1862	ST2000NM0033-9ZM175
3	✓	1862	ST2000NM0033-9ZM175
4	✓	1862	ST2000NM0033-9ZM175
5	✓	1862	ST2000NM0033-9ZM175
6	✓	1862	ST2000NM0033-9ZM175
7	✓	1862	ST2000NM0033-9ZM175

Summary	Shows summary information about the RAID array.
Graphic	Displays the position and status of each disk in the RAID array. Hover the cursor over each disk to view details.
RAID Level	Displays the selected RAID level. Click <i>Change</i> to change the selected RAID level. When you change the RAID settings, all data is deleted.
Status	Displays the overall status of the RAID array.
Disk Space Usage	Displays the total size of the disk space, how much disk space is used, and how much disk space is free.
Disk Management	Shows information about each disk in the RAID array.
Disk Number	Identifies the disk number for each disk.
Disk Status	Displays the status of each disk in the RAID array. <ul style="list-style-type: none"> <i>Ready</i>: The hard drive is functioning normally. <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. <i>Initializing</i>: The FortiManager unit is writing to all the hard drives in the device in order to make the array fault tolerant. <i>Verifying</i>: The FortiManager unit is ensuring that the parity data of a redundant drive is valid. <i>Degraded</i>: The hard drive is no longer being used by the RAID controller. <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.
Size (GB)	Displays the size, in GB, of each disk.
Disk Model	Displays the model number of each disk.

Checking RAID from command line

Use command line to check if your device uses hardware or software RAID.

To check RAID type from the command line:

1. Select the *CLI Console* from the GUI banner.
2. Type the command `diagnose system raid status` and press *Enter*.
3. The following information is shown in the output:
 - Mega RAID - this output shows that the device uses hardware RAID.
 - Software RAID - this output shows that the device uses software RAID.

Sample command line output showing hardware RAID:

```
[Product_Name_Model] # diagnose system raid status
Mega RAID: <-- this is hardware RAID
RAID Level: Raid-50
RAID Status: OK
RAID Size: 11175GB
Groups: 2
```

```
[Product_Name_Model] # diagnose system raid status
Software RAID: <-- this is software RAID
RAID Level: Raid-50
RAID Status: OK
RAID Size: 11175GB
Groups: 2
```

Swapping hard disks

If a hard disk on a FortiManager unit fails, it must be replaced. On FortiManager devices that support hardware RAID, the hard disk can be replaced while the unit is still running - known as hot swapping. On FortiManager units with software RAID, the device must be shutdown prior to exchanging the hard disk.

To identify which hard disk failed, read the relevant log message in the *Alert Message Console* widget. See [Alert Messages Console widget on page 538](#).



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 538](#) for information.
4. Configure the RAID level. See [Configuring the RAID level on page 549](#).
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 598](#).



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 57](#).

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 *FortiView*, *Log View*, *Incidents & Events*, and *Reports* panes are also displayed per ADOM. You select the ADOM you need to work in when you log into the FortiManager unit. [Switching between ADOMs on page 19](#).



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 562](#).
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.



FortiManager does not support splitting FortiGate VDOMs between multiple ADOMs in different device modes.

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*
- *FortiView*
- *System Settings*

To create backup ADOMs:

1. Go to *System Settings > All ADOMs*, and click *Create New*.
2. Set the following options, and click *OK*:

Name	Type a name for the ADOM.
Type	Select the type of device and ADOM version.
Devices	Select a device. Alternately, you can add a device to the ADOM later by using the <i>Add Device</i> wizard.
Mode	Select <i>Backup</i> .

The ADOM in backup mode is created.

Importing objects to backup ADOMs

You can use the *Add Device* wizard to add FortiGate devices to an ADOM in backup mode. The wizard also lets you import Firewall address and service objects. Policies are not imported.

Alternately, you can import objects after adding devices by using the *Import 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:

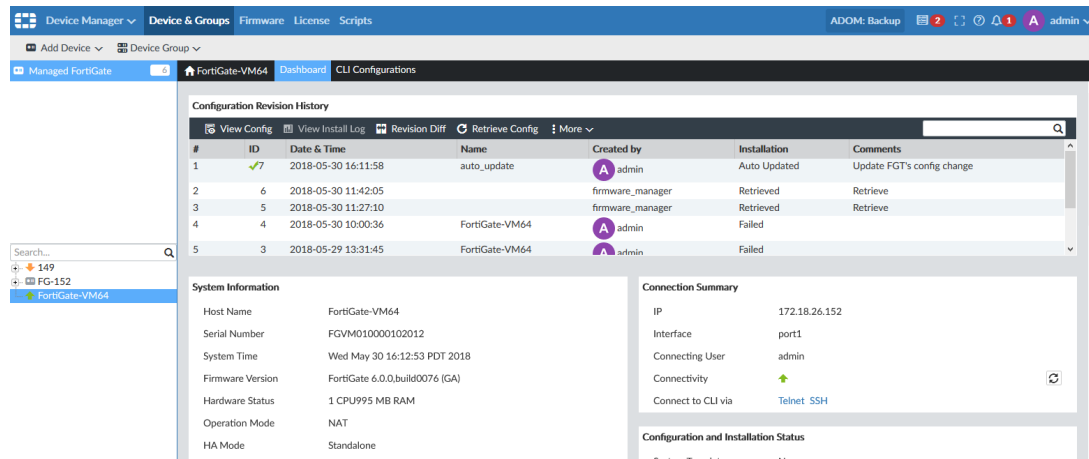
1. Go to *Device Manager > Device & Groups*.
2. Select a device and click *Import Policy*.
The objects are imported into the Device Manager database.
3. Go to the *Policy & Objects* pane to view the objects.
You can also create, edit, and delete objects.

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 70](#).



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 553](#).

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 558 .
Edit	Edit the selected ADOM. This option is also available from the right-click menu. See Editing an ADOM on page 562 .
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 562 .
Enter ADOM	Switch to the selected ADOM. This option is also available from the right-click menu.
More	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 ADOM versions on page 563 . These options are also available from the right-click menu.
Search	Enter a search term to search the ADOM list.
Name	The name of the ADOM. ADOMs are listed in the following groups: <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.
Firmware Version	The firmware version of the ADOM. Devices in the ADOM should have the same firmware version. See ADOM versions on page 563 for more information.
Central VPN	Whether or not central VPN management is enabled for the ADOM.
Allocated Storage	The amount of hard drive storage space allocated to the ADOM.
Devices	The number of devices and VDOMs that the ADOM contains. The device list can be expanded or by clicking the triangle.

Creating ADOMs

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 554](#).
- 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 553](#).
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 FortiGate 6.0 6.2 6.4

Comments 0/128

Devices

+ Select Device

Name	IP Address	Platform
No Device.		

Mode ☒ Normal ☐ Backup

Central Management ☐ VPN ☒ FortiAP ☐ SD-WAN ☒ FortiSwitch

Default Device Selection for Install ☒ Select All ☐ Deselect All

Perform Policy Check Before Every Install

Auto-Push Policy Packages When Device Back Online ☐ Enable ☒ Disable

4. Configure the following settings, then click **OK** to create the ADOM.

Name	Type a name that allows you to distinguish this ADOM from your other ADOMs. ADOM names must be unique.
Type	Select 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.
Version	Select the version of the devices in the ADOM. The ADOM version cannot be edited.
Devices	Add a device or devices with the selected versions to the ADOM. The search field can be used to find specific devices. See Assigning devices to an ADOM on page 561 .
Mode	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 ADOM modes on page 555 for more information.
Central Management	Select the <i>VPN</i> checkbox to enable central VPN management. Select the <i>SD-WAN</i> checkbox to enable central SD-WAN management.

	<p>Select the <i>FortiAP</i> checkbox to enable central FortiAP management. This checkbox is selected by default.</p> <p>This option is only available when the <i>Mode</i> is <i>Normal</i>.</p>
Default Device Selection for Install	<p>Select either <i>Select All</i> or <i>Unselect All</i>.</p> <p>This option is only available when the <i>Mode</i> is <i>Normal</i>.</p>
Perform Policy Check Before Every Install	<p>Turn <i>On</i> to perform a policy consistency check before every install. Only added or modified policies are checked. See Perform a policy consistency check on page 200.</p>
Action When Conflicts Occur During Policy Check	<p>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>.</p>
Auto-Push Policy Packages When Device Back Online	<p>Automatically push policy package updates to currently offline managed devices when the devices come back online.</p>
Data Policy	<p>Specify how long to keep logs in the indexed and compressed states.</p> <p>This section is only available when FortiAnalyzer features are enabled. See FortiAnalyzer Features on page 20.</p>
Keep Logs for Analytics	<p>Specify how long to keep logs in the indexed state.</p> <p>During the indexed state, logs are indexed in the SQL database for the specified amount of time. Information about the logs can be viewed in the <i>FortiView > FortiView, Incidents & Events/FortiSoC</i>, and <i>Reports</i> modules. After the specified length of time expires, Analytics logs are automatically purged from the SQL database.</p>
Keep Logs for Archive	<p>Specify how long to keep logs in the compressed state.</p> <p>During the compressed state, logs are stored in a compressed format on the FortiManager unit. When logs are in the compressed state, information about the log messages cannot be viewed in the <i>FortiView > FortiView, Incidents & Events/FortiSoC</i>, or <i>Reports</i> modules. After the specified length of time expires, Archive logs are automatically deleted from the FortiManager unit.</p>
Disk Utilization	<p>Specify how much disk space to use for logs.</p> <p>This section is only available when FortiAnalyzer features are enabled. See FortiAnalyzer Features on page 20.</p>
Maximum Allowed	<p>Specify the maximum amount of FortiManager disk space to use for logs, and select the unit of measure.</p> <p>The total available space on the FortiManager unit is shown.</p>
Analytics : Archive	<p>Specify the percentage of the allotted space to use for Analytics and Archive logs.</p> <p>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.</p>
Alert and Delete When Usage Reaches	<p>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.</p>

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 554](#)). 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 558](#).

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 616](#)), 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 561](#).

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

Each ADOM is associated with a specific firmware version, based on the firmware version of the devices that are in that ADOM. This version is selected when creating a new ADOM. See [Creating ADOMs on page 558](#).

ADOM version N can manage devices with firmware version N. For example, ADOM version 6.4 can manage devices with firmware version 6.4.

When upgrading firmware for managed devices, ADOM version N can tolerate to manage devices with firmware version N+1. For example, ADOM version 6.2 can manage devices with firmware 6.2 and 6.4. This allows you to continue to manage an ADOM as normal while upgrading the devices within that ADOM. You can only update the ADOM version from N to N+1 after all of the devices within the ADOM have been updated to firmware version N+1.

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.

The general steps for upgrading an ADOM containing multiple devices running FortiOS 6.2 from 6.2 to 6.4 are as follows:

1. In the ADOM, upgrade one of the FortiGate units to FortiOS 6.4, and then resynchronize the device. See [Firmware on page 98](#) for more information.
All of the ADOM objects, including Policy Packages, remain as 6.2 objects.
 2. Upgrade the rest of the FortiGate units in the ADOM to FortiOS 6.4.
 3. Upgrade the ADOM to 6.4. See [Upgrading an ADOM on page 566](#) for more information.
All of the database objects will be converted to 6.4 format, and the GUI content for the ADOM will change to reflect 6.4 features and behavior.
-



An ADOM can only be upgraded after all the devices within the ADOM have been upgraded.

Global database version

The global database ADOM supports its own version plus one version. For example, if the global database ADOM version is 6.0, the global database ADOM can manage version 6.0 and 6.2, but not 6.4 or 5.6.

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 565](#)

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, such as upgrading firmware for a device. If you are making changes at the ADOM level, you can leave the ADOM unlocked and lock policy packages or objects independently.

The padlock icon, shown next to the ADOM name on the banner and in the *All ADOMs* list, will turn from gray to green when you lock an ADOM. If it is red, it means that another administrator has locked the ADOM.

Optionally, ADOM lock override can be enabled, allowing an administrator to unlock an ADOM that has been locked by another administrator and discard all of their unsaved changes.

To lock an ADOM:

- Ensure that you are in the specific ADOM that you will be editing (top right corner of the GUI), then select *Lock* from the banner.
- Or, go to *System Settings > All ADOMs*, right-click on an ADOM, and select *Lock* from the right-click menu.

The ADOM will now be locked, allowing you to make changes to it and preventing other administrators from making changes unless lock override is enabled. The lock icon will turn into a green locked padlock. For other administrators

To unlock an ADOM:

- Ensure you have saved any changes you may have made to the ADOM then select *Unlock ADOM* from the banner.
- Or, go to *System Settings > All ADOMs*, right-click on an ADOM, and select *Lock* from the right-click menu.

If there are unsaved changes to the ADOM, a dialog box will give you the option of saving or discarding your changes before unlocking the ADOM. The ADOM will now be unlocked, allowing any administrator to lock the ADOM and make changes.

To enable or disable ADOM lock override:

Enter the following CLI commands:

```
config system global
    set lock-preempt {enable | disable}
end
```

Upgrading an ADOM

To upgrade an ADOM, you must be logged in as a super user administrator.



An ADOM can only be upgraded after all the devices within the ADOM have been upgraded. See [ADOM versions on page 563](#) 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:

Certificate Name	The name of the certificate.
Subject Information	<p>Select the ID type from the dropdown list:</p> <ul style="list-style-type: none"> • <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. • <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. • <i>Email</i>: Select to use an email address. Enter the email address in the <i>Email Address</i> field.
Optional Information	
Organization Unit (OU)	The name of the department. You can enter a series of OUs up to a maximum of 5. To add or remove an OU, use the plus (+) or minus (-) icons.
Organization (O)	Legal name of the company or organization.
Locality (L)	Name of the city or town where the device is installed.
State/Province (ST)	Name of the state or province where the FortiGate unit is installed.
Country (C)	Select the country where the unit is installed from the dropdown list.
E-mail Address (EA)	Contact email address.
Subject Alternative Name	<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"> • e-mail address • IP address • URI • DNS name (alternatives to the Common Name) • directory name (alternatives to the Distinguished Name) <p>You must precede the name with the name type. Examples:</p> <ul style="list-style-type: none"> • IP:1.1.1.1 • email:test@fortinet.com • email:my@other.address • URI:http://my.url.here/
Key Type	The key type can be <i>RSA</i> or <i>Elliptic Curve</i> .

Key Size	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> .
Curve Name	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> .
Enrollment Method	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:

Type	Select the certificate type from the dropdown list: <i>Local Certificate</i> , <i>PKCS #12 Certificate</i> , or <i>Certificate</i> .
Certificate File	Click <i>Browse...</i> and locate the certificate file on the management computer, or drag and drop the file onto the dialog box.
Key File	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> .
Password	Enter the certificate password. This option is only available when <i>Type</i> is <i>PKCS #12 Certificate</i> or <i>Certificate</i> .
Certificate Name	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

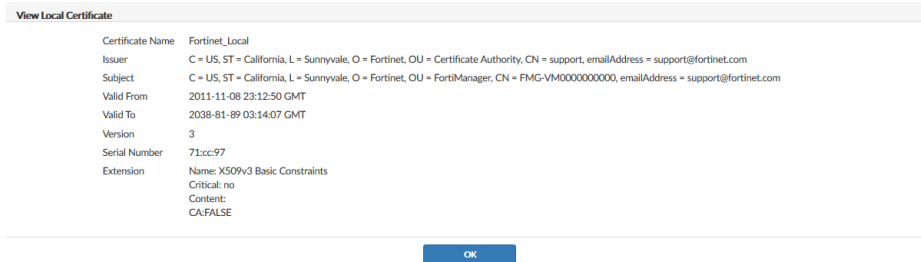
To delete a local certificate or certificates:

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 572](#).
2. On the client, send the fetch request to the server. See [Fetch requests on page 573](#).
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 574](#).
4. On the server, review the request, then either approve or reject it. See [Request processing on page 574](#).
5. Monitor the fetch process on either FortiManager. See [Fetch monitoring on page 575](#).
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 20](#).

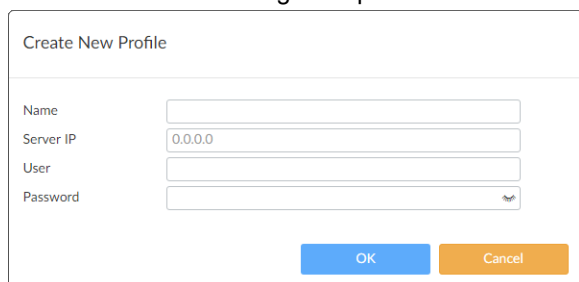
Fetching profiles

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.



The dialog box titled "Create New Profile" contains four input fields: "Name", "Server IP" (with the value "0.0.0.0"), "User", and "Password" (with a toggle icon). At the bottom are "OK" and "Cancel" buttons.

3. Configure the following settings, then click *OK* to create the profile.

Name	Enter a name for the profile.
Server IP	Enter the IP address of the fetch server.
User	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.
Password	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

3. 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.

Name	Displays the name of the fetch server you have specified.
Server IP	Displays the IP address of the server you have specified.
User	Displays the username of the server administrator you have provided.
Secure Connection	Select to use SSL connection to transfer fetched logs from the server.
Server ADOM	Select the ADOM on the server the logs will be fetched from. Only one ADOM can be fetched from at a time.
Local ADOM	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.
Devices	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> .
Enable Filters	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.
Time Period	Specify what date and time range of log messages to fetch.
Index Fetch Logs	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 to 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-VM0000000001)	admino	Waiting for approval	Review
Fetch Request(1)				

- 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*.
- 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	<table> <tr> <th>ADOM</th><th>Device</th><th>VDOM</th></tr> <tr> <td>root</td><td>FGVMEV0000000000</td><td>*</td></tr> </table>	ADOM	Device	VDOM	root	FGVMEV0000000000	*
ADOM	Device	VDOM					
root	FGVMEV0000000000	*					
Filters	None						
Time Period	16:02 2016/01/30 - 16:02 2017/02/02						
Secure Connection	<input checked="" type="checkbox"/>						

[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.

You may need to rebuild the ADOM after the transfer is complete depending on the Log Fetch settings.

To perform post fetch actions:

Is <i>Index Fetched Logs</i> enabled in the <i>Log Fetch</i> settings?	Yes	The ADOM is rebuilt automatically and the log fetch workflow is complete.
	No	You will need to rebuild ADOM manually from the CLI.

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 ^ mP34AgCu6bvs1x64BD8OF //otJysxG1cKhIWjSf7mPJjm
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:

Add Filter	Filter the event log list based on the log level, user, sub type, or message. See Event log filtering on page 578 .
Last...	Select the amount of time to show from the available options, or select a custom time span or any time.
Download	Download the event logs in either CSV or the normal format to the management computer.
Raw Log / Formatted Log	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.
Historical Log	Click to view the historical logs list.
Back	Click the back icon to return to the regular view from the historical view.
View	View the selected log file. This option is also available from the right-click menu, or by double-clicking on the log file. This option is only available when viewing historical event logs.
Delete	Delete the selected log file. This option is also available from the right-click menu. This option is only available when viewing historical event logs.
Clear	Clear the selected file of logs. This option is also available from the right-click menu. This option is only available when viewing historical event logs.

Type	<p>Select the type from the dropdown list:</p> <ul style="list-style-type: none"> Event Log FDS Upload Log: Select the device from the dropdown list. 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. <p>This option is only available when viewing historical logs.</p>
Search	<p>Enter a search term to search the historical logs.</p> <p>This option is only available when viewing historical event logs.</p>
Pagination	Browse the pages of logs and adjust the number of logs that are shown per page.

The following information is shown:

#	The log number.																												
Date/Time	The date and time that the log file was generated.																												
Device ID	The ID of the related device.																												
Sub Type	<p>The log sub-type:</p> <table> <tr> <td>System manager event</td><td>HA event</td></tr> <tr> <td>FG-FM protocol event</td><td>Firmware manager event</td></tr> <tr> <td>Device configuration event</td><td>FortiGuard service event</td></tr> <tr> <td>Global database event</td><td>FortiClient manager event</td></tr> <tr> <td>Script manager event</td><td>FortiMail manager event</td></tr> <tr> <td>Web portal event</td><td>Debug I/O log event</td></tr> <tr> <td>Firewall objects event</td><td>Configuration change event</td></tr> <tr> <td>Policy console event</td><td>Device manager event</td></tr> <tr> <td>VPN console event</td><td>Web service event</td></tr> <tr> <td>Endpoint manager event</td><td>FortiAnalyzer event</td></tr> <tr> <td>Revision history event</td><td>Log daemon event</td></tr> <tr> <td>Deployment manager event</td><td>FIPS-CC event</td></tr> <tr> <td>Real-time monitor event</td><td>Managed devices event</td></tr> <tr> <td colspan="2">Log and report manager event</td></tr> </table>	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	
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																													
User	The user that the log message relates to.																												
Description	A description of the event.																												
Message	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

Use the task monitor to view the status of the tasks you have performed.

Go to *System Settings > Task Monitor* to view the task monitor. The task list size can also be configured; see [Advanced Settings on page 596](#).

To filter the information in the monitor, enter a text string in the search field.

+ Group Error Devices Delete View Task Detail Show Status Column Settings Q									
ID	Source	Description	User	Status	Time Used	ADOM	Start Time	End Time	
<input type="checkbox"/> 37	Install Configuration	Push config to device.	admin	<div><div></div></div> (80%)	14s	root	Tue Jan 28 2020 3:16:40 PM	N/A	
<input type="checkbox"/> 36	Install Package	Install Package 'default'	admin	Success: 1	2s	root	Tue Jan 28 2020 3:16:37 PM	Tue Jan 28 2020 3:16:39 PM	
<input type="checkbox"/> 35	Firmware Manager	Device Image Upgrade	admin	Success: 1	4m 1s	root	Tue Jan 28 2020 3:12:31 PM	Tue Jan 28 2020 3:16:32 PM	
<input type="checkbox"/> 34	Device Manager	Add/delete Unauthorized Devices	Auto link	<div><div></div></div> (50%)	4m 40s	root	Tue Jan 28 2020 3:12:14 PM	N/A	
<input type="checkbox"/> 33	Device Manager	pm devprof adom root default scope member	admin	Success: 1	4s	root	Tue Jan 28 2020 3:10:59 PM	Tue Jan 28 2020 3:11:03 PM	
<input type="checkbox"/> 32	Device Manager	Add Device	admin	Success: 1	6s	root	Tue Jan 28 2020 3:10:52 PM	Tue Jan 28 2020 3:10:58 PM	
<input type="checkbox"/> 31	Device Manager	Delete Device	admin	Success: 1	3s	root	Tue Jan 28 2020 3:10:12 PM	Tue Jan 28 2020 3:10:15 PM	
<input type="checkbox"/> 30	Install Configuration	Push config to device.	admin	Success: 1	22s	root	Tue Jan 28 2020 2:55:17 PM	Tue Jan 28 2020 2:55:39 PM	
<input type="checkbox"/> 29	Device Manager	Add/delete Unauthorized Devices	Auto link	Success: 1	43s	root	Tue Jan 28 2020 2:54:56 PM	Tue Jan 28 2020 2:55:39 PM	
<input type="checkbox"/> 28	Device Manager	Add Device	admin	Success: 1	5s	root	Tue Jan 28 2020 2:54:18 PM	Tue Jan 28 2020 2:54:23 PM	
<input type="checkbox"/> 27	Device Manager	Add/delete Unauthorized Devices	admin	Success: 1	2s	root	Tue Jan 28 2020 2:54:02 PM	Tue Jan 28 2020 2:54:04 PM	
<input type="checkbox"/> 26	Device Manager	Delete Device	admin	Success: 1	3s	root	Tue Jan 28 2020 2:49:23 PM	Tue Jan 28 2020 2:49:26 PM	
<input type="checkbox"/> 25	Install Configuration	Push config to device.	admin	Error: 1	32s	root	Tue Jan 28 2020 2:46:09 PM	Tue Jan 28 2020 2:46:41 PM	
<input type="checkbox"/> 24	Install Package	Install Package 'default'	admin	Success: 1	2s	root	Tue Jan 28 2020 2:46:06 PM	Tue Jan 28 2020 2:46:08 PM	

The following options are available:

Group Error Devices	Create a group of the failed devices, allowing for re-installations to be done only on the failed devices.
Delete	Remove the selected task or tasks from the list. This changes to <i>Cancel Running Task(s)</i> when <i>View</i> is <i>Running</i> .
View Task Detail	View the task <i>Index</i> , <i>Name</i> , <i>Status</i> , <i>Time Used</i> , and <i>History</i> , in a new window. Click the icons in the <i>History</i> column to view the following information:

	<ul style="list-style-type: none"> • History • Promotion of device in FortiManager with autolink • Upgrade remote device firmware • Retrieve remote device configuration • Installation of device templates • Installation of policy packages • Execution of additional scripts <p>To filter the information in the task details, enter a text string in the search field. This can be useful when troubleshooting warnings and errors.</p>
Show Status	Select which tasks to view from the dropdown list, based on their status. The available options are: <i>All</i> , <i>Pending</i> , <i>Running</i> , <i>Canceling</i> , <i>Canceled</i> , <i>Done</i> , <i>Error</i> , <i>Aborting</i> , <i>Aborted</i> , and <i>Warning</i> .
Column Settings	Select the columns you want to display from the dropdown.

The following information is available:

ID	The identification number for a task.
Source	The platform from where the task is performed.
Description	The nature of the task. Double-click the task to display the specific actions taken under this task.
User	The user or users who performed the tasks.
Status	<p>The status of the task:</p> <ul style="list-style-type: none"> • <i>Success</i>: Completed with success. • <i>Error</i>: Completed without success. • <i>Canceled</i>: User canceled the task. • <i>Canceling</i>: User is canceling the task. • <i>Aborted</i>: The FortiManager system stopped performing this task. • <i>Aborting</i>: The FortiManager system is stopping performing this task. • <i>Running</i>: Being processed. In this status, a percentage bar appears in the Status column. • <i>Pending</i> • <i>Warning</i>
Time Used	The number of seconds to complete the task.
ADOM	The ADOM associated with the task.
Start Time	The time that the task was started.
End Time	The time that the task was completed.

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 type="checkbox"/> Terminus	✓	✓	<input checked="" type="checkbox"/>
<input type="checkbox"/> Trantor	✓	✓	<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 type="checkbox"/> Daneel	Authentication, No Privacy		
<input type="checkbox"/> Fallom	Authentication, Privacy		
<input type="checkbox"/> Golan	No Authentication, No Privacy		

The following information and options are available:

SNMP Agent	Select to enable the SNMP agent. When this is enabled, it sends FortiManager SNMP traps.
Description	Optionally, type a description of this FortiManager system to help uniquely identify this unit.

Location	Optionally, type the location of this FortiManager system to help find it in the event it requires attention.
Contact	Optionally, type the contact information for the person in charge of this FortiManager system.
SNMP v1/2c	The list of SNMP v1/v2c communities added to the FortiManager configuration.
Create New	Select <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 SNMP v1/v2c communities on page 581 .
Edit	Edit the selected SNMP community.
Delete	Delete the selected SNMP community or communities.
Community Name	The name of the SNMP community.
Queries	The status of SNMP queries for each SNMP community. The enabled icon indicates that at least one query is enabled. The disabled icon indicates that all queries are disabled.
Traps	The status of SNMP traps for each SNMP community. The enabled icon indicates that at least one trap is enabled. The disabled icon indicates that all traps are disabled.
Enable	Enable or disable the SNMP community.
SNMP v3	The list of SNMPv3 users added to the configuration.
Create New	Select <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 SNMP v3 users on page 584 .
Edit	Edit the selected SNMP user.
Delete	Delete the selected SNMP user or users.
User Name	The user name for the SNMPv3 user.
Security Level	The security level assigned to the SNMPv3 user.
Notification Hosts	The notification host or hosts assigned to the SNMPv3 user.
Queries	The status of SNMP queries for each SNMP user. The enabled icon indicates queries are enabled. The disabled icon indicates they are disabled.

SNMP v1/v2c communities

An SNMP community is a grouping of equipment for network administration purposes. You must configure your FortiManager to belong to at least one SNMP community so that community's SNMP managers can query the FortiManager system information and receive SNMP traps from it.



These SNMP communities do not refer to the FortiGate devices the FortiManager system is managing.

Each community can have a different configuration for SNMP traps and can be configured to monitor different events. You can add the IP addresses of up to eight hosts to each community. Hosts can receive SNMP device traps and information.

To create a new SNMP community:

1. Go to *System Settings > 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"/>

3. Configure the following options, then click *OK* to create the community.

Name	Enter a name to identify the SNMP community. This name cannot be edited later.
Hosts	<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>
IP Address/Netmask	<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>

Interface	Select the interface that connects to the network where this SNMP manager is located from the dropdown list. This must be done if the SNMP manager is on the Internet or behind a router.
Delete	Click the delete icon to remove this SNMP manager entry.
Add	Select to add another entry to the Hosts list. Up to eight SNMP manager entries can be added for a single community.
Queries	Enter the port number (161 by default) the FortiManager system uses to send v1 and v2c queries to the FortiManager in this community. Enable queries for each SNMP version that the FortiManager system uses.
Traps	Enter the Remote port number (162 by default) the FortiManager system uses to send v1 and v2c traps to the FortiManager in this community. Enable traps for each SNMP version that the FortiManager system uses.
SNMP Event	<p>Enable the events that will cause SNMP traps to be sent to the community.</p> <ul style="list-style-type: none"> • <i>Interface IP changed</i> • <i>Log disk space low</i> • <i>CPU Overuse</i> • <i>Memory Low</i> • <i>System Restart</i> • <i>CPU usage exclude NICE threshold</i> • <i>HA Failover</i> • <i>RAID Event</i> (only available for devices that support RAID) • <i>Power Supply Failed</i> (only available on supported hardware devices) • <i>Fan Speed Out of Range</i> • <i>Temperature Out of Range</i> • <i>Voltage Out of Range</i> <p>FortiAnalyzer feature set SNMP events:</p> <ul style="list-style-type: none"> • <i>High licensed device quota</i> • <i>High licensed log GB/day</i> • <i>Log Alert</i> • <i>Log Rate</i> • <i>Data Rate</i>

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.

User Name	The name of the SNMP v3 user.
Security Level	<p>The security level of the user. Select one of the following:</p> <ul style="list-style-type: none"> • <i>No Authentication, No Privacy</i> • <i>Authentication, No Privacy</i>: Select the <i>Authentication Algorithm</i> (SHA1, MD5) and enter the password. • <i>Authentication, Privacy</i>: Select the <i>Authentication Algorithm</i> (SHA1, MD5), the <i>Private Algorithm</i> (AES, DES), and enter the passwords.
Queries	Select to enable queries then enter the port number. The default port is 161.
Notification Hosts	The IP address or addresses of the host. Click the add icon to add multiple IP addresses.

SNMP Event

Enable the events that will cause SNMP traps to be sent to the SNMP manager.

- *Interface IP changed*
- *Log disk space low*
- *CPU Overuse*
- *Memory Low*
- *System Restart*
- *CPU usage exclude NICE threshold*
- *HA Failover*
- *RAID Event* (only available for devices that support RAID)
- *Power Supply Failed* (only available on supported hardware devices)
- *Fan Speed Out of Range*
- *Temperature Out of Range*
- *Voltage Out of Range*

FortiAnalyzer feature set SNMP events:

- *High licensed device quota*
- *High licensed log GB/day*
- *Log Alert*
- *Log Rate*
- *Data Rate*

To edit an SNMP user:

1. Go to *System Settings > 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
FORTINET-CORE-MIB.mib	The proprietary Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor Fortinet unit configuration settings and receive traps from the Fortinet SNMP agent.
FORTINET-FORTIMANAGER-MIB.mib	The proprietary FortiManager MIB includes system information and trap information for FortiManager units.
RFC-1213 (MIB II)	The Fortinet SNMP agent supports MIB II groups with the following exceptions. <ul style="list-style-type: none"> • No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10). • Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all Fortinet traffic activity. More accurate information can be obtained from the information reported by the Fortinet MIB.
RFC-2665 (Ethernet-like MIB)	The Fortinet SNMP agent supports Ethernet-like MIB information with the following exception. No support for the dot3Tests and dot3Errors groups.

SNMP traps

Fortinet devices share SNMP traps, but each type of device also has traps specific to that device type. For example FortiManager units have FortiManager specific SNMP traps. To receive Fortinet device SNMP traps, you must load and compile the FORTINET-CORE-MIB into your SNMP manager.

Traps sent include the trap message as well as the unit serial number (fnSysSerial) and host name (sysName). The Trap Message column includes the message that is included with the trap, as well as the SNMP MIB field name to help locate the information about the trap.

Trap message	Description
ColdStart, WarmStart, LinkUp, LinkDown	Standard traps as described in RFC 1215.
CPU usage high (fnTrapCpuThreshold)	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 <percentage value> end</pre>
CPU usage excluding NICE processes (fmSysCpuUsageExcludedNice)	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 <percentage value> end</pre>
Memory low	Memory usage exceeds 90 percent. This threshold can be set in the CLI using the following commands:

Trap message	Description
(fnTrapMemThreshold)	<pre>config system snmp sysinfo set trap-low-memory-threshold <percentage value> end</pre>
Log disk too full (fnTrapLogDiskThreshold)	Log disk usage has exceeded the configured threshold. Only available on devices with log disks.
Temperature too high (fnTrapTempHigh)	A temperature sensor on the device has exceeded its threshold. Not all devices have thermal sensors. See manual for specifications.
Voltage outside acceptable range (fnTrapVoltageOutOfRange)	Power levels have fluctuated outside of normal levels. Not all devices have voltage monitoring instrumentation.
Power supply failure (fnTrapPowerSupplyFailure)	Power supply failure detected. Available on some devices that support redundant power supplies.
Interface IP change (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.
HA switch (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
fnSysSerial	Fortinet unit serial number.

Administrator accounts:

MIB field	Description
fnAdminNumber	The number of administrators on the Fortinet unit.

MIB field	Description
fnAdminTable	Table of administrators.
fnAdminIndex	Administrator account index number.
fnAdminName	The user name of the administrator account.
fnAdminAddr	An address of a trusted host or subnet from which this administrator account can be used.
fnAdminMask	The netmask for fnAdminAddr.

Custom messages:

MIB field	Description
fnMessages	The number of custom messages on the Fortinet unit.

MIB fields and traps

MIB field	Description
fmModel	A table of all FortiManager models.
fmTrapHASwitch	The FortiManager HA cluster has been re-arranged. A new primary has been selected and asserted.

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.

SMTP Server Name	Enter a name for the SMTP server.
Mail Server	Enter the mail server information.
SMTP Server Port	Enter the SMTP server port number. The default port is 25.
Enable Authentication	Select to enable authentication.
Email Account	Enter an email account. This option is only accessible when authentication is enabled.
Password	Enter the email account password. This option is only accessible when authentication is enabled.

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	<input type="text"/>
IP address (or FQDN)	<input type="text"/>
Syslog Server Port	<input type="text" value="514"/>

OK Cancel

3. Configure the following settings and then select *OK* to create the mail server.

Name	Enter a name for the syslog server.
IP address (or FQDN)	Enter the IP address or FQDN of the syslog server.
Syslog Server Port	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			
Meta Fields	Length	Importance	Status
System Administrator (2)			
Contact Email	50	Optional	Enabled
Contact Phone	50	Optional	Enabled
Device (5)			
City	50	Optional	Enabled
Company/Organization	50	Optional	Enabled
Contact	50	Optional	Enabled
Country	50	Optional	Enabled
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:

- Go to *System Settings > Advanced > Meta Fields*.
- 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

- Configure the following settings and then select *OK* to create the meta field.

Object

The object this metadata field applies to: *System Administrators, Devices, Device Groups, Chassis, Administrative Domain, Firewall Addresses, Firewall Address Groups, Firewall Services, Firewall Service Groups, or Firewall Policy.*

Name	Enter the label to use for the field.
Length	Select the maximum number of characters allowed for the field from the dropdown list: 20, 50, or 255.
Importance	Select <i>Required</i> to make the field compulsory, otherwise select <i>Optional</i> .
Status	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 20](#).

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

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*:

Registered Device Logs	
Roll log file when size exceeds	Enter the log file size, from 10 to 500MB. Default: 200MB.
Roll log files at scheduled time	Select to roll logs daily or weekly. <ul style="list-style-type: none"> <i>Daily</i>: select the hour and minute value in the dropdown lists. <i>Weekly</i>: select the day, hour, and minute value in the dropdown lists.

Upload logs using a standard file transfer protocol	Select to upload logs and configure the following settings.
Upload Server Type	Select one of <i>FTP</i> , <i>SFTP</i> , or <i>SCP</i> .
Upload Server IP	Enter the IP address of the upload server.
User Name	Enter the username used to connect to the upload server.
Password	Enter the password used to connect to the upload server.
Remote Directory	Enter the remote directory on the upload server where the log will be uploaded.
Upload Log Files	Select to upload log files when they are rolled according to settings selected under <i>Roll Logs</i> , or daily at a specific hour.
Upload rolled files in gzip file format	Select to gzip the logs before uploading. This will result in smaller logs and faster upload times.
Delete files after uploading	Select to remove device log files from the FortiManager system after they have been uploaded to the Upload Server.
Local Device Log	
Send the local event logs to FortiAnalyzer / FortiManager	Select to send local event logs to another FortiAnalyzer or FortiManager device.
IP Address	Enter the IP address of the FortiAnalyzer or FortiManager.
Upload Option	Select to upload logs in real time or at a scheduled time. When selecting a scheduled time, you can specify the hour and minute to upload logs each day.
Severity Level	Select the minimum log severity level from the dropdown list. This option is only available when <i>Upload Option</i> is <i>Realtime</i> .
Reliable log transmission	Select to use reliable log transmission.
Secure connection	Select to use a secure connection for log transmission. This option is only available when <i>Reliable log transmission</i> is selected.

Configuring rolling and uploading of logs using the CLI

Log rolling and uploading can be enabled and configured using the CLI. For more information, see the [FortiManager CLI Reference](#).

Enable or disable log file uploads

Use the following CLI commands to enable or disable log file uploads.

To enable log uploads:

```
config system log settings
```



```
config rolling-regular
  set upload enable
end
```

To disable log uploads:

```
config system log settings
  config rolling-regular
    set upload disable
  end
```

Roll logs when they reach a specific size

Use the following CLI commands to specify the size, in MB, at which a log file is rolled.

To roll logs when they reach a specific size:

```
config system log settings
  config rolling-regular
    set file-size <integer>
  end
```

Roll logs on a schedule

Use the following CLI commands to configure rolling logs on a set schedule, or never.

To disable log rolling:

```
config system log settings
  config rolling-regular
    set when none
  end
```

To enable daily log rolling:

```
config system log settings
  config rolling-regular
    set upload enable
    set when daily
    set hour <integer>
    set min <integer>
  end
```

To enable weekly log rolling:

```
config system log settings
  config rolling-regular
    set when weekly
    set days {mon | tue | wed | thu | fri | sat | sun}
    set hour <integer>
    set min <integer>
  end
```

File Management

FortiManager allows you to configure automatic deletion of device log files, quarantined files, reports, and content archive files after a set period of time.

Go to *System Settings > Advanced > File Management* to configure file management settings.

File Management

Automatically Delete

<input type="checkbox"/> Device log files older than	365	Days	Scheduled daily at time	00:00
<input type="checkbox"/> Reports older than	365	Days	Scheduled daily at time	00:00
<input type="checkbox"/> Content archive files older than	365	Days	Scheduled daily at time	00:00
<input type="checkbox"/> Quarantined files older than	365	Days	Scheduled daily at time	00:00

Apply

Configure the following settings, and then select *Apply*:

Device log files older than	Select to enable automatic deletion of compressed log files. Enter a value in the text field, select the time period (<i>Days</i> , <i>Weeks</i> , or <i>Months</i>), and choose a time of day.
Reports older than	Select to enable automatic deletion of reports of data from compressed log files. Enter a value in the text field, select the time period, and choose a time of day.
Content archive files older than	Select to enable automatic deletion of IPS and DP archives from Archive logs. Enter a value in the text field, select the time period, and choose a time of day.
Quarantined files older than	Select to enable automatic deletion of compressed log files of quarantined files. Enter a value in the text field, select the time period, and choose a time of day.

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 20](#).

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*:

Offline Mode	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.
ADOM Mode	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.
Download WSDL file	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.
Chassis Management	Enable chassis management, then enter the chassis update interval, from 4 to 1440 minutes. Default: 15 minutes.
Configuration Changes Received from FortiGate	Select to either automatically accept changes (default) or to prompt the administrator to accept the changes.
Task List Size	Set a limit on the size of the task list. Default: 2000.
Verify Installation	Select to preview the installation before proceeding.
Allow Install Interface Policy Only	Select to manage and install only interface based policies, instead of all device and policy configuration.
Policy Hit Count	Enable or disable policy hit counting.
Display Policy & Objects in Dual Pane	Enable to display both the <i>Policy Packages</i> and <i>Object Configurations</i> tabs on a single pane in the <i>Policy & Objects</i> module. See Display options on page 190 .
Display Device/Group tree view in Device Manager	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 633](#) for more information.

In workflow mode, approval matrices can be create and managed on the *Approval Matrix* pane. See [Workflow approval on page 518](#) for more information.

This section contains the following topics:

- [Trusted hosts on page 598](#)
- [Monitoring administrators on page 599](#)
- [Disconnecting administrators on page 599](#)
- [Managing administrator accounts on page 599](#)
- [Administrator profiles on page 616](#)
- [Authentication on page 623](#)
- [Global administration settings on page 633](#)
- [Two-factor authentication on page 637](#)

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:

User Name	The name of the administrator account. Your session is indicated by <i>(current)</i> .
IP Address	The IP address where the administrator is logging in from. This field also displays the logon type (GUI, jsconsole, or SSH).
Start Time	The date and time the administrator logged in.
Time Out (mins)	The maximum duration of the session in minutes (1 to 480 minutes).

Disconnecting administrators

Administrators can be disconnected from the FortiManager unit from the *Admin Session List*.

To disconnect administrators:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, in the *Current Administrators* field, click the *Current Session List* button. The *Admin Session List* opens in the widget.
3. Select the administrator or administrators you need to disconnect.
4. Click *Delete* in the toolbar, or right-click and select *Delete*.

The selected administrators will be automatically disconnected from the FortiManager device.

Managing administrator accounts

Go to *System Settings > Admin > Administrator* to view the list of administrators and manage administrator accounts.

Only administrators with the *Super_User* profile can see the complete administrators list. If you do not have certain viewing permissions, you will not see the administrator list. When ADOMs are enabled, administrators can only access the ADOMs they have permission to access.

+ Create New Edit Clone Delete Table View Column Settings						
Seq.#	Name	Type	Profile	ADOMs	Policy Packages	Trusted IPv4 Hosts
1	123456	LOCAL	Super_User	All ADOMs	All Packages	0.0.0.0/0.0.0.0
2	Blue	Restricted Admin LOCAL	qwer	FG60		0.0.0.0/0.0.0.0
3	PKI	PKI	Standard_User	All ADOMs	52to56:default FG60:default FG60:Root/FortiGate-VM64_root	0.0.0.0/0.0.0.0
4	Restrict	LOCAL	Restricted_User	All ADOMs	All Packages	0.0.0.0/0.0.0.0
5	admin	LOCAL	Super_User	All ADOMs	All Packages	0.0.0.0/0.0.0.0
6	dap	LDAP Wildcard	Standard_User	FG60 fg56 fg54 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:

Create New	Create a new administrator. See Creating administrators on page 601 .
Edit	Edit the selected administrator. See Editing administrators on page 605 .
Clone	Clone the selected administrator.
Delete	Delete the selected administrator or administrators. See Deleting administrators on page 606 .
Table View/Tile View	Change the view of the administrator list. Table view shows a list of the administrators in a table format. Tile view shows a separate card for each administrator in a grid pattern.
Column Settings	Change the displayed columns.
Search	Search the administrators.
Change Password	Change the selected administrator's password. This option is only available from the right-click menu. See Editing administrators on page 605 .

The following information is shown:

Seq.#	The sequence number.
Name	The name the administrator uses to log in.
Type	The user type, as well as if the administrator uses a wildcard.
Profile	The profile applied to the administrator. See Administrator profiles on page 616
ADOMs	The ADOMs the administrator has access to or is excluded from.
Policy Packages	The policy packages the administrator can access.
Comments	Comments about the administrator account. This column is hidden by default.
Trusted IPv4 Hosts	The IPv4 trusted host(s) associated with the administrator. See Trusted hosts on page 598 .

Trusted IPv6 Hosts	The IPv6 trusted host(s) associated with the administrator. See Trusted hosts on page 598 . This column is hidden by default.
Contact Email	The contact email associated with the administrator. This column is hidden by default.
Contact Phone	The contact phone number associated with the administrator. This column is hidden by default.

Creating administrators

To create a new administrator account, you must be logged in 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 623](#) 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.

User Name	Enter the name of the administrator will use to log in.
Avatar	Apply a custom image to the administrator. Click <i>Add Photo</i> to select an image already loaded to the FortiManager, or to load an new image from the management computer. If no image is selected, the avatar will use the first letter of the user name.
Comments	Optionally, enter a description of the administrator, such as their role, location, or the reason for their account.
Admin Type	Select the type of authentication the administrator will use when logging into the FortiManager unit. One of: <i>LOCAL</i> , <i>RADIUS</i> , <i>LDAP</i> , <i>TACACS+</i> , <i>PKI</i> , or <i>Group</i> . See Authentication on page 623 for more information.

Server or Group	<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>
Match all users on remote server	<p>Select this option to automatically add all users from a LDAP server specified in <i>Admin>Remote Authentication Server</i>. All users specified in the <i>Distinguished Name</i> field in the LDAP server will be added as FortiManager users with the selected Admin Profile.</p> <p>If this option is not selected, the <i>User Name</i> specified must exactly match the LDAP user specified on the LDAP server.</p> <p>This option is not available if the <i>Admin Type</i> is <i>LOCAL</i> or <i>PKI</i>.</p>
Subject	<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>
CA	<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>
Required two-factor authentication	<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>
New Password	<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>
Confirm Password	<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>
Force this administrator to change password upon next log on.	<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 Password policy on page 635.</p>
Admin Profile	<p>Select an administrator profile from the list. The profile selected determines the administrator's access to the FortiManager unit's features. See Administrator profiles on page 616.</p>
JSON API Access	<p>Select the permission for JSON API Access. Select <i>Read-Write</i>, <i>Read</i>, or <i>None</i>. The default is <i>None</i>.</p>
Administrative Domain	<p>Choose the ADOMs this administrator will be able to access.</p> <ul style="list-style-type: none"> • <i>All ADOMs</i>: The administrator can access all the ADOMs. • <i>All ADOMs except specified ones</i>: The administrator cannot access the selected ADOMs. • <i>Specify</i>: The administrator can access the selected ADOMs. Specifying

	<p>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.</p> <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 Administrative Domains on page 552.</p>
Policy Package Access	<p>Choose the policy packages this administrator will have access to.</p> <ul style="list-style-type: none"> • <i>All Packages</i>: The administrator can access all the packages. • <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. <p>This option is only available when the <i>Admin Profile</i> is not a <i>Restricted Admin</i> profile. See Restricted administrators on page 606.</p>
Web Filter Profile	<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 & Objects > Object Configuration</i>. See Managing objects and dynamic objects on page 245.</p>
IPS Sensor	<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 & Objects > Object Configuration</i>. See Managing objects and dynamic objects on page 245.</p>
Application Sensor	<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 & Objects > Object Configuration</i>. See Managing objects and dynamic objects on page 245.</p>
Trusted Hosts	<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 Trusted hosts on page 598 for more information.</p>
Meta Fields	<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 Workflow mode on page 517.</p>
Advanced Options	<p>Configure advanced options, see Advanced options below.</p> <p>For more information on advanced options, see the <i>FortiManager CLI Reference</i>.</p>

Advanced options

Option	Description	Default
change-password	Enable or Disable changing password.	disable
ext-auth-accprofile-override	Enable or Disable overriding the account profile by administrators configured on a Remote Authentication Server.	disable
ext-auth-adom-override	Enable or Disable overriding the ADOM by administrators configured on a Remote Authentication Server.	disable
ext-auth-group-match	Specify the group configured on a Remote Authentication Server.	-
first-name	Specify the first name.	-
last-name	Specify the last name.	-
mobile-number	Specify the mobile number.	-
pager-number	Specify the pager number.	-
restrict-access	Enable or Disable restricted access.	disable

Editing administrators

To edit an administrator, you must be logged in as a super user administrator. The administrator's name cannot be edited. An administrator's password can be changed using the right-click menu, if the password is not a wildcard.

To edit an administrator:

1. Go to *System Settings > 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 16](#) 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 517](#).

When a restricted administrators logs in to the FortiManager, they enter the *Restricted Admin Mode*. This mode consists of a simplified GUI where they can make changes to the profiles that they have access to, and then install those changes using the *Install* command in the toolbar, to their designated ADOM.

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. At the bottom, there is a 'File Filter' section with checkboxes for 'Log' and 'Scan Archived Contents', and a 'File Filter Rule' table.

Category	Authenticate
Local Categories	
Potentially Liable	
Adult/Mature Content	
Bandwidth Consuming	
Security Risk	
General Interest - Personal	
General Interest - Business	
Unrated	

Category	Quota
No record found.	

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 620](#).
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 601](#)



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

Web filtering restricts or controls user access to web resources.

To create a profile:

1. Log in as a Restricted Administrator.
2. In the tree menu, select *Web Filter*, and then select a profile category.
3. In the toolbar, click *Create New*.
4. Configure the profile settings, and click *OK*.



To clone an existing profile, right-click the profile in the content pane, and select *Clone*.

To edit a profile:

1. Log in as a Restricted Administrator.
2. In the tree menu, select *Web Filter*, and then select a profile category.
3. In the content pane select a profile and take one of the following actions:
 - In the toolbar, click *Edit*.
 - Right-click the profile, and select *Edit*.
4. Edit the settings, and click *OK*.

Edit Web Filter Profile

Name: default

Comment: Default web filtering. 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	Configure advanced options, including: <ul style="list-style-type: none">• <i>https-replacemsg</i>: enable/disable• <i>replacemsg-group</i>: select a group from the list• <i>web-filter-activex-log</i>: enable/disable• <i>web-filter-command-block-log</i>: enable/disable• <i>web-filter-cookie-removal-log</i>: enable/disable• <i>web-filter-js-log</i>: enable/disable• <i>web-filter-jscript-log</i>: enable/disable• <i>web-filter-referrer-log</i>: enable/disable• <i>web-filter-unknown-log</i>: enable/disable• <i>web-filter-vbs-log</i>: enable/disable

	<ul style="list-style-type: none"> • <i>wisp</i>: enable/disable • <i>wisp-algorithm</i>: <i>auto-learning</i>, <i>primary-secondary</i>, or <i>round-robin</i>
Inspection Mode	Select <i>Proxy</i> or <i>Flow Based</i> .
Log all URLs	Select to log all URLs.
FortiGuard Categories	<p>Select FortiGuard categories.</p> <p>Right-click on a category to change the action: <i>Allow</i>, <i>Block</i>, <i>Warning</i>, <i>Monitor</i>, <i>Authenticate</i>, or, if available, <i>Disable</i>.</p> <p>Use the filter drop-down menu to filter the categories shown in the table based on the action.</p>
Allow Users to override blocked categories	<p>Select to allow users to override blocked categories.</p> <p>This option is only available if <i>Inspection Mode</i> is <i>Proxy</i>.</p>
Override Permit	Select the override permits: <i>bannedword-override</i> , <i>contenttype-check-override</i> , <i>fortiguard-wf-override</i> , and <i>urlfilter-override</i> .
Groups that can override	Select groups that can override blocked categories.
Profile can switch to	Select profiles that the user can switch to.
Switch applies to	Select what the switch applies to: <i>ask</i> , <i>browser</i> , <i>ip</i> , <i>user</i> , or <i>user-group</i> .
Switch Duration	Select the switch duration, either <i>ask</i> or <i>constant</i> .
Duration	<p>Enter the duration of the switch.</p> <p>This option is only available if <i>Switch Duration</i> is <i>constant</i>.</p>
Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex	<p>Select to enforce <i>Safe Search</i>.</p> <p>This option is only available if <i>Inspection Mode</i> is <i>Proxy</i>.</p>
Restrict YouTube Access	<p>Select to restrict access to YouTube. Select <i>Strict</i> or <i>Moderate</i>.</p> <p>This option is only available if <i>Inspection Mode</i> is <i>Proxy</i>.</p>
Log all search keywords	<p>Select to log all search keywords.</p> <p>This option is only available if <i>Inspection Mode</i> is <i>Proxy</i>.</p>
Block Invalid URLs	<p>Select to block invalid URLs.</p> <p>This option is only available if <i>Inspection Mode</i> is <i>Proxy</i>.</p>
URL Filter	<p>Select to enable URL filters.</p> <p>Select URL filters from the dropdown list, and/or create and manage filters in the table.</p>
Block malicious URLs discovered by FortiSandbox	Select to block URLs that FortiSandbox deems malicious.
Web Content Filter	Select to apply web content filters. Click <i>Add</i> to add filters to the table. Edit and delete filters as required.

Allow Websites When a Rating Error Occurs	Select to allow access to websites if a rating error occurs.
Rate URLs by Domain and IP Address	Select to rate URLs by both their domain and IP address.
Block HTTP Redirects by Rating	Select to block HTTP redirects based on the site's rating. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
Rate Images by URL (Blocked images will be replaced with blanks)	Select to rate images based on the URL. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
Restrict Google account usage to specific domains	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> .
Provide Details for Blocked HTTP 4xx and 5xx Errors	Select to receive details about blocked HTTP errors. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
HTTP POST Action: Block	Select to set the HTTP POST action to block. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
Remove Java Applet Filter	Select to remove the Java applet filter. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
Remove ActiveX Filter	Select to remove the ActiveX filter. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
Remove Cookie Filter	Select to remove the cookie filter. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .

Intrusion Prevention

Use intrusion prevention to detect and block network-based attacks.

To create a profile:

1. Log in as a Restricted Administrator.
2. In the tree menu, select *Intrusion Prevention*, and then select a profile category.
3. In the toolbar, click *Create New*.
4. Configure the profile settings, and click *OK*.



To clone an existing profile, right-click the profile in the content pane, and select *Clone*.

To edit a profile:

1. Log in as a Restricted Administrator.
2. In the tree menu, select *Intrusion Prevention*, and then select a profile category.

3. In the content pane, select a profile, and take one of the following actions:

- In the toolbar, click *Edit*.
- Right-click the profile, and select *Edit*.

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

Edit 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.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*.

	<p>Right-click on a signature to change the action (<i>Pass</i>, <i>Monitor</i>, <i>Block</i>, <i>Reset</i>, <i>Default</i>, or <i>Quarantine</i>), and to enable or disable <i>Packet Logging</i>.</p> <p>The CVE ID filter allows you to filter IPS signatures based on CVE IDs or with a CVE wildcard, ensuring that any signatures tagged with that CVE are automatically included.</p> <p>You can delay new signatures to avoid false positives. Signatures that are on hold will be set to <i>Monitor</i> rather than being disabled. If the signature is matched, the message <i>Signature is on hold</i>, is appended to the log.</p>
IPS Filters	<p>Click <i>Add Filter</i> to add IPS filters to the table. The filters list can be searched and filtered to simplify adding them.</p> <p>Right-click on a signature to change the action (<i>Pass</i>, <i>Monitor</i>, <i>Block</i>, <i>Reset</i>, <i>Default</i>, or <i>Quarantine</i>), and to enable or disable <i>Packet Logging</i>.</p>
Rate Based Signatures	Enable the required rate based signatures, then configure its options: <i>Threshold</i> , <i>Duration</i> , <i>Track By</i> , <i>Action</i> , and <i>Block Duration</i> .
Advanced Options	Enable or disable blocking malicious URLs.

To add an IPS CVE filter:

1. Log in as a Restricted Administrator.
2. Go to *Intrusion Prevention > Profiles*.
3. Create a new profile or select the profile you want to update.
4. In the *IPS Signatures and Filters* section, create a new filter or select a filter to update. The *Create New IPS Signatures and Filters* dialog box is displayed.
5. Add the CVE filter.
 - a. Click the *Filter* icon.
 - b. Click *Add Filter > CVE ID*.
 - c. Enter the CVE ID, then click *Use Filters*, and click *OK*.
6. Click *OK*.

To delay an IPS signature activation:

1. Log in as a Restricted Administrator.
2. Go to *Device Manager > Device & Groups*.
3. Select a managed device.
4. In the toolbar, click *CLI Configuration*. To display the menu, see [CLI Configurations menu on page 70](#).
5. In configurations menu, go to *System > IPS*. The *system ips* dialog box is displayed.
6. Ensure *override-signature-hold-by-id* is enabled.
7. In the *signature-hold-time* field, enter the number of days or hours hold and monitor the IPS signatures. For example, *1d12h*

Application Control

Application control sensors specify what action to take with network traffic generated by a large number of applications.

To create a profile:

1. Log in as a Restricted Administrator.
2. In the tree menu, select *Application Control*, and then select a profile category.
3. In the toolbar, click *Create New*.
4. Configure the profile settings, and click *OK*.



To clone an existing profile, right-click the profile in the content pane, and select *Clone*.

To edit a profile:

1. Log in as a Restricted Administrator.
2. In the tree menu, select *Application Control*, and then select a profile category.
3. In the content pane select a profile, and take one of the following actions:
 - In the toolbar, click *Edit*.
 - Right-click the profile, and select *Edit*.
4. Edit the settings, and click *OK*.

Edit Application Control Profile

Name: default

Comments: Monitor all applications. 25/255

Categories

Monitor Botnet	Monitor Game	Monitor Proxy	Monitor Video/Audio
Monitor Business	Monitor General Interest	Monitor Remote Access	Monitor VoIP
Monitor Cloud.IT	Monitor Mobile	Monitor Social Media	Monitor Industrial
Monitor Collaboration	Monitor Network Service	Monitor Storage Backup	Monitor Web Client
Monitor Email	Monitor P2P	Monitor Update	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 >

Apply

Name	The profile name.
Comment	Optionally, enter a description of the profile.
Categories	Select the action to take for each of the available categories: <i>Allow</i> , <i>Monitor</i> , <i>Block</i> , <i>Traffic Shaping</i> , <i>Quarantine</i> , or <i>Reset</i> .
Application Overrides	Click <i>Add Signatures</i> 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 (<i>Allow</i> , <i>Monitor</i> , <i>Block</i> , <i>Traffic Shaping</i> , <i>Quarantine</i> , or <i>Reset</i>).
Filter Overrides	Click <i>Add Filter</i> 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 (<i>Allow</i> , <i>Monitor</i> , <i>Block</i> , <i>Traffic Shaping</i> , <i>Quarantine</i> , or <i>Reset</i>).
Deep Inspection of Cloud Applications	Select to enable deep inspections of cloud applications.
Allow and Log DNS Traffic	Select to allow and log DNS traffic.
Replacement Messages for HTTP-based Applications	Select to enable replacement messages for HTTP based applications.
Logging of Other Applications	Select to enable the logging of other applications.
Logging of Unknown Applications	Select to enable the logging of unknown applications.
Advanced Options	Configure advanced options: <ul style="list-style-type: none"> p2p-block-list: Select from <i>bittorent</i>, <i>edonkey</i>, and <i>skype</i>. replacemsg-group: Select an option from the dropdown list.

Installing profiles

Restricted administrators can install the profiles they can access to their designated devices. Administrators can also view where a profile is used.



Restricted administrators must have *Allow to Install* enabled to install a profile. See [Creating administrator profiles on page 620](#).

To view where a profile is used:

1. Log in as a Restricted Administrator.
2. In the tree menu, select a profile.
3. In the content pane, right-click a profile, and select *Where Used*.
4. Click *Close*.

To install a profile:



Use this option to install a modified profile to specified devices, such as a test environment.

1. Log in as a Restricted Administrator.
2. In the tree menu, select a profile.
3. In the content pane, right-click a profile, and select *Install*. The *Select Installation Targets* window opens.

4. In the *Available Entries* pane, double-click a device to add it to the *Selected Entries* pane.
5. Click *OK*. The *Install* window opens and a progress bar appears at the top of the page.
6. Click *Close*.

To install all modified profiles:

1. Log in as a Restricted Administrator.
2. At the top-left side of the page, click *Quick Install*
3. Click *OK*. The *Install* window opens and a progress bar appears at the top of the page.
4. Click *Close*.

Administrator profiles

Administrator profiles are used to control administrator access privileges to devices or system features. Profiles are assigned to administrator accounts when an administrator is created. The profile controls access to both the FortiManager GUI and CLI.

There are four predefined system profiles:

Restricted_User	Restricted user profiles have no system privileges enabled, and have read-only access for all device privileges.
Standard_User	Standard user profiles have no system privileges enabled, and have read/write access for all device privileges.
Super_User	Super user profiles have all system and device privileges enabled. It cannot be edited.
Package_User	Package user profile have read/write policy and objects privileges enabled, and have read-only access for system and other privileges.

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:

Create New	Create a new administrator profile. See Creating administrator profiles on page 620 .
Edit	Edit the selected profile. See Editing administrator profiles on page 623 .
Clone	Clone the selected profile. See Cloning administrator profiles on page 623 .
Delete	Delete the selected profile or profiles. See Deleting administrator profiles on page 623 .
Search	Search the administrator profiles list.

The following information is shown:

Name	The name the administrator uses to log in.
Type	The profile type, either <i>System Admin</i> or <i>Restricted Admin</i> .
Description	A description of the system and device access permissions allowed for the selected profile.

Permissions

The below table lists the default permissions for the 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
System Settings system-setting	Read-Write	None	None	Read-Only
Administrative Domain adom-switch	Read-Write	Read-Write	None	Read-Write
FortiGuard Center fgd_center	Read-Write	None	None	Read-Only
License Management fgd-center-licensing	Read-Write	None	None	Read-Only
Firmware Management fgd-center-fmw-mgmt	Read-Write	None	None	Read-Only
Advanced	Read-Write	None	None	Read-Only

Setting	Predefined Administrator Profile			
	Super User	Standard User	Restricted User	Package User
fgd-center-advanced				
Device Manager device-manager	Read-Write	Read-Write	Read-Only	Read-Write
Add/Delete/Edit Devices/Groups device-op	Read-Write	Read-Write	None	Read-Write
Retrieve Configuration from Devices config-retrieve	Read-Write	Read-Write	Read-Only	Read-Only
Revert Configuration from Revision History config-revert	Read-Write	Read-Write	Read-Only	Read-Only
Delete Device Revision device-revision-deletion	Read-Write	Read-Write	Read-Only	Read-Write
Terminal Access term-access	Read-Write	Read-Write	Read-Only	Read-Only
Manage Device Configurations device-config	Read-Write	Read-Write	Read-Only	Read-Write
Provisioning Templates device-profile	Read-Write	Read-Write	Read-Only	Read-Write
SD-WAN device-wan-link-load-balance	Read-Write	Read-Write	Read-Only	Read-Write
Policy & Objects policy-objects	Read-Write	Read-Write	Read-Only	Read-Write
Global Policy Packages & Objects global-policy-packages	Read-Write	Read-Write	None	Read-Write
Assignment assignment	Read-Write	None	None	Read-Only

Setting	Predefined Administrator Profile			
	Super User	Standard User	Restricted User	Package User
Policy Packages & Objects adom-policy-packages	Read-Write	Read-Write	Read-Only	Read-Write
Policy Check consistency-check	Read-Write	Read-Write	Read-Only	Read-Only
Edit Installation Targets set-install-targets	Read-Write	Read-Write	Read-Only	Read-Write
Lock/Unlock ADOM adom-lock	Read-Write	Read-Write	Read-Only	Read-Write
Lock/Unlock Device/Policy Package device-policy-package-lock	Read-Write	Read-Write	Read-Only	Read-Write
Install Policy Package or Device Configuration deploy-management	Read-Write	Read-Write	Read-Only	Read-Write
Import Policy Package import-policy-packages	Read-Write	Read-Write	Read-Only	Read-Write
Interface Mapping intf-mapping	Read-Write	Read-Write	Read-Only	Read-Write
AP Manager device-ap	Read-Write	Read-Write	Read-Only	Read-Write
FortiClient Manager device-forticlient	Read-Write	Read-Write	Read-Only	Read-Write
FortiSwitch Manager device-fortiswitch	Read-Write	Read-Write	Read-Only	Read-Write
VPN Manager vpn-manager	Read-Write	Read-Write	Read-Only	Read-Write
FortiView log-viewer	Read-Write	Read-Write	Read-Only	Read-Only
Log View/FortiView log-viewer	Read-Write	Read-Write	Read-Only	Read-Only
Incidents & Events	Read-Write	Read-Write	Read-Only	Read-Only

Setting	Predefined Administrator Profile			
	Super User	Standard User	Restricted User	Package User
event-management				
Reports	Read-Write	Read-Write	Read-Only	Read-Only
report-viewer				
CLI only settings				
realtime-monitor	Read-Write	Read-Write	Read-Only	Read
read-passwd	Read-Write	None	None	Read-Only



The *FortiView* setting is only available when FortiAnalyzer features are disabled. The *Log View/FortiView*, *Incidents & Events*, and *Reports* settings are only available when FortiAnalyzer features are enabled. See [FortiAnalyzer Features on page 20](#).

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:

Profile Name	Enter a name for this profile.
Description	Optionally, enter a description for this profile. While not a requirement, a description can help to know what the profiles is for, or the levels it is set to.
Type	Select the type of profile, either <i>System Admin</i> or <i>Restricted Admin</i> .
Permission	Select which permissions to enable from <i>Web Filter</i> , <i>Application Control</i> , and <i>Intrusion Prevention</i> . This option is only available when <i>Type</i> is <i>Restricted Admin</i> . See Restricted administrators on page 606 for information.
Allow to Install	Allows restricted administrators to install Web Filters, Intrusion Prevention, and Application Control profiles. See Installing profiles on page 615 .
Permissions	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> .
Privacy Masking	Enable/disable privacy masking. This option is only available when FortiAnalyzer features are enabled.
Masked Data Fields	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> .
Data Mask Key	Enter the data masking encryption key. You need the <i>Data Mask Key</i> to see the original data.
Data Unmasked Time(0-365 Days)	Enter the number of days the user assigned to this profile can see all logs without masking. The logs are masked if the time period in the <i>Log View</i> toolbar is greater than the number of days in the <i>Data Masked Time</i> field.
	 <ul style="list-style-type: none"> • Only integers between 0-365 are supported. • Time frame masking does not apply to real time logs. • Time frame masking applies to custom view and drill-down data.

4. Click *OK* to create the new administrator profile.**To apply a profile to an administrator:**

1. Go to *System Settings > Administrators*.
2. Create a new administrator or edit an existing administrator. The *Edit Administrator* pane is displayed.

3. From the *Admin Profile* list, select a profile.

Editing administrator profiles

To edit an administrator profile, you must be logged in to an account with sufficient privileges, or as a super user administrator. The profile's name cannot be edited. The *Super_User* profile cannot be edited, and the predefined profiles cannot be deleted.

To edit an administrator:

1. Go to *System Settings > Admin > 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 624](#) 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 626](#), [RADIUS servers on page 628](#), [TACACS+ servers on page 630](#), and [Remote authentication server groups on page 630](#) 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 FortiManager.
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 FortiManager.
2. Go to *Certificate Management > End Entities > Users*.
3. Select the certificate and select *Export* in the toolbar to save the administrator certificate to your management computer. The saved CA certificate's filename is `admin_fortinet.com.p12`. This PKCS#12 file is password protected. You must enter a password on export.

To import the administrator certificate into your browser:

1. In Mozilla Firefox, go to *Options > Advanced > Certificates > View Certificates > Import*.
2. Select the file `admin_fortinet.com.p12` and enter the password used in the previous step.

To import the CA certificate into the FortiManager:

1. Log into your FortiManager.
2. Go to *System Settings > Certificates > CA Certificates*.
3. Click *Import*, and browse for the `ca_fortinet.com.crt` file you saved to your management computer, or drag and drop the file onto the dialog box. The certificate is displayed as `CA_Cert_1`.

To create a new PKI administrator account:

1. Go to *System Settings > Admin > Administrator*.
2. Click *Create New*. The *New Administrator* dialog box opens.
See [Creating administrators on page 601](#) for more information.
3. Select *PKI* for the *Admin Type*.
4. Enter a comment in the *Subject* field for the PKI administrator.
5. Select the CA certificate from the dropdown list in the *CA* field.
6. Click *OK* to create the new administrator account.



PKI authentication must be enabled via the FortiManager CLI with the following commands:

```
config system global
    set clt-cert-req enable
end
```



When connecting to the FortiManager GUI, you must use HTTPS when using PKI certificate authentication.



When `clt-cert-req` is set to optional, the user can use certificate authentication or user credentials for GUI login.

Managing remote authentication servers

The FortiManager system supports remote authentication of administrators using LDAP, RADIUS, and TACACS+ remote servers. To use this feature, you must configure the appropriate server entries for each authentication server in your network, see [LDAP servers on page 626](#), [RADIUS servers on page 628](#), and [TACACS+ servers on page 630](#) 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:

Create New

Add an LDAP, RADIUS, or TACACS+ remote authentication server. See [LDAP servers on page 626](#), [RADIUS servers on page 628](#), and [TACACS+ servers on page 630](#).

Edit	Edit the selected remote authentication server. See Editing remote authentication servers on page 626 .
Delete	Delete the selected remote authentication server or servers. See Deleting remote authentication servers on page 626 .

The following information is displayed:

Name	The name of the server.
Type	The server type: <i>LDAP</i> , <i>RADIUS</i> , or <i>TACACS+</i> .
ADOM	The administrative domain(s) which are linked to the remote authentication server.
Details	Details about the server, such as the IP address.

Editing remote authentication servers

To edit a remote authentication server, you must be logged in to an account with sufficient privileges, or as a super user administrator. The server's name cannot be edited.

To edit a remote authentication server:

1. Go to *System Settings > 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 626](#), [RADIUS servers on page 628](#), and [TACACS+ servers on page 630](#) 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.

3. Configure the following settings, and then click *OK* to add the LDAP server.

Name	Enter a name to identify the LDAP server.
Server Name/IP	Enter the IP address or fully qualified domain name of the LDAP server.
Port	Enter the port for LDAP traffic. The default port is 389.
Common Name Identifier	The common name identifier for the LDAP server. Most LDAP servers use <i>cn</i> . However, some servers use other common name identifiers such as <i>UID</i> .
Distinguished Name	The distinguished name is used to look up entries on the LDAP server. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier. Clicking the <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.
Bind Type	Select the type of binding for LDAP authentication: <i>Simple</i> , <i>Anonymous</i> , or <i>Regular</i> .
User DN	When the <i>Bind Type</i> is set to <i>Regular</i> , enter the user DN.
Password	When the <i>Bind Type</i> is set to <i>Regular</i> , enter the password.
Secure Connection	Select to use a secure LDAP server connection for authentication.
Protocol	When <i>Secure Connection</i> is enabled, select either LDAPS or STARTTLS.

Certificate	When <i>Secure Connection</i> is enabled, select the certificate from the dropdown list.
Administrative Domain	Choose the ADOMs that this server will be linked to for reporting: <i>All ADOMs</i> (default), or <i>Specify</i> for specific ADOMs.
Advanced Options	
adom-attr	Specify an attribute for the ADOM.
attributes	Specify the attributes such as <i>member</i> , <i>uniquemember</i> , or <i>memberuid</i> .
connect-timeout	Specify the connection timeout in millisecond.
filter	Specify the filter in the format <code>(objectclass=*)</code>
group	Specify the name of the LDAP group.
memberof-attr	Specify the value for this attribute. This value must match the attribute of the group in LDAP Server. All users part of the LDAP group with the attribute matching the <i>memberof-attr</i> will inherit the administrative permissions specified for this group.
profile-attr	Specify the attribute for this profile.
secondary-server	Specify a secondary server.
tertiary-server	Specify a tertiary server.

RADIUS servers

Remote Authentication Dial-in User (RADIUS) is a user authentication and network-usage accounting system. When users connect to a server they type a user name and password. This information is passed to a RADIUS server, which authenticates the user and authorizes access to the network.

You can create or edit RADIUS server entries in the server list to support authentication of administrators. When an administrator account's type is set to RADIUS, the FortiManager unit uses the RADIUS server to verify the administrator password at log on. The password is not stored on the FortiManager unit.

To use a RADIUS server to authenticate administrators, you must configure the server before configuring the administrator accounts that will use it.

To add a RADIUS server:

1. Go to *System Settings > Admin > Remote Authentication Server*.
2. Select *Create New > RADIUS Server* from the toolbar. The *New RADIUS Server* pane opens.

Name	<input type="text" value="test-Radius"/>
Server Name/IP	<input type="text" value="10.2.0.159"/>
Port	<input type="text" value="1812"/>
Server Secret	<input type="password" value="*****"/>
Connection Status	✔ Successful <input type="button" value="Test Connectivity"/> <input type="button" value="Test User Credentials"/>
Secondary Server Name/IP	<input type="text"/>
Secondary Server Secret	<input type="password" value="*****"/>
	<input type="button" value="Test Connectivity"/> <input type="button" value="Test User Credentials"/>
Authentication Type	<input type="text" value="ANY"/>
Advanced Options >	

OK

Cancel

3. Configure the following settings, and then click *OK* to add the RADIUS server.

Name	Enter a name to identify the RADIUS server.
Server Name/IP	Enter the IP address or fully qualified domain name of the RADIUS server.
Port	Enter the port for RADIUS traffic. The default port is 1812. Some RADIUS servers use port 1645.
Server Secret	Enter the RADIUS server secret. Click the eye icon to Show or Hide the server secret.
Test Connectivity	Click <i>Test Connectivity</i> to test the connectivity with the RADIUS server. Shows success or failure.
Test User Credentials	Click <i>Test User Credentials</i> to test the user credentials. Shows success or failure.
Secondary Server Name/IP	Enter the IP address or fully qualified domain name of the secondary RADIUS server.
Secondary Server Secret	Enter the secondary RADIUS server secret.
Authentication Type	Select the authentication type the RADIUS server requires. If you select the default <i>ANY</i> , FortiManager tries all authentication types.
Advanced Options	
nas-ip	Specify the IP address for the Network Attached Storage (NAS).

TACACS+ servers

Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol that provides access control for routers, network access servers, and other network computing devices via one or more centralized servers. It allows a client to accept a user name and password and send a query to a TACACS authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies network access to the user. The default TCP port for a TACACS+ server is 49.

If you have configured TACACS+ support and an administrator is required to authenticate using a TACACS+ server, the FortiManager unit contacts the TACACS+ server for authentication. If the TACACS+ server can authenticate the administrator, they are successfully authenticated with the FortiManager unit. If the TACACS+ server cannot authenticate the administrator, the connection is refused by the FortiManager unit.

To use a TACACS+ server to authenticate administrators, you must configure the server before configuring the administrator accounts that will use it.

To add a TACACS+ server:

1. Go to *System Settings > Admin > Remote Authentication Server*.
2. Select *Create New > TACACS+ Server* from the toolbar. The *New TACACS+ Server* pane opens.

3. Configure the following settings, and then click **OK** to add the TACACS+ server.

Name	Enter a name to identify the TACACS+ server.
Server Name/IP	Enter the IP address or fully qualified domain name of the TACACS+ server.
Port	Enter the port for TACACS+ traffic. The default port is 49.
Server Key	Enter the key to access the TACACS+ server. The server key can be a maximum of 16 characters in length.
Authentication Type	Select the authentication type the TACACS+ server requires. If you select the default <i>ANY</i> , FortiManager tries all authentication types.

Remote authentication server groups

Remote authentication server groups can be used to extend wildcard administrator access. Normally, a wildcard administrator can only be created for a single server. If multiple servers of different types are grouped, a wildcard administrator can be applied to all of the servers in the group.

Multiple servers of the same type can be grouped to act as backups - if one server fails, the administrator can still be authenticated by another server in the group.

To use a server group to authenticate administrators, you must configure the group before configuring the administrator accounts that will use it.

Remote authentication server groups can only be managed using the CLI. For more information, see the [FortiManager CLI Reference](#).

To create a new remote authentication server group:

1. Open the admin group command shell:
`config system admin group`
2. Create a new group, or edit an already create group:
`edit <group name>`
3. Add remote authentication servers to the group:
`set member <server name> <server name> ...`
4. Apply your changes:
`end`

To edit the servers in a group:

1. Enter the following CLI commands:
`config system admin group`
`edit <group name>`
`set member <server name> <server name> ...`
`end`
Only the servers listed in the command will be in the group.

To remove all the servers from the group:

1. Enter the following CLI commands:
`config system admin group`
`edit <group name>`
`unset member`
`end`
All of the servers in the group will be removed.

To delete a group:

1. Enter the following CLI commands:
`config system admin group`
`delete <group name>`
`end`

SAML admin authentication

SAML can be enabled across devices, enabling smooth movement between devices for the administrator. FortiManager can play the role of the identity provider (IdP) or the service provider (SP) when an external identity provider is available.

Devices configured to the IdP can be accessed through the Quick Access menu which appears in the top-right corner of the main menu. The current device is indicated with an asterisk (currently only supported between FAZ/FMG).

Logging into an SP device will redirect you to the IdP login page. By default, it is a Fortinet login page. After successful authentication, you can access other SP devices from within the same browser without additional authentication.



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)

☒ Redirects to HTTPS

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

HTTP Port	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.
HTTPS Port	Enter the TCP port to be used for administrative HTTPS access. Default: 443.
HTTPS & Web Service Server Certificate	Select a certificate from the dropdown list.

Idle Timeout	Enter the number of minutes an administrative connection can be idle before the administrator must log in again, from 1 to 480 (8 hours). See Idle timeout on page 636 for more information.
---------------------	--

View Settings

Language	Select a language from the dropdown list. See GUI language on page 636 for more information.
Theme	Select a theme for the GUI. The selected theme is not applied until you click <i>Apply</i> , allowing you to sample different themes. Default: Blueberry.

Password Policy	Click to enable administrator password policies. See Password policy on page 635 and Password lockout and retry attempts on page 635 for more information.
------------------------	--

Minimum Length	Select the minimum length for a password, from 8 to 32 characters. Default: 8.
Must Contain	Select the types of characters a password must contain.

Admin Password Expires after	Select the number of days a password is valid for, after which it must be changed.
Display Options on GUI	Click to expand the display options.
Show Script	Display the <i>Script</i> menu item. This menu is located on the <i>Device Manager</i> pane. This is an advanced FortiManager feature.
Show Add Multiple Button	Display the <i>Add Multiple Devices</i> option. This option is located on the <i>Device Manager > Devices & Groups</i> pane, under the <i>More</i> option in the toolbar. This is an advanced FortiManager feature.
Show Device List Import/Export	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 > Devices & 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.

Minimum Length	Specify the minimum number of characters that a password must be, from 8 to 32. Default: 8.
Must Contain	Specify the types of characters a password must contain: uppercase and lowercase letters, numbers, and/or special characters.
Admin Password Expires after	Specify the number of days a password is valid for. When the time expires, an administrator will be prompted to enter a new password.

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:

Username	Enter a user name for the local user.
Password creation	Select Specify a password from the dropdown list.
Password	Enter a password. The password must be a minimum of 8 characters.
Password confirmation	Re-enter the password. The passwords must match.
Allow RADIUS authentication	Enable to allow RADIUS authentication.
Role	Select the role for the new user.
Enable account expiration	Optionally, select to enable account expiration. For more information see the <i>FortiAuthenticator Administration Guide</i> .

4. Click **OK** to continue to the *Change local user* page.

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

Disabled	Select to disable the local user.
Password-based authentication	Leave this option selected. Select <i>[Change Password]</i> to change the password for this local user.
Token-based authentication	Select to enable token-based authentication.
Deliver token code by	Select to deliver token by FortiToken, email, or SMS. Click <i>Test Token</i> to test the token.
Allow RADIUS authentication	Select to allow RADIUS authentication.
Enable account expiration	Optionally, select to enable account expiration. For more information see the <i>FortiAuthenticator Administration Guide</i> .
User Role	
Role	Select either <i>Administrator</i> or <i>User</i> .
Full Permission	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> .
Web service	Select to allow Web service, which allows the administrator to access the web service via a REST API or by using a client application. This option is only available when <i>Role</i> is <i>Administrator</i> .
Restrict admin login from trusted management subnets only	Select to restrict admin login from trusted management subnets only, then enter the trusted subnets in the table. This option is only available when <i>Role</i> is <i>Administrator</i> .
Allow LDAP Browsing	Select to allow LDAP browsing. This option is only available when <i>Role</i> is <i>User</i> .

Create a RADIUS client:

1. Go to *Authentication > RADIUS Service > Clients*.
2. Click *Create New* in the toolbar.

3. Configure the following settings, then click **OK**.

Name	Enter a name for the RADIUS client entry.
Client name/IP	Enter the IP address or Fully Qualified Domain Name (FQDN) of the FortiManager.
Secret	Enter the server secret. This value must match the FortiManager RADIUS server setting at <i>System Settings > Admin > Remote Authentication Server</i> .
First profile name	See the <i>FortiAuthenticator Administration Guide</i> .
Description	Enter an optional description for the RADIUS client entry.
Apply this profile based on RADIUS attributes	Select to apply the profile based on RADIUS attributes.
Authentication method	Select <i>Enforce two-factor authentication</i> from the list of options.
Username input format	Select specific user name input formats.
Realms	Configure realms.
Allow MAC-based authentication	Optional configuration.
Check machine authentication	Select to check machine based authentication and apply groups based on the success or failure of the authentication.
Enable captive portal	Enable various portals.
EAP types	Optional configuration.



For more information, see the *FortiAuthenticator Administration Guide*, available in the [Fortinet Document Library](#).

Configuring FortiManager

On the FortiManager, you need to configure the RADIUS server and create an administrator that uses the RADIUS server for authentication.

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**.

Name	Enter a name to identify the FortiAuthenticator.
Server Name/IP	Enter the IP address or fully qualified domain name of your FortiAuthenticator.
Server Secret	Enter the FortiAuthenticator secret.

Secondary Server Name/IP	Enter the IP address or fully qualified domain name of the secondary FortiAuthenticator, if applicable.
Secondary Server Secret	Enter the secondary FortiAuthenticator secret, if applicable.
Port	Enter the port for FortiAuthenticator traffic.
Authentication Type	Select the authentication type the FortiAuthenticator requires. If you select the default <i>ANY</i> , FortiManager tries all authentication types. Note: 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 601](#).
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 five units: one primary unit with up to four backup or secondary units. All units in the cluster must be of the same FortiManager series. All units are visible on the network.

The primary unit and the secondary units can be in the same location or different locations. FortiManager HA supports geographic redundancy so the primary unit and secondary units can be in different locations attached to different networks as long as communication is possible between them (for example, on the Internet, on a WAN, or in a private network).

Administrators connect to the primary unit GUI or CLI to perform FortiManager operations. Managed devices connect with the primary unit for normal management operations (configuration push, auto-update, firmware upgrade, and so on). If FortiManager is used to distribute FortiGuard updates to managed devices, managed devices can connect to the primary FortiManager unit or one of the secondary units.

If the primary FortiManager unit fails you must manually configure one of the secondary units to become the primary unit. The new primary unit will keep its IP address. FortiManager's IP address registered on FortiGate will be automatically changed when 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 FortiManager *Primary* and *Secondary* units both have FortiAnalyzer features enabled on them, all the FortiAnalyzer features available on the *Primary* unit are also available on the *Secondary* unit.



When devices with different licenses are used to create an HA cluster, the license that allows for the smallest number of managed devices is used.

Synchronizing the FortiManager configuration and HA heartbeat

All changes to the FortiManager database are saved on the primary unit, and then these changes are synchronized to the backup units. The FortiManager configuration of the primary unit is also synchronized to the backup units, except for

the following settings:

- Hostname
- System time and NTP server
- FortiCloud
- FortiGuard database downloaded by FortiManager
- Network
- HA
- Local certificates
- SNMP
- Mail server
- Syslog server
- FortiGuard settings (FortiManager CM database also known as CMDB)

Aside from these settings, the backup units always match the primary unit. So if the primary unit fails, a backup unit can be configured to take the place of the primary unit and continue functioning as a standalone FortiManager unit.

While the FortiManager cluster is operating, all backup units in the cluster exchange HA heartbeat packets with the primary unit so the primary unit can verify the status of the backup units and the backup units can verify the status of the primary unit. The HA heartbeat packets use TCP port 5199. HA heartbeat monitoring, as well as FortiManager database and configuration synchronization takes place using the connections between the FortiManager units in the cluster. As part of configuring the primary unit you add peer IPs and peer serial numbers of each of the backup FortiManager units in the cluster. You also add the peer IP of the primary unit and the primary unit serial number to each of the backup units.



Depending on the peer IPs that you use, you can isolate HA traffic to specific FortiManager interfaces and connect those interfaces together so they function as synchronization interfaces between the FortiManager units in the cluster. Communication between the units in the cluster must be maintained for the HA cluster to operate.

The interfaces used for HA heartbeat and synchronization communication can be connected to your network. However, if possible you should isolate HA heartbeat and synchronization packets from your network to save bandwidth.

If the primary or a backup unit fails

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. For settings that are not synchronized, you must configure the settings on each cluster unit. For a list of settings not synchronized, see [Synchronizing the FortiManager configuration and HA heartbeat on page 641](#).

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:

Cluster Status	Monitor FortiManager HA status. See Monitoring HA status on page 647 .
SN	The serial number of the device.
Mode	The high availability mode, either <i>Primary</i> or <i>Secondary</i> .
IP	The IP address of the device.
Enable	Shows if the peer is currently enabled.
Module Data Synchronized	Module data synchronized in bytes.
Pending Module Data	Pending module data in bytes.
Cluster Settings	

Operation Mode	<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>
Peer IP	<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>
Peer SN	Type the serial number of the FortiManager unit corresponding to the entered IP address.
Cluster ID	A number between 1 and 64 that identifies the HA cluster. All members of the HA cluster must have the same cluster ID. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different cluster ID. The FortiManager GUI browser window title changes to include the cluster ID when FortiManager unit is operating in HA mode.
Group Password	<p>A password for the HA cluster. All members of the HA cluster must have the same password.</p> <p>If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different password. The maximum password length is 19 characters.</p>
File Quota	<p>Enter the file quota, from 2048 to 20480 MB (default: 4096 MB).</p> <p>You cannot configure the file quota for backup units.</p>
Heart Beat Interval	<p>The time the primary unit waits between sending heartbeat packets, in seconds. The heartbeat interval is also the amount of time that backup units waits before expecting to receive a heartbeat packet from the primary unit.</p> <p>The default heartbeat interval is 5 seconds. The heartbeat interval range is 1 to 255 seconds. You cannot configure the heartbeat interval on the backup units.</p>
Failover Threshold	<p>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.</p> <p>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.</p>

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.

Download Debug Log

Select to download the HA debug log file to the management computer.

General FortiManager HA configuration steps

1. Configure the FortiManager units for HA operation:
 - Configure the primary unit.
 - Configure the backup units.
2. Change the network configuration so the remote backup unit and the primary unit can communicate with each other.
3. Connect the units to their networks.
4. Add basic configuration settings to the cluster:
 - Add a password for the admin administrative account.
 - Change the IP address and netmask of the port1 interface.
 - Add a default route.

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:

Operation Mode	Primary
Peer IP	172.20.120.23
Peer SN	<serial_number>

Peer IP	192.268.34.23
Peer SN	<serial_number>
Cluster ID	15
Group Password	password
File Quota	4096
Heartbeat Interval	5 (Keep the default setting.)
Failover Threshold	3 (Keep the default setting.)

4. Click *Apply*.

To configure the backup unit on the same network for HA operation:

1. Connect to the backup unit GUI.
2. Go to *System Settings > HA*.
3. Configure HA settings.

Example local backup configuration:

Operation Mode	Secondary
Priority	5 (Keep the default setting.)
Peer IP	172.20.120.45
Peer SN	<serial_number>
Cluster ID	15
Group Password	password
File Quota	4096
Heartbeat Interval	5 (Keep the default setting.)
Failover Threshold	3 (Keep the default setting.)

4. Click *Apply*.

To configure a remote backup unit for HA operation:

1. Connect to the backup unit GUI.
2. Go to *System Settings > HA*.
3. Configure HA settings.

Example remote backup configuration:

Operation Mode	Secondary
Priority	5 (Keep the default setting.)
Peer IP	192.168.20.23
Peer SN	<serial_number>

Cluster ID	15
Group Password	password
File Quota	4096
Heartbeat Interval	5 (Keep the default setting.)
Failover Threshold	3 (Keep the default setting.)

4. Click *Apply*.

To change the network configuration so that the remote backup unit and the primary unit can communicate with each other:

Configure the appropriate firewalls or routers to allow HA heartbeat and synchronization traffic to pass between the primary unit and the remote backup unit using the peer IPs added to the primary unit and remote backup unit configurations.

HA traffic uses TCP port 5199.

To connect the cluster to the networks:

1. Connect the cluster units.
No special network configuration is required for the cluster.
2. Power on the cluster units.
The units start and use HA heartbeat packets to find each other, establish the cluster, and synchronize their configurations.

To add basic configuration settings to the cluster:

Configure the cluster to connect to your network as required.

Monitoring HA status

Go to *System Settings > HA* to monitor the status of the FortiManager units in an HA cluster. The FortiManager HA status pane displays information about the role of each cluster unit, the HA status of the cluster, and the HA configuration of the cluster.



The FortiManager GUI browser window title changes to indicate that the FortiManager unit is operating in HA mode. The following text is added to the title *HA (Group ID: <group_id>)*. Where <group_id> is the HA Group ID.



You can use the CLI command `get system ha` to display the same HA status information.

The following information is displayed:

Cluster Status	The cluster status can be <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.
Mode	The role of the FortiManager unit in the cluster. The role can be: <ul style="list-style-type: none"> • <i>Primary</i>: for the primary unit. • <i>Secondary</i>: for the backup units.
Module Data Synchronized	The amount of data synchronized between this cluster unit and other cluster units.
Pending Module Data	The amount of data waiting to be synchronized between this cluster unit and other cluster units.

Upgrading the FortiManager firmware for an operating cluster

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.

FortiManager support for FortiAnalyzer HA

You can manage FortiAnalyzer HA via FortiManager. FortiManager retrieves the cluster member list and updates the information whenever it changes, including FortiAnalyzer HA failover or a change in members.

To enable support for FortiAnalyzer HA:

1. Go to *Device Manager > Device and Groups*.
2. Click the down arrow next to *Add Devices*. Select *Add FortiAnalyzer*.

The Add FortiAnalyzer dialog opens.

Add FortiAnalyzer

Discover

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

IP Address: 10.3.121.202

Username: admin

Password: [masked]

Next > Cancel

3. From the *Add FortiAnalyzer* box, add FortiAnalyzer HA to FortiManager DVM by HA cluster's VIP, and click *Next*. The FortiAnalyzer HA is discovered with its HA status information. Click *Next* to continue.

Add FortiAnalyzer

The following information has been discovered from the device:

IP Address	10.3.121.202
Host Name	FAZVM64-HA
SN	FAZ-VMTM20001379
Model	FortiAnalyzer-VM64
Firmware Version	6.4.0, build5792 (GA)
HA Status	Active - Passive
Administrator	admin

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

Name: FAZVM64-HA

Description: [empty]

Next > Cancel

FortiAnalyzer HA is added successfully. Click *Finish*.

Add FortiAnalyzer

Status:

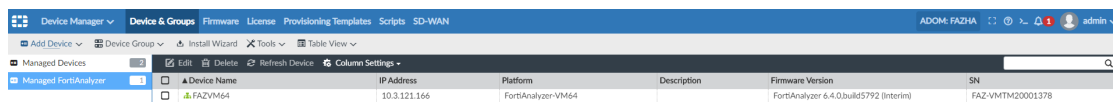
✓ FortiAnalyzer Added Successfully

Finish

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

Device Name	IP Address	Platform	Description	Firmware Version	SN
FAZVM64	10.3.121.202	FortiAnalyzer-VM64		FortiAnalyzer 6.4.0, build5792 (Interim)	FAZ-VMTM20001379

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



The screenshot shows the FortiManager GUI with the 'Managed FortiAnalyzer' table. The table has columns for Device Name, IP Address, Platform, Description, Firmware Version, and SN. A single device, FAZVM64, is listed with IP 10.3.121.166, Platform FortiAnalyzer-VM64, Description FortiAnalyzer 6.4.0.build5792 (Interim), and SN FAZ-VM64M20001378.

Device Name	IP Address	Platform	Description	Firmware Version	SN
FAZVM64	10.3.121.166	FortiAnalyzer-VM64		FortiAnalyzer 6.4.0.build5792 (Interim)	FAZ-VM64M20001378



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

To check the DVM device list in the CLI:

1. View the DVM device list once FortiAnalyzer HA is added to FortiManager:

```
diagnose dvm device list
```

It will have correct HA cluster information, including member list and role.

2. View the DVM device list after the failover on FortiAnalyzer:

```
diagnose dvm device list
```

It will have the updated HA cluster information. The previous primary changes to secondary and vice versa.

Management Extensions

The *Management Extensions* pane allows you to enable licensed applications that are released and signed by Fortinet. The following applications are available as management extensions to FortiManager:

- [SD-WAN Orchestrator](#)
Starting in FortiManager 6.4.1, you must be in a 6.4 ADOM to access the *SD-WAN Orchestrator* application in the *Management Extensions* pane.
- [FortiWLM on page 651](#)
You must be in the root ADOM to access the *FortiWLM* application in the *Management Extensions* pane.

The applications are installed and run on FortiManager.

See also [Enabling management extension applications on page 651](#).

SD-WAN Orchestrator

You can use SD-WAN Orchestrator to configure, manage, and monitor FortiGates in an SD-WAN network. For details about using SD-WAN Orchestrator, see the *SD-WAN Orchestrator Administration Guide* on the [Document Library](#).

When SD-WAN Orchestrator is enabled, the FortiManager configuration backup includes the configuration for SD-WAN Orchestrator too. See [Backing up the system on page 534](#).

When SD-WAN Orchestrator is enabled, you should use SD-WAN Orchestrator for all configuration of your SD-WAN network. You should not configure the SD-WAN network by using SD-WAN Orchestrator and the SD-WAN options available in the *Device Manager* module of FortiManager.

FortiWLM

You can use FortiWLM to monitor, operate, and administer wireless networks on FortiGates that are managed by FortiManager. For details about using FortiWLM, see the *FortiWLM Administration Guide* on the [Document Library](#).

When FortiWLM is enabled, the FortiManager configuration backup includes the configuration for FortiWLM too. See [Backing up the system on page 534](#).

When FortiWLM is enabled, you can use it to monitor your wireless network. You must configure the wireless network by using the *Device Manager* and *AP Manager* modules of FortiManager.

Enabling management extension applications

FortiManager provides access to applications that are released and signed by Fortinet.



Only administrators with a *Super_User* profile can enable management extensions.
A CA certificate is required to install management extensions on FortiManager. See [CA certificates on page 569](#).

To enable management extensions:

1. Go to *Management Extensions*.
The *FortiWLM* application is available only in the root ADOM, if ADOMs are enabled.
2. Click a grayed out tile to enable the application.
Grayed out tiles represent disabled applications. In the following example, SD-WAN Orchestrator is enabled, and FortiWLM is disabled.



3. Click *OK* in the dialog that appears. It might take some time to install the application.

CLI for management extensions

You can use the CLI console to enable, disable, update, debug, and check the management extension.

To enable management extensions:

1. Enable the production registry:

```
FMG-VM64 # config system docker
(docker)# set status
enable Enable production registry.
```
2. Enable the management application.

```
(docker)# set
status Enable and set registry.
sdwancontroller Enable/disable container.
```

To disable management extensions:

```
config system docker
(docker)# get
(docker)# set {fortiportal|sdwancontroller} disable
```

To update management extensions:

```
diagnose docker upgrade {fortiportal|sdwancontroller}
```

To debug management extensions:

```
diagnose debug application docker
```

To clean up or check management extensions:

```
diagnose docker {cleanup|status}
```

Appendix A - Supported RFC Notes

This section identifies the request for comment (RFC) notes supported by FortiManager.

RFC 2548

Description:

Microsoft Vendor-specific RADIUS Attributes

Category:

Informational

Webpage:

<http://tools.ietf.org/html/rfc2548>

RFC 3414

Description:

User-Based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).

Category:

Standards Track

Webpage:

<http://tools.ietf.org/html/rfc3414>

RFC 2665

Description:

Ethernet-like MIB parts that apply to FortiManager units.

Category:

Standards Track

Webpage:

<http://tools.ietf.org/html/rfc2665>

RFC 1213

Description:

MIB II parts that apply to FortiManager units.

Category:

FortiManager (SNMP)

Webpage:

<http://tools.ietf.org/html/rfc1213>

Notes

RFC support for SNMP v3 includes Architecture for SNMP Frameworks (as described in [RFC 3411](#)). Generic Fortinet traps : ColdStart, WarmStart, LinkUp, LinkDown (as described in [RFC 1215](#)).